CRYPTOCURRENCY TRANSACTION ANALYSIS FROM A NETWORK PERSPECTIVE

EDITED BY: Zhong-Yuan Zhang, Jianguo Liu, Xiao Fan Liu and Cuneyt Gurcan Akcora

PUBLISHED IN: Frontiers in Physics

frontiers Research Topics

frontiers

ISSN 1664-8714
ISBN 978-2-88976-799-1
DOI 10.3389/978-2-88976-799-1

About Frontiers

Frontiers is more than just an open-access publisher of scholarly articles: it is a pioneering approach to the world of academia, radically improving the way scholarly research is managed. The grand vision of Frontiers is a world where all people have an equal opportunity to seek, share and generate knowledge. Frontiers provides immediate and permanent online open access to all its publications, but this alone is not enough to realize our grand goals.

Frontiers Journal Series

The Frontiers Journal Series is a multi-tier and interdisciplinary set of open-access, online journals, promising a paradigm shift from the current review, selection and dissemination processes in academic publishing. All Frontiers journals are driven by researchers for researchers; therefore, they constitute a service to the scholarly community. At the same time, the Frontiers Journal Series operates on a revolutionary invention, the tiered publishing system, initially addressing specific communities of scholars, and gradually climbing up to broader public understanding, thus serving the interests of the lay society, too.

Dedication to Quality

Each Frontiers article is a landmark of the highest quality, thanks to genuinely collaborative interactions between authors and review editors, who include some of the world's best academicians. Research must be certified by peers before entering a stream of knowledge that may eventually reach the public - and shape society; therefore, Frontiers only applies the most rigorous and unbiased reviews.
Frontiers revolutionizes research publishing by freely delivering the most outstanding research, evaluated with no bias from both the academic and social point of view. By applying the most advanced information technologies, Frontiers is catapulting scholarly publishing into a new generation.

What are Frontiers Research Topics?

Frontiers Research Topics are very popular trademarks of the Frontiers Journals Series: they are collections of at least ten articles, all centered on a particular subject. With their unique mix of varied contributions from Original Research to Review Articles, Frontiers Research Topics unify the most influential researchers, the latest key findings and historical advances in a hot research area! Find out more on how to host your own Frontiers Research Topic or contribute to one as an author by contacting the Frontiers Editorial Office: frontiersin.org/about/contact

CRYPTOCURRENCY TRANSACTION ANALYSIS FROM A NETWORK PERSPECTIVE

Topic Editors:
Zhong-Yuan Zhang, Central University of Finance and Economics, China
Jianguo Liu, Shanghai University of Finance and Economics, China
Xiao Fan Liu, City University of Hong Kong, SAR China
Cuneyt Gurcan Akcora, University of Manitoba, Canada

Citation: Zhang, Z.-Y., Liu, J., Liu, X. F., Akcora, C. G., eds. (2022). Cryptocurrency Transaction Analysis From a Network Perspective. Lausanne: Frontiers Media SA. doi: 10.3389/978-2-88976-799-1

Table of Contents

frontiers in Physics

EDITORIAL
published: 21 March 2022
doi: 10.3389/fphy.2022.876983

Editorial: Cryptocurrency Transaction Analysis From a Network Perspective

Xiao Fan Liu[1], Cuneyt Gurcan Akcora[2], Zhong-Yuan Zhang[3] and Jian-Guo Liu[4]*

[1]Department of Media and Communication, City University of Hong Kong, Kowloon, Hong Kong SAR, China, [2]Department of Computer Science, University of Manitoba, Winnipeg, MB, Canada, [3]School of Statistics and Mathematics, Central University of Finance and Economics, Beijing, China, [4]Institute of Accounting and Finance, Shanghai University of Finance and Economics, Shanghai, China

Keywords: cryptocurrency, blockchain analytics, bitcoin, ethereum, network science

Editorial on the Research Topic

Cryptocurrency Transaction Analysis From a Network Perspective

The past 2 years have seen a surge of research articles themed on cryptocurrency analytics [1]. We are glad that our research topic, Cryptocurrency Transaction Analysis from a Network Perspective, which consists of nine novel contributions, can join this exciting trend and has already drawn attention from academia and industry.

There are two common data sources available for cryptocurrency analytics. The first is blockchain data. Public blockchains, such as Bitcoin and Ethereum, store transactions transparently in an open database. With a bit of effort unpacking the transactions from a compact storage format, one can readily use network science methods and machine learning tools to mine for knowledge, be it regulatory intelligence or market signal. The second is market information. The quotation ticks and trading volumes of the 10,000 + cryptocurrencies and tokens traded in many centralized and decentralized exchanges are curated by market monitoring sites like coinmarketcap. These data enable insightful research of the cryptocurrency market's risk and potential market manipulation activities. Articles in our research topic cover both lines of work with significant findings.

A fundamental property of cryptocurrency systems' public-key-private-key design is that the pseudonyms, i.e., blockchain addresses, recorded in the database cannot be associated with any physical identity, such as an IP address or email address. However, various heuristic algorithms have been proposed to "link" addresses together, that is, to associate multiple blockchain addresses to the same holder. Fischer et al. integrated a spectrum of address-linking algorithms and used a network-based clustering method to synthesize a new method that can reliably associate the addresses.

Another fundamental property of blockchain data is traceability, i.e., one can trace the genuine money flow through a chain of addresses. Naturally, crypto services that deliberately obfuscate such traceability, also known as mixing services, have been created for laundering (often illicit) money. Liu et al. proposed a conceptual modeling framework to analyze the different roles of blockchain addresses in the bitcoin mixing services. Their model helped find and characterize the organizer, soldiers, and communicators in a money laundering case study.

The cryptocurrency transactions can be viewed as a complex network in which the blockchain addresses are the nodes, and the money flow in the transactions are the edges linking the nodes. As a constantly expanding network, physicists are interested in the underlying mechanism of its growth. Preferential attachment [2] is one of the most prominent governing growth mechanisms of many natural and man-made complex networks, as well as bitcoin [3]. Collibus et al. showed that Ethereum and its most market-capitalized ERC-20 token habitants Binance, USDT, and Chainlink also obey such law, but with a super-linear variance.

Edited and reviewed by:
Matjaž Perc,
University of Maribor, Slovenia

****Correspondence:***
Xiao Fan Liu
xf.liu@cityu.edu.hk

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *16 February 2022*
Accepted: *28 February 2022*
Published: *21 March 2022*

Citation:
Liu XF, Akcora CG, Zhang Z-Y and Liu J-G (2022) Editorial: Cryptocurrency Transaction Analysis From a Network Perspective. Front. Phys. 10:876983. doi: 10.3389/fphy.2022.876983

From a machine learning perspective, the network structure of transaction data helps construct rich features for downstream tasks, such as inferring the identities of blockchain addresses. Lin et al. constructed a transaction network from Ethereum transactions with temporal and weighted edges to capture the network topology evolution. By applying graph embedding algorithms on this dynamic network, they are able to recognize labeled phishing addresses from others.

The article that attracted the most attention (more than 25 k online views) as of February 2022 is Jiang and Liu's analysis of the CryptoKitties game's transaction history. They characterized the evolution of the transaction network and proposed several reasons why the game gained sudden attention from players but also collapsed quickly, just within 1 month. Their suggestions to blockchain game design may shed light on the current development of the non-fungible token (NFT) industry.

Volatility is a rate that describes the price change of an asset over a particular period. It is a fundamental indicator guiding cryptocurrency investments. Can volatility be predicted from market signals? The answer is positive and definite. Barjašić and Antulov-Fantulin found that bitcoin-related tweets, bitcoin trade volume, and bid-ask spread can be incorporated into generalized autoregressive conditional heteroscedasticity (GARCH) models to predict volatility.

If two assets are affected by similar market factors, they may experience a synchronized price trend or volatility level. The latter case is also called volatility connectedness or volatility spillover. The current global cryptocurrency market is still in its early development. One crypto asset can be traded in multiple exchanges, and each exchange may have different asset listings and price momentum. The intertwined market is indeed highly interconnected, volatility-wise. Chen and Dong's analysis of six bitcoin-fiat money pairs and Li et al. examination of seven major cryptocurrencies all found volatility spillover effects. Liu and Liu found that if two crypto projects share the same investors or similar market embeddedness, as measured by the structural properties in a co-investment network, they may also share similar market performance, including volatility and others. The strong spillover effects imply the ineffectiveness of the cryptocurrency market.

We believe that the research on cryptocurrencies will continue to prosper in the coming years as the market develops. We hope that the series of articles that we have collected here can serve as a bedrock for the future development of cryptocurrency analytics. Finally, we would like to take this chance and thank all the authors and reviewers for your contribution. We also refer the readers to some sister issues in Frontiers in Blockchain: Blockchain Through the Lens of Network Science and Non-Financial Applications of Blockchains: Systematizing the Knowledge that address similar research topics.

AUTHOR CONTRIBUTIONS

XFL wrote the editorial, CGA, Z-YZ, and J-GL edited.

REFERENCES

1. Liu XF, Jiang X-J, Liu S-H, Tse CK. Knowledge Discovery in Cryptocurrency Transactions: A Survey. *IEEE Access* (2021) 9:37229–54. doi:10.1109/ACCESS.2021.3062652
2. Barabási AL, Albert R. Emergence of Scaling in Random Networks. *Science* (1999) 286(5439):509–12.
3. Kondor D, Pósfai M, Csabai I, Vattay G. Do the Rich Get Richer? an Empirical Analysis of the Bitcoin Transaction Network. *Plos One* (2014) 9:e86197. doi:10.1371/journal.pone.0086197

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 30 June 2020
doi: 10.3389/fphy.2020.00204

T-EDGE: Temporal WEighted MultiDiGraph Embedding for Ethereum Transaction Network Analysis

Dan Lin[1,2], *Jiajing Wu*[1,2]*, *Qi Yuan*[1,2] *and Zibin Zheng*[1,2]

[1] School of Data and Computer Science, Sun Yat-sen University, Guangzhou, China, [2] National Engineering Research Center of Digital Life, Sun Yat-sen University, Guangzhou, China

Recently, graph embedding techniques have been widely used in the analysis of various networks, but most of the existing embedding methods omit the network dynamics and the multiplicity of edges, so it is difficult to accurately describe the detailed characteristics of the transaction networks. Ethereum is a blockchain-based platform supporting smart contracts. The open nature of blockchain makes the transaction data on Ethereum completely public and also brings unprecedented opportunities for transaction network analysis. By taking the realistic rules and features of transaction networks into consideration, we first model the Ethereum transaction network as a Temporal Weighted Multidigraph (TWMDG) where each node is a unique Ethereum account and each edge represents a transaction weighted by amount and assigned a timestamp. We then define the problem of Temporal Weighted Multidigraph Embedding (T-EDGE) by incorporating both temporal and weighted information of the edges, the purpose being to capture more comprehensive properties of dynamic transaction networks. To evaluate the effectiveness of the proposed embedding method, we conduct experiments of node classification on real-world transaction data collected from Ethereum. Experimental results demonstrate that T-EDGE outperforms baseline embedding methods, indicating that time-dependent walks and the multiplicity characteristic of edges are informative and essential for time-sensitive transaction networks.

Keywords: network embedding, ethereum, machine learning, temporal network, transaction network

OPEN ACCESS

Edited by:
Jianguo Liu,
Shanghai University of Finance and Economics, China

Reviewed by:
Shiyuan Wang,
Southwest University, China
Yongxiang Xia,
Hangzhou Dianzi University, China
Zhihai Rong,
University of Electronic Science and Technology of China, China

***Correspondence:**
Jiajing Wu
wujiajing@mail.sysu.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *25 March 2020*
Accepted: *11 May 2020*
Published: *30 June 2020*

Citation:
Lin D, Wu J, Yuan Q and Zheng Z (2020) T-EDGE: Temporal WEighted MultiDiGraph Embedding for Ethereum Transaction Network Analysis. Front. Phys. 8:204. doi: 10.3389/fphy.2020.00204

1. INTRODUCTION

The network is a kind of data form that is often used to describe the relationship between objects. The past decade has witnessed an explosive growth in network data, which have been used to present information in various areas, such as social networks, biological networks, computer networks, and financial transaction networks [1]. Analysis of large-scale networks has attracted increasing attention from both academia and industry. With the rapid development of machine learning technology, the question of how to analyze the data effectively for large-scale complex networks is becoming a hot topic in the field of artificial intelligence.

Financial transaction networks are widespread in the real world. However, there have been relatively few analytical studies on financial transaction networks because the transaction data are usually private for the sake of security and interest. Fortunately, the recent emergence of

blockchain technology makes transaction data mining more feasible and reliable. Blockchain is a new technology that is described as an innovative application mode of distributed data storage, peer-to-peer transmission, consensus mechanisms, encryption algorithms, and other computer technologies in the Internet era [2, 3]. Generally speaking, blockchain is a new distributed ledger, and the transaction data is stored on the chain in chronological order. Ethereum [4] is the largest blockchain platform that supports smart contracts. The Ethereum system introduces the concept of *account* and allocates storage space for recording account balance, transaction time, codes, etc. Compared with a traditional database, blockchain technology naturally has the characteristics of traceability, anti-tampering, and publicity. The openness of public blockchain provides favorable conditions for transaction data mining [5].

In fact, cryptocurrency and blockchain are highly coupled, since blockchain technology is born from Bitcoin. The study of cryptocurrency transaction networks has very high application value and there have already been some studies, including graph analysis, price prediction, portfolio management, anti-market manipulation, ponzi scheme detection, and so on [6–12]. In 2013, Ron et al. [6] described Bitcoin schemes and investigated a large number of statistical properties of the full Bitcoin transaction network. By analyzing the subgraph of the largest transactions, they revealed several characteristics in the Bitcoin transaction graph: long chains, fork-merge patterns with self-loops, keeping bitcoins in "savings accounts," and binary tree-like distributions. In 2017, Jiang and Liang [7] presented a deterministic deep reinforcement learning method for cryptocurrency portfolio management. The trading algorithm takes the historical prices of a set of financial assets as input and outputs the portfolio weights of the set. In 2018, Liang et al. [8] traced the properties of three representative cryptocurrencies, Bitcoin, Ethereum, and Namecoin, over time and characterized their dynamics by constructing a monthly transaction network.

Since it is extremely time-consuming to process the whole blockchain transaction network, it is necessary to find an effective and efficient way to analyze Ethereum transaction data. As we know, the performance of machine learning tasks depends to a large extent on the selection of data features, so a key problem is how to reasonably represent the feature information in large-scale transaction networks. In addition, using a machine learning-based algorithm often requires feature information for samples, but the account profiles of the transaction networks are often difficult to obtain. The implicit characteristics of the accounts can be mined by means of graph embedding algorithms.

Graph embedding is an effective method for representing node features in a low-dimensional space for network analysis and downstream machine learning tasks [13]. Graph embedding algorithms can effectively reduce the data dimension of the transaction network and transform the large-scale and sparse high-dimensional one-hot node vectors into dense low-dimensional node vectors. Previous graph embedding research has been conducted in domains, such as social networks, language networks, citation networks, collaboration networks, webpage networks, biological networks, communication networks, and traffic networks [13]. This implies that existing graph embedding techniques may not be suitable for a transaction network. Using the traditional network embedding algorithm for transaction network analysis will present the following challenges. New transactions are generated over time, but existing methods ignore the multiplicity and dynamics of transactions. Random walks in transaction networks are meaningful and sequential, but existing methods based on social networks, like DeepWalk and node2vec, do not incorporate temporal information.

The random walk mechanism has been widely proved to be an effective technique for measuring the local similarity of networks for a variety of domains [14]. Among various graph embedding methods, a series of random-walk based approaches have been proposed for learning a mapping function from an original graph to a low-dimensional vector space by maximizing the likelihood of co-occurrence of neighbor nodes. For the traditional graph embedding method, DeepWalk [15], it was verified through experiments that nodes in the random walk sequence and words in the document all follow the power-law, so word2vec [16] was applied to learn node representations. Similar to DeepWalk, node2vec [17] introduced biased random walks, which smoothly search between breadth-first sampling and depth-first sampling strategies. Recently, to better extract temporal information from dynamic networks, Nguyen et al. [18] proposed a general framework called Continuous-Time Dynamic Network Embeddings (CTDNE) to incorporate temporal dependencies into existing random walk-based network embedding models. However, these previous methods omit the network dynamics and the multiplicity of edges, so it is difficult to accurately describe the detailed characteristics of the transaction networks.

To this end, to capture more comprehensive properties of dynamic transaction networks, we propose a novel framework named ***T**emporal W**E**ighted Multi**D**i**G**raph **E**mbedding* (T-EDGE) for the Ethereum transaction network. The main contributions of our paper are as follows:

- To the best of our knowledge, this is the *first* work to understand Ethereum transaction records via graph embedding, aiming to capture the non-negligible temporal properties and important money-transfer tendencies of time-sensitive transaction networks.
- We propose a novel graph embedding method called Temporal Weighted Multidigraph Embedding (T-EDGE), which incorporates transaction information from both time and amount domains, and experiments on realistic Ethereum data demonstrate its superiority over existing methods.
- To evaluate our proposed algorithm, we consider an important and practical machine learning task, namely node classification with transaction records of phishing and non-phishing accounts collected from Ethereum. The dataset can be accessed on XBlock (xblock.pro).

The remainder of this paper is organized as follows. First, section 2 demonstrates our workflow for Ethereum transaction network analysis. Then, section 3 describes how we model

the transaction records as a temporal weighted multidigraph. Then, we introduce our proposed network embedding algorithm, T-EDGE, in section 4 and evaluate our algorithm by conducting node classification in section 5. Finally, section 6 concludes the paper.

2. FRAMEWORK

In this section, we describe the workflow of Ethereum transaction network analysis presented in this work. As **Figure 1** shows, the four main steps of the proposed framework for Ethereum transaction network analysis are data acquisition, network construction, graph embedding, and downstream tasks.

(a) Data acquisition. The data collection is the basis of transaction network analysis. Thanks to the openness of blockchain, researchers are able to autonomously access Ethereum transaction records. Through the API of Etherscan (etherscan.io), a block explorer and analytics platform for Ethereum, we can easily obtain the historical transaction data of the target account. As the size of the total transaction records is extremely large, we adopt the K-order subgraph sampling method [19], to obtain the local structure of the target accounts.

(b) Network construction. This step abstracts the original transaction record into a network structure for further analysis. In most existing studies on blockchain transaction networks, the transaction networks are constructed as simple graphs, that is, multiple transactions between a pair of accounts are merged into one edge, thus ignoring the multiplicity and dynamics of transactions between accounts. Differently from prior work, in this work, we model the multiple interactions between accounts as a Temporal Weighted Multidigraph [19] to facilitate a more comprehensive analysis of transaction behaviors.

(c) Graph embedding. In the framework of Ethereum transaction network analysis, the role of network embedding is to mine the implicit features of accounts in the transaction network and reduce the transaction data dimension. In order to learn the meaningful node representation vectors in the dynamic transaction network, we propose an improved embedding algorithm called Temporal Weighted Multidigraph Embedding (T-EDGE) based on temporal random walk. T-EDGE aims to capture the time and amount information that cannot be ignored in the Ethereum transaction network.

(d) Downstream tasks. We evaluate our model by conducting experiments on a typical machine learning task, namely node classification. Good performance of the downstream tasks reflects the effectiveness of embedding methods. Besides, analytical applications can be regarded as the ultimate goal of the Ethereum transaction network embedding. In this paper, we incorporate two current hot topics—cryptocurrency transaction analysis and machine learning, and use machine learning technology to help us make more accurate predictions about the future of the Ethereum transaction network.

3. ETHEREUM TRANSACTION NETWORK

Being the largest public blockchain-based platform that supports smart contracts, Ethereum introduces the concept of *account* to facilitate the implementation of smart contracts. An Ethereum account is formally an address but adds storage space for recording account balances, transactions, codes, etc. Ethereum addresses are composed of the prefix "0x," a common identifier for hexadecimal, concatenated with the rightmost 20 bytes of the public key. One example is: "0x00b2ed34791c97206943314ee9cbd9530762a320." The corresponding cryptocurrency on Ethereum, known as *Ether*, can be transferred between accounts and used to compensate participant mining nodes.

The Ethereum blockchain consists of infinite linked blocks, which can be viewed as data-packages, including a series of transactions and some other information. In detail, the transaction data packages obtained from the Etherscan website are as followed: the *TxHash* field is a unique 66-character identifier of a transaction, the *Value* field is the value being transacted in Ether, and the *Timestamp* field is the time at which a transaction is mined. Besides, the *From* and *To* fields are the sending party and receiving party of a transaction, respectively.

In this section, we abstract the original transaction record as a Temporal Weighted Multidigraph (TWMDG). **Figure 2** is a microcosm of transaction activities on Ethereum. In prior work on blockchain transaction network analysis, the transaction network was constructed as a simple network, that is, multiple transactions between nodes were accumulated as one edge. The multiplicity and dynamics of transactions between accounts were ignored. Therefore, we adopt Temporal Weighted Multidigraph (TWMDG) to represent Ether transfer between accounts more comprehensively.

Based on collected four-tuples *(From, To, Value, Timestamp)*, we can model the Ethereum transaction records as a Temporal Weighted Multidigraph $G = (V, E)$, where each node represents a unique account and each edge represents a unique Ether transfer transaction. In such a graph, V is the set of nodes and E is the set of edges. Each edge is unique and is represented as $e = (u, v, w, t)$, where u is the source node, v is the target node, w is the weight value and t is the timestamp.

4. NETWORK EMBEDDING

In the analysis of the Ethereum transaction network, our goal is to learn an embedding vector for each node, the purpose being to mine the implicit characteristics of nodes in the transaction network and incorporate the time and amount information of the transaction network into the node vector. For the network model TWMDG built in the previous section, this paper proposes

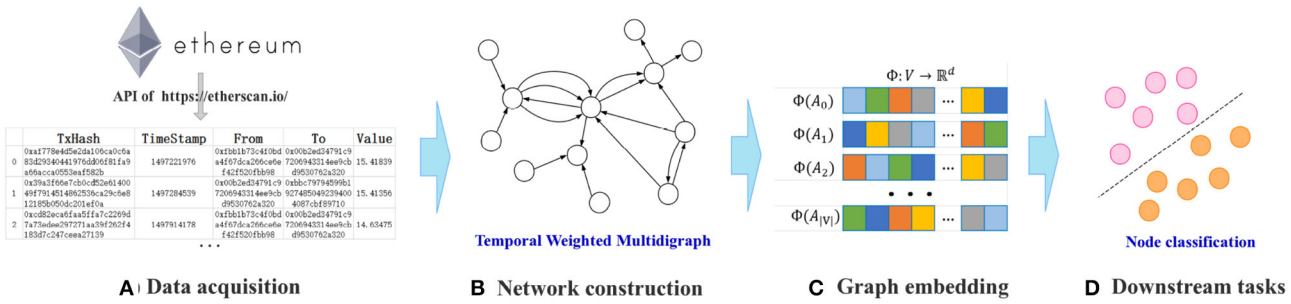


FIGURE 1 | The architecture of the proposed framework for network analysis of Ethereum.

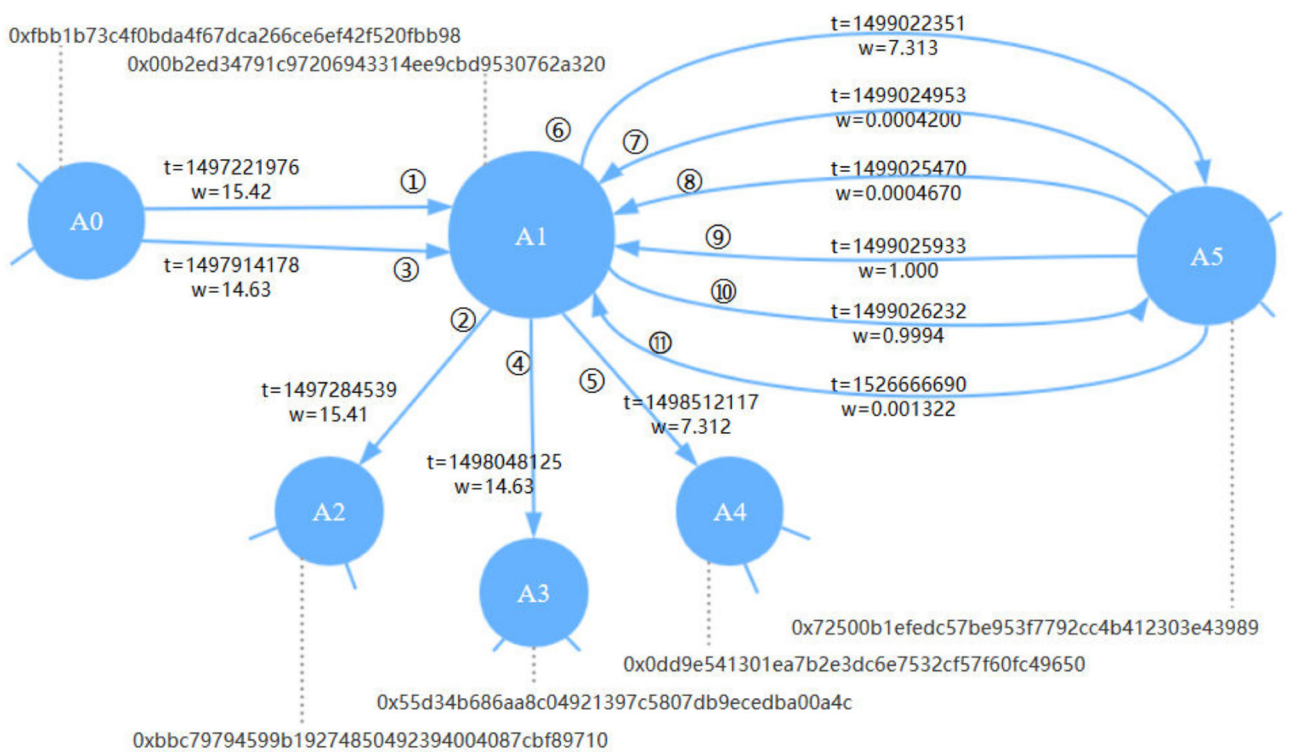


FIGURE 2 | Schematic of the Ethereum transaction network. Each node represents an Ethereum account. Each edge represents a transaction, with a timestamp *t* and amount value *w* (in *Ether*) attached to it and indexed in increasing order of *t*.

an improved network embedding algorithm based on a random walk. We now define the specific problem as follows.

Temporal WEighted MultiDiGraph Embedding (T-EDGE): Given a temporal weighted multidigraph $G = (V, E)$, let V be the set of nodes and E be the set of edges. Each edge is unique and is represented as $e = (u, v, t, w)$, where u is the source node, v is the target node, t is the timestamp, and w is the weight (Specifically, w is the amount value of a transaction in Ethereum transaction network). We define the following mapping functions: for $\forall e \in E$, $Src(e) = u$, $Dst(e) = v$. Function $W(e) = w$ maps an edge to its weight, and function $T(e) = t$ maps an edge to its timestamp. Our principal goal is to learn an embedding function $\Phi : V \rightarrow \mathbb{R}^d$ ($d \ll |V|$) that preserves the original network information.

The learned representations aim to include node similarity as well as temporal and weighting properties specifically for financial transaction networks, thus enhancing predictive performance on downstream machine learning tasks. The proposed method, T-EDGE, learns more appropriate and meaningful dynamic node representations using a general embedding framework consisting of two main parts:

- The first part is the temporal walk generator with temporal restriction and walking strategies.
- The second part is the update process based on skip-gram, and the parameters are updated by a Stochastic Gradient Descent algorithm.

4.1. Random Walk

For scalable network representation learning, the random walk mechanism has been widely proven to be an effective technique for capturing structural relationships between nodes [15]. We employ a temporal walk for transaction networks by considering temporal dependencies and multiplicity of edges. This kind of random walk sequence contains the practical meaning of money flow in transaction networks.

In a temporal weighted multidigraph, the *temporal walk* is defined as the sequential incremental path from the beginning node to the end node. Such a temporal walk is represented as a sequence of l nodes $walk_n = \{v_1, v_2, ..., v_l\}$ together with a sequence of $(l-1)$ edges $walk_e = \{e_1, e_2, ..., e_{l-1}\}$, where $Src(e_i) = v_i$, $Dst(e_i) = v_{i+1}$ $(1 \leq i \leq (l-1))$, and $T(e_i) \leq T(e_{i+1})$ $(1 \leq i \leq (l-2))$. This temporal restriction is a novel idea designed for the temporal walk.

Consider a temporal walk that just traversed edge e_{i-1} and is now stopping at node v_i at time $t = T(e_{i-1})$. The next node v_{i+1} of the random walk is decided by selecting a temporally valid edge e_i. We define the *temporal edge neighborhood* for a node u as $N_t(u) = \{e \mid Src(e) = u, T(e) \geq t\}$. Let $\eta_- : \mathbb{R} \to \mathbb{Z}^+$ to be a function that maps the timestamps of edges to a descending ranking, and let $\eta_+ : \mathbb{R} \to \mathbb{Z}^+$ be a function that maps the timestamps of edges to an ascending ranking. Here are our walking strategies used in Ethereum transaction network embedding.

4.1.1. T-EDGE

In the temporal weighted multidigraphs discussed here, a random walk generator of T-EDGE samples uniformly from the neighbors. All candidate edges in N_t have the same probability of being selected as the next edge of the random walk. The expression of the probability is

$$P(e) = \frac{1}{|N_t(v_i)|}. \tag{1}$$

4.1.2. T-EDGE (TBS)

TBS refers to Temporal Biased Sampling. For financial transaction networks, the similarity between accounts is time-dependent and dynamic. Naturally, there is a strong transaction relationship between accounts with frequent transactions. The probability of selecting each edge $e \in N_t(v_i)$ can be given as:

$$P(e) = P_{TBS}(e) = \frac{\eta_-(T(e))}{\sum_{e' \in N_t(v_i)} \eta_-(T(e'))}. \tag{2}$$

4.1.3. T-EDGE (WBS)

WBS refers to Weighted Biased Sampling. The weight value of each transaction indicates the significance of interactions between the two accounts involved. The transaction amount can reflect the importance of transactions between accounts and then reflect the degree of correlation between accounts. In most cases, there is a strong similarity between accounts with a large amount of transactions. The probability of each edge $e \in N_t(v_i)$ being selected is

TABLE 1 | Four types of T-EDGE variation for the Ethereum transaction network.

Algorithms	Time domain		Amount domain	
	Unbiased	Biased	Unbiased	Biased
T-EDGE	√		√	
T-EDGE (TBS)		√	√	
T-EDGE (WBS)	√			√
T-EDGE (TBS+WBS)		√		√

$$P(e) = P_{WBS}(e) = \frac{\eta_+(W(e))}{\sum_{e' \in N_t(v_i)} \eta_+(W(e'))}. \tag{3}$$

4.1.4. T-EDGE (TBS+WBS)

We combine the aforementioned sampling probabilities considering information from both temporal and weighted domains by

$$P_{TBS+WBS}(e) = P_{TBS}(e)^{\alpha} P_{WBS}(e)^{(1-\alpha)}, (0 \leq \alpha \leq 1), \tag{4}$$

$$P(e) = \frac{P_{TBS+WBS}(e)}{\sum_{e' \in N_t(v_i)} P_{TBS+WBS}(e')}, \tag{5}$$

for $\forall e \in N_t(v_i)$. Here, $\alpha = 0.5$ is the default value for balancing between TBS (time domain) and WBS (amount domain).

When ending up with a leaf node, we return the walk immediately. This setting is just the same as in the methods used for comparison, DeepWalk and node2vec.

Note that T-EDGE can be regarded as a specific version of DeepWalk for temporal and directed multigraphs like the transaction networks. As **Table 1** shows, all candidate edges (temporal edge neighborhood) are equally likely to be selected by T-EDGE. T-EDGE (TBS) and T-EDGE (WBS) denote adding sampling preference on the time domain and the amount domain, respectively. T-EDGE (TBS+WBS) means adding sampling preference on both the time domain and the amount domain.

4.2. Learning Process

In the previous subsection, we described how to get the sampling sequence of temporal walk related to time and weight. In this part, we will formally describe the process of learning node vectors using the skip-gram model [16, 20].

The essence of the skip-gram model is a three-layer neural network model, including an input layer, hidden layer, and output layer. First, we train a neural network model based on the sampling walk sequences, but the purpose of training is not to use the model to predict the test set but to use the parameters learned from the model, namely the hidden layer parameters, as our node vectors. Then, by making an analogy between a natural language sentence and a truncated random walk sequence (as shown in **Table 2**), node representations are learned by maximizing the

TABLE 2 | Comparison between language model word2vec and graph model Deepwalk.

Research domain	Example	Input	Output
Natural language processing	word2vec	Sequence of word (sentences)	Word vectors
Graph representation learning	deepwalk	Sequence of nodes (random walks)	Node vectors

probability of observing the neighborhood of a node conditioned on its embedding. This cost function is as follows:

$$\min_{\Phi} -\Pr(\{v_{i-k},...,v_{i+k}\}\backslash v_i|\Phi(v_i)), \tag{6}$$

where k is the window size. According to the conditional independent assumption in the skip-gram model, we have:

$$\Pr(\{v_{i-k},...,v_{i+k}\}\backslash v_i|\Phi(v_i)) = \prod_{j=i-k,j\neq i}^{i+k} \Pr(v_j|\Phi(v_i)). \tag{7}$$

Similar to DeepWalk, we employ the "hierarchical softmax" technique [15] to accelerate the computation of $\Pr(v_j|\Phi(v_i))$. We first apportion $|V|$ nodes to the leaf nodes of a Huffman Tree and then transform the computation of $\Pr(v_j|\Phi(v_i))$ into computing the probability of walking randomly from the root of the Huffman Tree with inputting node v_i and outputting node v_j. The probability is

$$\Pr(v_j|\Phi(v_i)) = \prod_{t=1}^{\lceil \log|V| \rceil} \Pr(b_t|\Phi(v_i)), \tag{8}$$

where b_t is from $\{b_0 = root, b_1, ..., b_{\lceil \log|V| \rceil} = v_j\}$. We then model $\Pr(b_t|\Phi(v_i)$ with a *sigmoid* function:

$$\Pr(b_t|\Phi(v_i) = \frac{1}{1+\exp(-\Phi(v_i)\cdot\Phi(b_{t-1}))}, \tag{9}$$

where $\Phi(b_{t-1})$ is the representation of b_t's parent node in the Huffman tree. The skip-gram model then uses a back-propagation algorithm and Stochastic Gradient Descent to update the weight.

Random walk-based graph embedding methods have been proved to be scalable and effective for large graphs. The time complexity of the temporal walk part and the skip-gram learning procedure is $O(r|V|L)$ and $O(|V|\log|V|)$, respectively, where $|V|$ is the number of nodes, r denotes walks per node, and L refers to the length of random walk.

5. EXPERIMENTS AND RESULTS

Downstream tasks, such as node classification are commonly considered for the verification of graph embedding methods. To evaluate the performance of the proposed T-EDGE algorithms, we conduct node classification experiments to classify the labeled phishing accounts and unlabeled accounts (treated as non-phishing accounts) on Ethereum. The better performance of classification demonstrates that our T-EDGE algorithms outperform baseline embedding methods, and at the same time, node classification for detecting phishing accounts on Ethereum is also of great value. A phishing scam is a new type of cybercrime that arises along with the emergence of online business [21]. It is reported to account for more than 50% of all cyber-crimes on Ethereum since 2017 [22].

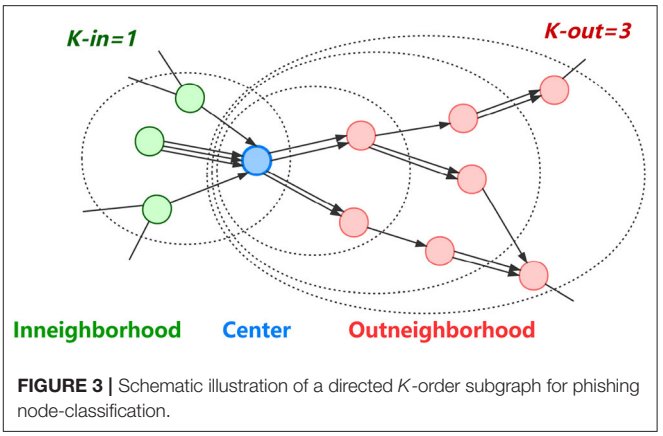


FIGURE 3 | Schematic illustration of a directed K-order subgraph for phishing node-classification.

5.1. Data Acquisition

To train our node classification model using supervised learning, we obtain 445 phishing nodes labeled by Etherscan and the same number of randomly selected unlabeled nodes as our objective nodes.

K-order sampling is an effective method for obtaining the local information of objective accounts [19]. Centered by each objective account, we obtain a directed K-order subgraph, where K-in and K-out are two parameters for controlling the depth of sampling inward and outward from the center, respectively. As shown in **Figure 3**, we make an assumption that for a typical *Ether* transfer flow centered on a phishing node, the previous node of the phishing node may be a victim, and the next one to three nodes may be bridge nodes with money-laundering behaviors. Therefore, we collect subgraphs with K-in = 1, K-out = 3 for each of the 890 objective nodes and then splice them into a large-scale network with 86,623 nodes.

5.2. Setting

In the experiments, we compare the proposed T-EDGE algorithms with two baseline random walk-based graph embedding methods:

- **DeepWalk** is the pioneering work in employing random walks to learn a latent space representation of social interactions. Borrowing the idea of word2vec, the learned representation encodes community structure so that it can be easily exploited by standard classification methods [15].

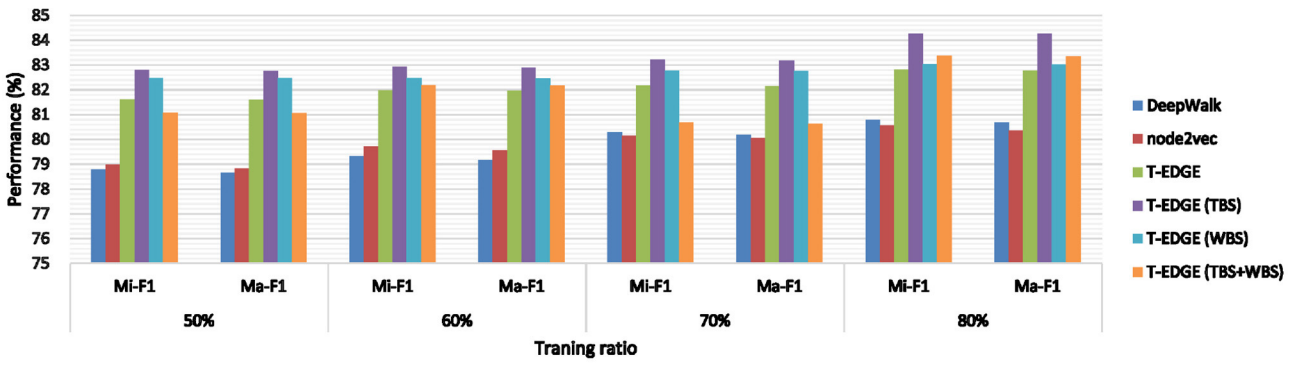


FIGURE 4 | Node classification performance with different training ratios.

- **Node2vec** further exploits a flexible neighborhood sampling strategy, i.e., Breadth-First Sampling (BFS) and Depth-First Sampling (DFS), with parameters p and q to capture both local and global structure [17].

To ensure a fair comparison, we implement the directed versions of DeepWalk and node2vec using OpenNE (an open-source package for network embedding, github.com/thunlp/openne). For these random walk-based embedding methods, we set several hyperparameters: the node embedding dimension $d = 128$, the size of window $k = 4$, the length of walk $l = 10$, and walks per node $r = 4$. For node2vec, we grid search over $p, q \in \{0.50, 1.0, 1.5, 2.0\}$ according to [17]. For DeepWalk, we set $p = q = 1.0$, as it is a special case of node2vec. We implement the skip-gram model by using a Python library named Gensim [23], a framework for fast Vector Space Modeling.

5.3. Metrics

To make a comprehensive evaluation, we randomly select {50%, 60%, 70%, 80%} of the objective nodes as a training set and the remaining objective nodes as the test set, respectively. We train a classic binary classifier, namely, a Support Vector Machine (SVM), with the training set to classify the samples of the test set. Note that we use 5-fold cross-validation to train the classifier and evaluate it on the test set.

For a binary classification task based on a supervised learning framework, it can be divided into the following four cases according to the actual labels of the samples and the prediction results of the classifier.

- True Positive (TP): Samples whose labels are positive and are also predicted to be positive.
- True Negative (TN): Samples whose labels are positive but are predicted to be negative.
- False Positive (FP): Samples whose labels are negative but are predicted to be positive.
- False Negative (FN): Samples whose labels are negative and are also predicted to be positive.

In classification tasks, micro-F1 (Mi-F1) and macro-F1 (Ma-F1) are generally used to evaluate classification accuracy. First, we have

- *precision*: $\frac{TP}{TP+FP}$,
- *recall*: $\frac{TP}{TP+FN}$.

F1-score is an indicator used to measure the accuracy of the binary classification model. The calculation formula is

$$2 \times \frac{precision \times recall}{precision + recall}. \tag{10}$$

Macro-F1 refers to calculating the total *precision* and *recall* of all categories for F1-score, while Micro-F1 refers to the calculation of F1-score after calculating the average of *precision* and *recall* for each category.

5.4. Results

The results of micro-F1 (Mi-F1) and macro-F1 (Ma-F1) are shown in **Figure 4**. According to **Figure 4**, we have the following observations:

1. Our proposed methods T-EDGE, T-EDGE (TBS), T-EDGE (WBS), and T-EDGE (TBS+WBS) overwhelmingly outperform DeepWalk and node2vec;
2. Both T-EDGE (TBS) and T-EDGE (WBS) attain better performance than T-EDGE, in which the random walk generator has uniform probability;
3. Both T-EDGE (TBS) and T-EDGE (WBS) perform better than T-EDGE (TBS+WBS), which considers both temporal and amount information with parameter $\alpha = 0.5$.

All in all, our proposed methods learn effective node representations incorporating rich information, which does help us get better performance in the classification task. The result also indicates that time-dependent walks and edge information are essential in transaction networks.

5.5. Parameter Analysis of α

Furthermore, the third observation mentioned above inspires us to analyze the coupling parameter α. Larger α means more time-domain information is considered in the random walk, while smaller α means more amount domain information is considered. **Figure 5** compares the classification performance on the parameter α with different training ratios in terms of

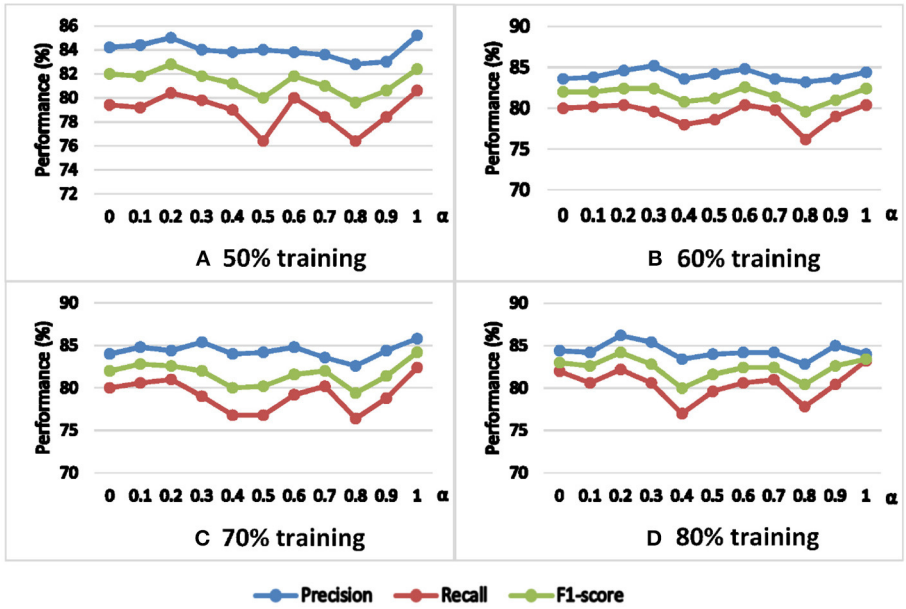


FIGURE 5 | Classification performance on the parameter α with different training ratios.

precision, *recall*, and F1-score. We find that $\alpha = 0.8$ is a poor choice, but there is no single α that is a clear winner. Nevertheless, we can observe that $\alpha \in [0.2, 0.3]$ and $\alpha = 1$ are relatively better choices. This result indicates that it is better to consider or favor a single strategy than to consider both strategies equally at the same time.

6. CONCLUSION

In this work, we proposed a novel framework for Ethereum analysis via network embedding. Particularly, we constructed a temporal weighted multidigraph to retain information as much as possible and present a graph embedding method called T-EDGE that incorporates temporal and weighted information of financial transaction networks into node embeddings. We implemented the proposed and two baseline embedding methods on a realistic Ethereum network for a predictive task with practical relevance, namely phishing/non-phishing node classification. Experimental results demonstrated the effectiveness of the proposed T-EDGE embedding method while indicating that a temporal weighted multidigraph can more comprehensively represent the temporal and financial properties of dynamic transaction networks. Moreover, this work opens up research on graph embedding in a new domain, financial transaction networks. Traditional random walk-based methods can be extended to a temporal version with temporal walks and edge sampling strategies. For future work, we could use the proposed embedding method to investigate more applications of Ethereum or extend the current framework to analyze other large-scale temporal or domain-dependent networks.

DATA AVAILABILITY STATEMENT

The datasets presented in this study can be found in online repositories (https://github.com/lindan113/xblock-network_analysis/tree/master/Phishing%20node%20classification) and are also accessible on our dataset website, XBlock (http://xblock.pro).

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct and intellectual contribution to the work, and approved it for publication.

FUNDING

The work described in this paper was supported by the National Key Research and Development Program (2016YFB1000101), the National Natural Science Foundation of China (61973325, 61503420), and the Fundamental Research Funds for the Central Universities under Grant No. 17lgpy120.

ACKNOWLEDGMENTS

This manuscript has been released as a pre-print at https://arXiv.org [24].

REFERENCES

1. Volpp L. Complex networks: structure and dynamics. *Phys Rep*. (2006) **424**:175–308. doi: 10.1016/j.physrep.2005.10.009
2. Swan M. *Blockchain: Blueprint for a New Economy*. Cambridge, MA: O'Reilly Media, Inc. (2015).
3. Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. (2008). Available online at: https://bitcoin.org/bitcoin.pdf
4. Wood G. Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Pap*. (2014) **151**:1–32. Available online at: https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper.pdf
5. Chen W, Zheng Z. Blockchain data analysis: a review of status, trends and challenges. *J Comput Res Dev*. (2018) **55**:1853–70. doi: 10.7544/issn1000-1239.2018.20180127
6. Ron D, Shamir A. Quantitative analysis of the full bitcoin transaction graph. In: *International Conference on Financial Cryptography and Data Security*. Okinawa: Springer (2013). p. 6–24. doi: 10.1007/978-3-642-39884-1_2
7. Jiang Z, Liang J. Cryptocurrency portfolio management with deep reinforcement learning. In: *2017 Intelligent Systems Conference (IntelliSys)*. IEEE (2017). p. 905–13. Available online at: https://ieeexplore.ieee.org/abstract/document/8324237
8. Liang J, Li L, Zeng D. Evolutionary dynamics of cryptocurrency transaction networks: an empirical study. *PLoS ONE*. (2018) **13**:e0202202. doi: 10.1371/journal.pone.0202202
9. Feder A, Gandal N, Hamrick J, Moore T. The impact of DDoS and other security shocks on Bitcoin currency exchanges: evidence from Mt. Gox. *J Cybersec*. (2018) **3**:137–44. doi: 10.1093/cybsec/tyx012
10. Chen T, Zhu Y, Li Z, Chen J, Li X, Luo X, et al. Understanding ethereum via graph analysis. In: *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. Honolulu, HI: IEEE (2018). p. 1484–92. Available online at: https://ieeexplore.ieee.org/abstract/document/8486401/
11. Chen W, Wu J, Zheng Z, Chen C, Zhou Y. Market manipulation of bitcoin: evidence from mining the Mt. Gox transaction network. In: *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE (2019). p. 1484–92. Available online at: https://ieeexplore.ieee.org/abstract/document/8737364/
12. Chen W, Zheng Z, Cui J, Ngai E, Zheng P, Zhou Y. Detecting Ponzi Schemes on ethereum: towards healthier blockchain technology. In: *Proceedings of the 2018 World Wide Web Conference. International World Wide Web Conferences Steering Committee*. (2018). p. 1409–18. Available online at: https://dl.acm.org/doi/abs/10.1145/3178876.3186046
13. Cai H, Zheng VW, Chang KCC. A comprehensive survey of graph embedding: problems, techniques and applications. *IEEE Trans Knowl Data Eng*. (2018) **30**:1616–37. doi: 10.1109/TKDE.2018.2807452
14. Spitzer F. *Principles of Random Walk*. Ithaca, NY: Springer Science & Business Media (2013).
15. Perozzi B, Al-Rfou R, Skiena S. Deepwalk: online learning of social representations. In: *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM (2014). p. 701–10. Available online at: https://dl.acm.org/doi/abs/10.1145/2623330.2623732
16. Mikolov T, Chen K, Corrado G, Dean J. Efficient estimation of word representations in vector space. *arXiv*. (2013). Available online at: https://arxiv.org/abs/1301.3781
17. Grover A, Leskovec J. Node2Vec: scalable feature learning for networks. In: *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM (2016). p. 855–64. Available online at: https://dl.acm.org/doi/abs/10.1145/2939672.2939754
18. Nguyen GH, Lee JB, Rossi RA, Ahmed NK, Koh E, Kim S. Continuous-time dynamic network embeddings. In: *Companion Proceedings of the The Web Conference 2018. International World Wide Web Conferences Steering Committee*. (2018). p. 969–76. Available online at: https://dl.acm.org/doi/abs/10.1145/3184558.3191526
19. Lin D, Wu J, Yuan Q, Zheng Z. Modeling and understanding ethereum transaction records via a complex network approach. *IEEE Transactions on Circuits and Systems-II: Express Briefs*. (2020). Available online at: https://ieeexplore.ieee.org/abstract/document/8964468/
20. Mikolov T, Sutskever I, Chen K, Corrado GS, Dean J. Distributed representations of words and phrases and their compositionality. In: Burges CJC, Bottou L, Welling M, Ghahramani Z, Weinberger KQ, editors. *Advances in Neural Information Processing Systems 26*. Curran Associates, Inc. (2013). p. 3111–9. Available online at: http://papers.nips.cc/paper/5021-distributed-representations-of-words-and-phrases-and-their-compositionality.pdf
21. Liu J, Ye Y. *Introduction to E-Commerce Agents: Marketplace Marketplace Solutions, Security Issues, and Supply and Demand*. Berlin; Heidelberg: Springer Berlin Heidelberg (2001).
22. Konradt C, Schilling A, Werners B. Phishing: An economic analysis of cybercrime perpetrators. *Comput Sec*. (2016) **58**:39–46. doi: 10.1016/j.cose.2015.12.001
23. Řehůřek R, Sojka P. Software framework for topic modelling with large corpora. In: *Proceedings of the LREC 2010 Workshop on New Challenges for NLP Frameworks*. Valletta: Springer (2010). p. 45–50.
24. Wu J, Lin D, Yuan Q, Zheng Z. T-EDGE: Temporal WEighted MultiDiGraph Embedding for ethereum transaction network analysis. *arXiv*. (2019) 190508038. Available online at: https://arxiv.org/abs/1905.08038

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 24 July 2020
doi: 10.3389/fphy.2020.00243

Risk Connectedness Heterogeneity in the Cryptocurrency Markets

Zhenghui Li[1], *Yan Wang*[2] *and Zhehao Huang*[1]*

[1] Guangzhou International Institute of Finance, Guangzhou University, Guangzhou, China, [2] School of Economics and Statistics, Guangzhou University, Guangzhou, China

This paper examines the risk connectedness across seven cryptocurrencies, Bitcoin, Ethereum, Ripple, Litecoin, Stellar, Monero, and Dash, which have large capitalizations in the cryptocurrency market. The data sample is from August 7, 2015, to February 15, 2020. We measure the return risks of the cryptocurrencies by using the CAViaR model, showing that they have similar risk tendencies, with volatility clusterings from the beginning of 2017 to the end of 2018. The net pairwise spillover index developed by Diebold and Yilmaz [1] is used as the measure of the risk connectedness among the cryptocurrencies. We find that the risk spillover directions are highly correlative with the market capitalizations of the cryptocurrencies. Cryptocurrencies with small market capitalization transmit risks to those with large market capitalization. When there is a downward risk tendency, the risk spillover levels among the cryptocurrencies are stronger than when there is an upward risk tendency, while the spillover directions remain the same under both risk tendencies, except for the cryptocurrency Monero, the particularity of which may be due to the difference in its trading volume compared to the others. We use generalized forecast error variance decomposition for the spillover index and explore the risk connectedness across the cryptocurrencies at different timescales, namely, the short term (0–4 days), medium term (4–30 days) and long term (30–300 days). The risk spillovers can be neglected at the short-term frequency, which implies a delayed effect. The risk spillovers at medium-term frequency are mostly stronger than those at long-term frequency. The dynamic connectedness results show that the means of risk spillover at a long-term frequency are larger than those at medium-term frequency. An inverse result holds for the ranges of risk spillover. The fluctuations of risk spillover at long-term and medium-term frequencies admit the same comparison result with the means of risk spillover in these two frequencies. The findings in this paper provide some suggestions for regulators controlling market stability and cryptocurrency investors generating investment strategies.

Keywords: DY spillover index, net pairwise spillover, risk tendency, time-frequency decomposition, cryptocurrency

OPEN ACCESS

Edited by:
Jianguo Liu,
Shanghai University of Finance and Economics, China

Reviewed by:
Satyam Mukherjee,
Indian Institute of Management Udaipur, India
Chengyi Xia,
Tianjin University of Technology, China

***Correspondence:**
Zhehao Huang
zhehao.h@gzhu.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *22 March 2020*
Accepted: *03 June 2020*
Published: *24 July 2020*

Citation:
Li Z, Wang Y and Huang Z (2020) Risk Connectedness Heterogeneity in the Cryptocurrency Markets. Front. Phys. 8:243. doi: 10.3389/fphy.2020.00243

1. INTRODUCTION

The cryptocurrency markets have recently seen a remarkable increase in prices, leading to some suggestion that cryptocurrencies could be considered as a new kind of financial asset. The market capitalization created by Bitcoin, the classical and most well-known cryptocurrency, grew from 10.1 to 79.7 billion during the period from Oct 2016 to Oct 2017. The price jumped from 616 to 4,800

US dollars. The high returns from the cryptocurrency markets may respond rationally to their high volatilities [2, 3]. They are characterized by a distributed payment system built on cryptographical protocols. This takes advantage of the anonymity, low cost, and fast speed of P2P transactions [4]. Cryptocurrencies are easy to generate speculative bubbles [5], which may spread contagion in return, weakening financial stability [6]. Hence, there has been a great number of papers analyzing cryptocurrencies as financial assets and aiming to identify the information transmission patterns among the cryptocurrency markets and other asset categories like equities, bonds, commodities, currencies, and so on [7–12].

A great deal of literature pays attention to relationships among cryptocurrencies and financial variables due to their roles as new asset classes [9] and important elements in the global financial market [13]. Most of them focus on Bitcoin. However, with the development of cryptocurrency markets, some newly produced cryptocurrencies like Ethereum, Ripple, Litecoin, Stellar, Monero, and Dash have gradually been cutting into the dominant share of market value taken by Bitcoin. This suggests that cryptocurrency investors are taking a breather from Bitcoin and meanwhile looking at other alternative cryptocurrencies. These new cryptocurrencies, which have taken some of the conceptual and technological advantages of Bitcoin (e.g., blockchain technology), are attracting more and more attention as well as creating a mass of opportunities for cryptocurrency investors. Actually, we have to explain that this is not a surprising event, given the fact that each alternative cryptocurrency outperformed Bitcoin in 2017, delivering astonishing returns, which ranged from 5,000% (Litecoin) to 36,000% (Ripple) compared with the 1,300% price appreciation of Bitcoin [14].

The growing interest in the new alternative cryptocurrency markets for investment purposes is accompanied by a lack of knowledge about the interaction between one leading cryptocurrency and another. In fact, the rapid development of cryptocurrency markets results in some relative heterogeneity among mainstream cryptocurrencies. It is helpful to extend the limited literature on connectedness among cryptocurrency markets for use by cryptocurrency investors in devising investment and trading strategies that may involve introducing cryptocurrencies into the portfolio. On the other hand, it is also helpful to construct connectedness networks for use by policy-makers in formulating policies aimed at preserving financial stability. Investors and risk managers can benefit from establishing a connectedness network across many asset classes to generate their investment and hedging decisions. Generally, building connectedness networks is hardly new in conventional assets. Prior works have uncovered connected network structures among or within different assets/markets, including equities [15, 16], bonds [17, 18], currencies [19, 20], commodities [21, 22], and interest rates [18]. However, few works have constructed networks of connectedness in the cryptocurrency market, which is becoming an appealing investment ground for investors. Wei [23] examined the liquidity for 456 kinds of cryptocurrencies. He showed that return predictability weakens in cryptocurrencies with high market liquidity and claimed that liquidity has a significant impact on market efficiency and return predictability for new cryptocurrencies. Yi et al. [24] focused on both static and dynamic volatility connectedness among eight leading cryptocurrencies, revealing their cyclic volatility connectedness, with an evident rising trend at the end of 2016. They linked 52 cryptocurrencies by constructing a volatility connectedness network making use of a variance decomposition framework and found that the 52 cryptocurrencies are interconnected tightly. The so-called "mega-cap" cryptocurrencies are more likely to spread volatility shocks to others. Connectedness among leading cryptocurrencies can also be investigated via return and volatility spillovers, as in Ji et al. [14], where the results achieved implied that the return of each cryptocurrency and its volatility connectedness with others did not necessarily depend heavily on its market size. Some authors have taken the perspective of evolutionary dynamics; for example, ElBahrawy et al. [25] took this approach to analyze the behavior of 1,469 cryptocurrencies and revealed some statistical properties for cryptocurrency markets.

Motivated by the current works on connectedness among the cryptocurrency markets, in this paper, we focus on risk connectedness for the sake of portfolio diversification and risk management. Risk connectedness and spillover have been widely treated, for example, connectedness among stock markets [26, 27], credit markets [28], financial institutions [29], and sovereigns [30, 31] and connectedness between stock and oil markets [32, 33], stock prices and exchange rates [34], energy and carbon markets [35], and so forth. Understanding the risk connectedness among cryptocurrency markets provides valuable information regarding investment and hedging decisions. Moreover, it also provides potential information for systematic risk in the whole cryptocurrency system, according to which the regulators can generate strategies to control risk contagion. The current paper differs from the existing literature in several ways. We use the daily data of seven leading cryptocurrencies, Bitcoin, Ethereum, Ripple, Litecoin, Stellar, Monero, and Dash, to compute their risk levels and investigate the risk connectedness among cryptocurrency markets by providing risk spillovers among these leading cryptocurrencies, accounting for more than 75% of the cryptocurrency market value. The most notable contribution of our work is heterogeneity analysis of the risk connectedness of cryptocurrencies. Two heterogeneities are considered in this paper. The first heterogeneity is the asymmetric risk spillovers at times of upward risk tendency and downward risk tendency in the cryptocurrency markets. The connectedness asymmetry under different risk tendencies is mainly determined by investor expectation. The second heterogeneity is captured by the differences in risk spillovers among the cryptocurrencies at different timescales, namely, in the short term (0–4 days), medium term (4–30 days), and long term (30–300 days). The heterogeneity of risk spillovers at different timescales mainly originates from the persistence of investor attention. Our findings are highly informative for market participants, who can adjust their hedging strategies according to different market tendencies or time horizons.

The paper is organized as follows. Section 2 details the risk measurements for the selected cryptocurrencies. Section 3 shows the static risk connectedness among the cryptocurrency markets. The heterogeneity of risk spillovers under upward risk tendency and downward risk tendency is analyzed. Section 4 explores the risk connectedness at different timescales, which shows the heterogeneity of risk spillovers among the cryptocurrencies in the short term, medium term, and long term. Section 5 concludes with some policy implications.

2. RISK MEASUREMENT FOR THE CRYPTOCURRENCIES

It is well-known that the cryptocurrency returns are extremely volatile, with clustering phenomena. Bollerslev [36] used GARCH models to capture these characteristics well. GARCH models have been widely popular as tools for measuring market risk by the VaR method due to their relative simplicity and various extensions. Unfortunately, their limitations, especially the unrealistic parametric assumptions, such as normality or i.i.d returns, which does not fit the case of cryptocurrencies, are also evident. To overcome these problems, in this paper, we apply the semi-parametric Conditional Autoregressive Value at Risk (CAViaR) method developed by Engle and Manganelli [37] to estimate VaR models for cryptocurrencies, avoiding any extreme assumption invoked by the existing methodologies. Unlike GARCH and GAS, which model the whole distribution, CAViaR directly models the quantile of the return distribution, extending the standard quantile regression approach introduced by Koenker and Basset [38]. The CAViaR model uses an autoregressive formulation straight to the quantile.

2.1. CAViaR Model

In short, the CAViaR method is particular in estimating VaRs directly through an autoregressive specification for quantiles rather than the usual approach of inverting a conditional distribution of returns in a purely parametric framework [39]. This autoregressive dynamics for the quantile over time, as well as some unknown parameters, is then determined by the regression quantile framework [38]. Besides, the autoregressive nature of CAViaR directly captures some stylized facts in the distribution tails, like autocorrelation in daily returns arising from market microstructure biases and partial price adjustment [40], volatility clustering [36], and time-varying skewness and kurtosis [41].

In this paper, following Engle and Manganelli [37], we consider a cryptocurrency return vector $\{y_t\}_{t=1}^{T}$. Let θ be the probability associative to VaR, x_t a observable variable vector, and β_θ a unknown parameter vector. Let $f_t(\beta) \equiv f(x_{t-1}, \beta_\theta)$ be the θ-quantile of the cryptocurrency return distribution at time t, formed at time $t-1$. Then a general CAViaR model is specified as follows:

$$f_t(\beta) = \gamma_0 + \sum_{i=1}^{q} \gamma_i f_{t-i}(\beta) + \sum_{i=1}^{p} \alpha_i l(x_{t-i}, \varphi), \tag{1}$$

where $\beta' = (\alpha', \gamma', \varphi')$ and l is the function of a finite value depending on lagged values of observable variables. Engle and Manganelli [37] introduced an autoregressive term $\gamma_i f_{t-i}(\beta)$, $i = 1, 2, \cdots, q$, allowing a smooth transition quantile. In addition, they introduced the term $l(x_{t-i}, \varphi)$ in order to permit a relationship between the θ-quantile $f_t(\beta)$ and the observable variables. On the basis of general CAViaR formulation, Engle and Manganelli [37] developed four alternative specifications for the function l:

$$\begin{aligned}
\textit{Adaptative} &: f_t(\beta) = f_{t-1}(\beta) + \beta((1 \\
&+ \exp(G(y_{t-1} - f_{t-1}(\beta))))^{-1} - \theta), \qquad (2)\\
\textit{Symmetric Absolute Value} &: f_t(\beta) = \beta_1 + \beta_2 f_{t-1}(\beta) + \beta_3 |y_{t-1}|, \qquad (3)\\
\textit{Asymmetric Slope} &: f_t(\beta) = \beta_1 + \beta_2 f_{t-1}(\beta) + \beta_3 (y_{t-1})^{+} \\
&+ \beta_4 (y_{t-1})^{-}, \qquad (4)\\
\textit{Indirect GARCH}(1,1) &: f_t(\beta) = (\beta_1 + \beta_2 f_{t-1}^2(\beta) + \beta_3 y_{t-1}^3)^{1/2}. \qquad (5)
\end{aligned}$$

In the first specification, G is a positively finite value satisfying that the last term converges to $\beta_1(I(y_{t-1} \leq f_{t-1}(\beta_1) - \theta))$ as $G \to \infty$, where $I(\cdot)$ is an indicator function. As explained by Engle and Manganelli [37], the *Adaptative* specification allows that whenever one exceeds one's VaR, one should directly increase it. Otherwise, one should decrease it very slightly. The second and fourth specifications both respond symmetrically to past returns with mean reverting, as the coefficient of the lagged VaR is unconstrained to equal to one. The third model is also mean reverting but with less restrictions in the sense that it permits asymmetric response to both positive and negative past returns. The asymmetric CAViaR specification has become the most popular one for practitioners due to its consideration of the skewness and kurtosis properties of financial series [29, 39, 42]. In this paper, asymmetric CAViaR is also employed for measurement of the risk of cryptocurrency returns, which is verified through test statistics (see also [43] for a cryptocurrency risk measurement study).

2.2. Data and Sample Analysis

We collected daily price data on seven cryptocurrencies, Bitcoin, Ethereum, Ripple, Litecoin, Stellar, Monero, and Dash, so as to obtain sufficient price data for the 10 largest cryptocurrencies by market capitalization listed on the website https://coinmarketcap.com. Indeed, they cover almost a two-and-a-half-year period, allowing us to make the most of our empirical results and analysis. The sample interval ranges from August 7, 2015, to February 15, 2020 (1,654 daily observations) for this paper. Each selected cryptocurrency possesses a market value exceeding 5 billion USD. The total market value of these seven cryptocurrencies represents 79.5% of the entire cryptocurrency market. The empirical study is built on daily return, calculated by the difference in the log of price.

Figure 1 shows the risk level tendencies of the seven cryptocurrencies. On the whole, the cryptocurrencies show similar risk tendencies. In particular, volatility clusterings happen during the period from the beginning of 2017 to the end of 2018, since the cryptocurrencies received substantial price appreciations during this period. We can also identify some mild peculiarities of Dash and Monero. With regard to Dash, volatility clustering was common in the whole sample period, whereas

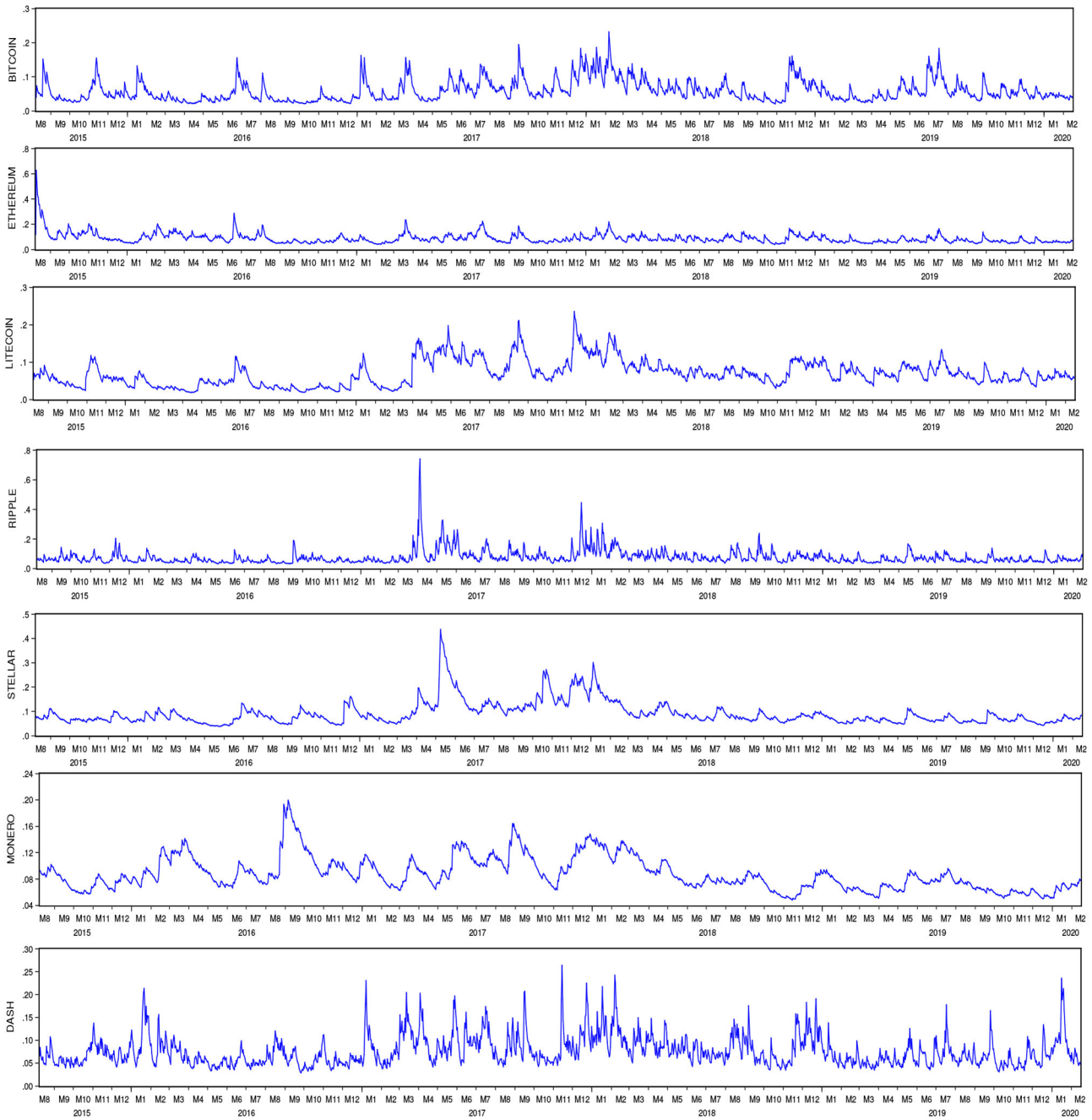


FIGURE 1 | Risk level tendencies of the selected cryptocurrencies.

for Monero, it reached its peak earlier, in the middle of August 2016, than others, whose peaks arose during the period from the beginning of 2017 to the end of 2018. Besides, they both have wider volatility ranges.

The summary statistics for the risks of cryptocurrencies, including risks under upward and downward tendencies, are given in **Table 1**. In Panel A, the highest mean of risk is for Stellar, followed by Ethereum and Monero together. Ripple and Stellar have the highest standard deviation, followed by Ethereum. Interestingly, as the most popular cryptocurrency in the market, Bitcoin shows the lowest mean risk and a relatively low standard deviation, only higher than Monero. In fact, these are not surprising observations. In 2017, each of the other six cryptocurrencies under study increased in value by at least 5,000%, while Bitcoin increased by 1,300%. Excess levels of kurtosis arise in all cryptocurrencies, especially Ripple. All

TABLE 1 | Summary statistics for cryptocurrency risks.

