Cryptoeconomic User Behavior in the Acute Stages of Geopolitical Conflict

Jorão Gomes Jr., *Member, IEEE*, Heder Bernardino, *Member, IEEE*, Alex Borges Vieira, Verena Dorner, and Davor Svetinovic, *Senior Member, IEEE*

***Abstract*—Geopolitical conflicts significantly impact financial networks and systems, e.g., Russia and Ukraine. Cryptoeconomic blockchains such as Bitcoin and Ethereum were introduced as substitutes for traditional financial systems and might behave differently under significant stress. The Russia–Ukraine conflict allowed us to analyze the impact of such complex geopolitical conflicts on the user behaviors of cryptoeconomic blockchains. This article investigates the early stage of such geopolitical conflict using time-varying graphs. We collected and analyzed all the transactions for Bitcoin and Ethereum that took place 2 weeks before and after the conflict started, i.e., we focused on what can be defined as the acute impact of such an event. Our results suggest that the early stage of such geopolitical conflicts may significantly affect cryptoeconomic blockchains' user behaviors. For instance, we detected that some users behaved more cautiously during the preconflict phase and resumed normalcy during the postconflict phase but exhibited a shift in their behavior. This article analyzes the relationship between the early stages of geopolitical conflicts and cryptoeconomic systems.**

***Index Terms*—Behavior analysis, blockchain (BC), cryptoeconomic, geopolitical conflicts, time-varying graphs.**

I. Introduction

GEOPOLITICAL conflicts and tensions such as wars, pandemics, and energy crises have had a significant worldwide impact during the last few year [1], [2], [3]. Geopolitical conflicts can strongly impact the world economy [4]. Russia–Ukraine conflict is one of the main ones the world experienced in 2022, where significant impacts were evident in equity markets, energy markets, etc. [1], [3]. Restrictions were imposed on banking services in some regions with significant monetary losses [5], [6]. Entities must find another way to transact their money without the capacity to exchange money through frontiers.

Cryptoeconomic assets came as a solid alternative to allow users to regain control of their accounts. Cryptoeconomic assets have the inner characteristic of privacy and security preservation, giving the users full control of their assets [7]. For example, cryptoeconomic blockchain users can have as many accounts (wallets) as they need. These accounts are anonymous (or pseudoanonymous) and are only controlled by the owners of these accounts and do not have any centralized control as a bank or government entity. Besides that, in theory, no one knows who owns that account if they do not reveal themselves. That pseudoanonymous and distributed characteristic makes the user of cryptoeconomic assets privacy-protected and secure since no centralized or third-party agency can control and lock the assets of the users [8].

During geopolitical conflicts, the increasing use of cryptoeconomic blockchains such as Bitcoin and Ethereum has drawn attention to their potential as alternative financial systems allowing individuals to maintain control over their financial transactions in the face of government restrictions [9]. Analyzing the behavior of crypto users during such events is critical to understanding the potential impact of geopolitical conflicts on the cryptoeconomics blockchains [9], [10]. Therefore, it is essential to investigate how users behaved during the conflict to determine the resilience and adaptability of these assets and their potential to function as a viable alternative financial system.

Blockchains can be characterized as complex network systems [11], [12], [13]. Several methods have been used to analyze complex networks and the behaviors of their users [11], [12], [13], [14], [15], [16]. However, very few studies have specifically focused on the behaviors of users of cryptoeconomic blockchains during a geopolitical conflict [10]. Even more, no one has analyzed the behaviors of users of multiple cryptoeconomic blockchains during a geopolitical conflict in a time-varying way. The time-varying approach can be used to analyze the growth and usability of these assets over time, evaluating the changes in the network and providing a more comprehensive understanding of how cryptoeconomic blockchains were used within a time frame, generating a realist model of the system [10], [17].

In this sense, this article aims to investigate the impacts and advances of cryptoeconomics blockchains during the early,

Manuscript received 17 April 2023; revised 20 October 2023 and 11 April 2024; accepted 20 May 2024. *(Corresponding author: Davor Svetinovic.)*

Jorão Gomes Jr. and Verena Dorner are with the Institute for Digital Ecosystems, Department of Information Systems and Operations Management, Vienna University of Economics and Business, Vienna 1090, Austria (e-mail: jorao.gomes.junior@wu.ac.at; verena.dorner@wu.ac.at).

Heder Bernardino and Alex Borges Vieira are with the Department of Computer Science, Federal University of Juiz de Fora (UFJF), Juiz de Fora 36036-900, Brazil (e-mail: heder@ice.ufjf.br; alex@ice.ufjf.br).

Davor Svetinovic is with the Center for Secure Cyber-Physical Systems, Department of Computer Science, Khalifa University, Abu Dhabi, UAE, and also with the Department of Information Systems and Operations Management, Vienna University of Economics and Business, Vienna 1090, Austria (e-mail: dsve@acm.org).

Digital Object Identifier 10.1109/TCSS.2024.3404590

acute stages of the Russia–Ukraine conflict in a time-varying graph way. To do so, we analyzed the current leading cryptoeconomics blockchains: Bitcoin and Ethereum. The three research questions (RQ) that we answer in this article are as follows.

1) RQ1: How does the usage of cryptoeconomic blockchains change?
2) RQ2: How does the cryptoeconomic blockchain users' behavior change regarding account activities?
3) RQ3: What are the comparative aspects of user behavior on programmable platform blockchain (Ethereum) compared to pure monetary blockchain (Bitcoin)?

To answer the RQs, we collected all transactions that occurred 2 weeks before and 2 weeks after the beginning of the conflict. The analysis was performed through time-varying graphs where each node represents an account, and each edge represents a transaction between two accounts. Our findings offer a more thorough comprehension of how the cryptoeconomic blockchains were used during the early stages of the geopolitical conflict. The results show that the early stage of a geopolitical conflict significantly impacts cryptoeconomics blockchains' user behaviors. For instance, the users behaved differently for each blockchain. The users' behavior remained stable for Ethereum for a short time, while Bitcoin users became more cautious during the preconflict phase but resumed normalcy during the postconflict phase. Furthermore, Ethereum users had a small number of active accounts with a higher activity level, while Bitcoin exhibited a shift in user behavior over time regarding the funds transferred.

The remainder of the article is structured as follows. Section II presents the background. Section III presents the related work. Section IV presents the data acquisition and preprocessing. Section V presents the time-varying graph modeling. Section VI presents the results. Section VII discusses the results and study limitations. Finally, Section VIII presents our conclusions and future directions.

II. Background

This section presents the background of this article. We present information about cryptoeconomics, blockchains, complex network modeling, and behavior analysis.

A. Cryptoeconomics and Blockchains

The study of the creation and application of cryptography tools, such as blockchains, to establish protocols that control the production, distribution, and consumption of products and services in a decentralized way is known as cryptoeconomics. Cryptoeconomics research uses a combination of computer science, economics, and game theory to understand and define how to reward desirable behaviors in decentralized networks [8], [18].

As first presented by Nakamoto [8], blockchains are distributed decentralized databases (or decentralized ledgers) that employ encryption to store and transport data securely. They enable the construction of tamper-evident records of transactions known as blocks, which are linked in a chronological chain, generating the term blockchain. A transaction (tx) is an atomic transfer of data on a blockchain, and it consists of an input (in) and an output (out), where the input is a reference to a previous transaction output and the output is a new owner of the transferred asset. A block B is a data structure containing a set of transactions (T) and a header. The header contains metadata, such as a timestamp and a reference to the previous block. The hash of the header, denoted $H(B)$, is used to identify the block uniquely. The following equations present the definition of a transaction and the definition of a block, respectively:

$$tx = (\text{in}, \text{out}) \tag{1}$$

$$B = (T, H(B)). \tag{2}$$

A blockchain (BC) is a distributed ledger of blocks. It is a growing list of blocks linked together using the hash of the previous block's header. The hash of the first block, known as the genesis block, is hardcoded into the blockchain. The blockchain is append-only, meaning new blocks can only be added to the end of the chain. Any tampering with a block needs recalculating all following blocks, making it currently unfeasible due to the amount of computing power required [19]. This architecture allows blockchains to be resistant to data alteration. The following equation defines a blockchain where B_0 is the genesis block and B_i is the ith block in the chain:

$$\text{BC} = [B_0, B_1, B_2, \ldots, B_n]. \tag{3}$$

Blockchains have attracted considerable interest due to their application in cryptocurrencies, such as Bitcoin and Ethereum [8], [18]. These blockchains record and verify transactions without a central authority, using consensus protocols, such as proof-of-work and proof-of-stake, allowing a direct peer-to-peer value exchange. However, blockchains have potential applications beyond cryptocurrencies, such as supply chain management [20], [21], [22], voting systems [23], [24], and Internet of Things [25], [26]. As a result, extensive research and development are being conducted on the subject of cryptoeconomics to understand better and maximize the usage of blockchains and other cryptographic approaches in diverse contexts [27], [28], [29].

B. Behavior Analysis and Complex Networks

Behavior analysis has a long history and has been used in many sectors such as education, psychology, and business [30], [31]. Identifying the elements that affect behavior is an essential component of behavior analysis as it may assist in developing interventions that are more likely to reach desired goals successfully.

