


Please cite the Published Version

Shahen Shah, AFM, Karabulut, Muhammet Ali, Akhter, AFM Suaib, Mustari, Nazifa, Pathan, Al-Sakib Khan, Rabie, Khaled M  and Shongwe, Thokozani (2023) On the vital aspects and characteristics of cryptocurrency - a survey. IEEE Access, 11. pp. 9451-9468. ISSN 2169-3536

DOI: <https://doi.org/10.1109/ACCESS.2023.3240103>

Publisher: IEEE

Version: Published Version

Downloaded from: <https://e-space.mmu.ac.uk/632921/>

Usage rights:  [Creative Commons: Attribution 4.0](https://creativecommons.org/licenses/by/4.0/)

Additional Information: This is an open access article which originally appeared in IEEE Access.

Enquiries:

If you have questions about this document, contact rsl@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

SURVEY

On the Vital Aspects and Characteristics of Cryptocurrency—A Survey

A. F. M. SHAHEN SHAH¹, (Senior Member, IEEE),
MUHAMMET ALI KARABULUT², (Member, IEEE),
A. F. M. SUAIB AKHTER³, (Member, IEEE),
NAZIFA MUSTARI¹, (Graduate Student Member, IEEE),
AL-SAKIB KHAN PATHAN⁴, (Senior Member, IEEE),
KHALED M. RABIE^{5,6}, (Senior Member, IEEE),
AND THOKOZANI SHONGWE⁶, (Senior Member, IEEE)

¹Department of Electronics and Communication Engineering, Yildiz Technical University, 34220 Istanbul, Turkey

²Department of Electrical and Electronics Engineering, Kafkas University, 36000 Kars, Turkey

³Department of Computer Engineering, Sakarya University of Applied Sciences, Serdivan, 54050 Sakarya, Turkey

⁴Department of Computer Science and Engineering, United International University, Dhaka 1212, Bangladesh

⁵Department of Engineering, Manchester Metropolitan University, M15 6BH Manchester, U.K.

⁶Department of Electrical and Electronics Engineering, University of Johannesburg, Johannesburg 1809, South Africa

Corresponding author: A. F. M. Shahen Shah (shah@yildiz.edu.tr)

ABSTRACT Cryptocurrencies acquire user confidence by making the whole creation and transaction history transparent to the public. In exchange, the transaction history accurately captures the complete range of user activities related to cryptocurrencies. It is thought to be one of the safest and simplest payment methods that may be employed in the future. The trend of banks and other financial institutions investing in cryptocurrencies has increased rapidly in recent years. Therefore, it is necessary to synthesize the findings of previous studies on cryptocurrencies. In this paper, the use of data mining methods in Bitcoin transactions is analyzed and summarized. Cryptocurrencies, similar to the well-known Bitcoin, were targeted to ensure transaction security and privacy and overcome the drawbacks of traditional banking systems as well as other centralized systems. In addition, a comprehensive analysis of the literature on the challenges and applications of electronic currencies is conducted. The evolution of digital currency from electronic cash to cryptocurrencies is summarized and the methods used to increase user privacy are highlighted. The security threats in existing cryptocurrency systems (that compromise the privacy of Bitcoin users) are also highlighted. Finally, several research gaps and trends are identified that need to be further explored.

INDEX TERMS Cryptocurrencies, electronic cash, privacy, security threats.

I. INTRODUCTION

Investments are made with the intention of reselling them for profit [1]. Today, a new electronic alternative trade payment mechanism called cryptocurrencies has been developed which gained wide acceptance, with substantial ramifications for emerging nations and the global market in general [2]. Due to the widespread use of cryptocurrencies, trading in cryptocurrencies is often thought of as one of the most

well-liked and fascinating forms of profitable investments. Virtual currency has several appealing qualities that appeal to an expanding range of customers of various types that use a specific technology for their own purposes [3].

Without a centralized banking institution, a cryptocurrency employs encryption to safeguard its transactions and confirm the movement of digital assets via the Internet. Since its first introduction in 2009, bitcoin has been the most widely used cryptocurrency. The market value of cryptocurrencies has now topped USD \$472 billion, with Bitcoin making up around USD \$185 billion of that amount.

The associate editor coordinating the review of this manuscript and approving it for publication was Luca Bedogni¹.

It is widely believed that Bitcoin was an anonymous cryptocurrency in its early years. On the other hand, coin history tracking is a familiar problem that involves the potential for examining the trail of a spent coin to link individuals to addresses. It is feasible owing to the fact that the Bitcoin blockchain is open to the public, meaning that anybody can see the transfer of currency from address A to address B. Knowing A and B by themselves is insufficient to identify the addresses of the owners since the addresses are just random strings produced using the public keys of the owners. However, it becomes conceivable to speculate about who could be the owner of the address if either of A and B is in a transaction's history or in future can be connected to a real person. Different methods, such as network analysis, monitoring, or just googling the address, may be used to find out someone's identify. Thus, there is a big market for cryptocurrency that is anonymous. A short history of Bitcoin and other cryptocurrencies is shown in Figure 1.

By merging cryptocurrency money with blockchain technology to conceal the path leading back to the asset's initial source, transaction anonymity has been made possible [4]. While sellers might get money sooner to maintain a stronger liquidity position due to upfront payment, the flexible payment deadline is advantageous to customers [5].

Everyone has the right to financial transactions that are private and untraceable, and this right extends to Bitcoin transactions as well. While some cryptocurrencies prioritize user privacy, others concentrate more on simple payment methods or quick transactions. A cryptocurrency that is meant to have strong cryptographic properties for its users' privacy is called an anonymous cryptocurrency. In general, the following information must be provided by the anonymous cryptocurrency.

- Privacy: It is made sure that potential enemies cannot see the sources, destinations, or values of any transactions.
- Untraceability: All coins transmitted or received are completely untraceable and cannot be linked to a specific transaction.
- Fungibility: All coins are guaranteed to be interchangeable with one another since they cannot be distinguished from one another in a random sample.

The distinction between this survey and other survey publications is further explained in Table 1. In this study, research on privacy delivery methods and privacy-related constraints on current electronic currencies is reviewed. A concise review of the privacy-related features of digital payment systems, now relevant to more modern crypto money systems, is presented. The key components of the Bitcoin ecosystem and the roles played by various players are outlined. Key trust concerns that have an impact on the acceptance and reliability of cryptocurrencies, directly or indirectly, are examined. To assess the relative trustworthiness of each, the top five cryptocurrencies and their supporting technical infrastructures are evaluated.

The remainder of the paper is organized as follows. The background of cryptocurrencies is covered in Section II. Section III presents cryptocurrency privacy, as well as anonymity. Contributions are presented in Section IV. Before concluding the paper in Section VI, promising research directions are discussed in Section V.