Variable	Mean	Max	Min	Std. Dev	Skewness	Kurtosis	Jarque-Bera
Panel A							
Bitcoin	0.059	0.232	0.020	0.031	1.413	5.053	840.549***
Ethereum	0.088	0.628	0.040	0.041	4.115	37.626	87242.330***
Litecoin	0.070	0.235	0.019	0.034	1.019	4.248	393.467***
Ripple	0.075	0.741	0.032	0.048	4.782	45.539	130932.800***
Monero	0.088	0.200	0.048	0.025	1.083	4.283	436.434***
Dash	0.076	0.264	0.029	0.033	1.587	6.299	1443.842***
Stellar	0.091	0.437	0.038	0.048	2.630	12.615	8274.153***
Panel B	Upward						
Bitcoin	0.082	0.194	0.031	0.041	1.203	3.732	12.656**
Ethereum	0.098	0.186	0.050	0.032	0.824	3.196	5.507*
Litecoin	0.085	0.209	0.047	0.027	2.351	10.852	167.525***
Ripple	0.104	0.306	0.040	0.048	1.967	8.543	92.391***
Monero	0.078	0.133	0.051	0.020	1.086	3.663	10.309**
Dash	0.107	0.218	0.049	0.041	0.831	3.084	5.543*
Stellar	0.080	0.177	0.047	0.025	1.824	6.866	56.507***
Panel C	Downward						
Bitcoin	0.059	0.175	0.022	0.027	1.217	4.610	86.619***
Ethereum	0.080	0.354	0.042	0.030	3.861	31.794	9035.059***
Litecoin	0.074	0.201	0.021	0.030	1.206	5.071	102.727***
Ripple	0.066	0.349	0.034	0.032	4.093	29.890	8032.833***
Monero	0.082	0.143	0.051	0.021	0.903	3.224	33.690***
Dash	0.069	0.188	0.031	0.025	1.498	6.302	202.136***
Stellar	0.087	0.348	0.041	0.044	3.018	14.743	1772.576***

*Denotes the significance at a 10% level. **Denotes the significance at a 1% level. ***Denotes the significance at a 0.1% level.

cryptocurrencies show positive skewness. When risks increased (Panel B), Dash has the highest mean risk level and the second-highest standard deviation. Meanwhile, Ripple has the highest standard deviation and the second-highest mean risk. High levels of kurtosis and positive skewness arise in all cryptocurrencies. Litecoin occupies the highest levels in terms of both kurtosis and skewness. Moving to the statistics of decreased risks (Panel C), Stellar has the highest mean risk and standard deviation. Excess levels of kurtosis and positive skewness arise in all cryptocurrencies, where Ethereum and Ripple are dominant in both these two statistics.

The risk correlation matrices for the selected seven cryptocurrencies are shown in **Table 2**. Overall, weak to moderately positive correlations happen among the risk levels of the selected cryptocurrencies. In particular, the highest correlation coefficient is for the pair Bitcoin and Litecoin, given as 0.68, whereas the pair Ethereum and Stellar permits the lowest correlation coefficient given as 0.07. Focusing on the risk correlations at times of upward and downward tendencies, the correlations under an upward tendency are generally stronger than those under a downward tendency. Under an upward risk tendency, the pair Bitcoin and Ethereum has the highest correlation coefficient, 0.87, followed by the pair Ethereum and Dash, 0.79, whereas the lowest correlations are for the pairs Bitcoin and Stellar and Ethereum and Stellar, with coefficients 0.25 and 0.26, respectively. The pairs Bitcoin and Monero and Ethereum and Monero are uncorrelated under an upward risk tendency. Under a downward risk tendency, Bitcoin and Litecoin are the most positively correlated, with a coefficient of 0.70, followed by the pair Bitcoin and Dash, for which it is 0.67, while Ethereum and Stellar are uncorrelated. Overall, the correlation between Bitcoin and Litecoin is unsurprisingly much stronger than for the other pairs in the results of all three tests.

3. STATIC RISK CONNECTEDNESS IN THE CRYPTOCURRENCY MARKETS

We follow [1] for the methodological framework for constructing connectedness measures. In this paper, static risk connectedness networks under upward and downward tendencies, as well as static and dynamic risk connectedness at different timescales, are built.

3.1. Static Risk Connectedness Measurement

Suppose a stationary covariance seven-variable VAR(p) given as

$$R_t = \sum_{i=1}^{p} \Phi_i R_{t-i} + \varepsilon_t, \tag{6}$$

TABLE 2 | Correlations among the cryptocurrencies.

	Bitcoin	Ethereum	Litecoin	Ripple	Monero	Dash	Stellar
Panel A							
Bitcoin	1.00						
Ethereum	0.40***	1.00					
Litecoin	0.68***	0.23***	1.00				
Ripple	0.38***	0.20***	0.54***	1.00			
Monero	0.27***	0.18***	0.27***	0.25***	1.00		
Dash	0.63***	0.33***	0.53***	0.46***	0.28***	1.00	
Stellar	0.30***	0.07***	0.56***	0.54***	0.38***	0.28***	1.00
Panel B	Upward						
Bitcoin	1.00						
Ethereum	0.87***	1.00					
Litecoin	0.75***	0.76***	1.00				
Ripple	0.48***	0.58***	0.52***	1.00			
Monero	0.22	0.22	0.37**	0.44***	1.00		
Dash	0.70***	0.79***	0.69***	0.53***	0.30*	1.00	
Stellar	0.25*	0.26*	0.40***	0.55***	0.77***	0.28*	1.00
Panel C	Downward						
Bitcoin	1.00						
Ethereum	0.53***	1.00					
Litecoin	0.70***	0.39***	1.00				
Ripple	0.44***	0.32***	0.60***	1.00			
Monero	0.51***	0.38***	0.55***	0.41***	1.00		
Dash	0.67***	0.43***	0.64***	0.48***	0.44***	1.00	
Stellar	0.29***	0.08	0.50***	0.53***	0.47***	0.28***	1.00

*Denotes the significance at a 10% level. **Denotes the significance at a 1% level. ***Denotes the significance at a 0.1% level.

where R_t is the 7×1 cryptocurrency risk vector, Φ_t are 7×7 autoregressive coefficient matrices, and ε_t is the error term vector assumed to be serially uncorrelated. If the VAR model above is a stationary covariance, then one can write a moving-average representation as

$$R_t = \sum_{j=0}^{\infty} A_j \varepsilon_{t-j}, \tag{7}$$

where the 7×7 coefficient matrix A_j obeys a recursion of the form

$$A_j = \Phi_1 A_{j-1} + \Phi_2 A_{j-2} + \cdots + \Phi_p A_{j-p}, \tag{8}$$

where A_0 is the $n \times n$ identity matrix and $A_j = 0$ for $j < 0$. One can measure pairwise connectedness, directional connectedness, and total connectedness on the basis of a generalized forecast-error variance decomposition (FEVD) approach by using the moving-average framework. The advantage of FEVD is that it eliminates any disturbance induced in the results by the variable ordering.

Denote the H-step-ahead generalized forecast-error variance decomposition [14] by

$$\theta_{ij}(H) = \frac{\sigma_{jj}^{-1} \sum_{h=0}^{H-1} (e_i' A_h \Sigma e_j)^2}{\sum_{h=0}^{H-1} (e_i' A_h \Sigma A_h' e_i)}, \tag{9}$$

where $\theta_{ij}(H)$ is the variance contribution of variable j to variable i, σ_{jj} is the standard deviation of the error term in the j'th equation, and Σ is the variance matrix of the error vector ε. e_i is a selection vector with a value of 1 for the i'th element. Otherwise, take it as 0. The spillover index yields an $n \times n$ matrix $\theta(H) = [\theta_{ij}(H)]$, where each entry gives the contribution of variable j to the forecast-error variance of variable i. Own-variable and cross-variable contributions are involved in the main diagonal and off-diagonal elements, respectively, of the $\theta(H)$ matrix. Each entry in the $\theta(H)$ matrix is normalized by the row sum

$$\tilde{\theta}_{ij}(H) = \frac{\theta_{ij}(H)}{\sum_{j=1}^{N} \theta_{ij}(H)}, \tag{10}$$

to ensure that the row sum is equal to 1. There are several spillovers, such as total spillovers, directional spillovers, net spillovers, and net pairwise spillovers [14, 24, 44, 45]. In this paper, we construct the net pairwise spillovers to investigate the information spillovers among the whole cryptocurrency market system.

With respect to the net pairwise connectedness, according to the definition of FEVD, in general, $\tilde{\theta}_{ij} \neq \tilde{\theta}_{ji}$. Consequently, the difference between $\tilde{\theta}_{ij}$ and $\tilde{\theta}_{ji}$, $\tilde{\theta}_{ij} - \tilde{\theta}_{ji}$, can be used to measure the net pairwise connectedness as well as the net spillover effect from variable j to variable i. A directional connectedness network

TABLE 3 | Net pairwise risk spillover among the cryptocurrencies.

	Bitcoin	Ethereum	Ripple	Litecoin	Stellar	Monero
Ethereum	−0.047					
Ripple	−0.035	−0.001				
Litecoin	0.768	−0.034	1.187			
Stellar	1.316	0.462	1.679	0.887		
Monero	2.520	4.665	1.925	1.959	1.189	
Dash	0.870	1.746	0.729	0.478	−0.490	−1.095

This table presents the net pairwise risk spillovers among the selected cryptocurrencies over the period from August 7, 2015, to February 15, 2020. Net pairwise risk spillover transmitted by one cryptocurrency to another, where positive (negative) values suggests that the cryptocurrency in question is a net receiver (transmitter) of spillovers to another cryptocurrency.

can then be built on the basis of net pairwise connectedness. Each market is regarded as a node in the network. The condition in which a directional edge from i to j exists in the network is $\tilde{\theta}_{ij} - \tilde{\theta}_{ji} > 0$.

3.2. Static Risk Connectedness Over the Full Sample

Table 3 presents the matrix depicting net pairwise risk spillovers among the cryptocurrency markets, that is, net spillovers between two cryptocurrencies, where positive (negative) values mean that the cryptocurrencies in question are net receivers (transmitters) of spillover effects. Accordingly, we claim that the risk spillover is highly correlative with the capitalization of the cryptocurrency market. Mostly, risk spills over from cryptocurrencies with small capitalizations to those with large capitalizations. In particular, Bitcoin transmits little risk to Ethereum and Ripple, where the spillover indexes are given as 0.047 and 0.035%, respectively, whereas it receives more risk from Stellar, Monero, and Dash, where the spillover indexes are 1.316, 2.520, and 0.870%, respectively. Similar results are seen with regard to Ethereum, which mainly receives risks from other cryptocurrencies with small capitalizations (spillover indexes from three cryptocurrencies, Stellar, Monero, and Dash, to Ethereum are 0.462, 4.665, and 1.746%, respectively, but those from Ethereum to Ripple and Litecoin are only 0.001 and 0.034%, respectively). A similar analysis holds for Ripple and Litecoin.

Although the empirical results we get do not agree with the return spillover directions in the existing literature, we believe that there is some relation between the risk spillover and return spillover in the cryptocurrency markets. Cryptocurrencies with large capitalization dominate the market efficiency and price fluctuation, leading the market development tendency. The rapid growth of cryptocurrencies into new classes of financial assets creates a major challenge for traditional financial markets and even impacts the whole financial market. In general, cryptocurrency investors focus on those cryptocurrencies with large capitalizations. They may take these cryptocurrencies as references when making investment strategies in the cryptocurrency markets. This results in return spillovers from cryptocurrencies with large capitalization to those with small capitalization. The return spillovers will cause violent fluctuations in cryptocurrency prices with small capitalization and then vary their return risks. The investors who intend to invest in cryptocurrencies with small capitalization still rely on the price tendencies of cryptocurrencies with large capitalization. Thus, investor attention influences the return risks of cryptocurrency markets with large capitalization, and the return risks spill over from markets with small capitalization to those with large capitalization. Indeed, this also reflects the dominant roles of cryptocurrencies with large capitalization in the whole cryptocurrency market.

3.3. Static Risk Connectedness in Upward and Downward Tendencies

Risk spillovers among the cryptocurrency markets under downward risk tendency are more remarkable than spillovers under upward risk tendency. Spillover indexes under downward risk tendency are mostly higher than those under upward risk tendency. In particular, the spillover index between Bitcoin and Ripple is shown to be −0.920% under downward risk tendency, whereas it is −0.513% under upward risk tendency. Besides, Bitcoin transmits the risks to Stellar and Dash, where the spillover indexes under downward tendency are 2.607 and 2.231%, respectively, whereas they are given correspondingly as 1.824 and 0.689% under upward tendency. Similar results are seen in Ripple and Litecoin. In fact, the asymmetrical spillover under different risk tendencies is due to the difference in the regulatory mechanism in cryptocurrency markets. Under an upward risk tendency, the cryptocurrencies not only reduce their own risks but also withstand spillovers from others more effectively. The investors generate investment strategies more prudently when the market risks are increasing. More concentrated attention on their target cryptocurrency markets results in weak spillovers among the cryptocurrencies in periods of upward risk tendency. On the contrary, markets with decreasing risks attract a large number of investors, whose confidences enhance significantly. This is again due to the regulatory mechanism of the markets themselves. The investors still pay attention to cryptocurrencies with large capitalization like Bitcoin and Ethereum, considering their dominant roles when they are generating their investment strategies. The investor attention expedites communications among the markets and impacts the risk connectedness. In summary, the cryptocurrencies spill more risks to others at times of downward risk tendency than when there is upward risk tendency. In addition, this asymmetric effect is prominent in cryptocurrencies with large capitalization.

Attention should be paid to the different spillover directions between Monero and other cryptocurrencies under upward and downward risk tendencies. One can see from **Table 4** that among the twenty-one pairwise spillovers, six pairwise spillovers change their spillover directions in different risk tendencies, and four of them involve Monero. According to the signs of net pairwise spillovers, Monero mainly accepts spillovers from cryptocurrencies with large capitalization under upward risk tendency, whereas it transmits risk to these cryptocurrencies under downward risk tendency. This result agrees well with what

TABLE 4 | Net pairwise risk spillover under upward and downward risk tendencies.

	Bitcoin	Ethereum	Ripple	Litecoin	Stellar	Monero
Panel A	Upward					
Ethereum	2.174					
Ripple	−0.513	−2.443				
Litecoin	−0.320	−3.491	0.030			
Stellar	1.824	0.385	4.145	2.684		
Monero	−1.218	−3.246	−0.415	0.094	0.603	
Dash	0.689	−2.894	0.516	0.313	−2.011	1.662
Panel B	Downward					
Ethereum	−0.325					
Ripple	−0.920	−0.505				
Litecoin	−0.183	0.087	0.370			
Stellar	2.607	3.130	3.691	3.431		
Monero	2.219	2.937	2.356	2.412	−1.996	
Dash	2.231	2.889	3.017	2.841	−0.335	0.756

This table presents the net pairwise risk spillovers among the selected cryptocurrencies under upward and downward risk tendencies over the period from August 7, 2015, to February 15, 2020. The Panel A presents spillovers during upward risk tendency, while Panel B presents spillovers during downward risk tendency.

is shown in **Figure 1**. In **Figure 1**, one can see that the risk tendency of Monero differs from those of other cryptocurrencies before the steep rise in prices of cryptocurrency markets at the beginning of 2017. Monero reached its risk peak while the other cryptocurrencies stayed in their risk troughs. However, this phenomenon disappeared after 2017. This interesting result is due to the trading volumes of cryptocurrencies. The trading volume of Monero was different from those of the others before 2017. For instance, from August 2016 to October 2016, the trading volume of Monero fluctuated strongly, whereas the others were weakly fluctuating. After 2017, the trading volume of Monero comoved with other cryptocurrencies but with a higher amplitude of fluctuation. We can capture that the differences in trading volumes between Monero and other cryptocurrencies mostly happened under downward risk tendency. The increase in cryptocurrency trading volumes drove Monero to transmit its risk to other cryptocurrencies. Thus, Monero spilled over risk, as a transmitter in the market, under a downward risk tendency. So we have to acknowledge the specific role played by Monero in the whole cryptocurrency market.

4. TIME-FREQUENCY CONNECTEDNESS OF CRYPTOCURRENCY RISKS

In fact, the analysis in section 3 implies that risk connectedness among the cryptocurrency markets might show heterogeneities at different timescales, which will be verified in this section. In this section, we explore the net pairwise spillovers among the selected cryptocurrencies at different timescales, namely in the short term (<4 days), medium term (more than 4 days but <30 days), and long term (more than 30 days but <300 days). The methodology for time-frequency connectedness measurement refers to [46].

4.1. Time-Frequency Connectedness Measurements

In this paper, the spectral representation framework of generalized forecast error variance decomposition (GFEVD) is applied to the frequency decomposition. Define the generalized causation spectrum over frequency $\omega \in (-\pi, \pi)$ by

$$(f(\omega))_{k,j} = \frac{\Sigma_{j,j}^{-1} |(R(e^{-i\omega})\Sigma)_{k,j}|^2}{(R(e^{-i\omega})\Sigma R'(e^{i\omega}))_{k,k}}, \tag{11}$$

where $R(e^{-i\omega}) = \sum_h e^{-i\omega h} R_h$, $h = 1, 2, \cdots, H$, is the Fourier transform of R, with $i = \sqrt{-1}$. As noted by [46], the forecast horizon H makes no difference, since the GFEVD here is unconditional. To obtain the generalized variance decompositions on frequency band d, $d \in (a, b)$, $a, b \in (-\pi, \pi)$, we weight $(f(\omega))_{k,j}$ by the frequency shares of the jth volatility variance. Thus, the weighting function can be defined as

$$\Gamma_k(\omega) = \frac{2(R(e^{-i\omega})\Sigma R'(e^{i\omega}))_{k,k}}{\int_{-\pi}^{\pi} (R(e^{-i\lambda})\Sigma R'(e^{i\lambda}))_{k,k} d\lambda}. \tag{12}$$

The generalized variance decompositions on frequency band d are denoted by

$$(\Theta_d)_{k,j} = \frac{1}{2} \int_d^{\infty} \Gamma_k(\omega)(f(\omega))_{k,j} d\omega. \tag{13}$$

With the spectral representation of the generalized variance decompositions, we can easily calculate the scaled generalized variance decompositions as

$$(\widetilde{\Theta}_d)_{k,j} = \frac{(\Theta_d)_{k,j}}{\sum_j (\Theta_\infty)_{k,j}}, \ (\Theta_\infty)_{k,j} = \frac{1}{2} \int_{-\pi}^{\pi} \Gamma_k(\omega)(f(\omega))_{k,j} d\omega. \tag{14}$$

Then, the net pairwise spillovers in different frequencies are given as

$$S_{k,j} = ((\widetilde{\Theta}_d)_{k,j} - (\widetilde{\Theta}_d)_{j,k}) \cdot 100. \tag{15}$$

4.2. Static Risk Connectedness at Different Timescales

Table 5 shows the static net pairwise risk spillovers among the cryptocurrency markets at short-, medium-, and long-term frequencies. It is evident that spillovers happen at medium- and long-term frequencies. Spillovers between any two cryptocurrencies are almost zero in the short term. They show signs of recovery until 4 days later. This is due to the investor attitude on the cryptocurrency markets and information exchange among them. The risk spillovers among the cryptocurrency markets result from the return spillovers and information exchange among them. As analyzed in section 3, cryptocurrencies with large capitalization play key roles in the overall market. Investment strategies are generated according to the price fluctuations of cryptocurrencies with large

TABLE 5 | Static net pairwise risk spillovers at different timescales.

	Bitcoin	Ethereum	Ripple	Litecoin	Stellar	Monero
Panel A	Short term					
Ethereum	6.50e-03					
Ripple	−3.2e-02	−3.9e-02				
Litecoin	5.39e-02	2.11e-02	6.5e-02			
Stellar	2.53e-03	1.64e-04	5.2e-02	6.93e-05		
Monero	3.98e-03	3.56e-03	−8.5e-05	1.12e-03	6.40e-05	
Dash	−4.9e-03	−4.8e-02	2.08e-02	−5.9e-02	1.99e-03	5.20e-03
Panel B	Medium term					
Ethereum	0.019					
Ripple	−0.053	−0.075				
Litecoin	0.231	0.101	0.245			
Stellar	0.049	0.002	0.263	−0.001		
Monero	0.033	0.031	−0.006	0.008	0.002	
Dash	−0.163	−0.093	0.065	−0.249	0.003	0.024
Panel C	Long term					
Ethereum	0.059					
Ripple	−0.015	−0.002				
Litecoin	0.092	0.024	0.078			
Stellar	0.027	0.002	0.009	−0.032		
Monero	0.028	0.019	−0.006	0.015	0.003	
Dash	−0.032	0.047	0.008	−0.074	0.007	0.008

This table presents the static net pairwise risk spillovers among the selected cryptocurrencies at different timescales. Panel A presents the spillovers at short-term frequency (0–4 days). Panel B presents the spillovers at medium-term frequency (4–30 days). Panel C presents the spillovers at long-term frequency (30–300 days).

capitalization. Thus, investments in cryptocurrencies with small capitalization rely on the price fluctuations of cryptocurrencies with large capitalization, and so the information exchange among the cryptocurrency markets leads to risk spillovers among them. Moreover, the spillovers are not immediate but are delayed, which results from the investor attitudes and asymmetry of information. Although the investment decisions rely on the prices of cryptocurrencies with large capitalization, as emerging financial assets, cryptocurrencies are easily influenced by major events such that they show strong uncertainty. Thus, the investors first off look at the markets. On the other hand, information in the cryptocurrency markets shows asymmetry between investors and speculators, which also results in a delay in risk spillovers among the cryptocurrency markets.

Furthermore, comparing the net pairwise spillovers among the selected cryptocurrencies in the medium and long term in **Table 5**, one can catch that risk spillovers at medium-term frequency are mostly stronger than those at long-term frequency, while the spillover directions remain almost the same. In particular, only five pairwise spillover indexes at long-term frequency are larger than their corresponding indexes at medium-term frequency. Meanwhile, there is only one pairwise spillover index that changes its sign (Ethereum and Dash). The results imply that risk spillovers among the cryptocurrencies followed an upturned "U" with respect to time frequency. One may question the origin for such a phenomenon, and our reply is that it is due to dynamic investor attention on the markets. When news involving a cryptocurrency market issue or a major event enters circulation, most investors just monitor the markets without making investments, which results in slight risk spillovers among the cryptocurrencies. With sensationalization from speculators or market properties, such as trading volumes and prices varying distinctly, the investors pay their maximum attention to the markets. Considering the dominant roles of cryptocurrencies with large capitalization in the whole market, risk spillovers among the cryptocurrency markets also attain their peaks. As the market gradually acclimatizes itself to the changing information or shocks on prices caused by major events, the market efficiency of an individual cryptocurrency may increase, which reduces the risk spillovers to others. However, the increasing market efficiency of an individual cryptocurrency cannot result in a change of status in the whole market for the individual cryptocurrency. Thus, at different timescales, the risk spillover directions remain the same. Summing up, risk spillovers among the cryptocurrencies are the most remarkable in the medium term, rather than in the short term or long term. Moreover, these spillovers show persistence.

4.3. Dynamic Risk Connectedness at Different Timescales

Table 6 presents the statistics for dynamic risk connectedness among the cryptocurrency markets at medium- and long-term frequencies. The risk spillover means and ranges among the cryptocurrencies are remarkably discrepant at different timescales. In addition, several spillover directions change.

TABLE 6 | Statistics for dynamic risk connectedness at medium- and long-term frequencies.

	Medium term			Long term		
	Mean	**Std. Dev**	**Range**	**Mean**	**Std. Dev**	**Range**
Bit-Eth	0.077	0.411	8.870	0.181	0.429	5.356
Lit-Ste	−0.039	0.454	7.808	−0.055	0.615	7.555
Lit-Mon	0.001	0.526	7.895	−0.112	0.688	5.949
Ste-Mon	0.018	0.646	12.844	−0.151	0.831	6.362
Ste-Das	0.021	0.519	9.260	0.139	0.477	5.847
Bit-Rip	0.002	0.481	7.231	0.118	0.289	4.638
Bit-Lit	0.172	0.522	4.214	0.007	0.457	3.760
Bit-Ste	−0.039	0.501	12.483	−0.084	0.550	6.641
Bit-Mon	0.053	0.435	10.138	−0.022	0.586	6.327
Bit-Das	−0.204	0.969	8.524	0.148	0.503	4.614
Eth-Rip	−0.031	0.549	7.876	0.076	0.275	5.408
Eth-Lit	−0.025	0.431	6.695	−0.164	0.528	5.784
Eth-Ste	−0.167	0.829	10.486	−0.120	0.585	5.485
Eth-Mon	−0.009	0.432	10.516	−0.148	0.548	6.390
Eth-Das	−0.069	0.616	7.388	0.121	0.431	5.463
Rip-Lit	0.101	0.495	4.419	−0.171	0.383	5.389
Rip-Ste	0.165	0.768	7.275	−0.233	0.439	5.463
Rip-Mon	−0.082	0.497	9.120	−0.205	0.410	4.854
Rip-Das	−0.068	0.583	7.471	−0.065	0.304	5.540
Lit-Das	−0.039	0.625	5.785	0.197	0.436	3.982
Mon-Das	0.131	0.588	9.120	0.285	0.749	7.241
Sum.	No.of	$\|M_L\| > \|M_M\|$	16	No. of	$\|SD_L\| > \|SD_M\|$	8
	No.of	changed sign	9	No. of	$\|R_L\| > \|R_M\|$	0

This table presents the statistics for dynamic net pairwise risk spillovers among the selected cryptocurrencies at medium- and long-term frequencies. M_L, SD_L, and R_L stand for the mean, standard deviation, and range, respectively at the long-term frequency.
For lack of space, we present the statistics rather than figures depicting the risk spillovers among the cryptocurrencies. Readers can ask for the figure from the authors.

The mean spillover at long-term frequency is larger than that at medium-term frequency, whereas the spillover range at medium-term frequency is wider than that at long-term frequency. In **Table 6**, there are sixteen pairwise spillovers whose spillover indexes at long-term frequency are larger than at medium-term frequency. Since the mean depends heavily on the length of the sample interval, we catch the dynamic characteristics of risk spillovers among the cryptocurrencies through spillover range and standard deviation. The spillover range at long-term frequency is remarkably lower than that at medium-term frequency. Similar to the analysis in subsection 4.2, this results from the collection of risk spillovers among the cryptocurrencies at medium-term frequency. The delays of price transmissions among the cryptocurrencies result in the collection of risk spillovers at medium-term frequency. Meanwhile, attentional heterogeneity in different market participants leads to wide-ranging fluctuation in risk spillover levels among the cryptocurrencies. In particular, speculators and arbitragers may get more returns due to the convenience and timeliness with which they get market information. Thus, these market participants may magnify the risk spillovers among the markets. On the other hand, speculators and arbitragers pursue medium-term profits in general, while investors prefer long-term programs. This also suggests the amplification of risk spillovers at medium-term frequency.

Referring to subsection 4.2, we divide the net pairwise spillovers into two groups. In group one, the risk spillovers at long-term frequency are stronger than those at medium-term frequency, while group two holds the inverse case. One can see from **Table 6** that the risk spillover between two cryptocurrencies whose spillover at long-term frequency is stronger than that at medium-term frequency shows a strong fluctuation at long-term frequency. However, the risk spillover fluctuation at long-term frequency between two cryptocurrencies whose spillover at long-term frequency is weaker than that at medium-term frequency is remarkably weaker than that at medium-term frequency. This is due to the persistence of risk spillovers among the cryptocurrencies. In terms of Bitcoin and Ethereum, the investors will pay continuous attention to these two cryptocurrencies when they are generating investment decisions, on account of their high similarity. This leads to a longer persistence of risk spillover between Bitcoin and Ethereum, which results in the risk spillover fluctuation at long-term frequency being stronger than that at medium-term frequency. In terms of those cryptocurrencies with weak similarity, the dominant roles of cryptocurrencies with large capitalization result in stronger risk spillover fluctuations in the medium term. Summing up,

we declare the heterogeneity in dynamic characteristics of risk spillovers among the cryptocurrencies at different timescales.

5. CONCLUSIONS AND POLICY IMPLICATIONS

In this paper, we study risk connectedness among the cryptocurrency markets through net pairwise risk spillover measurement. We select seven leading cryptocurrencies, Bitcoin, Ethereum, Ripple, Litecoin, Stellar, Monero, and Dash, whose capitalizations are among the top 20 in the cryptocurrency market. The data sample interval ranges from August 7, 2015, to February 15, 2020. The methodology measuring the risk spillover used in this paper is the DY index. We first explore the net pairwise risk spillovers among the selected cryptocurrencies over the whole sample. We then discuss the asymmetric spillovers at times of upward and downward risk tendency. Finally, we identify risk spillover heterogeneity at different timescales through the decomposed DY index on the basis of time frequency. The conclusion of this paper is summarized as follows.

First, the risk spillover directions are highly correlative with the capitalizations of cryptocurrencies. The risks spill over from the cryptocurrencies with small capitalization to those with large capitalization. For instance, the spillover indexes from Bitcoin to Ethereum and Ripple are 0.047 and 0.035%, respectively, while Bitcoin accepts risks from Stellar, Monero, and Dash, with spillover indexes of 1.316, 2.520, and 0.870%, respectively. Similar results also hold for Ethereum, which accepts risks from Stellar, Monero, and Dash, measured by the spillover indexes as 0.462, 4.665, and 1.746%, respectively.

Second, the risk spillovers among the cryptocurrencies under a downward risk tendency are stronger than those under an upward risk tendency. A difference in spillover direction under upward and downward risk tendencies exists in the Monero market. In particular, the risk spillover index between Bitcoin and Ripple is −0.513% under upward risk tendency while it is −0.920% under downward risk tendency. Similarly, the risk spillover indexes from Bitcoin to Stellar and Dash are 1.824 and 0.689%, respectively, under upward risk tendency, while they are 2.607 and 2.231% under downward risk tendency. Monero accepts risk transmissions from the other cryptocurrencies with large capitalization under risk upward tendency, while it transmits the risks to those cryptocurrencies in downward risk tendency. The risk spillovers in other pairs of cryptocurrencies mostly maintain the same directions under upward and downward risk tendencies.

Third, the mean and range of risk spillover at different timescales show heterogeneity. The static risk spillovers mainly happen at medium- and long-term frequencies. The risk spillovers at medium-term frequency are mostly stronger than those at long-term frequency, while the spillover directions mostly remain the same. Focusing on the dynamic characteristics of risk spillovers among the cryptocurrencies, the means of risk spillover at long-term frequency are relatively larger than those at medium-term frequency, while the ranges of risk spillovers at medium-term frequency are distinctly larger than those at long-term frequency. In addition, the risk spillover fluctuations at long-term frequency are stronger than those at medium-term frequency if the corresponding risk spillover levels maintain the same comparison at long-term and short-term frequencies. However, for cryptocurrencies whose risk spillover levels at long-term frequency are lower than at medium-term frequency, the risk spillover fluctuations at long-term frequency are distinctly weaker than those at medium-term frequency.

The empirical results have some policy implications for regulators. Regulators should establish a monitoring and warning system for risk. The risk spillovers among the cryptocurrencies show heterogeneity under different risk tendencies, whereas the spillover directions almost remain the same. Thus, a risk monitoring and warning system would be able to identify market behavior well and transmit valuable market information. In addition, some regulatory policies should aim at risk spillovers within 4–30 days. The large risk spillover fluctuations and ranges among the cryptocurrencies in the medium term pose new challenges for market supervision. Thus, the regulators should generate policies, such as determining a trading threshold, to control the risk spillovers among the cryptocurrencies, improving the market efficiency in the medium term. For the investors, the delayed effect of risk spillovers among the cryptocurrencies should be paid attention to when generating investment strategies. Major events may shock the cryptocurrency markets strongly. Study of the delayed effects of the shocks helps investors generate investment strategies unifying their own situations. The analysis of the heterogeneity in risk spillovers among the cryptocurrencies at different timescales can provide information with which investors to identify the effects of event shocks. Furthermore, our empirical results also provide some suggestions for government supervision of the design of a new cryptocurrency. On the one hand, we should monitor the risks of cryptocurrencies with large capitalization and construct a warning system. On the other hand, two restrictions on trading volumes of cryptocurrencies should be considered. Firstly, we should use different restrictions on trading volumes under different conditions. Under downward risk tendency, we can set lower thresholds for trading volume to prevent the large-dollar investors from entering the markets, leading to a risk increase for new cryptocurrencies, whereas under an upward risk tendency, investors should be attracted into the markets by setting higher thresholds for trading volume and stimulated to trade more frequently, driving the market mechanism to reduce the risks. Secondly, we should restrict trading volumes of medium-term investors. In this way, the uncertainty of spillover among the cryptocurrency markets can be reduced, and market stability can be well-protected.

DATA AVAILABILITY STATEMENT

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct and intellectual contribution to the work, and approved it for publication.

FUNDING

This work was supported by the National Natural Science Foundation of China (No. 11701115) and Guangdong Natural Science Foundation (No. 2018A030313115).

REFERENCES

1. Diebold F, Yilmaz K. Better to give than to receive: predictive directional measurement of volatility spillovers. *Int J Forecast*. (2012) **28**:57–66. doi: 10.1016/j.ijforecast.2011.02.006
2. Vandezande N. Virtual currencies under EU anti-money laundering law. *Comput Law Sec Rev*. (2017) **33**:341–53. doi: 10.1016/j.clsr.2017.03.011
3. Gyamerah SA. Modelling the volatility of Bitcoin returns using GARCH models. *Quant Finance Econ*. (2019) **3**:739–53. doi: 10.3934/QFE.2019.4.739
4. Bariviera A, Basgall M, Hasperué W, Naiouf M. Some stylized facts of the Bitcoin market. *Phys A Stat Mech Appl*. (2017) **484**:82–90. doi: 10.1016/j.physa.2017.04.159
5. Fry J, Cheah E. Negative bubbles and shocks in cryptocurrency markets. *Int Rev Financ Anal*. (2016) **47**:343–52. doi: 10.1016/j.irfa.2016.02.008
6. Yarovaya L, Brzeszczyński A, Lau C. Intra-and inter-regional return and volatility spillovers across emerging and developed markets: evidence from stock indices and stock index futures. *Int Rev Financ Anal*. (2016) **43**:96–114. doi: 10.1016/j.irfa.2015.09.004
7. Bouri E, Jalkh N, Molnár P, Roubaud D. Bitcoin for energy commodities before and after the December 2013 crash: diversifier, hedge or safe haven? *Appl Econ*. (2017) **49**:5063–73. doi: 10.1080/00036846.2017.1299102
8. Bouri E, Das M, Gupta R, Roubaud D. Spillovers between Bitcoin and other assets during bear and bull markets. *Front Neurosci*. (2018) **50**:5935–49. doi: 10.1080/00036846.2018.1488075
9. Corbet S, Meegan A, Larkin C, Yarovaya L. Exploring the dynamic relationships between cryptocurrencies and other financial assets. *Econ Lett*. (2018) **165**:28–34. doi: 10.1016/j.econlet.2018.01.004
10. Ji Q, Bouri E, Gupta R, Roubaud D. Network causality structures among Bitcoin and other financial assets: a directed acyclic graph approach. *Q Rev Econ Finance*. (2018) **70**:203–13. doi: 10.1016/j.qref.2018.05.016
11. Ji Q, Bouri E, Kristoufek L. Information interdependence among energy, cryptocurrency and major commodity markets. *Energy Econ*. (2019) **81**:1042–55. doi: 10.1016/j.eneco.2019.06.005
12. Nan Z, Kaizojir T. Bitcoin-based triangular arbitrage with the Euro/U.S. dollar as a foreign futures hedge: modeling with a bivariate GARCH model. *Quant Finance Econ*. (2019) **3**:347–65. doi: 10.3934/QFE.2019.2.347
13. Gajardo G, Kristjanpoller W, Minutolo M. Does Bitcoin exhibit the same asymmetric multifractal cross-correlations with crude oil, gold and DJIA as the Euro, Great British Pound and Yen? *Chaos Solit Fract*. (2018) **109**:195–205. doi: 10.1016/j.chaos.2018.02.029
14. Ji Q, Bouri E, Lau C, Roubaud D. Dynamic connectedness and integration in cryptocurrency markets. *Int Rev Financ Anal*. (2019) **63**:257–72. doi: 10.1016/j.irfa.2018.12.002
15. Shahzad S, Hernandez J, Rehman M, Al-Yahyaee K, Zakaria M. A global network topology of stock markets: transmitters and receivers of spillover effects. *Phys A Stat Mech Appl*. (2018) **492**:10127–34. doi: 10.1016/j.physa.2017.11.132
16. Zhang D, Lei L, Ji Q, Kutan A. Economic policy uncertainty in the US and China and their impact on the global markets. *Econ Modell*. (2019) **79**:47–56. doi: 10.1016/j.econmod.2018.09.028
17. Ahmad W, Mishra A, Daly K. Financial connectedness of BRICS and global sovereign bond markets. *Emerg Markets Rev*. (2018) **37**:1–16. doi: 10.1016/j.ememar.2018.02.006
18. Louzis D. Measuring spillover effects in Euro area financial markets: a disaggregate approach. *Empir Econ*. (2015) **49**:1367–400. doi: 10.1007/s00181-014-0911-x
19. Baruník J, Kočenda E, Vácha L. Asymmetric volatility connectedness on the forex market. *J Int Money Finance*. (2017) **77**:39–56. doi: 10.1016/j.jimonfin.2017.06.003
20. Singh V, Nishant S, Kumar P. Dynamic and directional network connectedness of crude oil and currencies: evidence from implied volatility. *Energy Econ*. (2018) **76**:48–63. doi: 10.1016/j.eneco.2018.09.018
21. Ji Q, Geng J, Tiwari A. Information spillovers and connectedness networks in the oil and gas markets. *Energy Econ*. (2018) **75**:71–84. doi: 10.1016/j.eneco.2018.08.013
22. Ji Q, Zhang D, Geng J. Information linkage, dynamic spillovers in prices and volatility between the carbon and energy markets. *J Clean Prod*. (2018) **198**:972–8. doi: 10.1016/j.jclepro.2018.07.126
23. Wei W. Liquidity and market efficiency in cryptocurrencies. *Econ Lett*. (2018) **168**:21–24. doi: 10.1016/j.econlet.2018.04.003
24. Yi S, Xu Z, Wang G. Volatility connectedness in the cryptocurrency market: is Bitcoin a dominant cryptocurrency. *Int Rev Financ Anal*. (2018) **60**:98–114. doi: 10.1016/j.irfa.2018.08.012
25. ElBahrawy A, Alessandretti L, Kandler A, Pastor-Satorras R, Baronchelli A. Evolutionary dynamics of the cryptocurrency market. *R Soc Open Sci*. (2017) **4**:170623. doi: 10.1098/rsos.170623
26. Yang K, Wei Y, Li S, He J. Asymmetric risk spillovers between Shanghai and Hong Kong stock markets under China's capital account liberalization. *North Am J Econ Finance*. (2020) **51**:101100. doi: 10.1016/j.najef.2019.101100
27. Mensi W, Hammoudeh S, Kang S. Risk spillovers and portfolio management between developed and BRICS stock markets. *North Am J Econ Finance*. (2017) **41**:133–55. doi: 10.1016/j.najef.2017.03.006
28. Collet J, Ielpo F. Sector spillovers in credit markets. *J Banking Finance*. (2018) **94**:267–78. doi: 10.1016/j.jbankfin.2018.07.011
29. Wang G, Xie C, He K, Stanley H. Extreme risk spillover network: application to financial institutions. *Quant Finance*. (2017) **17**:1417–33. doi: 10.1080/14697688.2016.1272762
30. Buse R, Schienle M. Measuring connectedness of euro area sovereign risk. *Int J Forecast*. (2019) **35**:25–44. doi: 10.1016/j.ijforecast.2018.07.010
31. Debarsy N, Dossougoin C, Ertur C, Gnabo J. Measuring sovereign risk spillovers and assessing the role of transmission channels: a spatial econometrics approach. *J Econ Dyn Control*. (2018) **87**:21–45. doi: 10.1016/j.jedc.2017.11.005
32. Shahzad S, Hernandez J, Al-Yahyaee K, Jammazi R. Asymmetric risk spillovers between oil and agricultural commodities. *Energy Policy*. (2018) **118**:182–98. doi: 10.1016/j.enpol.2018.03.074
33. Wen D, Wang G, Ma C, Wang Y. Risk spillovers between oil and stock markets: a VAR for VaR analysis. *Energy Econ*. (2019) **80**:524–35. doi: 10.1016/j.eneco.2019.02.005
34. Reboredo J, Rivera-Castro M, Ugolini A. Downside and upside risk spillovers between exchange rates and stock prices. *J Banking Finance*. (2016) **62**:76–96. doi: 10.1016/j.jbankfin.2015.10.011
35. Balcilar M, Demirer R, Hammoudeh S, Nguyen D. Risk spillovers across the energy and carbon markets and hedging strategies for carbon risk. *Energy Econ*. (2016) **54**:159–72. doi: 10.1016/j.eneco.2015.11.003
36. Bollerslev T. Generalized autoregressive conditional heteroskedacticity. *J Economet*. (1986) **31**:307–27. doi: 10.1016/0304-4076(86)90063-1
37. Engle R, Manganelli S. CAViaR: conditional autoregressive value at risk by regression quantiles. *J Bus Econ Stat*. (2004) **22**:367–81. doi: 10.1198/073500104000000370
38. Koenker R, Basset G. Regression quantiles. *Econometrica*. (1978) **46**:33–50. doi: 10.2307/1913643

39. Joets M. Energy price transmissions during extreme movements. *Econ Modell*. (2014) **40**:392–9. doi: 10.1016/j.econmod.2013.11.023
40. Ahn D, Boudoukh J, Richardson M, Whitelaw R. Partial adjustment or stale prices? Implications from stock index and futures return autocorrelations. *Rev Financ Stud*. (2002) **15**:655–89. doi: 10.1093/rfs/15.2.655
41. Jondeau E, Rockinger M. Testing for differences in the tails of stock-market returns. *J Empir Finance*. (2003) **10**:559–81. doi: 10.1016/S0927-5398(03)00005-7
42. Laporta A, Merlo L, Petrella L. Selection of value at risk models for energy commodities. *Energy Econ*. (2018) **74**:628–43. doi: 10.1016/j.eneco.2018.07.009
43. Li Z, Dong H, Huang Z, Failler P. Asymmetric effects on risks of virtual financial assets (VFAs) in different regimes: a case of Bitcoin. *Quant Finance Econ*. (2018) **2**:860–83. doi: 10.3934/QFE.2018.4.860
44. Chow H. Volatility spillovers and linkages in Asian stock markets. *Emerg Markets Finance Trade*. (2017) **53**:2770–81. doi: 10.1080/1540496X.2017.1314960
45. Prasad N, Grant A, Kim S. Time varying volatility indices and their determinants: evidence from developed and emerging stock markets. *Int Rev Financ Anal*. (2018) **60**:115–26. doi: 10.1016/j.irfa.2018.09.006
46. Baruník J, Křehlík T. Measuring the frequency dynamics of financial connectedness and systemic risk. *J Financ Economet*. (2018) **16**:271–96. doi: 10.1093/jjfinec/nby001

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 26 November 2020
doi: 10.3389/fphy.2020.582817

Dynamic Network Connectedness of Bitcoin Markets: Evidence from Realized Volatility

Shuanglian Chen[1] *and Hao Dong*[2]*

[1]Guangzhou International Institute of Finance and Guangzhou University, Guangzhou, China, [2]School of Economics and Statistics, Guangzhou University, Guangzhou, China

In this paper, we explore the volatility spillovers across different Bitcoin markets. We decompose the realized volatility into common and idiosyncratic volatilities, as well as the good and bad volatilities. Then the asymmetry in volatility spillovers between Bitcoin markets is measured by the DY (Diebold and Yilmaz) index. In addition, we construct statistics to test the asymmetry in volatility spillovers between different Bitcoin markets. The results are achieved as follows. The spillovers of systematic and idiosyncratic volatilities dominate the connectedness among different Bitcoin markets. In addition, the idiosyncratic volatility spillovers are more easily influenced by policies. Good volatility spillovers dominate the Bitcoin markets and change over time. The further results suggest that there is significant asymmetry between systematic and idiosyncratic volatility spillovers in the Bitcoin markets, while the asymmetries between good and bad volatility spillovers are heterogeneous in different markets. The findings in this paper can provide some suggestions for regulators controlling market stability and investors generating investment strategies.

Keywords: asymmetric, connectedness, bitcoin, realized volatility, good and bad volatility, common and idiosyncratic volatility

OPEN ACCESS

Edited by:
Jianguo Liu,
Shanghai University of Finance and Economics, China

Reviewed by:
Jie Cao,
Nanjing University of Finance and Economics, China
Qing Cheng,
National University of Defense Technology, China

***Correspondence:**
Hao Dong
donghao@e.gzhu.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *13 July 2020*
Accepted: *30 September 2020*
Published: *26 November 2020*

Citation:
Chen S and Dong H (2020) Dynamic Network Connectedness of Bitcoin Markets: Evidence from Realized Volatility. Front. Phys. 8:582817. doi: 10.3389/fphy.2020.582817

1 INTRODUCTION

Both the market value and amount of cryptocurrency have risen greatly since 2016. Meanwhile, the increased price has been accompanied with strong volatility. For instance, the Bitcoin as the leading cryptocurrency fell more than 40% to less than $12,000 within a month from more than $20,000 on December 17, 2017. Some people attribute such a rapid rise to the block chain technology, believing that Bitcoin can exceed $100,000, while some others deem that cryptocurrencies are speculation products rather than exchange mediums (10; [17, 37]; and Bitcoin is prone to bubble [20, 31]. In order to further recognize the price discovery function of Bitcoin in the financial market, meeting the investors demand on cryptocurrencies, the U.S. financial corporations CME and CBOE have issued Bitcoin futures, respectively. In addition, Bitcoin is an option for portfolio, asset allocation, and hedging [28] as it is distinctly different in return, volatility, and correlation from other assets [11]. The Bitcoin, which is a leading cryptocurrency with a long history as well as the largest market capitalization, has a total amount at the early design stage. The Bitcoin markets, whose pricing data are available immediately and free of charge to anyone worldwide with internet access, usually behave differently in prices across different markets. Price volatility as an important indicator investigating market dynamics, reflects the market reaction to new information, and influences the trading volume, whose fluctuation reflects different investor understanding on the new information.

Indeed, connectedness among price volatilities across different Bitcoin markets provides knowledge on the spread and absorption of market information flows and extend to which price reflects the market information. The volatility connectedness has been explored in stock markets [16, 19, 48, 53], futures markets [36, 58], and commodity markets [3, 4, 21, 34]. We believe that it is necessary to pay attention to the volatility connectedness across Bitcoin markets. Reference [61] analyzed the cross-correlations of the return-volume relationship across the Bitcoin markets. Reference [52] identified the price inconsistencies across the markets. In this paper, the volatility connectedness across the Bitcoin markets is addressed.

Systematic and idiosyncratic decompositions for financial variables have been considered important in main stream finance literature [32]. Reference [50] used the quantile-on-quantile Granger causality test to investigate extreme risk spillover from the crude oil market to firm return in China. They provided evidence of extreme risk spillovers from crude oil price shocks to firm returns. Their results indicate that the industrial characteristics of a firm matters. Reference [18] investigated the relationship between crude oil and stock using firm-level data and a bottom-up approach. Following the same logic of Ref. [47]; they explicitly modeled systematic and idiosyncratic risks using a capital asset pricing model in the oil-stock relationship for each stock and then aggregated them for the market-wide results. Reference [45] investigated the inter-connectedness between WTI oil price returns and the returns of listed firms in the U.S. energy sector. They focused on the issue of whether firm-level idiosyncratic information matters. A generalized dynamic factor model was used to separate systematic components from idiosyncratic components in these energy stocks. On the other hand, systematic and idiosyncratic contagion are underlined in the existing literature. In a financial system, systematic contagion is driven by common factors that affect all the participants, while idiosyncratic contagion is caused by factors that are specific to the individuals [6]. This distinction contributes to making clear the potential contagion drivers and the channels by which contagion occurs. They are essential for regulators and policymakers to monitor financial stability. Some works distinguish the systematic and idiosyncratic contagion through the traditional regression models [9, 25–27]. Reference [6] applied principal component analysis and a generalized vector autoregressive framework proposed by Ref. [22]) to differentiate the systematic and idiosyncratic contagion. Ref. [38] proposed a network-based framework to distinguish systematic and idiosyncratic contagion and dealt with the situation that the number of financial institutes involved in the contagion is sufficiently large. Most existing literature on systematic and idiosyncratic decomposition contribute to the oil-stock relationship and financial crisis. To our knowledge, it has not been applied in the cryptocurrency market. In this paper, we will explore systematic and idiosyncratic volatility in the Bitcoin markets. In addition, network connectedness of systematic and idiosyncratic volatility in the Bitcoin markets is constructed.

Despite the popularity and versatility of the DY index, which was developed by Ref. [22] to measure both total and directional volatility spillovers, it cannot not distinguish potential asymmetry in spillovers that originate due to both good and bad uncertainty. A market volatility may be higher as institutes in that market make it advantageous for firms to take risks that lead to greater market growth [1, 24, 39]. Alternatively, a market volatility may also be high because of the market-specific forces, such as political risks, that impose risks on firms that they can not shed [8]. In the former case, volatility is good as it results from positive shocks that enable markets to be more productive. In contrast, the bad volatility associated with the latter case can destabilize the market and prevent its growth. As suggested by Ref. [54]; one can decompose the aggregate volatility into "good" and "bad" volatility components, which are associated with positive and negative innovations to market returns. These two volatility components have opposite impacts on asset prices and market growth. Ref. [7] decomposed the realized daily volatility calculated by intraday returns into good and bad volatility, which separately captured the volatility component associated with positive and negative movements in oil prices and the exchange rate, permitting someone to determine whether good volatility shocks propagate differently across currency and oil markets compared to bad volatility shocks. Ref. [13] quantified asymmetries in volatility spillovers that emerge due to bad and good volatility by using data covering most liquid U.S. stocks in seven sectors. They provided sample evidence for the asymmetric connectedness of stocks at the disaggregate level, while they provided evidence for asymmetric volatility connectedness on forex markets by showing how bad and good volatility propagate through forex markets [14]. Reference [15] analyzed total, asymmetric, and frequency connectedness between the oil and forex markets using high-frequent intraday data by employing variance decompositions and spectral representation in combination with realized semi-variances to account for asymmetric and frequency connectedness. Reference [2] paid attention to the potential asymmetries from good and bad volatility in the causal linkages between the crude oil and forex markets. Reference [55] examined asymmetric volatility spillovers between crude and international stock markets. They provided evidence that bad total volatility spillovers dominate the system and change over time, suggesting that a pessimistic mood and uninformed traders who tend to increase volatility dominate in the markets. However, among the existing literature on asymmetries from good and bad volatility, as well as their volatility spillovers, we should note that sufficient attention has not been paid in the cryptocurrency markets. In this paper, we will construct a network connectedness of good volatility and bad volatility among Bitcoin markets and explore the asymmetric spillovers of good and bad volatility in Bitcoin markets.

The contribution of the current paper can be summarized as follows. First, we explore the time-varying characteristic of leading roles played by systematic and idiosyncratic volatilities in different Bitcoin markets. The time-varying dominance of common volatility and characteristic volatility spillovers in the Bitcoin markets helps to identify the influencing factors of Bitcoin price changes, that is, whether the Bitcoin price changes are caused by the evolution of Bitcoin itself or by changes in market

policy attitudes and investor sentiment. The leading roles between Bitcoin markets enable global investors to use Bitcoin assets for the purposes of diversification and to reduce risks. The leading roles also allow the possibility of forming portfolios to increase returns, which can generate clear benefits for financial market investors and risk management. Second, we continue to explore the time-varying characteristic of leading roles played by good and bad volatilities in different Bitcoin markets. In this way, we complete the construction of network connectedness of Bitcoin markets. This dominant time variability helps investors identify the impact of policy news on Bitcoin price volatility. Concretely, volatility is good in that it results from positive policy news that enables Bitcoin price to be more productive. In contrast, the bad volatility associated with negative policy news can destabilize the market and prevent its growth. Third, we examine the asymmetric spillovers of systematic and idiosyncratic volatility in Bitcoin markets and lastly, asymmetric spillovers of good and bad volatility are addressed as well. This could shed light on whether spillovers are higher or lower during a specific period. Asymmetric spillover in volatility on Bitcoin markets indicates that past returns are highly correlated with present volatility. As volatility is transferred across markets by spillovers, it is reasonable to believe that volatility spillovers exhibit asymmetries as well and that such asymmetries might stem from qualitative differences due to different information. Our evidence supports this prediction. In this way, we construct the asymmetric network connectedness of Bitcoin markets.

The paper is organized as follows. In **Section 2**, we present the network connectedness of systematic and idiosyncratic volatility in Bitcoin markets, involving the measurement of systematic and idiosyncratic volatility, and static and dynamic analysis of the network connectedness. Similar results for good and bad volatility in Bitcoin markets are presented in **Section 3**. The asymmetric network connectedness in Bitcoin markets is addressed in **Section 4**. In **Section 5**, we conclude the paper with some policy implications.

2 NETWORK CONNECTEDNESS OF COMMON AND IDIOSYNCRATIC VOLATILITY IN BITCOIN MARKETS

2.1 The Measurement of Realized Volatility

The realized volatility can better reflect the Bitcoin price volatility. On the one hand, different from traditional financial assets, as it does not admit price limit, together with the globalization and convenience, the Bitcoin price can fluctuate strongly in a short time. Accordingly, we measure the Bitcoin price volatility by using highly frequent data. On the other hand, the price of Bitcoin, which is one of speculative assets, can be influenced by information acquisition and propagation rate. Considering the instantaneity of information, highly frequent data may better reflect the effects of information on the Bitcoin price volatility [33, 57]. Accordingly, we use the realized volatility, proposed by Ref. [5]; to measure the price volatilities in different Bitcoin markets.

Denote by $r^i_{t,j}$ the return rate in the Bitcoin market i:

$$r^i_{t,j} = 100 * \left(ln\, p^i_{t,j} - ln\, p^i_{t,j-1} \right).$$

where $i = 1, 2, \ldots, 6$ represents different Bitcoin markets, which are USD, EUR, JPY, PLN, IDR, and KRW. t represents the time while j represents the time period. In this paper, we use the data with 5-min frequency, which suggest that $j = 1, 2, \ldots, (1440/5) = 288$. $lnp^i_{t,j}$ and $lnp^i_{t,j-1}$ represent the Logarithmic prices of Bitcoin market i at time j and j-1 in trading day t.

Accordingly, for the market i and a specific business day t, the realized volatility RV^i_t can be calculated as the sum of the squared intraday returns $r^i_{t,j}$:

$$RV^i_t = \sum_{j=1}^{288} r^{i,2}_{t,j},\ t = 1, 2, \ldots, T,$$

where T is the sample period.

In this paper, we decompose the realized volatility into systematic and idiosyncratic volatilities, to explore the asymmetry between systematic and idiosyncratic volatility spillovers. To identify the role of idiosyncratic information in the spillover among the Bitcoin markets, this paper employs generalized dynamic factor models (GDFM), proposed by Ref. [12]; to decompose the realized volatility into both systematic and idiosyncratic components. The method is also used by Ref. [30]. Consider a six-dimensional vector of realized volatility $\{Y_{it}\} = (RV^1_t, RV^2_t, \ldots, RV^6_t)'$, which can be decomposed into a systematic volatility X_{it} and an idiosyncratic volatility Z_{it}, such as:

$$Y_{it} = X_{it} + Z_{it} =: \sum_{k=1}^{Q} b_{ik}(L) u_{kt} + Z_{it}.$$

where, $\{X_{it}\} = (RV^{S1}_t, RV^{S2}_t, \ldots, RV^{S6}_t)$ is systematic volatility, $\{Z_{it}\} = (RV^{I1}_t, RV^{I2}_t, \ldots, RV^{I6}_t)$. Q is the number of systematic volatility factors, which is determined by the variance contribution rate. Additionally, u_{kt} stands for orthonormal white noise, L is the lag operator and $b_{ik}(L)$ are one-sided square-summable filters.

2.2 The Measurement of Network Connectedness

In this paper, we measure the connectedness among different Bitcoin markets by the DY spillover index. Most existing literature measures connectedness by the DCC-GARCH model [46, 56] and copula model (41; [35, 44]. On the one hand, these models focus on the connectedness of two or three markets rather than measuring the connectedness among many markets. On the other hand, the delay effect of Bitcoin price volatility and the interplay among the Bitcoin markets motivate us to investigate the volatility spillovers. Recently the connectedness model, which is based on a VAR model approach proposed by Ref. 23, has been widely used to measure system spillover in the finance and commodity market [40–43, 59, 60]. Using forecasting error variance decomposition (FEVD) of the VAR model and a rolling-windows approach, the method provides a simple yet effective way for understanding the static and dynamic spillovers among different Bitcoin markets.

Start from a p -th order, the VAR(p) model is as follows:

$$RV_t = \sum_{i=1}^{p} \phi_i RV_{t-i} + \varepsilon_t. \quad (1)$$

$$RV_t = \sum_{i=1}^{\infty} A_i \varepsilon_{t-i}, \quad (2)$$

where, $RV_t = (RV_t^1, RV_t^2, \ldots, RV_t^6)$, i is the delay order, obtained by the AIC or BIC criterion. ε_t is the vector of disturbances and are assumed to be independently and identically distributed. Given the assumption of stationarity of the VAR model, **Eq. 1** can be converted into **Eq. 2** in an infinite order vector moving average (VMA) representation, where A_i is the 6×6 coefficient matrix, defined as

$$A_i = \phi_1 A_{i-1} + \phi_2 A_{i-2} + \cdots + \phi_p A_{i-p}.$$

Standard FEVD results tend to be sensitive to the ordering of variables in VAR models. Reference 23 suggested to use the generalized FEVD approach [51] to solve this problem. They define $\theta_{ij}(H)$ as the contribution from market i to market j, which is written as

$$\theta_{ij}(H) = \frac{\sigma_{ii}^{-1} \sum_{h=0}^{H} \left(e_i' A_h \Sigma e_j \right)^2}{\sum_{h=0}^{H} \left(e_i' A_h \Sigma A_h' e_i \right)^2},$$

where Σ is the variance-covariance matrix of the error term, σ_{ii} is the standard deviation of ε_i; e_j is a selection vector, which equals one for the jth element and 0 otherwise. The contributions of $\theta_{ij}(H)$ can be normalized in the form of $\tilde{\theta}_{ij}(H) = \theta_{ij}(H) / \sum_{j=1}^{N} \theta_{ij}(H)$, whereas it is easy to prove that $\sum_{j=1}^{N} \tilde{\theta}_{ij}(H) = 1$ and $\sum_{i,j=1}^{N} \tilde{\theta}_{ij}(H) = N$.

By excluding self-contributions in the system, the total spillover index (TSI), denoted by S(H), can be written as:

$$S(H) = 100 \times \frac{\sum_{i,j=1, i \neq j}^{N} \tilde{\theta}_{ij}(H)}{\sum_{i,j=1}^{N} \tilde{\theta}_{ij}(H)} = 100 \times \frac{\sum_{i,j=1, i \neq j}^{N} \tilde{\theta}_{ij}(H)}{N}.$$

We calculate the from and to spillovers among different Bitcoin markets by **Formulas (3)** and **(4)**

$$To_i(H) = 100 \times \sum_{j=1, i \neq j}^{N} \tilde{\theta}_{ji}(H), \quad (3)$$

$$\mathbf{From}_i(H) = 100 \times \sum_{j=1, i \neq j}^{N} \tilde{\theta}_{ij}(H). \quad (4)$$

Furthermore, we calculate the net spillover

$$S_{i,net}(H) = To_i(H) - From_i(H).$$

Similarly, the net pairwise measure can be written as

$$NPS_{ij}(H) = \left(\tilde{\theta}_{ji}(H) - \tilde{\theta}_{ij}(H) \right) \times 100.$$

2.3 Asymmetric Network Connectedness of Common and Idiosyncratic Volatility

In this paper, we chose six Bitcoin markets according to their trading volume, which were USD (BitStamp), EUR (Kraken), JPY (Coincheck), PLN (BitBay), IDR (Infomax), and KRW (Korbit), where the largest trading platforms in corresponding Bitcoin markets are pointed out in the brackets. According to the availability, the data range from March 6, 2016 to March 15, 2020. The measurement for spillover is through R-3.6.3, while the network figure is through Gephi-0.9.2.

The empirical results show the static and dynamic spillovers of systematic volatility and idiosyncratic volatility among different Bitcoin markets. According to the AIC criterion, we applied the VAR model with a delay order of three to measure the realized volatility in Bitcoin markets while the VAR model with a lagged value of four was applied to measure the systematic and idiosyncratic volatility in Bitcoin markets. Accordingly, we calculated the static volatility spillovers among Bitcoin markets. With regard to dynamic spillovers, in this paper, we set the roll-windows by 60 according to the duration of Bitcoin volatility. We set the n. ahead describing dynamic spillovers of systematic volatility among the Bitcoin markets by 20, while it was set by 10 to describe dynamic spillovers of idiosyncratic volatility among the Bitcoin markets. The numbers 20 and 10 reflect the periods when the volatility shocks in the Bitcoin markets become stable. **Table 1** shows the static volatility spillovers among different Bitcoin markets.

The spillovers between systematic volatility and idiosyncratic volatility dominate the connectedness across different Bitcoin markets. The volatility spillovers among Bitcoin markets after volatility decomposition are significantly stronger than that before decomposition. We can see from the rows "Net" in **Table 1** that the most significantly enhanced volatility spillover after volatility decomposition compared with the total realized volatility spillover before volatility decomposition is

TABLE 1 | Static spillover in realized, common, and idiosyncratic volatility.

	USD	EUR	JPY	PLN	IDR	KRW	From
Panel a: Realized volatility							
USD	75.98	16.60	5.41	0.82	1.14	0.05	4.00
EUR	10.69	83.22	4.33	0.52	1.20	0.03	2.80
JPY	11.52	5.29	77.16	0.69	5.31	0.02	3.81
PLN	12.70	5.76	3.68	74.49	3.34	0.02	4.25
IDR	13.58	5.81	16.17	0.99	63.41	0.03	6.10
KRW	0.76	0.31	0.46	0.04	0.40	98.02	0.33
To	8.21	5.63	5.01	0.51	1.90	0.03	21.29
Net	4.21	2.83	1.2	–3.74	–4.2	–0.3	—
Panel B: Systematic volatility							
USD	40.72	42.34	7.20	1.92	7.59	0.23	9.88
EUR	40.46	42.28	7.17	1.88	7.98	0.23	9.62
JPY	41.04	41.07	6.98	1.95	8.71	0.25	15.50
PLN	41.50	41.58	6.52	2.47	7.64	0.28	16.25
IDR	41.20	41.25	7.32	1.81	8.20	0.22	15.30
KRW	33.67	19.98	12.87	1.32	22.19	9.96	15.01
To	32.98	31.04	6.85	1.48	9.02	0.20	81.57
Net	23.1	21.42	–8.65	–14.77	–6.28	–14.81	—
Panel c: Idiosyncratic volatility							
USD	16.75	3.52	32.82	30.84	10.07	6.00	13.87
EUR	9.47	10.66	32.95	31.85	10.18	4.90	14.89
JPY	6.71	5.30	32.92	32.29	6.61	16.17	11.18
PLN	7.00	5.66	30.95	37.81	6.71	11.87	10.37
IDR	8.14	8.29	37.07	32.73	11.41	2.36	14.76
KRW	6.12	6.73	17.27	42.36	4.93	22.59	12.90
To	6.24	4.92	25.18	28.35	6.42	6.88	77.98
Net	–7.63	–9.97	14	17.98	–8.34	–6.02	—

captured in the KRW market, which are given as 14.81/0.3 = 49 and 6.99/0.3 = 20. It is followed by the JPY market, which is 8.65/1.2 = 7 and 14/1.2 = 11. The most insignificantly enhanced volatility spillover after volatility decomposition compared with the total realized volatility spillover before volatility decomposition is captured in the IDR market, which is 6.28/4.2 = 1.5 and 8.34/4.2 = 2. With regard to spillover direction, the systematic volatility spillover direction is almost consistent with the overall volatility spillover direction, while the idiosyncratic volatility spillover direction is significantly different from that of overall volatility spillover. The volatility spillovers change their directions in the USD, EUR, JPY, and PLN markets, but they stayed the same in the IDR and KRW markets, which can be seen by the signs of values in the rows "Net" in **Table 1**.

The difference of Bitcoin market efficiency determines the asymmetry between systematic volatility spillover and idiosyncratic volatility spillover. On the one hand, the market efficiency determines the level variation of volatility spillover. The market efficiency determines market ability replying to shocks. Considering the speculative nature of Bitcoin, the higher market efficiency leads to stronger market ability replying to shocks, that is a Bitcoin market can well eliminate spillover effects from other Bitcoin markets. Hence, for those entities who have more comprehensive financial markets like USD and EUR, their cryptocurrency markets, like Bitcoin, are more likely to show a stronger ability when replying to market shocks. Due to China's policies on the Bitcoin market, the barycenter of the Bitcoin market has begun to shift to the KRW and JPY markets. Many investors are attracted to invest on these markets, resulting in new challenges for market efficiency. However, the market efficiency cannot realize regulation and control, which results in a larger variation of volatility spillovers in the KRW and JPY markets. Besides, considering aims of speculators to pursue excess return, the development of emerging Bitcoin markets affects the investing decisions of speculators. Accordingly, spillovers from markets like IDR vary weakly.

On the other hand, the market efficiency determines the variation of spillover directions. The markets with higher efficiency, like USD and EUR, play leading roles in the development of Bitcoin. Hence, both USD and EUR show positive spillover directions of systematic volatility, namely that USD and EUR transmit volatilities to other markets. The idiosyncratic volatility reflects the particular roles played by different markets in the development of Bitcoin. The USD and EUR markets usually attract investor attention from other Bitcoin markets, which may affect their price evolution. Thus, the efficiency of Bitcoin markets determines their roles in the price evolution of Bitcoin. This implies the importance of systematic and idiosyncratic volatility spillovers among the Bitcoin markets. We will further analyze the net pairwise spillovers of systematic and idiosyncratic volatility among different Bitcoin markets.

Figure 1 shows the net pairwise spillovers of systematic and idiosyncratic volatility among different Bitcoin markets. The size of the node represents the self-spillover of Bitcoin markets. The lines between two nodes represent the net pairwise spillovers between two Bitcoin markets, while the arrows represent the spillover direction. We can see from **Figure 1** that the spillover direction of systematic volatility is significantly different from that of idiosyncratic volatility. With regard to systematic volatility, it mainly spills from markets with large capitalization to those with small capitalization. More precisely, the systematic volatilities spill significantly from the USD, EUR, and JPY markets to the KRW, PLN, and IDR markets. With regard to idiosyncratic volatility, it spills from markets with small capitalization like KRW, PLN, and IDR to those with large capitalization like USD, EUR, and JPY. These phenomena result from the heterogeneity of different Bitcoin markets in leading the price volatility characteristics of Bitcoin. The systematic volatility

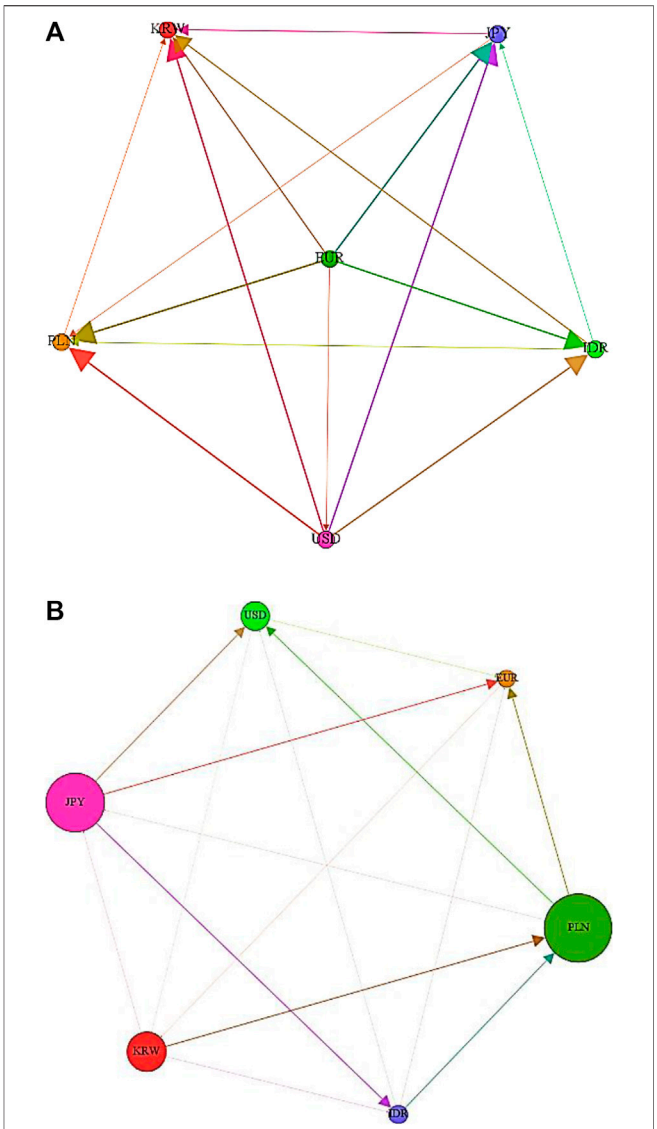


FIGURE 1 | Net pairwise spillover in different Bitcoin markets. Note: I. The lines between two nodes represent the net pairwise spillovers between two Bitcoin markets, while the arrows represent the spillover direction. II. **(A)** stands for net pairwise spillover for systematic volatility, while **(B)** stands for idiosyncratic volatility.