Complex network modeling is an effective method for analyzing the structure and dynamics of complex systems [32]. It entails modeling the interactions between elements in a system as a network, with each element represented as a node and each relationship represented as an edge. This method allows for examining network architecture and connection patterns, offering insights into the behavior and attributes of the system. Complex network modeling is used in many fields, including biology, physics, computer science, and social sciences, to study systems such as epidemic interactions, neural networks, and

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

social networks [33], [34], [35], [36]. It may be used for directed or undirected, weighted or unweighted, and static or dynamic networks. To evaluate the network structure and extract useful information, approaches such as graph theory, network centrality metrics, community discovery, and temporal evaluation methods can be applied [37], [38], [39].

The intersection of behavioral analysis, complex networks, and blockchain networks can be useful tools for analyzing and forecasting individual and group behavior inside decentralized systems. For example, by evaluating the interactions between different parts of a blockchain network, patterns of behavior that may be utilized to construct more effective interventions or methods for forecasting, and, consequently, ways for reducing potential dangers may be identified (e.g., suspicious activity detection, market forecasting, etc.) [40], [41]. Similarly, complex network models might aid in identifying the fundamental drivers of behavior within decentralized systems and design interventions that are more likely to achieve desired outcomes.

III. Related Work

This section presents the related work of this article. We focus on articles working with behavioral analyses, complex networks, and temporal analyses. First, we present the works that have not necessarily presented analyses during geopolitical conflicts and then the ones that have.

Valadares et al. [16] presented a way to identify the user behavior profiles in Ethereum using machine learning techniques. The authors looked at machine learning to categorize a user profile as a common or professional user based on the characteristics of their transactions. The authors argue that identifying user behavior patterns while maintaining anonymity regarding their identities offers the potential to leverage the platform. The findings demonstrated strong performance with more than 90% model accuracy, and it was also highlighted which features were most important for detecting user activity on Ethereum.

Agarwal et al. [42] proposed an approach for detecting malicious accounts in permissionless blockchains using time-varying graph properties. This research looked at how blockchain accounts have changed over time. The authors contend that it is feasible to comprehend account activity and foresee whether an account is classified as malicious or harmless by applying a temporal network characterization. Many machine-learning techniques were used to determine the most effective method for detecting criminal activity on the Ethereum blockchain. The results show that detecting suspicious accounts within different temporal time markers is possible.

Zanelatto et al. [43] addressed the lack of in-depth analysis of blockchain-based systems beyond Bitcoin, focusing on the Ethereum network. The authors modeled the network as a time-varying graph using a 3-year dataset comprising 38M unique accounts and almost 300M transactions. The analysis highlights the centralization tendency of the network in terms of users and time, as well as the formation of communities and the evolution of connected components. Overall, that work provides insights into the dynamics of a more recent blockchain platform gaining a significant share in the cryptocurrency market.

Chen et al. [35] presented a network modeling to evaluate disease propagation and predict the trend of COVID-19. Using a time-dependent SIR model, the authors show that their 1-day prediction errors are almost less than 3%. The model was extended to consider the impact of undetectable infections and illustrate the effectiveness of social distancing by analyzing the independent cascade model for disease propagation in a random network configuration. The results show that social distancing can reduce the effective speed of disease.

Oliveira et al. [10] explored the impact of the Russia–Ukraine conflict on using cryptocurrencies, particularly the Ethereum network. The study collected transaction data from 2 weeks before and after the start of the conflict, analyzing the behavior of accounts and their interactions with the Flashbots Auction service. Time-varying graphs were modeled to represent the network, and graph metrics were used to analyze changes in user behavior. The results revealed transaction volume variations and user behavior changes, indicating the potential impact of significant geopolitical conflicts on cryptocurrency usage.

In Trusin et al. [1], the authors analyzed the impacts of the Ukraine–Russia conflict over the Internet exchanges points (IXP). That work presented that the damage to the Russian network was not as severe as to the Ukrainian network, which experienced several outages. The authors demonstrate through a study of network behavior that each IXP has lost connection to an average of 11.12% of Ukrainian autonomous systems (ASes), and they have identified five significant outages as the cause of this loss. That study was performed with data collected before and after the conflict started (from 19 February 2022 to 29 April 2022).

Liadze et al. [5] used the National Institute Global Econometric Model to estimate the impact of the Russia–Ukraine conflict on the global economy in 2022. The authors estimate that the conflict would cost 1% of global gross domestic product (GDP), equivalent to $1.5 trillion in purchasing power parity, with the most significant impact on Europe, particularly Germany, France, and Italy, and the most considerable shrinkage of GDP in “developing Europe” where Ukraine is the most prominent representative, with a shrink of 30%. The authors also pointed out that the conflict should increase by 2% to global inflation in 2022 and 1% in 2023. It should be noted that no evaluation of the potential impact on the cryptocurrency market is presented in that article.

Basdekis et al. [3] presented a study that examines the interdependencies between stock market indices, exchange rates, and crude oil prices from Jan 2021 to July 2022, including the COVID-19 post-vaccination phase and Russia–Ukraine conflict. It finds strong correlations between all variables during different periods. A particular interest is the finding that the RTS Index (RTSI), the index of 50 Russian stocks traded on the Moscow Exchange, affects both European and American stock markets and determines the evolution of the Russian currency. Investors and policymakers can use the findings of that study to make decisions and limit systemic risks in capital markets.

Khalfaoui et al. [9] examined the impact of the Ukraine–Russia conflict on cryptocurrency values using Google Trends. The authors pointed out that this conflict attention negatively

TABLE I
COMPARISON BETWEEN RELATED WORK

Paper	Attributes						
	Geopolitical Event	Blockchains		Time-Varying Model	Impacts		
		Bitcoin	Ethereum		User Behavior	Network Changes	Financial and Business
Valadares et al. [16]			✓		✓		
Agarwal et al. [42]			✓	✓	✓	✓	
Zanelatto et al. [43]			✓	✓	✓	✓	
Chen et al. [35]	✓			✓	✓	✓	
Oliveira et al. [10]	✓		✓	✓	✓	✓	
Trusin et al. [1]	✓				✓	✓	
Liadze et al. [5]	✓				✓		✓
Basdekis et al. [3]	✓				✓		✓
Khalfaoui et al. [9]	✓	✓	✓		✓		✓
Thieri et al. [44]	✓	✓	✓		✓	✓	✓
Mariana et al. [45]	✓	✓	✓			✓	✓
Yousaf and Ali [46]	✓	✓	✓			✓	✓
Aspembitova et al. [41]	✓	✓	✓		✓		✓
Harb et al. [47]	✓	✓	✓		✓	✓	✓
This paper	✓	✓	✓	✓	✓	✓	✓

affects all cryptocurrencies in the short term under bearish markets and positively under normal markets, which suggests that investors respond to conflict attention by seeking liquidity. It should be noted that only crypto market value was analyzed, and no in-depth evaluation of crypto behavior was presented.

Thieri et al. [44] conducted a study on the liquidity of Bitcoin and Ethereum during the Russia–Ukraine war. They found that these cryptocurrencies' liquidity response to the conflict was not uniform. The research results indicate a notable yet transient influence of the Russia–Ukraine conflict on the liquidity of Bitcoin and Ethereum. Liquidity levels demonstrated an initial uptick within two days surrounding the event, followed by a subsequent return to preevent levels. Nevertheless, it is important to note that the liquidity response of BTC and ETH cryptocurrencies to the Russian invasion of Ukraine varied.

Mariana et al. [45] investigated whether Bitcoin and Ethereum can be considered safe havens for stocks. They found that both cryptocurrencies exhibited short-term safe-haven properties during the pandemic. This research highlights the potential role of cryptocurrencies as alternative investment assets during crisis periods. The authors found dynamic correlations and regressions, and the results show that Bitcoin and Ethereum display short-term safe-haven characteristics for stocks. Moreover, they showed that Ethereum might be a better safe haven than Bitcoin during a short extreme stock market downturn, although Ethereum exhibits higher return volatility than Bitcoin.

Yousaf and Ali [46] explored the interlinkages between Bitcoin and Ethereum during the COVID-19 pandemic. They discovered bidirectional and negative volatility spillovers between the two cryptocurrencies before the pandemic. This study contributes to understanding the relationship between Bitcoin and Ethereum and their behavior during crisis events. Optimal portfolio weights suggested decreasing investments in Bitcoin and Ethereum during the COVID-19 period, while hedge ratios indicated higher hedging costs but greater effectiveness in risk management.

Aspembitova et al. [41] focused on the behavioral structure of users in the cryptocurrency market. They observed that the composition of user behavior differed between the Bitcoin and Ethereum markets during local price fluctuations and large systemic events. They found evidence that during local events, Bitcoin users exhibit a preference for short-term perspectives, while Ethereum users adopt a longer-term outlook. In contrast, Ethereum users consistently display a more pessimistic stance toward the market's future during major systemic events, while Bitcoin users tend to be more optimistic.

Harb et al. [47] examined the volatility interdependence between cryptocurrencies, equity, and bond markets. They identified a unidirectional volatility spillover from Ethereum to Bitcoin. This study provides insights into the interconnectedness of different financial markets and the impact of cryptocurrencies on market volatility during crisis events. They found that during crises, investors seeking to safeguard against downturns in bond markets might find Ethereum a valuable asset to include in their portfolio. They believe policymakers can use their findings to inform market intervention timing, helping stabilize markets and manage uncertainties during stressful periods.

Given this overview, we highlight the difference between the related works and this article in Table I. In contrast to the other work, this article introduces a novel study of utilizing time-varying graph models to analyze the Bitcoin and Ethereum networks in the lead-up and aftermath of a significant event. To the best of our knowledge, this is the first analysis of time-varying graphs for Bitcoin and Ethereum blockchains during the early stage of a geopolitical conflict. According to our findings, this temporal model showed that the early stage of geopolitical conflicts might significantly impact the behavior of users of cryptoeconomic blockchains.