II. BACKGROUND OF CRYPTOCURRENCY

This section includes a brief history of digital currency on topics important to the evaluation. To emphasize various methods, including blind signatures, utilized to ensure the anonymity of the user, a range of electronic currency systems are described in particular. These methods are concentrated since they have lately been applied to cryptocurrencies and have gained relevance. Additionally, an introduction to cryptocurrencies is provided where Bitcoin gets a bit more preference, outlining the fundamental terms and system operations. Table 1 presents top-5 cryptocurrency platforms.

A. THE BIRTH OF A CRYPTOCURRENCY

In [2], Satoshi Nakamoto integrates tried-and-true concepts [15], [16], [17] into a fully functional currency that operates independently from banks or other institutions of authority. Every transaction that takes place on the network in Bitcoin is recorded in a ledger of blocks, creating a shared "truth" among network members. An assortment of transactions, a hash value to the block before it, and a random number called nonce that is utilized to verify transactions make up a block (Proof-of-Work). A Bitcoin transaction is the exchange of money between two addresses, or anonymous identifiers i.e., public keys. By possessing the corresponding private key, a member will be able to exchange an amount of Bitcoin. The IDs will have control over several outputs holding the cash since the output of Bitcoin is formed on the unspent transaction rather than a balance.

B. BLOCKCHAIN TECHNOLOGY

A blockchain, which is essentially a series of blocks, offers a decentralized method of bookkeeping. Any kind of record may be embedded inside a block, and blocks are connected by hash values. Depending on how the blockchain is set up, a proof field may be used to contain various pieces of evidence to support the accuracy of this block. Each participant in the system has a local copy of the blockchain on their own computer, and they use a predetermined consensus procedure to decide which block will be added next.

Applications of blockchain technology extend the peer-to-peer payment system. To enable Internet of Things (IoT) apps to work with the system's distributed storage, this provides the system with integrity, security, trust, preservation of privacy, attack prevention, etc. features based on a distributed ledger [18]. The benefit of this approach is that it is decentralized and completely secures the whole environment, allowing only appending of new blocks. Many blockchains and cryptocurrencies are led by the blockchain application

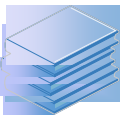







2008	2009	2010	2011	2014	2015	2018	2019
							
Bitcoin.org registered White paper published	First Bitcoin transaction	10,000 Bitcoin spent for pizza	25% of total Bitcoin generated	The combined value all of bitcoins in circulation reaches 1 billion USD	Ethereum and Tether released	Initial Coin Offering for the EOS blockchain raises a record 4.1 billion USD	Facebook launches new cryptocurrency called Libra China's Central Bank Prioritizes Development of Digital Currency

FIGURE 1. A brief history of Bitcoin and other cryptocurrencies.

TABLE 1. Comparison of this survey to other survey papers.

Reference	Privacy and Anonymity	Price Prediction	Benefits and Challenges	Applications of cryptocurrency	Privacy and Security	Ecosystem of Cryptocurrency	Blockchain Technology
[6]	√	X	X	X	√	X	X
[7]	√	X	√	X	√	X	X
[8]	√	X	√	X	X	X	√
[9]	X	X	X	X	√	√	√
[10]	X	X	X	√	√	X	√
[11]	X	√	X	X	√	X	√
[12]	X	X	√	X	√	X	√
[13]	√	X	X	X	√	X	√
[14]	X	X	√	X	√	X	√
This Survey	√	√	√	√	√	√	√

areas. Blockchain and cryptocurrency are related because they provide incentives to machines and consume power for blockchain validation. Cryptocurrency is a relatively new sort of digital money that makes use of the blockchain to boost decentralization, transparency, and immutability [19]. Cryptocurrency use is growing along with the use of blockchain technology. This includes the network’s intrinsic worth depending on numerous criteria. This procedure creates a new kind of money that stores values and improves comprehension of price fluctuations depending on their significance.

For a blockchain system to provide a secure and reliable platform for cryptocurrencies, it must offer a few fundamental qualities. These qualities consist of:

- Trustless— to stop centralized organizations from manipulating and controlling the money.
- Decentralization— to allow a decentralized system via peer-to-peer (P2P) networks to give users power, to eliminate the failure of centralized systems, to lower the likelihood of security attacks, to guarantee there are

no scams or frauds by enabling algorithmic techniques rather than creating user-oriented systems, and to confirm veracity and transparency via the design of open systems.

- Distributed ledger technology— the provision stores a copy of the database by each node, the avoidance of malicious record modifications, the fair participation of users, the implementation of consistent participation rule throughout the network.
- Tamper-resistant environment— in order to guarantee that, after-being committed, transactions can never be changed or eliminated.
- Security and privacy— to employ hash keys for anonymization and computationally challenging cryptography techniques.
- Faster transactions— to give algorithms authority over the system, rather than people.

By lowering transaction processing costs compared to centralized systems similar to banks, payment networks, and exchanges, blockchain technologies also benefit Bitcoin

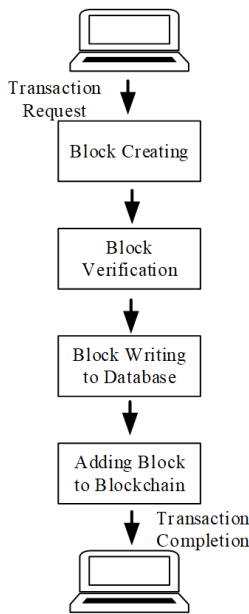


FIGURE 2. A simplified flowchart of cryptocurrency transactions.

consumers. Figure 2 presents a flowchart of cryptocurrency transaction.

Similar to any other newly developed technology, using Bitcoin has its advantages and disadvantages, as well as a number of potential hazards. Bitcoin is said to have both the following advantages and disadvantages.

C. BENEFITS

- **No Third-Party Seizure:** Since all money transfers take place peer-to-peer, much physical cash, no central authority can control or confiscate the currency. In particular, as the central authority does not print, possess, or control bitcoins in the same ways that it controls other cryptocurrencies, it cannot seize the Bitcoins.
- **Transparency and anonymity:** It is difficult to identify Bitcoin users' wallet addresses unless they make them publicly available. But, even if the wallet addresses are made public, it is simple to create a new wallet address. When opposed to conventional monetary systems, where attackers may gain control of the financial information of users, the Bitcoin system greatly enhances privacy. Furthermore, since all bitcoin transactions are stored in blocks similar to a public ledger, this pseudonymity is accomplished without compromising system transparency. Unfortunately, a lot of research works have demonstrated that flow analysis and clustering are more realistic methods for tracking Bitcoin transactions and identifying the owner involved [20], [21]. However, many efforts have been done to improve Bitcoin's privacy and anonymity issues, and several research community-proposed techniques have succeeded in enhancing anonymity [22], [23], [24], [25], [26], [27].