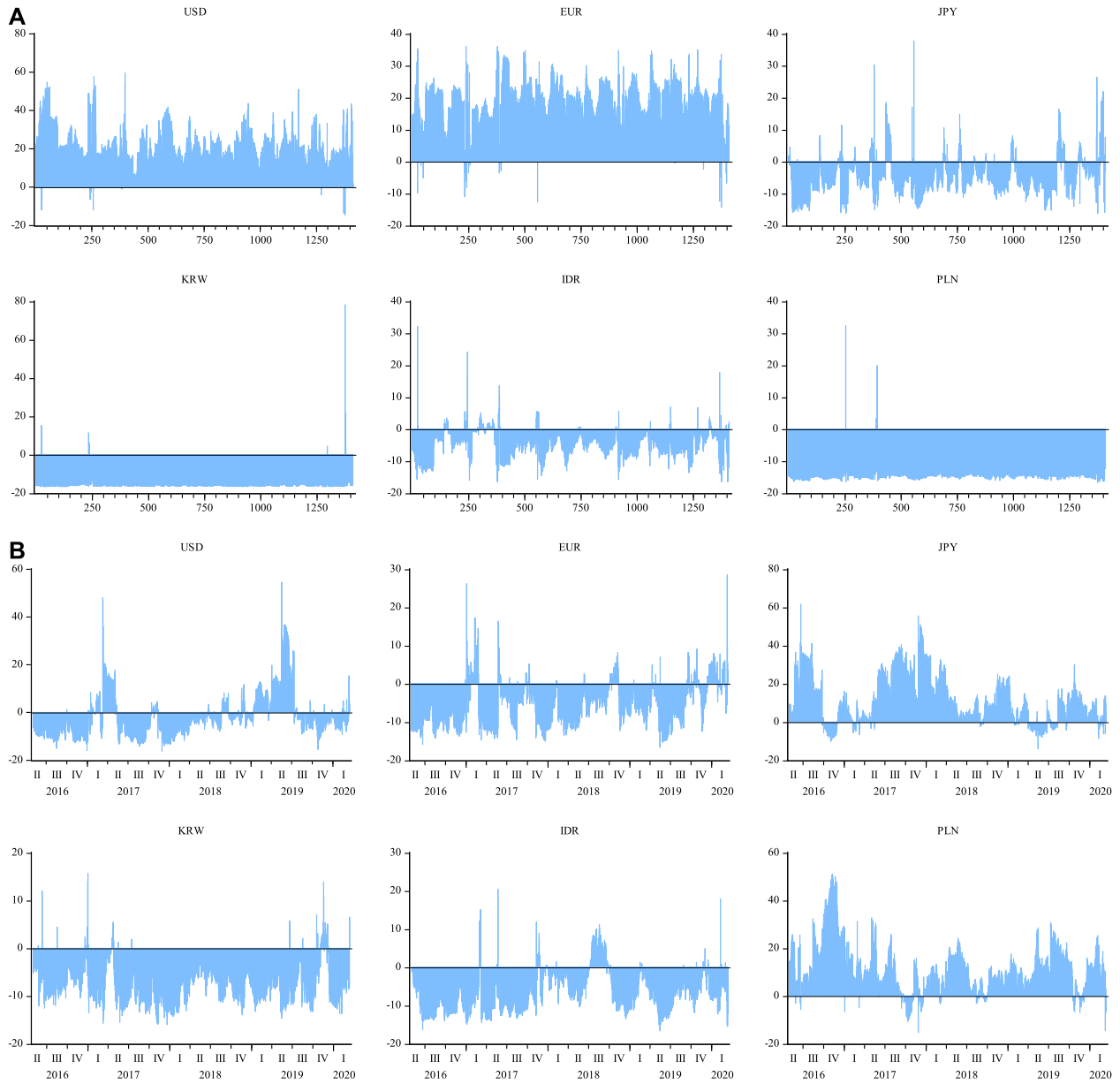


FIGURE 2 | Dynamic net spillover among different Bitcoin markets. **(A)** stands for the dynamic spillover for systematic volatility; **(B)** reports the dynamic spillover for idiosyncratic volatility.

depicts the roles played by different markets in the price volatility characteristics. Markets with small capitalization usually learn from markets with large capitalization on Bitcoin price. More investors are attracted to catch more information on price from markets with large capitalization and generate investment strategies in other Bitcoin markets. Thus the systematic volatility spills from markets with large capitalization to those with small capitalization. The idiosyncratic volatility mainly embodies the heterogeneity of market efficiency. The Bitcoin markets with small capitalization usually admit low market efficiency, which result in a weak ability when replying to price volatility. Markets with large capitalization have strong ability when replying to price volatility. Therefore, as the Bitcoin price fluctuates, the markets with small capitalization show higher market risks due to their weak stability, while those markets with large capitalization show stronger stability. At this time, investors disperse their investment risks by investing across different Bitcoin markets. Accordingly, the idiosyncratic volatility spills from markets with small capitalization to those with large capitalization.

The idiosyncratic volatility spillovers among different Bitcoin markets are more easily influenced by policies. With regard to systematic volatility spillover, the spillover directions almost stay the same in the sample period. In addition, spillovers fluctuate

moderately. We can see from **Figure 2A** that the net spillovers between USD and other markets are almost positive, which is also the case in the EUR market. However, it is not the case in the KRW, PLN, IDR, and JPY markets. With regard to idiosyncratic volatility, the spillover directions change more frequently and the spillover fluctuates strongly. This implies the effects of major events on the idiosyncratic volatility spillovers among different Bitcoin markets. For instance, since September 2017, China has forbidden the issue and trading of cryptocurrencies like Bitcoin. The global Bitcoin market has shifted to the JPY and KRW markets. At this moment, the systematic volatility spillovers among Bitcoin markets fluctuate moderately, while the idiosyncratic volatility spillovers in the JPY and KRW markets fluctuate strongly. Besides, volatility spillovers from other financial markets like stock markets to Bitcoin markets are almost dominated by idiosyncratic volatility spillovers. At the beginning of 2018, regular stock markets around the world were in a state of stagnation. More and more investors began to pay attention to Bitcoin, which resulted in the strong price volatility of Bitcoin. Similarly, the systematic volatility spillovers fluctuated moderately, while the idiosyncratic volatility spillovers among the Bitcoin markets showed stronger fluctuations. As the attitudes to Bitcoin positively grew in different countries, the idiosyncratic volatility spillovers as well as the spillover fluctuations became weaker.

3 NETWORK CONNECTEDNESS OF GOOD AND BAD VOLATILITY IN BITCOIN MARKETS

3.1 The Measurement of Good and Bad Volatility

The transmission of good and bad information among different Bitcoin markets also catches the attention of investors. In fact, the bad volatilities of Bitcoin are related to negative information, such as earnings, spending, and investor sentiment, while the good volatilities are related to the positive information of these variables. Accordingly, we further explored the spillovers between good and bad volatilities in Bitcoin returns. Recently, Ref. [7] decomposed the realized volatility into estimators of realized semi-variance (*RS*) that captured the variance due to negative or positive movements in bad and good volatility of Bitcoin markets. The technique was quickly adopted in several recent contributions (29; [49, 54]. This method can better measure the evolution of good and bad volatilities in the sample period. Concretely, the good volatility of Bitcoin is measured by the positive return of Bitcoin, while the bad volatility is measured by negative return. Accordingly, this method can better reflect the good and bad volatilities of Bitcoin. In addition, it can better capture the relationship between the Bitcoin volatilities in the future and the Bitcoin returns in the past. Thus, we used the realized semi-variance in a similar manner. The negative and positive realized semi-variances ($RS^{i,+}$ and $RS^{i,-}$) of the Bitcoin market are defined as follows:

$$RS_t^{i,-} = \sum_{j=1}^{M_{1i}} I\left(r_{t,j}^i < 0\right) r_{t,j}^{i,2}.$$

$$RS_t^{i,+} = \sum_{j=1}^{M_{2i}} I\left(r_{t,j}^i \geq 0\right) r_{t,j}^{i,2}.$$

where M_{1i} represents the time period when the return is less than 0 in the market i, M_{2i} represents the time period when the return is larger than 0 in the market i. In each Bitcoin market, there holds $M_{1i} + M_{2i} = 288$. Thus, the relationship among realized volatility, and good and bad volatilities can be written as follows:

$$RV_t^i = RS_t^- + RS_t^+$$

and can serve as a measure of downside and upside risk. For instance, negative semi-variance corresponds to bad information causing the return volatility of Bitcoin, and we can use the measure as the empirical proxy for bad volatility as in Ref. [54]. Similarly, positive semi-variance corresponds to good information causing the return volatility of Bitcoin and serves as a proxy for good volatility. In this section, we substitute $RV_t = (RV_t^{1,+}, RV_t^{2,+}, \ldots, RV_t^{6,+})$ and $RV_t = (RV_t^{1,-}, RV_t^{2,-}, \ldots, RV_t^{6,-})$ into (1) and analyze the static and dynamic volatility spillovers among different Bitcoin markets.

TABLE 2 | Static spillover in realized, good, and bad volatility.

	USD	EUR	JPY	PLN	IDR	KRW	From
Panel a: Realized volatility							
USD	75.98	16.60	5.41	0.82	1.14	0.05	4.00
EUR	10.69	83.22	4.33	0.52	1.20	0.03	2.80
JPY	11.52	5.29	77.16	0.69	5.31	0.02	3.81
PLN	12.70	5.76	3.68	74.49	3.34	0.02	4.25
IDR	13.58	5.81	16.17	0.99	63.41	0.03	6.10
KRW	0.76	0.31	0.46	0.04	0.40	98.02	0.33
To	8.21	5.63	5.01	0.51	1.90	0.03	21.29
Net	4.21	2.83	1.2	–3.74	–4.2	–0.3	—
Panel B: Good volatility							
USD	74.83	13.63	8.38	0.30	2.83	0.03	4.19
EUR	15.22	76.09	5.96	0.15	2.56	0.01	3.98
JPY	19.03	7.21	64.06	0.36	9.32	0.01	5.99
PLN	16.37	7.59	3.34	67.46	5.21	0.02	5.42
IDR	19.12	9.12	10.87	0.45	60.43	0.01	6.59
KRW	1.16	0.64	0.66	0.03	0.64	96.88	0.52
To	11.82	6.37	4.87	0.21	3.43	0.01	26.71
Net	7.63	2.39	–1.12	–5.21	–3.16	-0.51	—
Panel c: Bad volatility							
USD	71.55	24.46	2.77	0.72	0.45	0.05	4.74
EUR	4.84	91.93	2.28	0.43	0.48	0.04	1.35
JPY	6.20	5.31	85.64	0.63	2.19	0.03	2.39
PLN	5.46	9.23	1.68	81.85	1.75	0.02	3.03
IDR	7.28	2.90	20.92	1.26	67.61	0.03	5.40
KRW	0.34	0.10	0.31	0.03	0.22	98.99	0.17
To	4.02	7.00	4.66	0.51	0.85	0.03	17.07
Net	–0.72	5.65	2.27	–2.52	–4.55	–0.14	—

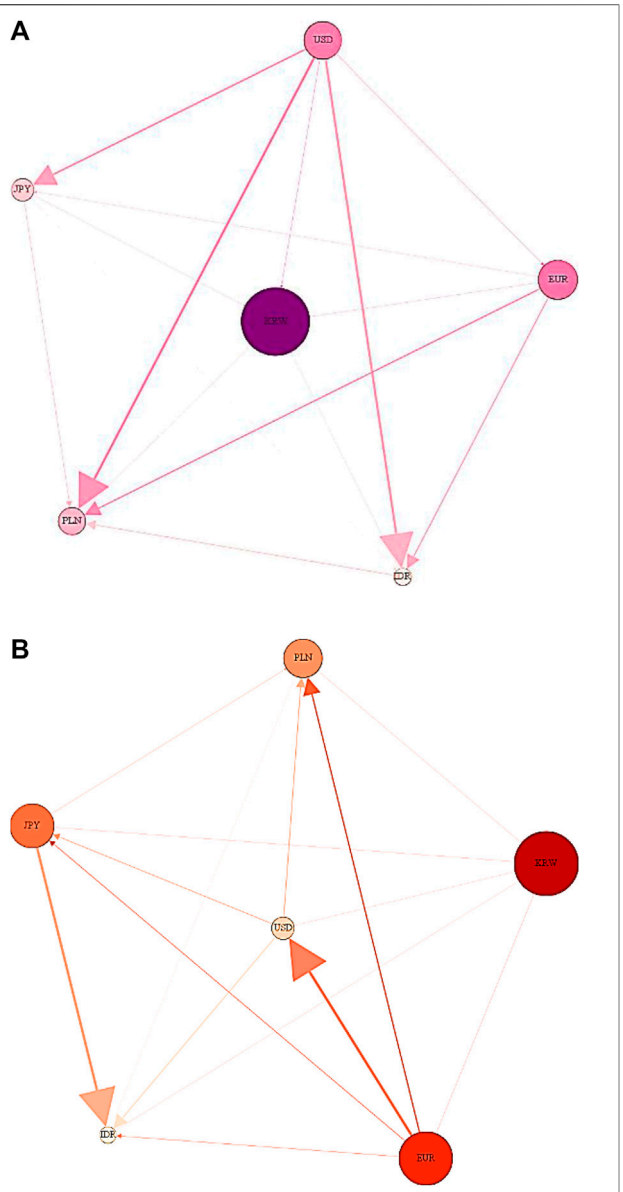


FIGURE 3 | Net pairwise spillover in good and volatility. Note: I. The lines between two nodes represent the net pairwise spillovers between two Bitcoin markets, while the arrows represent the spillover direction. II. **(A)** stands for net pairwise spillover for good volatility, while **(B)** stands for bad volatility.

3.2 Static Analysis of Asymmetric Network Connectedness

Considering the heterogeneity in investor reactions to good (bad) information, we discuss the static asymmetry of good and bad volatility spillovers among different Bitcoin markets. **Table 2** shows the static spillovers of good and bad volatility. **Figure 3** shows the net pairwise spillover of good and bad volatility.

The good volatility dominates the spillovers among different Bitcoin markets. With regard to good volatility spillover, the self-spillovers of individual markets are all weaker than that of the full sample, which suggests that in the environment of good information, the connectedness across different Bitcoin markets is stronger than that in the full sample. On the contrary, for bad volatility spillover, the self-spillovers of individual markets are stronger than that of the full sample, which suggests that in the environment of bad information, the connectedness across different Bitcoin markets is weaker than that in the full sample. This results from the heterogeneity of investor expectation in good and bad volatility spillovers. Therefore, we further analyze the asymmetry between good volatility spillover and bad volatility spillover.

The asymmetry between good and bad volatility spillover among the Bitcoin markets is captured by the self-spillovers of individual markets and mutual spillovers among different markets. The diagonal elements in Panel b and c of **Table 2** depicts the self-spillovers of individual Bitcoin markets, while the net spillover depicts the spillovers among the markets. With regard to the self-spillover, except the U.S. market, other markets show stronger bad volatility spillovers. With regard to mutual spillovers among the markets, the spillover directions of both good and bad volatility are almost the same, while the spillover degrees are significantly different. More precisely, we can see from the rows of "Net" that the spillover levels in the USD, PLN, and KRW markets decrease, while they increase in the EUR, JPY, and IDR markets compared with good volatility. This may result from the heterogeneity of investor expectation in different markets. Good information leads to positive investor expectation on the Bitcoin price. Due to heterogeneous conveniences catching information of investors, besides assimilating good information in the autologous markets, the Bitcoin investors usually obtain information from other markets to generate their investment strategies. Thus, good volatility spillovers among different Bitcoin markets are stronger. On the contrary, bad information not only decreases the investor expectations on Bitcoin, but also challenges the market system. On the one hand, for those markets with more comprehensive market systems like USD, considering the regulation complexity caused by spillovers as well as protecting investors, they usually reduce the spillovers to other markets, reaching a balance status. On the other hand, the migration of primary Bitcoin markets influences the development of the market system. With regard to bad information, for those weakly stable markets like the PLN and KRW markets, investors decide their investor expectation by looking at the price trend of Bitcoin in other markets and then generate their investment strategies. Besides, the markets reduce spillovers from other markets by setting relevant admittance criterion. Thus, relative to good volatility spillovers, the bad volatility spillovers in the USD, PLN, and KRW markets are significantly reduced. The digestive ability of the market itself also determines the asymmetry of spillover. To reply to bad information, the market implements the digestion of information by enhancing autologous efficiency and perfecting an autologous system. At this moment, the self-spillovers of the Bitcoin markets are strong. However, for those markets where investors are diversiform, like EUR, JPY, and IDR, increasing the autologous spillovers cannot better digest bad information. They have to strengthen the connectedness with other markets. Accordingly, relative to good volatility spillovers, the bad

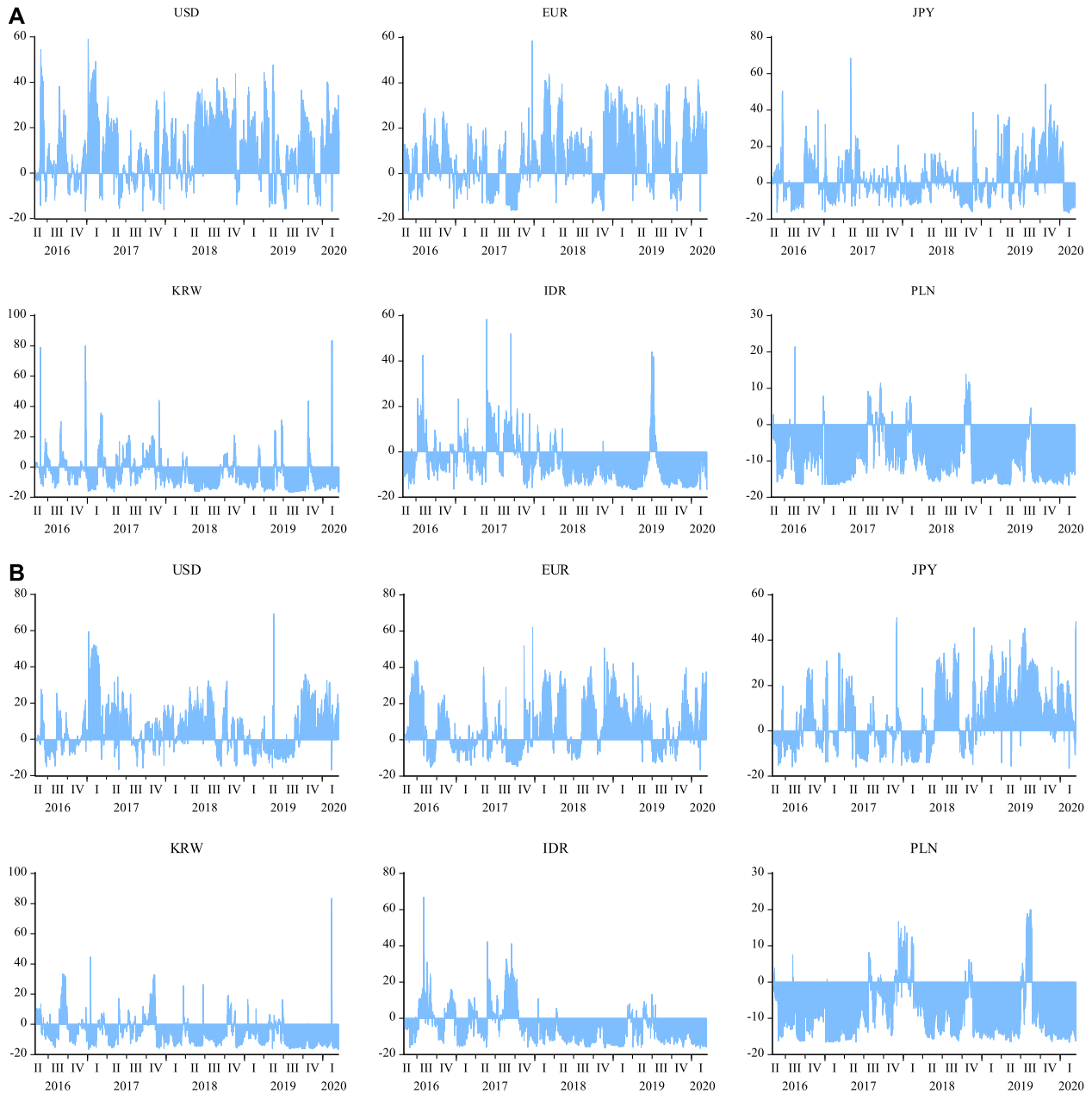


FIGURE 4 | Dynamic net spillover between different Bitcoin markets. **(A)** stands for the dynamic spillover for good volatility; **(B)** reports the dynamic spillover for bad volatility.

volatility spillovers in the EUR, JPY, and IDR markets are significantly enhanced.

The asymmetry of spillover direction between good volatility and bad volatility is not evident. We can see from the arrows in (a) and (b) of **Figure 3** that except the USD, EUR, and KRW markets, both the good volatility and bad volatility spill from markets with large capitalization to markets with small capitalization. It also deserves to be noted that good volatility spills from USD to EUR, while the bad volatility spills from EUR to USD. Besides, KRW receives both good and bad volatility spillovers.

As the markets with large capitalization play the leading roles in the development of Bitcoin price, investors from markets with small capitalization generate rational investment strategies to earn more profits by looking at the price trend of Bitcoin. For the USD and EUR markets, the similarity and superiority of the market system determine the asymmetry of good and bad volatility spillover directions between these two markets. Meanwhile, the policy attitude on financial assets like Bitcoin in the USD and EUR markets also determines the asymmetry of spillover directions. In addition, the particularity of the KRW

market creates opportunities for Bitcoin investors to transfer risks. Due to China's policy attitude toward Bitcoin, the KRW and JPY are gradually becoming primary Bitcoin markets, which attract a great deal of investors. But as the JPY market follows some superior design of the market system, it can better reply to good and bad volatility spillovers of Bitcoin. The instability of the KRW market creates opportunities for speculators to earn excessive profits. Meanwhile, as the attitude of KRW on Bitcoin and the advance of internet technology, the KRW market has been an accepter of volatility spillover.

3.3 Dynamic Analysis of Asymmetric Network Connectedness

Figure 4 shows the dynamic net spillovers of good and bad volatility among different Bitcoin markets, where a) shows the good volatility spillovers and b) shows the bad volatility spillovers. The leading roles of good and bad volatility spillovers are time-varying and heterogeneous in different markets. The good and bad volatility spillover levels determine their leading roles. We can see from the figure that good volatility spillover played a leading role in the USD market before 2017 and after 2018, while the bad volatility spillover played the leading role in other time periods. The bad volatility spillovers played a leading role in the EUR market before 2017, while both good and bad volatility spillovers played the leading roles in the market after then. For the JPY market, both good and bad volatility spillovers played leading roles before 2018 while the bad volatility spillover played the leading role after 2018. The good volatility spillover played the leading role in the KRW market during the whole period of the sample. For the IDR market, before 2017 the bad volatility spillover played the leading role. The good volatility spillover played the leading role during the periods of 2017II-2018I and 2019II-2019III. Both good and bad volatility spillovers played the leading roles the rest of the time. With regard to the PLN market, the bad volatility spillover played the leading role during the periods of 2017IV-2018I and 2019III-2020I, while both the good and bad volatility spillovers played the leading roles in other time periods.

The difference of market system determines the heterogeneity in leading roles of good and bad volatility spillovers among the Bitcoin markets. The policy attitude from the USD market on new assets like cryptocurrencies and the developing trend of Bitcoin in the USD market provide a favorable environment for investors to generate investment strategies. The good information from the USD market enhances the investor expectations. Thus, the leading role of good volatility in the USD market persists during the whole sample period. However, the development of other cryptocurrencies challenged Bitcoin during 2017 to 2018. At this moment, the Bitcoin price volatility induced by bad information had begun to contaminate different Bitcoin markets, resulting in the joint leading roles played by good and bad volatility spillovers in the USD market. Protecting investors in the USD market enhances the market efficiency. The increase of the Bitcoin market efficiency gradually digests price volatility caused by bad information. Therefore, after 2018, the good volatility spillover recovered the leading role in the USD market.

The different perfection levels of the Bitcoin markets determine the heterogeneity in leading roles of good and bad volatility spillovers among different markets. This may result from the effects of major events on the Bitcoin markets. Bitcoin futures were born in December 2017 and were welcomed into the USD and EUR markets. This provided an opportunity for the EUR market. With a similar system to the USD market, EUR attracts many investors into the market, changing the leading role of EUR in volatility spillover. On the other hand, although JPY followed the system from other markets, it cannot perfect the market to adapt to the increase of investors. The JPY market highlighted the legality of Bitcoin by issuing some relevant laws in 2018. However, as the investor heterogeneity, the issued laws cannot well serve the market perfection. Thus, JPY mainly spilled bad volatility after 2018. Due to the instability of the KRW market, it has been the main receiver of both good and bad volatility spillovers. Besides, as the newly developing Bitcoin markets, IDR and PLN, the origins leading to market imperfection and investor complexity are still unclear. The investor expectations fluctuate strongly. Thus, the leading roles of good and bad volatility spillovers in the IDR and PLN markets do not show evident characteristics.

4 TEST ASYMMETRIC DYNAMIC NETWORK CONNECTEDNESS IN BITCOIN MARKETS

Using the results of dynamic spillovers in **Sections 2** and **3**, in this section, we test the asymmetry between systematic (good) volatility and idiosyncratic (bad) volatility. In the first subsection, we construct statistical magnitudes to test the asymmetry. In the second subsection, we test the asymmetry between systematic and idiosyncratic volatility spillovers, while in the third subsection, we test the asymmetry between good and bad volatility spillovers.

4.1 Conducting Test Statistics of Asymmetric Dynamic Network

We now describe how to test asymmetries in volatility spillovers. This procedure is addressed by two steps. In the first step, we propose a hypothesis, while in the second step, we construct statistical magnitudes.

A comparison of the spillover values opens the following possibilities. If the systematic (good) volatility spillovers equal to the idiosyncratic (bad) volatility spillovers, the spillovers are symmetric, and we expect the spillovers to be of the same magnitude as spillovers from *RV*. The test for dynamic net pairwise spillover among the markets also follows this principle. These properties enable us to test the following hypotheses:

$$H_0^1 : S_{net}^1 = S_{net}^2 \; against \; H_A : S_{net}^1 \neq S_{net}^2.$$
$$H_0^2 : S_{netpair}^1 = S_{netpair}^2 \; against \; H_A : S_{netpair}^1 \neq S_{netpair}^2.$$

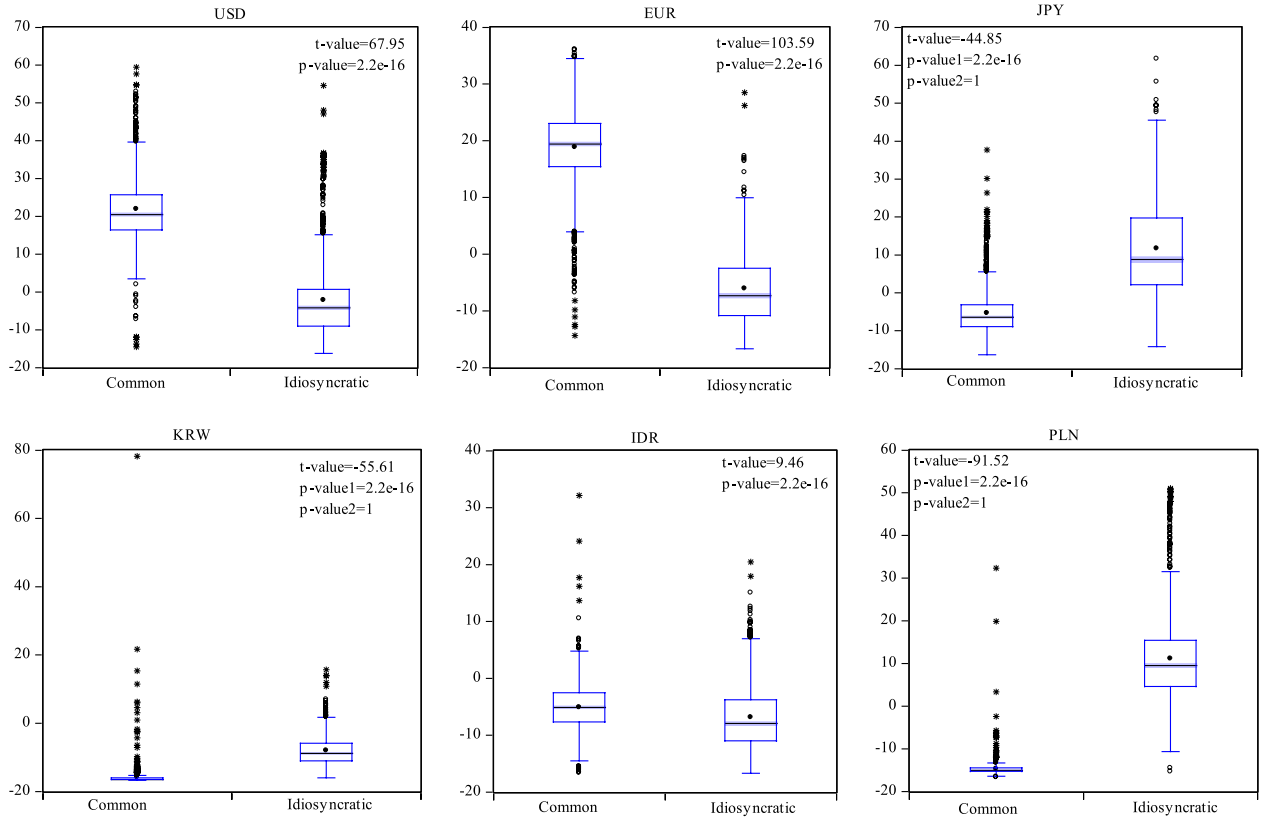


FIGURE 5 | Test results of net spillover between systematic and idiosyncratic volatilities ($p < 0.05$). Note: I: The boxplot show the dynamic net pairwise spillovers of systematic and idiosyncratic volatilities among the Bitcoin markets. II: The t-value is the value of t-statistics. The *p*-value1 is the *p*-value of test (1). The *p*-value2 is the *p*-value of test (2). If both the *p*-value1 and *p*-value2 are smaller than 0.05, then it is replaced by *p*-value. III: Test (1): $TAM_{1i} = 0.$ vs $TAM_{1i} \neq 0.$ Test (2): $TAM_{1i} < 0.$ vs. $TAM_{1i} > 0.$

where S^1_{net} represents the dynamic systematic (good) volatility spillovers, S^2_{net} represents the dynamic idiosyncratic (bad) volatility spillovers. $S^1_{netpair}$ represents the dynamic net pairwise spillovers of systematic (good) volatilities, $S^2_{netpair}$ represents the dynamic net pairwise spillovers of idiosyncratic (bad) volatilities.

If the null hypothesis holds, it suggests that the spillover levels are coincident in the time dimension among different Bitcoin markets. Accordingly, we construct four statistical magnitudes as **Eqs 5–8**:

$$TAM_{1i} = S^S_{neti} - S^I_{neti}. \tag{5}$$

$$TAM_{1ij} = S^S_{NPSij} - S^I_{NPSij},\ i \neq j. \tag{6}$$

$$TAM_{2i} = S^G_{neti} - S^B_{neti} \tag{7}$$

$$TAM_{2ij} = S^G_{NPSij} - S^B_{NPSij},\ i \neq j. \tag{8}$$

where **Eqs 5** and **6** are statistical magnitudes testing the dynamic spillovers and net pairwise spillovers of systematic and idiosyncratic volatilities, while **Eqs 7** and **8** are statistical magnitudes testing the dynamic spillovers and net pairwise spillovers of good and bad volatilities. $i, j = 1, 2, \ldots, 6$ represent the number of Bitcoin markets. Accordingly, S^S_{neti} represents the dynamic spillover of systematic volatility in the market i, while S^I_{neti} represents the dynamic spillover of idiosyncratic volatility in the market i. S^S_{NPSij} represents the net pairwise spillover of systematic volatility between the market i and market j, and S^I_{NPSij} represents the net pairwise spillover of idiosyncratic volatility between the market i and market j. S^G_{neti}, S^B_{neti}, S^G_{NPSij}, and S^B_{NPSij} are similar statistical magnitudes for good and bad volatilities.

According to the hypothesis and statistical magnitudes, the hypotheses in this paper are as follows:

$$\text{Test (1)} : TAM_{1i(j)} = 0. \quad \text{vs} \quad TAM_{1i(j)} \neq 0. \tag{9}$$

$$\text{Test (2)} : TAM_{1i(j)} < 0. \quad \text{vs} \quad TAM_{1i(j)} > 0. \tag{10}$$

$$\text{Test (3)} : TAM_{2i(j)} = 0. \quad \text{vs} \quad TAM_{2i(j)} \neq 0. \tag{11}$$

$$\text{Test (4)} : TAM_{2i(j)} < 0. \quad \text{vs} \quad TAM_{2i(j)} > 0. \tag{12}$$

where (1) and (2) test the asymmetry of dynamic spillovers (net pairwise spillovers) between systema-tic and idiosyncratic volatilities, while (3) and (4) test the asymmetry of dynamic spillovers (net pairwise spillovers) between good and bad volatilities. In addition, $i \neq j$.

In this paper, we first address test (1) and test (3), namely that the comparison of dynamic spillovers or net pairwise spillovers between systematic (good) and idiosyncratic (bad) volatilities. After rejecting the null hypothesis, we further test the spillover levels, namely test 2) and test (4).

Test the Asymmetric Connectedness of Common and Idiosyncratic Volatility

In this section, we report the asymmetry of systematic and idiosyncratic volatility dynamic spillovers among different Bitcoin markets. On the basis of the static spillovers of systematic and idiosyncratic volatilities in **Section 3**, **Figure 5** shows the dynamic spillovers of systematic and idiosyncratic volatilities among the Bitcoin markets. **Table 3** discusses the dynamic net pairwise spillover of systematic and idiosyncratic volatilities among the Bitcoin markets.

The asymmetry between systematic and idiosyncratic volatility spillovers is captured. In **Figure 5**, t-value is the value of t-statistics, *p*-value1 represents the *p*-value of test (1), while *p*-value2 represents the *p*-value of test (2). If the *p*-value1 and *p*-value2 are both smaller than the confidence level 0.05, then it is replaced by the *p*-value. From the *p*-value or *p*-value1, we can find the significant asymmetry between the dynamic spillovers of systematic and idiosyncratic volatilities. Furthermore, we test and compare the dynamic spillover levels of systematic and idiosyncratic volatilities. We can see that in the USD, EUR, and IDR markets, the *p*-value2 is smaller than 0.05, while in the JPY, KRW, and PLN markets, *p*-value2 is larger than 0.05. According to the null hypothesis and alternative hypothesis of test (2), in the USD, EUR, and IDR markets, the dynamic spillovers of systematic volatilities are significantly stronger than that of idiosyncratic volatilities. Inverse results hold in the JPY, KRW, and PLN markets.

On the one hand, the asymmetry between systematic and idiosyncratic volatility spillovers is induced by the heterogeneity of the influencing mechanism. The systematic volatility is influenced by the autologous information and price evolution of Bitcoin, while the idiosyncratic volatility is influenced by the idiosyncratic information in different markets. From the perspective as a financial asset, the effect of systematic information on the Bitcoin price depends on the autologous security, convenience, and particularity. Decentralization is the most significant characteristic in the development of Bitcoin. The blockchain is the primary technique support. This particularity provides convenience for investors to generate investment strategies, which attracts many investors to consider Bitcoin as a financial asset. Meanwhile, due to the rapid development of the internet, Bitcoin thefts happen all the time. Its security is another problem that should be paid attention to. From the perspective of markets, the effect of idiosyncratic information on the Bitcoin price depends on the shocks of major events and policy attitudes. The idiosyncratic policy attitude determines the legality and security of Bitcoin transactions in the market as well as the protection for investors, which can enhance the investment expectation of Bitcoin investors. The development of financial integration results in that one market may receive spillovers of policy attitudes from other markets, which may make differences to the investment expectations of investors. Accordingly, there shows significant asymmetry between systematic and idiosyncratic volatility spillovers among different Bitcoin markets.

On the other hand, the asymmetry between systematic and idiosyncratic volatility spillovers among different Bitcoin markets results from the heterogeneity of roles played by different markets in deciding the price evolution of Bitcoin. The USD and EUR, as the markets with large capitalization, focus more on the advantages brought by the development of Bitcoin, especially the development of blockchain technology. The attitude of IDR, who focuses more on technology, toward Bitcoin determines the impact of the IDR market on the Bitcoin price evolution. Due to China's policy attitude toward Bitcoin, the weight shifts to the JPY and KRW markets, such that more speculators flood into their markets, which results in the weakening of market stability. Meanwhile, that supervision is supplemented sparingly is another reason for the weakening of market stability. Even though one market focuses more on technology, the idiosyncratic characteristics of individual markets still impact the Bitcoin price evolution. These markets reflect the roles of different markets in the Bitcoin price evolution. More precisely, USD, EUR and IDR influence the Bitcoin price by spreading public information, while JPY, KRW, and PLN spread idiosyncratic information.

This shows asymmetry between systematic and idiosyncratic volatility spillovers. Panel a in **Table 3** reports the dynamic net pairwise spillovers among different Bitcoin markets. On the basis of asymmetry in panel a, in this paper, we further test the dynamic

TABLE 3 | Test results of net pairwise spillover between systematic and idiosyncratic volatility.

	USD	EUR	JPY	PLN	IDR
Panel a			**Test (1)**		
EUR	1.53 (0.13)	—	—	—	—
JPY	−61.85 (0.00)	−80.60 (0.00)	—	—	—
PLN	−101.57 (0.00)	−123.84 (0.00)	−13.45 (3.32e-39)	—	—
IDR	−52.46 (0.00)	−72.76 (0.00)	47.08 (0.00)	69.71 (0.00)	—
KRW	−72.56 (0.00)	−95.51 (0.00)	12.56 (5.88e-35)	57.07 (0.00)	−35.69 (6.35e-227)
Panel b			**Test (2)**		
EUR	—	—	—	—	—
JPY	−61.85 (1.00)	−80.60 (1.00)	—	—	—
PLN	−101.57 (1.00)	−123.84 (1.00)	−13.45 (1.00)	—	—
IDR	−52.46 (1.00)	−72.76 (1.00)	47.08 (0.00)	69.71 (0.00)	—
KRW	−72.56 (1.00)	−95.51 (1.00)	12.56 (2.94e−35)	57.07 (0.00)	−35.69 (1.00)

Note: I. This table shows t-value and p*-value. The* p*-value was shown in parentheses. II: Test (1):* $TAM_{1ij} = 0$. *vs* $TAM_{1ij} \neq 0$. *Test (2):* $TAM_{1ij} < 0$. *vs* $TAM_{1ij} > 0$.

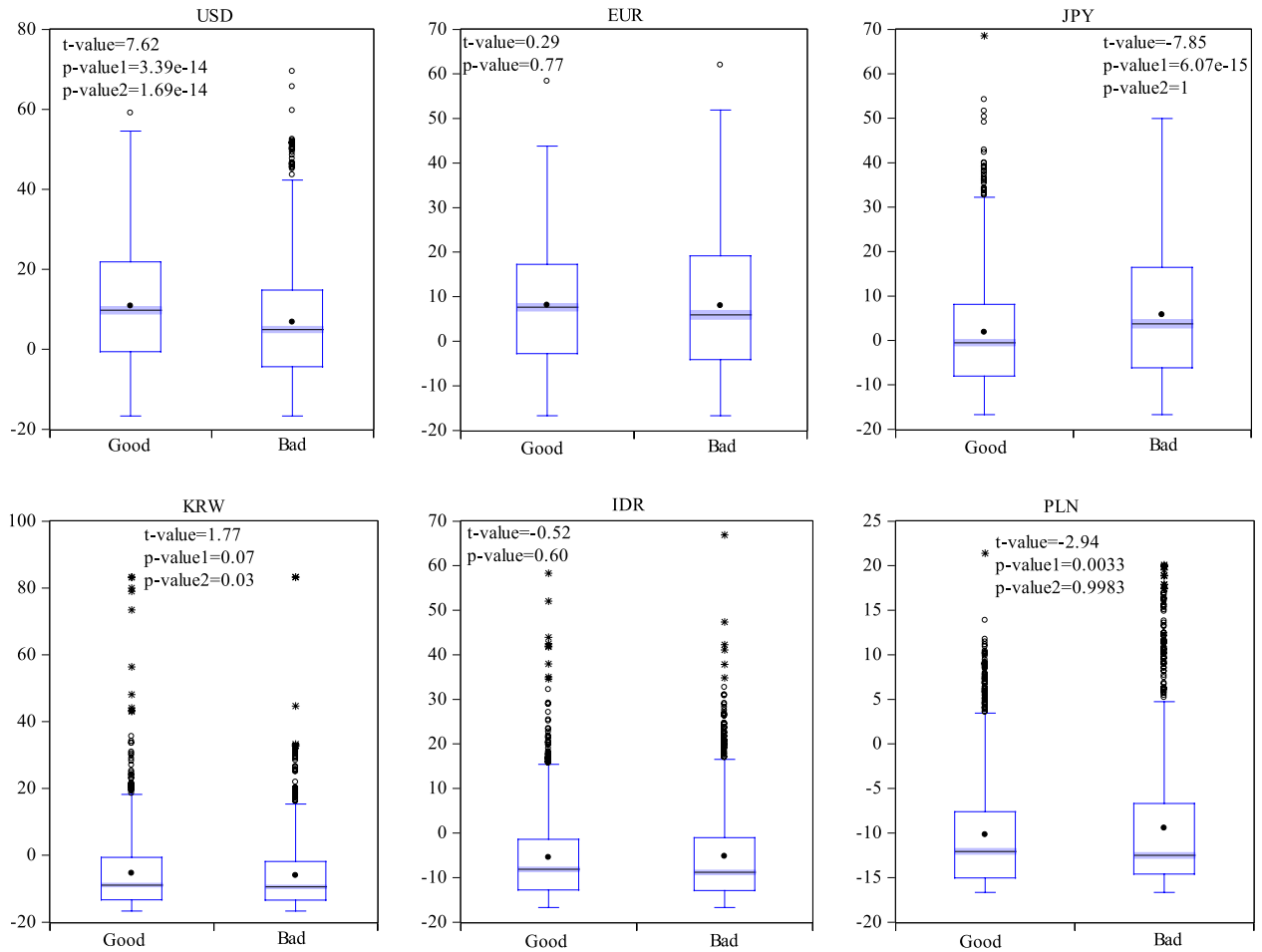


FIGURE 6 | Test results of net spillovers between good and bad volatilities ($p < 0.05$). Note: I. The boxplot show the dynamic net spillovers of good and bad volatilities among different Bitcoin markets. II. The t-value is the value of t-statistics. The p-value1 is the p-value of test (3). The p-value2 is the p-value of test (4). If the p-value1 is larger than 0.05, it is replaced by p-value. III: Test (3): $TAM_{2i} = 0$. vs $TAM_{2i} \neq 0$. Test (4): $TAM_{2i} < 0$. vs.$TAM_{2i} > 0$.

net pairwise spillover levels of systema-tic and idiosyncratic volatilities in different markets, see panel b in **Table 3**. From panel a in **Table 3**, it can be seen that among the fifteen net pairwise spillovers, only the pair USD-EUR accepts the null hypothesis on the inexistence of asymmetry, which reflects the almost asymmetry of dynamic net pairwise spillovers. Further looking at panel b in **Table 3**, among the fourteen asymmetric net pairwise spillovers, ten pairs show that the dynamic spillovers of systematic volatility are weaker than that of idiosyncratic volatility. Accordingly, from the net pairwise spillovers among the markets, the idiosyncratic volatility spillover plays a leading role among the Bitcoin markets.

The effect of idiosyncratic information on the Bitcoin price evolution highlights the leading roles of idiosyncratic volatility spillover among the Bitcoin markets. The development of Bitcoin has driven the development of emerging technology such as blockchain technology. The development of this technology attracts much attention from different countries and regions. However, the security of Bitcoin challenges the design of financial systems and the supervision of financial risk in the countries and regions. The difference between cryptocurrency assets like Bitcoin and traditional assets leads to different policy attitudes of markets on the Bitcoin. The difference of policy attitudes gives rise to barriers for investors and speculators to earn profits. Meanwhile, one market may be infected by policy attitudes from other markets, leading to the fluctuation of investor expectations and change of market stability, resulting in the price volatility of Bitcoin in the market. However, as with the similar market systems of USD and EUR, there does not appear to be any asymmetric net pairwise spillovers between systematic and idiosyncratic volatilities in these two markets.

4.2 Test the Asymmetric Connectedness of Good and Bad Volatility

In this section, we report the asymmetry between good and bad volatility dynamic spillovers among different Bitcoin markets. On the basis of the dynamic net spillovers of good and bad volatilities

in **Section 4**, **Figure 6** shows the dynamic net spillovers of good and bad volatilities among different Bitcoin markets. **Table 4** shows the dynamic net pairwise spillovers of good and bad volatilities among different Bitcoin markets.

The asymmetry of good and bad volatility spillovers is heterogeneous in different markets. In **Figure 6**, the t-value is the value of statistics t. The *p*-value1 is the *p*-value of test (3). The *p*-value2 is the *p*-value of test (4). If the *p*-value1 is larger than 0.05, then it is replaced by *p*-value. From the *p*-value or *p*-value1 in **Figure 6**, we can see the significant heterogeneity of asymmetry between good and bad volatility dynamic spillovers in different markets. More precisely, the *p*-value suggests accepting the null hypothesis on the inexistence of asymmetry in the EUR and IDR markets. The *p*-value2 is less than 0.05 in the USD and KRW markets, while it is more than 0.05 in the JPY and PLN markets. According to the null hypothesis and alternative hypothesis of test (4), we can see that the good volatility dynamic spillovers are significantly stronger than the bad volatility dynamic spillovers in the USD and KRW markets, while the inverse case holds in the JPY and PLN markets.

The market information brought into the public determines the heterogeneity of asymmetric spillovers between good and bad volatilities among different markets. If more market information is brought to the public, the investors can better grasp the Bitcoin price and generate correct investment strategies, which may strengthen the market stability. Thus, the Bitcoin price admits positive returns. On the contrary, if less market information is brought into the markets, the uncertainty of investor expectations may be higher and the market stability is lower, resulting in stronger volatility. At this moment, the Bitcoin price admits negative returns. For the USD and KRW markets, influenced by the necessity to protect investor interests and construct financial market systems, the good volatility spillovers are significantly stronger than the bad volatility spillovers. From the perspective of protecting investor interests, the investor can better grasp the Bitcoin price by the market information brought into the public. Moreover, the market may release advantageous information to prevent the instability of other markets from influencing the price in the autologous markets. At this moment, the investors may show good expectations and generate rational investment strategies. In addition, the insecurity of Bitcoin markets, such as events like hacker attacking and Bitcoin theft, requires the markets to enhance the perfection of autologous market systems. This enhancement shows positive effects on the Bitcoin price. Therefore, the good volatility contributes more to the Bitcoin price than the bad volatility in the USD and KRW markets. The inverse case arises in the JPY and PLN markets. Influenced by the shift of key Bitcoin markets, there is a high proportion of speculators in the JPY and PLN markets. At this moment, the market stability is lower and the investor expectations are unstable. This causes some issues for investors when generating investment strategies. Thus, the bad information produces a negative effect on the Bitcoin price. In the EUR and IDR markets, the good and bad information shows almost equivalent effects on the Bitcoin price volatility. Furthermore, we analyze the spillover effects of price volatility across different Bitcoin markets.

The bad volatility spillovers play leading roles in the Bitcoin markets with large capitalization. Panel a in **Table 4** reports the asymmetry of dynamic net pairwise spillovers among the Bitcoin markets. On the basis of asymmetry existing in the markets in panel a, we further test the levels of dynamic net pairwise spillovers of good and bad volatilities in different markets, see panel b in **Table 4**. From panel a in **Table 4**, among the fifteen pairs of net pairwise spillovers, only the pairs EUR-PLN and EUR-IDR accept the null hypothesis on the inexistence of asymmetry. Therefore, the dynamic net pairwise spillovers among different Bitcoin markets are almost all asymmetric. By looking at panel b in **Table 4**, among the thirteen asymmetric net pairwise spillovers, there are six pairs showing that good volatility spillovers are weaker than bad volatility spillovers, where five of them are relevant to the USD market. Accordingly, the results of net pairwise spillovers suggest the heterogeneity in dynamic spillovers of good and bad volatilities among different Bitcoin markets.

The Bitcoin market system design leads to the heterogeneity in asymmetric spillovers of good and bad volatilities. The efficiency and perfection of the USD market are both higher than other markets. This market superiority can well protect the profits of investors. The investor expectations are also higher. At this moment, the investors and policy makers aim to decrease the market volatility, through releasing advantageous information. Therefore, the good volatility spillover plays a leading role from the USD market to other markets. The difference between virtual assets like Bitcoin and traditional financial assets means that the Bitcoin can be shocked greatly by

TABLE 4 | Test results of net pairwise spillover between good and bad volatilities

	USD	EUR	JPY	PLN	IDR
Panel a			**Test (3)**		
EUR	−3.11 (0.002)	—	—	—	—
JPY	−10.40 (6.89e−25)	−5.16 (2.51e−07)	—	—	—
PLN	−8.12 (6.76e−16)	−0.88 (0.37)	5.81 (7.03e−09)	—	—
IDR	−4.59 (4.43e−06)	−0.31 (0.75)	4.57 (5.02e−06)	2.62 (0.008)	—
KRW	−4.69 (2.80e−06)	1.82 (0.06)	4.28 (1.85e−05)	2.69 (0.007)	3.91 (9.35e−07)
Panel b			**Test (4)**		
EUR	−3.11 (0.99)	—	—	—	—
JPY	−10.40 (1.00)	−5.16 (0.99)	—	—	—
PLN	−8.12 (1.00)	—	5.81 (3.51e−09)	—	—
IDR	−4.59 (0.99)	—	4.57 (2.51e−06)	2.62 (0.004)	—
KRW	−4.69 (0.99)	1.82 (0.034)	4.28 (9.27e−06)	2.69 (0.003)	3.91 (4.67e−05)

Note: This table shows t-value and p*-value. The* p*-value was shown in parentheses. Test (3): $TAM_{2ij} = 0$. vs $TAM_{2ij} \neq 0$. Test (4): $TAM_{2ij} < 0$. vs $TAM_{2ij} > 0$.*

major events, which challenges the design of Bitcoin market systems. At present, most markets are in the stage of exploring Bitcoin. There shows higher uncertainty of investor expectations in the markets. This uncertainty enhances the instability of markets and then the Bitcoin price volatility. Thus, the bad volatility spillovers play leading roles in the connectedness of other Bitcoin markets.

5 CONCLUSIONS AND POLICY IMPLICATIONS

Information transmission is an important link of Bitcoin price volatility spillovers. In this paper, the sample data were from six Bitcoin markets whose capitalizations are within the top ten. The sample period was from March 6, 2016 to March 15, 2020. First, we measured the realized volatilities of Bitcoin in each market with the data frequency of 5 min. Second, we decomposed the realized volatility into systematic and idiosyncratic volatilities (good and bad volatilities), and then analyzed the static and dynamic spillovers. Finally, we tested the asymmetry between systematic and idiosyncratic volatility spillovers (good and bad volatility spillovers) by constructing statistics. The conclusions are summarized as follows:

The spillovers between systematic and idiosyncratic volatilities in different Bitcoin markets play leading roles. In addition, the idiosyncratic volatility spillovers are more easily influenced by policies. The most enhancement on volatility spillover after decomposition of the realized volatility was found in the KRW market, which was given as 14.81/0.3 = 49 and 6.99/0.3 = 20, which was followed by the JPY market, given as 8.65/1.2 = 1 and 14/1.2 = 11. The least enhancement on volatility spillover after decomposition of the realized volatility was found in the IDR market, which was given as 6.28/4.2 = 1.5 and 8.34/4.2 = 2. The spillover directions changed after decomposition in the USD, EUR, JPY, and PLN markets, while they did not change in the IDR and KRW markets. Besides, the systematic volatility spillovers almost did not change their signs during the sample period. The signs of the idiosyncratic volatility spillovers among different markets showed strong relationship to policies.

Good volatility spillovers dominated the Bitcoin markets and changed over time. More precisely, comparing the good and bad volatility spillovers, the spillover levels decreased in the USD, PLN, and KRW markets, while they increased in the EUR, JPY, and IDR markets. Good volatility spillovers played leading roles in the USD market before 2017 and after 2018, while bad volatility spillovers played leading roles in other time periods. Bad volatility spillovers played leading roles in the EUR market before 2017, while both the good and bad volatility spillovers played leading roles after 2017. Both the good and bad volatility spillovers played leading roles in the JPY market before 2018, while the bad volatility spillovers played the leading roles after 2018. Good volatility spillovers played leading roles in the sample period. In the IDR market, bad volatility spillovers played the leading roles before 2017. The good volatility spillovers played leading roles during the periods from 2017II to 2018I and 2019II to 2019III. Both the good and bad volatility spillovers played the leading roles in other time periods. In the PLN market, the bad volatility spillovers played the leading roles during the periods from 2017IV to 2018I and 2019III to 2020I. Both the good and bad volatility spillovers played the leading roles in other time periods.

There was significant asymmetry between systematic and idiosyncratic volatility spillovers among different Bitcoin markets. The asymmetries between good and bad volatility spillovers were heterogeneous in different markets. More precisely, the dynamic spillovers of systematic volatility were significantly stronger than that of idiosyncratic volatility in the USD, EUR, and IDR markets. With regard to good and bad volatility spillovers, there was no asymmetry in the EUR and IDR markets. The dynamic spillovers of good volatility in the USD and KRW markets were significantly stronger than that of bad volatility. The inverse results hold in the JPY and PLN markets.

Indeed, the empirical results in this paper can provide some policy suggestions for regulators and investors. For the regulators, on the one hand, it should strengthen the establishment of market systems and information public degrees. The Bitcoin price volatility results from the difficulties for investors to obtain information, the strong hysteresis, and the imperfection of market systems. We should be familiar with the Bitcoin price evolution and its internal logic by strengthening the establishment of market systems, which is important to take the advantages of Bitcoin and protect the legal interests of investors. On the other hand, it should prevent information shocks from other markets. The regulators should guide the investors to invest rationally. Markets should learn form those markets with higher perfection like USD and EUR to prevent idiosyncratic information from other markets from causing strong volatility of the Bitcoin price. For the investors, the heterogeneity of information volatilities among cryptocurrencies should be paid attention to for the generation of investment strategies. Information and major events have large impacts on the Bitcoin price volatility. The investors should grasp the information of Bitcoin price by various ways and invest rationally. The investors should well filter the information and generate investment strategies. The analysis on the asymmetry of volatility spillovers among different Bitcoin markets provides some help for investors to estimate event shocks.

DATA AVAILABILITY STATEMENT

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

AUTHOR CONTRIBUTIONS

Substantial contributions to the conception or design of the work: SC and HD. The acquisition, analysis, or interpretation of data for the work: SC and HD. Drafting the work or revising it critically for important intellectual content: SC and HD. SC and HD provided approval for the publication of the content.

FUNDING

This research was funded by the National Science Foundation of Guangdong Province, grant number 2020A1515010746.

REFERENCES

1. Acemoglu D, Zilibotti F. Was prometheus unbound by chance? Risk, diversification, and growth. *J Polit Econ* (1997) 105(4):709–51. doi:10.1086/262091
2. Alam MS, Shahzad SJH, Ferrer R. Causal flows between oil and forex markets using high-frequency data: asymmetries from good and bad volatility. *Energy Econ* (2019) 84:104513. doi:10.1016/j.eneco.2019.104513
3. Algieri B, Leccadito A. Assessing contagion risk from energy and non-energy commodity markets. *Energy Econ* (2017) 62:312–22. doi:10.1016/j.eneco.2017.01.006
4. An S, Gao X, An H, Liu S, Sun Q, Jia N. Dynamic volatility spillovers among bulk mineral commodities: a network method. *Resour Pol* (2020) 66:101613. doi:10.1016/j.resourpol.2020.101613
5. Andersen TG, Bollerslev T. Answering the skeptics: yes, standard volatility models do provide accurate forecasts. *Int Econ Rev* (1998) 39(4):885–905. doi:10.2307/2527343
6. Ballester L, Casu B, González-Urteaga A. Bank fragility and contagion: evidence from the bank CDS market. *J Empir Finance* (2016) 38:394–416. doi:10.1016/j.jempfin.2016.01.011
7. Barndoff-Nielsen O, Kinnebrock S, Shephard N. Measuring downside risk-realized semi variance. In: T Bollerslev, J Russell, M Watson, editors. *Volatility and time series econometrics: essays in honor of Robert F. Engle*. Oxford, UK: Oxford University Press (2010) p. 117–36.
8. Bartram SM, Brown G, Stulz RM. Why are U.S. Stocks more volatile? *J Finance* (2012) 67(4):1329–70. doi:10.1111/j.1540-6261.2012.01749.x
9. Baur DG. Financial contagion and the real economy. *J Bank Finance* (2012) 36(10):2680–92. doi:10.1016/j.jbankfin.2011.05.019
10. Baur DG, Hong KH, Lee A. Bitcoin: medium of exchange or speculative assets? *J Int Financ Mark Inst Money* (2017) 54:177–89. doi:10.1016/j.intfin.2017.12.004
11. Baur DG, Dimpfl T, Kuck K. Bitcoin, gold and the US dollar--A replication and extension. *Finance Res Lett* (2017) 25:103–10. doi:10.1016/j.frl.2017.10.012
12. Barigozzi M, Hallin M. Generalized dynamic factor models and volatilities: recovering the market volatility shocks. *Econom J* (2016) 19(1):33–60. doi:10.1111/ectj.12047
13. Baruník J, Kočenda E, Vácha L. Asymmetric connectedness on the U.S. stock market: bad and good volatility spillovers. *J Financ Mark* (2016) 27:55–78. doi:10.1016/j.finmar.2015.09.003
14. Baruník J, Kočenda E, Vácha L. Asymmetric volatility connectedness on the forex market. *J Int Money Finance* (2017) 77:39–56. doi:10.1016/j.jimonfin.2017.06.003
15. Barunik J, Kocenda E. Total, asymmetric and frequency connectedness between oil and forex markets. *Energy J* (2019) 40(01):3233. doi:10.5547/01956574.40.si2.jbar
16. BenSaïda A, Litimi H, Abdallah O. Volatility spillover shifts in global financial markets. *Econ Modell* (2018) 73:343–53. doi:10.1016/j.econmod.2018.04.011
17. Blau BM. Price dynamics and speculative trading in bitcoin. *Res Int Bus Finance* (2017) 41:493–9. doi:10.1016/j.ribaf.2017.05.010
18. Broadstock DC, Fan Y, Ji Q, Zhang D. Shocks and stocks: a bottom-up assessment of the relationship between oil prices, gasoline prices and the returns of Chinese firms. *Energy J* (2016) 37(01):2703. doi:10.5547/01956574.37.si1.dbro
19. Chow HK. Volatility spillovers and linkages in Asian stock markets. *Emerg Mark Finance Trade* (2017) 53(12):2770–81. doi:10.1080/1540496x.2017.1314960
20. Corbet S, Lucey BM, Yarovaya L. Datestamping the bitcoin and ethereum bubbles. *Finance Res Lett* (2017) 26:81–8. doi:10.1016/j.frl.2017.12.006
21. Nicola Fd., De Pace P, Hernandez MA. Co-movement of major energy, agricultural, and food commodity price returns: a time-series assessment. *Energy Econ* (2016) 57:28–41. doi:10.1016/j.eneco.2016.04.012
22. Diebold FX, Yilmaz K. Better to give than to receive: predictive directional measurement of volatility spillovers. *Int J Forecast* (2012) 28(1):57–66. doi:10.1016/j.ijforecast.2011.02.006
23. Diebold FX, Yilmaz K. On the network topology of variance decompositions: measuring the connectedness of financial firms. *J Econom* (2011) 182(1):119–34. doi:10.2139/ssrn.1937613
24. Dong H, Chen L, Zhang X, Failler P, Xu S. The asymmetric effect of volatility spillover in global virtual financial asset markets: the case of Bitcoin. *Emerg Mark Finance Trade* (2020) 56(6):1293–311. doi:10.1080/1540496x.2019.1671819
25. Dungey M, Fry R, Martin VL. Equity transmission mechanisms from Asia to Australia: interdependence or contagion? *Aust J Manag* (2003) 28(2):157–82. doi:10.1177/031289620302800203
26. Dungey M, Martin VL. Unravelling financial market linkages during crises. *J Appl Econ* (2007) 22(1):89–119. doi:10.1002/jae.936
27. Dungey M, Gajurel D. Contagion and banking crisis - international evidence for 2007-2009. *J Bank Finance* (2015) 60(11):271–83. doi:10.1016/j.jbankfin.2015.08.007
28. Dyhrberg AH. Hedging capabilities of bitcoin. Is it the virtual gold? *Finance Res Lett* (2016) 16(16):139–44. doi:10.1016/j.frl.2015.10.025
29. Feunou B, Jahan-Parvar MR, Tédongap R. Modeling market downside volatility*. *Rev Finance* (2013) 17(1):443–81. doi:10.1093/rof/rfr024
30. Forni M, Lippi M. The generalized dynamic factor model: representation theory. *Econom Theory* (2001) 17(6):1113–41. doi:10.1017/s0266466601176048
31. Fry J, Cheah E-T. Negative bubbles and shocks in cryptocurrency markets. *Int Rev Financ Anal* (2016) 47(47):343–52. doi:10.1016/j.irfa.2016.02.008
32. Goyal A, Santa-Clara P. Idiosyncratic risk matters! *J Finance* (2003) 58(3):975–1007. doi:10.1111/1540-6261.00555
33. Gyamerah SA. Modelling the volatility of Bitcoin returns using GARCH models. *Quant Finance Econ* (2019) 3(4):739–53. doi:10.3934/QFE.2019.4.739
34. He Z, He L, Wen F. Risk compensation and market returns: the role of investor sentiment in the stock market. *Emerg Mark Finance Trade* (2019) 55(3):704–18. doi:10.1080/1540496x.2018.1460724
35. Kumar S, Tiwari AK, Chauhan Y, Ji Q. Dependence structure between the BRICS foreign exchange and stock markets using the dependence-switching copula approach. *Int Rev Financ Anal* (2019) 63:273–84. doi:10.1016/j.irfa.2018.12.011
36. Kapar B, Olmo J. An analysis of price discovery between Bitcoin futures and spot markets. *Econ Lett* (2019) 174:62–4. doi:10.1016/j.econlet.2018.10.031
37. Li Z, Dong H, Dong H, Huang Z, Failler P Asymmetric effects on risks of virtual financial assets (VFAs) in different regimes: a case of bitcoin. *Quantitative Finance and Economics* (2018) 2(4):860–83. doi:10.3934/qfe.2018.4.860
38. Li J, Yao Y, Li J, Zhu X. Network-based estimation of systematic and idiosyncratic contagion: the case of Chinese financial institutions. *Emerg Mark Rev* (2019) 40:100624. doi:10.1016/j.ememar.2019.100624
39. Li Z, Zhong J. Impact of economic policy uncertainty shocks on China's financial conditions. *Finance Res Lett* (2020) 35:101303. doi:10.1016/j.frl.2019.101303
40. Luo J, Ji Q. High-frequency volatility connectedness between the US crude oil market and China's agricultural commodity markets. *Energy Econ* (2018) 76:424–38. doi:10.1016/j.eneco.2018.10.031
41. Ji Q, Bouri E, Roubaud D, Shahzad SJH. Risk spillover between energy and agricultural commodity markets: a dependence-switching CoVaR-copula model. *Energy Econ* (2018) 75:14–27. doi:10.1016/j.eneco.2018.08.015
42. Ji Q, Bouri E, Roubaud D. Dynamic network of implied volatility transmission among US equities, strategic commodities, and BRICS equities. *Int Rev Financ Anal* (2018) 57:1–12. doi:10.1016/j.irfa.2018.02.001
43. Ji Q, Zhang D. How much does financial development contribute to renewable energy growth and upgrading of energy structure in China? *Energy Pol* (2019) 128:114–24. doi:10.1016/j.enpol.2018.12.047
44. Ji Q, Liu B-Y, Fan Y. Risk dependence of CoVaR and structural change between oil prices and exchange rates: a time-varying copula model. *Energy Econ* (2019) 77:80–92. doi:10.1016/j.eneco.2018.07.012
45. Ma Y-R, Zhang D, Ji Q, Pan J. Spillovers between oil and stock returns in the US energy sector: does idiosyncratic information matter? *Energy Econ* (2019) 81:536–44. doi:10.1016/j.eneco.2019.05.003
46. Nan Z, Kaizoji T, Kaizoji T Bitcoin-based triangular arbitrage with the Euro/U.S. dollar as a foreign futures hedge: modeling with a bivariate GARCH model. *Quant Finance Econ* (2019) 3(2):347–65. doi:10.3934/qfe.2019.2.347
47. Narayan PK, Sharma SS. New evidence on oil price and firm returns. *J Bank Finance* (2011) 35(12):3253–62. doi:10.1016/j.jbankfin.2011.05.010

48. Nishimura Y, Sun B. The intraday volatility spillover index approach and an application in the Brexit vote. *J Int Financ Mark Inst Money* (2018) 55:241–53. doi:10.1016/j.intfin.2018.01.004
49. Patton AJ, Sheppard K. Good volatility, bad volatility: signed jumps and the persistence of volatility. *Rev Econ Stat* (2015) 97(3):683–97. doi:10.1162/rest_a_00503
50. Peng C, Zhu H, Guo Y, Chen X. Risk spillover of international crude oil to China's firms: evidence from granger causality across quantile. *Energy Econ* (2018) 72:188–99. doi:10.1016/j.eneco.2018.04.007
51. Pesaran MH, Shin Y. An autoregressive distributed-lag modelling approach to cointegration analysis. *Econ Soc Monogr* (1998) 31:371–413. doi:10.1017/CCOL0521633230.011
52. Pieters G, Vivanco S. Financial regulations and price inconsistencies across bitcoin markets. *Inf Econ Pol* (2017) 39:1–14. doi:10.1016/j.infoecopol.2017.02.002
53. Prasad N, Grant A, Kim S-J. Time varying volatility indices and their determinants: evidence from developed and emerging stock markets. *Int Rev Financ Anal* (2018) 60:115–26. doi:10.1016/j.irfa.2018.09.006
54. Segal G, Shaliastovich I, Yaron A. Good and bad uncertainty: macroeconomic and financial market implications. *J Financ Econ* (2015) 117(2):369–97. doi:10.1016/j.jfineco.2015.05.004
55. Wang X, Wu C. Asymmetric volatility spillovers between crude oil and international financial markets. *Energy Econ* (2018) 74:592–604. doi:10.1016/j.eneco.2018.06.022
56. Wang Y, Pan Z, Liu L, Wu C. Oil price increases and the predictability of equity premium. *J Bank Finance* (2019) 102(5):43–58. doi:10.1016/j.jbankfin.2019.03.009
57. Wen F, Zhao Y, Zhang M, Hu C. Forecasting realized volatility of crude oil futures with equity market uncertainty. *Appl Econ* (2019) 51(59):6411–27. doi:10.1080/00036846.2019.1619023
58. Yarovaya L, Brzeszczyński J, Lau CKM. Asymmetry in spillover effects: evidence for international stock index futures markets. *Int Rev Financ Anal* (2017) 53:94–111. doi:10.1016/j.irfa.2017.07.007
59. Zhang D, Broadstock DC. Global financial crisis and rising connectedness in the international commodity markets. *Int Rev Financ Anal* (2020) 68:101239. doi:10.1016/j.irfa.2018.08.003
60. Zhang D, Ji Q, Kutan AM. Dynamic transmission mechanisms in global crude oil prices: estimation and implications. *Energy* (2019) 175:1181–93. doi:10.1016/j.energy.2019.03.162
61. Zhang W, Wang P, Li X, Shen D. Multifractal detrended cross-correlation analysis of the return-volume relationship of bitcoin market. *Complexity* (2018) 2018:8691420. doi:10.1155/2018/8691420

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 03 March 2021
doi: 10.3389/fphy.2021.631665

CryptoKitties Transaction Network Analysis: The Rise and Fall of the First Blockchain Game Mania

Xin-Jian Jiang[1] *and Xiao Fan Liu*[2]*

[1]School of Computer Science and Engineering, Southeast University, Nanjing, China, [2]Web Mining Laboratory, Department of Media and Communication, City University of Hong Kong, Hong Kong, China

CryptoKitties was the first widely recognized blockchain game. Players could own, breed, and trade kitties, which are the only prop in the game. The game gained explosive growth upon its release but quickly collapsed in a short time. This study analyzes its entire player activity history for the first time in literature and tries to find the reasons for the rise and fall of this first blockchain game mania. First, we extracted the five million transaction records among 100 thousand addresses involved in CryptoKitties in the past three years. Based on the numbers of addresses involved in the game each day, we divide the game progress into four stages: the primer, the rise, the fall, and the serenity. We construct a temporal kitty ownership transfer network and analyze the varying network parameters in the four stages. We find that a large number of players poured in during the 10th and 18th days since the game release and quickly exited in the following month. Since then, a few big players have gradually dominated the game, concentrating the game resources. Through further analysis, we find that the main reason for the rapid increase in the game popularity was the increase of public attention by media outlets, while the reasons for the rapid decline in the game popularity include the oversupply of kitties, the decreasing of player income, a widening gap between the rich and poor players, and the limitations of blockchain systems. Based on these observations, we advise on the further blockchain game design: (1) to finely control the production of props and avoid an oversupply, (2) to balance the gaming cost and revenue and protect the enjoyment of players, (3) to narrow down the gap between rich and poor and create an equal gaming community, (4) to consider the limitations of blockchain systems in their game designs.

Keywords: cryptokitties, blockchain game, ethereum, transaction network, game design

OPEN ACCESS

Edited by:
Hui-Jia Li,
Beijing University of Posts and Telecommunications (BUPT), China

Reviewed by:
Xiapu Luo,
Hong Kong Polytechnic University, Hong Kong
Jiajing Wu,
Sun Yat-Sen University, China

***Correspondence:**
Xiao Fan Liu
xf.liu@cityu.edu.hk

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *20 November 2020*
Accepted: *21 January 2021*
Published: *03 March 2021*

Citation:
Jiang X-J and Liu XF (2021) CryptoKitties Transaction Network Analysis: The Rise and Fall of the First Blockchain Game Mania. Front. Phys. 9:631665. doi: 10.3389/fphy.2021.631665

1 INTRODUCTION

Blockchain, emerged as the underlying supporting technology for Bitcoin [1], is a distributed ledger system providing non-tampering and traceability functionalities. Ethereum [2], also known as the blockchain 2.0 platform, further adds supports for smart contracts, which are programs that can be stored and executed on the blockchain system [3]. Developers can use smart contracts to create various decentralized applications, especially games.

Blockchain games are considered to have unique advantages over traditional online games in that their gaming data and logic are transparently stored and executed on blockchains [4]. These advantages particularly suit games with in-game payment and chance mechanisms, e.g., gambling,

which often suffered from trust issues in traditional online environment. As a result, current designs of blockchain games mainly revolve around the generation, ownership, and trading of virtual assets [5].

Cryptokitties is a blockchain game released on Ethereum in late November 2017. Players can own, trade, and create virtual kitties, represented by non-fungible tokens meeting the ERC-721 token standard in the game. The attributes and transactions of kitties are recorded in the Ethereum blockchain. Once released, CryptoKitties soon gained massive popularity that its transactions accounted for more than 10% of the entire Ethereum traffic in early December 2017 [6].

Nonetheless, Min et al. [4] claimed that most of the current blockchain games lack playability. Possible reasons include that current blockchain platforms restrict developers from implementing complex game functions, current developers are paying insufficient attention to the players' gaming experience, and lack a competitive market in the blockchain game industry. Not surprisingly, the popularity of CryptoKitties only lasted for a short period, too.

In this study, we aim to fully unveil the collective user behaviors in the game and the reasons leading to the game's rapid rise and fall by analyzing blockchain transaction records. Specifically, we first construct a kitty ownership transfer network and investigate the network structural changes over time. Then, we conjecture and verify the possible reasons for the rapid changes in gaming popularity from four perspectives: the supply and demand of kitties, the profitability in the game, the inequality of players' wealth, and the limitations of blockchain systems. Based on our observations, we pinpoint the deficiencies in the design of CryptoKitties and provide suggestions for further development of blockchain games.

Network analysis methods have been applied to cryptocurrency transaction records in many previous works. Chen et al. [7] constructed three graphs with ether transfer, contract creation, and contract invocation, found a power-law degree distribution, and revealed anomalies in these graphs. Somin et al. [8] also found a power-law degree distribution in the ERC20 token transfer network. Guo et al. [9] further revealed a bow-tie structure in the Ethereum transaction network. Except for the Ethereum blockchain, similar methods have also been used to analyze transactions on other blockchains, such as EOSIO [10].

The rest of this paper is organized as follows. CryptoKitties' gaming rules are introduced in **Section 2**. In **Section 3**, we construct the kitty ownership transfer network and define network structural properties. In **Section 4**, we divide the progress of the game into four stages and examine the changes of network parameters in different stages. We will discuss the reasons for the rapid change in the popularity of CryptoKitties in **Section 5**. **Section 6** concludes the study and provides suggestions for the further development of blockchain games.