IV. Data Acquisition and Preprocessing

In this section, we discuss the data acquisition and preprocessing methods employed. To ensure clarity in our networking modeling and results sections, we have standardized the

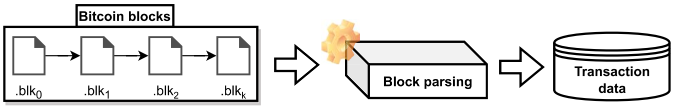

Fig. 1. Pipeline to collect the Bitcoin blockchain.

term "account" to refer to the term "wallet address" for both blockchains, thus avoiding any confusion or misinterpretation of our findings.

A. Bitcoin On-Chain Data

Bitcoin transactions are based on the unspent transaction output (UTXO) model [8]. Each transaction made by users includes inputs and outputs, except the coinbase transactions, which miners generate as a reward for adding a new block to the blockchain. The outputs of a transaction contain scripts that specific recipients can only unlock, while the input fields reference previous, unspent outputs. As a result, each new transaction is linked to the previous unspent UTXO. It is important to note that every UTXO must be fully spent and is considered invalid for future transactions. This allows for the bundling of multiple UTXOs from different transactions into a single transaction; for example, if a user received 1.0 BTC twice in two different transactions, they could bundle those UTXOs together and transfer 1.5 BTC to another account and 0.5 BTC back to an account the user generates for change [48].

As Bitcoin is a UTXO-based blockchain, it is necessary to process the whole blockchain data and map all the UTXO to create a user-based graph network ($\text{address}_1 \xrightarrow{\text{transaction}} \text{address}_2$). We set up a full Bitcoin node to connect with the blockchain to collect and model all the Bitcoin UTXO. The full node creates a copy of the Bitcoin blockchain and allows the user to download all the blocks appended to the blockchain. These blocks are stored in *.blk* files, and each file contains one or more Bitcoin blocks. The content of the *.blk* file corresponds to a binary format of the block data set. We decoded the data inside each *.blk* file to be able to collect the transactions in each block.

To perform it, we used a Bitcoin blockchain parser to parser the *.blk* file. The parser works as a decoder, translating the binary data into a readable format. The parser used in this work is open-sourced, and the code is free-available in [49]. This process is presented in Fig. 1. After the parsing process, each transaction collected was composed of the following features: timestamp, transaction hash, input-transaction hash, input vout, output account, output index, value, *.blk* file number, and script type. Table II presents the description of each feature.

We created a user-based network by mapping all the UTXOs. To accomplish this, we mapped all the input-transaction hash and input-vout to their corresponding UTXOs. These UTXOs correspond to the output-account of another transaction at a specific output-index, which in turn becomes the input-account of the transaction that spends that particular UTXO. In other words, combining the input transaction hash and vout is a unique identifier for a specific UTXO. We utilized Google BigQuery,[1] a data warehouse tool, to execute optimized SQL queries and perform the mapping of the UTXOs. We employed Neo4j to conduct the final modeling and visualization in the final stage. Neo4j[2] is a highly efficient graph database management system that utilizes a graph data model to represent data as nodes and relationships, facilitating effective querying and manipulation of large and complex data sets. As shown in Fig. 2, this combined approach allowed us to map and visualize the user-based Bitcoin network effectively.

TABLE II
BITCOIN TRANSACTION ATTRIBUTES

Attribute	Description
Timestamp	Epoch timestamp of when the transaction was successfully mined
Transaction hash	Unique identifier of the new UTXO generated by this transaction
Input transaction hash	Unique identifier of the UTXO from which this transaction originates
Input-vout	Index of the output in the previous transaction's output field
Output account	Hash code of the account that received a certain amount of coins
Output index	Index of the output account
Value	Amount of coins transferred
Block file number	Number of the *.blk* file where the transaction is stored
Script type	Type of script used to lock/unlock the transaction

B. Ethereum On-Chain Data

In contrast to Bitcoin, which is a UTXO-based network, Ethereum is an account-based network [18]. This means that Ethereum uses a different approach to manage the state of transactions and balances compared to a UTXO-based blockchain. In Ethereum, each user has a unique account associated with a balance. These balances are stored in a global state, which is updated with each transaction. When a user wants to make a transaction, the account of the recipient, the amount of Ether to be transferred, and the gas (fee used in Ethereum to process the transaction) required for the transaction to be processed must be specified. The amount of Ether then decreases the balance of the sender's account transferred, and the same amount increases the balance of the recipient's account.

The account-based model has some advantages over the UTXO model. For this article, the significant advantage of the account-based model is that it allows for more flexibility in how transactions can be structured, as it eliminates the need to reference previous transactions. This makes creating a user-based graph network more manageable once the accounts and the values transferred in each transaction are directly mapped in contrast to Bitcoin as presented in Section IV-A.

We used Etherscan.io, a widely used block explorer for the Ethereum blockchain to collect the Ethereum data. Etherscan.io[3] provides an easy-to-use interface for browsing the

[1]https://cloud.google.com/bigquery
[2]https://neo4j.com/
[3]https://etherscan.io/

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

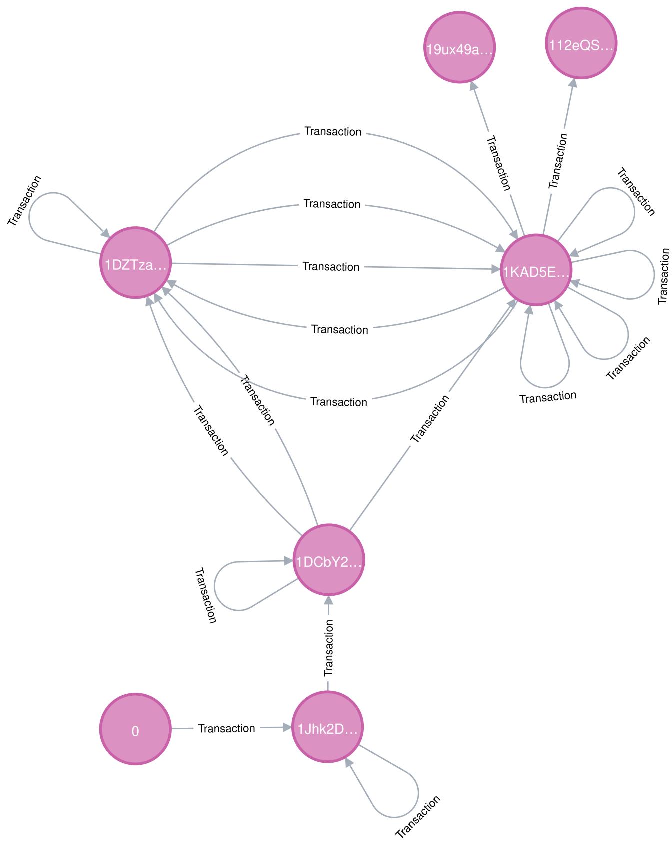

Fig. 2. Bitcoin user-based network. The self-loops correspond to the new transaction that generated UTXOs as a "change" of the transaction.

TABLE III
ETHEREUM TRANSACTION ATTRIBUTES

Attribute	Description
Timestamp	Epoch timestamp of when the transaction was successfully mined
Transaction hash	Unique identifier of the transaction via hash code
Input account	Hash code of the account that initiated the transaction
Output account	Hash code of the account that received the Ether
Value	Quantity of Ether transferred in the transaction
Block number	Number of the block where the transaction was mined

blockchain and allows users to view information about specific transactions, accounts, and smart contracts. Additionally, it offers a set of APIs that makes it easy to access and analyze the data stored in the Ethereum blockchain, including information about token holders, gas prices, and more. Using the Etherscan.io API, we extracted the following attributes from the Ethereum blockchain: transaction hash, timestamp, out-account, in-account, and transaction value. These attributes are presented in Table III along with a brief description of each feature.

In the final step, Neo4j was also used to perform the final modeling and visualization as described for the Bitcoin network in Section IV-A. The final modeling of Ethereum is similar to the one present in Fig. 2.

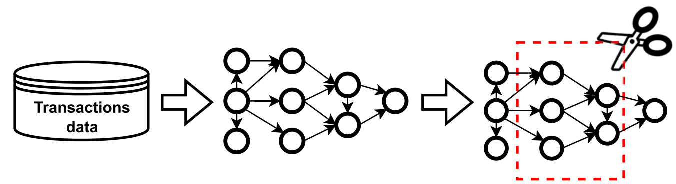

Fig. 3. Blockchain data filtering. The red dashed rectangle corresponds to the filtered data after the modeling that is analyzed.

C. Data Filtering

We filtered all the transactions confirmed within a predefined time frame to perform the analysis considering only data from the start of the Russia–Ukraine conflict. The filtered data corresponds to the data from 2 weeks before the conflict and 2 weeks after the conflict starts (from February 10th to March 10th of 2022, GMT+00:00). Fig. 3 presents an illustrative example of the temporal snapshot.

The temporal snapshot corresponds to the transactions extracted from the blocks in between the block numbers 720 000[4] and 730 000[5] for Bitcoin blockchain. The transactions analyzed in this work were extracted from the blocks in between the block numbers 14 174 989,[6] and 14 355 747[7] for Ethereum blockchain.