- **No taxes and lower transaction fees:** There are no taxes and cheaper transaction costs with Bitcoin because of its decentralized structure and pseudonymous-ness. In the past, Bitcoin offered quick transactions for almost little money. Even today, bank transfers, Paypal, and credit cards are more expensive than using Bitcoin for transactions. The cheaper transaction cost, however, is only advantageous when a user does significant overseas transactions. This is due to the fact that the modest value transfers and transactions, such as paying for common household items, result in higher average transaction fees in Bitcoin.
- **Stealing resilience:** Until the assailant obtains the private keys (often stored offline) linked to the user's wallet, it is impossible to steal Bitcoins. For example, similar to the credit card, it does not require revealing the secret PIN (Personal Identification Number) number every time one conducts a transaction in Bitcoin and this security is offered by design. Additionally, once committed, a transaction is impossible to change as Bitcoins are immune to charge-backs. As soon as the transferred Bitcoins are received, the ownership address is changed to the new owner, making a reverse transaction impossible. This makes sure that receiving Bitcoins is completely risk-free.

D. CHALLENGES

- **High energy usage:** The PoW technique is used by the Bitcoin blockchain to create distributed consensus to ensure the integrity of the chain. Despite the fact that it requires high computational power and time to perform PoW, it keeps the system protected from attacks similar to double spending, Sybil attack, etc. [28], [29]. By altering the nonce, miners combine a number of transactions to construct and mine a block. Although hashing does not need a lot of work, a miner must repeatedly do the operation until the result has the right number of zeros. The Bitcoin network's miners all work in parallel to complete this thousand times per day hashing and rehashing operations. As a result, it uses a lot of energy. The energy cost for Bitcoin transactions is higher than it is for traditional financial transactions for the reasons described above. For instance, each bitcoin transaction requires approximately 5,000 times more energy than a credit card (e.g., Visa Card) transaction. So, more enhancements are needed for this case [30]. To guarantee that Bitcoin has a sustainable future, breakthrough solutions that save energy are urgently needed. Furthermore, the time required to execute a Bitcoin transaction is growing as a result of the constant rise in network traffic and energy usage.
- **Wallets may be lost:** As the private keys are digitally stored in a wallet, problems similar to hardware or software damage may result in the loss of the key, and the number of coins in that wallet will become unusable.

The Bitcoins will remain orphaned in the system forever since there is nothing that can be done to reclaim them. A rich Bitcoin investor might go bankrupt in a matter of seconds.

- **Contribute to or enable criminal behavior:** Criminal conduct is made easier by the pseudonymity offered by Bitcoin, which is used to facilitate a variety of illegal operations including money laundering, tax evasion, and ransomware [31]. However, since the transactions of Bitcoin are pseudonymous as well as the transaction history is open publicly, law enforcement agencies may be able to apprehend criminals with a thorough study of blockchain data. As a result, criminals are beginning to employ alternative digital currencies similar to ZCash and Monero, which are designed to improve user anonymity.

Risk, as defined by [32], is the potential for loss due to Bitcoin technology, albeit this definition is generic enough to apply to any digital currency. The following are some of the most serious threats to the widespread adoption of Bitcoin payment systems.

- **Social risks:** Social risks include things similar to bubble development, the “cool” factor, chain building, and the introduction of additional currencies.
- **Legal risks:** Bitcoin’s decentralized ledger technology runs counter to centralized authority; thus, it faces resistance from regulators. The legal system’s response to Bitcoin-related financial, operational, consumer protection and security breaches is also a potential threat.
- **Economic risks:** Volatility, deflation, and delays in locating a block are all economic concerns that might drive consumers away from Bitcoin and toward other cryptocurrencies that provide their services more quickly.
- **Technological risks:** The Bitcoin network is subject to a number of technological dangers, such as the potential destruction of network hardware, changes in the parameters of the peer-to-peer network, the existence of malicious software that could compromise the system, the potential failure of hash functions, and the inherent security risks of the software used to run the network.

E. FUTURE OPPORTUNITIES

One of the biggest technical advances in recent years has been the development of cryptocurrencies, the newest class of digital assets. The cryptocurrency industry has been instrumental in advancing numerous important advancements, notably in 2021. In order to achieve spectacular development, cryptocurrencies have gone through three key stages: acceptance, innovation, and integration. But it is also critical to consider the potential of cryptocurrencies and what that means for all of us. After the enormous rise in 2021, experts warn that the next few years may be sluggish. In the last year, interest in cryptocurrencies has increased significantly, by a factor of two. It is interesting to note that cryptocurrency

is no longer only a subject for investors; many celebrities have begun to associate themselves with crypto assets. The discussion that follows explains the forecasts for the future of cryptocurrencies and their consequences for investors. To be ready for changes in the cryptocurrency ecosystem over the next five to ten years, it may be helpful to understand the potential future for cryptocurrencies.

Since the introduction of Bitcoin, many have been leery about cryptocurrencies. But circumstances have changed a lot, and interest in crypto-based solutions is constantly growing. The current condition of cryptocurrencies unquestionably provides the ideal bases for optimistic cryptocurrency future forecasts. However, given the volatility of different cryptocurrencies, predicting their future is challenging. Some improbable forecasts about long-term developments in the cryptocurrency world reflect a bullish outlook on the industry’s future. At the same time, it is necessary to keep an eye out for the crucial elements that might precisely determine the future use of cryptocurrencies.

III. PRIVACY AND ANONYMITY IN BITCOIN

By only allowing the parties engaged in the transaction and the reliable third-party access to the information, the conventional banking system attains a certain amount of privacy. On the other hand, in Bitcoin, every user linked to the network may see all the transaction information thanks to the public blockchain. However, by severing the information flow halfway along the Bitcoin transaction processing chain, privacy may still be protected to a certain extent. Bitcoin does this by maintaining the secrecy of its public keys, allowing anybody to transmit money to another person while keeping their identities hidden. It is suggested to employ a fresh key pair for every transaction to prevent users from being identified in order to further improve user privacy. However, multi-input transactions that inevitably show that all of their inputs were held by the same owner are still capable of being linked. Additionally, there is a chance that linking might expose other transactions associated with the identical user if the owner of a key is made public. By tracking the movement of money using a reliable blockchain analysis process, it is feasible to trace certain transactions to a specific user in particular since Bitcoin enables partial unlikability.

Although the privacy of the Bitcoin system is strong, pseudonymous addresses (or their hashes), which are vulnerable and readily broken by many methods, are the sole source of privacy in Bitcoin. This strategy entails, among other things, the reuse of Bitcoin addresses, tracking payments using blockchain analysis tools, “taint” analysis, IP address monitoring nodes, and web-spidering. Once compromised, restoring this privacy may be difficult and expensive.