2 GAMING RULES

As shown in **Table 1**, the CryptoKitties game has five smart contracts: the Core contract, GeneScience contract, Offers contract, SalesAuction contract, and SiringAuction contract. The names of these contracts could be found on Etherscan [11]. Based on these contracts, players can trade or transfer kitties with other players and breed new kitties.

TABLE 1 | CryptoKitties's smart contracts.

Contract name	Main functions
Core	Record all kitties' attributes and owner information
SalesAuction	As an intermediary to help player trade kitties
Offers	As an intermediary to help player trade kitties
SiringAuction	As an intermediary to help player rent kitties
GeneScience	Calculate the genes of newborn kitties

There are three ways to trade or transfer a kitty. (1) Using the SalesAuction contract. The seller lists a kitty for sale with an initial price, a final price, and a price change period to the SalesAuction contract. The initial price is usually higher than the final price. After the auction begins, the kitty price will change linearly from the initial price to the final price at a constant rate during the price change period. The price will not change after this period. Unless bid by a buyer or canceled by the seller, the kitty will remain in the SalesAuction contract. Upon receiving a bid, the SalesAuction contract will send the kitty to the buyer and transfer the payment to the seller. The game publisher also sells 0-generation kitties to players in this way. (2) Using the Core contract. A player can either call the transfer function to transfer his kitty to another player or the approve function to allow other players to transfer his kitty. Authorized players can call transfer from function to transfer other players' kitties. Transferring a kitty in this way does not necessarily mean that the player is trading the kitty but can also be sending a kitty as a gift to a friend. (3) Using the Offers contract. In this way, the buyer initiates a request to the seller and sends the purchase fee to the Offers contract. If the seller accepts the request, the Offers contract will transfer the kitty to the buyer's address and send the purchase fee to the seller.

When trading kitties through the SalesAuction, the game publisher charges the sellers for 3.75% of the dealing price as a handling fee. Same rate of dealing price will be charged to the buyers using the Offers contracts. When calling any function in each contract, the players also need to pay gas fees to Ethereum miners through their Ethereum wallet. The gas fee is usually between 0.0001eth and 0.01eth.

There are two ways to breed a new kitty. (1) A player selects two of his own kitties as parameters and call the breed With Auto function in the Core contract with a breeding fee. After this operation, the mother kitties (can be arbitrarily chosen between the two) will become pregnant for a period. After this period, a player, also called the midwife, will call the give birth function in the Core contract to give birth to the new kitty. The newborn kitty will be transferred to the owner of the mother kitty. The breeding fee will be compensated to the midwife for their Ethereum gas fees paid. (2) A player breeds with one of his own kitties and another rented from the Siring Auction contract, which lists a number of kitties owned by the lenders. A midwife is also needed in this case.

When a kitty is rented out through the Siring Auction contract, the game publisher will charge the lender 3.75% of the rent as a handling fee.

The breeding fee varied over time (see **Figure 1**). It was set to 0.002eth at the game's release. However, due to the congestion of the Ethereum network resulting from the gaming transactions, the gas fee was raised. The game publisher increased the breeding fee to 0.015eth and later adjusted it to 0.008eth. Such adjustment happened several times afterward, but despite that, the breeding fee has been stable at 0.008eth.

3 DATA AND METHODS

3.1 Blockchain Transactions

We synchronized an Ethereum parity client in full mode and used the eth_getLogs method to extract the transactions in CryptoKitties. The transactions span from November 23, 2017, to May 19, 2020. The data involved 1,923,901 kitties, 104,517 addresses, and 5,173,521 transfer records. There are nine types of transactions (see **Table 2**) related to the movements of kitties, including the trading, transferring, and the new birth of kitties. Consider participation rate as the ratio of the number of addresses that take part in a specific activity to the number of all addresses in CryptoKitties, buying kitties through the SalesAuction contract has the highest participation rate (84.6%), indicating that most players would buy at least one kitty from the official marketplace. Participation rates are also high for breeding kitty (64.9%) and selling kitty through the SalesAuction contract (51.8%). Players showed low interest in lending (38.1%) and renting kitties (26.6%). Only a very small number of players (less than 1%) traded kitties through the Offers contract.

TABLE 2 | Nine types of transactions related to the movements of kitties.

Transaction type	From	To	Amount
Kitty birth	0x	Owner	1,923,901
Listing on the SalesAuction contract	Seller	SalesAuction	1,126,964
Cancel listing on the SalesAuction contract	SalesAuction	Seller	241,614
Buying from the SalesAuction contract	SalesAuction	Buyer	668,981
Transferring through the core contract	Sender	Reviver	633,208
Trading through the offers contract	Seller	Buyer	2,336
Listing on the SiringAuction contract	Lender	SiringAuction	326,553
Cancel listing on the SiringAuction contract	SiringAuction	Lender	92,507
Rental finished	SiringAuction	Lender	157,457

3.2 Constructing Ownership Transfer Network of Kitties

The actual ownership of the kitties only changes when (1) the sales auction on the SalesAuction contract is fulfilled, (2) the trading through the Offers contract is fulfilled, and (3) kitties are transferred directly using functions in the Core contract. Therefore, We construct the kitty ownership transfer network $G = (V, E)$, where V is the set of addresses belong to kitty owners, including the game publisher and players, who have the actual ownership of kitties, and E is the set of directed edges representing the actual ownership changes. The directed edges $e = (u, v, t)$ are temporal, where u represents the address of kitty's previous owner, v represents the address of kitty's new owner, and t represents the time when the ownership change occurred. The network contains 104,514 nodes and 1,304,525 edges. We further use three days as the window size and construct a series of temporal networks $G = (G_1, G_2, \ldots)$, where G_t is the network in time window t.

3.3 Network Structural Properties

We use the average degree, non-zero in-/out-degree ratio, Gini coefficient of in-, out-, and total degrees, average clustering coefficient, density, reciprocity, and assortativity to describe the structural properties of the network.

The average degree $\overline{k} = 2M/N$ represents the average number of kitties transferred in and out of the addresses, where M is the number of edges and N is the number of nodes in the temporal network.

The non-zero in-/out-degree ratio $\alpha = N_{\text{out}>0}/N_{\text{in}>0}$ is defined as the ratio of the number of nodes with an out-degree greater than zero ($N_{\text{out}>0}$) to those with an in-degree greater than zero

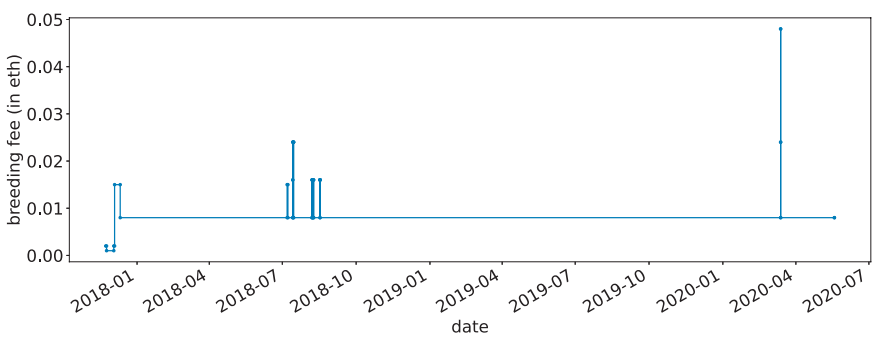


FIGURE 1 | Changes of the breeding fee.

($N_{\text{in}>0}$) in the temporal network. It can also be considered as the ratio of the number of sellers to buyers in the game.

The Gini coefficient G_k of the total degree k of all nodes in the temporal network reflects the gap between the players' activeness in the number of kitties transferred in and out of the address, i.e.,

$$G_k = \frac{1}{N}\left(N + 1 - \frac{2\sum_{i=1}^{N}(N+1-i)k_i}{\sum_{i=1}^{N}k_i}\right),$$

where k_i is the degree of node i indexed in non-decreasing order ($k_i \le k_{i+1}$) and N is the number of nodes in the network. The Gini coefficients for the in-degrees $G_{k\text{in}}$ and out-degrees $G_{k\text{out}}$ of all nodes can be defined likewise.

The average clustering coefficient c is used to measure the clustering degree of the network, which is defined as

$$c = \frac{1}{N}\sum_{v \in V}\frac{T_v}{k_v(k_v-1) - 2k_v^r},$$

where T_v is the number of directed triangles passing through the node v, k_v is the degree of node v, and k_v^r is the number of bidirectional edges of node v. Multiple edges between u and v are considered as one even with the same t in this case. High average clustering coefficient means that players interact closely with other players.

Network density $d = M/(N(N-1))$ describes the portion of the potential connections in the network that are actual connections. Again, multiple edges between u and v are considered as one even with the same t in this case.

The reciprocity $\rho = 2M_u/M$ describes the ratio of the number of edges pointing in both directions to the total number of edges in the network, where M_u is the number of undirected edges in the network. High reciprocity means that the relationship between addresses is relatively strong, and the owners of these addresses are likely to know each other. Multiple edges between u and v are considered as one even with the same t in this case.

The degree assortativity coefficient r measures the similarity of connections in the network with respect to the node degree:

$$r = \frac{\sum_{ij}\left(A_{ij} - k_ik_j/2M\right)k_ik_j}{\sum_{ij}\left(k_i\delta_{ij} - k_ik_j/2M\right)k_ik_j},$$

where A_{ij} is an element in the adjacency matrix, k_i and k_j are the degrees of node i and j, and δ_{ij} is the Kronecker function. The direction of edge is ignored and multiple edges are considered in the calculation.

4 COLLECTIVE BEHAVIORS OF CRYPTOKITTIES PLAYERS

4.1 The Four Stages of Game Progress

Using the numbers of daily addresses related to CryptoKitties transactions, the game can be divided into four stages: the primer, the rise, the fall, and the serenity, as shown in **Figure 2**.

1. The primer: The game was released on November 23, 2017. There were not many players before December 2, 2017.
2. The rise: A large number of players entered the game since December 2, 2017. The game popularity rapidly increased before reaching a peak on December 10.
3. The fall: Since then, the popularity has dropped sharply. At the beginning of 2018, the game's popularity is less than 10% of its peak.
4. The serenity: After January 15, 2018, the popularity stabilized into a long-term slow downward trend. **Figure 3** shows four snapshots of the network in each of the stages. The network size shrinks apparently over time.

4.2 Evolution of the Network Structure

The evolution of network structural properties in the four stages are shown in **Figure 4**. In the first stage, the Gini coefficient of out-degrees decreased suddenly. This is because almost all 0-generation kitties were transferred from the game publisher's addresses to the players in the first few days. Soon after that, players began to breed new kitties and sell them to each other. The decreases in average degree, network density, and average clustering coefficient result from early players entering the game and expanding the network. Meanwhile, the assortativity coefficient stayed negative because low-degree players tended to trade with high-degree players, who are the game publisher.

In the second stage, the network density stayed low due to the large number of players entering the game. The degree

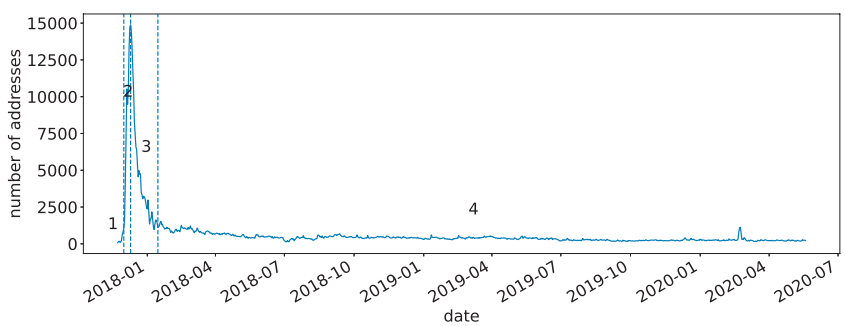


FIGURE 2 | Four stages of the game. The three dotted lines correspond to December 1, 2017, December 10, 2017, and January 15, 2018, respectively.

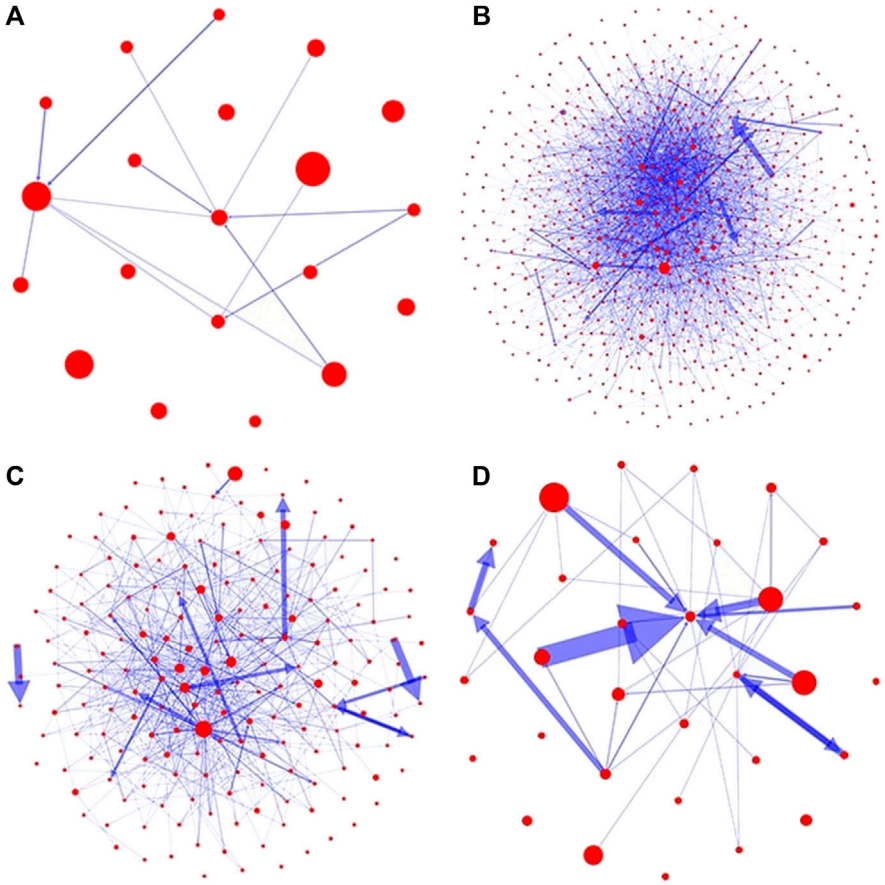


FIGURE 3 | Visualizations of typical networks in every stage. Nodes in the network are filtered by out-degree. **(A)** There aren't many early players in stage 1. **(B)** The network contains a large number of nodes in stage 2. **(C)** The network shrinks in stage 3. **(D)** Only long-term players are left in stage 4.

assortativity coefficient increased to zero, meaning that low-activity players tended to transfer kitties among themselves rather than trading with high-activity players.

In the third stage, the non-zero in-/out-degree ratio maintained an upward trend, indicating that the ratio of sellers to buyers was increasing, and market competition was intensifying. The Gini coefficient of out-degrees decreased gently, indicating that even the seller/buyer ratio increased, the gap between sales volume among sellers was narrowing. However, in-degrees' Gini coefficient went up suddenly. The anomalous data point around December 23, 2017, was caused by an exceptionally large number of transactions made by a handful of addresses.

In the fourth stage, the increasing average degree and reciprocity indicate that the players left in the games were actively trading with each other. The Gini coefficients all maintained an upward trend, indicating a large gap forming in these players: some big players were gradually dominating the game.

Note that the average degree, Gini coefficients, and reciprocity suddenly increased in June 2019. We found that they were caused by the launch of Wrapped Cryptokitties (WCK), which is an ERC-20 token contract, enabling players to exchange unwanted ERC-721 kitties for WCK and use WCK to exchange other kitties. The replacement of a large number of ERC-721 kitties with WCK resulted in a sudden fluctuation in the network structure.

4.3 Changes in the Kitty Ownership Transferring Methods

There are three ways to transfer the ownership of kitties: through the SalesAuction, Offers, or Core contracts. The changes in the proportions of the three methods over time are shown in **Figure 5**. In the early days of the game, the ownership transfer of kitties was mainly realized through the SalesAuction contract. Later, the proportion of transferring kitties with the method in Core contract gradually increased. After April 2019, this method had become the main way of transferring kitty ownerships. The number of kitties transferred through the Offers contract was always small.

Cost was the main reason for this change. Players tend to transfer kitties at a lower cost. When buying and selling kitties through the SalesAuction and Offers contracts, players need to pay a transaction fee to the game publisher, usually 3.75% of the transaction amount. Using the transfer method in the Core contract, in contrast, only requires a gas fee payment.

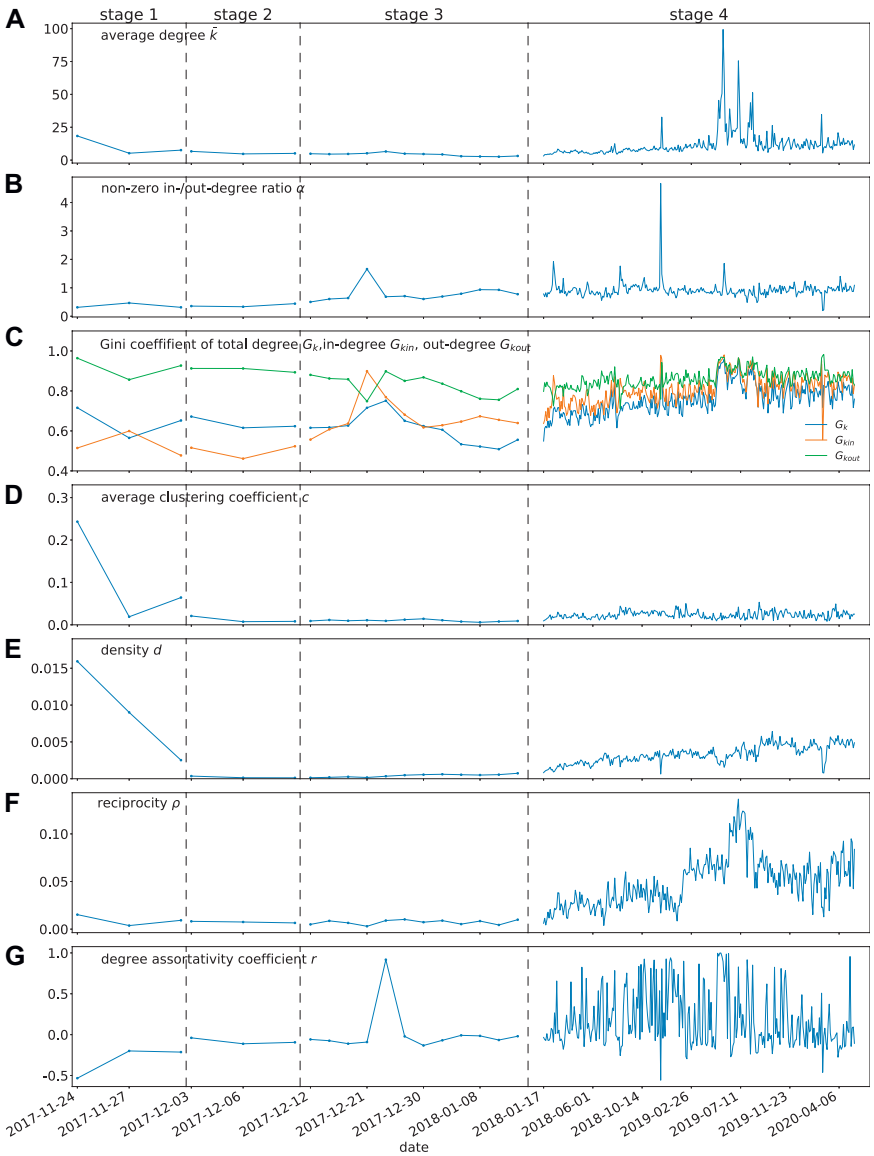


FIGURE 4 | Evolution of the network structural properties over time. **(A)** The average degree, **(B)** the non-zero in-/out-degree ratio, **(C)** the Gini coefficients of in-, out-, and total degrees, **(D)** the average clustering coefficient, **(E)** network density, **(F)** reciprocity, and **(G)** assortativity. Dotted lines separates the four stages. The labels on the *x*-axis represent the middle date of time windows. The *x*-axis are re-scaled to better illustrate the parameter dynamics in stages 1, 2 and 3.

Therefore, some third-party trading platforms emerged to help players trade kitties, charging fewer transaction fees. For example, the transaction fee charged by the OpenSea trading platform is only 2.5%.

5 REASONS FOR THE RISE AND FALL OF CRYPTOKITTIES

5.1 Reasons for the Explosive Growth of Game Popularity

On December 2, 2017, the kitty with ID 1 was sold for 247eth, i.e., more than US $100,000 [12]. This message spread quickly on the Internet, generating a large amount of attentions. **Figure 6** shows the Google trend index of CryptoKitties and number of daily addresses related to CryptoKitties transactions. Kitties traded at extremely high prices will undoubtedly attract media attention and bring many new players to the game. The increased attention from Internet users eventually led to the explosive growth of the game's popularity. We cannot rule out the possibility that the game publisher deliberately made the news that a special kitty has being sold at an extremely high price. In fact, almost all transactions with an amount greater than 100eth occurred in early December 2017, which corresponds precisely to the rise stage of the game. Nonetheless, despite of the cause, media exposure had indeed increased the game popularity significantly.

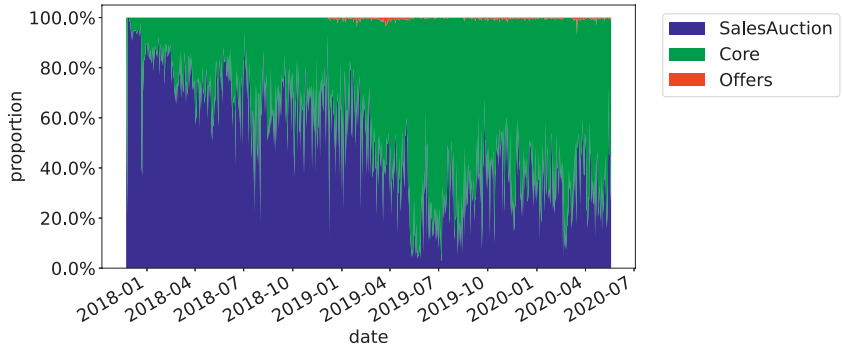


FIGURE 5 | The change in proportion of three methods to transfer the kitties.

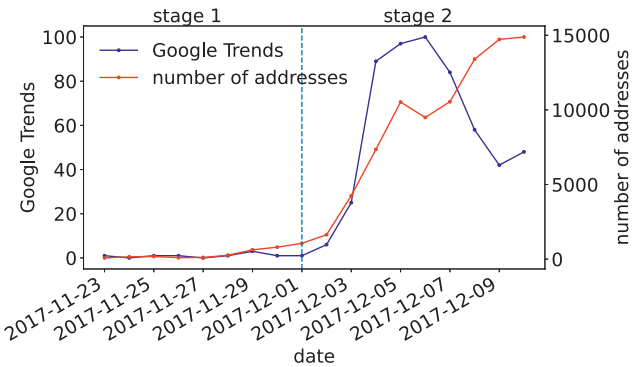


FIGURE 6 | Google Trends of CryptoKitties and the numbers of daily active addresses.

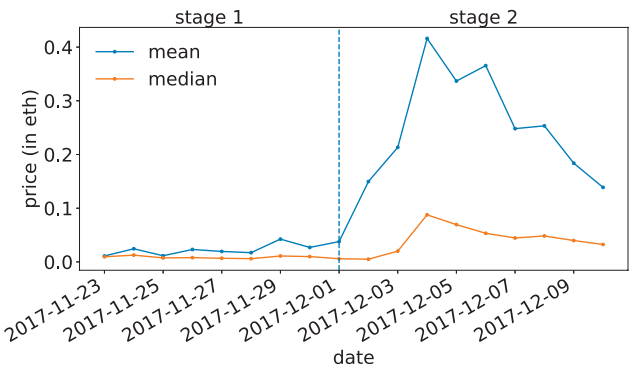


FIGURE 7 | Mean and median prices of the kitties sold in each day.

Cryptocurrencies, such as Bitcoin, show a positive correlation between their prices and the sizes of the user groups [13–15]. The kitties in the game are ERC-721 token, and therefore, the same rule applies. On the one hand, the expansion of the player community has increased the demand for kitty tokens and promoted the rise of kitty price. On the other hand, the increase in kitty price attracted more players to join the community. Eventually, the entry of a large number of players into the game has led to a surge in demand for kitties, hence the kitty price (see **Figure 7**). The mean price of kitties in each day is significantly higher than the median price because a small number of kitties were sold at significantly higher prices than average.

5.2 Reasons for the Rapid Fading of Game Popularity

The rapid growth of game popularity only lasted less than ten days. Since then, the number of players has dropped sharply. Lee et al. [16] noted that users' playing behaviors in CryptoKitties are affected by speculative and enjoyable factors. Here, we propose four specific reasons that could account for the rapid decline in game popularity: the out-of-balance of the supply and demand of kitties; the loss of profit in kitty trading; the increasing gap between the rich and poor players, and the limitations of blockchain systems.

5.2.1 The out of Supply and Demand Balance

The large number of players poured in during the explosive growth stage bred a large number of kitties in a very short time. Since December 4, 2017, the number of new kitty listings has significantly exceeded the number of kitties sold every day, resulting in a rapid increase in the number of kitties left on sale, i.e., stock inventory (see **Figure 8A**). The kitty market has become a buyer's market, and the competition has intensified. The ratio of a successful sale for kitties listed on each day also decreased (see **Figure 8B**), and the turnover time, i.e., the average time interval between kitty listing and trade closing becomes longer (see **Figure 8C**).

5.2.2 The Loss of Profit in Kitty Trading

Buchholz et al. [17] pointed out that the value of cryptocurrencies has no benchmark but purely depend on the supply and demand in the market. As the supply of kitties significantly overwhelmed the demand, the price of kitties dropped significantly. Profit is an important motivation to encourage the players to stay in the game. If their revenue from selling kitties becomes lower than the costs, the players' enthusiasm will decline or even disappear.

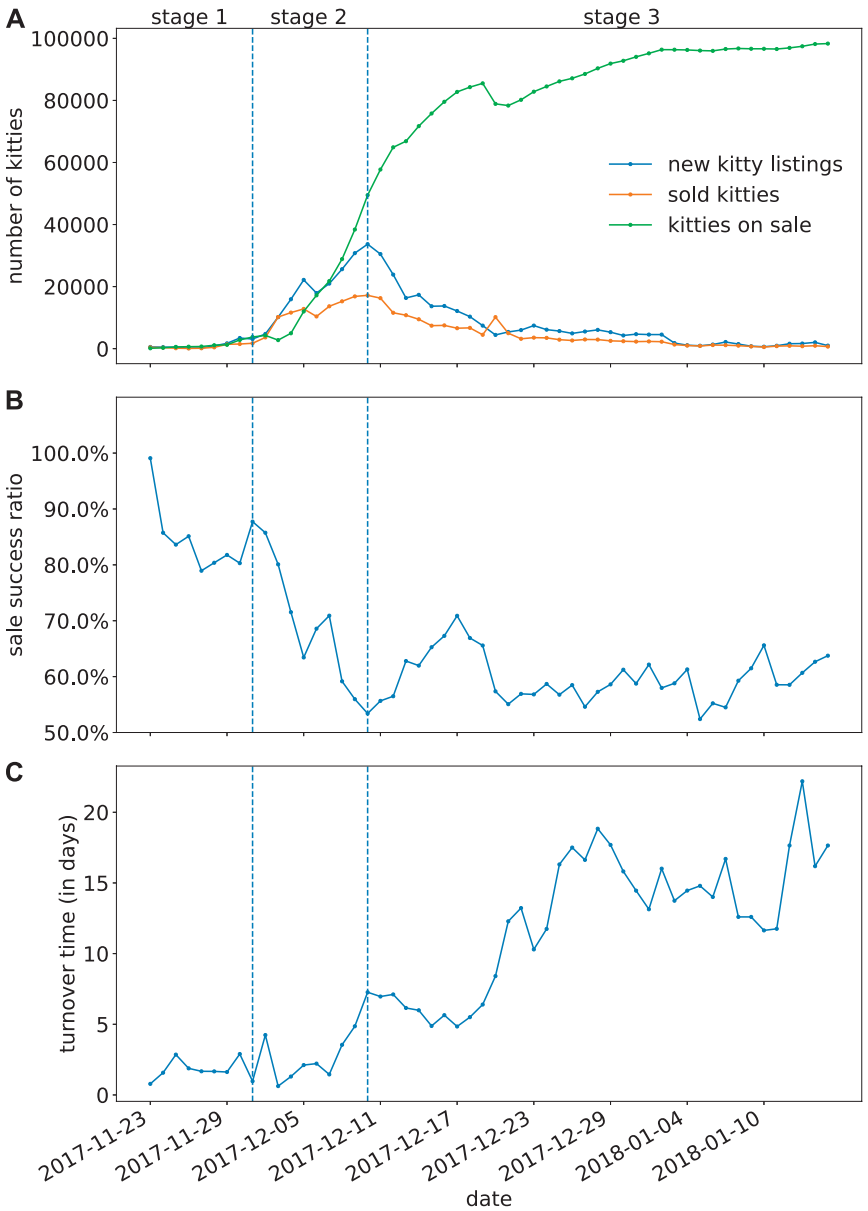


FIGURE 8 | The supply and demand of kitties in the market. **(A)** The numbers of new kitty listings, kitties sold, and kitties on sale in the market every day. **(B)** The ratio of successful sale for kitties listed on each day. **(C)** Turnover time, i.e., the average time interval between kitty listing and trade closing for kitties listed on each day. Dotted lines separates the stage 1, 2 and 3.

Teoretically, suppose a player uses two of his own kitties to breed a new kitty and sell it at the median kitty price (excluding the 0-generation kitties) through the SalesAuction contract on the same day. The average cost of breeding and selling a kitty in one day can be written as

$$c = f_{\text{breed}} + g_{\text{breed}} + g_{\text{sell}},$$

where f_{breed} is the average breeding fee, g_{breed} is the average gas fee for kitty breeding, and g_{sell} is the average gas fee to sell a kitty through SalesAuction contract on a particular day. The profit of a kitty sale on the same day can be written as

$$p = 0.9625 \times v_{\text{median}} - c,$$

where v_{median} is the median price of kitties (excluding 0-generation kitties) sold on that day. The seller can only receive 96.25% of the dealing price after deducting the 3.75% handling fee received by the game publisher.

Figure 9A shows that the cost break-down for breeding and selling increased sharply in stage 2. Among all the costs, the breeding fee is the highest, followed by the miner's fee for the selling operation, and the miner's fee for the breeding operation is the lowest. **Figure 9B** shows that starting from December 13, 2017, the average profit for a player to breed and sell a kitty

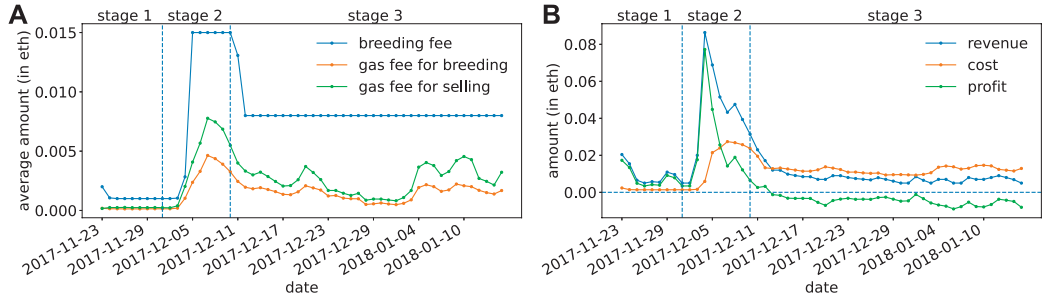


FIGURE 9 | The loss of profit in kitty sales. **(A)** The average breeding fee, gas fee for breeding, and gas fee for selling a kitty through SalesAuction contract on each day. **(B)** The revenue (median price of kitties), cost, and profit for breeding and selling a kitty on each day. Dotted lines separates the stage 1, 2 and 3.

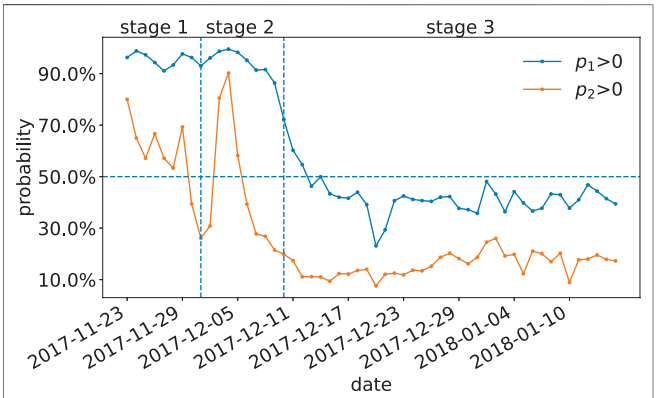


FIGURE 10 | The probability of generating positive profit in selling a kitty each day. Dotted lines separates the stage 1, 2 and 3.

became negative, indicating that the player may lose money when playing the game.

The actual in-game breeding and sale may not happen on the same day. For every kitty sold, the seller's actual profit can be evaluated by the difference between the breeding or acquisition cost and selling revenue. Here, we also estimate the actual profit of kitties sold each day. For the kitty sold for the first time, the seller's profit can be written as

$$p_1 = 0.9625 \times v - f_{\text{breed}} - g_{\text{breed}} - g_{\text{sell}} - r - g_{\text{rent}},$$

where v is the price at which the kitty is sold, f_{breed} is the breeding fee, g_{breed} is the gas fee for kitty breeding, and g_{sell} is the gas fee to sell the kitty. If the player rents another player's kitty, he has to pay the rent r and gas fee g_{rent}. The seller can only receive 96.25% of the dealing price after deducting the 3.75% handling fee for the game publisher. For the kitties that are bought from others and resold, the seller's profit can be written as

$$p_2 = 0.9625 \times v_{\text{sold}} - v_{\text{purchase}} - g_{\text{purchase}} - g_{\text{listing}},$$

where v_{sold} is the sold price, v_{purchase} is the purchase price, g_{purchase} and g_{listing} are the gas fees paid in purchasing and selling the kitty. The seller can only receive 96.25% of the dealing price after deducting the 3.75% handling fee for the game publisher.

Figure 10 shows the probability of generating a positive profit by selling kitties each day. After December 6, 2017, this probability for kitty resales became less than 50%. After December 13, 2017, this probability for selling self-bred kitties became less than 50%. Whether the player sells kitties bred by self or previously purchased, there is a great chance of losing money.

5.2.3 The Increasing Gap Between the Rich and Poor

Players receive revenue from selling and lending kitties. In the first stage of the game, the Gini coefficient of daily revenue from selling and leasing increased significantly (see **Figure 11A**), and that of the cumulative revenue for all the addresses also increased significantly (see **Figure 11B**). After entering the third stage, although the Gini coefficient of the revenue earned by players from selling and renting fluctuated, they all remained at a relatively high level (greater than 0.6). The Gini coefficient of accumulated revenue stayed at a high level (greater than 0.8). Since 0-generation kitties were mainly sold by game publisher, these sales were not considered when counting the revenue of players. Our results show that the gap between the rich and poor in the game expanded. A few players earned most of the money from the game, while most can only get very little income, if any. The increasing gap in the revenue has caused most players' gaming experience to deteriorate, and they gradually withdrew from the game.

Not only the revenues, kitty ownerships were also gradually concentrated to a few players. The Gini coefficient of the number of kitties owned by all addresses at each stage is shown in **Figure 12**. When counting the number of kitties belong to an address, unsold kitties in the SalesAuction contract belong to the seller, and unrented kitties in the SiringAuction contract belong to the lender. In the first and second stages, many new players entered the game, all making purchasing, and the Gini coefficient gradually decreased. However, as the number of new players decreased and existing players quit, the Gini coefficient rose in the third stage and kept rising in the fourth stage. As of April 2020, the Gini coefficient of kitties with addresses has exceeded 0.8. At this time, the resources in CryptoKitties became highly concentrated.

5.2.4 Limitations of Blockchain Systems

The cost of performing operations on a public blockchain system is highly volatile due to the unstable price of

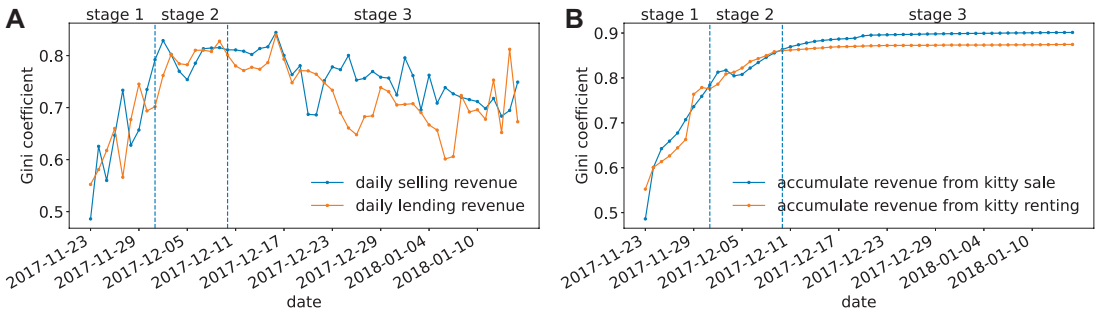


FIGURE 11 | Gini coefficients of **(A)** daily selling and lending revenue and **(B)** the accumulate revenue from kitty sale and renting for all the addresses. Dotted lines separates the stage 1, 2 and 3.

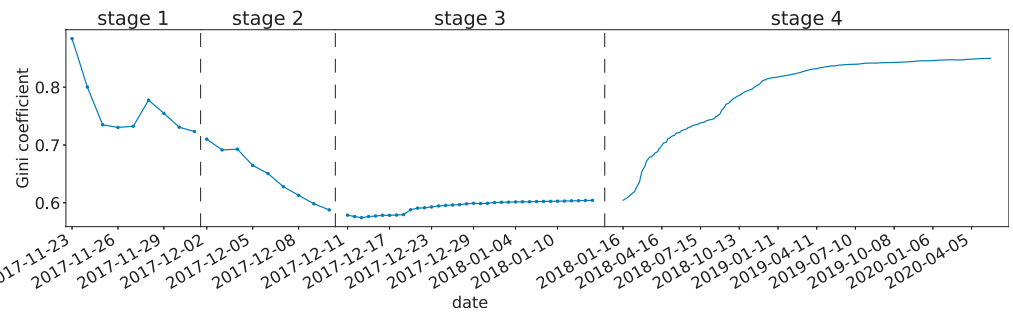


FIGURE 12 | The Gini coefficient of kitties owned by all addresses. Dotted lines separates the four stages. The *x*-axis are re-scaled to better illustrate the parameter dynamics in stages 1, 2 and 3.

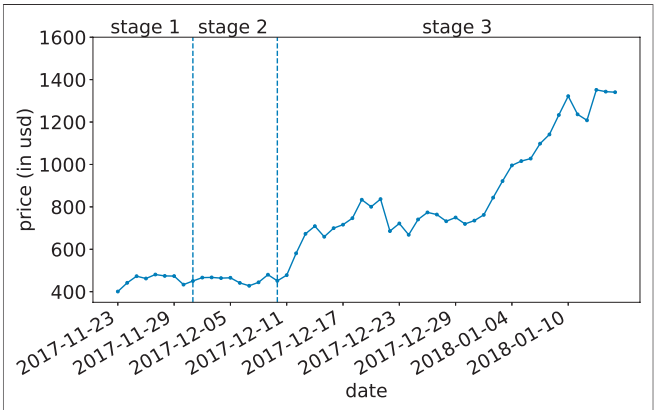


FIGURE 13 | The Ether price. Dotted lines separates the stage 1, 2 and 3.

cryptocurrencies, resulting in it difficult to control the cost of the applications deployed on the blockchain. As CryptoKitties was deployed on Ethereum, the cost of playing the game (including the costs of buying, breeding, and renting kitties, as well as the fees paid to Ethereum miners) has risen significantly due to the rapid rise of Ether price in the third stage. Ether price increased from US $451 on December 10, 2017, to US $1,322 on January 10, 2018 (see **Figure 13**), resulting in a significant increase in the cost of playing the game, raising the bars for new players entering the game.

In addition to the cryptocurrency price, other potential limitations of blockchain systems include the unnecessary gas cost by poorly designed smart contracts and the low system throughput (measured in transaction per second, TPS). Under-optimized smart contracts will consume more gas than necessary [18], making it more expensive for users to play games. Chen et al. [19, 20] studied the gas cost mechanism of Ethereum and proposed a way to optimize smart contracts through analyzing bytecodes, potentially reducing the gaming costs. The low throughput of Ethereum [21] has rendered that concurrent operations by many users are not feasible. Once too many players have joined the game, the time needed to validate operations in the game takes too long, therefore sabotaging the players' gaming experiences.

6 CONCLUSION

This paper is the first to fully unveil the user activities in the once most popular blockchain game CryptoKitties and

identify the reasons for its rise and fall. Based on the number of addresses associated with the game every day, we divide the process of CryptoKitties into four stages: the primer, the rise, the fall, and the serenity. We extracted all the five million kitty transactions from the Ethereum blockchain and constructed the kitty ownership transfer network for characterizing the user behaviors. We found that a large number of players flooded in the game in the early days but quickly withdrew later, and a few big players gradually took control of the game.

We found that the public attention drew by the message that a special kitty was sold at an extremely high price eventually led to the explosive growth of game popularity. For the rapid decline of the popularity, reasons including 1) the oversupply of game props, i.e., the kitties, 2) the loss of profit in the game prop trading, 3) the increasing gap between the wealth distribution among the players, and 4) the limitations of blockchain are accounted for.

Drawing from these observations, we advise on the designing of future blockchain games as follows.

1. Design a reasonable prop output mechanism to keep a balance between supply and demand.
2. Provide a mechanism for adjusting player income to prevent players losing money in prop trading with a high probability.
3. Design a mechanism to narrow down the gap between the rich and poor and prevent the revenue from being gained by only a few players.
4. To fully consider the limitations of blockchain systems in the game design.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. This data can be found here: https://github.com/jiangxjcn/Cryptokitties-analysis.git.

AUTHOR CONTRIBUTIONS

Both authors designed the study and wrote the paper. XJJ conducted data analysis.

FUNDING

This work is supported by CityU Start-up Grant for New Faculty (No. 7200649) and CityU Strategic Research Grant (No. 11503620).

ACKNOWLEDGMENTS

We thank Si-Hao Liu and Ying-Hao Zhang for their suggestions on the revision of this article.

REFERENCES

1. Nakamoto S. *Bitcoin: A peer-to-peer electronic cash system* (2008).
2. Buterin V. *Ethereum white paper: a next generation smart contract & decentralized application platform* (2014).
3. Mohanta BK, Panda SS, Jena D. An overview of smart contract and use cases in blockchain technology. In: 2018 9th International conference on computing, communication and networking technologies (INCCCNT); 2018 July 10–12; Bangalore, India. NEW YORK: IEEE (2018), 1–4.
4. Min T, Wang H, Guo Y, Cai W. Blockchain games: a survey. In: 2019 IEEE Conference on Games (CoG); 2019 August 20–23; London, United Kingdom. NEW YORK: IEEE (2019). p. 1–8.
5. Scholten OJ, Hughes NGJ, Deterding S, Drachen A, Walker JA, Zendle D. Ethereum crypto-games: mechanics, prevalence, and gambling similarities. In: Chi Play'19: Proceedings of the Annual Symposium on Computer-Human Interaction in Play; 2019 October 17; Barcelona, Spain. New York: ACM (2019) 379–89.
6. *Cryptokitties craze slows down transactions on ethereum* (2017). Available from: http://www.bbc.com/news/technology-42237162 (Accessed December 5, 2017).
7. Chen T, Zhu Y, Li Z, Chen J, Li X, Luo X, et al. Understanding ethereum via graph analysis. In: IEEE INFOCOM '18 conference on computer communications; 2018 April 16–19; Honolulu, HI, USA. NEW YORK: IEEE (2018a). p. 1484–92.
8. Somin S, Gordon G, Altshuler Y. Social signals in the ethereum trading network (2018). p. 12097. Available from: arXiv:1805.12097.
9. Guo D, Dong J, Wang K. Graph structure and statistical properties of ethereum transaction relationships. *Inf Sci* (2019) 492:58–71. doi:10.1016/j.ins.2019.04.013
10. Huang Y, Wang H, Wu L, Tyson G, Luo X, Zhang R, et al. Understanding (Mis)Behavior on the EOSIO blockchain. *Proc ACM Meas Anal Comput Syst* (2020) 4(2):1–28. doi:10.1145/3392155
11. Etherscan. *The ethereum block explorer* (2017). Available from: https://etherscan.io/ (Accessed May 19, 2020).
12. Tepper F. *People have spent over $1 m buying virtual cats on the ethereum blockchain* (2017). Available from: https://techcrunch.com/2017/12/03/people-have-spent-over-1m-buying-virtual-cats-on-the-ethereum-blockchain/ (Accessed December 4, 2017).
13. Baumann A, Fabian B, Lischke M. Exploring the bitcoin network. In: 10th International Conference on Web Information Systems and Technologies volume 2: WEBIST '14; 2014 Apr 3–5; Barcelona, Spain. Setúbal, Portugal: SciTePress (2014), 369–74.
14. Sorgente M, Cibils C. *The reaction of a network: exploring the relationship between the bitcoin network structure and the bitcoin price* (2014). Available from: http://snap.stanford.edu/class/cs224w-2014/projects/cs224w-27-final.pdf (Accessed December 10, 2014).
15. Szücs I, Kiss A. Quantitative analysis of bitcoin exchange rate and transactional network properties. In: 9th International Conference on Applied Informatics; 2014 Jan 29–Feb 1; Eger, Hungary. (2015), vol. 1, 201–11.
16. Lee J, Yoo B, Jang M. Is a blockchain-based game a game for fun, or is it a tool for speculation? an empirical analysis of player behavior in crypokitties. In: Xu JJ, Zhu B, Liu X, Shaw MJ, Zhang H, Fan M, editors. *The ecosystem of e-business: technologies, stakeholders, and connections. WEB 2018. Lecture Notes in Business Information Processing*. vol. 357. Cham, Switzerland: Springer International Publishing (2018). p. 141–8.
17. Buchholz M, Delaney J, Warren J, Parker J. *Bits and bets, information, price volatility, and demand for bitcoin* (2012). Available from: https://www.reed.edu/economics/parker/s12/312/finalproj/Bitcoin.pdf (Accessed May 19, 2020).
18. Chen T, Li X, Luo X, Zhang X. Under-optimized smart contracts devour your money. In: 2017 IEEE 24th international conference on software analysis, evolution and reengineering (SANER); 2017 Feb 20–24; Klagenfurt, Austria. NEW YORK: IEEE (2017). p. 442–6.
19. Chen T, Li Z, Zhou H, Chen J, Luo X, Li X, et al. ving money in Towards saving money in using smart contracts. In: 2018 IEEE/ACM 40th international

conference on software engineering: new ideas and emerging technologies results (ICSE-NIER); 2018 May 27–June 3; Gothenburg, Sweden. NEW YORK: IEEE (2018b). p. 81–4.

20. Chen T, Li X, Wang Y, Chen J, Li Z, Luo X, et al. An adaptive gas cost mechanism for ethereum to defend against under-priced DoS attacks. In: Liu J, Samarati P, editors. International conference on information security practice and experience; 2017 December 13–15; Melbourne, Australia. Cham, Switzerland: Springer (2017b). p. 3–24.
21. Tang H, Shi Y, Dong P. Public blockchain evaluation using entropy and topsis. *Expert Syst Appl* (2019) 117:204–10. doi:10.1016/j.eswa.2018.09.048

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 16 March 2021
doi: 10.3389/fphy.2021.631659

Co-Investment Network of ERC-20 Tokens: Network Structure Versus Market Performance

Si-Hao Liu[1] *and Xiao Fan Liu*[2]*

[1]Department of Computer Science and Technology, School of Computer Science and Engineering, Southeast University, Nanjing, China, [2]Web Mining Laboratory, Department of Media and Communication, City University of Hong Kong, Hong Kong, China

Cryptocurrencies have attracted extensive attention from individual and institutional investors in recent years. In this emerging and inefficient capital market, the roles that institutional investors play can have a remarkable impact on the market. This paper investigates the ERC-20 token investment market from a network perspective. Using a dataset containing 317 ERC-20 tokens and their institutional investors at the end of June 2020, we construct a co-investment network of tokens connected by the sharing of institutional investors. Specifically, we examine whether the tokens' market embeddedness, measured by their network structural properties, can influence their market performance, as well as whether the tokens' structural similarity in the co-investment network can influence similarity of their market performance. Our results indicate that strength centrality, closeness centrality, betweenness centrality, and clustering coefficient have a significant impact on trading volume and liquidity of the market. And there is a significantly positive correlation between the Jaccard similarity index and tokens' market performance similarity. This work demonstrates the non-negligible influence of the institutional investors and the diffusion of such influence through co-investment relationships in the cryptocurrency market. We expect the analysis could further enhance the understanding of the inefficiency and vulnerability of this emerging market.

Keywords: Cryptocurrency, Ethereum, ERC-20, co-investment, complex networks, institutional investors

OPEN ACCESS

Edited by:
Hui-Jia Li,
Beijing University of Posts and Telecommunications (BUPT), China

Reviewed by:
Jianhong Lin,
University of Zurich, Switzerland
Xiao-Pu Han,
Hangzhou Normal University, China

***Correspondence:**
Xiao Fan Liu
xf.liu@cityu.edu.hk

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *20 November 2020*
Accepted: *20 January 2021*
Published: *16 March 2021*

Citation:
Liu S-H and Liu XF (2021) Co-Investment Network of ERC-20 Tokens: Network Structure Versus Market Performance. Front. Phys. 9:631659. doi: 10.3389/fphy.2021.631659

1 INTRODUCTION

As the end of 2020, there are more than 7,000 cryptocurrencies in circulation worldwide. The total cryptocurrency market value has exceeded 300 billion US dollars, with a daily trading volume topping 200 billion [1]. However, only a few hundred of these cryptocurrencies run on their own blockchains, while others reside on Ethereum-like blockchain platforms, which support users to issue smart contract-based cryptocurrencies, also known as tokens, following token standards such as ERC-20, ERC-721, and ERC-777. The number of smart contract-based tokens on Ethereum is more than 300,000 as of 2020 [2], though not all are publicly traded in cryptocurrency exchanges.

Despite the soaring capitalization, the emerging cryptocurrency market also exhibits extremely high volatility. Hence, finding the driving forces of the market is crucial to the understanding of the formation and development of cryptocurrencies' prices. All the evidence points out that this market is highly inefficient. Buchholz et al. [3] claimed that the supply and demand in the market are among the main drivers of the bitcoin price. Wijk [4] emphasized the role of global macroeconomic

indicators, e.g., stock indices, exchange rates, and oil prices, in determining Bitcoin's price. He found that the Dow Jones Index, the euro-dollar exchange rate, and the WTI oil price have a long-term and significant effect on Bitcoin's value. Kristoufek [5] found that the price of Bitcoin was significantly and positively correlated with public interests measured by Google Trends and Wikipedia queries, as well as technical indexes, such as hash rates and mining difficulty, in the long run. Moreover, the cryptocurrency market' performance has also been found to be related to media exposure [6, 7], policies and regulations [8, 9], and other financial assets [10, 11], all revealing the inefficiency of the market.

An inefficient market is easily manipulated, especially by large investors. Compared to individual investors, institutional investors can rely on their capital, talent, and information advantages to profit [12], and they also have a stronger ability to capture and conceal bad news in the market [13]. In the case of ERC-20 tokens, institutional investors play a crucial role in both the primary and secondary markets. In a typical ERC-20 token initial offering (ICO) process, i.e., the primary market, the institutional investors would first purchase a large chunk of tokens from the issuer and redistribute a proportion to individual investors before public listing while retaining some tokens for market-making in the secondary market. Institutional investors commonly invest in more than one token to disperse their risks among multiple projects. As a result, they act as intermediaries between different tokens, therefore transmitting market influences from one token to another. To the best of our knowledge, there is still a lack of research on the relationship between institutional investors' investment preference and the performance of the cryptocurrency market.

This paper investigates the impact of institutional investors' dispersed investments on the cryptocurrency market, i.e., how the individual ERC-20 tokens' market performances, e.g., price, volatility, and trading volume, are affected by their sharing of institutional investors. We construct a co-investment network that uses ERC-20 tokens as nodes and the pairwise sharing of institutional investors as edges. From the macroscopic perspective, such a co-investment network offers a panorama of the institutional investors' influence distribution. While from the microscopic perspective, we can closely examine the intertwining influence of multiple institutional investors on the individual ERC-20 tokens.

Specifically, we try to answer two research questions. First, how the market "embeddedness" of individual ERC-20 tokens, in analogy to Granottever's market embeddedness of social-economical actors [14] and measured by the corresponding nodes' network structural properties, affects the tokens' market performance. Second, whether tokens with similar "embeddedness", measured by the similarity of their network structure, and therefore experiencing similar market impacts, also have converged market performance.

The rest of the paper is organized as follows. **Section 2** describes the data and their sources. **Section 3** describes the research methods, including the selection and calculation of six indicators quantifying market performance, as well as the construction and calculation of the co-investment network. **Section 4** presents the empirical results of the research hypothesis in detail and makes an in-depth analysis of the results. **Section 5** summarizes the whole paper and discusses the direction of future work.

2 DATA

The institutional investors' investments into ERC-20 tokens can be obtained from Block123.com [15]. As of June 2020, the website listed 556 cryptocurrency projects, of which 317 are ERC-20 tokens, and their institutional investors. At the time of data acquisition, all 317 ERC-20 tokens were actively trading in the cryptocurrency market. To the best of the authors' knowledge, block123.com provides the largest and most complete token-investor relationship dataset that is publicly available. A detailed description of the dataset is given in **Supplementary Section 1**.

Market data, including the daily closing price, trading volume, and market capitalization (all in USD), of the 317 tokens are obtained from CoinMarketCap.com. Since cryptocurrencies are traded 7/24, we take the last reported price in one day as the daily closing price. The market data range from 1 to 31 July 2020, spanning one month after the acquisition of the token-investor dataset. And 85% of the 317 tokens are valued in the top 20% of the market.

Moreover, we consider three previously claimed drivers of token prices by Liu et al. [16] as extra factors influencing market performance. First, the numbers of tokens' transactions on the blockchains are used as a proxy for adopters' activity. The data are obtained from Etherscan [2]. Second, the indicators of tokens' attention on social platforms, including Twitter followers, Telegram channel subscribers, Reddit board activities, and website rankings are used to represent public interests to the tokens. The data are obtained through the CoinGecko API [17]. Third, the technical indicators of the cryptocurrency projects, such as the Github popularity, are used to indicate the blockchain projects' technical development. The data are also obtained from CoinGecko. These control variables are summarized in **Table 1**. Note that reddit_discussions and tech_score are combined values of similar factors. Details of the combination methods are described in **Supplementary Section 2**.

3 METHODS

3.1 ERC-20 Tokens' Market Performance and Similarity

We use six indicators to quantify the market performance of ERC-20 tokens. Daily price p_t, trading volume v_t, and market capitalization m_t are as provided in the data, while daily return, volatility, and (il)liquidity are defined as follows.

The daily return r_t is defined as

$$r_t = \frac{p_t - p_{t-1}}{p_{t-1}}.$$

The volatility ν in a W-day window is defined as

TABLE 1 | Descriptions of the control variables.

Name	Symbol	Description
Adoptor activity	transfers	Number of a token's transactions
Public interests	twitter_followers	Number of followers on a token's twitter account
	tg_subscribers	Number of subscribers to a token's telegram channel
	reddit_subscribers	Number of subscribers to a token's reddit board
	reddit_discussions	Average user activity per hour on reddit within 48 h
	reddit_active_users	Average active users per hour on reddit within 48 h
	web_rank	Global ranking of visits to a token's official website (alexa ranking)
Technical development	tech_score	A token's technical attention on github

$$\nu = \begin{cases} \sqrt{\frac{1}{W-1}\sum_{t=1}^{W}\left(r_{\ln,t} - \overline{r_{\ln}}\right)^2}, & W \geq 30, \\ \sqrt{\frac{1}{W}\sum_{t=1}^{W}\left(r_{\ln,t} - \overline{r_{\ln}}\right)^2}, & W < 30, \end{cases}$$

where $r_{\ln,t} = \ln p_t - \ln p_{t-1}$ is the daily logarithm return and $\overline{r_{\ln}} = 1/W\sum_{t=1}^{W} r_{\ln,t}$ is the average return in the W-day window. ILLIQ [18] is the most commonly used indicator to measure market liquidity. For a W-day window,

$$\text{ILLIQ} = \frac{1}{W}\sum_{t=1}^{W}\frac{|r_t|}{v_t/10^6}.$$

ILLIQ is a direct reflection of how sensitive the prices is to volume. The larger its value is, the higher the level of price change per unit trading volume is. Since the average trading volume is in millions of dollars, we divide the unit of volume by 1,000,000.

The monthly (July 2020) price (n = 317, min = 0.0000126, max = 482, mean = 27.3, skewness = 17.40), market capitalization (n = 290, min = 13,810.12, max = 2638,362,922.00, mean = 40,925,401.09, skewness = 10.78), volume (n = 317, min = 0.06, max = 737,208,083.20, mean = 8,808,034.45, skewness = 11.42), return (n = 317, min = −0.04, max = 0.26, mean = 0.01, skewness = 4.61), volatility (n = 317, min = 0.00289, max = 0.581, mean = 0.0866, skewness = 3.11), and illiquidity (n = 316, min = −0.000011, max = 1,390,000.00, mean = 804, skewness = 14.40) of the tokens show a highly inequality in the cryptocurrency market. We calculate monthly illiquidity and volatility based on a 30-days window, and mean values of all daily data for monthly price, market capitalization, trading volume and return. All the indicators' standard deviations are greater than their mean, meaning that the market quotations of different tokens varies greatly, and therefore, are highly heterogeneous.

Bitcoin and Ether, the original cryptocurrency of Ethereum, are the leaders in the cryptocurrency market. To capture the similarity between the market performance of two tokens, we use partial correlation coefficient of their market indicator time series, eliminating the same influence brought by the market leaders. For example, the partial correlation between two daily return series r_i and r_j is

$$\rho_{r_i,r_j(r_{\text{Ether}})} = \frac{\rho_{r_i,r_j} - \rho_{r_i,r_{\text{Ether}}}\rho_{r_j,r_{\text{Ether}}}}{\sqrt{1-\rho^2_{r_i,r_{\text{Ether}}}}\sqrt{1-\rho^2_{r_j,r_{\text{Ether}}}}},$$

where ρ_{r_i,r_j} is the Pearson correlation coefficient

$$\rho_{i,j} = \frac{\text{Cov}(r_i, r_j)}{\sigma_{r_i}\sigma_{r_j}},$$

and r_{Ether} is the daily return of Ether to eliminate. Time series of liquidity and volatility are composed of results calculated based on a 3-days window, and the other four indicators' series are daily values. Refer to **Supplementary Section 3** for a detailed analysis.

3.2 Construction of the Co-investment Network

We define the co-investment network $G = (V, E)$, where V is a set of nodes representing the ERC-20 tokens and E is a set of edges connecting the nodes and representing the sharing of institutional investors between the two tokens. The edges are weighted by the numbers of shared investors between tokens. **Figure 1** shows a visualization of the ERC-20 token co-investment network.

3.3 Market Embeddedness Measures

The market embeddedness of ERC-20 tokens can be measured by various network structural properties, each reflecting a unique aspect of their market status.

Strength centrality of a node v is defined as

$$C_s(v) = \sum w(u,v),\ (u,v) \in E,$$

where $w(u, v)$ is the weight of the edge connecting nodes u and v, i.e., the numbers of shared institutional investors between these two tokens. A higher strength centrality infers that the current token has more shared institutional investors with other tokens, and hence, the more commonly selected by institutional investors in their portfolios. When the edge weights $w(u, v)$ are not considered, the strength centrality is equivalent to degree centrality.

Closeness centrality is the reciprocal of the average distance of the node to other vertices. i.e.,

$$C_c(v) = \frac{N-1}{\sum_{u\neq v} d_{u,v}}.$$

$d_{u,v}$ is the shortest path length from node u to v. For the unweighted centrality, all edge lengths are considered to be equal. When calculating the weighted centrality, the reciprocal

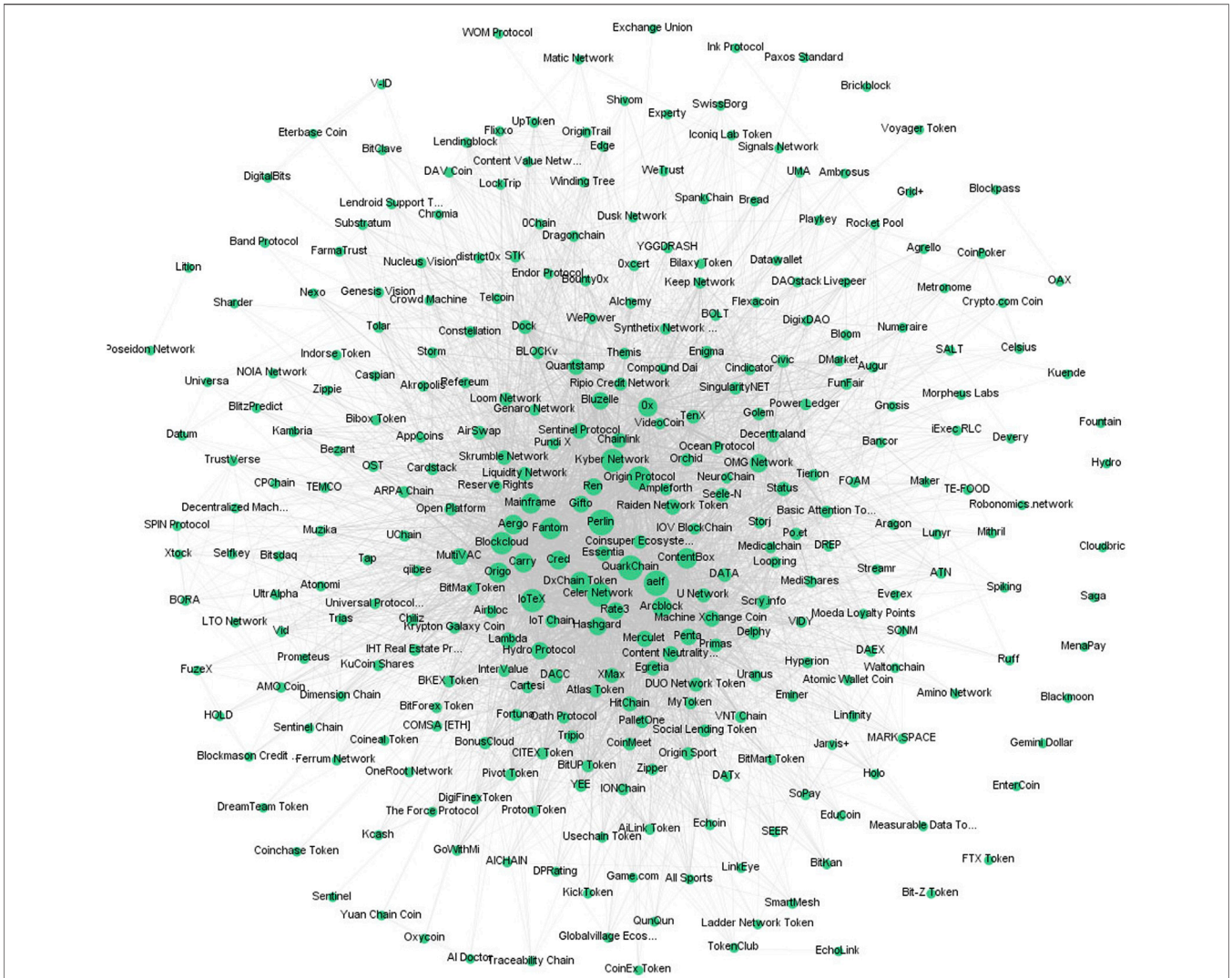


FIGURE 1 | Co-investment network of ERC-20 Tokens. The sizes of the nodes are scaled by their degrees.

of the edge weight is used as the edge's length. The higher the closeness centrality of a node is, the more central it is in the network. Tokens near the center of the network can be affected by other tokens in the whole network faster and more directly than peripheral ones, and therefore receive a more direct influence from market factors.

Betweenness centrality of a node v is the sum of the fraction of all-pairs of shortest paths that pass through v.

$$C_b(v) = \sum_{s \neq v \neq t \in V} \frac{g_{s,t}(v)}{g_{s,t}},$$

where $g_{s,t}$ is the number of shortest paths from node s to t, and $g_{s,t}(v)$ is the number of those paths passing through node v. For the unweighted centrality, all edge lengths are considered to be equal. When calculating the weighted centrality, the reciprocal of the edge weight is used as the edge's length. Betweenness centrality describes the degree to which a node acts as a connection mediator between other nodes. A token with high betweenness centrality plays a key role in the investment network, as it passes the market influence between different sectors.

Local clustering coefficient $c(v)$ of node v is the fraction of possible triangles through that node, i.e.,

$$c(v) = \frac{2T(v)}{k(v)(k(v)-1)},$$

where $T(v)$ is the number of triangles through node v and $k(v)$ is the degree of v. From the perspective of structural hole theory [19], the lower the local clustering coefficient of a node is, the more structural holes are around it. The existence of structural holes makes the node dominating the spread of influence among its neighbors. So the lower the clustering coefficient a token has, the greater influence it passes on to other tokens through shared institutional investors.

TABLE 2 | Comparison of network properties between the co-investment network and randomized networks.

	N	*M*	$\bar{k}$	*D*	*L*	$\bar{c}$	*ρ*
Co-investment network	317	5,654	35.67	5.0	2.09	0.72	0.11
Randomized network	–	–	–	4.2	2.02	0.44	–
Percentile of the empirical value in random values				79.7	100	100	

3.4 Structural Similarity Measure

The Jaccard index defines the structural similarity between different nodes based on common neighbors, i.e.,

$$J(u,v) = \frac{|\Gamma(u) \cap \Gamma(v)|}{|\Gamma(u) \cup \Gamma(v)|},$$

where $\Gamma(v)$ is the set of neighbor nodes of node v. Regarding two directly connected nodes as a portfolio, the higher the Jaccard index, the higher degree of overlap between the investment portfolios of the two tokens. Therefore, they may be affected by similar market factors through institutional investors.

4 RESULTS

4.1 Structure Properties of the Co-investment Network

Structural properties, i.e., the number of nodes N, number of edges M, average degree $\bar{k}$, network diameter D, average path length L, average clustering coefficient $\bar{c}$, and the density ρ, of the ERC-20 co-investment network as of June 2020 are shown in **Table 2**. For comparative analysis, we also construct 1,000 randomized networks with the same degree distribution as the token network based on the edge rewiring algorithm. We find that the average clustering coefficient $\bar{c}$ in the co-investment network is significantly higher than that in the randomized networks, indicating that the co-investment network is a typical small-world network like many real networks [20]. **Figure 2** shows the cumulative degree distribution of the co-investment network on a semilog coordinate. CDF(k) is the proportion of nodes with degree greater than k in the whole network. The distribution follows an exponential function $\mathrm{CDF}(k) \sim e^{-k/36.49}$, based on non-linear least squares fitting. The Kolmogorov-Smirnov test statistics for the goodness of fit is 0.06 with a corresponding p-value of 0.69.

4.2 Market Embeddedness Versus Market Performance

In light of the high skewness of market indicators, we pre-process them before further analysis. The price, market capitalization, and trading volume are taken logarithm transformations; the illiquidity is taken a negative logarithm transformation. Furthermore, all variables are standardized as $x_i = x_i - \bar{x}/\sigma$, where $\bar{x}$ is the mean value, σ is the standard deviation.

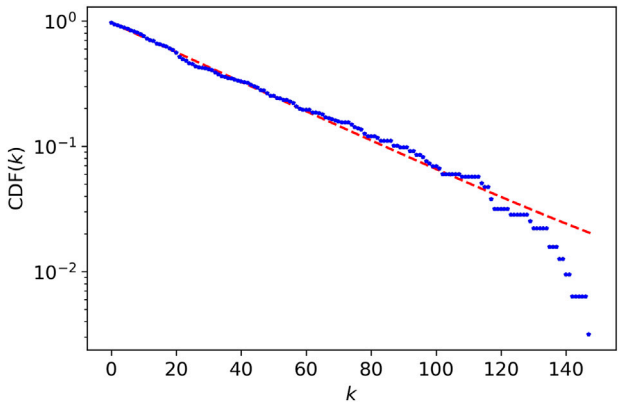


FIGURE 2 | Cumulative degree distribution of the co-investment network.

Figure 3 shows the correlations between the market indicators and the market embeddedness and control variables. The logged price, market capitalization, volume, and liquidity have medium correlations ($\pm 0.2 \sim 0.3$) with most market embeddedness measures and control variables. However, the return and volatility do not show strong correlations with any of the independent variables.

We adopt ordinary least squares (OLS) linear regression models to analyze the relationship between market performance and various market embeddedness measures of the tokens in the co-investment network. For each market indicator, e.g., price p, we first develop a baseline multiple linear regression (MLR) model

$$p = \alpha_0 + \alpha_1 * V_{\text{control}}, \quad (1)$$

where V_{control} is the vector of control variables. Then, for each of the market embeddedness measures e_i, we construct another MLR model

$$p = \alpha_0 + \alpha_1 * e_i + \alpha_2 * V_{\text{control}}. \quad (2)$$

We are interested in examining the statistical significance of e_i in model 2 and the difference ΔR^2 in the predictability, i.e., the R^2s, in the two models.

Table 3 shows the regression results for model 1 on all six market indicators. The R^2s range from 0.05 to 0.43. p-values indicate that we cannot reject the hypotheses that the number of blockchain transfers and public interests (Alexa ranking) both has

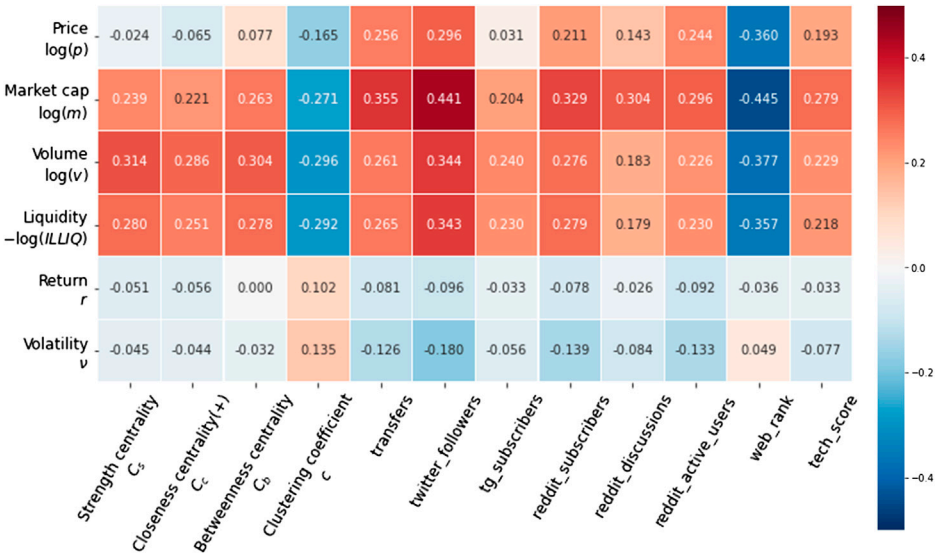


FIGURE 3 | Correlation heat map between the market indicators and the market embeddedness and control variables.