V. Time-Varying Graph Model

We created a user-based time-varying graph using the data described in Section IV-C. A standard graph model represents a collection of objects and their relationships. These objects are represented as nodes or vertices in the graph, and the relationships between them are represented as edges [50]. The basic structure of a graph is defined as a pair $G = (V, E)$, where V is a set of nodes shown in

$$V = \{v_0, v_1, \ldots, v_n | \, n \in \mathbb{R}\} \tag{4}$$

and E is a set of edges that represents a relationship between nodes shown in

$$E = \{(u_0, v_0), (u_1, v_1), \ldots, (u_n, v_m) \, |n, m \in \mathbb{R}, (u, v) \in V\}. \tag{5}$$

Besides that, the edges in G can be weighted to represent the importance of the relationship between the nodes or not weighted to represent that all the relationships have the same importance between the nodes.

Our time-varying graph model is based on the standard G; however, a discrete feature t is combined with the G to include the temporal feature [51]. The new G is a tuple in a format $G = (V, E, T)$, where T is a set of time instances shown in

$$T \subseteq \{0, 1, 2, \ldots, t | t \in \mathbb{N}\} \tag{6}$$

Like the standard graph, v and u represent nodes in V, and the pair (u, v) represents a relationship between the nodes u

[4]https://www.blockchain.com/explorer/blocks/btc/720000
[5]https://www.blockchain.com/explorer/blocks/btc/730000
[6]https://www.blockchain.com/explorer/blocks/eth/14174989
[7]https://www.blockchain.com/explorer/blocks/eth/14355747

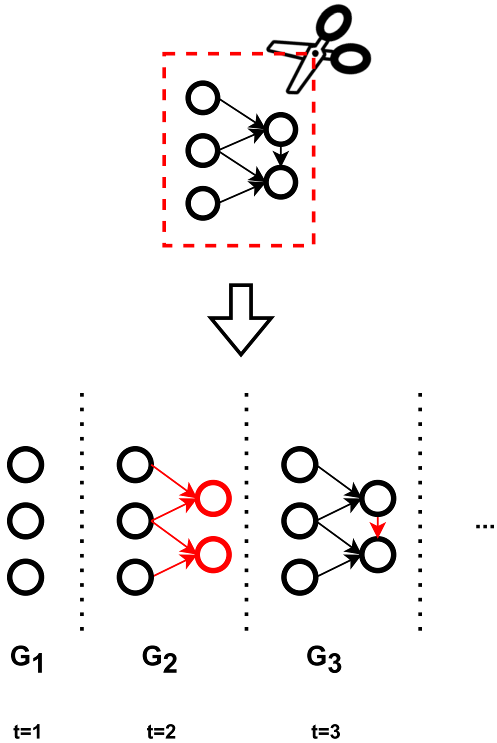

Fig. 4. Sequence of static graphs based on the temporal snapshot presented in Fig. 3. The t variable represents the timestamp of the time-varying graph, and the red color represents the new edges and nodes created after each temporal step.

and v in E. However, for time-varying graphs, (u, v) only exists in a specific time instance t that belongs to T. The time-varying graph can be represented as a sequence of static graphs $G_1, G_2, \ldots, G_t$, where each graph G_t corresponds to a subset of G at time instance t in

$$G \subseteq \{G_1, G_2, \ldots, G_t | G_t = (V, E, t), t \in T\}. \tag{7}$$

Fig. 4 presents an example of the sequence of static graphs in different timestamps based on the temporal snapshot presented in Fig. 3

To model the dynamics of the user-based time-varying graph, we can use the concept of edge activation and deactivation [52]. As presented in Fig. 4, new edges and nodes can be created after each temporal step. An edge (u, v) is defined as activated at time instance t if a transaction occurs between the nodes u and v at t, and deactivated at time instance $t + 1$ if no transaction occurs between the users u and v at $t + 1$. Besides that, edge persistence can also be used for time-varying graphs. The edge persistence is the time an edge (u, v) remains active in the graph and can be used to identify patterns, such as recurring transactions between specific users.

Based on this description, we created two user-based time-varying graphs, one for Bitcoin and another for Ethereum. For both models, we assume that each node in the time-varying graph is an account and each edge is a transaction. No weight is used for the edges. To perform the analyses, t was used to define the temporal feature in terms of weeks. In other words, G_1 refers to the first week, G_2 to the second week, and so on. As we analyze 1 month of transactions, T contains values from 1 to 4.

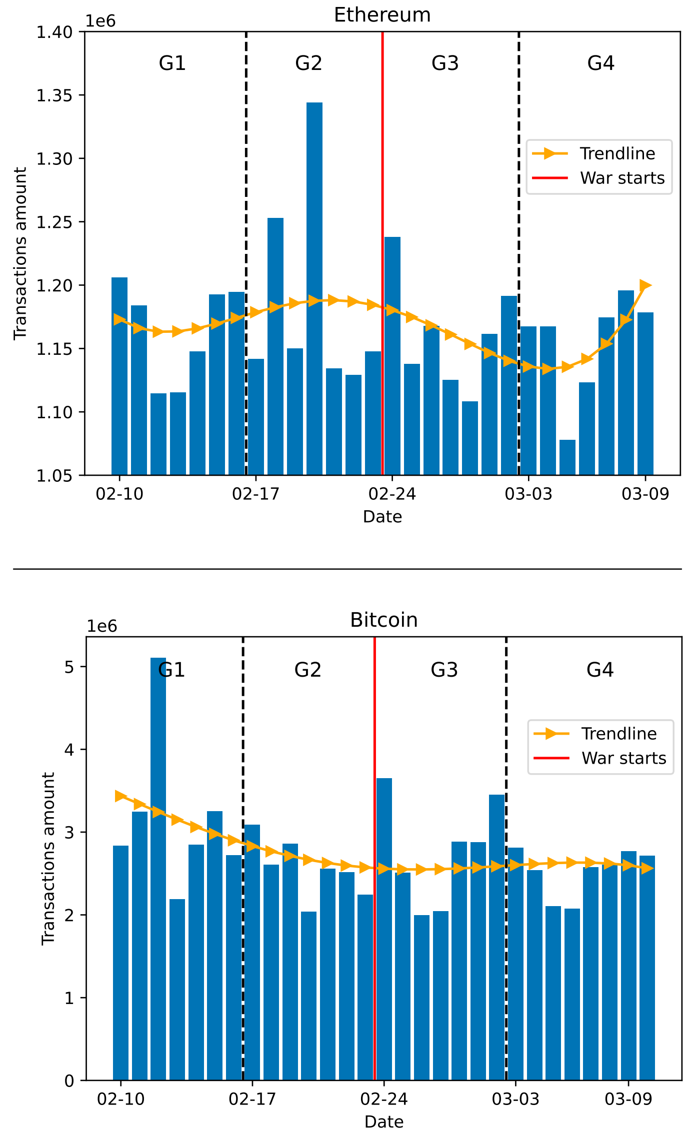

Fig. 5. Number of transactions for each time-varying graph. The red line divides the data before and after the conflict begins. Read G1, G2, G3, and G4 as time-varying graph for the first week, second week, third week, and fourth week.

VI. Results

This section presents the results and discussions. We aim to answer three RQs in this section. To do so, we performed three evaluations: the number of transactions, account activities, and funds transferred during the conflict. This section aims to present the answer to the RQs by characterizing the blockchains during the geopolitical conflict.

A. *Number of Transactions*

We generated a chart correlating the number of transactions with the corresponding date to analyze the total number of trades for each temporal subgraph. Fig. 5 presents the number of transactions and provides insights into the Russia–Ukraine conflict's impact on the networks' trading activity. Furthermore, to comprehend the overall trend in transaction volume over time, we applied a trendline of degree 4 to the chart. This degree value was chosen because we have four time-varying graphs, and we intended to identify one turning point on each.

For Ethereum, Fig. 5 shows a significant surge in transactions during mid-February, with prominent peaks occurring in the network, reaching a maximum of approximately 1.35 million trades around February 20th. However, after 20 February, there was an evident drop in the number of transactions. The total daily transactions decreased to less than 1.10 million at the beginning of March. These findings suggest that the invasion had a profound impact on the trading activity of the network. The transaction surge may indicate a reaction to the conflict, with users buying or selling assets in response to the invasion. Also, the trendline for the number of transactions supports this conclusion and shows that the user tended to decrease the number of transactions on Ethereum. On the other hand, the decline in the number of transactions after the conflict may reflect a loss of confidence in the network or a shift in user behavior, for instance, starting using another blockchain (e.g., Bitcoin). Overall, the analysis of transaction data provides valuable insights into the network dynamics and the impact of external events on its activity.

When the Bitcoin chart is analyzed, observing a contrary behavior to the Ethereum network is possible. Although it is possible to observe a peak during the first week before the conflict begins, the transactions in the network tended to be stable during the conflict. Furthermore, soon after the conflict begins, another peak appears and shows that the users start using the network more than before. Regardless of the number of transactions of each blockchain, the tendency to use Bitcoin during the conflict instead of Ethereum is evident. The Bitcoin trendline confirms that users started to use even more Bitcoin networks after the conflict. This behavior is expected for crypto users since Bitcoin is supposed to be a hedge against inflation, and so used to save money, even though the network has not yet proven this behavior and has still been studied by academia and economists [53], [54], [55]. Users of other blockchains (e.g., Ethereum) might have shifted/increased the number of transactions in Bitcoin to look for a safer way to protect their savings.