The work in [4] draws attention to the fact that Bitcoin lacks a directory to store the log and other transaction-related data. On the other hand, a foe may link offline information similar to emails and shipping addresses to online data and get personal data about peers. A recent thorough assessment [6]

gives an overview and in-depth analysis of the preservation of privacy and anonymity in several cryptocurrencies.

A. RELATED WORK

Blockchain technology is being used in an increasing number of businesses and industries. The use of blockchain has been deemed to be of utmost importance for information systems' penetration into a variety of fields, including cybersecurity [33]. Despite being in the exploratory stage of implementation, in [34], authors emphasized the potential advantages for the logistics industry with the use of blockchain technology. Although there are several issues, many sectors including insurance have been preparing for blockchain applications and future technologies. The ongoing academic research works might further help in this regard [35].

B. BLOCKCHAIN TECHNOLOGY

In decentralized technologies and applications, such as storage, computation, security, interface, and transaction, blockchain, an emerging technology, plays a significant role. Blockchain technology has the ability to revolutionize corporate practices as well as spur their invention [36]. The sudden increase in the price of Bitcoin since it was originally launched and used in the financial market in 2008 has astounded the whole globe, with more and more focus being placed on the blockchain technology that underpins it. Blockchain has been already used in various fields and sectors as a distributed ledger technology [36], [37], [38], [39].

Because of the dearth of knowledge, academics have devoted their early careers to researching the technical details and potential applications of blockchain. The following nine qualities, in order, best capture the fundamental technological properties of blockchain technology: decentralization, disintermediation, anonymity, immutability, smart contract, cost reduction, traceability and provenance, transparency, security, and privacy [40], [41], [42], [43]. Specifically,

- **Decentralization:** Each node (participant) in the blockchain operates actively and equally and independently in a decentralized system.
- **Disintermediation:** Because there is no centralized supervisor or control, participants do not need to deal with trust difficulties. Every eligible block should have undergone verification and participant consent voting.
- **Immutability:** Algorithms for consensus and encryption are linked with blockchain. The data is hard to alter without the consent of most nodes.
- **Anonymity:** To avoid participant verification and credentialing, blockchain offers an encrypted coded record for every conceivable transaction.
- **Smart contract:** This programming language is used to carry out queries relating to blockchain data. Accuracy, security, and interoperability are all guaranteed by smart contracts.
- **Traceability and Provenance:** A blockchain database contains all confirmed data. Participants have simple

access to data including comprehensive transaction procedures.

- **Cost reduction:** Blockchain is open-source, free platform. Participants do not incur any fees beyond those related to mining operations.
- **Transparency:** A blockchain system provides equal access to all users. There are no secret assets since the block ledger is transparent.
- **Security and Privacy:** A blockchain system is a private and secure platform because it combines encryption, consensus methods, and smart contracts [40], [41], [42], [43].

C. NETWORKING INFRASTRUCTURE OF BITCOIN

Bitcoin's primary communication structure is an unstructured P2P network [44] built on persistent Transmission Control Protocol (TCP) connections that are not encrypted. The peers in an unstructured P2P network are arranged flatly or hierarchically in a random graph. To find peers with relevant data items, it uses flooding and other comparable opportunistic approaches similar to expanding-ring, random walks, Time-to-Live (TTL) search, etc. Unstructured overlays are often simple to set up and resistant to extremely dynamic network topologies, that is, peers entering and departing regularly. In order to obtain agreement on the blockchain, information must be distributed as quickly as possible, making these networks ideal for Bitcoin. However, using the Bitcoin network and protocol for testing presents a hurdle. There are now a few ways to go about doing this assignment. Connecting to the testnet or mainnet, often known as the active Bitcoin network, is one option. Utilizing simulation platforms similar to Shadow [45] event discrete simulator, which seeks to simulate massive Bitcoin networks while maintaining complete control of all components, is another option.

A DNS (Domain Name System) server bootstraps the list of IP addresses that Bitcoin nodes retain for possible peers, and new addresses are traded between peers. Each peer actively seeks new connections if the total number of associates is less than 8, with the goal of maintaining a minimum of 8 unencrypted TCP connections per peer in the overlay. Peers by default watch for incoming connections on port 8333. Peers carry out an application layer handshake, which consists of version and track messages when they establish a new connection. A timestamp for time synchronization, the protocol version, and IP addresses are all included in the messages. A node chooses its peers at random, then after a certain period of time, it selects a new group of peers. By doing this, the risk and consequences of a netsplit attack—in which an attacker gives the attacked node an inconsistent image of the network (and the blockchain)—are reduced. Bitcoin has supported IPv6 since version 0.7. Bitcoin employs a soft-state strategy to identify when peers have departed. Peers will send a greeting message to maintain the connection if it has been 30 minutes since the last communication was sent between them.

The hash of the mined block is provided in INV messages; which miners constantly monitor for fresh block announcements. A miner sends a GETDATA message to one of its neighbors if it learns that it does not possess a freshly announced block. The neighbor then reacts by sending a BLOCK message with the desired information. The miner disconnects that specific neighbor and requests the same information from another neighbor if the required block is not received within 20 minutes. Nodes publicly request and share transactions that have not yet been added to the blockchain in a series known as GETDATA, INV, and TX messages, which is how transactions are propagated. Newly found transactions and blocks are spread across the whole network (via flooding) to create a distributed consensus. New transactions are stored by miners for mining reasons, but if they are rejected by the blockchain they are eventually removed. The originator of the transaction is accountable for ensuring that all network peers receive the transaction. For this reason, if the transaction was unsuccessful in entering the blockchain the first time, the originator may need to broadcast it again. It is done to guarantee that the transaction is taken into account in the next block.

Bitcoin needs the rapid distribution of freshly created transactions and mined blocks in order to preserve the consistent global picture of the blockchain at the network nodes and prevent blockchain forking. The Bitcoin networking infrastructure is, however, exposed to a variety of routing assaults because of this necessity. An attacker on the forwarding path, for instance, may reject, eavesdrop on, edit, or inject Bitcoin messages since Bitcoin connections are delivered in plain text and without any integrity checks. In order to launch the double spend and netsplit attacks, an attacker might also cause a delay in the propagation of both new transactions and mined blocks. The propagation period may potentially be prolonged under certain conditions, as illustrated in [46]. The work in [47] outlines a classification of routing attacks and how they affect Bitcoin, taking into account both small-scale attacks that target specific nodes and large-scale assaults that target the whole network. Adversaries may squander a large amount of mining power by isolating some portions of the network or stalling block propagation, which might result in revenue losses and open the network up to a variety of attacks. Due to the following two factors, identifying and thwarting these network attacks is a difficult task.