TABLE 3 | Regressions between the market indicators and the control variables (model 1).

	Price log(p)	Market cap log(m)	Volume log(v)	Liquidity −log(ILLIQ)	Return *r*	Volatility *v*
transfers	0.19*	0.14**	0.18*	0.25*	0.00	−0.01
twitter_followers	0.11	0.17	0.22	0.33	0.00	−0.02
tg_subscribers	−0.13	0.07	0.26**	0.33**	0.00	0.00
reddit_subscribers	0.00	0.04	0.09	0.13	0.00	0.00
reddit_discussions	0.10	0.11*	0.04	0.01	0.00	0.00
reddit_active_users	0.08	0.10	0.16	0.18	0.00	0.00
web_rank	−0.35***	−0.23***	−0.33***	−0.30**	0.00	0.00
tech_score	0.06	0.06	0.11	0.10	0.00	0.00
F-value	6.71	16.47	10.79	10.27	1.13	1.93
R^2	0.22	0.43	0.31	0.30	0.05	0.07

$*p < 0.05$, $**p < 0.01$, $***p < 0.001$.

TABLE 4 | Regressions between the market indicators and the tokens' market embeddedness (model 2).

		Price log(p)	Market cap log(m)	Volume log(v)	Liquidity −log(ILLIQ)	Return *r*	Volatility *v*
Strength centrality C_s	Coef	−0.06	0.08	0.36***	0.40***	0.00	−0.01
	F-value	6.00	15.06	12.24	11.28	1.01	1.89
	ΔR^2	0.00	0.01	0.06	0.05	0.00	0.01
Closeness centrality (+) C_c	Coef	−0.05	0.10*	0.40***	0.44***	0.00	−0.01
	F-value	5.99	15.32	12.96	11.86	1.02	1.91
	ΔR^2	0.00	0.01	0.07	0.06	0.00	0.01
Betweenness centrality C_b	Coef	0.04	0.08	0.26**	0.27*	0.00	0.00
	F-value	5.97	15.14	11.06	10.15	1.07	1.71
	ΔR^2	0.00	0.01	0.03	0.02	0.00	0.00
Clustering coefficient *c*	Coef	−0.12	−0.19***	−0.44***	−0.54***	0.00	0.01*
	F-value	6.24	17.29	13.81	13.53	1.09	2.43
	ΔR^2	0.01	0.04	0.08	0.09	0.00	0.03

$*p < 0.05$, $**p < 0.01$, $***p < 0.001$, *(+)weighted*.

TABLE 5 | Regressions between the partial correlations of market indicators and the Jaccard similarity between nodes (model 3).

	Price	Market cap	Volume	Liquidity	Return	Volatility
Coef	0.34***	0.48***	0.05***	0.08***	0.14***	0.04**
F-value	247.03	345.30	13.94	72.30	196.62	7.78
R^2	0.01	0.01	0.00	0.00	0.00	0.00

*$p < 0.05$, **$p < 0.01$, ***$p < 0.001$.

impacts on the price, market capitalization, volume, and liquidity of tokens. Meanwhile, the number of Telegram subscribers has a significant impact on the volume and liquidity; while the Reddit user activities can have an impact on the tokens' market capitalization. However, none of the control variables are significantly correlated with market return and volatility. Moreover, the effect sizes of public interest and social network user activities are larger than blockchain activities. It means that people may prefer to treat tokens as an investment tool instead of using them for actual transactions or consumption.

Table 4 shows the regression results of model 2. Specifically, strength centrality, at a significance level of 0.1%, improves the R^2s of trading volume and liquidity by 0.06 and 0.05, respectively. It means that the more favored by institutional investors, the larger a token's market trading volume and liquidity will be. Closeness centrality is significant at the level of 0.1% for the trading volume and liquidity of tokens, and significant at the level of 5% for the market value, with positive estimated coefficients of 0.40, 0.44, and 0.10, respectively. It suggests that the more direct market impact the tokens receive through institutional investors, the higher their market trading activity will be. Betweenness centrality is significant at the level of 1% for the trading volume with a positive estimated coefficient of 0.26, 5% for the liquidity with a positive estimated coefficient of 0.27. It shows that the stronger the mediation power a token has in the market, the larger liquidity. Clustering coefficient is significantly negatively correlated with the market capitalization, trading volume, and liquidity of tokens at a level of 0.1%, and significantly positively correlated with tokens' volatility. This evidence indicates that tokens with less local influence have a low market capitalization and trading volume, poor liquidity, and high volatility. Also, we can infer that the tokens with greater local influence have better market liquidity and lower volatility. For market embeddedness measures with both weighted and unweighted definitions, only those with better regression results are reported here. Other results can be found in **Supplementary Section 4**.

4.3 Structural Similarity Versus Market Performance Similarity

Again, we use OLS regression models to test our hypothesis that token nodes with similar network structures in the co-investment network, hypothetically impacted by similar market factors, will lead to convergence in their market performance.

The linear regression model between the structure similarity and the partial correlation coefficient of the tokens' market indicators is defined as

$$\rho_{i,j(\text{Ether})} = \beta_0 + \beta_1 * J(i,j), \tag{3}$$

where $J_{i,j}$ represents the Jaccard similarity between node i and node j, and $\rho_{i,j(\text{Ether})}$ represents the partial correlation coefficient.

Table 5 shows the regression results of model 3. We can find that the Jaccard similarity index is significantly positively correlated with all the market indicators' partial correlations, confirming our hypothesis. That is to say, the more common neighbors the two token nodes have in the co-investment network, i.e., the more overlapped their portfolios are, the more similar their market performance, including price, market capitalization, trading volume, liquidity, return, and volatility, will be.

5 CONCLUSION AND DISCUSSION

This paper studies the role institutional investors play in the ERC-20 token market and how they affect the market performance of tokens, e.g., price, trading volume, market capitalization, liquidity, return, and volatility. We construct a co-investment network with ERC-20 tokens as nodes and the pairwise sharing of institutional investors as edges. As such, the intertwined influences of institutional investors on different tokens are embedded in the network.

The significant correlations between the strength centrality, closeness centrality, betweenness centrality, clustering coefficient of tokens, and their market performance reveal institutional investors' positive impact on promoting market liquidity and reducing market volatility. Moreover, token nodes' structural similarity measured by the Jaccard index is significantly positively correlated with their market indicator similarity, suggesting that the sharing of investment institutions between tokens may result in converged market performance.

Our work demonstrates the inefficiency and vulnerability of this emerging market and the non-negligible influence of the institutional investors and the diffusion of such influence through co-investment relationships in the cryptocurrency market. Furthermore, we also remind individual investors to pay extra attention in this highly speculative market, for that institutional investors may deliberately manipulative the market, creating bubbles and crushes for profit.

Note that our dataset contains only the institutional investors' investments in 317 tokens out of approximately 7,000 tokens in circulation as of 2020. Nonetheless, as the tokens are mostly highly valued ones, we believe that the co-investment network of these tokens is a representative sample of the core of the cryptocurrency market, hence our conclusions being able to be generalized to other parts of the cryptocurrency market.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. This data can be found here: https://github.com/SuperLSH/-dataset_co-investment.git.

AUTHOR CONTRIBUTIONS

Both authors designed the study and wrote the paper. S-HL conducted data analysis.

FUNDING

This work is supported by CityU Start-up Grant for New Faculty (no. 7200649) and CityU Strategic Research Grant (no. 11503620).

SUPPLEMENTARY MATERIAL

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fphy.2021.631659/full#supplementary-material.

REFERENCES

1. *Coinmarketcap* (2020). Available from: https://coinmarketcap.com/. (Accessed August 5, 2020).
2. *Etherscan* (2020). Available from: https://etherscan.io/. (Accessed July 31, 2020).
3. Buchholz M, Delaney J, Warren J, Parker J. Bits and bets, information, price volatility, and demand for bitcoin. Portland, OR:Reed College (2012). Available from: https://www.reed.edu/economics/parker/s12/312/finalproj/Bitcoin.pdf (Accessed October 19, 2020).
4. van Wijk D. *What can be expected from the bitcoin?*.[Financial Economics thesis]. Rotterdam (Netherlands): Erasmus School of Economics (2013).
5. Kristoufek L. What are the main drivers of the bitcoin price? evidence from wavelet coherence analysis. *PLoS One* (2015) 10:e0123923. doi:10.1371/journal.pone.0123923
6. Kristoufek L. Bitcoin meets google trends and wikipedia: quantifying the relationship between phenomena of the internet era. *Sci Rep* (2013) 3:3415. doi:10.1038/srep03415
7. Rognone L, Hyde S, Zhang SS. News sentiment in the cryptocurrency market: an empirical comparison with forex. *Int Rev Financial Anal* (2020) 69. doi:10.1016/j.irfa.2020.101462
8. Shanaev S, Sharma S, Ghimire B, Shuraeva A. Taming the blockchain beast? regulatory implications for the cryptocurrency market. *Res Int Business Finance* (2020) 51. doi:10.1016/j.ribaf.2019.101080
9. Aysan AF, Demir E, Gozgor G, Lau CKM. Effects of the geopolitical risks on bitcoin returns and volatility. *Res Int Business Finance* (2018) 47.
10. Corbet S, Meegan A, Larkin C, Lucey B, Yarovaya L. Exploring the dynamic relationships between cryptocurrencies and other financial assets. *Econ Lett* (2018) 165:28–34. doi:10.1016/j.econlet.2018.01.004
11. Charfeddine L, Benlagha N, Maouchi Y. Investigating the dynamic relationship between cryptocurrencies and conventional assets: implications for financial investors. *Econ Model* (2020) 85:198–217. doi:10.1016/j.econmod.2019.05.016
12. Bushee BJ, Goodman TH. Which institutional investors trade based on private information about earnings and returns? *J Account Res* (2007) 45:323–31. doi:10.1111/j.1475-679x.2007.00234.x
13. Griffin JM, Harris JH, Shu T, Topaloglu S. Who drove and burst the tech bubble? *J Finance* (2011) 66:1251–90. doi:10.1111/j.1540-6261.2011.01663.x
14. Granovetter M. Economic action and social structure: the problem of embeddedness. *Am J Sociol* (1985) 91:481–510. doi:10.1086/228311
15. Block123 (2020). Available from: https://www.block123.com/en/. (Accessed June 21, 2020).
16. Liu XF, Lin ZX, Han XP. Homogeneity and heterogeneity of cryptocurrencies. Available from: https://arxiv.org/abs/1910.01330 (2019). (Accessed June 10, 2020).
17. *Coingecko* (2020). Available from: https://www.coingecko.com/en/. (Accessed July 31, 2020).
18. Amihud Y. Illiquidity and stock returns: cross-section and time-series effects. *J Financial Markets* (2002). 5(1):31–56. doi:10.1016/S1386-4181(01)00024-6
19. Lazega E, Burt RS. Structural holes: the social structure of competition. *Revue Française de Sociologie* 36, 779 (1995). doi:10.2307/3322456
20. Watts DJ, Strogatz SH. Collective dynamics of 'small-world' networks. *Nature* (1998) 393:440–2. doi:10.1038/30918

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 21 May 2021
doi: 10.3389/fphy.2021.644102

Time-Varying Volatility in Bitcoin Market and Information Flow at Minute-Level Frequency

Irena Barjašić[1] *and Nino Antulov-Fantulin*[2]*

[1]*Department of Physics, Faculty of Science, University of Zagreb, Zagreb, Croatia,* [2]*Computational Social Science, ETH Zürich, Zürich, Switzerland*

In this article, we analyze the time series of minute price returns on the Bitcoin market through the statistical models of the generalized autoregressive conditional heteroscedasticity (GARCH) family. We combine an approach that uses historical values of returns and their volatilities—GARCH family of models, with a so-called Mixture of Distribution Hypothesis, which states that the dynamics of price returns are governed by the information flow about the market. Using time series of Bitcoin-related tweets, the Bitcoin trade volume, and the Bitcoin bid–ask spread, as external information signals, we test for improvement in volatility prediction of several GARCH model variants on a minute-level Bitcoin price time series. Statistical tests show that GARCH(1,1) and cGARCH(1,1) react the best to the addition of external signals to model the volatility process on out-of-sample data.

Keywords: bitcoin, volatility, econometrics, generalized autoregressive conditional heteroscedasticity, social media

OPEN ACCESS

Edited by:
Cuneyt Gurcan Akcora,
University of Manitoba, Canada

Reviewed by:
Jiuchuan Jiang,
Nanjing University of Finance and Economics, China
Asim Kumer Dey,
The University of Texas at Dallas, United States
Dorcas Ofori-Boateng,
Portland State University, United States

***Correspondence:**
Nino Antulov-Fantulin
anino@ethz.ch

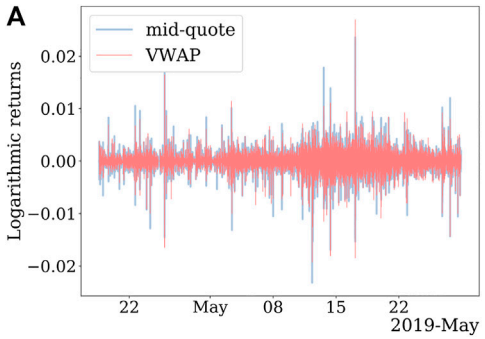
Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *19 December 2020*
Accepted: *30 April 2021*
Published: *21 May 2021*

Citation:
Barjašić I and Antulov-Fantulin N (2021) Time-Varying Volatility in Bitcoin Market and Information Flow at Minute-Level Frequency. Front. Phys. 9:644102. doi: 10.3389/fphy.2021.644102

1 INTRODUCTION

The first mathematical description of the evolution of price changes in a market dates back to Bachelier [1] (later rediscovered as Brownian motion, or random walk model), Mandelbrot [2] (price increments are Lévy stable distribution), and truncated Lévy processes [3]. An opposing hypothesis (later named "Mixture of Distribution Hypothesis") was introduced by Clark [4], where the non-normality of price returns distribution is assigned to the varying rate of price series evolution during different time intervals. The process that is driving the rate of price evolution is proposed to be the information flow available to the traders. Due to the governing of the information flow, the number of summed price changes per observed time interval varies substantially, and the central limit theorem cannot be applied to obtain the distribution of price changes. Nevertheless, a generalization of the theorem provides a Gaussian limit distribution conditional on the random variable directing the number of changes [4]. In a different approach, the autoregressive conditional heteroscedasticity (ARCH) [5] model, originally introduced by Engle, describes the heteroscedastic behavior (time-varying volatility) of logarithmic price returns relying only on the information of previous price movements. In addition to the previous values of price returns, its generalized variant GARCH [6] introduces previous conditional variances as well when calculating the present conditional variance. GARCH is thus able to account for volatility clustering and for the leptokurtic distribution of price returns, both the stylized statistical properties of returns. An alternative view comes from the GARCH-Jump model [7], which assumes that the news process can be represented as $\epsilon_t = \epsilon_{1,t} + \epsilon_{2,t}$, a superposition of a normal component $\epsilon_{1,t} = \sigma_t z_t$ and a jump-like Poisson component with intensity λ. The constant intensity was generalized to autoregressive conditional jump intensity $\lambda_t = f(\lambda_{t-1})$ in [8].



B

	mid-quote	VWAP
mean	0.000009	0.000009
median	0.000000	0.000000
max	0.023623	0.026982
min	-0.023225	-0.019309
std.dev.	0.001006	0.000952
skewness	-0.452133	-0.445740
kurtosis	39.310171	40.866263

FIGURE 1 | Volume-weighted and mid-quote logarithmic returns for the Bitcoin market. **(A)** Time series. **(B)** Descriptive statistics.

Contrary to other studies about news jump dynamics and impact on daily returns [8, 9], we will model the volatility and external signals on a minute-level granularity. On this timescale, our external signals are not modeled with Poisson-like dynamics, but added directly as an exogenous observable variable I_{t-1} to form GARCHX model.

In this article, we compare price volatility predictions of GARCH(1,1) with those of GARCHX (1,1) to explore how information is absorbed into the emerging cryptocurrency market of Bitcoin. The Bitcoin [10] is a cryptocurrency system operated through the peer-to-peer network nodes, with a publicly distributed ledger called blockchain [11]. Similar to the foreign exchange markets, Bitcoin markets [12, 13] allow the exchange to fiat currencies and back. Different studies on Bitcoin quantify the price formation [14, 15], bubbles [16, 17], volatility [18, 19], systems dynamics [20–22], and economic value [23–25]. Various studies [26–29] have used social signals from social media, WWW, search queries, sentiment, comments, and replies on forums, and [30] added information from the blockchain as an external signal to the GARCH model. Several models from the GARCH family have been used for modeling and forecasting of multiple cryptocurrencies [31, 32] on a daily level and IGARCH was shown to be superior to other models. Twitter data have been exploited to give successful daily [33] predictions on Bitcoin volume and volatility using only Twitter volume, and successful hourly predictions on returns and volatility with the added Twitter sentiment [34]. We focus this study on understanding Bitcoin volatility process and the statistical quantification of the predictive power of the class of GARCH models with exogenous signals from social media tweets, trading volume, and order book on a minute level timescale.

2 DATA

We used two types of price definitions, the mid-quote price and the volume-weighted price, both calculated at a minute level. Mid-quote price was constructed as the average between the maximum bid and the minimum ask price on the last tick per minute, and the volume-weighted average price (VWAP) as the volume-weighted average of transaction prices per minute.

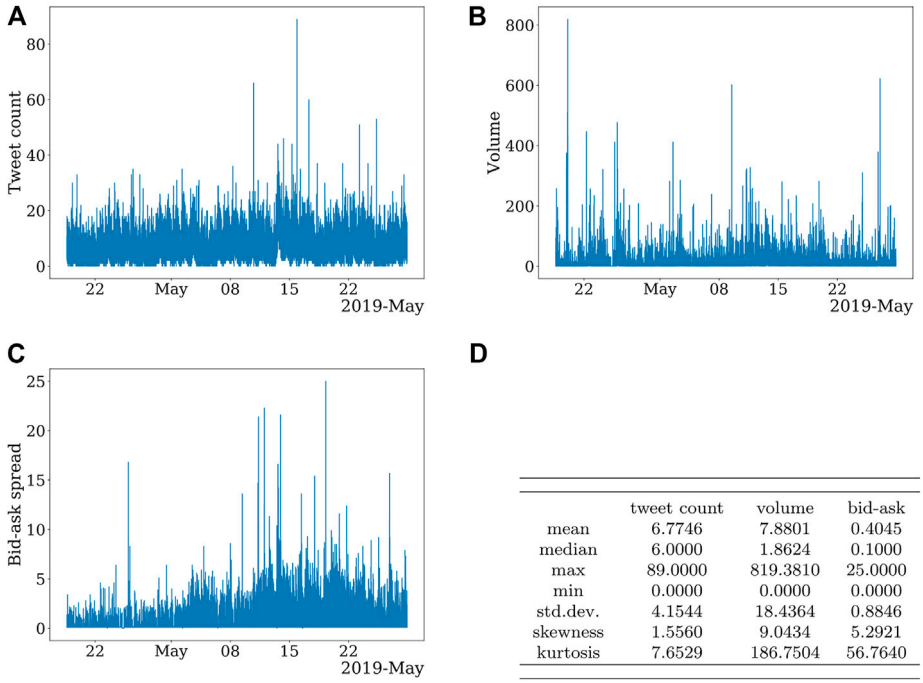
Sampling prices at such a high frequency brings up the issue of microstructure effects, such as bid–ask bounce, that introduces the autocorrelation between consecutive prices. Because of that, in addition to volume weighted prices, we use mid-quote prices that have a significantly smaller first order of autocorrelation, as explained in [35], to strengthen the robustness of the results. An autocorrelation plot for both types of price returns is shown in the Appendix.

The Bitcoin prices were obtained from the Bitfinex exchange, and logarithmic returns were calculated as a natural logarithm of two consecutive prices. The period we observed spans from April 18th, 2019, to May 30th, 2019, with 58,000 observations in total, 50,000 observations as in-sample, and 8,000 as out-of-sample, and is shown on **Figure 1A**. In the table in **Figure 1B**, we can see the descriptive statistics of both kinds of logarithmic returns; the mean values of the returns are very close to zero $(8 \cdot 10^{-6})$, with standard deviations of $9.41 \cdot 10^{-4}$ and $9.94 \cdot 10^{-4}$, both distributions are negatively skewed and leptokurtic.

Three different datasets for external signals were available as the external information proxy—a time series of the number of tweets mentioning cryptocurrency-related news [36], a time series of Bitcoin trade volumes from Bitfinex market, and a time series of Bitcoin bid–ask spread, created as a time series of absolute differences between the maximum bid and the minimum ask price at every recorded instant, also from Bitfinex market. The data are collected on a second level and shown in **Figures 2A–C**, with the descriptive statistics in **Figure 2D**. All three time series were aggregated to the minute level. The data were not normalized.

3 MIXTURE OF DISTRIBUTION HYPOTHESIS

The "Mixture of Distribution Hypothesis" models the non-normality of price returns distribution with the varying rate of price series evolution due to the different information flow during different time intervals. Practically, Clark [4] hypothesizes that this can be observed as a linear relationship between the proxy for the information flow I_t and the price change variance r_t^2, and suggests trading volume



	tweet count	volume	bid-ask
mean	6.7746	7.8801	0.4045
median	6.0000	1.8624	0.1000
max	89.0000	819.3810	25.0000
min	0.0000	0.0000	0.0000
std.dev.	4.1544	18.4364	0.8846
skewness	1.5560	9.0434	5.2921
kurtosis	7.6529	186.7504	56.7640

FIGURE 2 | (A) Time series external signal of cryptocurrency-related tweets. **(B)** Time series of trading volume on Bitfinex market for BTC-USD pair. **(C)** Time series of bid–ask spread on Bitfinex market for BTC-USD pair. **(D)** Descriptive statistics of external signals for Bitcoin market.

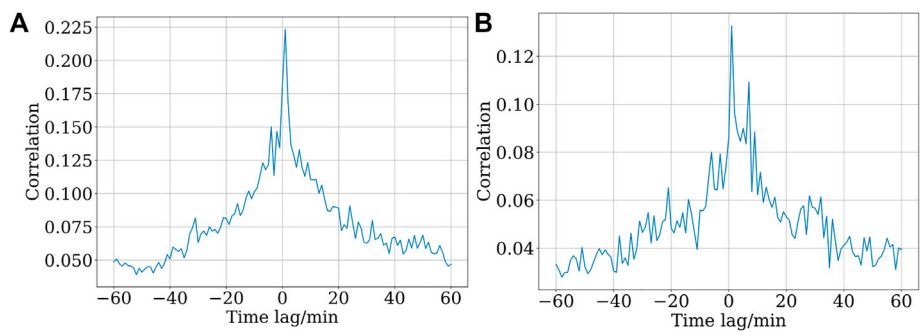


FIGURE 3 | (A) Squared volume-weighted price returns–volume correlation. All values of correlation are statistically significant (p-value ≤ 0.001). Permutation significance check indicates no statistically significant correlation between time-permuted squared price returns and volume series. **(B)** Squared volume-weighted price returns–bid–ask spread correlation. All values of correlation are statistically significant (p-value ≤ 0.001). Permutation significance check indicates no statistically significant correlation between time-permuted squared price returns and volume series.

v_t as the proxy. Tauchen and Pitts [37] state a bivariate normal mixture model which conditions the price returns and trading volume on the information flow as:

$$r_t = \sum_{i=1}^{I_t} r_{t,i}, \quad r_{t,i} \in \mathcal{N}(0, \sigma_1). \tag{1}$$

$$v_t = \sum_{i=1}^{I_t} v_{t,i}, \quad v_{t,i} \in \mathcal{N}(\mu_2, \sigma_2). \tag{2}$$

Both, the price return and trading volume are mixture of independent normal distributions with the same mixing variable I_t, which represents the number of new pieces of information arriving to market. Conditioned on I_t, price changes are distributed as $\mathcal{N}(0, I_t\sigma_1)$ and the trading volume is distributed as $\mathcal{N}(I_t\mu_2, I_t\sigma_2)$, and the model can be rewritten as:

$$r_t = \sigma_1\sqrt{I_t}z_{1t}, \quad z_{1t} \in N(0,1). \tag{3}$$

$$v_t = \mu_2 I_t + \sigma_2\sqrt{I_t}z_{2t}, \quad z_{2t} \in N(0,1). \tag{4}$$

The relationship between price variance and trading volume immediately follows:

$$Cov(r_t^2, v_t) = \sigma_1\mu_2 Var(I_t), \tag{5}$$

and the stochastic term in **Eq. 4** shows that the above-proposed linear relationship is only an approximation.

To start our analysis, we calculated correlation plots for the relationship between the external signals and the squared VWAP price returns. The correlation between squared price returns and volume was calculated for different time lags of the volume time series, as shown in **Figure 3A**. Both have a peak when the external series leads the squared price returns by 1 min. The significant correlation, that is, normalized covariance between squared price returns and trading volume indicates an approximately linear relationship between the volatility and the two proxies for information flow (see **Eq. 3**). The result we got using the bid–ask spread as an external signal can be seen (**Figure 3B**) to be analogous to the one obtained for volume.

In Appendix, we plot the same correlation calculation for cryptocurrency-related tweets (see **Figure A2A**). We do not observe a similar correlation (covariance) pattern as for volume and bid–ask spread signals. Multiple reasons could be behind this: 1) a large noise in the Twitter signal might be covering the information flow w.r.t. trading volume signal, 2) linear dependence might not be enough to capture the relationship, or 3) Twitter signal might not contain a sufficient information flow to influence price volatility. If noise is i.i.d., then "integrated external signal" $\tilde{I}(t) = \int_{t-\delta}^{t} I_t dt$ should filter the noise component. We observe that the stronger correlation pattern is present after the Twitter series is integrated with $\delta = 30$ min (see **Appendix Figure A2B**), which indicates that strong noise is present in Twitter series.

4 TRANSFER ENTROPY BETWEEN INFORMATION FLOW AND VOLATILITY PROXY

To proceed, we move from the linear dependence that is captured with correlation $\rho(r_t^2, v_t)$ to check the nonlinear dependence argument between the squared returns and external information flow I_t signals (volume, bid–ask spread, and Twitter) in causal setting $r_t^2 = f(I_{t-1}, r_{t-1})$. In particular, for the squared price return process $\{r_t^2\}$ and external information proxy process $\{I_t\}$, we calculate transfer entropy (TE) [38].

$$TE_{I \to r^2} := H\left(r_{t+1}^2 \middle| r_t^2\right) - H\left(r_{t+1}^2 \middle| r_t^2, I_t\right), \tag{6}$$

where $H(X|Y) := -\sum_{i,j} p(x_i, y_j) \log[p(x_i|y_j)]$ denotes the conditional Shannon entropy. Transfer entropy is an information-theoretic measure that is both nonlinear and nonsymmetric, and it does not require a Gaussian assumption for the time series [39]. The nonsymmetry allows us to distinguish the direction of information exchange between time series, I_t and r_t^2. In **Figure 4**, we present the results for transfer entropy from external variables to squared returns time series and conversely. The stationarity of the series was checked using the ADF test and the hypothesis of the unit root was rejected at a 1% significance. Results of the transfer entropy analysis show that values are significant, with the largest one being the transfer entropy from squared returns to trading volume. The statistical significance (p-value) of transfer entropy was estimated by a bootstrap method of the underlying Markov process [40]. To account for the finite sample size, we use the effective transfer entropy (ETE) measure:

$$ETE_{I \to r^2} = T_{I \to r^2} - \frac{1}{M} \sum_{m=1}^{M} T_{I_{(m)} \to r^2}, \tag{7}$$

where $I_{(m)}$ is the mth shuffled series of I [41]. We observe a stronger information transfer from the volume signal and the bid–ask spread to squared returns than from the Twitter signal to squared returns. At this point, we conclude that all external signals show significant dependence toward the proxy for volatility signal, that is, squared returns.

5 GENERALIZED AUTOREGRESSIVE CONDITIONAL HETEROSCEDASTICITY WITH EXTERNAL INFORMATION FLOW

Using the transfer entropy analysis, we have found statistically significant dependence between historical information proxy and volatility proxy, but not the actual functional dependence. Therefore, we now turn to the class of generalized autoregressive conditional heteroscedasticity models [6] that will describe the price return process and augment it with the external information flow proxy signal.

The GARCH(1,1) model conditions the volatility on its previous value and the previous value of price returns:

$$r_t = \mu_t + \varepsilon_t, \quad \varepsilon_t = \sigma_t z_t, \quad z_t \in N(0,1). \tag{8}$$

$$\sigma_t^2 = \omega + \alpha \varepsilon_{t-1}^2 + \beta \sigma_{t-1}^2. \tag{9}$$

Large α coefficient indicates that the volatility reacts intensely to market movements, while large β shows that the impact of large volatilities slowly dies out. The volatilities defined by the model display volatility clustering and the respective distribution of price returns are leptokurtic, which agrees with the observations in the real data.

Motivated by MDH and TE analysis, we formed a GARCHX model by adding the proxy for the information flow I_{t-1} directly to the GARCH volatility equation:

$$\sigma_t^2 = \omega + \alpha \varepsilon_{t-1}^2 + \beta \sigma_{t-1}^2 + \gamma I_{t-1}. \tag{10}$$

We will compare price volatility predictions of GARCH(1,1) with those of GARCHX (1, 1) to explore how information is absorbed into the emerging cryptocurrency market of Bitcoin.

5.1 Volatility GARCHX Process analysis

We turn our attention to the statistical quantification of the GARCH volatility processes. For fitting the data to a GARCH process and making out-of-sample estimates, we use the rugarch library [42] in R, available from CRAN (https://cran.r-project.org/). Apart from expanding GARCH(1,1) to GARCHX(1,1), we add the exogenous variable to models eGARCH(1,1), cGARCH(1,1), and TGARCH(1,1) as well, to check for improvement in volatility predictions. The conditional

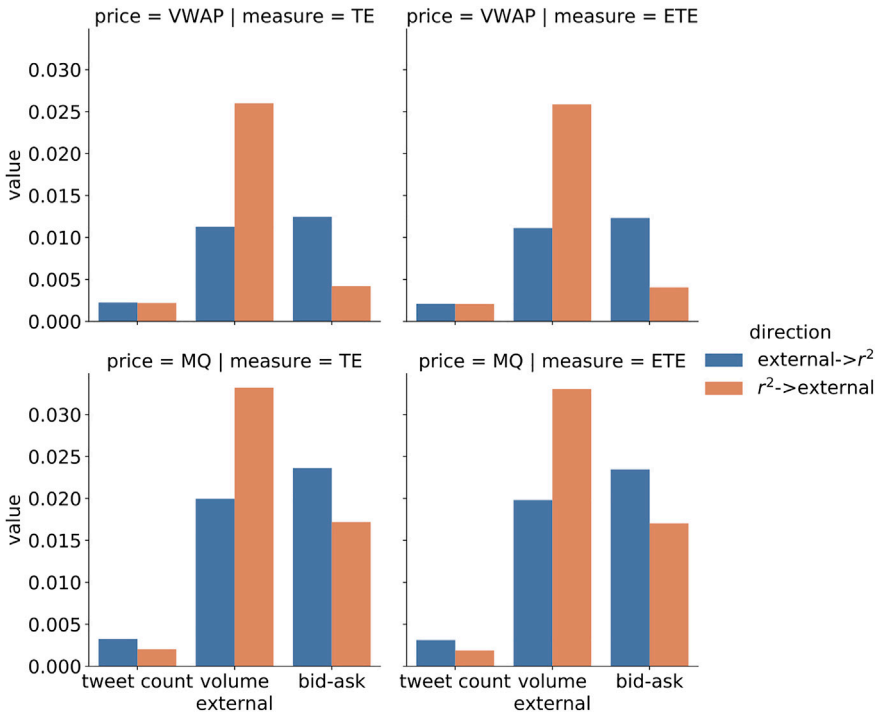


FIGURE 4 | Transfer entropy (TE) and effective transfer entropy (ETE) between external signals (Twitter, volume, and bid–ask spread) and squared returns (VWAP and mid-quote price returns). All transfer entropy results are statistically significant (p-value smaller than 0.001), additionally the presence of unit-roots was checked with augmented Dickey–Fuller test ($\alpha = 0.01$).

TABLE 1 | GARCH family.

eGARCH
$\ln(\sigma_t^2) = \omega + \alpha\left[\left\lvert\frac{\varepsilon_{t-1}}{\sigma_{t-1}}\right\rvert - E\left\lvert\frac{\varepsilon_{t-1}}{\sigma_{t-1}}\right\rvert\right] + \delta\frac{\varepsilon_{t-1}}{\sigma_{t-1}} + \beta\ln(\sigma_{t-1}^2)$
cGARCH
$\sigma_t^2 = q_t + \alpha(\varepsilon_{t-1}^2 - q_{t-1}) + \beta(\sigma_{t-1}^2 - q_{t-1})$ $q_t = \omega + \rho q_{t-1} + \theta(\varepsilon_{t-1}^2 - \sigma_{t-1}^2)$
TGARCH
$\sigma_t = \omega + \alpha\varepsilon_{t-1} + \beta\sigma_{t-1} + \phi\varepsilon_{t-1}1_{[\varepsilon_{t-1}<0]}$

variance equations corresponding to these models (see **Table 1**) are extensions of **Eq. 5**. eGARCH [43] and TGARCH [44] capture the asymmetry between positive and negative shocks, giving a greater weight to the later ones, with the difference between them being the multiplicative and the additive contribution of historical values, and cGARCH [45] separates long- and short-run volatility components.

To get the intuition on how good the GARCH volatility models are at explaining the volatility, we regress $a \cdot \sigma_t^2 + b$ on squared returns r_t^2 [46], where σ_t^2 is the squared GARCH volatility estimate (out-of-sample). Then, we measure the coefficient of determination R^2, that is, the proportion of the variance in the dependent variable that is predictable from the independent variable. We determine the statistical significance of with the F-test. Additionally, we measure the Pearson correlation coefficient (PCC) of estimated σ_t^2 and squared returns r_t^2, along with its statistical significance, **Figure 5**.

However, for a more precise statistical quantification of the difference between models and their GARCHX variants, more advanced statistical tests are needed. For that purpose, we employ predictive negative log-likelihood (NLLH) [47].

$$\begin{aligned}\tilde{\mathcal{L}} &= -\ln\left(\mathcal{L}\left(\mu_1, \ldots, \mu_n, \sigma_1, \ldots, \sigma_n\right)\right) \\ &= -\sum_{i=1}^{n}\left(\frac{1}{2}\ln(\sigma_i) + \frac{1}{2}\ln(2\pi) - \frac{(r_i - \mu_i)^2}{2\sigma_i^2}\right).\end{aligned} \tag{11}$$

We evaluated predictive negative log-likelihood (NLLH) on the out-of-sample period. Values of $\{\mu_i\}_{i=1}^n$ and $\{\sigma_i\}_{i=1}^n$ are predictions

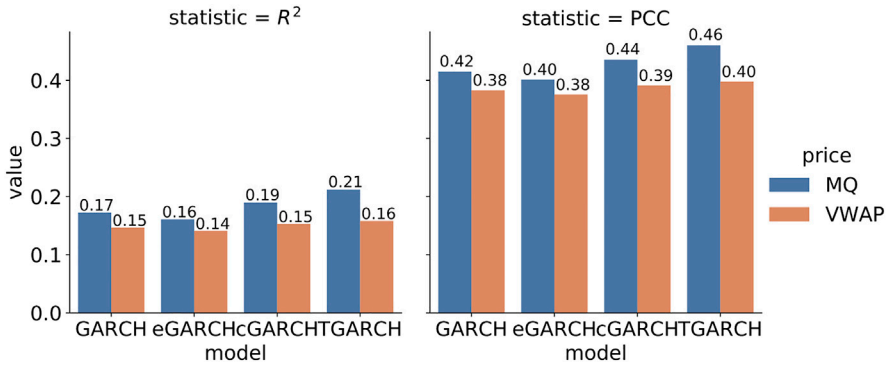


FIGURE 5 | Out-of-sample measures for the GARCH volatility process. In-sample consists of 50,000 points and out-of-sample consists of 8000 points. All PCC values are statistically significant. R^2 statistical significance was checked using F-statistic, and satisfied for all the values.

of the model, and $\{r_i\}_{i=1}^{n}$ is the observed price returns. To show whether the improvements can be considered significant, we employed the likelihood ratio test. It takes the natural logarithm of the ratio of two log-likelihoods as the statistic:

$$LR = -2\ln\left(\frac{\mathcal{L}(\theta_0)}{\mathcal{L}(\theta)}\right). \tag{12}$$

Since its asymptotic distribution is χ^2-distribution, a p-value is obtained using Pearson's chi-squared test. In **Figure 6**, we see from the p-values that the exogenous variables improve the NLLH significantly for all the models except for eGARCH, for logarithmic returns are created from VWAP. When mid-quote prices are used, a significant improvement is observed only for GARCH and cGARCH.

Note, that for two models with fixed parameters, the likelihood ratio test is the most powerful test at given significance level α, by Neyman–Pearson lemma.

In order to further test the robustness of the conclusions on different samples, we perform the bootstrapping. We restrict the lengths of in-sample and out-of-sample to $T = 1000$ points each and sample $N = 100$ such blocks with replacement from the original time series. Then, for each block, we fit a model on its in-sample data segment and calculate predictive out-of-sample NLLH $\{\tilde{\mathcal{L}}_i\}_{i=1}^{N}$.

In **Eq. 11**, M_i represents a model from the GARCH family {GARCH, cGARCH, eGARCH, and TGARCH} and $M_{i,j}$ denotes its corresponding GARCHX extension, where external signal $j \in$ {Volume, Twitter, Bid–ask spread}. Models M_i and $M_{i,j}$ will have empirical distribution functions $\psi_{M_i}(\tilde{\mathcal{L}})$ and $\psi_{M_{i,j}}(\tilde{\mathcal{L}})$, respectively (see boxplots estimates in **Figure 7**). We calculate the Kolmogorov–Smirnov (KS) statistics between corresponding empirical predictive out-of-sample NLLH distributions:

$$KS_{i,j} = \sup_{\tilde{\mathcal{L}}} \left|\psi_{M_i}(\tilde{\mathcal{L}}) - \psi_{M_{i,j}}(\tilde{\mathcal{L}})\right|, \tag{13}$$

and obtain its statistical significance. In **Figures 7**, **8**, we can see that both GARCH and cGARCH models show significant improvements with all the external variables and both price definitions, under the bootstrapping KS-NLLH robustness check. That is not surprising, as the nonparametric KS test is not very powerful [48]. However, significant differences for the GARCH and cGARCH models allow us to confirm that its predictive power is robust under temporal bootstrapping conditions. Finally, we take the GARCH volatility process as a

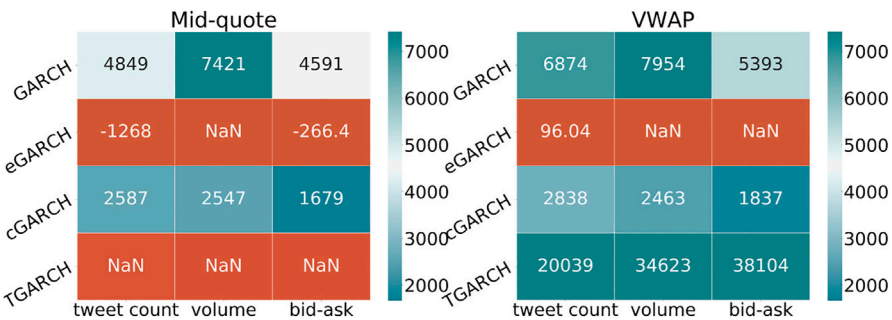


FIGURE 6 | Results of out-of-sample likelihood ratio test. In-sample consists of 50,000 points and out-of-sample consists of 8,000 points. *Blue palette represents the p-value smaller than 0.001. NaN—some algorithms had convergence problems.

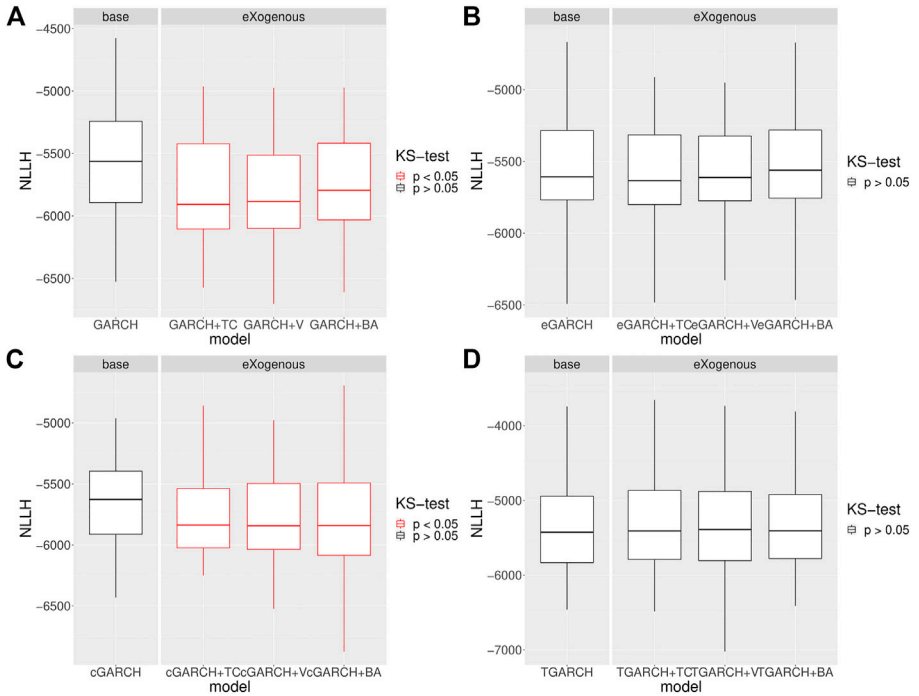


FIGURE 7 | Bootstrap robustness check over $N = 100$ splitting points with $T = 1{,}000$ training points and $T = 1{,}000$ test size for GARCH and GARCHX models. The price is defined as volume-weighted. The nonparametric Kolmogorov–Smirnov test of the equality of the NLLH out-of-sample distributions between the GARCH and GARCHX models is done. **(A)** KS test implies a significant difference for both external signals for the GARCH model. **(B)** KS test implies no significant difference for external signals for the eGARCH model. **(C)** KS test implies no significant difference for both external signals for the cGARCH model. **(D)** KS test implies no significant difference for external signals for the TGARCH model.

representative and perform additional bootstrapping KS–NLLH robustness checks on two additional segments (March–April 2019 and November–December 2019) and we see similar results (See **Appendix Figure A3**).

6 DISCUSSION

Although the theoretical foundations of the effects of information on markets have been proposed a long time ago [1, 2], they were further developed in 1970, as "weak", "semi-strong", and "strong" forms of efficient market hypothesis [49]. The mathematical models of information effects continued to advance in the 70s as well, by the proposition of the Mixture of Distribution Hypothesis [4], which states that the dynamics of price returns are governed by the information flow available to the traders. Following the growth of computerized systems and the availability of empirical data in the 80s, more elaborate statistical models were proposed, such as generalized autoregressive conditional heteroscedasticity models (GARCH) [6] and news Poisson-jump processes [7] with constant intensity. Furthermore, studies from the 2000s generalized the news Poisson-jump processes by introducing time-varying jump effects, supporting it with the statistical evidence of time variation in the jump size distribution [8, 9].

In this article, we have analyzed the effects of information flow on the cryptocurrency Bitcoin exchange market that appeared with the introduction of blockchain technology in 2008 [11]. Although the trading volume in the largest cryptocurrency markets has grown exponentially in the last 10 years, still the research on their (in)efficiency quantification is ongoing [50, 51]. We have focused on the Bitcoin, the largest cryptocurrency w.r.t. market capitalization, and used the reliable data of price returns and traded volume and bid–ask spread from Bitfinex exchange market [52] on a minute-level granularity. The price returns were calculated using two different definitions, VWAP and mid-quote, to account for possible market-microstructure noise. Another reason, why we have concentrated on the Bitcoin, was the availability of Twitter-related data [36]. We have used the social media signals from Twitter, trading volume and bid–ask spread from the Bitcoin market as a proxy for information flow together with the GARCH family of [53] processes to quantify the prediction power for the price volatility.

We started the analysis by employing recently developed nonparametric information-theoretic transfer entropy measures [38, 40, 41], to confirm the nonlinear relationship between the exogenous proxy for information (trading volume, bid–ask spread, and cryptocurrency related tweets) and squared price returns (proxy for volatility). Further on, we have made extensive experiments on the following models: GARCH, eGARCH,

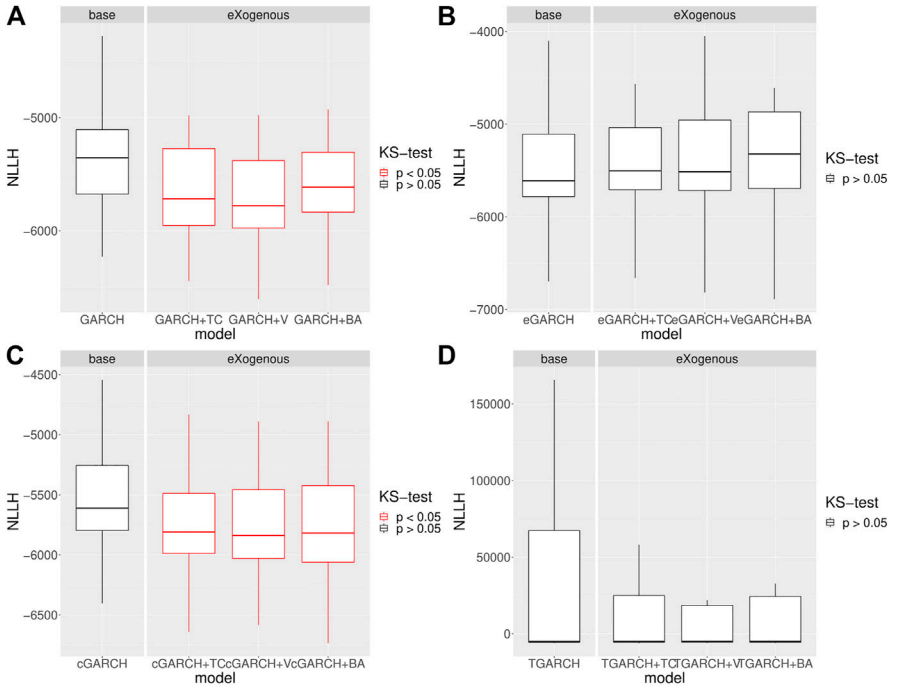


FIGURE 8 | Bootstrap robustness check over $N = 100$ splitting points with $T = 1{,}000$ training points and $T = 1{,}000$ test size for GARCH and GARCHX models. The price is defined as mid-quote. The nonparametric Kolmogorov–Smirnov test of the equality of the NLLH out-of-sample distributions between the GARCH and GARCHX models is done. **(A)** KS test implies a significant difference for both external signals for the GARCH model. **(B)** KS test implies no significant difference for external signals for the eGARCH model. **(C)** KS test implies no significant difference for both external signals for the cGARCH model. **(D)** KS test implies no significant difference for external signals for the TGARCH model.

cGARCH, and TGARCH on the minute-level data of price returns, Twitter volume, exchange volume data, and bid–ask spread. Our testing procedure consisted of multi-stage statistical checks: 1) out-of-sample R^2 and Pearson correlation measurements, 2) out-of-sample predictive likelihood measurements with the likelihood ratio test on 8,000 points, and 3) bootstrapped predictive likelihood measurements with the nonparametric Kolmogorov–Smirnov test. From the predictive perspective of the nonlinear parametric GARCH model, we have found that exogenous proxy for information flow significantly improves out-of-sample minute volatility predictions for the GARCH and cGARCH [54] models. It is not surprising that the basic GARCH model is outperforming more advanced models [46, 55] such as eGARCH [43] and TGARCH [44] on out-of-sample data. Also, a previous study [18] found that the cGARCH model on the Bitcoin market was performing the best on in-sample daily returns.

Finally, we have taken the GARCH model and applied the bootstrapping on two additional segments (March–April 2019 with 38,000 points and November–December 2019 with 52,000 points) and we observe that our observations still hold (see **Appendix Figure A3**). For future work, we leave focusing on other cryptocurrencies and analyzing the cross-market volatility spillovers, in which different market behavior modes could be studied separately.

DATA AVAILABILITY STATEMENT

For accessing the data please contact the corresponding author at anino@ethz.ch.

AUTHOR CONTRIBUTIONS

IB performed experiments, NA-F supervised the research, and both authors analyzed the results and wrote the manuscript.

FUNDING

NA-F acknowledges financial support from SoBigData++ through Grant Agreement No. 871042. IB acknowledges the SoBigData TransNational Access research visit and partial support form QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund-the Competitiveness and Cohesion Operational Program (Grant KK.01.1.1.01.0004, elementleader N.P.).

ACKNOWLEDGMENTS

We would like to thank Tian Guo and Fabrizio Lillo for helpful discussions.

REFERENCES

1. Bachelier L. *Louis Bachelier's Theory of Speculation: The Origins of Modern Finance*. New Jersey: Princeton University Press (2011). doi:10.1515/9781400829309
2. Mandelbrot B. The Variation of Certain Speculative Prices. *J Bus* (1963) 36(4): 394–419. doi:10.1086/294632
3. Stanley H, and Mantegna R. *An Introduction to Econophysics*. Cambridge: Cambridge University Press (2000).
4. Clark PK. A Subordinated Stochastic Process Model with Finite Variance for Speculative Prices. *Econometrica* (1973) 41(1):135. doi:10.2307/1913889
5. Engle RF. Autoregressive Conditional Heteroscedasticity with Estimates of the Variance of United Kingdom Inflation. *Econometrica* (1982) 50:987–1007. doi:10.2307/1912773
6. Bollerslev T. Generalized Autoregressive Conditional Heteroskedasticity. *J Econom* (1986) 31(3):307–27. doi:10.1016/0304-4076(86)90063-1
7. Jorion P. On Jump Processes in the Foreign Exchange and Stock Markets. *Rev Financ Stud* (1988) 1(4):427–45. doi:10.1093/rfs/1.4.427
8. Chan WH, and Maheu JM. Conditional Jump Dynamics in Stock Market Returns. *J Business Econ Stat* (2002) 20(3):377–89. doi:10.1198/073500102288618513
9. Maheu JM, and McCurdy TH. News Arrival, Jump Dynamics, and Volatility Components for Individual Stock Returns. *J Finance* (2004) 59(2):755–93. doi:10.1111/j.1540-6261.2004.00648.x
10. Chuen D. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Amsterdam: Academic Press (2015). doi:10.1016/C2014-0-01905-3
11. Nakamoto S. *Bitcoin: A Peer-To-Peer Electronic Cash System* (2008). https://bitcoin.org/bitcoin.pdf
12. Gandal N, Hamrick J, Moore T, and Oberman T. Price Manipulation in the Bitcoin Ecosystem (2017). CEPR Discussion Papers 12061.
13. Ciaian P, Rajcaniova M, and Kancs d. A. The Economics of Bitcoin Price Formation. *Appl Econ* (2016) 48:1799–815. doi:10.1080/00036846.2015.1109038
14. Cheah E-T, and Fry J. Speculative Bubbles in Bitcoin Markets? an Empirical Investigation into the Fundamental Value of Bitcoin. *Econ Lett* (2015) 130: 32–6. doi:10.1016/j.econlet.2015.02.029
15. Kristoufek La. What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis. *PloS one* (2015) 10(4):e0123923. doi:10.1371/journal.pone.0123923
16. Donier J, and Bouchaud J-P. Why Do Markets Crash? Bitcoin Data Offers Unprecedented Insights. *PLOS ONE* (2015) 10:1–11. doi:10.1371/journal.pone.0139356
17. Wheatley S, Sornette D, Huber T, Reppen M, and Gantner RN. Are Bitcoin Bubbles Predictable? Combining a Generalized Metcalfe's Law and the Lppls Model (March 15, 2018). Swiss Finance Institute Research Paper. Available at SSRN: https://ssrn.com/abstract=3141050 or http://dx.doi.org/10.2139/ssrn.3141050.
18. Katsiampa P. Volatility Estimation for Bitcoin: A Comparison of GARCH Models. *Econ Lett* (2017) 158:3–6. doi:10.1016/j.econlet.2017.06.023
19. Guo T, Bifet A, and Antulov-Fantulin N. "Bitcoin Volatility Forecasting with a Glimpse into Buy and Sell Orders," in 2018. *IEEE Int Conf Data Mining (Icdm) Nov* (2018) 989–94. doi:10.1109/ICDM.2018.00123
20. Ron D, and Shamir A. Quantitative Analysis of the Full Bitcoin Transaction Graph. In: *International Conference On Financial Cryptography And Data Security*. Springer (2013). p. 6–24. doi:10.1007/978-3-642-39884-1_2
21. ElBahrawy A, Alessandretti L, Kandler A, Pastor-Satorras R, and Baronchelli A. Evolutionary Dynamics of the Cryptocurrency Market, R. Soc. Open Sci. *R Soc Open Sci* (2017) 4(11):170623. doi:10.1098/rsos.170623
22. Antulov-Fantulin N, Tolic D, Piskorec M, Ce Z, and Vodenska I. Inferring Short-Term Volatility Indicators from the Bitcoin Blockchain. In: *Complex Networks And Their Applications VII*. Cham: Springer International Publishing (2019). p. 508–20. doi:10.1007/978-3-030-05414-4_41
23. Hayes A, "Cryptocurrency Value Formation: An Empirical Analysis Leading to a Cost of Production Model for Valuing Bitcoin."(2015). Telematics and Informatics, Forthcoming, Available at SSRN: https://ssrn.com/abstract=2648366,
24. Bolt W. On the Value of Virtual Currencies. De Nederlandsche Bank Working Paper No. 521 (2016). Available at SSRN: https://ssrn.com/abstract=2842557.
25. Nadarajah S, and Chu J. On the Inefficiency of Bitcoin. *Econ Lett* (2017) 150: 6–9. doi:10.1016/j.econlet.2016.10.033
26. Kristoufek L. Bitcoin Meets Google Trends and Wikipedia: Quantifying the Relationship between Phenomena of the Internet Era. *Scientific Rep* (2013) 3: 3415. doi:10.1038/srep03415
27. Li TR, Chamrajnagar AS, Fong XR, Rizik NR, and Fu F. Sentiment-based Prediction of Alternative Cryptocurrency Price Fluctuations Using Gradient Boosting Tree Model (2018). Papers 1805.00558, arXiv.org.
28. Kim YB, Kim JG, Kim W, Im JH, Kim TH, Kang SJ, et al.Predicting Fluctuations in Cryptocurrency Transactions Based on User Comments and Replies. *PloS one* (2016) 11. doi:10.1371/journal.pone.0161197
29. Garcia D, and Schweitzer F. Social Signals and Algorithmic Trading of Bitcoin. *R Soc Open Sci* (2015) 2(9):150288. doi:10.1098/rsos.150288
30. Dey AK, Akcora CG, Gel YR, and Kantarcioglu M. On the Role of Local Blockchain Network Features in Cryptocurrency Price Formation. *Can J Stat* (2020) 48(3):561–81. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/cjs.11547. doi:10.1002/cjs.11547
31. Naimy V, Haddad O, Fernández-Avilés G, and El Khoury R. The Predictive Capacity of Garch-type Models in Measuring the Volatility of Crypto and World Currencies. *PLOS ONE* (2021) 16(1):e0245904–17. doi:10.1371/journal.pone.0245904
32. Chu J, Chan S, Nadarajah S, and Osterrieder J. Garch Modelling of Cryptocurrencies. *J Risk Financial Manag* (2017) 10(4). [Online]. Available: https://www.mdpi.com/1911-8074/10/4/17. doi:10.3390/jrfm10040017
33. Shen D, Urquhart A, and Wang P. Does Twitter Predict Bitcoin? *Econ Lett* (2019) 174:118–22. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0165176518304634. doi:10.1016/j.econlet.2018.11.007
34. Gao X, Huang W, and Wang H. Financial Twitter Sentiment on Bitcoin Return and High-Frequency Volatility. *Virtual Econ* (2021) 4(1):7–18. Jan. [Online]. Available: https://www.virtual-economics.eu/index.php/VE/article/view/101. doi:10.34021/ve.2021.04.01(1)
35. Gatheral J, and Oomen RCA. Zero-intelligence Realized Variance Estimation. *Finance Stoch* (2010) 14(2):249–83. [Online]. Available: https://ideas.repec.org/a/spr/finsto/v14y2010i2p249-283.html. doi:10.1007/s00780-009-0120-1
36. Beck J, Huang R, Lindner D, Guo T, Ce Z, Helbing D, et al.Sensing Social Media Signals for Cryptocurrency News. In: *Companion Proceedings Of the 2019 World Wide Web Conference* (2019). p. 1051–4.
37. Tauchen GE, and Pitts M. The Price Variability-Volume Relationship on Speculative Markets. *Econometrica* (1983) 51(2):485–505. doi:10.2307/1912002
38. Schreiber T. Measuring Information Transfer. *Phys Rev Lett* (2000) 85(2): 461–4. doi:10.1103/physrevlett.85.461
39. Barnett L, Barrett AB, and Seth AK. Granger Causality and Transfer Entropy Are Equivalent for Gaussian Variables. *Phys Rev Lett* (2009) 103(23). doi:10.1103/PhysRevLett.103.238701
40. Dimpfl T, and Peter FJ. Using Transfer Entropy to Measure Information Flows between Financial Markets. *Stud Nonlinear Dyn Econom* (2013) 17(1):85–102. doi:10.1515/snde-2012-0044
41. Marschinski R, and Kantz H. Analysing the Information Flow between Financial Time Series. *Eur Phys J B* (2002) 30(2):275–81. doi:10.1140/epjb/e2002-00379-2
42. Ghalanos A, Rugarch: Univariate GARCH Models.,(2020), r package version 1.4-4.
43. Nelson DB. Conditional Heteroskedasticity in Asset Returns: A New Approach. *Econometrica* (1991) 59(2):347–70. doi:10.2307/2938260
44. Zakoian J-M. Threshold Heteroskedastic Models. *J Econ Dyn Control* (1994) 18(5):931–55. doi:10.1016/0165-1889(94)90039-6
45. Lee G, and Engle R. A Permanent and Transitory Component Model of Stock Return Volatility. In: WJ Granger *Cointegration, Causality And Forecasting: A Festschrift In Honor Of Clive* (1999). p. 475–97.
46. Andersen TG, and Bollerslev T. Answering the Skeptics: Yes, Standard Volatility Models Do Provide Accurate Forecasts. *Int Econ Rev* (1998) 39: 885–905. doi:10.2307/2527343
47. Wu Y, Hernández-Lobato JM, and Ghahramani Z. Gaussian Process Volatility Model. In: *NIPS* (2014). p. 1044–52.
48. Marozzi M. Nonparametric Simultaneous Tests for Location and Scale Testing: A Comparison of Several Methods. *Commun Stat - Simulation Comput* (2013) 42(6):1298–317. doi:10.1080/03610918.2012.665546
49. Fama EF. Efficient Capital Markets: A Review of Theory and Empirical Work. *J Finance* (1970) 25(2):383. doi:10.2307/2325486

50. Tran VL, and Leirvik T. Efficiency in the Markets of Crypto-Currencies, *Finance Res Lett*, 35 (2019). p. 101382. doi:10.1016/j.frl.2019.101382
51. Kristoufek L, and Vosvrda M. Cryptocurrencies Market Efficiency Ranking: Not So Straightforward. *Physica A: Stat Mech its Appl* (2019) 531:120853. doi:10.1016/j.physa.2019.04.089
52. Hougan M, Kim H, Lerner M, and Management BA. "*Economic and Non-economic Trading in Bitcoin: Exploring the Real Spot Market for the World's First Digital Commodity*. Bitwise Asset Management (2019). https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5574233-185408.pdf
53. Engle R. New Frontiers for Arch Models. *J Appl Econ* (2002) 17(5):425–46. doi:10.1002/jae.683
54. Engle RF, and Sokalska ME. Forecasting Intraday Volatility in the Us Equity Market. Multiplicative Component Garch. *J Financial Econom* (2012) 10(1): 54–83. doi:10.1093/jjfinec/nbr005
55. Jafari GR, Bahraminasab A, and Norouzzadeh P. Why Does the Standard Garch(1, 1) Model Work Well? *Int J Mod Phys C* (2007) 18(07):1223–30. doi:10.1142/s0129183107011261

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

APPENDIX

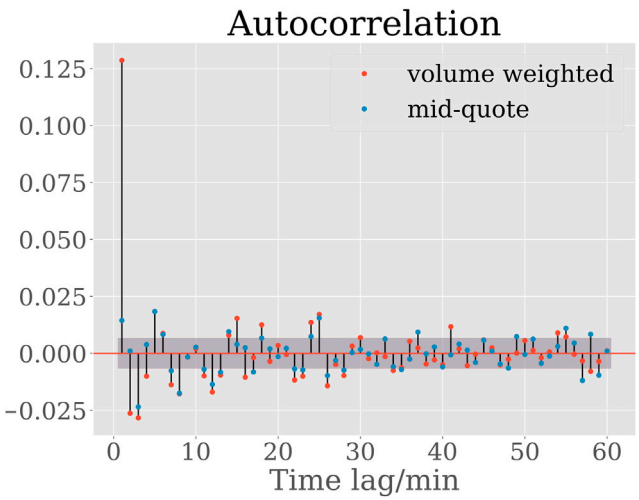


FIGURE A1 | Autocorrelation of price returns. The first-order autocorrelation of mid-quote price returns is significantly smaller than that of volume-weighted price returns, indicating a smaller level of microstructure noise in mid-quote price returns. Confidence interval.

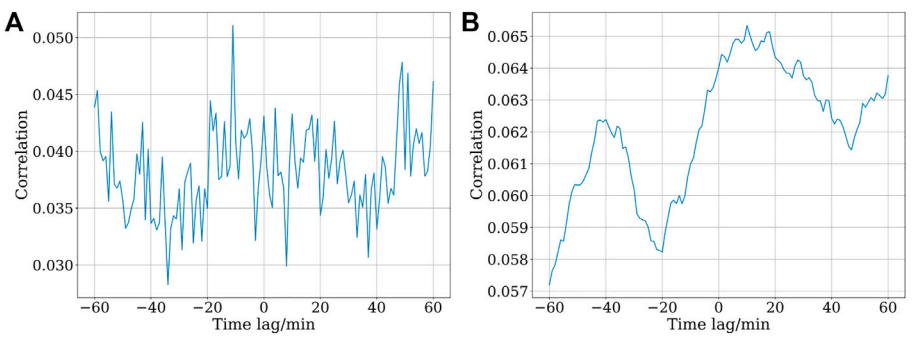


FIGURE A2 | (A) Correlation between squared price returns and Twitter volume. Permutation significance check indicates no statistically significant correlation between time-permuted squared price returns and Twitter time series. **(B)** Correlation between squared price returns and integrated Twitter volume (over a 30-min moving window). This test is only used to check whether the integrating operator is filtering noise. Correlation between squared price returns and Twitter time series. All values of correlation are statistically significant (p-value ≤ 0.001).

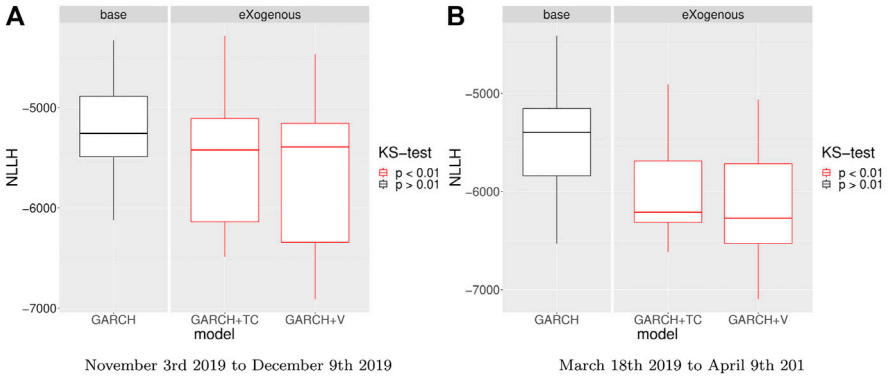


FIGURE A3 | Bootstrap robustness check over $N = 100$ splitting points with $T = 1000$ training points and $T = 1000$ points in test size for GARCH and GARCHX models. The nonparametric Kolmogorov–Smirnov test of the equality of the NLLH out-of-sample distributions between GARCH and GARCHX models is done. **(A)** KS test implies a significant difference for all external signals for the GARCH model in the period from November 3rd, 2019 to December 9th, 2019 with 52,000 observations. **(B)** KS test implies a significant difference for all external signals for the GARCH model in the period from March 18th, 2019, to April 9th, 2019, with 38,000 observations.

frontiers in Physics

ORIGINAL RESEARCH
published: 30 June 2021
doi: 10.3389/fphy.2021.681798

The Complex Community Structure of the Bitcoin Address Correspondence Network

Jan Alexander Fischer[1†], *Andres Palechor*[1†], *Daniele Dell'Aglio*[2,3*], *Abraham Bernstein*[3] *and Claudio J. Tessone*[4]

[1]Faculty of Business, Economics and Informatics, Universität Zürich, Zürich, Switzerland, [2]Department of Computer Science, Aalborg University, Aalborg, Denmark, [3]Department of Informatics, Universität Zürich, Zürich, Switzerland, [4]UZH Blockchain Center and URPP Social Networks, Universität Zürich, Zürich, Switzerland

Bitcoin is built on a blockchain, an immutable decentralized ledger that allows entities (users) to exchange Bitcoins in a pseudonymous manner. Bitcoins are associated with alpha-numeric addresses and are transferred *via* transactions. Each transaction is composed of a set of input addresses (associated with unspent outputs received from previous transactions) and a set of output addresses (to which Bitcoins are transferred). Despite Bitcoin was designed with anonymity in mind, different heuristic approaches exist to detect which addresses in a specific transaction belong to the same entity. By applying these heuristics, we build an Address Correspondence Network: in this representation, addresses are nodes are connected with edges if at least one heuristic detects them as belonging to the same entity. In this paper, we analyze for the first time the Address Correspondence Network and show it is characterized by a complex topology, signaled by a broad, skewed degree distribution and a power-law component size distribution. Using a large-scale dataset of addresses for which the controlling entities are known, we show that a combination of external data coupled with standard community detection algorithms can reliably identify entities. The complex nature of the Address Correspondence Network reveals that usage patterns of individual entities create statistical regularities; and that these regularities can be leveraged to more accurately identify entities and gain a deeper understanding of the Bitcoin economy as a whole.

Keywords: blockchain technology, bitcoin (BTC), label propagarion algorithm, network science, deanonymization

OPEN ACCESS

Edited by:
Zhong-Yuan Zhang,
Central University of Finance and Economics, China

Reviewed by:
Ju Xiang,
Changsha Medical University, China
Jie Cao,
Nanjing University of Finance and Economics, China

***Correspondence:**
Daniele Dell'Aglio
dade@cs.aau.dk

[†]*These authors have contributed equally to this work*

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *17 March 2021*
Accepted: *10 June 2021*
Published: *30 June 2021*

Citation:
Fischer JA, Palechor A, Dell'Aglio D, Bernstein A and Tessone CJ (2021) The Complex Community Structure of the Bitcoin Address Correspondence Network. Front. Phys. 9:681798. doi: 10.3389/fphy.2021.681798

1 INTRODUCTION

Cryptocurrencies are rapidly growing in interest, becoming a popular mechanism to perform pseudonymous exchanges between users (entities). They also allow payments in a decentralized manner without needing a trusted third party. The first and most popular cryptocurrency is Bitcoin, which uses an immutable and publicly available ledger to facilitate transactions between entities. Moreover, given its pseudo-anonymity, Bitcoin has also been used to perform activities in illegal markets. For example, Foley et al. [1] estimate that one-quarter of entities in the Bitcoin network are associated with illegal activity. Consequently, several governing challenges have arisen, and law enforcement agents are particularly interested in techniques that allow tracing the origin of funds. Specifically, in Bitcoin, given the ledger's public nature, tracing the funds can be achieved by inspecting the history of transactions in the system. However, identifying the entities is a complex

task because they can use different pseudonyms (addresses) in the system. By the Bitcoin protocol, it is impossible to completely de-anonymize the entities; however, not all entities prioritize anonymity [2], and it is possible to find recoverable traces of their activity in the transaction history.

The structure of the transactions allows, in some cases, tracing back address pseudonyms that potentially belong to the same entity. For example, Meiklejohn et al. [3] apply heuristics and then cluster together pseudonyms based on evidence of shared spending authority. In this paper, we study the application of several heuristics that leads to creating a sequence of Address Correspondence Networks. Each of these networks includes weighted links between addresses that potentially belong to the same entity, thus approaching entity identification from a network science perspective. Even though other approaches use networks to model some parts of the Bitcoin economic dynamics (e.g. [4–7]), to the best of our knowledge, network science approaches have not addressed the problem of analyzing the Address Correspondence Network to date. In this study, we show that the Address Correspondence Networks have a strong community structure and general-purpose clustering approaches are suitable for analyzing them. Furthermore, our experiments suggest that having a set of identified entities generates large gains in cluster quality—however, this gain quickly declines, and a small number of known entities is enough to produce significant increase in the quality of the detection.

The rest of this paper is organized as follows: **Section 2** explains the basics of the Bitcoin blockchain, heuristics, entity identification and related work. **Section 3** presents our methods for constructing Address Correspondence Networks, the clustering technique and its quality metrics. In **Section 4**, we discuss our findings, and finally, in **Section 5**, we discuss conclusion and future work.

2 BACKGROUND AND RELATED WORK

This section introduces the main concepts related to Bitcoin. Next, it discusses the task of identifying addresses controlled by the same entity, followed by a reviews of the main studies in the area.

2.1 The Bitcoin Blockchain

Bitcoin was introduced in [8] as a decentralized payment network and digital currency which would be independent of central bank authorities. It is built on a blockchain, an immutable decentralized ledger that allows users, i.e. entities, to exchange the units of account (Bitcoins) in a pseudonymous manner. Entities transacting in the Bitcoin network control addresses—unique identifiers which have the right to transfer specific amounts of Bitcoins.

There are different types of addresses, which determine how the associated Bitcoins are accessed. For example, to spend Bitcoins associated with an address of type Pay to Public Key Hash (P2PKH), the entity needs to present a valid signature based on their private key, and a public key that hashes to the P2PKH value. Another example is the Pay to Script Hash (P2SH) address type: it defines a script for custom validation, which may include several signatures, passwords and other user-defined requirements. We denote with a an address and with $\mathcal{A}$ the set of $\{a_1, \ldots, a_n\}$ addresses appearing in the Bitcoin blockchain. Furthermore, we denote an entity as e, with $\mathcal{E}$ representing the set $\{e_1, \ldots, e_k\}$ of entities that own Bitcoin addresses.