B. Account Activities

We created time charts that depict the activity of the nodes over the analyzed period, along with the volume of active accounts against the creation of new accounts. Our results, shown in Fig. 6, provide a comprehensive overview of the analyzed period. A similar trendline of degree 4 was created for this chart.

As shown in Fig. 6, for Ethereum, despite a slight decrease in active accounts between 10 and 24 February, there was a consistent activity level among the accounts, with the volume of active nodes remaining stable between 450 000 and 550 000. Following this period, a visible growth trend persisted until the beginning of March. These findings provide insights into the network dynamics, suggesting that the invasion did not significantly impact the account activity but only on the number of transactions, as shown in Fig. 5. The consistent activity

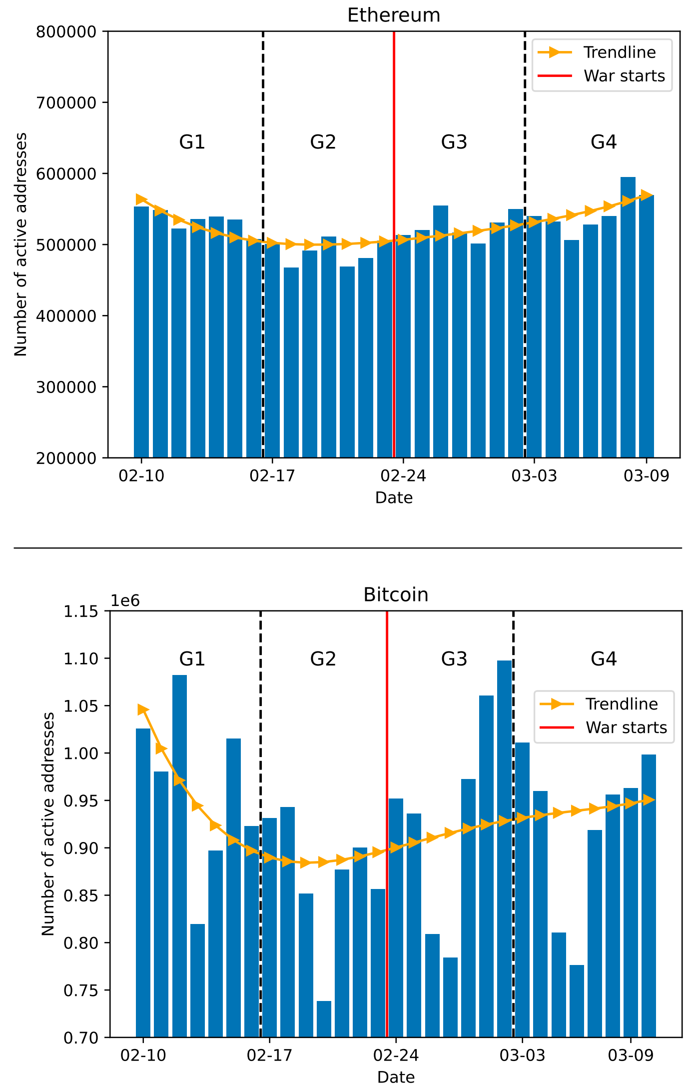

Fig. 6. Evolution of the networks in terms of active accounts. Read G1, G2, G3, and G4 as time-varying graphs for the first week, second week, third week, and fourth week.

level observed among the accounts indicates a stable user base. In contrast, the growth trends in the number of active nodes and new accounts suggest a positive outlook for the network's growth. Overall, combined with the results presented in Fig. 5, the analysis of Ethereum highlights the importance of examining account activity to gain insights into the network's dynamics and growth potential.

In contrast to Ethereum, Bitcoin did not exhibit the same level of consistency regarding active accounts, regardless of the number of active accounts for each blockchain. During the preconflict phase 10 to 24 February), a significant decline was observed in the number of active accounts using the network. This suggests that Bitcoin users became more cautious in their network activities, likely to protect their funds. This event coincides with the data presented in Fig. 5, where a similar decay is observed in the number of confirmed Bitcoin transactions. However, there was a resurgence in account activities in the postconflict phase (24 February to 10 March), indicating a return to normalcy.

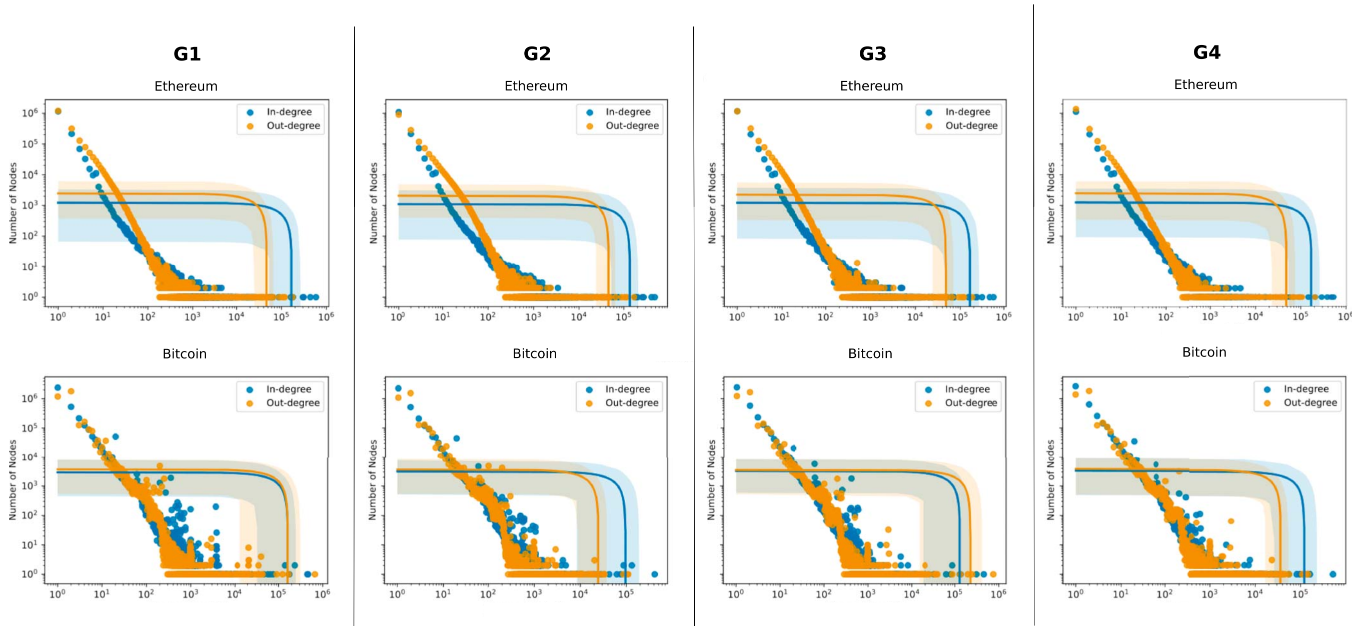

Fig. 7. Evolution of transferred funds per account. The in-degree stands for the number of transactions received by a node, and the out-degree stands for the number of transactions sent by a node. Read G1, G2, G3, and G4 as time-varying graphs for the first week, second week, third week, and fourth week.

C. Transferred Funds

We analyzed the transferred funds by examining the distribution of values of different inflows and outflows between accounts for each time-varying graph. Fig. 7 evaluates transferred funds per account. The results in Fig. 7 show the behavior of different accounts within the network and make it possible to identify patterns and trends in the flow of funds between accounts for each timestamp of the time-varying graph.

Fig. 7 shows that the accounts in Ethereum presented high in-degree, but the out-degree did not reach such high values. These results suggest a small number of accounts with a higher activity level in distributing transactions to different accounts. In contrast, the majority of accounts received only a few transactions. Furthermore, the curves of in-degree and out-degree are observed not to be very close to each other, indicating an unbalanced behavior of fund transfer in the network. This pattern is similar across all timestamps of the temporal subgraphs analyzed in this research, suggesting that the behavior of the network did not change significantly over time.

Analyzing temporal subgraphs in Bitcoin reveals a notable shift in user behavior over time. During the first week (G1), users sent and received funds roughly equally, with the in-degree and out-degree curves almost overlapping. However, this pattern changed in the second week (G2), as users began to receive more funds than they sent, and the in-degree curve began to lead the out-degree curve. The onset of conflict in the third week (G3) brought about a contradictory behavior, with users sending more funds instead of receiving them, resulting in the out-degree curve taking the lead over the in-degree curve. Finally, in the fourth week (G4), users reverted to receiving more funds than they sent, as demonstrated by the in-degree curve leading the out-degree curve once again. These findings provide valuable insights into the dynamic behavior of users in Bitcoin and highlight the potential impact of external events on crypto user behavior. Besides that, the findings in this chart connect to the ones presented previously in Figs. 5 and 6 for both blockchains.

VII. Discussion and Limitations

The implications of the early stage of the geopolitical strife on the behavior of users within the cryptoeconomic blockchain realm are reflected in our findings. This section addresses each RQ individually and provides a succinct overview of our charts and discussion.

Regarding RQ1, Ethereum experienced a surge in transactions during mid-February, followed by a decrease in transactions. The number of active accounts was stable, and a visible growth trend persisted until the beginning of March. Bitcoin experienced a peak in the number of transactions observed during the first week before the conflict began, and the transactions in the network tended to be stable during the event. There was a resurgence in account activities, indicating a return to normalcy after the conflict.