In order to ensure that information is distributed quickly across the network, Bitcoin utilizes an unstructured P2P network. The consistency of the blockchain's overall state, which depends on the efficiency of its consensus algorithm, is crucial to Bitcoin's security. The consensus protocol may suffer as a result of the transmission techniques' differences. If properly exploited, the existence of inconsistent blockchain states might result in double spending problem. In order to do this, it is crucial for the Bitcoin network to continue to be scalable, with bandwidth, and storage needs since doing so will make it easier for the network to grow and attract more trustworthy miners, which will improve the consensus

mechanism. Since it is the method that ensures security, all the nodes in Bitcoin download and validates every block beginning with the genesis block. Although not required, full nodes participate in the P2P network and aid in information propagation. As an alternative, the thin clients carry out transactions using the simplified payment verification (SPV). Without downloading the complete blockchain, the Bitcoin thin client uses the SPV to check if certain transactions are incorporated in a block. More exactly, rather than storing the full chain just download the block headers during synchronization and request the full block only if required. Nevertheless, using SPV results in costs for thin clients since it gives them vulnerabilities similar to Denial of Service and privacy leaks. In particular, the system still has limitations brought on by the Bitcoin protocol itself as well as the basic scalability concerns of unstructured overlays. Numerous findings point to the fact that scalability is still a challenge [52] and maintaining a completely decentralized network in the future is challenging [53], [54].

D. REGULATION IN CRYPTOCURRENCIES

Absolute anonymity is undesirable in certain applications and might impede the growth of cryptocurrencies owing to potential legal infringement. Anonymity offers a pretext for carrying out covert operations for a variety of illicit activities, including money laundering, drug trafficking, tax evasion, etc. Many cybercriminals use anonymous cryptocurrency as a means of money collection. A classic underground black market selling narcotics, firearms, and other illegal goods are the famed Silk Road. Because Bitcoin is used to conduct and transmit payments on Silk Road, there is no clear line between what steps the government and law enforcement may do to regulate the transactions.

Cryptocurrencies utilize a variety of strategies to preserve privacy, including commitment and zero-knowledge proof, which provide zero knowledge and concealment properties, respectively and are computationally infeasible for an outsider to crack. As a result, tracing the transactions is a theoretically unsolvable challenge, necessitating the development of additional approaches. In the next part, we evaluate the tracing techniques currently in use and note the few works that rely on cryptographic tools.

E. ECOSYSTEM OF CRYPTOCURRENCY

The essential elements of the cryptocurrency ecosystem must be first comprehended, which include coins, wallets, mining systems, exchanges, payment systems, blockchain, and important players, in order to measure confidence in the ecosystem of blockchain-based cryptocurrencies.

Cryptocurrencies must provide the exchangeability, quantifiable quantity, and value of money in addition to security measures. Additionally, cryptocurrencies are advantageous because they enable extraneous features similar to pseudonymization, which conceals the actual identities of the parties involved in a transaction, decentralization, which

TABLE 2. Top 5 Cryptocurrency platforms.

Cryptocurrency	Launch Year	Network	Maximum Supply	Hashing Algorithm	Measurement Unit	Difficulty Adjustment
Bitcoin [2]	2009	N/A	21 million	SHA256	Satoshi	2016 Blocks
Ethereum [48]	2015	Ethereum	unlimited	Sthash	Wei	1 Block
Litecoin [49]	2011	N/A	84 million	Sycript	Photon	2016 Blocks
Ripple [50]	2012	RippleNet	100 billion	N/A	Drop	1 Block
Tether [51]	2014	N/A	N/A	N/A	Tether	N/A

allows for multiparty transaction verification, rapid transmission of funds via overcoming institutional and geographical barriers, lower transaction fees compared to conventional payment methods, and trustlessness. Other desirable characteristics include the ability to be converted into fiat currency and other cryptocurrencies, rapid transaction settlement (which enables quick value exchange between parties transacting), irreversibility (which ensures that once a transaction is completed it cannot be undone), and controlled supply (which helps to maintain the proper equilibrium and good intrinsic value). However, cryptocurrencies are not strong enough to rule the currency markets, despite having these cutting-edge qualities.

To secure reliable transactions between Bitcoin stakeholders, a lot of work is required. More than 2100 cryptocurrencies are now in use (at the time of writing this article). Some of them have, however, become well-appreciated. Table 2 lists the five most popular cryptocurrencies with over 75% of the market capital as well as their essential characteristics [55]. Table 3 summarized a comparison of the top 5 cryptocurrency platforms.

Cryptocurrencies employ lengthy random character sequences called as secret passwords and public usernames to maintain user identities. Applications known as wallets are used to generate, store, organize keys, and carry out transactions. While each cryptocurrency has a native wallet with some basic functionality, the open-source community and business organizations are constantly developing more advanced wallets with increased security. For instance, some wallets facilitate an additional degree of security by enabling users to generate mnemonics—clear, short phrases—instead of lengthy private keys [56]. In order to increase security, hierarchical deterministic wallets also provide users the option to create and link numerous private keys to a single phrase. Integrated currency conversion, connected credit and debit cards, zero-fee off-chain and on-chain transactions, key recovery services, insurance, and assistance through email and SMS are a few further noteworthy features. Due to these added functionalities, there is a thin line separating cryptocurrency exchanges from wallets, with the majority of wallets offering functions that were previously essential to exchanges.

Borderless cross-platform and inter-platform transactions are made possible through exchanges. Exchanges may be

divided into three categories: order-bookings exchanges, trading platforms, and brokerage services. Exchanges for brokerage services are quite well-liked, and they allow businesses to acquire and sell cryptocurrencies. Different cryptocurrency trading engines may be used with the services offered by order-bookings exchanges. In order to integrate different cryptocurrencies, national fiat currencies, as well as digital goods and services, the trading platforms provide interoperable services. An exchange may function in one mode or many modes, depending on its size. According to a market study, major exchanges provide services in two modes, but tiny exchanges often operate in only one [57]. However, just 4% of small exchanges and 22% of major exchanges provide services across all three modalities. The exchanges' support for cryptocurrencies differs as well. Bitcoin is supported by every exchange assessed, whereas 43% and 35% of exchanges, respectively, support Ethereum and Litecoin. In a similar vein, the majority of exchanges (65%) allow trading in USD, followed by EUR (49%) and GBP (39%).

Payment service providers act as intermediary networks that connect cryptocurrencies with the mainstream economy. Payment rail and cryptocurrency payments are two main categories of payment networks. Utilizing cryptocurrency exchanges in the midst of the networks, the payment rail facilitates trading between the fiat currencies and the digital currencies at end-points. Payment rails are often used to carry out quick cross-border transactions, but since cryptocurrencies have been pseudonymized, governments have found it difficult to efficiently monitor and control these networks. The payment rails provide both business-to-business and inter-individual money transfer services. Alternately, cryptocurrency payment networks make sure that at least one end-point uses cryptocurrencies. These networks are used to handle payments for businesses that accept cryptocurrency via merchant services. These networks might also be used as standard cryptocurrency platforms.