To spend or receive Bitcoins, entities create transactions. A transaction t is composed of a set of input addresses, a set of output addresses, and information specifying the amount of Bitcoins to be allocated to each output address. Formally, let $\mathcal{T}$ be the set of transactions stored in the Bitcoin blockchain, and $\mathcal{P}(\mathcal{A})$ be the power set of $\mathcal{A}$. We model with $\mathrm{i} : \mathcal{T} \to \mathcal{P}(\mathcal{A})$ and $\mathrm{o} : \mathcal{T} \to \mathcal{P}(\mathcal{A})$ the mappings between a transaction and its input and output address sets. The sum of Bitcoins associated with the input addresses equals the sum of Bitcoins associated with the output addresses plus transaction fees. Therefore, if an entity wishes to spend only a partial amount of Bitcoins associated with the input addresses, the remainder is typically sent to an existing or newly created change address controlled by the initiating entity. Transaction outputs that have not yet been used as inputs to other transactions are referred to as UTXOs (unspent transaction outputs).

The transaction history is replicated on multiple nodes in the Bitcoin network. Entities broadcast new transactions to other nodes in the network. As part of Bitcoin's decentralized consensus protocol, specialized miner nodes are incentivized to solve proof-of-work puzzles that validate new transactions and group them into blocks. Blocks are sequentially appended to the blockchain; the number of blocks preceding a particular block is known as its block height. Furthermore, entities may specify a transaction's locktime. This is the minimum block height the blockchain must reach before miners should consider validating the transaction, i.e. a transaction with locktime j is added to block $j + 1$ or later.

A peculiar property of the Bitcoin network is the pseudonymity: entities conceal their identity through the use of nameless addresses (pseudonyms), linking an address to a real-world entity exposes their entire activity on the Bitcoin network, since the transaction history is publicly available. Entities are therefore advised to generate a new address for every transaction, so that each address is used once as a transaction output and once as a transaction input.

2.2 Address Clustering

The objective of address clustering is to find sets of addresses $\mathcal{A}_i \subseteq \mathcal{A}$ that are controlled by the same entity e_i. Formally, the objective is to find a map $\mathrm{e} : \mathcal{A} \to \mathcal{E}$ such that $\mathcal{A}_i = \{a_j | \mathrm{e}(a_j) = e_i\}$. There exist multiple heuristics for identifying address pairs controlled by the same entity. We consider seven heuristics implemented by Kalodner et al. [9], the majority of which seek to identify change addresses in the outputs of a transaction (linking these with the transaction inputs).

1) Multi-input: All input addresses of a transaction are assumed to be controlled by the same entity.

2) Change address type: If all input addresses of a transaction are of one address type (e.g. P2PKH or P2SH), the potential change addresses are of the same type.
3) Change address behavior: Since entities are advised to generate a new address for receiving change, an output address receiving Bitcoins for the first time may be a change address.
4) Change locktime: If a transaction's locktime is specified, outputs spent in different transactions on the same block as the specified locktime may be change addresses. Intuitively, this is because the entity initiating the transaction also knows its locktime.
5) Optimal change: If an output is smaller than any of the transaction inputs, it is likely a change address.
6) Peeling chain: In a peeling chain, a single address with a relatively large amount of Bitcoins begins by transferring a small amount of Bitcoins to an output address, with the rest being allocated to a one-time change address. This process repeats several times until the larger amount is reduced, meaning that addresses continuing the chain are potential change addresses Meiklejohn et al. [3].
7) Power of 10: This heuristic assumes that the sum of deliberately transferred Bitcoins in a transaction is a power of 10. If such an output is present, the other outputs may be change addresses.

2.3 Related Work

Address clustering in Bitcoin has been the subject of numerous studies. Initial studies focused on the multi-input heuristic. For example, Nick [10] identify more than 69% vulnerable addresses using only this heuristic. Also Harrigan and Fretter [11] consider the multi-input heuristic and attribute its effectiveness to frequent address reuse, as well as the presence of large address clusters having high centrality measures with respect to transactions between clusters. Furthermore, they suggest that incremental cluster growth and the avoidable merging of large clusters makes the multi-input heuristic suitable for real-time analysis. Fleder et al. [12] construct directed transaction graphs for periods of 24 h and 7 months. In such graphs, the nodes are addresses and each edge represents a transaction from an input address to an output address. They obtain address entity labels by scraping public forums and social networks. By applying the multi-input heuristic, they identify transactions where labeled addresses have interacted with a large number of known entities such as SatoshiDICE and Wikileaks.

Meiklejohn et al. [3] combines the multi-input heuristic with a second one, similar to the change address behavior heuristic. They identify major entities and interactions between them, and note that the change address heuristic tends to collapse address groups into large super-clusters. Zhang et al. [13] consider another variation of the change address behavior heuristic, and show that it improves clustering quality when address reduction is used as a performance measure. In this study, we focus on the heuristics introduced in Section 2.2 by Kalodner et al. [9].

Patel [14] proposes novel approaches to Bitcoin address clustering. He considers clustering an undirected, weighted heuristic graph, where the nodes are addresses, and each edge indicates the presence of at least one of eight heuristics (a superset of those introduced in Section 2.2) linking those addresses to the same entity. Each heuristic is assigned a positive weight, such that their sum is equal to one. The edge weight is the sum of the heuristic weights for which the corresponding heuristic is present between two addresses. The author applies a variety of generic graph clustering algorithms (e.g. k-means, spectral, DBSCAN) as well as graph sparsification and coarsening techniques to the constructed heuristic graph. In this study, we propose the address correspondence network, which is similar to the network built by Patel [14] However, in our correspondence network, an edge between two addresses represents the number of times the heuristics identify the pair as controlled by the same entity. We use a label propagation algorithm to build the clusters, using ground truth information to drive the algorithm.

There exist other approaches and extensions to address clustering. Ermilov et al. [15] show that higher cluster homogeneity can be achieved when transaction data is augmented with off-chain information from the internet. Biryukov and Tikhomirov [16] propose incorporating lower-level network information to enhance deanonymization. Furthermore, Harlev et al. [17] extend address clustering by using supervised machine learning to predict the type of entity controlling addresses in an unlabeled cluster. In our study, in addition to using a ground truth to guide the clustering construction, we introduce a temporal component in the analysis. We build address correspondence networks for various time intervals. In this way, we can analyze the evolution of the network over time.

3 METHODOLOGY

We expand upon the work of Patel [14] by performing address clustering on so-called Address Correspondence Networks, denoted $\mathcal{G}_{[o,c]}$, where $[o, c]$ is a time interval. Nodes are Bitcoin addresses that are involved in transactions between a time instant o and a time instant c. $\mathcal{G}_{[o,c]}$ contains an undirected link (a_i, a_j) between two addresses when at least one of the heuristics introduced in Section 2.2 detects a_i and a_j as belonging to the same entity. We posit that the topology of $\mathcal{G}_{[o,c]}$ encodes further insights on the identity of the entities and, ultimately, on the $\mathrm{e}(a_j)$ map.

For some addresses a_j, the controlling entity is known. Using the block explorer tool provided by Janda [18], we obtain entity labels for 28 million addresses involved in transactions before 2017. We refer to this data set as the ground truth. The mapping information contained in the ground truth is denoted with $\mathrm{e}^{\star}$, such that $\mathcal{A}^{\star} = \{a_j | \exists \mathrm{e}^{\star}(a_j)\} \subseteq \mathcal{A}$ is the set of addresses for which the entity label is known. We use the ground truth to 1) sample from $\mathcal{T}$ and 2) to evaluate the quality of address clustering methods.

The remainder of this section is organized as follows. Section 3.1 describes the method for sampling from $\mathcal{T}$. This sample is divided further into cumulative and partial subsets, which are described in Section 3.2. Section 3.3 details the construction of the

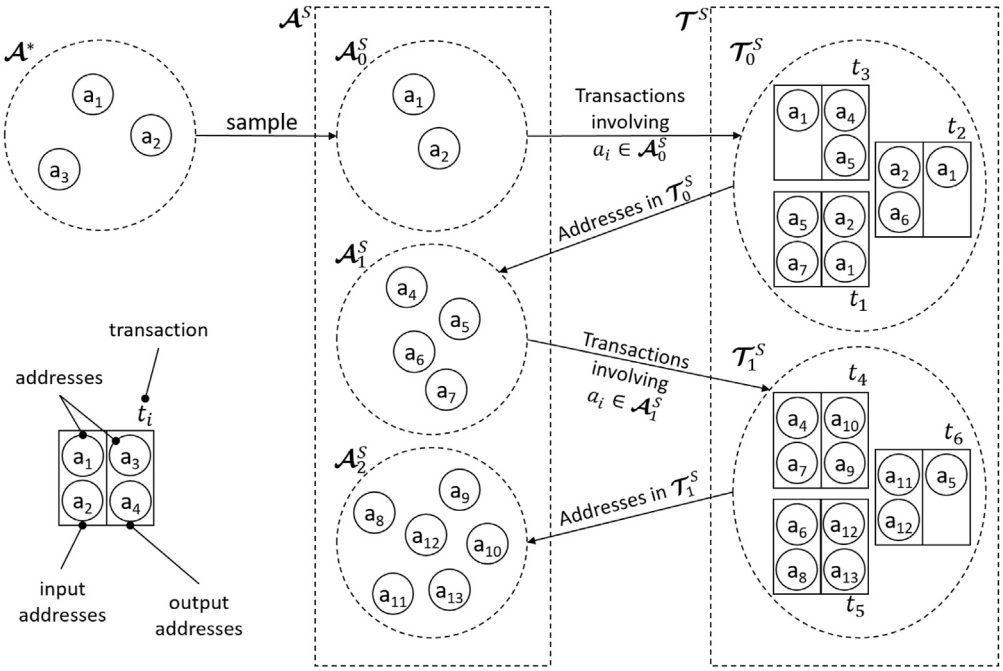


FIGURE 1 | The transaction sampling process.

Address Correspondence Networks. We explain our approach to clustering these networks in Section 3.4, while the metrics used to evaluate clustering quality are introduced in Section 3.5.

3.1 Transaction Sampling

For computational feasibility, we restrict our analysis to a sample of $\mathcal{T}$, as depicted in **Figure 1**. First, we randomly select a subset $\mathcal{A}_0^S \subseteq \mathcal{A}^\star$ of the addresses in the ground truth. Next, we select all transactions involving an address $a \in \mathcal{A}_0^S$ as an input or output, i.e., $\mathcal{T}_0^S = \{t \mid \exists a \in \mathcal{A}_0^S : a \in \mathrm{i}(t) \cup \mathrm{o}(t)\}$. We then build the set $\mathcal{A}_1^S$ of addresses that appear in transactions of $\mathcal{T}_0$ but not in $\mathcal{A}_0^S$, i.e. $\mathcal{A}_1^S = \{a \mid a \notin \mathcal{A}_0^S \wedge \exists t \in \mathcal{T}_0^S : a \in \mathrm{i}(t) \cup \mathrm{o}(t)\}$. The aforementioned process is then repeated in a similar manner. This involves finding the set $\mathcal{T}_1^S$ of transactions which include at least two addresses in $\mathcal{A}_1^S$, i.e., $\mathcal{T}_1^S = \{t \mid t \notin \mathcal{T}_0^S \wedge \exists a_1, a_2 \in \mathcal{A}_1^S : a_1 \in \mathrm{i}(t) \cup \mathrm{o}(t) \wedge a_2 \in \mathrm{i}(t) \cup \mathrm{o}(t) \wedge a_1 \neq a_2\}$. We set the condition on two addresses per transaction to reduce the size of the subsequently constructed Address Correspondence Networks. Finally, we build $\mathcal{A}_2^S$ as the addresses appearing in transactions of $\mathcal{T}_1^S$ and not already in $\mathcal{A}_0^S$ or $\mathcal{A}_1^S$, i.e. $\mathcal{A}_2^S = \{a \mid a \notin \mathcal{A}_0^S \cup \mathcal{A}_1^S \wedge \exists t \in \mathcal{T}_1^S : a \in \mathrm{i}(t) \cup \mathrm{o}(t)\}$.

As a result, this process constructs a set of sampled transactions $\mathcal{T}^S = T_0^S \cup T_1^S$ having addresses $\mathcal{A}^S = \mathcal{A}_0^S \cup \mathcal{A}_1^S \cup \mathcal{A}_2^S$. An advantage of this sampling method is that the constructed Address Correspondence Networks are centered around ground truth seed addresses, thereby exploiting the previous knowledge of controlling entities.

3.2 Partial and Cumulative Transaction Sets

To study the evolution of the Bitcoin Address Correspondence Network over time, we create temporal subsets of the transactions in $\mathcal{T}^S$. Each subset includes only the transactions in $\mathcal{T}^S$ that were generated in a specific time interval. We create time intervals using two different strategies, which we name cumulative and partial, summarized in **Figure 2**.

The cumulative strategy creates eight time intervals of progressively increasing width,[1] $\{[01.07.11, 30.06.y], [01.07.11, 31.12.y] \mid y \in [12, 15]\}$, while the partial strategy creates eight time intervals of fixed width, $\{[01.01.y, 30.06.y], [01.07.y, 31.12.y] \mid y \in [12, 15]\}$. It follows that cumulative time intervals overlap, while partial time intervals are disjoint.

Cumulative transaction sets are denoted with $\mathcal{T}^S_{[11s2,yss]}$, which refers to all transactions in $\mathcal{T}^S$ that were generated between the second semester of 2011 and the s^{th} semester of y, e.g., $\mathcal{T}^S_{[11s2,14s1]}$ includes transactions generated in the interval [01.07.11, 30.06.14]. Partial transaction sets are denoted with $\mathcal{T}^S_{[yss,yss]} \equiv \mathcal{T}^S_{[yss]}$, e.g., $\mathcal{T}^S_{[14s1]}$ refers to transactions generated in the interval [01.01.14, 30.06.14]. It is worth noting that while partial transaction sets do not share transactions, they may still share addresses which are used in multiple transactions.

3.3 Address Correspondence Network Construction

Let $\mathrm{w} : \mathcal{A} \times \mathcal{A} \to \mathbb{N}$ be a function that counts how often an address pair, (a_1, a_2), is detected by any of the seven heuristics introduced in Section 2.2 as being controlled by the same entity

[1]We represent dates in the use the DD.MM.YY format.

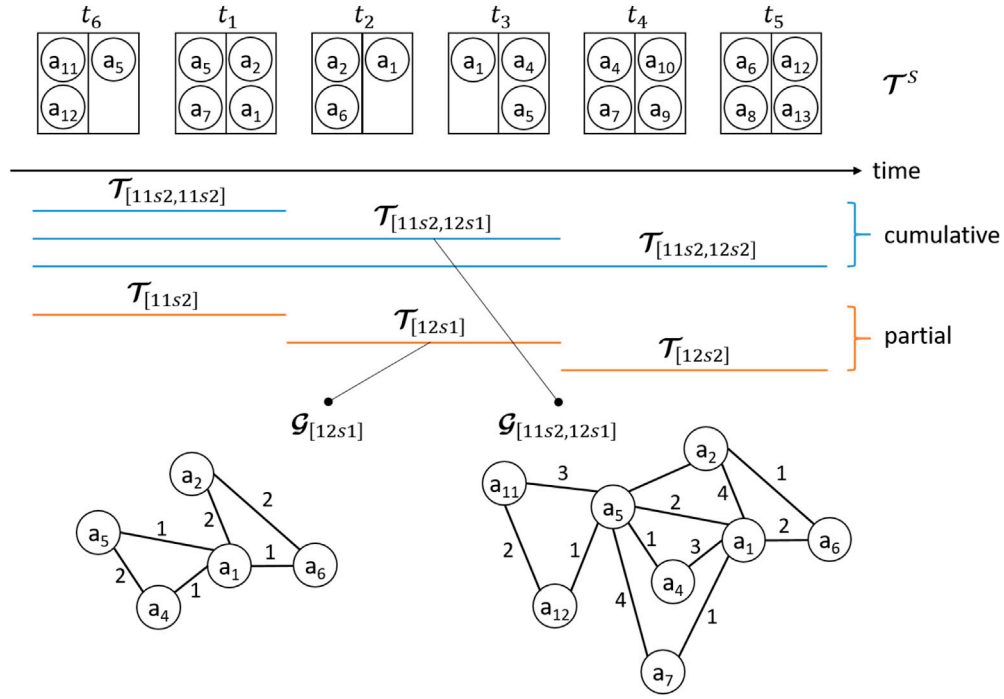


FIGURE 2 | Cumulative and partial transaction sets, and construction of the Address Correspondence Networks.

(considering only transactions in $\mathcal{T}^S_{[o,c]}$). It is worth noting that w is symmetric (or undirected), i.e. $\mathrm{w}(a_1, a_2) = \mathrm{w}(a_2, a_1)$.

The information captured by applying w to each pair of addresses in $\mathcal{A}^S_{[o,c]}$ is collected in Address Correspondence Networks, defined as undirected weighted graphs $\mathcal{G}_{[o,c]} = (\mathcal{A}^S_{[o,c]}, \mathcal{L}_{[o,c]}, \mathrm{w})$. The construction process is depicted in **Figure 2**. The addresses in $\mathcal{A}^S_{[o,c]}$ are the vertices of the graph, and w is the weight function. $\mathcal{L}_{[o,c]} \subseteq \mathcal{A}^S_{[o,c]} \times \mathcal{A}^S_{[o,c]}$ is the set of edges connecting address in two ways:

1) Pairs (a_i, a_o) such that it exists a transaction $t \in \mathcal{T}^S_{[o,c]}$ having respectively a_i and a_o in its input and output address sets $i(t)$ and $\mathrm{o}(t)$, and having $\mathrm{w}(a_i, a_o) > 0$.
2) Pairs (a_{i_1}, a_{i_2}) such that it exists a transaction $t \in \mathcal{T}^S_{[o,c]}$ having both a_{i_1} and a_{i_2} in its input set $i(t)$, and having $\mathrm{w}(a_{i_1}, a_{i_2}) > 0$.

Note that in a transaction, different heuristics can concur by identifying the same address as a change address, increasing the weights of the edges related to such an address. **Figure 3** shows the degree distribution of the Address Correspondence Networks $\mathcal{G}_{[11s2,12s1]}$ and $\mathcal{G}_{[11s2]}$. The two distributions show a similar shape, but note that the left plot is a cumulative graph and the right plot is a partial graph; this indicates that the correspondence networks appear to preserve common properties across time. **Table 1** provides descriptive statistics of the 16 Address Correspondence Networks we constructed from the eight partial and cumulative transaction sets. While the degree distributions cannot be assimilated to a single statistical distribution, they are skewed and fat-tailed, features that are recognized in complex networks of different contexts like biological, technological or social interactions [19].

Figure 4 shows the distribution of ground truth entities in the Address Correspondence Networks. In each plot, we compare a cumulative network and the partial network from its last six months, e.g. $\mathcal{G}_{[11s2,13s1]}$ with $\mathcal{G}_{[13s1]}$. The number of known entities in the networks from 2012 is small, $\mathcal{G}_{[12s1]}$ and $\mathcal{G}_{[12s2]}$ do not show any relation with their pairs. However, from 2013, the similarity between distributions of known entities of partial and cumulative networks is notorious.

3.4 Address Correspondence Network Clustering

Let $\mathcal{G}_{[o,c]} = (\mathcal{A}^S_{[o,c]}, \mathcal{L}_{[o,c]}, \mathrm{w})$ be the Address Correspondence Network for the time interval $[o, c]$. We approach the entity identification problem by applying a community detection algorithm to $\mathcal{L}_{[o,c]}$ (therefore assuming that communities are sets of addresses belonging to the same entity). In $\mathcal{G}_{[o,c]}$, highly interconnected vertices are clusters (communities) of addresses linked by one or several heuristics. Community detection algorithms find clusters of vertices highly interconnected but with sparse links between clusters. Specifically, the Label Propagation Algorithm (LPA) by Raghavan et al. [20] finds communities and has linear complexity on the number of edges $\mathcal{O}(\mathcal{L}_{[o,c]})$. The comparative study by Yang et al. [21] shows that the scalability of LPA outperforms other fast clustering algorithms, including Leading Eigenvector by Newman [22], Walktrap by Pons and Latapy [23], and Multilevel by Blondel et al. [24]. In LPA, each node is

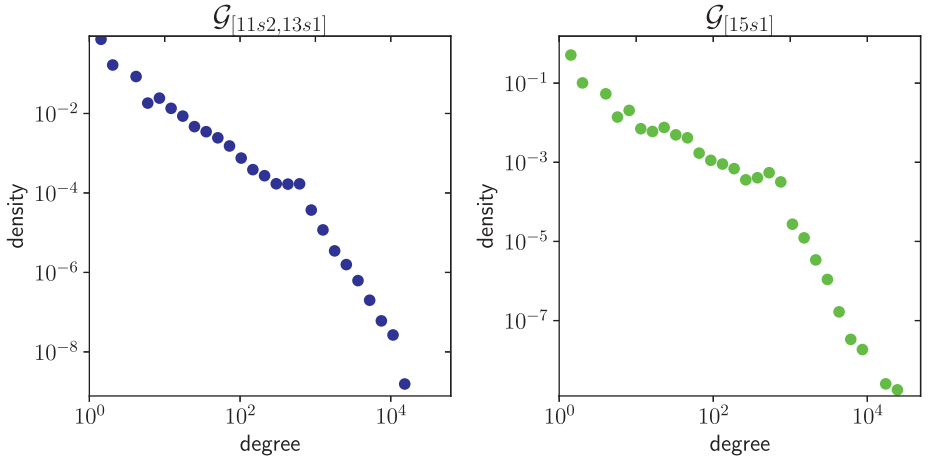


FIGURE 3 | Degree distribution for cumulative $\mathcal{G}_{[11s2,13s1]}$ and partial $\mathcal{G}_{[15s1]}$.

TABLE 1 | Number of nodes, edges and ground truth addresses of the partial and cumulative Address Correspondence Networks for each semester from 2012 to 2015.

y	*s*	**Partial:** $\mathcal{G}_{[\mathbf{yss}]}$			**Cumulative:** $\mathcal{G}_{[\mathbf{11s2,yss}]}$		
		$\lvert\mathcal{A}^{\mathbf{s}}_{[\mathbf{yss}]}\rvert$	$\lvert\mathcal{L}_{[\mathbf{yss}]}\rvert$	$\lvert\mathcal{A}^{\star}_{[\mathbf{yss}]}\rvert$	$\lvert\mathcal{A}^{\mathbf{s}}_{[\mathbf{11s2,yss}]}\rvert$	$\lvert\mathcal{L}_{[\mathbf{11s2,yss}]}\rvert$	$\lvert\mathcal{A}^{\star}_{[\mathbf{11s2,yss}]}\rvert$
2012	1	12	46	10	3,750	164,408	1,553
	2	5,054	1,239,850	5,029	8,804	1,404,258	6,582
2013	1	131,252	3,183,594	39,161	139,918	4,587,813	45,613
	2	191,453	45,965,678	155,449	329,240	50,552,843	199,614
2014	1	360,002	81,891,103	268,228	607,098	131,854,323	396,548
	2	505,748	31,121,336	233,609	1,092,560	162,948,611	621,919
2015	1	232,781	16,836,377	120,191	1,270,261	179,725,740	734,185
	2	990,117	52,732,659	211,174	2,184,445	232,416,368	935,599

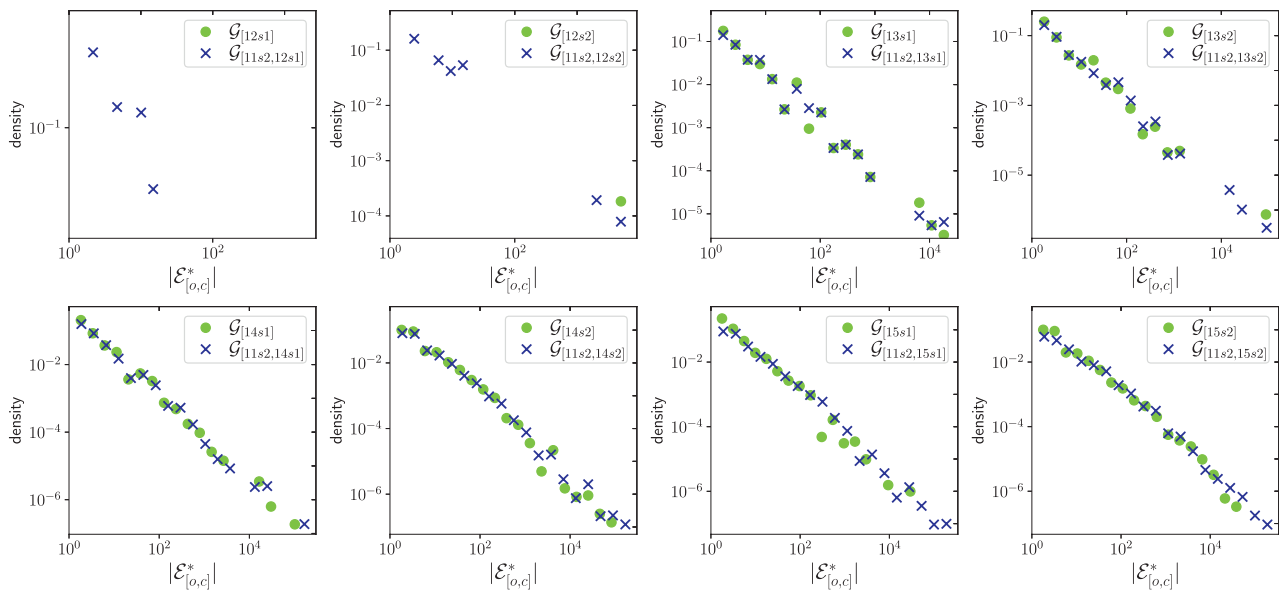


FIGURE 4 | Distribution of ground truth entity sizes, $\lvert\mathcal{E}^{\star}_{[o,c]}\rvert$.

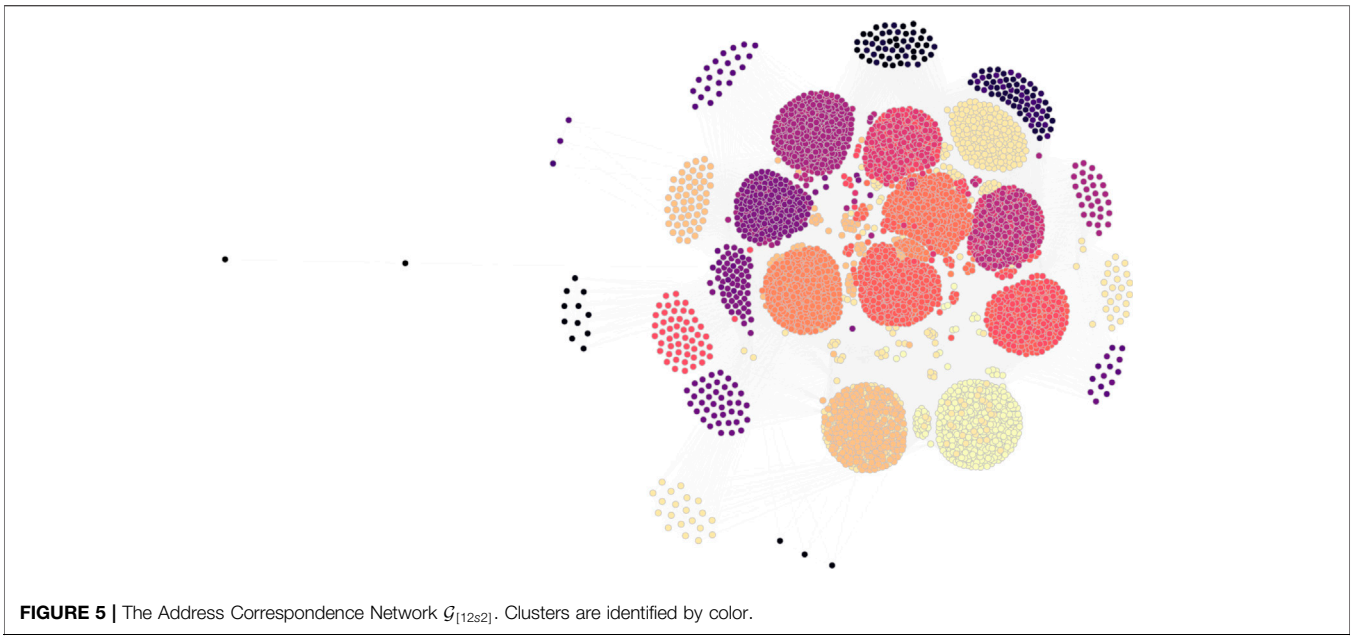


FIGURE 5 | The Address Correspondence Network $\mathcal{G}_{[12s2]}$. Clusters are identified by color.

initialized with a unique label, denoting the cluster it is part of (the controlling entity of an address). In the basic case, all the nodes are initially assigned a random label. Afterward, each node is randomly visited and assigned a label according to the majority voting of its neighbors. The process repeats until every node in the network gets a label to which most of its neighbors belong. **Figure 5** shows a clustering for the partial network $\mathcal{G}_{[12s2]}$.

To initialize parts of the nodes, we use the information from the ground truth $\mathrm{e}^{\star}$. Let $\mathcal{A}^{\star}_{[o,c]}$ denote the set of ground truth addresses in $\mathcal{G}_{[o,c]}$, i.e., $\mathcal{A}^{\star}_{[o,c]} = \mathcal{A}^{S}_{[o,c]} \cap \mathcal{A}^{\star}$, and let $\mathcal{E}^{\star}_{[o,c]}$ be the set of ground truth entities in $\mathcal{G}_{[o,c]}$, i.e. $\mathcal{E}^{\star}_{[o,c]} = \{\mathrm{e}^{\star}(a) \big| \exists a \in \mathcal{A}^{\star}_{[o,c]}\}$. We assign to a subset of nodes $\mathcal{A}^{I}_{[o,c]} \subseteq \mathcal{A}^{\star}_{[o,c]}$ the label from the ground truth, i.e. $\mathrm{e}^{\star}(a)$. It holds that $\mathcal{A}^{I}_{[o,c]} \subseteq \mathcal{A}^{\star}_{[o,c]} \subseteq \mathcal{A}^{S}_{[o,c]}$ and, concomitantly, $\left|\mathcal{A}^{I}_{[o,c]}\right| \leq \left|\mathcal{A}^{\star}_{[o,c]}\right| \leq \left|\mathcal{A}^{S}_{[o,c]}\right|$.

In this paper, we are interested in exploring the ability of community detection algorithms to provide additional information about the true identities of users. We hypothesize that the Address Correspondence Network encodes additional information about the entities that control specific addresses. We argue that successive applications of heuristics may lead to connections between addresses controlled by the same entity that are denser and higher weighted than connections between addresses of different entities. Following this argument, we apply LPA to obtain a disjoint set of clusters $\mathcal{C}_{[o,c]} = \{\mathcal{C}^{(1)}_{[o,c]}, \ldots, \mathcal{C}^{(k)}_{[o,c]}\}$, such that $\cup_{i=1}^{k} \mathcal{C}^{(i)}_{[o,c]} = \mathcal{A}^{S}_{[o,c]}$. Because of the additional information provided by the ground truth, we modified LPA to avoid that the addresses in $\mathcal{A}^{I}_{[o,c]}$ can change label, as they are associated with the actual entity according to the ground truth information.

In the experiments, we vary the proportion p of initialized nodes, that is defined as:

$$p = \left|\mathcal{A}^{I}_{[o,c]}\right| / \left|\mathcal{A}^{S}_{[o,c]}\right|.$$

Since $\left|\mathcal{A}^{\star}_{[o,c]}\right| / \left|\mathcal{A}^{S}_{[o,c]}\right|$ varies across networks and is an upper bound on the proportion of initialized nodes, the domains of the approximated functions also vary.

3.5 Cluster Quality Analysis

Finally, we quantify the clustering quality as a function of cluster size and entity size. Given an Address Correspondence Network $\mathcal{G}_{[o,c]}$ and set of clusters $\mathcal{C}_{[o,c]} = \{\mathcal{C}^{(1)}_{[o,c]}, \ldots, \mathcal{C}^{(k)}_{[o,c]}\}$ produced by LPA, we analyze the quality of $\mathcal{C}_{[o,c]}$ by defining a set of discrete random variables to describe characteristics of the network, and by five metrics: modularity to give information about the intrinsic quality of the clusters (and inherent topological structure of the network), homogeneity, entropy, Adjusted Mutual Information (AMI) and Adjusted Rand Index (ARI) to compare the clusters with the ground truth labels. Furthermore, all metrics are measured as functions of the proportion of initialized nodes p.

3.5.1 Random Variables

To study the characteristics of the network, we define the following discrete random variables associated with the distributions of entities, addresses, and known addresses in the address correspondence network.

The first random variable, E, assumes a value from the set of entities according to their frequency in the correspondence network. More specifically, E can assume the value $e \in \mathcal{E}^{\star}_{[o,c]}$ with probability equal to the numbers of addresses in $\mathcal{A}^{\star}_{[o,c]}$ mapped to e, divided by the total number of addresses in $\mathcal{A}^{\star}_{[o,c]}$, i.e.:

$$P(e) = \frac{\left|\left\{a \in \mathcal{A}^{\star}_{[o,c]} \middle| e = \mathrm{e}^{\star}(a)\right\}\right|}{\left|\mathcal{A}^{\star}_{[o,c]}\right|}.$$

In addition to E, we also define variables that assume values in the entity set according to their frequency in specific clusters. Let

E_i be the variable associated to the ith cluster, i.e. $i \in [1, |\mathcal{C}_{[o,c]}|]$. For each i, we build a histogram of the frequency of entities in $\mathcal{C}^{(i)}_{[o,c]}$, by counting for each entity e the number of addresses associated to e through the ground truth data in $\mathcal{C}^{(i)}_{[o,c]}$. Such a histogram is used to approximate the distribution of entities over $\mathcal{C}^{(i)}_{[o,c]}$ and serves to describe E_i. Formally let $\mathcal{A}^{(i)}_{[o,c]} = \mathcal{A}^{\star}_{[o,c]} \cap \mathcal{C}^{(i)}_{[o,c]}$ be the set of addresses in $\mathcal{C}^{(i)}_{[o,c]}$ which are part of the ground truth. E_i can assume a value e in $\mathcal{E}^{(i)}_{[o,c]} = \{\mathrm{e}^{\star}(a) \big| a \in \mathcal{A}^{(i)}_{[o,c]}\}$ with probability:

$$P(e) = \frac{\left|\left\{a \in \mathcal{A}^{(i)}_{[o,c]} \middle| e = \mathrm{e}^{\star}(a)\right\}\right|}{\left|\mathcal{A}^{(i)}_{[o,c]}\right|}.$$

The variable C assumes a cluster identifier according to its frequency over the addresses in the ground truth. C can assume a value $\mathcal{C}^{(i)}_{[o,c]} \in \mathcal{C}_{[o,c]}$ with probability defined by the number of addresses in $\mathcal{A}^{\star}_{[o,c]}$ and $\mathcal{C}^{(i)}_{[o,c]}$ (i.e. $\mathcal{A}^{(i)}_{[o,c]}$) divided by the total number of addresses in $\mathcal{A}^{\star}_{[o,c]}$, i.e.:

$$P\left(\mathcal{C}^{(i)}_{[o,c]}\right) = \frac{\left|\mathcal{A}^{(i)}_{[o,c]}\right|}{\left|\mathcal{A}^{\star}_{[o,c]}\right|}.$$

Finally, we define variables complementary to E_i to describe the frequency of clusters among each entity. We indicate with C_j the variable associated to the jth entity e_j, with $j \in [1, |\mathcal{E}^{\star}_{[o,c]}|]$. Given the entity e_j, we build the histogram of the appearance of e_j in each cluster of $\mathcal{C}_{[o,c]}$. As for the E_i variables, we approximate the real distribution using the ground truth data, and considering only the addresses from $\mathcal{A}^{\star}$ to build the bins. Formally, C_j can assume values in $\mathcal{C}_{[o,c]}$ with probability:

$$P\left(\mathcal{C}^{(i)}_{[o,c]}\right) = \frac{\left|\left\{a \in \mathcal{C}^{(i)}_{[o,c]} \middle| e_j = \mathrm{e}^{\star}(a)\right\}\right|}{\left|\left\{a \in \mathcal{A}^{\star}_{[o,c]} \middle| e_j = \mathrm{e}^{\star}(a)\right\}\right|}.$$

3.5.2 Metrics

Modularity, initially proposed by Newman and Girvan [25], compares the clusters with a random baseline. This is done by computing the difference between the number of edges inside the clusters with the expected value of edges using the same clusters but with random connections between the nodes. Let $|\mathcal{C}_{[o,c]}|$ be the number of clusters in the Address Correspondence Network $\mathcal{G}_{[o,c]}$, q_{ij} the ratio of edges connecting addresses between cluster $\mathcal{C}^{(i)}_{[o,c]}$ and cluster $\mathcal{C}^{(j)}_{[o,c]}$, and $r_i = \sum_j q_{ij}$ the ratio of edges with at least one end in $\mathcal{C}^{(i)}_{[o,c]}$. The modularity is defined as:

$$Q = \sum_{i=1}^{|\mathcal{C}_{[o,c]}|} (q_{ii} - r_i^2).$$

A value close to 0 indicates that the community structure is akin to a random network, while values close to 1 indicate strong community structures, meaning dense connections inside the communities and sparse connections between them.

Information Theory Metrics: Entropy, introduced in an information theory context by Shannon [26], quantifies the expected amount of information or uncertainty contained in a random variable. Let X be a discrete random variable, which can assume values $\{x_1, x_2, \ldots, x_k\}$ with probability $\{P(x_1), P(x_2), \ldots, P(x_k)\}$. The entropy of X is defined as:

$$H(X) = -\sum_{x\,\in\,1}^{k} P(x)\log_2 P(x),$$

while the normalized Shannon entropy is:

$$\widehat{H}(X) = \frac{H(X)}{H_{max}(X)} = \frac{H(X)}{\log_2(k)}.$$

We use the normalized entropy of E_i and C_j to study the clusters by the perspective of the entities and the one of the cluster themselves.

Entropy also gives important information of the interrelation between random variables. Let us consider two variables X and Y, and let $P(X, Y)$ be the joint probability distribution. The conditional entropy $H(Y|X)$ is defined as:

$$H(Y|X) = -\sum_{x\in X, y\in Y} P(x,y)\frac{\log_2 P(x,y)}{P(x)}$$

The conditional entropy indicates how much extra information is needed to describe Y given that X is known. Additionally, the amount of information needed on average to specify the value of two random variables is $H(X, Y) = H(X|Y) + H(Y)$.

We use conditional entropy to measure the quality of the clusters. We do it by comparing them with the distribution of the entities in the Address Correspondence Network, exploiting the variables E and C. Such a measure is named homogeneity and is initially introduced by Rosenberg and Hirschberg [27]. Ideally, a cluster should only contain addresses that are controlled by the same entity. In such a case, clusters are homogeneous and it holds $H(E|C) = 0$. The homogeneity score $h \in [0, 1]$ is defined by:

$$h = \begin{cases} 1 & \text{if } H(E,C) = 0 \\ 1 - H(E|C)/H(E) & \text{otherwise} \end{cases}.$$

The fundamental Mutual Information (MI) [28] quantifies the agreement between partitions. In addition to $\mathcal{C}_{[o,c]}$, let $\mathcal{K}_{[o,c]} = \{\mathcal{K}^{(1)}_{[o,c]}, \ldots, \mathcal{K}^{(k)}_{[o,c]}\}$ be an alternative set of clusters. We introduce the variable K to describe the distribution of the addresses in $\mathcal{K}_{[o,c]}$, similarly to how we defined C for $\mathcal{C}_{[o,c]}$ in Section 3.5.1. The MI of C and K is defined as:

$$\mathrm{MI}(C, K) = H(K) - H(K|C),$$

and quantifies the reduction of the uncertainty of $\mathcal{C}_{[o,c]}$ due to the knowledge of $\mathcal{K}_{[o,c]}$. The average MI value between $\mathcal{C}_{[o,c]}$ and $\mathcal{K}_{[o,c]}$ tends to increase as the number of clusters increases, even if there is no difference in the clustering methodology, e.g. if the partitions are assigned clusters randomly. The Adjusted Mutual Information defined by Vinh et al. [29] takes into account the randomness using the expected value of MI $E[\mathrm{MI}]$ and normalizes its value:

$$\mathrm{AMI}(C, K) = \frac{\mathrm{MI}(C,K) - E[\mathrm{MI}(C,K)]}{\langle H(C,K)\rangle - E[\mathrm{MI}(C,K)]}.$$

AMI gets values in the [0, 1] interval, and when two partitions perfectly match, AMI = 1.

Finally, we consider the Rand Index (RI), initially proposed by Rand [30], which compares two set of clusters while ignoring permutations. Let $\mathcal{C}_{[o,c]}$ and $\mathcal{K}_{[o,c]}$ be two sets of clusters. Let $x(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]})$ be the number of pairs of addresses from the ground truth $\mathcal{A}^{\star}_{[o,c]}$ which are in the same cluster in $\mathcal{C}_{[o,c]}$ and in the same cluster in $\mathcal{K}_{[o,c]}$, i.e.:

$$x(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]}) = |\{(a_1, a_2) | a_1, a_2 \in \mathcal{A}^{\star}_{[o,c]}, a_1 \neq a_2 \\ \wedge \exists \mathcal{C}^{(i)}_{[o,c]} \in \mathcal{C}_{[o,c]} : a_1, a_2 \in \mathcal{C}^{(i)}_{[o,c]} \\ \wedge \exists \mathcal{K}^{(j)}_{[o,c]} \in \mathcal{K}_{[o,c]} : a_1, a_2 \in \mathcal{K}^{(j)}_{[o,c]}\}$$

and let $y(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]})$ be the number of address pairs from the ground truth $\mathcal{A}^{\star}_{[o,c]}$ which are in different clusters of $\mathcal{C}_{[o,c]}$ and in different clusters of $\mathcal{K}_{[o,c]}$, i.e.:

$$y(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]}) = |\{(a_1, a_2) | a_1, a_2 \in \mathcal{A}^{\star}_{[o,c]}, a_1 \neq a_2 \\ \wedge \exists \mathcal{C}^{(i)}_{[o,c]}, \mathcal{C}^{(j)}_{[o,c]} \in \mathcal{C}_{[o,c]} : a_1 \in \mathcal{C}^{(i)}_{[o,c]}, a_2 \in \mathcal{C}^{(j)}_{[o,c]}, i \neq j \\ \wedge \exists \mathcal{K}^{(k)}_{[o,c]}, \mathcal{K}^{(l)}_{[o,c]} \in \mathcal{K}_{[o,c]} : a_1 \in \mathcal{K}^{(k)}_{[o,c]}, a_2 \in \mathcal{K}^{(l)}_{[o,c]}, k \neq l\}$$

The Rand Index is defined as:

$$\mathrm{RI}(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]}) = \frac{x(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]}) + y(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]})}{\left|\mathcal{A}^{\star}_{[o,c]}\right| \times \left(\left|\mathcal{A}^{\star}_{[o,c]}\right| - 1\right)},$$

where the denominator is the number of address pairs in $\mathcal{A}^{\star}_{[o,c]}$. As with MI/AMI, we consider an adjusted version of RI, the Adjusted Rand Index (ARI) as proposed by Hubert and Arabie [31], which accounts for chance:

$$\mathrm{ARI}(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]}) = \frac{\mathrm{RI}(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]}) - E[\mathrm{RI}(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]})]}{\max\langle \mathrm{RI}(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]})\rangle - E[\mathrm{RI}(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]})]},$$

where $E[\mathrm{RI}(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]})]$ denotes the expected value of $\mathrm{RI}(\mathcal{C}_{[o,c]}, \mathcal{K}_{[o,c]})$. As for AMI, an ARI value of 1 indicates perfectly matching partitions, while a value of 0 indicates independent partitions. Warrens [32] shows that ARI is equivalent to Cohen's Kappa Cohen [33], which is well suited for the evaluation of community detection methods, as discussed by Liu et al. [34].

4 RESULTS

We first analyze the size of the clusters identified by LPA for the Address Correspondence Networks described in **Section 3**, whose statistics are shown in **Table 1**. **Figure 6** shows the cluster size distribution of $\mathcal{G}_{[11s2,13s1]}$ and $\mathcal{G}_{[15s1]}$, for initialization proportions $p = 0$ and $p = 0.1$. Note that the density of the small clusters, in both cases, shifts to reach larger cluster sizes when $p = 0.1$, as well as the maximum cluster size of $\mathcal{G}_{[11s2,13s1]}$. This indicates that even a small proportion of initialized nodes, such as $p = 0.1$, considerably modifies the cluster distribution in the networks.

We also fit a power-law distribution to the cluster size distribution, shown by the dotted red lines with the corresponding alpha values in **Figure 6**. Furthermore, the power-law distribution fits the data significantly better than an exponential distribution, resulting in p-values of less than 0.1% using likelihood ratio tests [35]. The exponents are larger for $p = 0p = 0$ than for $p = 0.1p = 0.1$, in agreement with the observation related to the range of values in the cluster size. In general, the distributions are very heterogeneous. Additionally, the cluster size distribution suggests that, from a Correspondence Network perspective, there is a preferential attachment dynamic in the address generation where entities that control many addresses are likely to generate more addresses than others.

Next, we study the behavior of the intra-cluster total degree (number of edges connecting nodes that belong to the same cluster) and the inter-cluster degree (number of edges between nodes that belong to different clusters) as functions of the cluster size. For the total intra-cluster degree, there are two extreme behaviors that can be expected. On the one hand, a linear dependency on cluster size would signal that address reuse is negligible (therefore that privacy-preserving usage are commonplace), and the topology of the correspondence network encodes no additional information about the identity of the users that control the addresses. On the other hand, a quadratic relationship (close to the theoretical maximum $\propto c(c-1)/2$) would signal that the clusters are very densely interconnected, and the actual address reuse is high. Therefore, it would be possible to infer actual information about the users by directly inspecting the correspondence network through network science methods. In **Figure 7**, the extreme values of the intra-cluster degree of $\mathcal{G}_{11s2,13s1}$ and $\mathcal{G}_{15s1}$ are above a linear function (red dotted line) and below a quadratic function (yellow dashed line) of the cluster size. The same lines are depicted in the inter-cluster degree distributions showing that the intra-cluster degree grows faster. By applying an Ordinary Least Squares regression (OLS), the slope of a fitting line is in both networks bigger in the intra-cluster case. Furthermore, bigger entities preserve this behavior, showing that the correspondence network has an inherent community structure. Thus, this result is not valid only for entities that control a small number of addresses, and it follows that it is a general property of the network.

Figure 8 shows the number of clusters returned by LPA, $\left|\mathcal{C}_{[o,c]}\right|$, as a function of p. The dashed lines indicate the number of entities $\left|\mathcal{E}^{\star}_{[o,c]}\right|$ for each Address Correspondence Network. $\left|\mathcal{E}^{\star}_{[o,c]}\right|$ is a lower bound of the true number of entities, since each network also contains addresses not in the ground truth. This is supported by $\left|\mathcal{C}_{[o,c]}\right| \geq \left|\mathcal{E}^{\star}_{[o,c]}\right|$ holding for each test point. In general, $\left|\mathcal{C}_{[o,c]}\right|$ decreases sharply at small p, after which the rate of decrease slows and stabilises. $\left|\mathcal{C}_{[o,c]}\right|$ tends to be lower for partial networks than for cumulative networks, and can be explained by partial networks having a lower $\left|\mathcal{E}^{\star}_{[o,c]}\right|$.

The complexity and structure of the Address Correspondence Network are stable over time: **Figures 9–11** show AMI, ARI and homogeneity as functions of p. Since these metrics require ground truth labels, they are computed only for addresses in $\mathcal{A}^{\star}_{[o,c]}$. We observe that AMI and ARI lead to similar results: they rapidly increase before converging to the maximum value as p increases. In contrast, homogeneity exhibits no such initial rapid increase, and instead increases linearly with p. The mean levels of AMI, ARI and homogeneity do not consistently increase or decrease

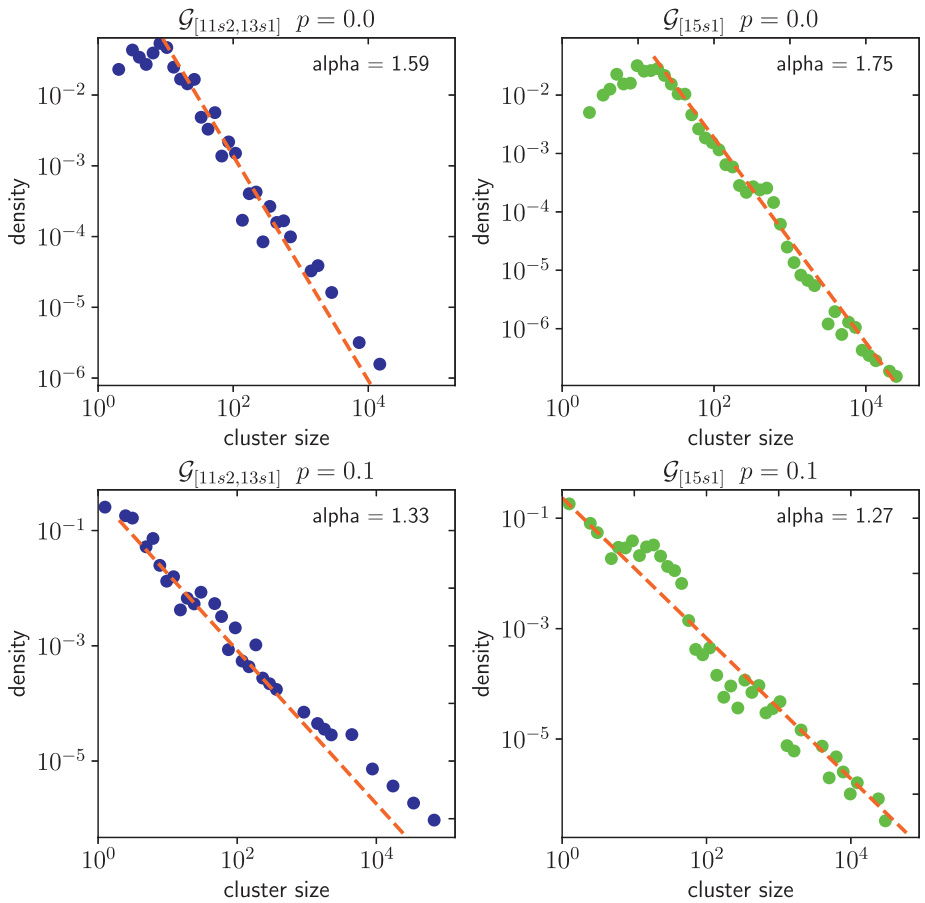


FIGURE 6 | Cluster size distribution of $\mathcal{G}_{[11s2,13s1]}$ and $\mathcal{G}_{[15s1]}$ for $p = 0.0p = 0.0$ and $p = 0.1p = 0.1$. The alpha values of the power-law distribution fits are also shown.

with increasing half-year. Furthermore, the mean metric levels for the partial networks appear to be comparable to those for the cumulative networks. This suggests that the complexity and structure of the Address Correspondence Network communities remain stable over time.

The effect of the node initialization: If the cost of labeling a Bitcoin address is assumed to be constant, the marginal gain in clustering quality per unit cost from increasing p quickly declines. Considering that homogeneity remains constant across all p, it appears that increasing p is cost-effective until around $p = 0.1$. At this point, $\mathcal{A}^I_{[o,c]}$ contains most of the information required to describe the community structure. The observed saturations in $|\mathcal{C}_{[o,c]}|$, AMI and ARI suggest that increasing p beyond 0.1 adds only idiosyncratic community information, yielding little improvement in clustering quality. This is further confirmed by studying clustering modularity as a function of p in **Figure 11**. Modularity appears mostly constant except for a sharp initial change, showing a robust community topology that is consistently detected after initializing a small proportion of nodes.

To assert the significance of the results presented in **Figures 8–12**, we repeated the experiments for 100 randomized versions of the $\mathcal{G}_{[11s2,13s1]}$ and $\mathcal{G}_{[15s1]}$ Address Correspondence Networks. The ii–th randomized network was obtained by performing $4i \cdot |\mathcal{L}_{[o,c]}|$ edge swaps on the original network, according to the algorithm proposed by Maslov [36], which preserves the network's degree distribution. With the exception of $|\mathcal{C}_{[11s2,13s1]}|$ for $\mathcal{G}_{[11s2,13s1]}$, the randomized results show little variation. However, all randomized results appear significantly different to those for the original networks. This suggests that the (non-randomized) results shown in **Figures 8–12** are a consequence of more complex network properties rather than solely the degree distribution.

Furthermore, the effect of node initialization order was studied by repeating the experiments for the $\mathcal{G}_{[11s2,13s1]}$ and $\mathcal{G}_{[15s1]}$ networks using 100 random orderings. The node initialization order does not seem to affect the general level and shape of the curves. Small perturbations observed in **Figures 8–12** appear to be idiosyncrasies of the chosen ordering, and may be larger for smaller networks (since the curves for $\mathcal{G}_{[11s2,13s1]}$ vary more than the ones for $\mathcal{G}_{[15s1]}$).

The effect of cluster and entity sizes: **Figure 13** shows $\widehat{H}(E_i)$ and $\widehat{H}(C_j)$ for the $\mathcal{G}_{[14s1]}$, $\mathcal{G}_{[11s2,14s1]}$, $\mathcal{G}_{[15s2]}$ and $\mathcal{G}_{[11s2,15s2]}$ networks. $\widehat{H}(E_i)$ and $\widehat{H}(C_j)$ are expressed as functions of the

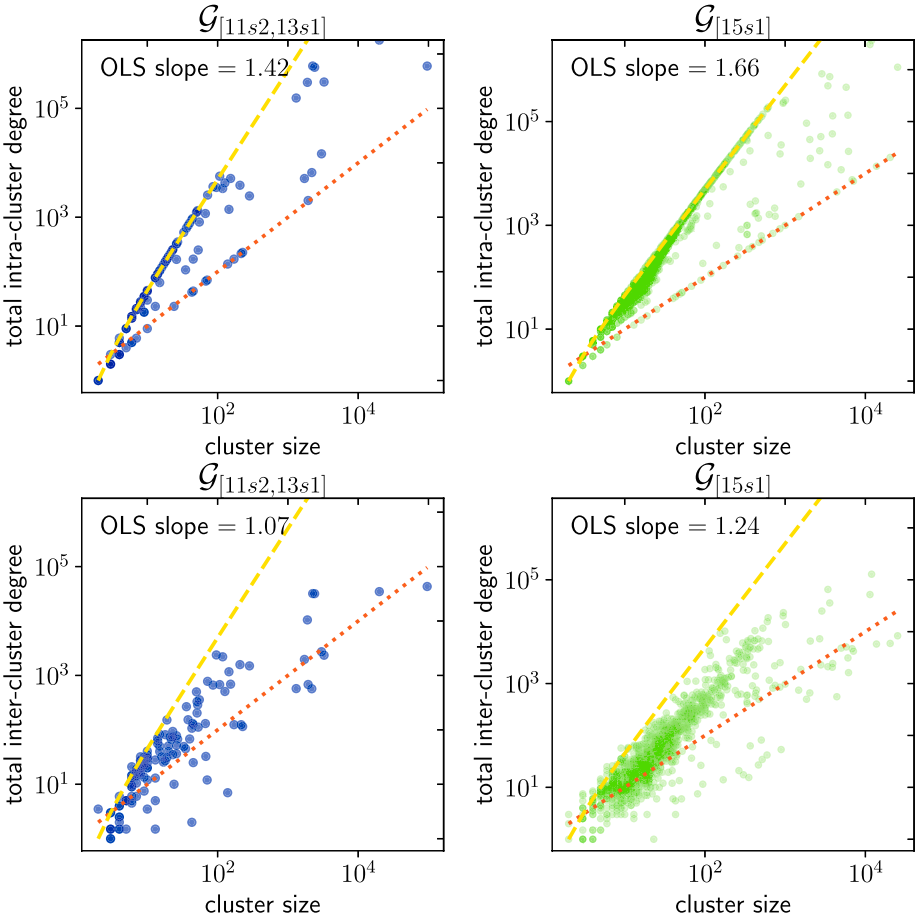


FIGURE 7 | Comparison of the total intra-cluster and inter-cluster degrees for $\mathcal{G}_{[11s2,13s1]}$ and $\mathcal{G}_{[15s1]}$. We also show the lines $y = x$ (red, dotted) and $y = x(x-1)/2$ (yellow, dashed).

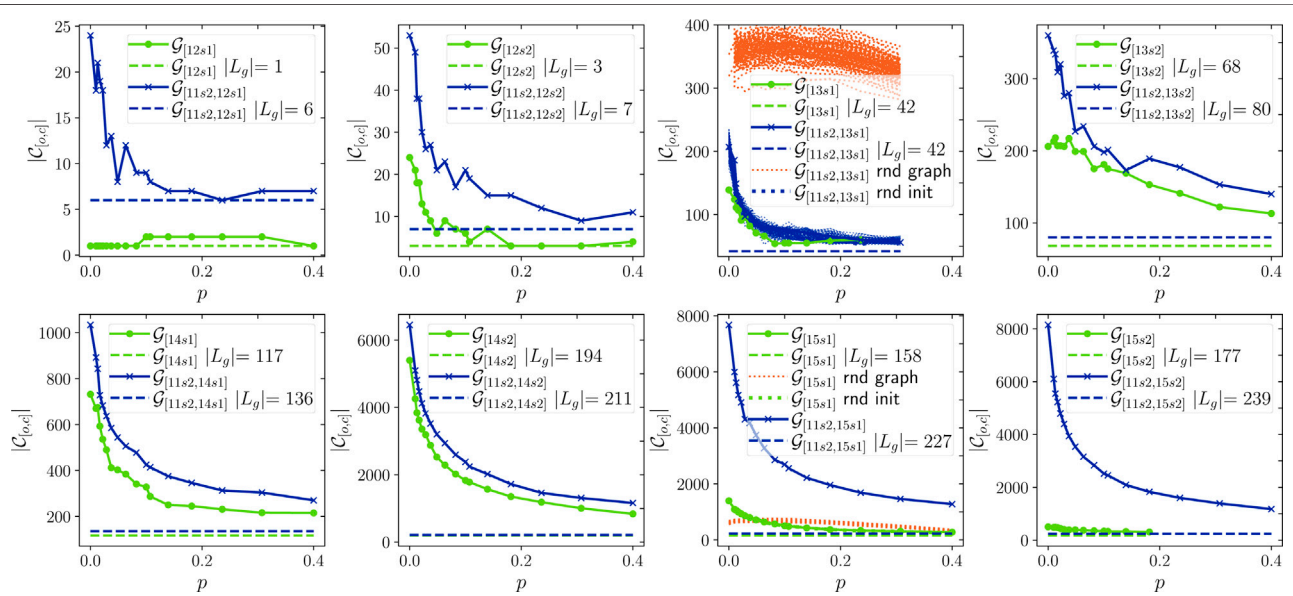


FIGURE 8 | Number of clusters as a function of p.

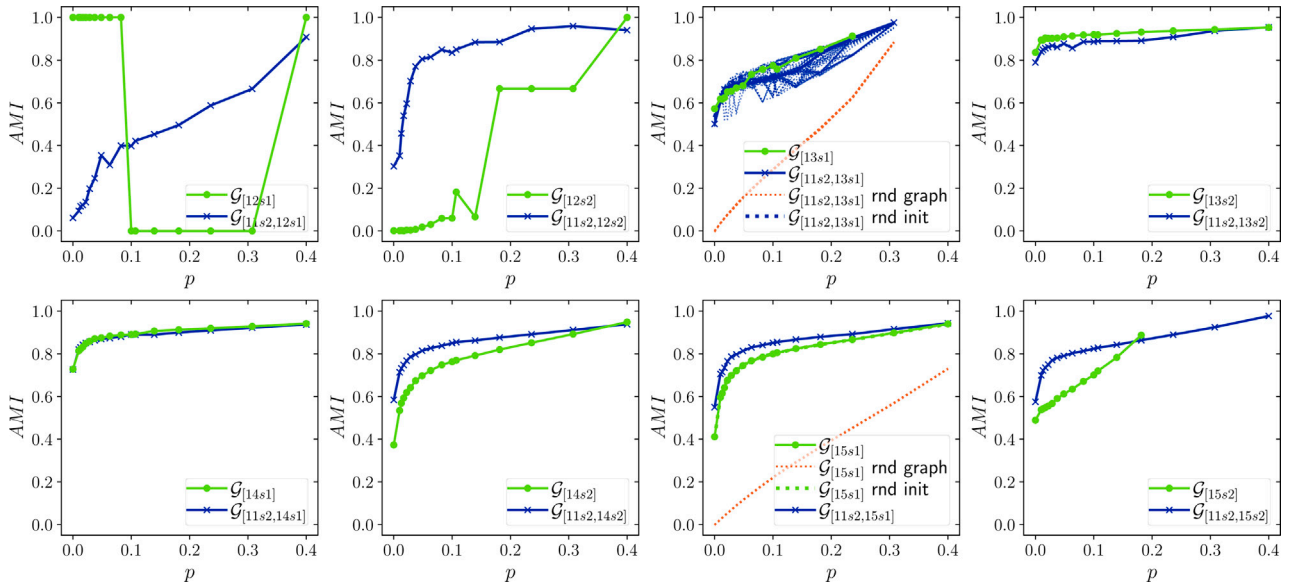


FIGURE 9 | AMI as a function of p.

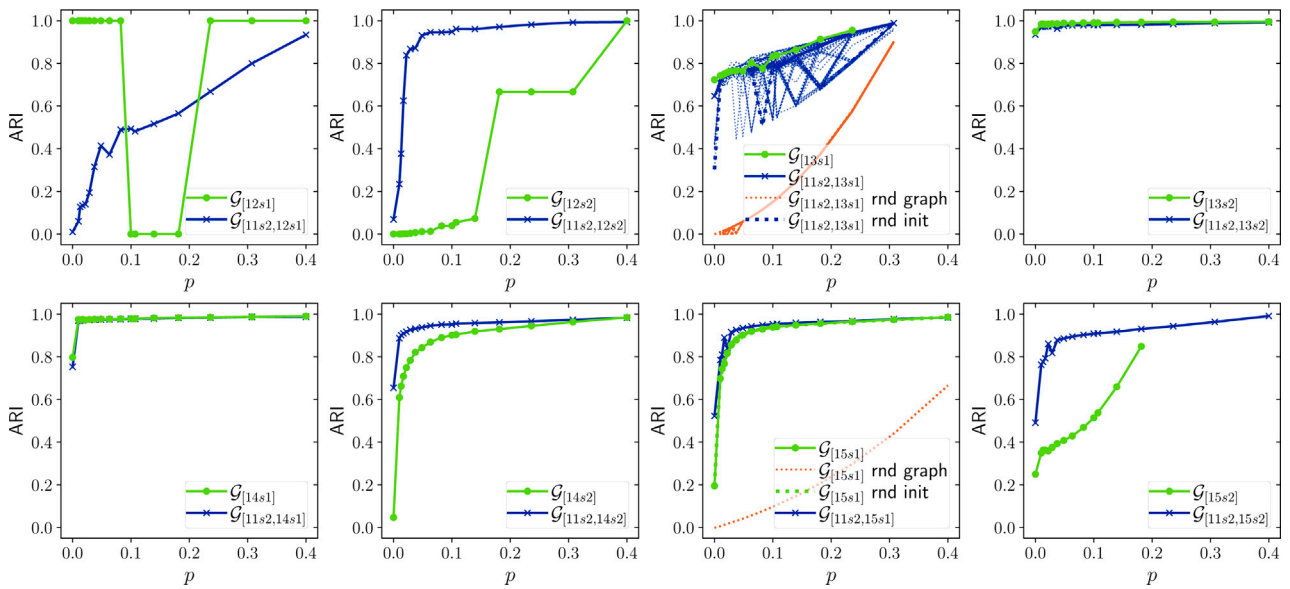


FIGURE 10 | ARI as a function of p.

relative cluster and entity sizes, i.e. normalized to $\left|\mathcal{A}^{\star}_{[o,c]}\right|$, respectively. We run experiments with $p = 0$ and $p = 0.1$. We note that $\widehat{H}(E_i)$ correlates negatively with the relative cluster size, and $\widehat{H}(C_j)$ correlates negatively with relative entity size. For small clusters and entities, there are strips of points located at the minimum and maximum values of $\widehat{H}(E_i)$ and $\widehat{H}(C_j)$. This is to be expected: if we consider a cluster with only two addresses, both associated with the same entity, $\widehat{H}(E_i)$ is minimum. If two addresses are mapped to different entities, we obtain a uniform entity label distribution, and $\widehat{H}(E_i)$ is maximum. Such extreme fluctuations become less likely as cluster size increases. Large clusters, therefore, tend to be purer than smaller clusters, corresponding to a higher clustering quality. Similarly, entities represented by more addresses are distributed more asymmetrically across clusters, again corresponding to a higher clustering quality. This is in agreement with the results in **Figure 7**, where the community structure is shown to become more apparent for larger clusters.

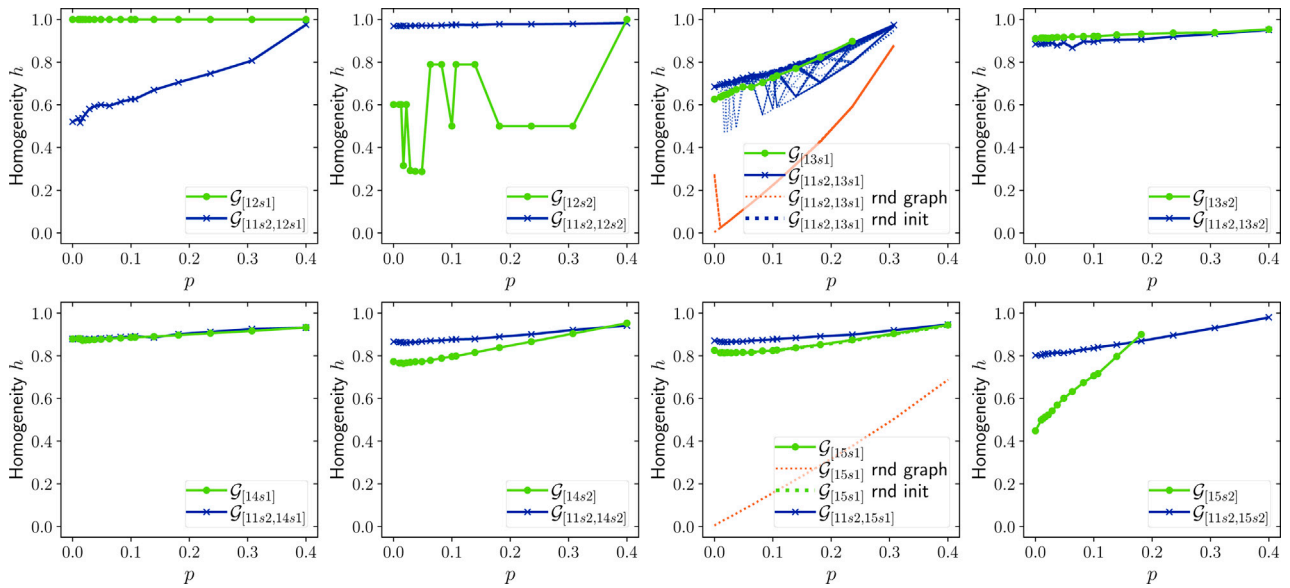


FIGURE 11 | Homogeneity as a function of p.

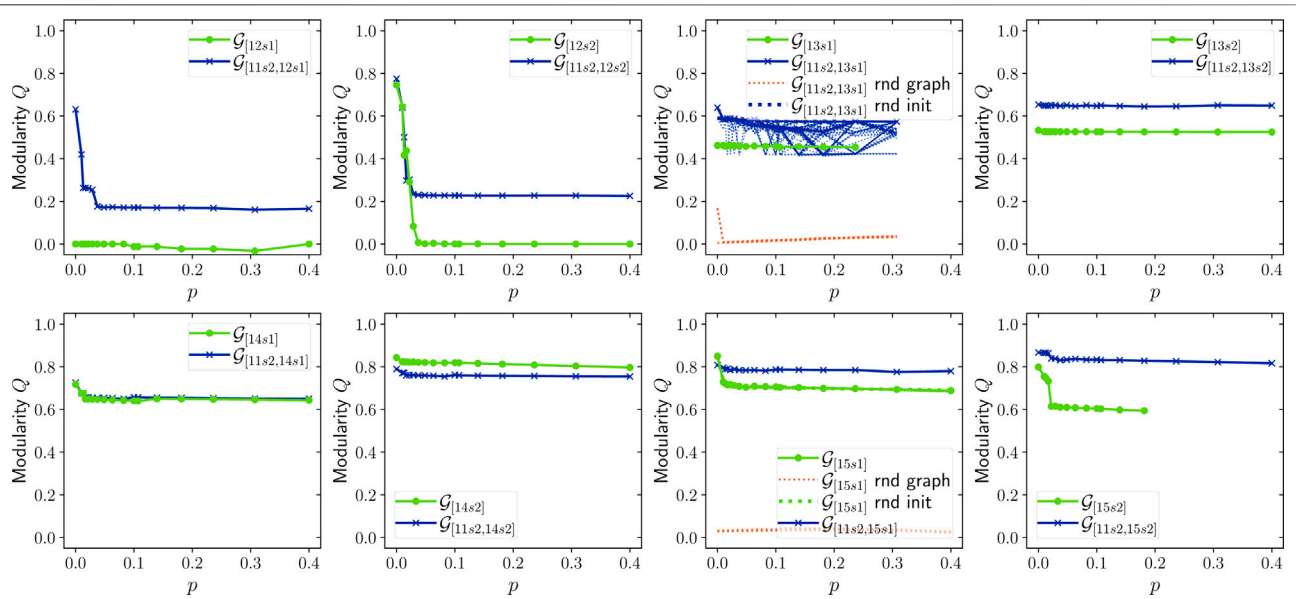


FIGURE 12 | Modularity as a function of p.

Furthermore, the mean levels of $\widehat{H}(E_i)$ and $\widehat{H}(C_j)$ for the partial networks are always less than or equal to the ones of the corresponding cumulative networks (comparing row 1–3 and row 2–4 in **Figure 13**). This suggests that partial networks allow a higher quality of interpretation regarding the community structure. A possible explanation for this is that Bitcoin entities have less time to obfuscate their activity: the longer the considered transaction history, the more the obfuscation attempts accumulate and the more difficult it becomes to detect the true community structure.

Interestingly, the average $\widehat{H}(E_i)$ and $\widehat{H}(C_j)$ increase after initialising 10% of nodes. The increase in $\widehat{H}(E_i)$ can be explained by the loss of small, homogeneous clusters with low $\widehat{H}(E_i)$. For $\widehat{H}(C_j)$, the increase is likely due to the decrease in the number of clusters, which in turn causes $H_{max}(E_i)$ to decrease.