Regarding RQ2, Ethereum experienced a consistent activity level observed among the accounts, with a small number of accounts having a higher activity level in distributing transactions to different accounts. The in-degree curve was higher than the out-degree curve, suggesting an unbalanced behavior of fund transfer. Bitcoin experienced a significant decline in active network accounts during the preconflict phase, indicating that Bitcoin users became more cautious in their network activities, likely to protect their funds. Users sent and received funds roughly equally during the first week, but this pattern changed over time due to external events. The in-degree and out-degree curves almost overlapped during the first week, but the in-degree curve began to lead the out-degree curve during the second week, and the out-degree curve took the lead over the in-degree curve during the third week. In the fourth week, users reverted to receiving more funds than they sent, with the in-degree curve again leading to the out-degree curve.

Regarding RQ3, Ethereum experienced a decrease in the number of transactions on Ethereum, reflecting a loss of confidence in the network or a shift in user behavior toward other blockchains, such as Bitcoin. On the other hand, Bitcoin experienced an increase in the number of transactions, suggesting that Bitcoin was seen as a hedge against inflation.

We used the efficient market hypothesis (EMH) to analyze the three RQs from the financial and economic perspective. EMH [56] is a theory suggesting that asset prices in financial markets fully reflect all available information. Note EMH is not solely about price movements. It encompasses the idea that all available information is efficiently incorporated into asset prices. This information includes not only price-related data but also fundamental, transactional, and other relevant information. As we examine how users' behavior and transaction patterns change in response to a significant geopolitical event, if market participants efficiently process and act upon this information, it should be reflected in prices and transaction volumes, account activities, and funds transferred. In the discussion below, we use the term *market metrics* to clarify this.

There are three forms of the EMH: weak, semistrong, and strong, discerning different claims about information reflected in market metrics. Our assumption on what one would expect to observe from the standpoint of the EMH in the context of Ethereum and Bitcoin during the acute phase of a geopolitical conflict.

1) In the weak form, market metrics would fully reflect all past trading information, such as historical prices and volumes. During the acute phase of a geopolitical conflict, one would expect that any information available up to that point is already reflected in the market metrics of Ethereum and Bitcoin. Therefore, market metric movements in response to the conflict may not necessarily be predicted by analyzing past market metric data alone.
2) In the semistrong form, market metrics would fully reflect all publicly available information, including past trading information and all public news and events. If the market is semistrong efficient, the market participants would have already incorporated information about the geopolitical conflict into the market metrics of Ethereum and Bitcoin before and during the conflict. Any new information or developments related to the conflict would lead to immediate market metric adjustments.
3) In the strong form, market metrics would fully reflect all information, including public and private information. If the market is strong-form efficient, it implies that even insider information would not provide an advantage, as all information is already priced. Therefore, any significant reactions in the market metrics of Ethereum and Bitcoin during the acute phase of the conflict would challenge the notion of strong-form efficiency, as it would suggest that some participants have access to information not yet reflected in market metrics.

So, if the crypto markets for Ethereum and Bitcoin are efficient, we expect market metrics to incorporate information about the geopolitical conflict already. Any significant market metric movements during the acute phase of the conflict would raise questions about the efficiency of these markets, especially in the semistrong and strong forms. Observing substantial market metric changes during this period could suggest that market participants are reacting to new information or uncertainties related to the conflict.

According to our findings, while there were no substantial price changes, Ethereum experienced a surge in transactions during mid-February, followed by a decrease in transactions. The number of active accounts remained stable, and there was a visible growth trend until the beginning of March. These observations suggest significant changes in Ethereum's usage and user behavior during the acute phase of the conflict. From an EMH perspective, this could indicate that market participants may not have fully incorporated all available information about the conflict into Ethereum's market metric and usage patterns. Otherwise, such pronounced changes might not be expected.

Our findings indicate that Bitcoin experienced a peak in the number of transactions just before the conflict, followed by stable transaction levels during the event. There was a resurgence in account activities, suggesting a return to normalcy after some time. Like Ethereum, these observations suggest that the conflict affected Bitcoin's usage patterns and user behavior. Significant changes in user behavior and transaction volumes might not be expected in an efficient market unless new information about the conflict emerges during this period.

Thus, given that the EMH suggests that market metrics and behavior should fully reflect available information if the markets for Ethereum and Bitcoin were completely efficient, one might not expect such noticeable changes in transaction patterns and user behavior during the acute phase of the geopolitical conflict. The observed changes in activity and behavior could imply that market participants were reacting to the unfolding events or that new information emerged during the conflict period.

While this information is important for interpreting the results, it is also important to remember that the EMH is a theory, and real-world markets may not always conform to its assumptions [57]. Factors like market sentiment, behavioral biases, and information dissemination mechanisms can lead to deviations from strict efficiency [58], [59].

In conclusion, our findings suggest that the Ethereum and Bitcoin markets did not fully adhere to the EMH during the acute phase of the geopolitical conflict. Instead, there were observable changes in transaction volumes and user behavior, which may indicate that market participants were reacting to new information or uncertainties related to the conflict. This underscores the complexity and nuance of real-world financial markets, especially in the context of rapidly changing geopolitical events.

In practical terms, our findings, which indicate shifts in transaction volumes, account activities, and fund transfers during the geopolitical conflict, have behavioral implications. These shifts could be seen as responses to new information or changes in market sentiment, which are central elements of EMH. Thus, the identified lack of adherence to EMH can inform the impacts of future events on cryptoeconomic systems along the lines.

1) There might be a significant information lag that can be exploited. The observed deviations from EMH suggest that information may not be instantaneously and fully incorporated into these cryptocurrencies' market metrics and behavior. This could imply that market participants take time to process and respond to new information, especially during significant geopolitical events.
2) There might still be a significant impact of behavioral factors. Market behavior in cryptocurrencies may be influenced by factors beyond rational assessments of information, e.g., fear, uncertainty, and other emotional factors that can drive market movements. The size of both Ethereum and Bitcoin seem not to be able to absorb them yet fully.
3) There are still significant inefficiencies present. The deviations from EMH indicate that some level of inefficiency exists in the cryptocurrency markets. Inefficient markets allow traders and investors to profit from market metric discrepancies or potential mispricing.
4) There is still significant market sensitivity present. Cryptocurrency markets, being relatively young and driven by a unique set of factors, might be more sensitive to external events like geopolitical conflicts.

In summary, the observation that Bitcoin and Ethereum do not fully adhere to the Efficient Market Hypothesis during geopolitical conflicts highlights the unique nature of cryptocurrency markets. Complex factors influence these markets, including rational information and behavioral elements assessments. The observed behavior changes can be considered indirect indicators of how market participants react to information, uncertainty, or external events, all of which are relevant to EMH. Understanding these dynamics is crucial for cryptocurrency ecosystem participants and researchers seeking to analyze, model, and improve these markets.

A. Limitations

The present study has certain limitations that need to be acknowledged. First, the data collection period was confined to 2 weeks before and after the commencement of the Russia–Ukraine conflict. Although this duration provided significant insights into the acute stage of the conflict, extending the data collection period could yield a more comprehensive understanding of cryptoasset usage during the chronic stages. Nonetheless, even with the given timeframe, the data analyzed in this study corresponds to more than 100 x 1e6 confirmed transactions among blockchains during the pre and postconflict phases.

Second, this study only evaluated two specific blockchains, Bitcoin and Ethereum, instead of assessing the entire crypto market. While these two blockchains are among the largest and most popular, they do not represent the entire crypto market. Future research should consider evaluating other smaller market capitalization blockchains and exploring their impact and resilience during geopolitical conflicts. Additionally, this study relied on publicly available data, which may not be entirely accurate or complete. Future research should consider incorporating additional data sources to enhance the reliability of the findings.

Third, we have chosen to utilize relatively straightforward data analytics techniques instead of more intricate network science analyses employed in our prior work [60] and in the parallel research by the same authors [48]. This decision is grounded in considering the applicability of network science techniques within financial analysis, particularly in the context of blockchain and cryptocurrency. While valuable for investigating complex network structures, network science methods often present challenges related to their complexity and interpretability when applied to financial data. In the context of blockchain, finding meaningful correlations can be elusive due to the high volatility and multifaceted nature of blockchain data. We were unable to do this in [60]. As our primary focus is to understand the impact of geopolitical conflicts on user behavior and transaction patterns within blockchain networks, particularly Ethereum and Bitcoin, we have opted for simpler data analytics techniques that are better suited for addressing our specific RQs. This choice ensured a more direct examination of changes in usage patterns and user behaviors during the acute phase of the conflict, aligning with the methodological suitability for our research objectives.

It is important to note that there is evidence that geopolitical conflicts can impact Bitcoin, affecting its correlation with other financial assets and its role as a safe haven or hedge. Research by Bouri et al. [61] indicates that Bitcoin's response to jumps in geopolitical risk highlights its potential as a hedge against such risks. Additionally, Kyriazis [62] emphasizes that geopolitical risk significantly influences Bitcoin's volatility and risk premia, underscoring the impact of uncertainties on the cryptocurrency.

Moreover, Su et al. [63] explore the influence of geopolitical risk on the Bitcoin market, suggesting that such risk can alter the correlation structure between Bitcoin and other assets. This implies that geopolitical events can impact Bitcoin's relationship with traditional financial instruments. Furthermore, Aysan et al. [64] suggest that Bitcoin can be a hedging tool against global geopolitical risks, showcasing its potential as a risk management instrument during uncertain times.