The key participants in cryptocurrencies are i) Users, or those who transmit or receive coins via programs, systems, or people. ii) Service providers, independent programmers, or businesses that provide cryptocurrency creation and trading platforms. iii) Those who establish policies, operational frameworks, regulations, and procedures for the moral and legal usage of cryptocurrency systems, including regulators,

TABLE 3. Comparison of top 5 cryptocurrency platforms.

Trust Issues	Bitcoin	Ethereum	Litecoin	Ripple	Tether
Transaction amount impact	High	High	Medium	Low	N/A
Price manipulation activities	High	High	High	Medium	High
Time of transaction response	Slow	Medium	Slow	Fast	N/A
Privacy attack	Yes	Yes	Yes	Yes	Yes
Security attack	Yes	Yes	Yes	Yes	Yes
Reputation attacks frequency	High	High	High	Low	High
Reputation in black market	High	Low	Low	Low	Low
Reported bump and dump activities	Yes	Yes	Yes	Yes	Yes
Volatility	High	High	High	Low	Low
Dishonest stakeholders potential	High	Low	High	Low	High

executives, businesses, representatives, and consortiums. iv) Validators—individuals or businesses who mine cryptocurrency and verify transactions.

F. PRIVACY AND SECURITY

A significant portion of blockchain technology research in recent years has focused on cryptocurrencies, including work on privacy and security issues [58], [59]. Major dangers to the Bitcoin system have been outlined in several studies, including double-spending assaults, attacks on mining pools, attacks in the network system, security in the client-side concerns affecting wallets, and that will harm privacy. They have also proposed approaches to address these problems and ideas to strengthen the security of the Bitcoin system [60], [61], [62]. The underlining technology of cryptocurrency is blockchain and the security and privacy aspects of blockchain have also been extensively researched [63], [64].

According to the authors of [65], who highlighted the privacy and security needs of blockchain, there are a number of areas that still need to be improved, including transaction unlikability, secrecy, and resistance to the 51% assault. In related research work, consensus protocols are examined and developed as a crucial part of preserving blockchain security and thwarting assaults [66], [67]. Additionally, it entails the creation of privacy-preserving technologies to resolve current privacy issues and improve blockchain's secrecy, anonymity, and user privacy control [68]. Although the privacy and several security aspects of cryptocurrencies have been thoroughly studied from a technical standpoint, end-user viewpoints and attitudes about these elements are little understood. Usability and user views of Bitcoin security are related, according to the work in [69]. However, Bitcoin users use a variety of privacy and security measures based on how risky they believe their intended use to be [70]. According to a poll of Bitcoin users, there are numerous misconceptions about how the network protects privacy and anonymity, and many users are not making full use of the security features of

Bitcoin management tools [71]. These insights emphasize the importance of understanding how users' views of the privacy and security of cryptocurrencies may affect their intentions to utilize the technology for certain use cases.

G. MOTIVATION

Numerous research works look at the fundamental reasons why individuals are drawn to interact with cryptocurrencies. Although there is no defined classification, several investigations have reported on related topics. The impending financial revolution, the empowerment that comes with using a decentralized cryptocurrency, perceived material worth, and an economic justification are all mentioned as having similar motivations.

IV. CHALLENGES AND APPLICATIONS

A. PUMP AND DUMP OF CRYPTOCURRENCY ACTIVITIES

A security mechanism's price is artificially inflated in a "pump and dump" operation. Beginning in the early days of the stock market, these fraudulent tactics have now extended to the cryptocurrency industry. The Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) have issued many warnings [87] about Bitcoin pump and dump schemes, indicating the seriousness of the problem.

Although marketing teams used pump and dump techniques in Initial Coin Offerings [88] in the beginning of cryptocurrencies, they now come in a variety of shapes and sizes. A gang of con artists, a secret or semi-secret communication channel where con artists may coordinate their illegal operations, and social media for orchestrating coordinated efforts to hype a particular currency are the three main components of a pump-and-dump scheme. In a typical situation, con artists set up groups on websites similar to Telegram or Reddit to organize mass purchases of a certain cryptocurrency while promoting it on Twitter. Normal traders may purchase the currency in the aim of foreseeing the next trend, which

would raise the price even more. These traders are oblivious of harmful activities and simply watch the price climb. When a certain price objective is achieved, the con artists start to sell (or “dump”) their shares, which causes the price to fall sharply.

B. CRYPTOCURRENCY PRICES PREDICTION

The forecasting of Bitcoin values may also be done using transaction characteristics. Here are some examples of accuracy indicators: 1) mean squared error, 2) root mean square error, 3) mean absolute percentage error. Predicting the possible price of coins across various works could not be comparable since these measurements are susceptible to bitcoin price scaling.

Deep Learning (DL) is a potent Machine Learning (ML) technique that uses a lot of data and precise predictions to solve complicated, nonlinear problems. Due to the wide range of values, it is difficult to estimate prices with accuracy; however, the deep learning technique solves this problem. [86] compared deep neural networks to Long Short Term Memory (LSTM) and merged their results with Bitcoin price prediction. The results of their methodology are shown, and they show that LSTM has a respectable level of accuracy when compared to other regression models. Regression analysis is an inadequate tool for analyzing deep learning models in the context of bitcoin trading, but this is what they tried to do. A methodology for trend categorization and prediction using deep learning is presented in [4], [76], [89], and [90] for non-stationary Bitcoin time series data. The outcomes of the created technique demonstrate how well the LSTM model performed based on a buy-and-hold strategy profitability study. The output findings of this system demonstrate that the LSTM generalized flawlessly in the bitcoin price prediction. The acronyms for this system are mentioned below. To assess prediction, the Diebold-Matiano test and Hansen’s Model confidence set are utilized. The comparison of a few comparable papers on cryptocurrency price prediction is provided in Table 4.

Various methods are studied for identifying users by analyzing the transaction graph of cryptocurrencies. A transaction graph is one in which the vertices represent transactions and the edges represent fund flows. Table 5 presents an overview of transaction graph analysis methods.

C. PRIVACY AND ANONYMITY

The idea of protecting user data privacy is not new. For instance, the majority of online social networks have centralized architectures with members who are continually exchanging data. Because the central organization has access to all user data and may provide extra access to third-party businesses, privacy issues are raised over user data. Social graphs, which depict the relationships, actions, and preferences among members of online social networks, include sensitive data that may be used to identify individuals’ true identities [95]. Decentralized social networks were presented

as a solution to these privacy issues. [95] assessed the privacy levels of several decentralized alternatives to online social networks. Although the study found that end-to-end encryption may provide secrecy, a recurring issue in decentralized social networks was concealing the social graphs that included private user information from storage providers using dispersed techniques. [96] presented a study regarding the protection of privacy in online social networks. The decentralized social networks Pisces and Lockr were explored, although Pisces was designed primarily for scaling and does not handle the problem of link privacy, which links one user to another in a social graph. Concerns about Bitcoin transaction privacy and anonymity are directly tied to link privacy and social networks. The constraints of privacy in digital currencies have been studied in many ways since the appearance of cryptocurrencies. The popularity of Bitcoin has led to many studies on de-anonymizing Bitcoin users [95], [96].