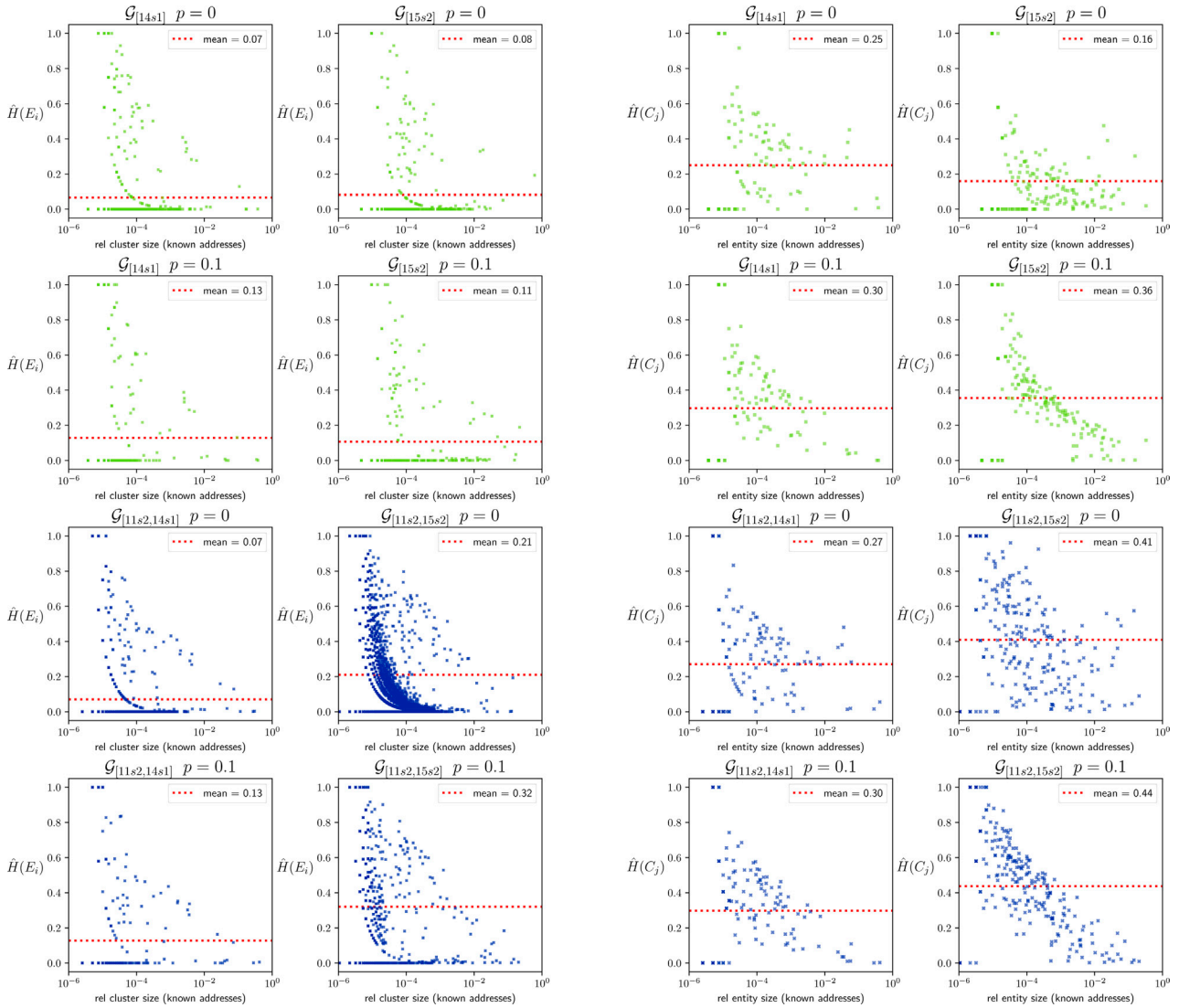


FIGURE 13 | Normalized entropy as a function of relative cluster size and relative entity size.

5 CONCLUSION AND FUTURE WORK

In this paper, we consider the application of a general-purpose community detection algorithm, LPA, to detect address clusters that are controlled by the same entity in the Bitcoin transaction history. Specifically, we apply LPA to Address Correspondence Networks, which incorporate information from a variety of simple address linking heuristics. We detect a strong community structure within these networks by inspecting their intra- and inter-cluster degrees. We find that the inter-cluster degree grows faster than the inter-cluster degree for cluster size increments. Address correspondence networks are therefore suitable for the application of general community detection methods from the broader field of network science—this creates an entry point for future researchers to move far beyond the application of primitive heuristics.

Since LPA is able to exploit ground truth information, we find that clustering quality improves as the number of labeled addresses in the Address Correspondence Networks increases. However, under the assumption that the cost of labeling a Bitcoin address is constant, we find that the marginal gain in clustering quality per unit cost quickly declines. Under this assumption, we propose that address labeling is cost-effective until around $p = 0.1$ $p = 0.1$, i.e. until 10% of all addresses in the Address Correspondence Network are identified. Furthermore, we find that choosing which addresses to label does not have a significant effect on clustering quality. Finally, we find that the structure of communities in the Address Correspondence Network remains stable over time. Partial Address Correspondence Networks are,

therefore, reasonable proxies for their cumulative counterparts (and far less demanding from a computational point of view).

For future work, we plan to conduct experiments to test the robustness of the heuristics and specific combinations between them. For example, analyzing their likelihood and studying their contribution to the links between addresses. From a network reconstruction perspective, link prediction is an interesting approach to improve the correspondence network by validating current links and predicting missing ones. Additionally, different machine learning approaches can be implemented to graph analysis; supervised methods are suitable if more ground truth information is available in the future.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. This data can be found here: https://bitcoin.org/en/download, https://www.walletexplorer.com/.

AUTHOR CONTRIBUTIONS

JF and AP developed the software, curated the data, run the analyses, created the visualizations, and wrote the initial draft. DD and CT contributed with the conceptualization and methodology, supervised the study and reviewed and edited the text. AB supervised the study and reviewed and edited the text. All authors discussed the results. All authors worked and agreed on the final version.

FUNDING

DD acknowledges partial funding from by the Swiss National Science foundation under contract #407550_167177. CT acknowledges financial support from the University of Zurich through the University Research Priority Program on Social Networks.

REFERENCES

1. Foley S, Karlsen JR, and Putniņš TJ. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? *Rev Financial Stud* (2019) 32: 1798–853. doi:10.1093/rfs/hhz015
2. Gaihre A, Luo Y, and Liu H. Do Bitcoin Users Really Care about Anonymity? an Analysis of the Bitcoin Transaction Graph. In: *2018 IEEE International Conference on Big Data (Big Data)* (2018). p. 1198–207. doi:10.1109/BigData.2018.8622442
3. Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, Voelker GM, et al. A Fistful of Bitcoins. *Commun ACM* (2016) 59:86–93. doi:10.1145/2896384
4. Kondor D, Pósfai M, Csabai I, and Vattay G. Do the Rich Get Richer? an Empirical Analysis of the Bitcoin Transaction Network. *PLoS ONE* (2014) 9: e86197. doi:10.1371/journal.pone.0086197
5. Javarone MA, and Wright CS. From Bitcoin to Bitcoin Cash. *Proc 1st Workshop Cryptocurrencies Blockchains Distributed Syst* (2018):77–81. doi:10.1145/3211933.3211947
6. Vallarano N, Tessone CJ, and Squartini T. Bitcoin Transaction Networks: An Overview of Recent Results. *Front Phys* (2020) 8:286. doi:10.3389/fphy.2020.00286
7. Bovet A, Campajola C, Mottes F, Restocchi V, Vallarano N, Squartini T, et al. The Evolving Liaisons between the Transaction Networks of Bitcoin and its price Dynamics. *arXiv:1907.03577 [physics, q-fin] ArXiv* (2019) 1907:03577.
8. Nakamoto S. *Bitcoin: A Peer-To-Peer Electronic Cash System* (2008). Available at SSRN: https://ssrn.com/abstract=3440802
9. Kalodner H, Goldfeder S, Chator A, Möser M, and Narayanan A. BlockSci: Design and Applications of a Blockchain Analysis Platform. *arXiv:1709.02489 [cs] ArXiv* (2017) 1709:02489.
10. Nick JD. *Data-Driven De-anonymization in Bitcoin. Tech. Rep.* Zurich: ETH Zurich (2015).
11. Harrigan M, and Fretter C. "The Unreasonable Effectiveness of Address Clustering". In 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld) (2016), 368–373. doi:10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0071
12. Fleder M, Kester MS, and Pillai S. Bitcoin Transaction Graph Analysis. *arXiv: 1502.01657 [cs] ArXiv* (2015) 1502:01657.
13. Zhang Y, Wang J, and Luo J. Heuristic-Based Address Clustering in Bitcoin. *IEEE Access* (2020) 8:210582–91. doi:10.1109/ACCESS.2020.3039570
14. Patel Y. *Deanonymizing Bitcoin Transactions an Investigative Study on Large-Scale Graph Clustering*. Princeton University Senior Theses, Princeton University (2018).
15. Ermilov D, Panov M, and Yanovich Y. Automatic Bitcoin Address Clustering. In: *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*. Mexico: Cancun IEEE (2017). p. 461–6. doi:10.1109/ICMLA.2017.0-118
16. Biryukov A, and Tikhomirov S. Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis. In: *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. Stockholm, Sweden: IEEE (2019). p. 172–84. doi:10.1109/EuroSP.2019.00022
17. Harlev MA, Sun Yin H, Langenheldt KC, Mukkamala RR, and Vatrapu R. Breaking Bad: De-anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning. In: *Proceedings of the 51st Hawaii International Conference on System Sciences 2018*. United States: Hawaii International Conference on System Sciences (HICSS) (2018). p. 3497–506. Proceedings of the Annual Hawaii International Conference on System Sciences.
18. [Dataset] Janda A. *WalletExplorer.com: Smart Bitcoin Block Explorer* (2017).
19. Barabási A-L, and Bonabeau E. Scale-Free Networks. *Sci Am* (2003) 288:60–9. doi:10.1038/scientificamerican0503-60
20. Raghavan UN, Albert R, and Kumara S. Near Linear Time Algorithm to Detect Community Structures in Large-Scale Networks. *Phys Rev E* (2007) 76:036106. doi:10.1103/PhysRevE.76.036106
21. Yang Z, Algesheimer R, and Tessone CJ. A Comparative Analysis of Community Detection Algorithms on Artificial Networks. *Sci Rep* (2016) 6: 30750. doi:10.1038/srep30750
22. Newman MEJ. Finding Community Structure in Networks Using the Eigenvectors of Matrices. *Phys Rev E* (2006) 74:036104. doi:10.1103/PhysRevE.74.036104
23. Pons P, and Latapy M. Computing Communities in Large Networks Using Random Walks. *Jgaa* (2006) 10:191–218. doi:10.7155/jgaa.00124
24. Blondel VD, Guillaume J-L, Lambiotte R, and Lefebvre E. Fast Unfolding of Communities in Large Networks. *J Stat Mech* (2008) 2008:P10008. doi:10.1088/1742-5468/2008/10/p10008
25. Newman MEJ, and Girvan M. Finding and Evaluating Community Structure in Networks. *Phys Rev E* (2004) 69. doi:10.1103/physreve.69.026113
26. Shannon CE. A Mathematical Theory of Communication. *Bell Syst Tech J* (1948) 27:379–423. doi:10.1002/j.1538-7305.1948.tb01338.x
27. Rosenberg A, and Hirschberg J. V-measure: A Conditional Entropy-Based External Cluster Evaluation Measure. In: *Proceedings of the 2007 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning (EMNLP-CoNLL)*. Prague, Czech Republic: Association for Computational Linguistics (2007). p. 410–20.

28. Cover TM, and Thomas JA. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. USA: Wiley-Interscience (2006).
29. Vinh NX, Epps J, and Bailey J. Information Theoretic Measures for Clusterings Comparison: Variants, Properties, Normalization and Correction for Chance. *J Machine Learn Res* (2010) 11:2837–54.
30. Rand WM. Objective Criteria for the Evaluation of Clustering Methods. *J Am Stat Assoc* (1971) 66:846–50. doi:10.1080/01621459.1971.10482356
31. Hubert L, and Arabie P. Comparing Partitions. *J Classification* (1985) 2: 193–218. doi:10.1007/BF01908075
32. Warrens MJ. On the Equivalence of Cohen's Kappa and the Hubert-Arabie Adjusted Rand Index. *J Classif* (2008) 25:177–83. doi:10.1007/s00357-008-9023-7
33. Cohen J. A Coefficient of Agreement for Nominal Scales. *Educ Psychol Meas* (1960) 20:37–46. doi:10.1177/001316446002000104
34. Liu X, Cheng H-M, and Zhang Z-Y. Evaluation of Community Detection Methods. *IEEE Trans Knowl Data Eng* (2019) 32:1. doi:10.1109/TKDE.2019.2911943
35. Clauset A, Shalizi CR, and Newman MEJ. Power-Law Distributions in Empirical Data. *SIAM Rev* (2009) 51:661–703. doi:10.1137/070710111
36. Maslov S. Specificity and Stability in Topology of Protein Networks. *Science* (2002) 296:910–3. doi:10.1126/science.1065103

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 06 July 2021
doi: 10.3389/fphy.2021.665399

Detecting Roles of Money Laundering in Bitcoin Mixing Transactions: A Goal Modeling and Mining Framework

Mingdong Liu[1], *Hu Chen*[2] *and Jiaqi Yan*[3]*

[1]School of Economics and Management, Southeast University, Nanjing, China, [2]School of Software Engineering, South China University of Technology, Guangzhou, China, [3]School of Information Management, Nanjing University, Nanjing, China

Cryptocurrency has become a new venue for money laundering. Bitcoin mixing services deliberately obfuscate the relationship between senders and recipients, making it difficult to trace suspicious money flow. We believe that the key to demystifying the bitcoin mixing services is to discover agents' roles in the money laundering process. We propose a goal-oriented approach to modeling, discovering, and analyzing different types of roles in the agent-based business process of the bitcoin mixing scenario using historical bitcoin transaction data. It adopts the agents' goal perspective to study the roles in the bitcoin money laundering process. Moreover, it provides a foundation to discover real-world agents' roles in bitcoin money laundering scenarios.

Keywords: goal modeling, money laundering, bitcoin mixing transactions, data analysis, agents' roles

OPEN ACCESS

Edited by:
Xiao Fan Liu,
City University of Hong Kong, SAR China

Reviewed by:
Daning Hu,
Southern University of Science and Technology, China
Hong-Liang Sun,
Nanjing University of Finance and Economics, China

***Correspondence:**
Jiaqi Yan
jiaqiyan@nju.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *08 February 2021*
Accepted: *07 May 2021*
Published: *06 July 2021*

Citation:
Liu M, Chen H and Yan J (2021) Detecting Roles of Money Laundering in Bitcoin Mixing Transactions: A Goal Modeling and Mining Framework. Front. Phys. 9:665399. doi: 10.3389/fphy.2021.665399

INTRODUCTION

Financial crimes not only directly disturb the national financial order and affect social stability but also occur with other crimes to provide financial support for various types of organized crimes. Money laundering is a financial criminal activity, which mainly refers to the processing of illegal income by various means to cover up and conceal its source and nature. It not only damages the security of the financial system and the reputation of financial institutions but also destroys the normal economic order and social stability of the country. Since money laundering is such a harmful activity, anti-money laundering is, therefore, a worthwhile endeavor.

Money laundering is a complex activity involving many entities and relationships. With the development of the Internet, money launderers utilize advanced technology and multiple channels to cover up their criminal behaviors through numerous transactions. Cryptocurrency has become a new venue for money laundering. The simplest form of bitcoin money laundering is that the bitcoin transactions are made under pseudonyms. Criminals use pseudonymous bitcoin addresses to hide the illegal source of funds. However, as studies have revealed that the pseudonyms of bitcoin addresses can be broken by aggregating addresses into clusters with identified users [1], more and more third-party bitcoin mixing services emerged to provide additional anonymity [2]. It is reported [3] that at least 4,836 bitcoins stolen by hacking Binance were laundered through the crypto mixing service.

The emergence of bitcoin mixing services makes it difficult to trace suspicious money flow as they deliberately obfuscate the relationship between senders and recipients [4]. However, there are limited existing studies investigating the bitcoin mixing services. The difficulties lie in detecting different roles of bitcoin addresses as there are an enormous number of bitcoin addresses involved. One of the earliest studies [5] on mixing services revealed that they bundle a large number of small transactions

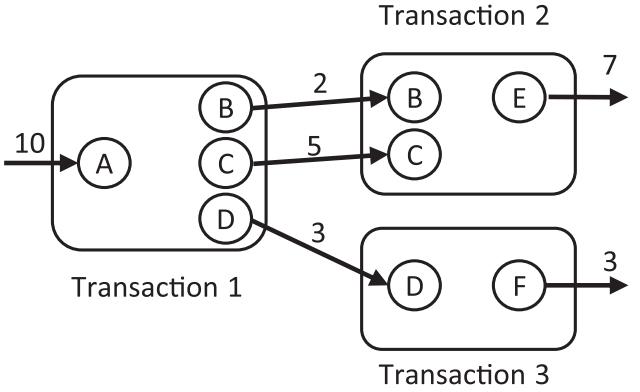


FIGURE 1 | UTXO-based transaction model.

into a small number of large transactions to create all outgoing transactions, hiding the connections between input addresses and output addresses.

In this article, we propose that the key to demystifying bitcoin mixing services is to discover agents' roles in the money laundering process. As money laundering is usually committed by collusive money launders, multiple agents are involved in the process. Different agents have different roles that perform different tasks in the bitcoin mixing process to achieve the ultimate goal of money laundering. Identifying the agents' roles in the bitcoin mixing process will be helpful to understand the context of bitcoin money laundering. In this paper, we propose a goal-oriented approach to modeling, discovering, and analyzing different types of roles in the agent-based business process of the money laundering scenario using historical transaction data from bitcoin mixing services. To the best of our knowledge, this paper is the first to apply goal-oriented modeling to represent the agents in bitcoin mixing transactions. It provides a foundation to understand the role and task assignment at cryptocurrency transactions in money laundering scenarios.

The rest of this paper is organized as follows. *Related Work* reviews *related works*. *Goal Modeling and Mining in Money Laundering* formalizes the problem and presents the framework. *Case Study* provides a case study and presents algorithms for goal mining in the money laundering processes. This article concludes with contributions and future research plans in *Conclusion*.

RELATED WORK

Cryptocurrency Transaction Analysis

A cryptocurrency transaction is a basic unit describing cryptocurrency flow from input to output addresses. Every input address in a cryptocurrency transaction is a reference to an unspent transaction output (UTXO), which is an output address in a previous transaction that has not been referenced in other transactions. In the bitcoin system, addresses are the basic identities that hold virtual values, which can be generated offline to a public key using the bitcoin's customized hash function. **Figure 1** presents a basic example of UTXOs. It is composed of three transactions. In Transaction 1, address A is the input with 10 BTC and B, C, and D are the output addresses. All outputs in Transaction 1 are UTXOs before they are referenced by Transactions 2 and 3.

As the complete transaction history is publicly available, the transparency of cryptocurrency transactions enables statistical analysis and graphical visualization techniques. Some scholars produced an organized review of major works in cryptocurrency transaction analysis. For example, Chen et al. [6] reviewed the status, trends, and challenges in blockchain data analysis and summarized seven typical research issues of cryptocurrency transaction analysis into entity recognition, privacy identification, network risk parsing, network visualization and portrait, analysis of cryptocurrency market, etc. Liu et al. [7] surveyed knowledge discovery in cryptocurrency transactions and summarized the existing research that uses data mining techniques into three aspects, including transaction tracing and blockchain address linking, the analysis of collective user behaviors, and the study of individual user behaviors.

Both reviews have identified many studies on transaction tracing, showing that the mechanism of the pseudonymity of cryptocurrency addresses used in transactions can be broken by entity recognition (or blockchain address linking) and privacy identification techniques. For example, to identify money laundering in bitcoin transactions, Hu et al. [8] proposed four types of classifiers based on the graph features that appeared on the transaction graph, including immediate neighbors, deep walk embedding, node2vc embedding, and decision tree-based. Once addresses are identified, money flows can be immediately revealed, leading to no anonymity in the bitcoin system.

Because the original design of bitcoin transactions is easy to trace, several solutions have been proposed to improve its anonymity. One typical solution is a mixing service, which is widely used in underground markets like the Silk Road to facilitate money laundering. Mixing services aim to solve cryptocurrencies' traceability issues by merging irrelevant transactions with methods including swapping and conjoining. Only a few previous works have been carried out to demystify mixing services. For instance, in one of the earliest studies on mixing services [5], a simple graph analysis was carried out based on data collected from experiments of selected mixing services, and alternative anti-money laundering strategies were sketched to account for imperfect knowledge of true identities. Although an essential anti-money laundering strategy is not provided, Seo et al. [2] mentioned that money laundering conducted in the underground market can be detected using a bitcoin mixing service. These explorations revealed the importance of understanding bitcoin mixing services.

Data Mining in Money Laundering

Money laundering is a complex, dynamic, and distributed process, which is often linked to terrorism, drug and arms trafficking, and exploitation of human beings. Detecting money laundering is notoriously difficult, and one promising method is data mining [9]. Rohit and Patel [10] reviewed detection of suspicious transactions in anti-money laundering using a data mining framework and classified the literature into the rule-based approach, clustering-based approach, classification-based approach, and model-based approach.

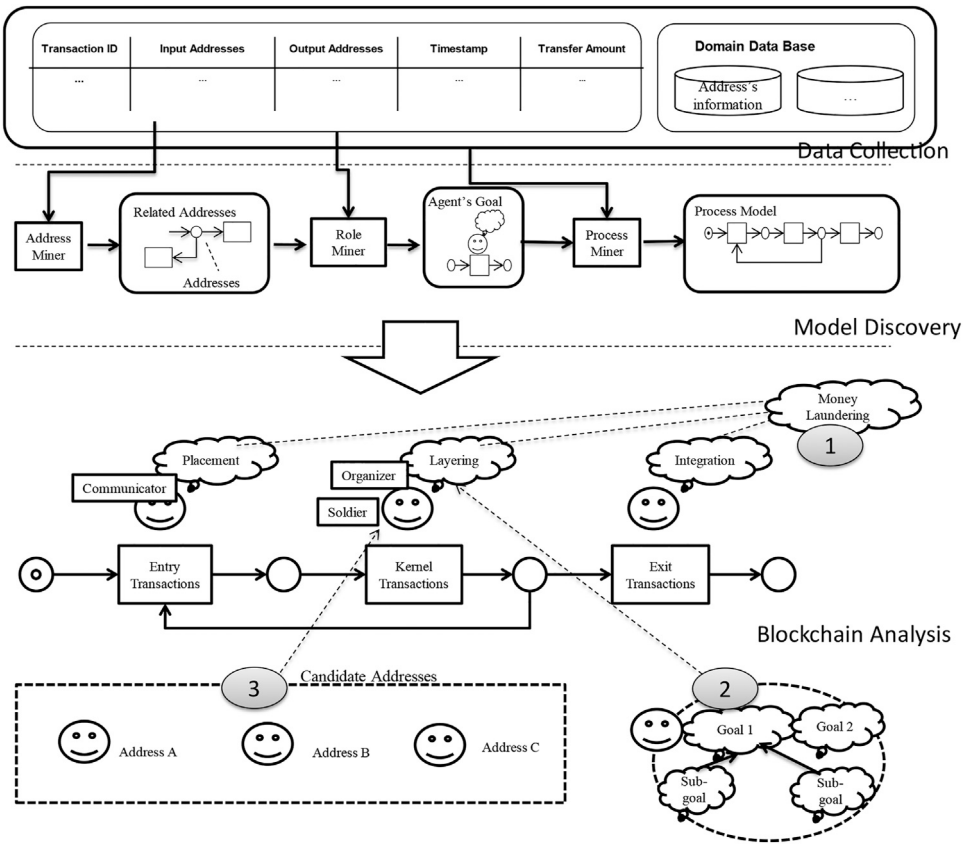


FIGURE 2 | Goal modeling and mining framework.

Generally, data mining in money laundering consists of the rule-based classification and machine learning approaches. In a rule-based approach, ontologies or other forms of rules are adopted to classify suspicious transactions. For instance, Rajput et al. [11] proposed an ontology-based expert system for suspicious transaction detection. The ontology consists of domain knowledge and a set of Semantic Web rules, and the native reasoning support in the ontology was used to deduce new knowledge from the predefined rules about suspicious transactions. A Secure Intelligent Framework for Anti-Money Laundering was presented to make use of an intelligent formalism by using ontologies and rule-based planning [12]. Bayesian approaches were adopted to assign a risk score to money laundering–related behavior [13]. It was designed based on rules suggested by the State Bank of Pakistan in its 2008 regulations to declare a transaction as suspicious.

Machine learning algorithms were also applied to group or classify the data, so as to predict suspicious money laundering transactions. Chen et al. [14] provided a comprehensive survey of machine learning algorithms and methods applied to detect suspicious transactions, including typologies, link analysis, behavioral modeling, risk scoring, anomaly detection, and geographic capability. A support vector machine–based classification system was developed to handle large amounts of data and take the place of traditional predefined-rule suspicious transaction data–filtering systems [15]. However, the limitation of the machine learning approach lies in its data dependence, with sometimes limited adaptability and scalability. As stated in [6], the model requirement of historical data makes it difficult to identify illicit operations performed by newcomers.

GOAL MODELING AND MINING IN MONEY LAUNDERING

In this section, we propose to model agents' roles in the money laundering process with goal-oriented modeling techniques. We adopt the goal modeling and mining approach [16] and assume that different agents have different roles, which perform different tasks in the process to achieve the ultimate goal of money laundering. As shown in **Figure 2**, the goal modeling and mining framework consists of three phases. In the data collection phase, we will collect not only cryptocurrency transaction data but also the domain data about the address entity information. The model discovery phase consists of the address miner, role miner, and process miner. The address miner will collect all related address information. The role miner will detect the goals of the agent who owns the addresses. The process miner will present the money laundering process.

In the blockchain analysis phase, we first analyze the goal of money laundering, which can be decomposed into three

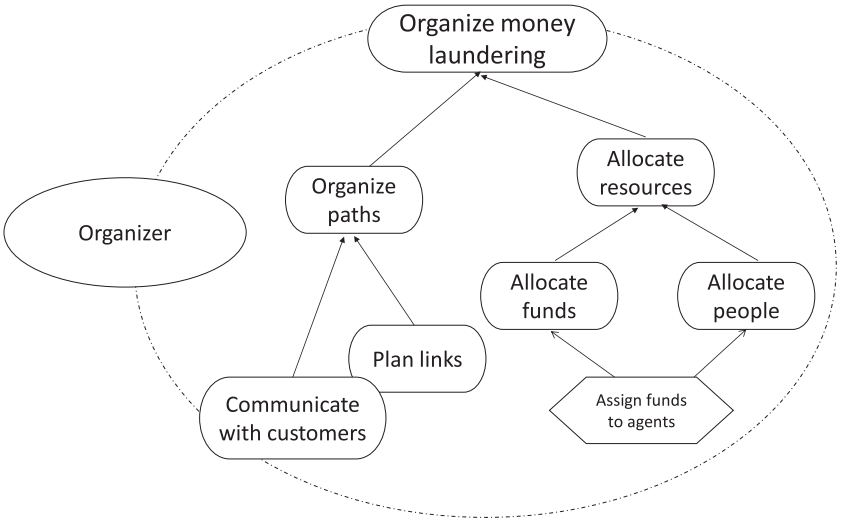


FIGURE 3 | Goal modeling of the organizer.

sub-objectives, **namely, placement, layering, and integration.** Placement aims to cut off the connections between illegal funds and upstream crimes of money laundering. It can be realized by the task of introducing illegal funds into the financial system. This task can be decomposed into sub-tasks like depositing money or remitting cash. Placement always involves breaking down the original large amount of funds into a lot of small ones. So, many soldiers will be employed to execute the tasks to introduce multiple illegal funds into the financial system without suspicion.

Layering is transferring the funds among different accounts or institutions so that the initial source of funds will be difficult to track. Layering can be realized by the task of obscuring the sources of the money. This can be decomposed into sub-tasks like transferring money or purchasing insurance from different institutions. Layering means that funds have entered the financial system for circulation. Soldiers may continue to do a lot of basic tasks, while communicators' main role is to transfer the funds.

Integration means to integrate the funds into the legitimate economy. Integration can be realized by the task of legalizing illegal funds. This task can be decomposed into sub-tasks like transferring money or purchasing insurance from different institutions, transferring overseas, withdrawing cash, or investing. Finally, the legalized funds will be possessed by the money laundering organizers. Communicators and organizers will work together to complete the task.

In the money laundering process, three roles are involved, as follows:

1) Organizer: Organizers are the core of the organization. As described in **Figure 3**, the organizer's goal is to organize money laundering, which can be decomposed to allocate resources and organizing paths. The goal of allocate resources can be decomposed into allocate funds and allocate people, which can be realized by the tasks of assign funds to agents. The goal of organizing paths can be realized by the task of assign funds to agents. The goal of organizing paths can be decomposed into communicate with customers and plan links.

Organizers organize the money laundering process collaborating with communicators and soldiers. Particularly, as shown in **Figure 4**, the organizer depends on communicators to communicate with customers while depending on soldiers to assign funds to agents. Communicators execute tasks from the organizer and employ soldiers to introduce illegal assets into the financial system.

2) Communicator: Communicators are at the middle level of the organization. The communicator's goal is to transmit information in the money laundering activity. The goal of transmitting information can be realized by the task of communicate with customers, which can be decomposed to inputs and outputs for customers.
3) Soldier: The soldier's goal is to become agents with chips. In **Figure 5**, soldiers are employed by the organizer to deal with some basic tasks. They are not related to the core organization, while they are the key to facilitate the flow of illegal funds into the financial system. The goal of agents with chips can be realized by the task of split funds and assign chips.

CASE STUDY

In this section, we present a case study to demonstrate the proposed framework. We investigated a popular mixing service. In this bitcoin mixing service, the smallest unit of deposit is 0.001 BTC. As shown in **Figure 5**, the deposit is divided into different chips, which are $2^k \times 0.001$ BTC. Users can send these chips to one or more different withdrawal addresses, as shown in **Figure 5**. In our experiment, we sent all five chips of 0.031 BTC to one withdrawal address.

We tracked withdrawal transactions through the btc.com website. In **Figure 6**, the box represents the address and the oval box represents the transaction (the text is the transaction time). The value on the line between the address and the transaction represents

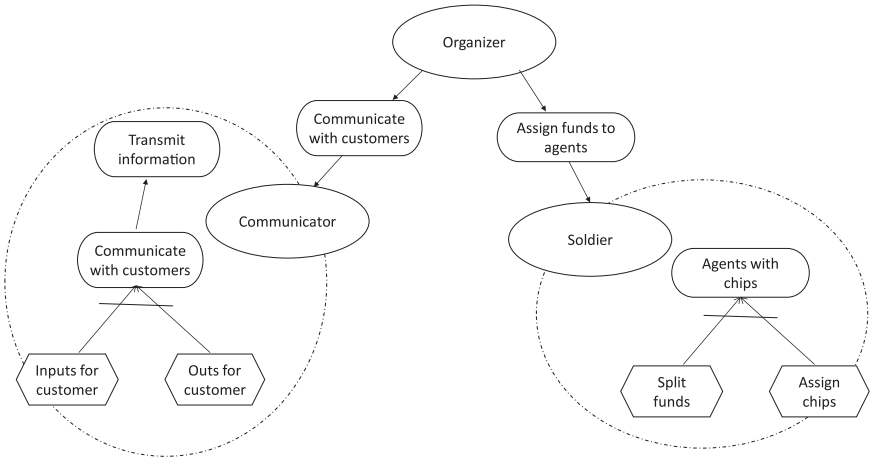


FIGURE 4 | Relationship between roles.

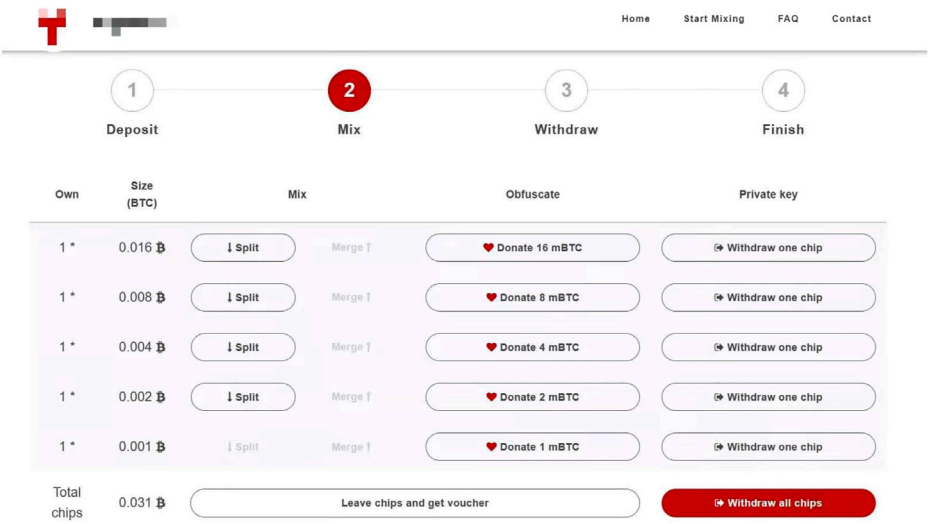


FIGURE 5 | 0.031 BTC is divided into five chips in a bitcoin mixing service.

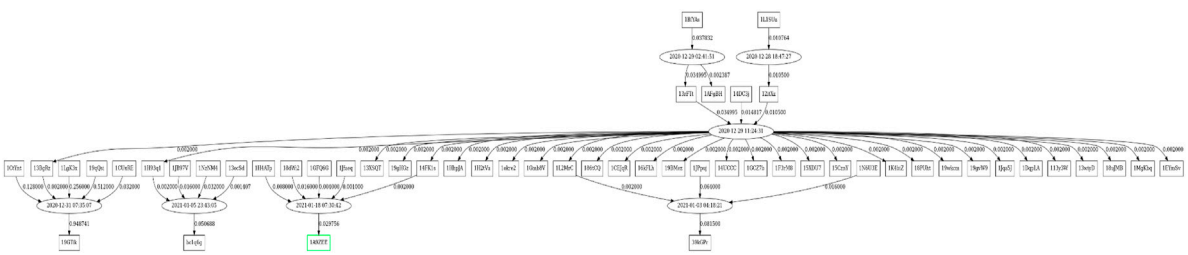


FIGURE 6 | Withdrawal transactions.

the bitcoin value that the address entered or output in this transaction. The address in green is our export address. We noticed that there are five exit addresses in the money laundering network, which are consistent with the chip division. These five addresses seem to correspond to five address pools of different amounts. We selected three other addresses in the address pool

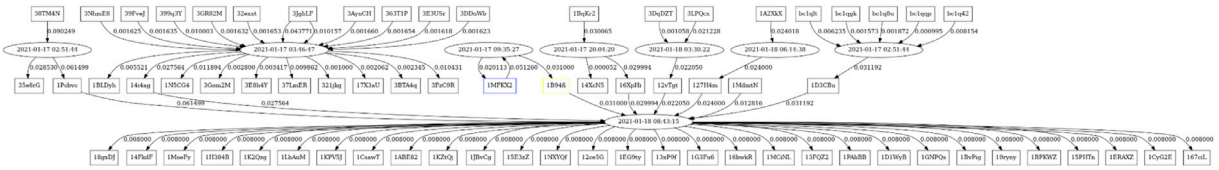


FIGURE 7 | Deposit transactions.

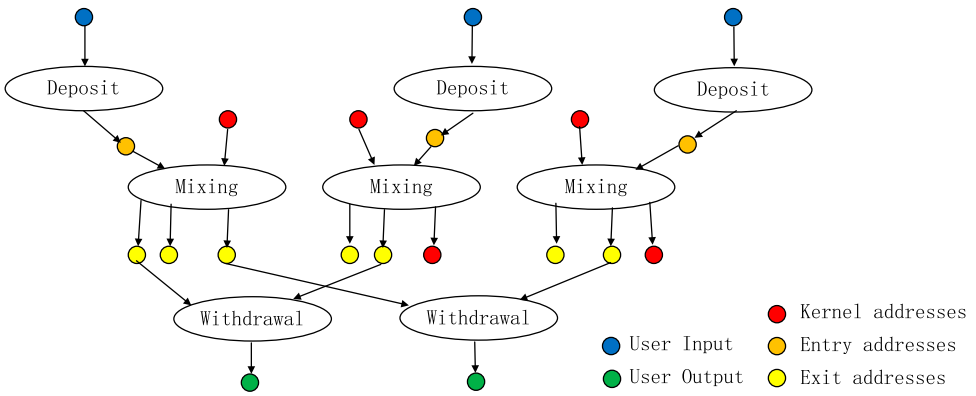


FIGURE 8 | Different tasks in the bitcoin mixing service.

with a bitcoin amount of 0.002 and found that these transactions were also combined to produce output from different address pools.

Deposit transactions are shown in **Figure 7**. In the figure, purple denotes the source address of the experiment and yellow–green is the entry address provided by the bitcoin mixing service. It can be seen that the money laundering entry address in this experiment is directly used to generate an address pool of 0.008 BTC.

As shown in **Figure 8**, we find that there are three categories of addresses: ***entry addresses (communicator), exit addresses (communicator),*** and ***kernel addresses (soldier).*** When a laundering request is issued, it will generate an *entry address* to receive the bitcoin from a user. After a while, some entry addresses and *kernel addresses* are combined as the inputs of one mixing transaction to generate some *exit addresses*. An important feature of the exit addresses is that their amount is 2^k×0.001 BTC. When it decides to send Y×0.001 BTC to one laundering output address, some *exit addresses* are selected according to Y. For example, if $Y = 0.031 = (16 + 8 + 4 + 2 + 1) \times 0.001$ BTC, then five addresses holding 0.016, 0.008, 0.004, 0.002, and 0.001 BTC are selected from its pools. These *exit addresses* are treated as inputs for a withdrawal transaction to send to the output address specified by the user.

Definitions for Identifying the Mixing Transactions

The transaction T with m input addresses $(a_1^I, \ldots, a_m^I)$ and n output addresses $(a_1^O, \ldots, a_n^O)$ is described as follows:

$$(a_1^I, c_1^I), \ldots, (a_m^I, c_m^I) \rightarrow (a_1^O, c_1^O), \ldots, (a_n^I, c_n^O), \tag{1}$$

where c_i^I and c_j^O $(1 \le i \le m, 1 \le j \le n)$ are the amount of input address a_i^I and output address a_j^O, respectively. Obviously, $\sum_{i=1}^{m} c_i^I \ge \sum_{j=1}^{n} c_i^O$. And the fee of T is $\sum_{i=1}^{m} c_i^I - \sum_{j=1}^{n} c_i^O$.

For a transaction T, the set of input addresses is defined as $A^I(T) = \{a_1^I, \ldots, a_m^I\}$ and the set of output addresses is defined as $A^O(T) = \{a_1^O, \ldots, a_n^O\}$.

Actually, we find two types of mixing transactions to generate the exit addresses, defined as follows:

[Definition 1] A transaction T with n outputs is type I transaction, if $c_j^O = 2^k$×0.001 BTC $(1 \le j \le n)$ and n>1.

[Definition 2] A transaction T with n outputs is type II transaction, if $c_j^O = 2^k$×0.001 BTC $(1 \le j \le n\text{-}1)$, $c_n^O \ne 2^l \times 0.001$ BTC, and n>2.

The withdrawal transactions are based on the *exit addresses*, described as follows:

[Definition 3] A transaction T with m inputs and one output is a *withdrawal transaction*, if

1. $c_i^I \ne c_j^I$, $i \ne j$, $1 \le i,j \le m$;
2. $c_i^I = 2^k$×0.001 BTC, $1 \le i \le m$ *or* m-1.

We design **Algorithm 1** to find the mixing transactions. There are three stages in the algorithm. The first stage (step 1) is to find all type I or II transactions T_1. In stage 2 (steps 2–10), we try to find the withdrawal transactions T_2 based on T_1. In the last stage, the transactions in T_1 are selected as the mixing ones according to T_2.

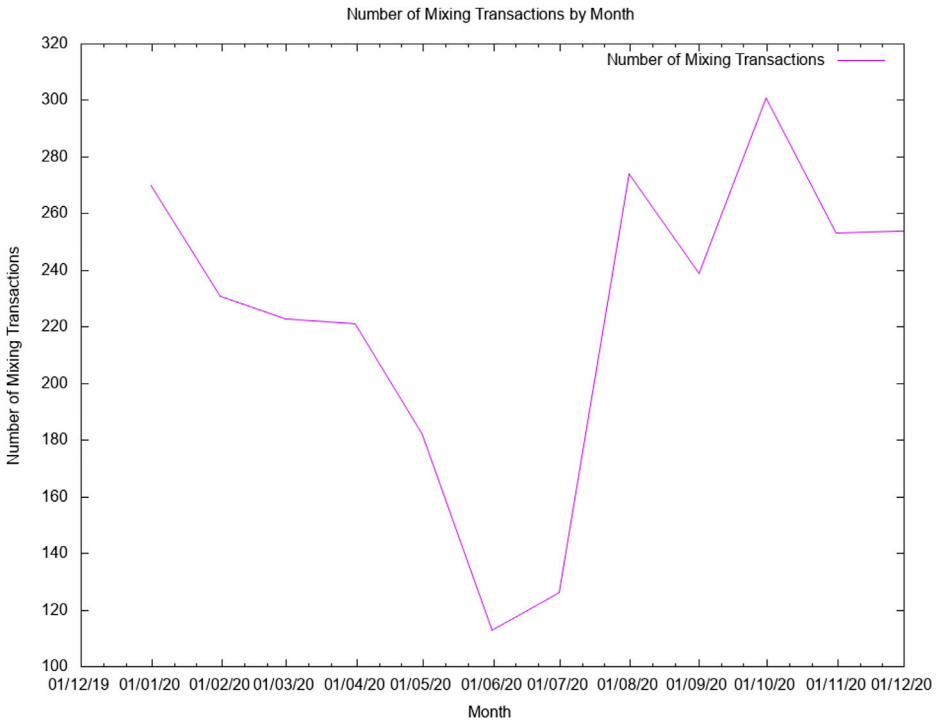


FIGURE 9 | The number of mixing transactions in each month of 2020.

Algorithm 1

Input: T, bitcoin transaction set from t_0 to t_1

Output: T_C, detected mixing transactions

1. Finding transaction set T_1 from T, where $t \in T_1$ is type I or type II transaction.
2. $T_2=\emptyset$
3. for each $T \in T$ - T_1
4. if T is *withdrawal transaction* then
5. if $c_i^I=2^k\times0.001$BTC **and** $a_i \in A^O(T_i)$ **and** $a_i \in A^I(T)$, $T_1 \in T_1$, $1 \le i \le m$ then
6. $T_2=T_2 \cup \{T\}$
7. endif
8. endif
9. endfor
10. $T_C=\emptyset$
11. for each $T \in T_1$
12. if all outputs of T are the inputs of some transactions in T_2
13. $T_C=T_C \cup \{T\}$
14. endif
15. endfor

Kernel addresses appear in different mixing transactions as the inputs. We use **Algorithm 2** to find them.

Algorithm 2

Input: T_C, detected mixing transactions

Ouput: A_k, kernel addresses

1. $A_k=\emptyset$
2. for each $T \in T_C$
3. for each $T_s \in T_C$, **and** $T_s \neq T$
4. $A_k=A_k \cup (A^I(T) \cap A^I(T_s)$

In the 2020 BTC transactions, we find 4,689 type I transactions and 3,124 type II transactions. With **Algorithm 1**, we determine that 2,687 are mixing transactions with 47,433 associated withdrawal transactions. The number of mixing transactions in each month of 2020 is shown in **Figure 9**.

With **Algorithm 2**, we find 2,451 kernel addresses, of which 2,143 (87%) are in one wallet [0005190b7a] according to walletexplorer.com. This proves that these addresses we discovered belong to an organization that has not been revealed before and can prove to be controlled by the mixing service provider.

We tracked money laundering transactions and discovered the transaction structure. From historical bitcoin transactions, we found a large number of mixing transactions with significant characteristics and kernel addresses related to the bitcoin mixing service. We can estimate the scale of money laundering based on such role analysis.

CONCLUSION

In this paper, we propose that the key to demystifying bitcoin mixing services is to discover agents' roles in the money laundering process and present a goal-oriented modeling framework to model different roles in the money laundering process. The framework consists of data collection, model discovery, and blockchain analysis. With this framework, the three roles of the organizer, soldier, and communicator are analyzed in the money laundering process of placement, layering, and integration.

We then apply the proposed framework to investigate a popular bitcoin mixing service. Specifically, we identify two types of mixing transactions to generate the exit addresses. We propose two algorithms to analyze the roles of the soldier and communicator in the money laundering process. With the identified roles, we can

estimate the scale of money laundering in the bitcoin mixing service.

DATA AVAILABILITY STATEMENT

The raw data supporting the conclusions of this article will be made available by the author, without undue reservation.

AUTHOR CONTRIBUTIONS

ML: Software, Investigation, Case Implementation, Validation, Methodology, Conceptualization. HC: Validation, Software, Data Curation, Case Implementation, Formal analysis, JY: Conceptualization, Editing, Visualization, Review, Supervision.

REFERENCES

1. Reid F, and Harrigan M. *An Analysis of Anonymity in the Bitcoin System. 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing* (2011). p. 1318–26. doi:10.1109/PASSAT/SocialCom.2011.79 An Analysis of Anonymity in the Bitcoin System.
2. Seo J, Park M, Oh H, and Lee K. "Money Laundering in the Bitcoin Network: Perspective of Mixing Services," in 2018 International Conference on Information and Communication Technology Convergence (ICTC) (2018) 1403–1405. Available at: https://www.researchgate.net/publication/329491846_Money_Laundering_in_the_Bitcoin_Network_Perspective_of_Mixing_Services. doi:10.1109/ictc.2018.8539548
3. Maria O. Chipmixer Used To Launder BTC from Recent Binance Hack. *Cryptocurrencynews* (2019). Available at: https://cryptocurrencynews.com/chipmixer-binance-hack-btc-laundering/ (Accessed May 30, 2021).
4. Wu L, Hu Y, Zhou Y, Wang H, Luo X, Wang Z, et al. *Towards Understanding and Demystifying Bitcoin Mixing Services* (2020).
5. Möser M, Böhme R, and Breuker D. An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. *2013 APWG ECrime Researchers Summit* (2013) 1–14. doi:10.1109/eCRS.2013.6805780
6. Chen Z, Van Khoa LD, Teoh EN, Nazir A, Karuppiah EK, and Lam KS. Machine Learning Techniques for Anti-money Laundering (AML) Solutions in Suspicious Transaction Detection: A Review. *Knowl Inf Syst* (2018) 57: 245–285. doi:10.1007/s10115-017-1144-z
7. Liu XF, Jiang X-J, Liu S-H, and Tse CK. Knowledge Discovery in Cryptocurrency Transactions: A Survey. *IEEE Access* (2021) 9:37229–37254. doi:10.1109/ACCESS.2021.3062652
8. Hu Y, Seneviratne S, Thilakarathna K, Fukuda K, and Seneviratne A. *Characterizing and Detecting Money Laundering Activities on the Bitcoin Network* (2019). ArXiv:1912.12060 [Cs]. Available at: http://arxiv.org/abs/1912.12060 (Accessed May 30, 2021).
9. Watkins RC, Reynolds KM, Demara R, Georgiopoulos M, Gonzalez A, and Eaglin R. Tracking Dirty Proceeds: Exploring Data Mining Technologies as Tools to Investigate Money Laundering. *Police Pract Res* (2003) 4(2):163–78. doi:10.1080/15614260308020
10. Rohit KD, and Patel DB. Review on Detection of Suspicious Transaction in Anti-money Laundering Using Data Mining Framework. *Int J Innovative Res Sci Technol* (2015) 1(8):129–133.
11. Rajput Q, Khan NS, Larik A, and Haider S. Ontology Based Expert-System for Suspicious Transactions Detection. *Comp Inf Sci* (2014) 7(1):103–114. doi:10.5539/cis.v7n1p103
12. Sobh TS. An Intelligent and Secure Framework for Anti-money Laundering. *J Appl Security Res* (2020) 15(4):517–46. doi:10.1080/19361610.2020.1812994
13. Khan NS, Larik AS, Rajput Q, and Haider S. A BAYESIAN APPROACH FOR SUSPICIOUS FINANCIAL ACTIVITY REPORTING. *Int J Comput Appl* (2015) 35(4):181–7.
14. Chen W, Zheng Z, Fronzetti Colladon A, and Remondi E. Blockchain Data Analysis: A Review of Status, Trends and Challenges Using Social Network Analysis to Prevent Money Laundering. *J Comp Res Development Expert Syst Appl* (2017) 5567(9):185349–7058. doi:10.1016/j.eswa.2016.09.029
15. Tang J, and Yin J. *Developing an Intelligent Data Discriminating System of Anti-money Laundering Based on SVM.* Machine Learning And Cybernetics *Proceedings of 2005 International Conference on* (2005).
16. Yan J, Hu D, Liao S, and Wang H. Mining Agents' Goals in Agent-Oriented Business Processes. *ACM Trans Manag Inf Syst* (2015) 5(4):20–120.22. doi:10.1145/2629448

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 27 October 2021
doi: 10.3389/fphy.2021.720708

Heterogeneous Preferential Attachment in Key Ethereum-Based Cryptoassets

Francesco Maria De Collibus [1]*, *Alberto Partida* [2], *Matija Piškorec* [1,3] and *Claudio J. Tessone* [1,4]

[1]Blockchain and Distributed Ledger Technologies Group, Universität Zürich, Zürich, Switzerland, [2]International Doctoral School, Rey Juan Carlos University, Madrid, Spain, [3]Rudjer Boskovic Institute, Zagreb, Croatia, [4]UZH Blockchain Center, Universität Zürich, Zürich, Switzerland

In this study, we analyse the aggregated transaction networks of Ether (the native cryptocurrency in Ethereum) and the three most market-capitalised ERC-20 tokens in this platform at the time of writing: Binance, USDT, and Chainlink. We analyse a comprehensive dataset from 2015 to 2020 (encompassing 87,780,546 nodes and 856,207,725 transactions) to understand the mechanism that drives their growth. In a seminal analysis, Kondor et al. (PLoS ONE, 2014, 9: e86197) showed that during its first year, the aggregated Bitcoin transaction network grew following linear preferential attachment. For the Ethereum-based cryptoassets, we find that they present in general super-linear preferential attachment, i.e., the probability for a node to receive a new incoming link is proportional to k^{α}, where k is the node's degree. Specifically, we find an exponent $\alpha = 1.2$ for Binance and Chainlink, for Ether $\alpha = 1.1$, and for USDT $\alpha = 1.05$. These results reveal that few nodes become hubs rapidly. We then analyse wealth and degree correlation between tokens since many nodes are active simultaneously in different networks. We conclude that, similarly to what happens in Bitcoin, "the rich indeed get richer" in Ethereum and related tokens as well, with wealth much more concentrated than in-degree and out-degree.

Keywords: preferential attachment, wealth, complex networks, Ethereum, Bitcoin, token, cryptocurrencies

OPEN ACCESS

Edited by:
Jianguo Liu,
Shanghai University of Finance and Economics, China

Reviewed by:
Zhen Wang,
Hangzhou Dianzi University, China
Jie Cao,
Nanjing University of Finance and Economics, China

***Correspondence:**
Francesco Maria De Collibus,
francesco.decollibus@business.uzh.ch

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *04 June 2021*
Accepted: *14 September 2021*
Published: *27 October 2021*

Citation:
De Collibus FM, Partida A, Piškorec M and Tessone CJ (2021) Heterogeneous Preferential Attachment in Key Ethereum-Based Cryptoassets. Front. Phys. 9:720708. doi: 10.3389/fphy.2021.720708

1 INTRODUCTION

Bitcoin and Ethereum are the two pioneering blockchain-based platforms. Nakamoto [1] created Bitcoin: the first and most popular cryptocurrency system since its launch in January 2009 and, so far, the one with the highest market capitalisation according to coinmarketcap [2]. Launched in 2015, Ethereum [3] is the second most popular public permissionless blockchain platform and the second most capitalised according to coinmarketcap [2]. Ethereum is considered "the world's distributed computer": the first platform to implement *smart contracts*, i.e., Turing-complete programs. This is pivotal for many new decentralised applications such as decentralised finance (DeFi).

At the intersection among economics, technology, and social sciences, Popper [4] states that blockchains constitute an inspiring and emerging research field since the original inception of Bitcoin by Nakamoto [1]. The use of blockchain-based distributed ledgers in our society grows steadily. On one side, Bitcoin is one of the fastest-growing assets in history, with market capitalisation records broken successively in the past. On the other side, blockchain is being successfully introduced in a wide array of use cases, ranging from secure voting to supply chain tracking. The vast majority of

currently available crypto-currencies uses a public distributed ledger based on a blockchain to transact and exchange value [5,6]. All transactions are registered in a readable distributed ledger, in such a way that anyone connected to the peer-to-peer network can verify independently the validity of the executed transactions.

Blockchains offer a new research opportunity to better analyse and understand complex social and economic systems. Access to transactions occurring in traditional payment systems is usually restricted: traditional exchanges remain confidential, protected by privacy laws, or trade secrets. Digital payments with credit cards and wire transfers carry a similar limitation, while payments with physical cash are *de facto* impossible to track on a massive scale. In contrast, transactions in a public blockchain are visible by definition, only limited by the pseudo-anonymity of the users as described by Reid and Harrigan [7]. The additional research boundary is the considerable amount of data that blockchain implementations produce when they are massively adopted. Extant research by [8–11] shows that market value growth has accelerated in parallel to the number of users and transactions. While in some cases, like in Bitcoin, the rate of data production is currently bounded by the limits imposed by design choices (block size, inter-block time), and in other systems, transaction data increase massively throughout time (like in Ethereum). The use of networks to describe interactions is a powerful resource: in our case, we represent Ethereum transaction data using a network of nodes (public addresses) interconnected by edges (transactions).

Network science refers to an interdisciplinary approach that helps to characterise complex systems composed of many interacting constituents. This approach permitted to unveil large-scale emergent properties in the most varied disciplines, ranging from biology to social sciences, and specifically socio-technical and economic and financial systems [12–17].

Growth in a wide range of networked systems presents a network version of the "rich-get-richer" effect. In terms of degree, this mechanism implies that nodes with a higher degree accrue links at a higher rate than lower-degree nodes. Price [18] calls this effect as *"cumulative advantage"*; Barabási and Albert [19]; Albert and Barabási [20]; Barabási and Pósfai [12] refer to it as *"preferential attachment"* (PA). This effect usually creates power-law degree distributions, facilitating the mathematical characterisation of a growth pattern in complex networks [21]. In practice, preferential attachment refers to the specific case in which the probability of receiving a new link is directly proportional to the node's degree k, producing a scale-free network characterised by a power-law degree distribution $p_k \sim k^{-\gamma}$ with exponent $2 \leq \gamma \leq 3$, as in Barabási and Pósfai [12]; Alstott et al. [22]. However, extensions of the model such as Krapivsky et al. [23] show that the emergent topology changes when the probability of a node to receive new links is a nonlinear function of the node's degree: while highly connected nodes in networks with sublinear PA do not play such a decisive role in network growth, in the case of networks showing super-linear PA, few nodes act like hubs and tend to connect to most network nodes (i.e., the network topology concentrates around *superhubs*).

Public blockchains are current examples of complex systems which are increasingly researched through complex network approaches Vallarano et al. [11]. By analysing a complete and unique dataset encompassing the first 5 years of Ethereum platform, i.e., 856,207,725 transactions and 87,780,546 addresses, we show that the native cryptocurrency of the Ethereum platform, Ether, and the most active tokens on it show a form of preferential attachment, with signs of super-linear PA.

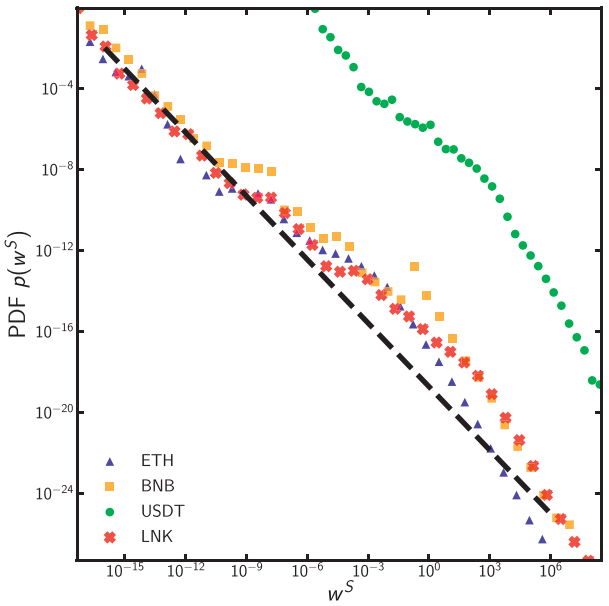


FIGURE 1 | PDF of wealth w^S for $w^S > 0$ in various tokens: ETH, BNB, USDT, and LNK. The dashed line (w^{-1}) is just added for visual reference.

This study is structured as follows. In **Section 2**, we review related literature on complex network approaches to understand cryptocurrencies and blockchain-based systems. **Section 3** presents the analysed dataset. In **Section 4**, we introduce the methodology while in **Section 5**, we display the results of empirical distributions of wealth and in- and out-degrees. We share the results for the nonlinear preferential attachment analysis in **Section 6**. Finally, in **Section 7**, we present the conclusions of this analysis.

2 RELATED LITERATURE

In [24,25], the authors analyse aggregated representations of the Bitcoin transaction network. They observe that highly connected nodes increase their connectivity with new edges either by receiving new transactions (in-degree) or starting new transactions (out-degree). Using a statistical approach based on rank, they conclude that the growth of the degree distribution in the Bitcoin transaction network displays linear preferential attachment (PA). They also identify that addresses with high balance increase their wealth more than addresses with low balance displaying a sublinear preferential attachment. In addition, they find that the in-degree of a node, i.e., the number of transactions received by an

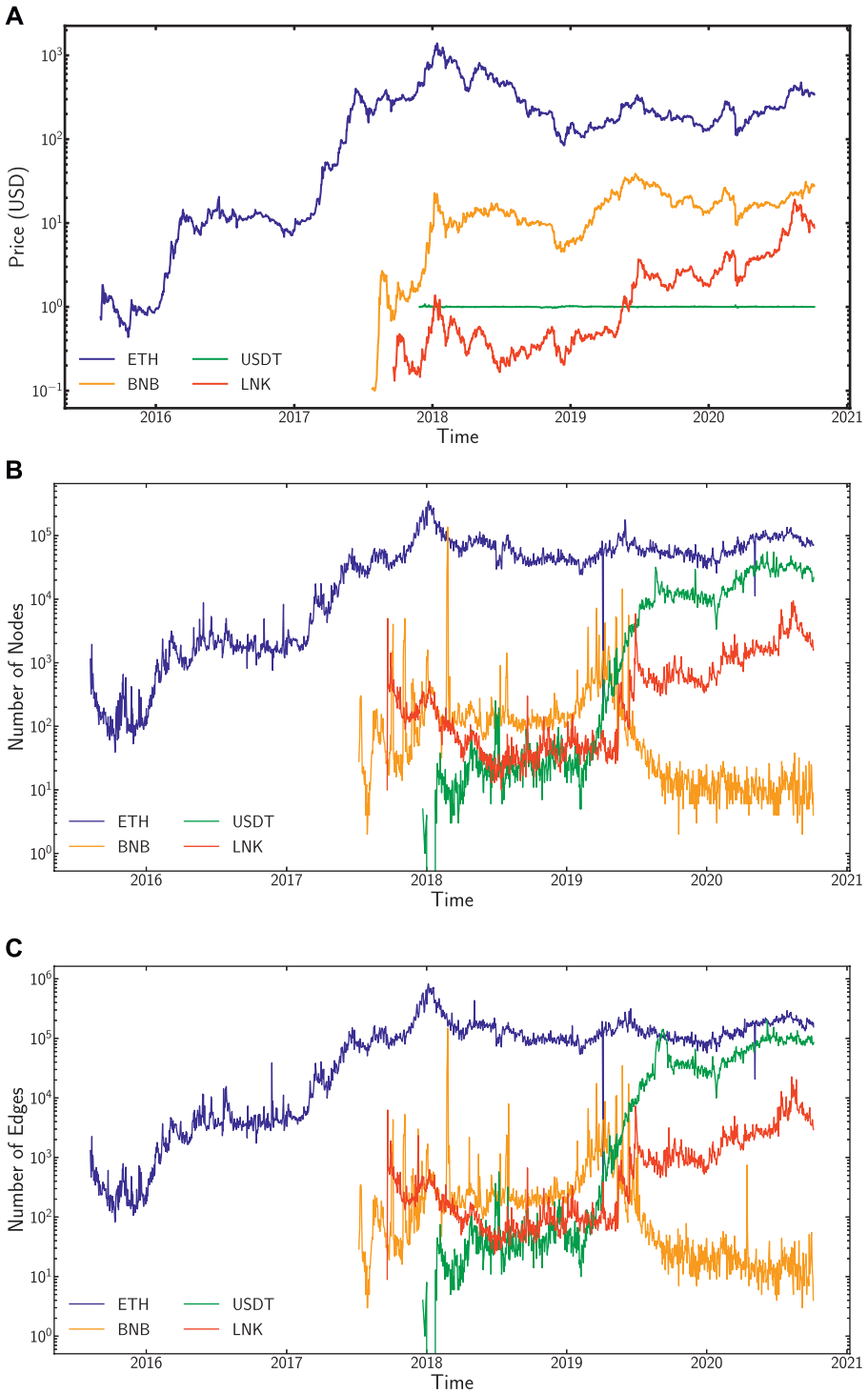


FIGURE 2 | We plot basic statistics of the data analysed. In the **(A),** we show, as a function of time the closing daily market price of ETH, BNB, USDT, and LNK in US Dollars. For the tokens, the time series begins with the deployment of the smart contract into the blockchain. In the **(B,C),** we show the number of new nodes (resp., edges) every day for the aggregate network introduced in this study.

address, is positively correlated with the Bitcoin balance of that address. Wealth distribution per address is highly heterogeneous, but this distribution is stable at different points of time. Instead of a power-law distribution, Kondor et al. [24] find for the majority of the samples a better approximation in the stretched exponential distribution.

With a focus on wealth, the Gini coefficient is computed over time, and they find that $G \approx 0.9$.

Bovet et al. [9] analyse more properties of the Bitcoin transaction network. The study includes more than 283M transactions between 304M addresses which can be reduced to around 16M users. The technical process to analyse data of this size is explained in Sommer [26]. They observe that when many users behave similarly by creating the same connectivity pattern (i.e., they display a sharper degree distribution with an increase in both number of links and number of nodes), then there are price surges. Once the price peak of a bubble is passed, the heterogeneity of the degree distribution of different participants widens. In their introduction, Bovet et al. [9] present four graphs that show features of the Bitcoin network: number of nodes, number of links, density, and price along a temporal axis. We follow a similar approach to introduce the four Ethereum-based transactions networks that we study in **Figure 2** and **Figure 3**.

A basic although crucial lesson learned from the literature review on Ethereum network analysis is indeed the very fast pace of change in this platform. Liang et al. [27] present a dynamic network analysis of three representative blockchain-based cryptocurrencies: Bitcoin, Ethereum, and Namecoin. The authors construct separate networks on a monthly basis, and they trace changes of typical network characteristics over time, including degree distribution, degree assortativity, clustering coefficient, and the largest connected component. They compare the three networks and conclude that the degree distribution of these monthly transaction networks cannot be fitted well by a power-law distribution. In addition, they find that both Bitcoin and Ether (ETH) networks are heavy-tailed with disassortative mixing; however, only the former can be treated as a "small world", i.e., most vertices can be reached from the others through a small number of edges. These network properties reflect the evolutionary characteristics and competitive power of these three cryptocurrencies. The dataset comprises of approximately 80M transactions from 2015 to late 2017. They identify a continuously increasing average degree except for a decrease in October 2016, when the network showed instability caused by several denial-of-service (DoS) attacks. They study the transaction volume and state that most of the users have limited incoming transactions while a small population receives a large amount of ETH. Liang et al. [27] identify that these cryptocurrency networks do not obey the densification law, and they argue that a plausible explanation is the minimal reuse of addresses (which is a standard practice in UTXO-based systems). They find that almost all degree distributions cannot be accepted as a power-law but still as a clear heavy-tailed distribution, which means that the majority of addresses have low degrees, while a small but not negligible number of addresses have relatively high degrees. Guo et al. [28] use a more reduced ETH datasets, one containing 100,000 blocks from 2015, and ca. 680,000 transactions and another containing 610,000 transactions from 2017. They find that the typical distance between any pair of anonymous users is extremely small, and the Ether paid by one node may return at a relatively high speed. As a result, they claim that ETH enjoys a good level of liquidity.

TABLE 1 | Summary of the different datasets analysed by different authors.

References	Token	Transactions (M)
Bovet et al. [9]	BTC	283
Liang et al. [27]	ETH	80
Guo et al. [28]	ETH	1.29
Kondor et al. [24]	BTC	17
This study	ETH	856

TABLE 2 | Summary of the datasets analysed in this study.

Token	Nonzero Txs	Addresses	ETH blocks
ETH	414 M	87 M	0–11 M
BNB	934 K	481 K	0–11 M
USDT	60 M	9 M	0–11 M
LNK	5 M	784 K	0–11 M

Somin et al. [29] provide the first analysis of the network properties of ERC-20 protocol-compliant tokens trading data. They analyse the properties of the transaction network by considering all trading wallets (i.e., addresses) as network nodes and constructing its edges using buy–sell trades. They examine several time periods and several data aggregation variants to demonstrate that the transaction network displays strong power-law properties. Both outgoing and incoming degrees present a power-law distribution. This means that most tokens are traded by an extremely small number of users. Only a few popular tokens are traded by a very large group of users during the examined time span. These results coincide with current network theory expectations. Somin et al. [29] provide the first scientific complex network validation for the ERC-20 trading data. The data they examine are composed of over 30 million ERC-20 tokens trades, performed by over 6.8 million unique wallets, encompassing a 2-year period between February 2016 and February 2018. Even studies that use a very limited ETH datasets such as Ferretti and D'Angelo [30], which in some cases used just a 1-h slot to study transactions, i.e., only around 240 blocks, conclude that the degree distribution is heavy-tailed suggesting that those degrees follow a power-law function. Somin et al. [31] analyse the dynamic properties of trading data from ERC-20 protocol compliant tokens using network theory. They examine the dynamics of ERC-20-based networks over time by analysing a meta-parameter of the network, i.e., the power of its degree distribution and their analysis demonstrates that this parameter can be modelled as an under-damped harmonic oscillator over time, enabling a year forward of network parameters predictions. Lin et al. [32] model the ETH transaction records as a complex network by incorporating time and amount features of the transactions and then design several flexible temporal walk strategies for random-walk-based graph representation of this large-scale network. Their experiments of temporal link prediction on real ETH data demonstrate that temporal information and multiplicity characteristic of edges are indispensable for accurate modelling and understanding of ETH transaction networks.

TABLE 3 | Basic Network properties for the different tokens. N is the number of nodes, $\langle k_{in} \rangle$ is the average in-degree, $\langle k_{out} \rangle$ is the average out-degree, GC is the Global Clustering Coefficient while s.d. GC is the standard deviation for the Global Clustering coefficient. ND is the network diameter, LSCC Size is the Largest Strongly Connected Component Size expressed in nodes while LSCC D is the Largest Strongly Connected Component Diameter.

Token	N	$\langle k_{in} \rangle$	$\langle k_{out} \rangle$	GC	s.d. GC	ND	LSCC size	LSCC D
ETH	84 ,227 988	2.1884	2.1884	1.1726 (–5)	6.4207 (–6)	10,004	52,093,628	10,004
BNB	4,81,138	1.4959	1.4959	4.0532 (–5)	4.4729 (–5)	37	171,291	37
USDT	9,3,02,425	3.0675	3.0675	3.3747 (–5)	1.0019 (–5)	52	8,290,551	52
LNK	784 373	1.7724	1.7724	6.4256 (–5)	4.9740 (–5)	21	504,595	19

3 DATA DESCRIPTION

A blockchain is a time-ordered sequence of blocks, each of them composed by a set of verified transactions. Transactions can change permanently the state of the Ethereum blockchain by transferring value through the native token (Ether) or by creating and executing smart contracts. Tokens built on top of Ethereum consist of a smart contract, i.e., a program run by the Ethereum Virtual Machine (EVM). The EVM is the distributed run-time environment of the Ethereum blockchain. Transactions are inserted in blocks, which are then mined, i.e., verified, using a proof of work-based consensus. For an overview of the different approaches, see Tasca and Tessone [5].

In our study, we analyse the Ethereum blockchain since its launch in 2015 until October 6, 2020 (block 11,000,000). In total, it contains 87,780,546 addresses and 856,207,725 transactions.

The data required to build the networks were extracted from the Ethereum blockhain using *ethereum-etl* tool from Medvedev [33]. *Ethereum-etl* performs ETL operations (Extract, Transform and Load) on raw Ethereum data. It enables the extraction of transactions, mined blocks, and token transfers in csv format from a fully synced Ethereum client with archive mode. Other data pipeline options are available as well. For this analysis, we use transactions with a nonzero value to reconstruct the Ether network. Transactions with zero value are usually smart contract calls. We use block extraction to assign timestamps to both native Ether and token transactions. We then aggregate transfers per token to conduct the analysis. There are thousands of tokens, but only few of them have a worth-analysing number of transactions. The vast majority of tokens have very few or no transactions at all. For this analysis, we selected three tokens, the most successful in market capitalisation at the time of writing. The other tokens were extracted but not used for this specific analysis. For further details, see the data availability statement section (**Section 7**). For market capitalisation data, we use quotations publicly available on coinmarketcap [2].

Table 1 compares the size of the datasets analysed by some of the authors mentioned in the literature review with our dataset, to underline the comprehensive scale of our analysis.

We study the dynamics of the *aggregated transaction network* in Ether (ETH), the native token of Ethereum, and in three key ERC-20 tokens built on top of Ethereum: Binance (BNB), Tether (USDT), and Chainlink (LNK). In our representation, the transaction network is composed of addresses (nodes) and directed edges representing transactions. A directed edge between two nodes means that there is at least one transaction from the sender address to the destination address. We create the networks and perform network calculations using the entire timeline mentioned in this section. In our analysis, repeated edges are disregarded. We additionally consider the timestamp of the transactions to analyse the time-based evolution of the network. We analyse as well balances of addresses at a certain point in time to study wealth distribution. The summary of the datasets used in this study is in **Table 2**.

As of this writing, according to coinmarketcap [2], ETH is the second most capitalised cryptocurrency (over USD 170 B) behind Bitcoin. We also analyse three ERC-20 tokens with the highest market capitalisation according to etherscan.io [34] in early March 2021: Binance (over USD 36 B), Tether (over USD 35 B), and Chainlink (over USD 11B).

ERC-20 Tokens: According to its specification [35], ERC-20 is the Ethereum standard for fungible tokens, where fungible means that every token of the same type behaves exactly the same and is completely interchangeable (in contrast to non-fungible tokens (NFT) where every token can be unique). ERC-20 is the interface that a smart contract (i.e., a program deployed on the Ethereum blockchain) can implement to exchange this kind of tokens. The interface provides functionalities such as token transfer from one account to another, current token balance of an account, total supply of the token available on the network, or approval for a specific token amount from an account to be spent by a third party account. An ERC-20 token contract is a smart contract that implements this interface. ERC-20 offers a viable and very successful standard to interact with non-native tokens. Non-native means not devised as part of the original protocol but implemented on top of it.