While Bitcoin is commonly viewed as a diversifier due to its low correlation with traditional assets, Song et al. [65] propose that Bitcoin can also function as a safe haven during violent geopolitical conflicts. This suggests that investors might consider Bitcoin a store of value in times of heightened geopolitical tensions.

Thus, the research supports the idea that Bitcoin's correlation with geopolitical conflicts is a significant study area and what our study has built upon. The findings suggest that Bitcoin's behavior can be influenced by geopolitical risk, and our findings have shown detailed insights into how it reflects within the system in the acute stages of the conflict.

In conclusion, while this study provides valuable insights into cryptoasset usage during the acute stage of the Russia–Ukraine conflict, it is crucial to consider the study's limitations when interpreting the results. Further research is necessary to expand the data collection period and evaluate the crypto market as a whole.

VIII. Conclusion

This study aimed to investigate the impacts and advances of cryptoassets during the Russia–Ukraine geopolitical conflict by analyzing the usage and behavior of cryptoassets in a time-varying graph way. The study collected and analyzed transactions that occurred 2 weeks before and 2 weeks after the beginning of the conflict for the two leading blockchains, Bitcoin and Ethereum, and aimed to answer RQs related to the increase of cryptoassets usage, the characterization of crypto assets' users' behavior, and the comparison of the behavior of users of different blockchains during the early stage of such geopolitical conflict.

The results of this study provide a more comprehensive understanding of how cryptoeconomic blockchains were used during this geopolitical conflict and can be used to understand how crypto users behave during events with social and economic impact. Our results might help predict how geopolitical conflicts can impact other cryptoeconomic blockchains. Future work aims to expand the study's timeframe to investigate the crypto market dynamics after the conflict and examine the impact of regulations and policies on crypto assets. Expanding the timeframe collected can improve the results by providing a more comprehensive understanding of the crypto market and its behavior during and after the geopolitical conflict.

References

[1] C. Trusin, L. Bertholdo, and J. J. Santanna, "The effect of the Russian-Ukrainian conflict from the perspective of internet exchanges," in *Proc. 18th Int. Conf. Netw. Service Manage. (CNSM),* Piscataway, NJ, USA: IEEE Press, 2022, pp. 261–267.

[2] H.-C. Sun, X.-F. Liu, Z.-W. Du, X.-K. Xu, and Y. Wu, "Mitigating COVID-19 transmission in schools with digital contact tracing," *IEEE Trans. Comput. Social Syst.*, vol. 8, no. 6, pp. 1302–1310, Dec. 2021.

[3] C. Basdekis, A. Christopoulos, I. Katsampoxakis, and V. Nastas, "The impact of the Ukrainian war on stock and energy markets: A wavelet coherence analysis," *Energies*, vol. 15, no. 21, 2022, Art. no. 8174.

[4] G. Schneider and V. E. Troeger, "War and the world economy: Stock market reactions to international conflicts," *J. Conflict Resolution*, vol. 50, no. 5, pp. 623–645, 2006.

[5] I. Liadze, C. Macchiarelli, P. Mortimer-Lee, and P. S., "Economic costs of the Russia-Ukraine war," *World Economy*, vol. 46, no. 4, pp. 874–886, 2023.

[6] M. Khudaykulova et al., "Economic consequences and implications of the Ukraine-Russia war," *Int. J. Manage. Sci. Bus. Admin.*, vol. 8, no. 4, pp. 44–52, 2022.

[7] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv. (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, 2008, Art. no. 21260.

[9] R. Khalfaoui, G. Gozgor, and J. W. Goodell, "Impact of Russia-Ukraine war attention on cryptocurrency: Evidence from quantile dependence analysis," *Finance Res. Lett.*, vol. 52, Mar. 2023, Art. no. 103365.

[10] P. H. F. Oliveira, D. M. Rezende, H. S. Bernardino, S. M. Villela, and A. B. Vieira, "Analysis of account behaviors in Ethereum during an economic impact event," 2022, *arXiv:2206.11846*.

[11] S. Ferretti and G. D'Angelo, "On the Ethereum blockchain structure: A complex networks theory perspective," *Concurrency Comput., Pract. Experience*, vol. 32, no. 12, 2020, Art. no. e5493.

[12] W. Song et al., "Blockchain data analysis from the perspective of complex networks: Overview," *Tsinghua Sci. Technol.*, vol. 28, no. 1, pp. 176–206, 2022.

[13] D. Lin, J. Wu, Q. Yuan, and Z. Zheng, "Modeling and understanding Ethereum transaction records via a complex network approach," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 11, pp. 2737–2741, Nov. 2020.

[14] X. Li, Y. Xin, C. Zhao, Y. Yang, S. Luo, and Y. Chen, "Using user behavior to measure privacy on online social networks," *IEEE Access*, vol. 8, pp. 108387–108401, 2020.

[15] J. Idrais, Y. El Moudene, and A. Sabour, "Characterizing user behavior in online social networks: Analysis of the regular use of Facebook," *Int. J. Elect. Comput. Eng.*, vol. 11, no. 4, 2021, Art. no. 3329.

[16] J. A. Valadares et al., "Identifying user behavior profiles in Ethereum using machine learning techniques," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Piscataway, NJ, USA: IEEE Press, 2021, pp. 327–332.

[17] Q. Bai, C. Zhang, N. Liu, X. Chen, Y. Xu, and X. Wang, "Evolution of transaction pattern in Ethereum: A temporal graph perspective," *IEEE Trans. Comput. Social Syst.*, vol. 9, no. 3, pp. 851–866, Jun. 2022.

[18] V. Buterin, "A next-generation smart contract and decentralized application platform," *White Paper*, vol. 3, no. 37, pp. 2–1, 2014.

[19] J. Gomes, S. Khan, and D. Svetinovic, "Fortifying the blockchain: A systematic review and classification of post-quantum consensus solutions for enhanced security and resilience," *IEEE Access*, vol. 11, pp. 74088–74100, 2023.

[20] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," *Transp. Res. P E, Logistics Transp. Rev.*, vol. 142, 2020, Art. no. 102067.

[21] S. E. Chang and Y. Chen, "When blockchain meets supply chain: A systematic literature review on current development and potential applications," *IEEE Access*, vol. 8, pp. 62478–62494, 2020.

[22] Z.-H. Sun, Z. Chen, S. Cao, and X. Ming, "Potential requirements and opportunities of blockchain-based industrial IoT in supply chain: A survey," *IEEE Trans. Comput. Social Syst.*, vol. 9, no. 5, pp. 1469–1483, Oct. 2022.

[23] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtỳsson, "Blockchain-based e-voting system," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Piscataway, NJ, USA: IEEE Press, 2018, pp. 983–986.

[24] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—Review and open research challenges," *Sensors*, vol. 21, no. 17, 2021, Art. no. 5874.

[25] Z. Qin, J. Ye, J. Meng, B. Lu, and L. Wang, "Privacy-preserving blockchain-based federated learning for marine Internet of Things," *IEEE Trans. Comput. Social Syst.*, vol. 9, no. 1, pp. 159–173, Feb. 2022.

[26] G. Cheng, Y. Chen, S. Deng, H. Gao, and J. Yin, "A blockchain-based mutual authentication scheme for collaborative edge computing," *IEEE Trans. Comput. Social Syst.*, vol. 9, no. 1, pp. 146–158, Feb. 2022.

[27] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[28] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[29] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Trans. Ind. Inform.*, vol. 17, no. 1, pp. 3–19, Jan. 2021.

[30] D. Deshpande and S. Deshpande, "Analysis of online user behavior detection methodologies and its evaluation," *Int. J. Comput. Appl.*, vol. 975, 2017, Art. no. 8887.

[31] S. Deep, X. Zheng, C. Karmakar, D. Yu, L. G. C. Hamey, and J. Jin, "A survey on anomalous behavior detection for elderly care using dense-sensing networks," *IEEE Commun. Surv. Tut.*, vol. 22, no. 1, pp. 352–370, Firstquarter 2020.

[32] L. A. Amaral and J. M. Ottino, "Complex networks," *Eur. Phys. J. B*, vol. 38, no. 2, pp. 147–162, 2004.

[33] C. Pizzuti, "A multiobjective genetic algorithm to find communities in complex networks," *IEEE Trans. Evol. Comput.*, vol. 16, no. 3, pp. 418–430, Jun. 2011.

[34] E. Estrada, N. Hatano, and M. Benzi, "The physics of communicability in complex networks," *Phys. Rep.*, vol. 514, no. 3, pp. 89–119, 2012.

[35] Y.-C. Chen, P.-E. Lu, C.-S. Chang, and T.-H. Liu, “A time-dependent SIR model for COVID-19 with undetectable infected persons,” *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 3279–3294, Oct./Dec. 2020.

[36] W. Song, Z. Wang, Z. Li, H. Dong, and Q.-L. Han, “Protocol-based particle filtering for nonlinear complex networks: Handling non-Gaussian noises and measurement censoring,” *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 1, pp. 128–139, Jan./Feb. 2022.

[37] Y. Lou, R. Wu, J. Li, L. Wang, and G. Chen, “A convolutional neural network approach to predicting network connectedness robustness,” *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 3209–3219, Oct./Dec. 2021.

[38] M. Waniek, P. Holme, and T. Rahwan, “Hiding in temporal networks,” *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1645–1657, May/Jun. 2022.

[39] L. Zhang, H. Zhang, H. Yang, Z. Liu, and F. Cheng, “An interactive coevolutionary framework for multi-objective critical node detection on large-scale complex networks,” *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 3, pp. 1722–1735, May/Jun. 2023.