D. TECHNOLOGICAL CHALLENGES

To create practical and effective blockchain-based applications, several industrial difficulties that have not yet been solved must be addressed and further investigated. The primary open issues are covered in the sections that follow. Table 6 presents a summary of technological challenges.

- **Benefits of a thorough analysis of the blockchain-based solution include:** Blockchain is a novel technology that, when used to replace old solutions [97], has the ability to upset the market by offering innovative ideas that might change society [98]. Therefore, it is crucial to determine if a blockchain is really necessary for a particular application [99].
- **Appropriate implementation:** Blockchain may be employed in a number of systems for a variety of purposes if it is developed properly and maturely. Blockchain technology includes many alternative structures and transactional methods, therefore putting it into practice is not an easy task. Therefore, an extensive and in-depth investigation is needed before it can be used in various applications [100].
- **Standard testing mechanism:** The need for a common testing method is yet another difficulty encountered while implementing a blockchain-based application.
- **Resilience to security risks:** It is necessary to explicitly establish resilience to security hazards. The blockchain may experience difficulties with large-scale applications as a result of the system architecture or hacks that aim to jeopardize its security.
- **Scalability:** The main cause of this problem is how slowly blockchain-based transactions are processed and confirmed. Processing transactions depends on how well the processing system performs. The limits of the suggested scaling approaches are mentioned in [100].

TABLE 4. Comparative analysis of related works on predicting cryptocurrency prices.

References	Method	Cryptocurrency	Technique
[72]	Utilizing the bitcoin transaction network to influence price predictions	Bitcoin	Single Layer NN
[73]	Predicting the price of bitcoin using ARIMA	Bitcoin	ARIMA
[74]	Utilizing Detrended Fluctuation Analysis and the Largest Lyapunov Exponent	Ripple	LSTM
[75]	For the ensemble regression tree, XGBoost and LSTM	Bitcoin	LSTM, RNN
[76]	Engineering features utilizing four classes	Bitcoin	LSTM, SVM
[77]	The telegram and trends data prediction	Ethereum	LSTM
[78]	To forecast bitcoin prices, use Google Trends and tweet sentiment. Improve your forecast by using Facebook and Wikipedia	Bitcoin	RNN, LSTM
[79]	Blockchain non-linear data capturing using a Bayesian NN	Bitcoin	MLP
[80]	Based on a genetic algorithm, the next day dependency price	Bitcoin	MLP
[81]	Using correlation analysis to study the bitcoin industry	Ethereum	Regression
[82-83]	Using linear correlation to predict the price of bitcoin	Bitcoin	Linear correlation
[79-80]	Predict the daily price of bitcoin and litecoin	Bitcoin	RF
[71, 81]	Price and direction of next 30 days	Bitcoin	LSTM

TABLE 5. An overview of transaction graph analysis methods.

References	Objective	Method	Requirements
[25]	Clustering addresses	Source and destination link with heuristic	Transaction graphs
[91]	Recognized user type	Pattern recognition	Known addresses
[92]	Link cluster to user	Scrape addresses	Known addresses
[93]	End-to-end throughput	Smart contract	Known addresses
[94]	Throughput and latency of blockchains	Hydra approaches	Known addresses

- **Integration with other systems:** This problem has a clear effect on businesses wanting to use blockchain-based technology. There will be expenses associated with changing the infrastructure, hiring skilled workers, hiring specialist developers, and managing management expectations [101].
- **Energy challenges:** There is no question that using blockchain would demand a lot more energy than normal. The requirement of too much energy can become an environmental concern [102].
- **Regulatory issues:** For blockchain-enabled products to be widely used and accepted, laws are crucial.

TABLE 6. A summary of technological challenges.

References	Technological Challenges
[97-99]	Benefits of a thorough analysis of the blockchain-based solution include
[100]	Proper implementation
[100]	Scalability
[101]	Integration with other systems
[102]	Energy challenges
[103]	Storage

TABLE 7. A summary of application of cryptocurrency.

References	Applications
[104]	Internet of Everything
[96]	Data Storage and Analytics
[105]	Artificial Intelligence
[106]	Vehicle-to-Vehicle Communications
[107-108]	Unmanned Aerial Vehicles

- **Storage:** The issue of data storage is brought up by the incorporation of blockchain with different data-intensive systems, including those built on the IoT. In fact, the blockchain stores information in small, data-constrained chunks. As suggested in [103], one option is storing blocks in the cloud to take use of the cloud’s expandable feature.

TABLE 8. A summary overview of the privacy-limitations from transaction.

Reference	Objective	Method	Limitations
[122-126]	Increase taint resistance	Centralized Mixing	Require trust in a server
[127-132]	Improve taint resistance	Decentralized Mixing	Limited anonymity set
[133-136]	Increase taint resistance	Non-interactive mixing	Limited anonymity set
[137]	Improve taint resistance	Coin Swapping	Require trust in a sender
[2], [138-141]	Increase taint resistance	Ring signatures	Limited anonymity set
[142]	Hide receiver	Stealth addresses	Participant must verify
[143]	Hide amounts	Confidential transaction	Requires proofs for verification
[144]	Unlikability	Zero knowledge proof	Comparatively computationally costly to verify
[145-150]	Hide IP	Mixnets	Vulnerable to DoS

E. APPLICATIONS OF CRYPTOCURRENCIES

In this section, the most significant blockchain technology research possibilities are covered. Table 7 presents a summary of application of cryptocurrency.

1) INTERNET OF EVERYTHING (IoE)

Compared to IoT, the IoE is broader in scope and aims to link people, processes, data, and objects intelligently. The unique function of IoE was explored in [104]. Business concepts and procedures are predicted to be reinvented by- the IoE. The first benefit of digital technology is the automation and optimization of procedures. Second, the use of digital technology makes it feasible for new business models in several sectors. From a commercial perspective, it will be fascinating to look into the effects of the various options when adopting IoE. It is required to compete with previously unheard-of business agility and velocity. Further study is needed to determine the effects of integrating blockchain-based technology for interoperability across various organizations.

2) ARTIFICIAL INTELLIGENCE (AI)

The ultimate objective of next-generation network communications is to make our civilization more advanced, super-efficient, and environment-friendly. A far deeper integration of AI is anticipated on all levels. It has been shown that using AI and machine learning approaches would enhance physical layer security, channel coding, and obstacle and range detection [105], [106]. It is clear that all these fields of study would require further research.