Ether (ETH): It is Ethereum's native token. In its foundational whitepaper Buterin [3], it is stated that Ethereum's mission is "to create an alternative protocol to build decentralised applications". Ethereum introduces a public blockchain with a built-in Turing-complete scripting language. Anyone can write smart contracts and decentralised applications to create their own arbitrary rules for ownership and value transaction. Ethereum, launched in 2015, constitutes an evolution from the pioneer Bitcoin blockchain. Bitcoin is based on unspent transaction outputs while Ethereum uses balance-based accounts, Turing-complete scripting, and smart contracts with their own address. Ether (ETH) is the native token that fuels the Ethereum network. With Ether, users buy "gas" that enable transactions and smart contracts calls to run. Gas is used as well to reward miners for incorporating transactions into the blocks, in addition to the usual mining block reward.

Binance Coin (BNB): The currency unit issued by Binance and—at the time of writing—the ERC-20 token based on

Ethereum with the highest market capitalisation according to etherscan. io [34]. Binance was founded in 2017 and is at the time of writing the largest cryptocurrency exchange by trading volume. "Binance" stems from "Binary Finance", as a portmanteau word of a whole new paradigm in finance. To sustain this vision, Binance launched in 2017 the Binance Coin (BNB), an initial coin offering (ICO) to fund the exchange activities, described in Binance [36]. BNB can be used to pay any fees on the exchange platform. Two important events affect BNB: First, the Binance team destroys BNB coins (a coin burn) on a quarterly basis to avoid coin value loss. Second, in April 2019, ERC-20 BNB coins were swapped with BNB coins based on the Binance Chain mainnet (BEP-2 BNB) to avoid ETH fees. BNB is currently no longer solely hosted on Ethereum but as well on its proprietary blockchain Binance Chain.

Tether (USDT): Originally proposed in 2012 as a "colored coin" inside Bitcoin and effectively launched in that network between 2014 and 2015, USDT since 2017 is traded as well as an ERC-20 token inside Ethereum. More recently, USDT has been made available even on further blockchains such as EOS, Algorand, or Tron. The philosophy and the vision behind this token are described in Tether [37]. It ranks second in market capitalisation for tokens based—among others—on Ethereum [34]. Tether is a stablecoin and can be described as a digital version of the USD, originally designed to be worth exactly $1.00, allegedly maintaining for this purpose the exact amount of reserves as USDT that are in circulation. This claim proved controversial in April 2019 when an official investigation was carried out. However, its current capitalisation indicates that markets still accept its role as digital USD, to whom it is "tethered" (hence its name "Tether").

Chainlink (LNK): It is the third most capitalised ERC-20 Ethereum-based token according to coinmarketcap.com [39] as of the time of writing. It has a high potential given its bridging nature between APIs, off-chain events, and smart contracts. Since 2020, as in coinmarketcap.com [38], LNK lists as the most capitalised decentralised finance (DeFi) token. The whitepaper by Ellis et al. [39] assigns to Chainlink the mission of building a decentralised oracle network connecting smart contracts with real-world data. Chainlink held an ICO in September 2017, raising 32 million USD, with a total supply of one billion LNK tokens. The ChainLink network utilises the LNK token to pay ChainLink node operators for the retrieval of data from off-chain data feeds (oracles), the formatting of data into blockchain readable formats, the off-chain computations, and the uptime guarantee they provide as operators. In order for a smart contract to use a ChainLink node, it needs to pay the chosen ChainLink node operator using LNK tokens, with prices usually being set by the node operator based on the demand for the off-chain resource their ChainLink node provides and the availability of other similar resources. The LNK token is an ERC-20 token, with the additional ERC-223 "transfer and call" functionality, allowing tokens to be received and processed by contracts within a single transaction.

4 METHODOLOGY

4.1 The Ethereum Network

As explained in **Section 1**, the core of our study is the characterisation of the network growth in the four transaction networks that we analyse: Ether (ETH), Binance (BNB), Tether (USDT), and Chainlink (LNK).

In the Ethereum network, we distinguish two kinds of accounts: externally owned accounts (EOA) and smart contracts. The former ones are controlled through their public/private key pairs and the latter ones *via* the logic of the code stored together with their account. We consider EOAs as human-controlled accounts while smart contracts are programs executed inside the blockchain. Smart contracts publish functions that can be invoked by EOAs or by other contracts. Smart contracts are created by EOAs by sending a contract creation transaction to the special 0x0 address.

EOAs have one or more private/public key pairs that allow them to control (receive, send, etc.) the native cryptocurrency or tokens by signing transactions with their private key. Smart contracts do not initiate transactions: they are executed when they are invoked. In their execution, smart contracts can call other contracts (they often need to for complex cases). There is always a transaction initiated by an EOA at the beginning of an smart contract execution chain.

Addresses (accounts) are the way agents are uniquely identified inside the blockchain. EOAs obtain their address from their public key. Smart contracts obtain their address as a function of the public key of their creator EOA and their specific "nonce". For further details about the functioning of Ethereum, see Antonopoulos and Wood [40].

All the interactions we see in the Ethereum blockchain occur between addresses (accounts): in our specific area of interest, tokens and cryptocurrencies are exchanged from one address to another. Both EOAs and smart contracts have addresses and balances: regardless of whether or not the account stores code, the two types are treated equally inside the Ethereum network; therefore, we do not distinguish between them in our network analysis. Native ETH tokens can be exchanged directly inside transactions. As ERC-20 tokens are built as smart contracts, any exchange of value has to pass by the smart contract address by invoking the dedicated ERC-20 transfer function.

In this study, we construct an aggregated transaction network $G^S(t) = (\mathcal{V}^S(t), \mathcal{E}^S(t))$ for symbol $S \in \{\text{ETH}, \text{BNB}, \text{USDT}, \text{LNK}\}$ at time t. In this network, the vertices $\mathcal{V}^S(t)$ are the set of addresses that have been used at least once since the first transaction of symbol S and time t. Conversely, the set of unweighted, directed edges $\mathcal{E}^S(t)$ consists of all the pairs of vertices among which there has been at least one transaction. In the directed edge (j_1, j_2), node j_1 is the sender of a transaction and j_2 is the recipient. We denote the in-degree $k^S_{\text{in},j}(t)$, of address j in symbol S the number of incoming edges received by the node before time t. Similarly, the out-degree denoted by $k^S_{\text{out},j}(t)$ represents the number of edges outgoing from the node representing the address in token S.

We also define the wealth $w_j^S(t)$ of address j at time t as the total amount of S directly controlled by this address at time t, which is obtained by issuing the *getBalance* and *balanceOf* functions for the specific token, i.e., its smart contract address in a given time and block. The output of these functions provides the unit of account for a token held by a certain address. This unit of account is defined per token, and it is arbitrarily assigned at the token definition. Preferential attachment is the network growth mechanism that happens when the probability of forming a new link is proportional to the degree of the target node, as in Barabási and Albert [19]. Preferential attachment can be linear or nonlinear, as in Dorogovtsev and Mendes [41]. In mathematical terms, we describe the probability π of forming a new link to an existing node j with in-degree $k_{\text{in},j}$ as a

$$\pi(k_{\text{in},j}) = \frac{(k_{\text{in},j})^{\alpha}}{\sum_{j'} (k_{\text{in},j'})^{\alpha}} \tag{1}$$

where $\alpha > 0$. If $\alpha = 1$, then it is said that preferential attachment is linear. If $\alpha < 1$ ($\alpha > 1$), then it is sublinear (resp., super-linear). Preferential attachment is linked to the growth mechanism of the network. We focus on the evolution of the network (and degree accruing process) where any existing network node can create links to others (regardless of their arrival or not).

When the probability of forming the new link is linear, i.e., $\alpha = 1$, then preferential attachment leads to a scale-free network. A scale-free network is a network whose degree distribution follows a power-law function $p(k_{\text{in}}) \sim (k_{\text{in}})^{-\gamma}$.

In a sublinear preferential attachment, the effect of nodes connecting with high-degree nodes is less patent. The degree distribution is a stretched exponential and not a power-law: $f_\beta(t) = e^{-t^\beta}$ or, using the same nomenclature as in **Eq. 1**, $\pi_\beta(t) = e^{-\pi^\beta}$ with a stretching exponent $\beta \in [0, 1]$. In the case of super-linear attachment, very few nodes (hubs) tend to connect to all nodes of the network, a situation termed "the winner takes it all". This is the reason why networks showing super-linear attachment are more vulnerable to attacks targeted at the hubs. Kunegis et al. [42] identify nonlinear preferential attachment in temporal networks with different values of α transcending the traditional linear relationship in the classical (linear) preferential attachment model studied by Barabási and Albert [19].

4.2 Identification of the Preferential Attachment Type

When a new, directed edge is added to the network (from an unspecified node), we assume that the destination node j is selected with a probability which is a function (solely) of its in-degree k^*_{in}, i.e., $\pi(k^*_{\text{in}})$. For the rest of our proposal, we assume that **Eq. (1)** holds. We further denote $\Pi(k_{\text{in}})$ the probability that a new link is created to *any* node with in-degree $k^\star$. Trivially,

$$\Pi(k^*, t) = \pi(k^*) \cdot \sum_{j=1}^{N(t)} \delta\left(k^*, k_{\text{in},j}(t)\right) = \pi(k^*) \cdot n_{\text{in}}(k^*, t) \tag{2}$$

where $\delta(\cdot, \cdot)$ represents the Kronecker delta, and—therefore—its sum yields the total number of nodes with in-degree k at time t, denoted by $n_{\text{in}}(k, t)$. Given that $\Pi(k^\star, t)$ is a time-dependent function, following Kondor et al. [24], we use the rank function $R(\alpha; k^*_{\text{in}}, t)$, computed for each link addition to a node with in-degree $k^\star$ at each time t. Specifically,

$$R(\alpha; k^*, t) = \frac{\sum_{j=1}^{N(t)} \Theta(k^* - k_{\text{in},j} + 1)\,(k_{\text{in},j})^{\alpha}}{\sum_{j=1}^{N(t)} (k_{\text{in},j})^{\alpha}} \tag{3}$$

$$= \frac{\sum_{k=0}^{k^*-1} n_{\text{in}}(k, t)\, k^{\alpha}}{\sum_{k} n_{\text{in}}(k, t)\, k^{\alpha}} \tag{4}$$

In the first expression, the function $\Theta(\cdot)$ is the Heaviside function, equal to one if the argument is positive, and zero otherwise. Thus, the sum in the denominator runs for all nodes whose degree is lower than k^*_{in}. The sum in the numerator runs over all degrees where $n_{\text{in}}(k, t) > 0$. When a new edge is created, if the target node is drawn with a probability following **Eq. (3)** for a given α_o, then we can replace **Eq. (2)** into **Eq. (4)**

$$R(\alpha_o; k^*, t) = \sum_{k=0}^{k^*-1} \Pi(k^*, t)$$

Thus, if α_o is the exponent of the non-preferential attachment, adding new edges is equivalent to a process of inverse transform sampling Devroye [43] on $R(\alpha_o; k^\star, t)$.

To obtain the value of α_o, we measure the corresponding K-S (Kolmogorov-Smirnoff) goodness of fit, i.e., the difference between the empirical distribution function (ECDF) calculated with different exponents α and the theoretical linear CDF distribution. The value α_o that minimises the distance to the uniform distribution is the best fit for the exponent. That specific value will be informative of the type of PA present in each of the transaction networks that we study.

As explained in **Section 3**, the size of the analysed data renders this task computationally demanding. To make the calculation more scalable, we only analyse each edge with a probability $p_{(R)} \ll 1$. We repeat the process multiple times to confirm results. The exact parameters used are detailed in chapter 6.

5 EMERGENT DISTRIBUTIONS

5.1 Wealth Distribution

We start by analysing wealth distribution across addresses for the four tokens considered. We compare native tokens (ETH) with second-level tokens built on top of the Ethereum network (BNB, USDT, LNK). For all the nodes that appear once in the evolution of the network, we extract their final wealth, i.e., their balance at block 11 M (October 6, 2020) and show the distribution in **Figure 1**.

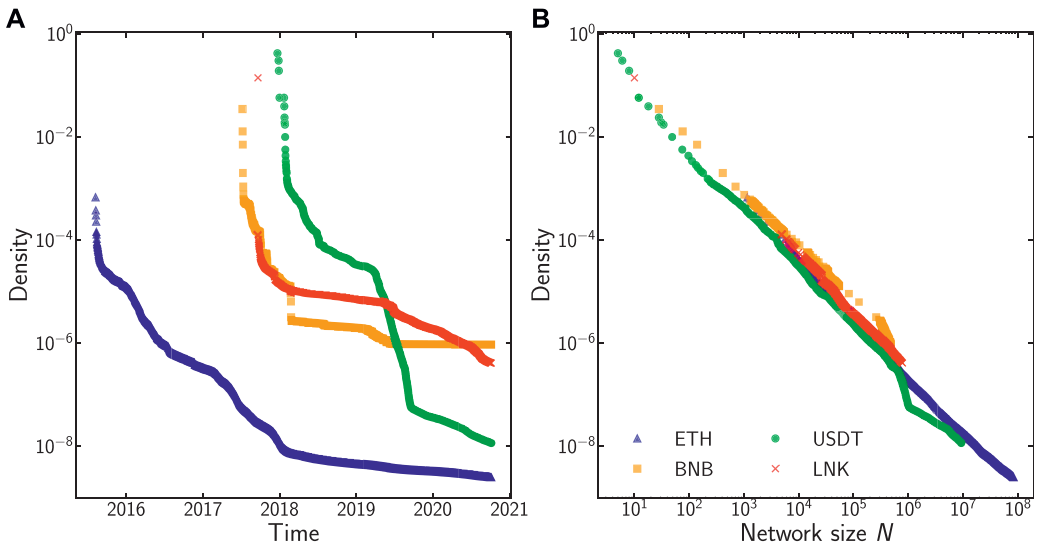


FIGURE 3 | On the **(A),** we show the time evolution of network density, while on the **(B),** we have the density as a function of the network size. Both figures show the results for all the cryptoassets considered.

We do this programmatically by extracting wealth data for all the nodes involved in the transaction network. This way we obtain the basic unit of account: for the Ether Network, the output of *getBalance* is the unit of account known as "wei" (equivalent to 10^{-18} Ether), while for BNB, USDT and LNK are the unit returned from the ERC-20 method *balanceOf*, which is custom-defined for every token. To obtain the well-known and traded token value we are commonly referring to, we have to divide the output of *balanceOf* method by the value specified in the *Decimal* field of the ERC-20 Contract. This value is 10^{18} for LNK and BNB (the same as ETH) and 10^{6} for USDT (see **Figure 1**). All four tokens seem to follow a power-law distribution. Ether (ETH), BNB, and LNK display a similar behaviour while Tether (USDT) exhibits a cutoff at a lower value. The very broad distributions with power-law compatible behaviour (spanning 14 orders of magnitude) are by itself quite remarkable, independent of the nature of the token considered.

While in this study, we do not dig into the mechanism that generates this emergence, it reflects a similar behaviour to the wealth distribution in real-world economies as shown in Levy and Solomon [44] and Brzezinski [45]. However, in this case, the distribution is much broader. This implies the existence of systemic agents in the system. When computing the Gini indices at the end of the period analyses Bovet et al. [9], we find out that the values for all distributions are often above 0.99. The reason for this excessive inequality is the underlying wealth distribution. The results of model selection—as in Clauset et al. [46]—for wealth distribution are pretty similar for all of the tokens, with strong evidence in support of power-law against exponential (p-values of 10^{-15}, 10^{-4}, 10^{-3}, and 10^{-9} for ETH, BNB, USDT, and LINK tokens, respectively), and not enough conclusive evidence against lognormal and truncated power-law (p-values larger than 0.3 with very weak support for lognormal and truncated power-law). The exponents γ_w of power-law are 1.81, 1.70, 2.14, and 1.97 for ETH, BNB, USDT, and LINK, respectively. Due to the high computational costs of fitting the distributions and performing model selection, only a random sample of around 1% of ETH and 8% of USDT nonzero balance addresses was used in analysis for these tokens.

5.2 Evolution of Basic Statistics

As an introduction to the analysis of the four tokens that we study, i.e., ETH, BNB, USDT, and LNK, in **Figure 2** we display a set of basic statistics: the market price of the tokens analysed, number of new daily nodes, and number of new daily edges as a function of time. We also list basic network properties fow the four tokens in **Table 3**. In the upper panel of **Figure 2**, we show the market price (in US Dollars), which is—arguably—a reasonable proxy measure to show the success of these tokens. Due to its stablecoin design, the daily market price for USDT fluctuates only minimally (around 1 USD) in comparison with other "traditional" cryptoassets, which show a high volatility.

We observe that the daily number of active nodes (i.e., the number of addresses) and the daily number of active edges (i.e., the number of transactions) in ETH have been steadily growing until the end of the bullish market in 2018 (**Figures 2B,C**). We identify a peak in both nodes and edges coinciding with the end of the 2018 bullish market for cryptocurrencies. A similar gradually growing scenario, although not covered by our graphs, has taken place during the first months of 2021. At the end of our data collection period, i.e., October 6, 2020, there were 87,780,546 Ethereum addresses and 856,207,725 transactions, of which 414,743,169 with a nonzero "value" field, i.e., with current transfers of native Ether. The remaining transactions with a zero

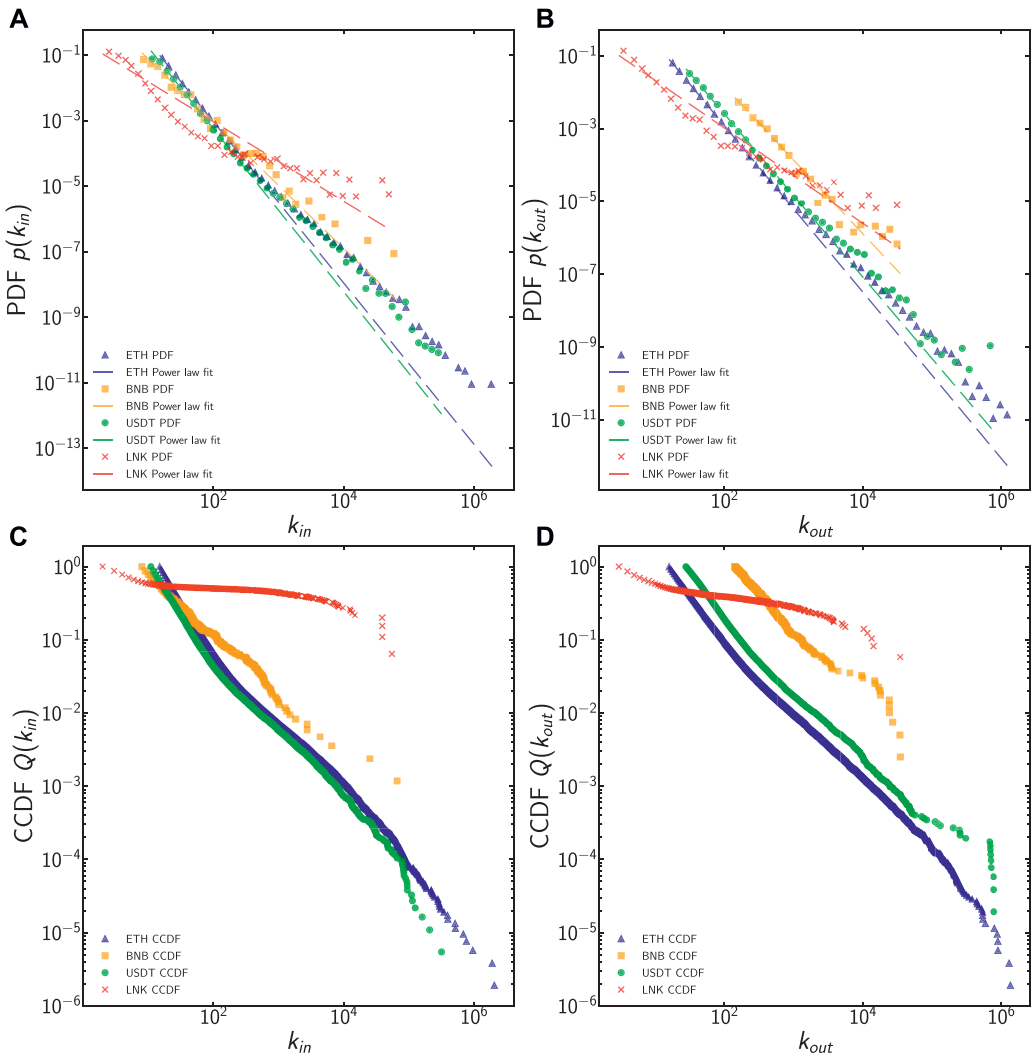


FIGURE 4 | PDF and CCDF for in-degree and out-degree in ETH, BNB, USDT, and LNK at the end of the observation period.

"ETH value" transfer value are smart contract transactions, which could transfer ERC-20 tokens (when calling the right smart contracts) but not directly native ETH. Regarding BNB, we observe how the move of their servers out of China in March 2018 triggered a temporary traffic peak, and the launch of the Binance Mainnet in April 2019 was decisive to bring the number of BNB nodes and edges on top of ETH to a very low number, almost constant as displayed in **Figures 2B,C**.

With regard to USDT and LNK, we observe as well an increase in activity since early 2019, in spite of the investigation by New York's Attorney General in 2019. Considering **Figure 2A**, USDT seems to have reached the status of a worth-investing stablecoin. For LNK, its growth in activity corresponds to the fast growth of DeFi in late 2020. On a qualitative basis, it is worth mentioning that price and new daily nodes/edges seem to follow a correlated dynamics (as apparent by the profile of local extremes).

We then compute the link density $d = L/N(N-1)$ where L is the number of edges and N is the number of nodes. We compute link density figures using the number of active nodes and edges within daily timeframes.

Figure 3 shows the results for the network density in our data. The left panel shows the evolution of network density as a function of time. The overall trend is a steady decrease in density during the initial phase of ETH until 2018. Since then, its density has remained constant at very low values. BNB and LNK, starting from their launch in 2017, show a similar behaviour in **Figure 3** but with a steeper fall. USDT density decreases rapidly in early 2018 since its start as ERC-20 token on top of Ethereum and, later on, in mid 2019, but this time at a slower pace, coinciding seemingly with an external event: the investigation in 2019 by New York's Attorney General (NY Attorney General Press Release [47]).

Figure 3A shows a parametric plot of the network density as a function of network size. Here, a common scaling $d \propto N^{-1}$ is apparent, showing that the number of edges grows linearly with network size which shows that each new node produces a limited

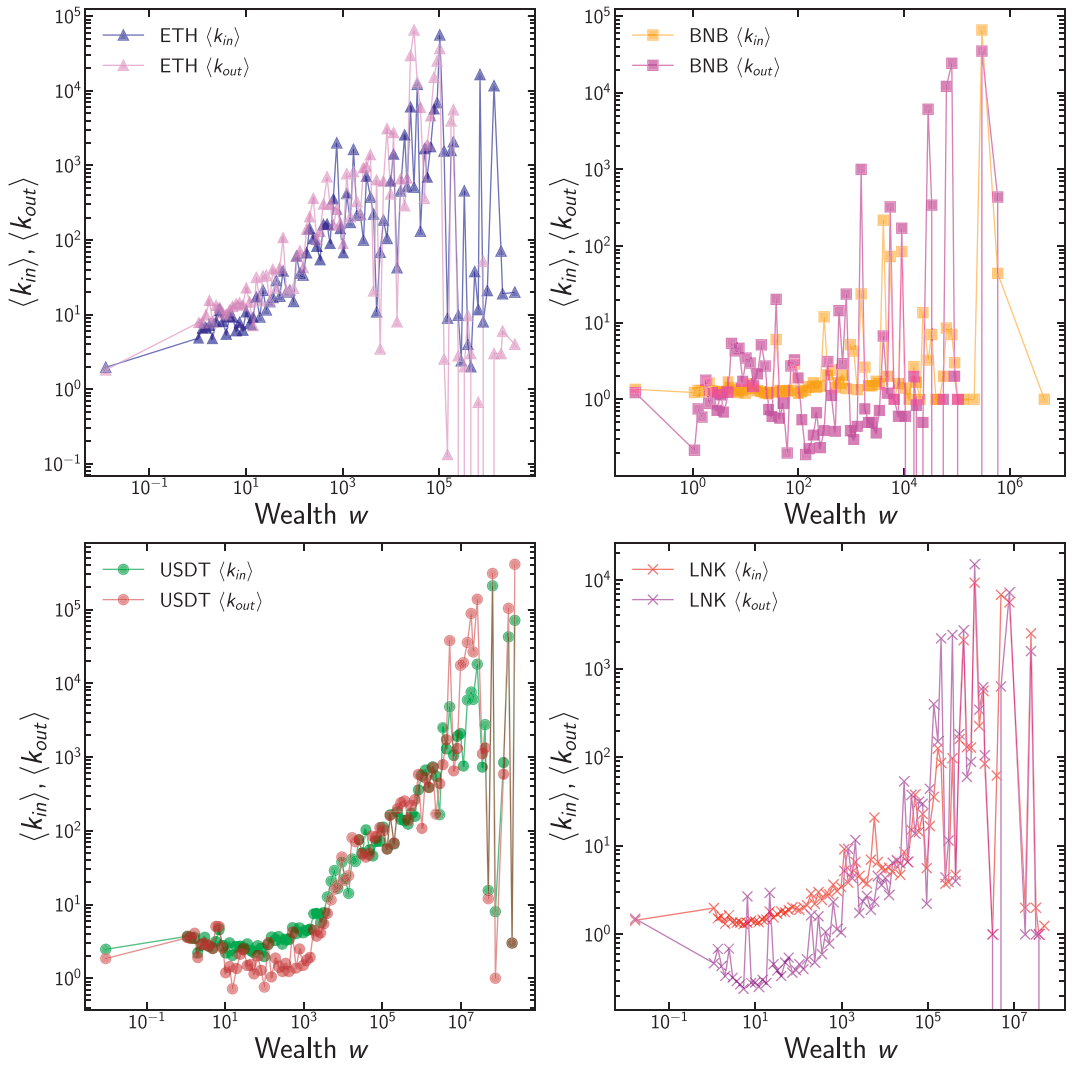


FIGURE 5 | Plot of mean for ETH, BNB, USDT, and LNK. $\langle k_{\text{in}} \rangle$ (in-degree), $\langle k_{\text{out}} \rangle$ (out-degree), $\langle w^S \rangle$ (wealth of the specific token).

amount of new connections in the aggregate network. Given that the transactions keep growing, this implies—from the aggregated network representation we consider—that transactions take place mostly across already existing links. This result is important for the modelling approach we consider: in preferential attachment models, the network density shows the same scaling as the one we observe in our data.

5.3 Degree Distributions

The simplest measure to characterise complex networks is its first-order node statistics, i.e., its degree distribution. The results are shown in **Figure 4**. First, in the left panels, we show the PDF and the CCDF of the in-degree of the network nodes, which is the focus of our extensive analysis in the next section. We observe that the distributions for in-degree and out-degree of the network nodes are heavy-tailedmeaning that the network contains nodes with degrees spanning several orders of magnitude, the largest of which is commonly referred to as *hubs*. Specifically, for the largest networks ETH and USDT, the results are largely compatible with a power-law distribution. This result is remarkable, considering the long evolution of the networks (for a period of six and 3 years, respectively) and the changing environment for its evolution (price, number of users, usage, etc.). In these plots, we see that LNK departs the most from this behaviour. In the right panels, it is possible to observe that the out-degree distribution exhibits a similar pattern. Common to all distributions is the existence of deviations from the power-law behaviour for very large values of in- and out-degrees k_{in} and k_{in}, and this means that nodes with large in- and out-degree are more common than those found in networks with scale-free degree distribution. This is characteristic of networks that have super-linear preferential attachment which leads to the formation of super-hubs.

The model selection process, as in Clauset et al. [46], shows that in ETH, both for in-degree and out-degree, the power-law is

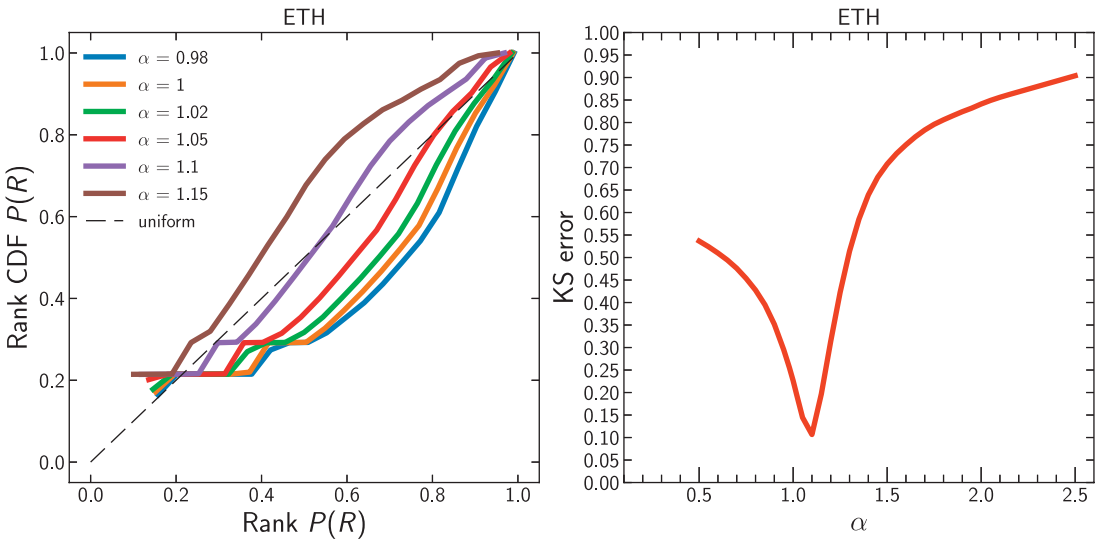


FIGURE 6 | ETH. Rank function for different α. KS distance. α value minimising error.

TABLE 4 | Spearman correlation between k_{in} (in-degree), k_{out} (out-degree), w^S (wealth) for each cryptoasset. All p-values are lower that 10^{-10}, implying that we can reject the null hypothesis that the variables are not correlated.

		Spearman correlation		
Token	**Property**	k_{in}	k_{out}	w^S
ETH	k_{in}	1	0.574	−0.157
—	k_{out}	0.574	1	−0.508
—	w^S	−0.157	−0.508	1
BNB	k_{in}	1	0.195	−0.085
—	k_{out}	0.195	1	0.169
—	w^S	−0.085	0.169	1
USDT	k_{in}	1	0.397	0.099
—	k_{out}	0.397	1	0.364
—	w^S	0.099	0.364	1
LNK	k_{in}	1	0.107	0.229
—	k_{out}	0.107	1	0.428
—	w^S	0.229	0.428	1

TABLE 5 | Spearman ρ correlation measures between cryptoassets for the measures of k_{in} (in-degree), k_{out} (out-degree), and w^S (wealth). All p-values are lower that 10^{-10}, implying that we can reject the null hypothesis that the variables are not correlated.

		Spearman correlation			
Property token		**ETH**	**BNB**	**USDT**	**LNK**
ETH	w^S	1	0.3288	0.2656	0.3187
BNB	—	0.3288	1	0.1637	0.1289
USDT	—	0.2656	0.1637	1	0.3065
LNK	—	0.1289	0.1637	0.3065	1
ETH	k_{in}	1	0.1634	0.2891	0.4330
BNB	—	0.1634	1	0.1634	0.2120
USDT	—	0.2891	0.1634	1	0.2489
LNK	—	0.4330	0.2120	0.2489	1
ETH	k_{out}	1	0.1956	0.1612	0.2193
BNB	—	0.1956	1	0.3790	0.3398
USDT	—	0.1612	0.3790	1	0.5060
LNK	—	0.2193	0.3398	0.5060	1

the best fit against exponential, lognormal, lognormal positive, stretched exponential. Only with truncated power-law, the advantage slightly diminishes (model selection: both for in-degree and out-degree $< 10^{-4}$, but with p-values (0.99 for in-degree and 0.98 for out-degree)) so high that the results do not bear significance. The fitted power-law exponents for ETH are γ_{in} = 2.4 for the in-degree (x_{min} = 15) and γ_{out} = 2.29 for the out-degree (x_{min} = 16). Value x_{min} designates a minimum degree where the scaling relationship of the power-law begins, and it is determined automatically by repeatedly performing a power-law fit on all unique degrees in the data and then choosing the one with the minimum Kolmogorov-Smirnov distance between the data and the fit (Clauset et al. [46]; Alstott et al. [22]).

The same pattern for in-degree and out-degree applies as well for USDT, where a similar pattern for truncated power-law applies. Additionally, USDT seems to have a better fit for lognormal (1.74, but with a p-value that is hardly meaningful 0.28). The fitted power-law exponents for USDT are γ_{in} = 2.485 for the in-degree (x_{min} = 11.0) and γ_{out} = 2.242 for the out-degree (x_{min} = 28.0).

Similar behaviour applies to BNB in-degree and out-degree. Power-law seems to fit better than truncated power-law, but with high p-values. Lognormal seems to fit better for in-degree, but with an inconclusive p-value (0.278), while for out-degree, the lognormal fit better (1.604) with a 0.102 p-value, almost significant, but still a bit too high. The fitted power-law exponents for BNB are γ_{in} = 1.927 for the in-degree (x_{min} = 8.0) and γ_{out} = 2.028 for the out-degree (x_{min} = 142.0).

LNK token in-degree behaves very similarly to ETH, with the same inconclusive behaviour for truncated power-law. Given the fact that all the better fits were inconclusive for too high p-values, we took as reference for in-degree and out-degree always power-law fits. The

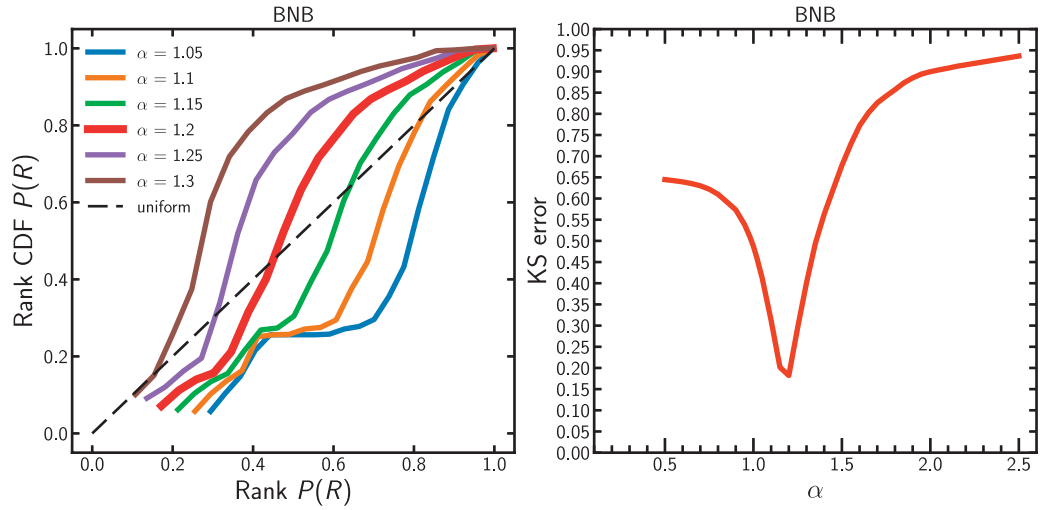


FIGURE 7 | BNB. Rank function for different α. KS distance. α value minimising error.

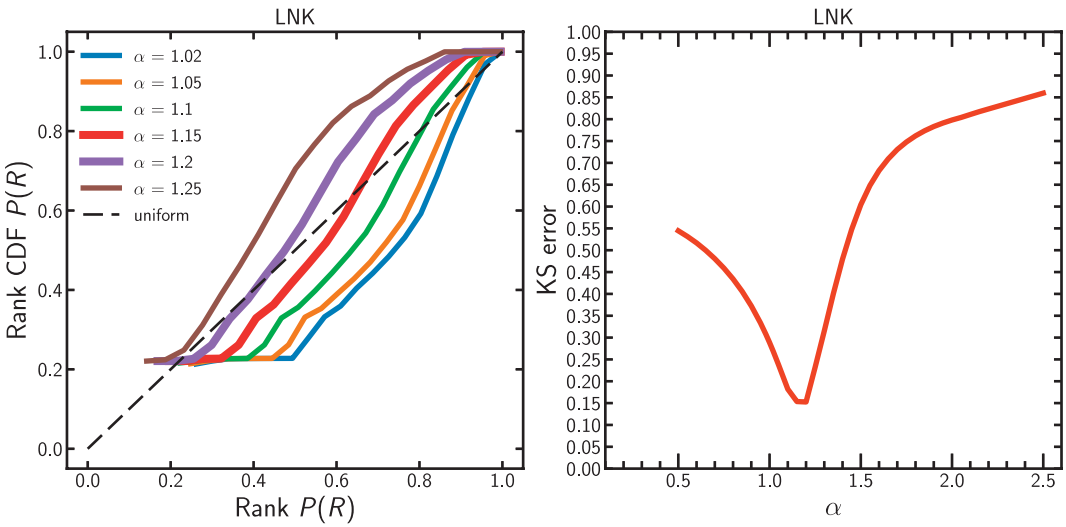


FIGURE 8 | USDT. Rank function for different α. KS distance. α value minimising error.

fitted power-law exponents for LNK are $\gamma_{in} = 2.955$ for the in-degree ($x_{min} = 6.0$) and $\gamma_{out} = 3.352$ for the out-degree ($x_{min} = 6.0$).

Kondor et al. [24] find that the in-degree of a node, i.e., the number of transactions received by an address is positively correlated with the BTC balance of that address. In our analysis, for the largest Ethereum-based cryptoassets, we obtain wealth in-degree and wealth out-degree correlation plots with wealth. The results are depicted in **Figure 5**. In the panels, we have first binned (logarithmically) the wealth and then computed the mean value of the in- and out-degree of the nodes within each range of wealth.

Overall, the trend is that for increasing wealth, the in- and out-degrees of the nodes are also larger. The sole exception seems to be ETH, but the reason for this is the large multitude of addresses with a nonzero value of wealth, but nominally small in Wei (because of leftovers of transactions execution). The bump in the relationship (at around 10^{-3} ETH) is explained by the actual usage of ETH as a medium of exchange, with the upwards, monotonic trend. We argue that very small values of w in the plot correspond to automated usage. A similar pattern is observed on all cryptoassets analysed.

Table 4 shows the comparison of the Spearman correlation measures between k_{in} (in-degree), k_{out} (out-degree), and w^S (wealth) for each asset. The results show always a positive and significant correlation in the wealth of all cryptoassets.

Also, **Table 5** shows the correlation between cryptoassets for each measurement considered so far. All tokens built on Ethereum are *smart contracts*, differently from the Ether token which is natively built inside the Ethereum network. Tokens built

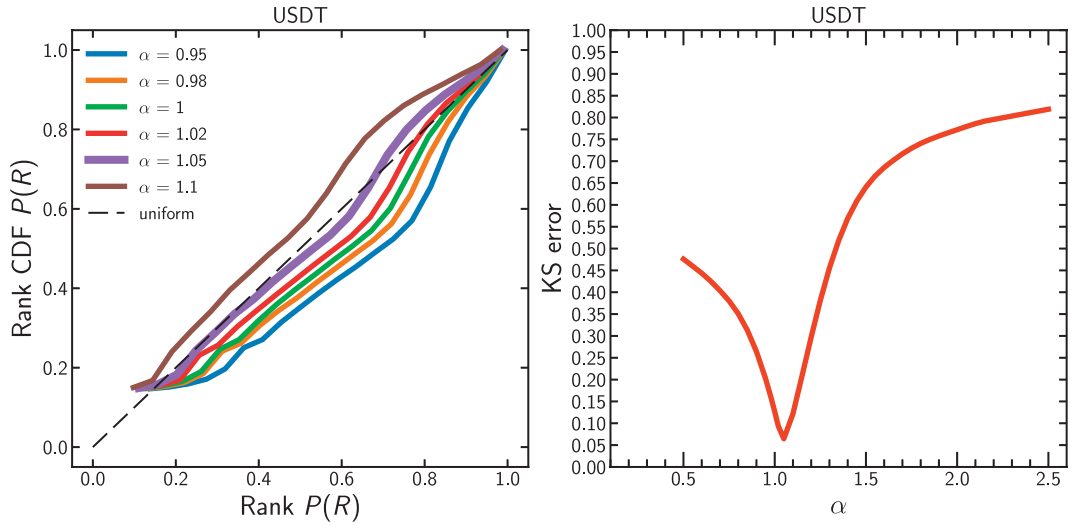


FIGURE 9 | LNK. Rank function for different α. KS distance. α value minimising error.

on top of Ethereum do not require nonzero-valued Ether transactions, i.e., Ethereum transactions moving Ether tokens. This means that addresses holding tokens built on Ethereum (such as BNB, USDT and LNK) are not always present in Ether network transactions (i.e., nonzero values transactions exchanged in Ethereum for Ether token), even though they eventually need some Ether to pay transaction fees. They might participate in just zero-valued transactions (i.e., smart contract calls). Consequently, the networks might overlap, but they do not coincide, so we can calculate the correlation between two studied tokens only based on the intersection subset of addresses, which appears on both token networks. Interestingly, as shown in **Table 5**, we find that in- and out-degree and wealth across cryptoassets are always positively correlated.

6 PREFERENTIAL ATTACHMENT

In this section, we complement our previous analysis on the in-degree distributions with an estimation of the exponent α in **Eq. (1)**. We calculate value of α that brings the K-S distance (or error) between the empirical distribution function and the theoretical one, in this case, a pure power-law function, to the minimum possible. If that error is minimum when $\alpha = 1$, then we can confirm that the preferential attachment we observe in the corresponding blockchain transaction network is linear. If $\alpha > 1$, then we identify to super-linear attachment, i.e., very few nodes in the network (superhubs) tend to connect to most nodes of the network. We perform a similar calculation for ETH, BNB, USDT, and LNK.

For ETH, we sample the network by running various iterations at $p_{(R)} = 10^{-3}$ or $p_{(R)} = 10^{-4}$, a value influenced by the network size, to decrease the computational demand, and we repeated the process at least 10 times to confirm the consistency of the results. For all the other tokens except USDT, we considered the complete dataset.

In **Figure 6** we plot the rank function presented in **Section 4.2**, and then, we calculate the value of α that minimises the error between the fit and the empirical function. The error to fit this function of probability is minimum with the exponent $\alpha = 1.1$. This means that we identify a slightly super-linear preferential attachment for ETH, which implies that very few nodes tend to connect to all nodes of the network.

We perform an identical exercise with the entire BNB transaction set, and without sampling, we took the whole dataset, since the smaller size made the required computations manageable. We reach a similar conclusion: preferential attachment in BNB is super-linear as well, but now with a larger value of $\alpha = 1.2$ which minimises the error in the rank function. As an additional methodological verification, we repeated the calculation with a reduced sample ($p_R = 0.05$) and obtained the same results, as in **Figure 7**. When we analyse the network dynamics for LNK, we also obtain a super-linear as with a value between $1.15 \leq \alpha \leq 1.2$ (because both minimise the error in the rank function in the compatible manner). These results are similar to those obtained for BNB. For LNK as well the full network dynamic was used to compute the rank function. The results are presented in **Figure 8**. Interestingly, when we analyse the stablecoin Tether/USDT, the results of the analysis change. Because of the size of the data, we sample the USDT network by taking a $p_R = 0.1$. We confirm a preferential attachment, in this case closer to linear preferential attachment than in any other studied case. The value of α that minimises the error in the rank function is $\alpha = 1.05$. The results are shown in **Figure 9**.

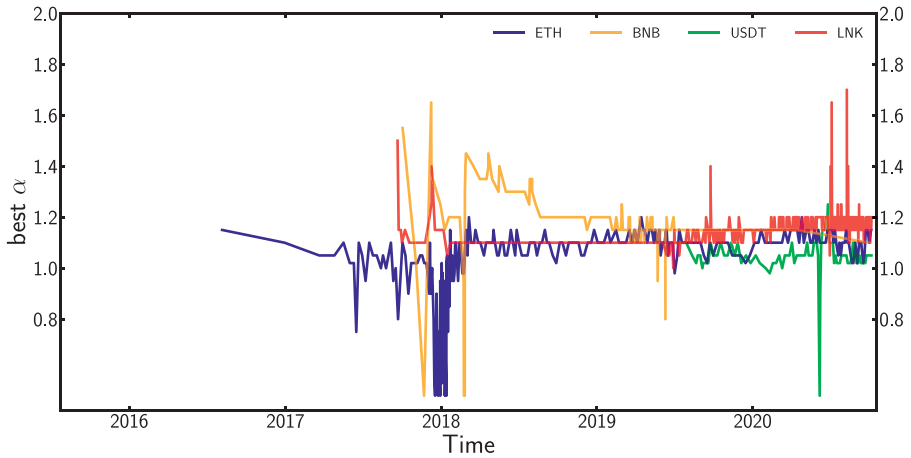


FIGURE 10 | (A): evolution of best fit α (cumulative) for preferential attachment throughout time. **(B)**: evolution of best fit α for preferential attachment computed individually and in isolation for every time windows.

In all these cases, the relatively large values of the KS statistic may be due to non-stationary nature of the preferential attachment process.

We finally show the evolution over time of the best fit for α for each token up to block 11 M. **Figure 10** displays how α changes throughout time. The top graph is a cumulative value up to the last block for each time unit. We confirm a greater PA super-linearity in the first months of BNB. This coincides with the early stages of the BNB token and with its launch on the ETH blockchain before its "commercial" release. Both Liang et al. [27] and Kondor et al. [24] refer to an early or initial phase for the tokens they study, in which network properties are different from their next longer phase, i.e., the trading phase. Changes in α throughout time for ETH, USDT, and LNK are, however, as the top graph of **Figure 10** displays, much less pronounced, although ETH's early phase shows a higher super-linearity around $\alpha = 1.15$ and only a phase of sublinearity during early 2018. In the bottom part of **Figure 10**, we take the best fit for α individually and not merged with the full history of best fit, to best display the variation in each individual timeframe.

A typical trait of preferential attachment is the fact that, if the preferential attachment is nonlinear, the maximum degree of the node in the network grows linearly with network size, while when preferential attachment is linear, the maximum degree of the node grows as a square root of the network size, as in Barabási and Pósfai [12]. In **Figure 11** we plot the evolution of max in-degree and out-degree $\max_i k^S_{\text{in},i}$ $\max_i k^S_{\text{out},i}$ during the evolution of network size N.

We compute the Gini Index G for in-degree and out-degree distribution as the network size N grows. Both are computed for monthly snapshots in each network. As displayed in **Figure 12**, the relation between network size and Gini Index G for in-degree does not appear always conclusive for all the tokens. It is clear enough for USDT, but more ambiguous and difficult to read for the other tokens.

From the graph, it is easy to recognize a relationship between network size and maximum in- and out-degree. This relationship could be expressed with the following formulas:

$$\ln(\max_i k^S_{in,i}) = \beta_0^{\text{in}} + \beta_1^{\text{in}} \ln(N)$$
$$\ln(\max_i k^S_{out,i}) = \beta_0^{\text{out}} + \beta_1^{\text{out}} \ln(N)$$

We run a linear regression to compute the coefficients, and the results of the slopes β_1^{in} and β_1^{out} are reported in **Table 6**. The slopes remark indeed a strong relationship, which was already evident from the plotted graphs.

As we see in **Table 6**, the exponents β_1^{in} and β_1^{out} are significantly larger than 1/2. This is a remarkable indication that some sort of nonlinear preferential attachment is taking place, as in the case of linear attachment (nonlinear preferential attachment), it should be β_1^{in} and β_1^{out}, (resp. 1). The non-stationarity of the process may be the reason to find intermediate values.

7 CONCLUSION

Blockchain-based systems are disrupting an increasing number of areas, in many cases under the claim of an increasing decentralisation in different facets. In this study, we focus on Ethereum—a public blockchain created in 2015 with the second-largest market capitalisation (as of this writing) after Bitcoin. It offers the capability to write smart contracts that enable the creation of arbitrary assets beyond the native cryptocurrency, Ether (ETH). The tokens with the largest market capitalisation are at the time of writing Binance (BNB), the currency token linked to the largest cryptoexchange in the world since 2018; Tether (USDT), the most capitalised USD-pegged stablecoin; and Link (LNK), the most used token to pay for oracle services (off-chain data providers) in the increasingly relevant decentralised finance (DeFi) environment.

For these cryptoassets (which are of different nature), we consolidate a large-scale dataset consisting of all the

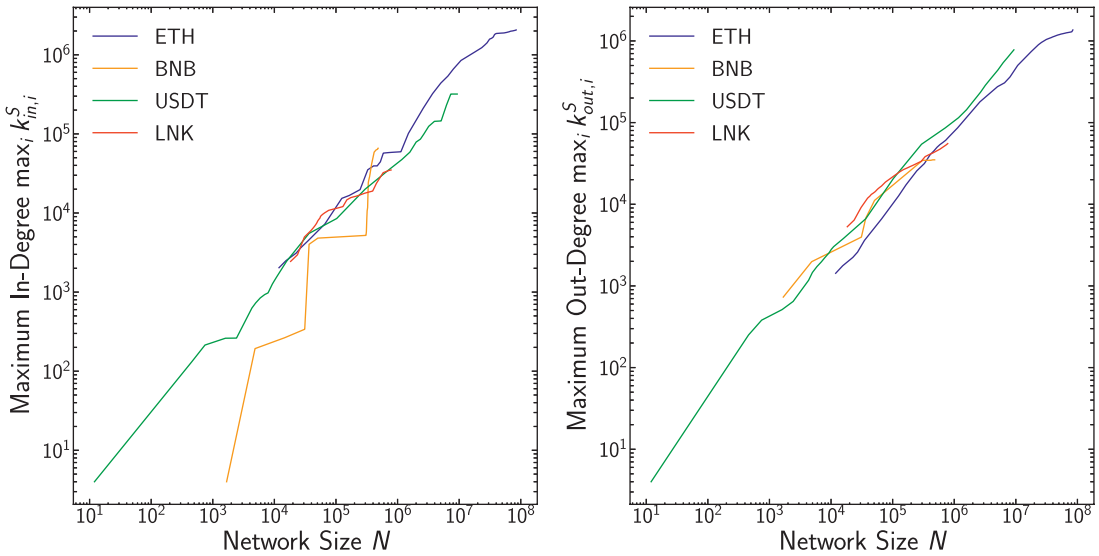


FIGURE 11 | We plot the maximum in-degree $\max_i k^S_{\text{in},i}$ **(A)** and maximum out-degree $\max_i k^S_{\text{out},i}$ **(B)** as a function of the network size N. The measurements are performed on a monthly basis.

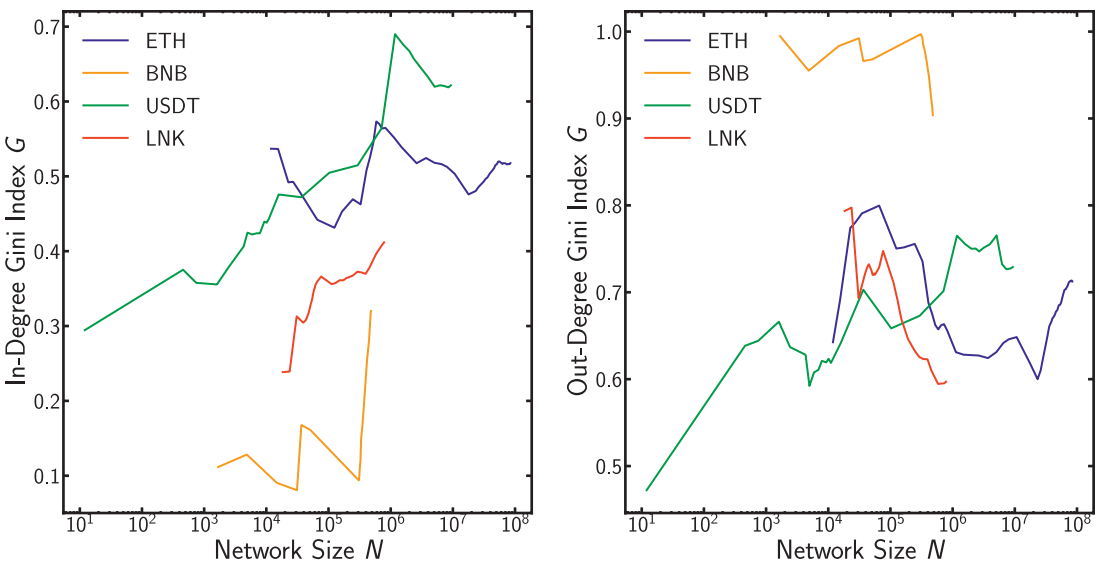


FIGURE 12 | We plot the network size as a number of nodes N against the Gini index G for the in-degree distribution and out-degree. We take monthly snapshots.

transactions since system creation to late 2020. Then, we build one directed aggregated network for each cryptoasset - **Figure 13** shows an example visualization for BNB network. This representation is useful to characterise the space of all transactions that ever took place in these economies. They allow us to further characterise and understand the economic processes (e.g. value exchange and wealth concentration) that take place in these systems.

We first analyse the distribution of wealth in the different crypto. We find that all of them are well described by a power-law distribution with an exponent close to or exceeding $\gamma_w = 2$ for each of the tokens. This is interesting as the model of creation, usage, or underlying concept they represent largely varies across the assets analysed. However, the degree distributions of the aggregate networks are different for each assets. All these two results hint at the fact that the economic processes are (at least) not entirely coupled to the network evolution. Further analyses show that the in- and out-degrees of nodes are only lightly correlated between network nodes present in the different tokens. This serves as a justification to — in this first study —

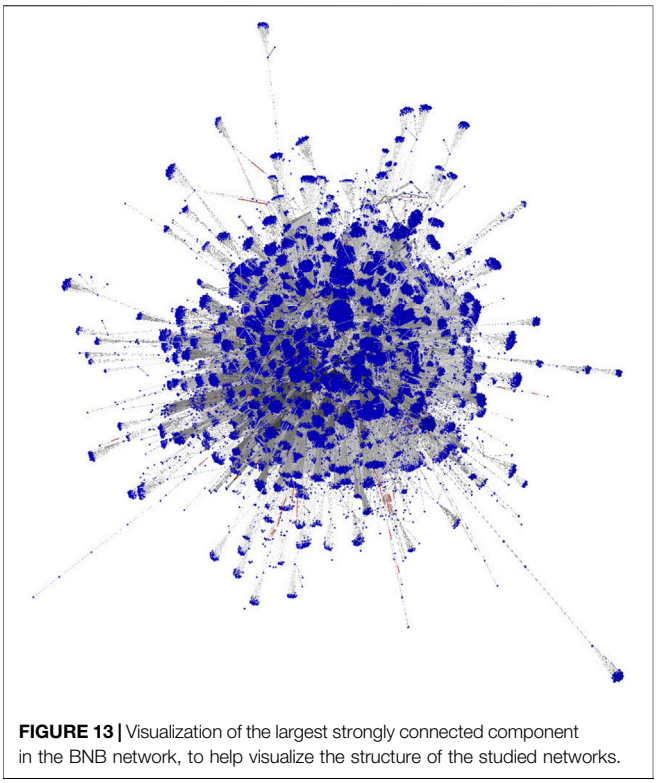


FIGURE 13 | Visualization of the largest strongly connected component in the BNB network, to help visualize the structure of the studied networks.

TABLE 6 | Gini Coefficients for wealth (w^S), in-degree (k_{in}), and out-degree (k_{out}). First, w^S filters out nonzero value (since the graph is cumulative, old addresses appearing in the network are accounted but might no longer hold tokens). For comparison, the second wealth includes instead all the addresses in the network.

Token	Gini $w^S > 0$	Gini w^S	Gini k_{in}	Gini k_{out}	β_1^{in}	β_1^{out}
ETH	0.9975	0.9986	0.5177	0.7124	0.8168	0.7647
BNB	0.9976	0.9985	0.3200	0.9038	1.4803	0.6857
USDT	0.9861	0.9969	0.6216	0.7290	0.8004	0.8401
LNK	0.9908	0.9971	0.4118	0.5971	0.5839	0.5546

analyse the network evolution of each token separately and without including economic aspects on it. However, more detailed approaches will require a multiplex network approach.

Our study hints that growth and concentration measures can be characterised by complex network topology calculations. First, we identify that the addition of new links to these networks increases linearly with network size (as in other preferential attachment growth processes) and that the degree distributions are characterised by heavy-tailed distributions with over-representation of hubs. In contrast to the previous analyses on Bitcoin by Kondor et al. [24], we find that preferential attachment (PA) in these public blockchain networks is slightly super-linear in ETH with an $\alpha = 1.1$ and super-linear in BNB and LNK with an $\alpha = 1.2$, and very close to linear in USDT with an $\alpha = 1.05$. A super-linear PA indicates a high degree of concentration of transactions in a few hub nodes induced by the way the network grows.

Kunegis et al. [42] measured preferential attachment coefficients in many online networks and argue that online interaction networks—those that consist of people interacting directly or indirectly between each other, commonly exhibit super-linear degree distributions. This includes online networks where interaction is direct, for example, in an online social network such as Twitter, as well as indirect where interaction happens through an intermediary content, for example in online forums. In such interaction networks, the users or content with which users interacted in the past tends to attract more interaction in the future in a super-linear fashion. Considering that blockchain transaction networks are also a form of an interaction network where users perform transactions between addresses associated with them, it is not surprising that they also exhibit a super-linear preferential attachment where a small number of nodes asymptotically collect most of the connections.

Given the hybrid nature of a socio-technical-economical system such as the cryptocurrency market, where speculative investments, software agents, and smart contracts play such a defining role, the characterisation of its transaction network as an interaction network leaves the door open for many interesting considerations.

Surprisingly, different aspects of the evolution of these economies show large-scale regularities that are unaffected by the heterogeneous nature of the agents involved, considering that data are composed of users, exchange markets, organisations, automated accounts, etc.

We suggest continuing this study by expanding its realm in two dimensions. First, by analysing all tokens in the Ethereum ecosystem in order to identify common regularities across them, we suggest to perform a similar study with other tokens and blockchains to make an attempt to generalise conditions under which PA turns super-linear in public blockchains and, additionally, to endeavour the identification of any other token with a different PA type than the underlying blockchain on top of which it runs. Second, by extending the analyses to include the more recent development because this period coincides with a strong bullish crypto-market with high record-breaking trading volumes and market prices. It is of interest to see whether the identified PA features remain roughly the same over time or whether they change fundamentally. Third, additional directions for future work include the inference of statistical properties of the entire history data and investigating the temporal properties of the entire transaction network as proposed by Guo et al. [28].

The seed of this study was the comparison of "nested" tokens, i.e., BNB, USDT, and LNK run on ETH. These tokens seem to exhibit a slightly different behaviour depending on their design and not on the infrastructure they share. We suggest to further research on how the design of every token affects their network dynamics and whether a more comprehensive taxonomy and clusterisation of the token network according to their network dynamic is possible. We propose as well to study the overlap of networks, accounts, and addresses and how they influence each other across tokens, a research direction that we hinted in this study.

Finally, we also suggest studying coupling patterns between these interconnected networks and comparing them with the

study by Dong et al. [48] on the optimal resilience of modular interacting networks.

DATA AVAILABILITY STATEMENT

The data is available in the ETH blockchain (which is a public ledger). Data was transformed with ethereum-etl tool. To gather Ethereum data, both OpenEthereum client and Turbogeth (now Erigon) were used. Besides the observations in the Data Description section, the dataset is publicly available on Google Cloud BigQuery as seen in [49] and can be queried directly from a web interface. The technical architecture of the solution connecting Google Cloud and ethereum-etl is well described in [50]. For intensive analysis (such as the ones conducted in this paper) we anyway always suggest to extract the data locally on your machine.

AUTHOR CONTRIBUTIONS

CT led this research providing key insights for the analysis. FD, AP, and CT designed the experiment and analysis. FD collected, cleaned and processed the data. FD and AP analysed the data and all the authors discussed the results. AP wrote successive drafts. MP performed additional computations and reviewed the paper. All authors wrote the final text and approved the final version.

FUNDING

CT acknowledges financial support from the University of Zurich through the University Research Priority Programme on Social Networks. AP has been partially supported by the Rey Juan Carlos University.

REFERENCES

1. [Dataset] Nakamoto S. Bitcoin: A Peer-To-Peer Electronic Cash System (2008). Available at: Nakamotoinstitute.org. Published online by https://bitcoin.org/bitcoin.pdf (Accessed April 11, 2016).
2. [Dataset] coinmarketcap. Today's Cryptocurrency Prices by Market Cap (2021). Available at: https://coinmarketcap.com (Accessed January 202124.
3. [Dataset] Buterin V. Ethereum White Paper (2013). Available at: https://ethereum.org/en/whitepaper/(Accessed February 28, 2021).
4. Popper N. *Digital Gold*. New York: HarperCollins (2015).
5. Tasca P, and Tessone CJ. A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger* (2019) 4:1-39. doi:10.5195/ledger.2019.140
6. Spychiger F, Tasca P, and Tessone CJ. Unveiling the Importance and Evolution of Design Components Through the "Tree of Blockchain". *Front Blockchain* (2021) 3:60. doi:10.3389/fbloc.2020.613476
7. Reid F, and Harrigan M. An Analysis of Anonymity in the Bitcoin System. In: 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing (2011). 1318–26. doi:10.1109/PASSAT/SocialCom.2011.79
8. Garcia D, Tessone CJ, Mavrodiev P, and Perony N. The Digital Traces of Bubbles: Feedback Cycles Between Socio-Economic Signals in the Bitcoin Economy. *J R Soc Interf* (2014) 11:20140623. doi:10.1098/rsif.2014.0623
9. Bovet A, Campajola C, Mottes F, Restocchi V, Vallarano N, Squartini T, et al. The Evolving Liaisons Between the Transaction Networks of Bitcoin and its Price Dynamics. *arXiv* [Preprint] (2019). Available from https://arxiv.org/abs/1907.03577.
10. Wheatley S, Sornette D, Huber T, Reppen M, and Gantner RN. Are Bitcoin Bubbles Predictable? Combining a Generalized Metcalfe's Law and the Log-Periodic Power Law Singularity Model. *R Soc Open Sci* (2019) 6:180538. doi:10.1098/rsos.180538
11. Vallarano N, Tessone CJ, and Squartini T. Bitcoin Transaction Networks: An Overview of Recent Results. *Front Phys* (2020) 8:286. doi:10.3389/fphy.2020.00286
12. Barabási A-L, and Pósfai M. *Network Science*. Cambridge: Cambridge University Press (2016).
13. Newman MEJ. The Structure and Function of Complex Networks. *SIAM Rev* (2003) 45:167–256. doi:10.1137/s003614450342480
14. Cimini G, Squartini T, Saracco F, Garlaschelli D, Gabrielli A, and Caldarelli G. The Statistical Physics of Real-World Networks. *Nat Rev Phys* (2019) 1:58–71. doi:10.1038/s42254-018-0002-6
15. Mariani MS, Ren Z-M, Bascompte J, and Tessone CJ. Nestedness in Complex Networks: Observation, Emergence, and Implications. *Phys Rep* (2019) 813:1–90. doi:10.1016/j.physrep.2019.04.001
16. Schweitzer F, Fagiolo G, Sornette D, Vega-Redondo F, Vespignani A, and White DR. Economic Networks: The New Challenges. *Science* (2009) 325:422–5. doi:10.1126/science.1173644
17. Vespignani A. Modelling Dynamical Processes in Complex Socio-Technical Systems. *Nat Phys* (2012) 8:32–9. doi:10.1038/nphys2160
18. Price DDS. A General Theory of Bibliometric and Other Cumulative Advantage Processes. *J Am Soc Inf Sci* (1976) 27:292–306. doi:10.1002/asi.4630270505
19. Barabási A-L, and Albert R. Emergence of Scaling in Random Networks. *Science* (1999) 286:509–12. doi:10.1126/science.286.5439.509
20. Albert R, and Barabási A-L. Statistical Mechanics of Complex Networks. *Rev Mod Phys* (2002) 74:47–97. doi:10.1103/RevModPhys.74.47
21. Eom Y-H, and Fortunato S. Characterizing and Modeling Citation Dynamics. *Plos One* (2011) 6:e24926–7. doi:10.1371/journal.pone.0024926
22. Alstott J, Bullmore E, and Plenz D. Powerlaw: A python Package for Analysis of Heavy-Tailed Distributions. *Plos One* (2014) 9(1):e85777. doi:10.1371/journal.pone.0085777
23. Krapivsky PL, Redner S, and Leyvraz F. Connectivity of Growing Random Networks. *Phys Rev Lett* (2000) 85:4629–32. doi:10.1103/PhysRevLett.85.4629
24. Kondor D, Pósfai M, Csabai I, and Vattay G. Do the Rich Get Richer? an Empirical Analysis of the Bitcoin Transaction Network. *Plos One* (2014) 9:e86197. doi:10.1371/journal.pone.0086197
25. Di Francesco Maesa D, Marino A, and Ricci L. Data-Driven Analysis of Bitcoin Properties: Exploiting the Users Graph. *Int J Data Sci Anal* (2018) 6:63–80. doi:10.1007/s41060-017-0074-x
26. [Dataset] Sommer D. Processing Bitcoin Blockchain Data Using a Big Data-specific Framework (2019). Available at: https://files.ifi.uzh.ch/CSG/staff/scheid/extern/theses/BA-D-Sommer.pdf (Accessed February 03, 2021).
27. Liang J, Li L, and Zeng D. Evolutionary Dynamics of Cryptocurrency Transaction Networks: An Empirical Study. *Plos One* (2018) 13(8):e0202202. doi:10.1371/journal.pone.0202202
28. Guo D, Dong J, and Wang K. Graph Structure and Statistical Properties of Ethereum Transaction Relationships. *Inf Sci* (2019) 492:58–71. doi:10.1016/j.ins.2019.04.013
29. Somin S, Gordon G, and Altshuler Y. Social Signals in the Ethereum Trading Network. *arXiv* [Preprint] (2018). Available from https://arxiv.org/abs/1805.12097.
30. Ferretti S, and D'Angelo G. On the Ethereum Blockchain Structure: A Complex Networks Theory Perspective. *Concurrency Comput Pract Experience* (2020) 32:e5493. doi:10.1002/cpe.5493
31. Somin S, Gordon G, Pentland A, Shmueli E, and Altshuler Y. Erc20 Transactions over Ethereum Blockchain: Network Analysis and Predictions. *arXiv* [Preprint] (2020). Available from https://arxiv.org/abs/2004.08201.
32. Lin D, Wu J, Yuan Q, and Zheng Z. Modeling and Understanding Ethereum Transaction Records via a Complex Network Approach. *IEEE Trans Circuits Syst* (2020) 67:2737–41. doi:10.1109/tcsii.2020.2968376
33. [Dataset] Medvedev E. Ethereum Etl (2020). Available at: https://github.com/blockchain-etl/ethereum-etl. A set of tool for Ethereum data transformation.
34. [Dataset] etherscan.io. Blockchain Size (Mb). The Total Size of the Blockchain Minus Database Indexes in Megabytes (2021). Available at: https://etherscan.

io/tokens?sortcmd=remove&sort=marketcap&order=desc (Accessed January 13, 2021).
35. Ethereum.org ERC-20 Specification.) (2015). Available from https://ethereum.org/en/developers/docs/standards/tokens/erc-20/ (Accessed March 5, 2021).
36. [Dataset] Binance. Binance Coin Whitepaper (2017). Available at: https://whitepaper.io/document/10/binance-whitepaper (Accessed March 06, 2021).
37. [Dataset] Tether. Tether Whitepater (2016). Available at: https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf (Accessed February 28, 2021).
38. [Dataset] coinmarketcap.com. Top Defi Tokens by Market Capitalization (2021). Available at: https://coinmarketcap.com/defi (Accessed February 03, 2021).
39. [Dataset] Ellis S, Juels A, and Nazarov S. Chainlink, a Decentralized Oracle Network (2017). Available at: https://link.smartcontract.com/whitepaper (Accessed March 05, 2021).
40. Antonopoulos A, and Wood G. *Mastering Ethereum (O'Reilly Media)* (2019).
41. Dorogovtsev SN, and Mendes JFF. Evolution of Networks. *Adv Phys* (2002) 51: 1079–187. doi:10.1080/00018730110112519
42. Kunegis J, Blattner M, and Moser C. Preferential Attachment in Online Networks: Measurement and Explanations. *arXiv* [Preprint] (2013). Available from https://ui.adsabs.harvard.edu/abs/2013arXiv1303.6271K.
43. Devroye L. *Non-Uniform Random Variate Generation*. New York: Springer-Verlag (1986).
44. Levy M, and Solomon S. New Evidence for the Power-Law Distribution of Wealth. *Physica A: Stat Mech its Appl* (1997) 242:90–4. doi:10.1016/s0378-4371(97)00217-3
45. Brzezinski M. Do wealth Distributions Follow Power Laws? Evidence from 'rich Lists'. *Physica A: Stat Mech its Appl* (2014) 406:155–62. doi:10.1016/j.physa.2014.03.052
46. Clauset A, Shalizi CR, and Newman MEJ. Power-law Distributions in Empirical Data. *SIAM Rev* (2009) 51:661–703. doi:10.1137/070710111
47. [Dataset] NY Attorney General Press Release. Attorney General Annouces Ongoing Investigation into Bitfinex and Tether (2019). Available at: https://ag.ny.gov/press-release/2019/attorney-general-james-announces-court-order-against-crypto-currency-company (Accessed March 12, 2021).
48. Dong G, Wang F, Shekhtman LM, Danziger MM, Fan J, Du R, et al. Optimal Resilience of Modular Interacting Networks. *Proc Natl Acad Sci USA* (2021) 118:e1922831118. doi:10.1073/pnas.1922831118
49. [Dataset] Medvedev E. Ethereum-etl Data in Google Cloud (2018). Available at: https://console.cloud.google.com/bigquery?p=bigquery-public-data&d=crypto_ethereum&t=transactions&page=table (Accessed August 03, 2021).
50. [Dataset] Medvedev E. Ethereum-etl in Google Cloud Deep Dive (2018). Available at: https://cloud.google.com/blog/products/data-analytics/ethereum-bigquery-how-we-built-dataset (Accessed August 03, 2021).

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Advantages of publishing in Frontiers

OPEN ACCESS
Articles are free to read for greatest visibility and readership

FAST PUBLICATION
Around 90 days from submission to decision

HIGH QUALITY PEER-REVIEW
Rigorous, collaborative, and constructive peer-review

TRANSPARENT PEER-REVIEW
Editors and reviewers acknowledged by name on published articles

Frontiers
Avenue du Tribunal-Fédéral 34
1005 Lausanne | Switzerland

Visit us: www.frontiersin.org
Contact us: frontiersin.org/about/contact

REPRODUCIBILITY OF RESEARCH
Support open data and methods to enhance research reproducibility

DIGITAL PUBLISHING
Articles designed for optimal readership across devices

FOLLOW US
@frontiersin

IMPACT METRICS
Advanced article metrics track visibility across digital media

EXTENSIVE PROMOTION
Marketing and promotion of impactful research

LOOP RESEARCH NETWORK
Our network increases your article's readership