[40] M. Ndiaye and P. K. Konate, “Cryptocurrency crime: Behaviors of malicious smart contracts in blockchain,” in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, 2021, pp. 1–8.

[41] A. T. Aspembitova, L. Feng, and L. Y. Chew, “Behavioral structure of users in cryptocurrency market,” *PLoS One*, vol. 16, no. 1, 2021, Art. no. e0242600.

[42] R. Agarwal, S. Barve, and S. K. Shukla, “Detecting malicious accounts in permissionless blockchains using temporal graph properties,” *Appl. Netw. Sci.*, vol. 6, no. 1, pp. 1–30, 2021.

[43] J. Z. G. Mascarenhas, A. Ziviani, K. Wehmuth, and A. B. Vieira, “On the transaction dynamics of the Ethereum-based cryptocurrency,” *J. Complex Netw.*, vol. 8, no. 4, 2020, Art. no. cnaa042.

[44] S. Theiri, R. Nekhili, and J. Sultan, “Cryptocurrency liquidity during the Russia–Ukraine war: The case of bitcoin and Ethereum,” *J. Risk Finance*, vol. 24, no. 1, pp. 59–71, 2023.

[45] C. D. Mariana, I. A. Ekaputra, and Z. A. Husodo, “Are Bitcoin and Ethereum safe-havens for stocks during the COVID-19 pandemic?” *Finance Res. Lett.*, vol. 38, 2021, Art. no. 101798.

[46] I. Yousaf and S. Ali, “Discovering interlinkages between major cryptocurrencies using high-frequency data: New evidence from COVID-19 pandemic,” *Financial Innov.*, vol. 6, no. 1, 2020, Art. no. 45.

[47] E. Harb, C. Bassil, T. Kassamany, and R. Baz, “Volatility interdependence between cryptocurrencies, equity, and bond markets,” *Comput. Econ.*, vol. 63, no. 3, pp. 951–981, 2024.

[48] A. Wahrstätter, J. Gomes, S. Khan, and D. Svetinovic, “Improving cryptocurrency crime detection: Coinjoin community detection approach,” *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 6, pp. 4946–4956, Nov./Dec. 2023.

[49] A. Wahrstätter, “Python-bitcoin-scraper.” GitHHub. [Online]. Available: https://github.com/Nerolation/python-bitcoin-scraper

[50] R. Gould, *Graph Theory*, Mineola, NY, USA: Dover Publications, Inc., 2012.

[51] P. Holme and J. Saramäki, “Temporal networks,” *Phys. Rep.*, vol. 519, no. 3, pp. 97–125, 2012.

[52] C.-y. Lin, C.-L. Lin, and T.-W. Hou, “A graph-based approach for automatic service activation and deactivation on the OSGi platform,” *IEEE Trans. Consum. Electron.*, vol. 55, no. 3, pp. 1271–1279, Aug. 2009.

[53] B. M. Blau, T. G. Griffith, and R. J. Whitby, “Inflation and Bitcoin: A descriptive time-series analysis,” *Econ. Lett.*, vol. 203, 2021, Art. no. 109848.

[54] L. A. Smales, “Cryptocurrency as an alternative inflation hedge?” *Account. Finance*. 2022. [Online]. Available: https://doi.org/10.1111/acfi.13193.

[55] S. Choi and J. Shin, “Bitcoin: An inflation hedge but not a safe haven,” *Finance Res. Lett.*, vol. 46, 2022, Art. no. 102379.

[56] E. F. Fama, “Efficient capital markets: II,” *J. Finance*, vol. 46, no. 5, pp. 1575–1617, 1991.

[57] A. G. Å¢iÅ£an, “The efficient market hypothesis: Review of specialized literature and empirical research,” *Procedia Econ. Finance*, vol. 32, pp. 442–449, 2015.

[58] M. Rossi, “The efficient market hypothesis and calendar anomalies: A literature review,” *Int. J. Managerial Financial Accounting*, vol. 7, no. 3–4, pp. 285–296, 2015.

[59] D. Peón, M. Antelo, and A. Calvo, “A guide on empirical tests of the EMH,” *Rev. Accounting Finance*, vol. 18, no. 2, pp. 268–295, 2019.

[60] I. Alqassem, I. Rahwan, and D. Svetinovic, “The anti-social system properties: Bitcoin network data analysis,” *IEEE Trans. Syst., Man Cybern., Syst.*, vol. 50, no. 1, pp. 21–31, Jan. 2020.

[61] R. G. Elie Bouri and X. V. Vo, “Jumps in geopolitical risk and the cryptocurrency market: The singularity of bitcoin,” *Defence Peace Econ.*, vol. 33, no. 2, pp. 150–161, 2022.

[62] N. A. Kyriazis, “Optimal portfolios of national currencies, commodities and fuel, agricultural commodities and cryptocurrencies during the Russian-Ukrainian conflict,” *Int. J. Financial Stud.*, vol. 10, no. 3, 2022. [Online]. Available: https://www.mdpi.com/2227-7072/10/3/75

[63] C.-W. Su, Y. Xi, R. Tao, and M. Umar, “Can Bitcoin be a safe haven in fear sentiment?” *Technol. Econ. Develop. Econ.*, vol. 28, no. 2, pp. 268–289, 2022.

[64] A. F. Aysan, E. Demir, G. Gozgor, and C. K. M. Lau, “Effects of the geopolitical risks on bitcoin returns and volatility,” *Res. Int. Bus. Finance*, vol. 47, pp. 511–518, Jan. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0275531918306810

[65] Y. Song, B. Chen, and X.-Y. Wang, “Cryptocurrency technology revolution: Are bitcoin prices and terrorist attacks related?” *Financial Innov.*, vol. 9, no. 1, 2023, Art. no. 29.

Jorão Gomes Jr. (Member, IEEE) received the B.Sc. degree in both exact sciences and computer science, and the M.Sc. degree in computer science from the Federal University of Juiz de Fora (UFJF), Brazil, in 2018, 2019, and 2021, respectively.

He worked as a Data Scientist at EtherCity and an R&D Technical Manager at “RECMEM – Recommendation of Educational Media,” sponsored by the Brazilian National Research and Educational Network (RNP). He is currently a Teaching and Research Associate at the Vienna University of Economics and Business (WU) and a Ph.D. Candidate in Economic and Social Sciences at WU. His research interests include (but not limited to) data mining, information retrieval, and complex networks.

Heder Bernardino (Member, IEEE) received the D.Sc. degree in computational modeling from the National Laboratory for Scientific Computing *(LNCC)*, Petrópolis, Brazil, in 2012.

Currently, he is a Research Productivity Grant from the National Council for Scientific and Technological Development (CNPq). He is also the Chair of the IEEE-CIS Task Force on Nature-Inspired Constrained Optimization. He co-chaired a special session in Congress on Evolutionary Computation (CEC), in 2013, 2022, and 2023. He has experience in computer science, and his research interests are evolutionary computation, data science, and high-performance computing.

Mr. Bernardino has published over 110 papers in peer-reviewed journals and conferences, and 12 book chapters. He is a member of ACM and the Computational Intelligence Society (IEEE-CIS).

Alex Borges Vieira received the Ph.D. degree in computer science from Federal University of Minas Gerais (UFMG), Belo Horizonte, Brazil, in 2010.

From 2019 to 2021, he was a Visiting Professor with the Federal University of Juiz de Fora (UFJF), Juiz de Fora, Brazil. Currently, he is an Associate Professor with the Computer Science Department of Federal University of Juiz de Fora (UFJF), Juiz de Fora, Brazil. His research interests include network modeling and analysis and network science.

Dr. Vieira has productivity in research scholarship, awarded by the Brazilian National Council for Technological and Scientific Development (CNPq).

Verena Dorner received the Ph.D. degree from the University of Passau, Passau, Germany.

She is a Professor in digital ecosystems with the Vienna University of Economics and Business, Vienna, Austria. After completing the Ph.D. degree she headed the Research Group Electronic Markets and User Behavior and the Experimental Lab KD2Lab, Karlsruhe Institute of Technology, Karlsruhe, Germany. Her research focuses on the interdependencies between digital (eco-)systems and user behavior.

Prof. Dorner work has been published in journals such as the *European Journal of Operational Research, Journal of the Association for Information Systems*, *Electronic Markets*, and *Journal of Economic Psychology*.

Davor Svetinovic (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Waterloo, Waterloo, ON, Canada, in 2006.

He is a Professor with the Department of Computer Science, Khalifa University, Abu Dhabi, UAE, and the Department of Information Systems and Operations Management, Vienna University of Economics and Business, Vienna, Austria (on leave), where he is the Head of the Institute for Distributed Ledgers and Token Economy, and the Research Institute for Cryptoeconomics. Previously, he worked with TU Wien, Vienna, Austria, and Lero—the Irish Software Engineering Center, Limerick, Ireland. He was a Visiting Professor and a Research Affiliate with MIT and MIT Media Lab, MIT, MA, USA. He has extensive experience working on complex multidisciplinary research projects. His research interests include cybersecurity, blockchain technology, crypto-economics, trust, and software engineering.

Dr. Svetinovic has published over 100 papers in leading journals and conferences and is a highly cited researcher in blockchain technology. His career has furthered his interest and expertise in developing advanced research capabilities and institutions in emerging economies. He is a ACM (Lifetime), and an affiliate of the Mohammed Bin Rashid Academy of Scientists.