3) DATA STORAGE AND ANALYTICS

In today's world, Thousands of devices are using the IoE to continually produce real-time streams of fresh data. First

and foremost, this requires effective data storage solutions. It is obvious that blockchain-enabled technologies have a lot of potential in that area. How to spread and mix these technologies in other fields is not yet evident; however, there are already various concepts in the field similar to fog, edge, and cloud computing-based solutions.

4) VEHICLE-TO-VEHICLE COMMUNICATIONS

One of the key applications that will succeed in the next ten years is Intelligent Transport Systems (ITS), which will call on the available technology capabilities, see e.g., [107], [108], [109], [110], [111], [112] and the references therein. Through simulation, a blockchain-based solution to defining the trust management of automobiles has been shown and assessed in [113]. The method's primary flaw was its restriction to ad hoc networks; therefore, further research is required to ensure efficiency in mobility and other required situations.

5) UNMANNED AERIAL VEHICLES (UAV)

Due to the need for high-data-rate requiring wireless communication, UAVs or drones will also play a crucial role in achieving this and are expected to be part of the future 6G mobile networks, see e.g., [114], [115], [116], [117], [119], [120] and the references therein. Here, blockchain has a significant opportunity to secure drone security and privacy and the information they gather [121]. In order to solve drone fleet security, IBM even submitted a blockchain patent [122]. Drones may be used in a variety of blockchain-based applications. First off, identity management may be arranged with the aid of blockchain technology. The management of air traffic may thus be set

TABLE 9. Reliability issues: Requirements and solutions.

Reliability Issues	Requirements	Solutions
Manipulation of exchange	Exchanges should function independently	Blockchain system based on proof of stake, Decentralized exchanges based on smart contracts
Transaction of high value	Prices should not rise due to the large number of transactions	The number of coins should be adjusted to maintain the proper balance of demand and supply
Market factors	All coin prices must move independently	Cryptocurrency platforms should simplify the technology and highlight its strengths
Dishonest stakeholders	There must be no dishonest stakeholders	All cryptocurrency wallets and exchanges should have a reporter tool enabled
Manipulated reputations	Reputations should not be manipulated by stakeholders	To ensure reputable stakeholders and networks, incentive mechanisms are required
Attacks of reputation	There must be no attacks on the reputation	Identify and punish the attackers
Activities of pump and dump	There must be no activities of reputation	Finding and monitoring activities of pump and dump
Attacks of privacy and security	There are no attacks on privacy and security	Users should be aware of all types of privacy attacks, To deal with privacy attacks, algorithmic approaches are required

up in a safe, precise, and effective manner. Finally, insurance firms may resolve disputes by using reliable records.

V. DISCUSSION AND FUTURE RESEARCH DIRECTIONS

Table 8 lists some systems that have been suggested to enhance cryptocurrency privacy. These ideas range from brand-new cryptographic techniques that use shielded addresses and zero-knowledge proofs to network broadcast techniques designed to conceal of the source address. But as can be seen in Table 8, extensive studies have been done in the field of cryptographic protocols. Even though it has been argued in earlier works that Dining Cryptographers network or Mixnets can impose unspecified broadcast between peers [125], [127], [133], in many cases, the anonymous broadcast will still let us construct the transaction graph and subsequently carry out a number of potent attacks on the users' anonymity. The collection of Zero-Knowledge transfer protocols, which lack a transaction graph, may reveal the true value of anonymous broadcast. Our study of the current obstacles to boosting blockchain trust in the bitcoin ecosystem is shown in Table 9.

Further investigation in this area is needed, and it should be customized to the sort of information that can be retrieved from the different systems since the propagation of transactions threatens both decoy-based as well as zero-knowledge-proof systems. In particular, network privacy for zero-knowledge systems may be improved via the creation of non-interactive anonymous broadcasting. Decoy-based systems, however, are exempt from anonymous broadcasting since an observer might still build the transaction graph in such systems. The field of non-interactive transaction accumulation across the propagation mechanism has to be investigated if these systems are to be effectively safeguarded. While

there are some encouraging recommendations in this area, there is yet no evidence of a significant improvement.

VI. CONCLUSION

In this paper, the vital aspects and characteristics of cryptocurrencies are examined; especially, a systematic literature review on privacy in the context of cryptocurrencies is conducted. It was observed that none of the solutions implemented in the area under study provided solid anonymity assurance to ordinary users. Additionally, the current approaches permit passive or active assaults that significantly affect the privacy of the system. A few techniques are also utilized to reduce network analysis, leaving many systems open to assault from a network observer. The actions and behaviors of users have been reliably recorded on the blockchain. Since discovering the depth of the blockchain based database, academia has generated a sizable corpus of study on Bitcoin transactions.

Bitcoin has already established itself as a well-appreciated digital cryptocurrency in the market. However, Bitcoin's notoriety has drawn haters who utilize the network for their own gain and convenience. Currently, there are almost 2000 distinct cryptocurrencies in use, many of which have just entered the market. The exceptional popularity and large market capital of Bitcoin among all these fiat currencies attract adversaries to launch numerous security risks. Our poll indicates that although the proof-of-work and consensus algorithms used in the development of the Bitcoin system (to safeguard user activities) are strong characteristics, they are also turning into a point of persuasion for online criminals.

Attacks against Bitcoin range from double spending to a wide variety, and they are all feared. Although some of these threats have remedies in the literature (at least the proposals

are available), there are currently no reliable and practical security measures that can guarantee Bitcoin's future functionality. The distributed nature of the Bitcoin blockchain has also caused issues with the users' demands for privacy and anonymity, in addition to security. In conclusion, this article is a lone effort to highlight the security and privacy concerns in several aspects of Bitcoin.

This study mainly focuses on the security and privacy features that are present across the Bitcoin system at different levels, from the time a transaction is created until it is successfully added to the blockchain, after briefly presenting the main elements of Bitcoin, its fundamental properties, and related ideas. Issues related to user privacy in this rapidly expanding e-commerce industry are examined and highlighted. It is hoped that this study will spur nascent researchers to take on the security and privacy problems with the Bitcoin system and other cryptocurrencies to provide a list of future study topics and open questions – possibly, to suggest effective solutions.

REFERENCES

- [1] Y. Wei and A. Dukes, "Cryptocurrency adoption with speculative price bubbles," *Marketing Sci.*, vol. 40, no. 2, pp. 241–260, Mar. 2021.
- [2] S. Nakamoto. (2009). *Bitcoin: A Peer-To-Peer Electronic Cash System*. Accessed: Nov. 21, 2022. <https://bitcoin.org/bitcoin.pdf>
- [3] B. Mobasher, "Data mining for web personalization," in *The Adaptive Web* (Lecture Notes in Computer Science), vol. 4321, P. Brusilovsky, A. Kobsa, and W. Nejdl, Eds. Berlin, Germany: Springer, 2007, pp. 90–135.
- [4] P. Koshy, D. Koshy, and P. D. McDaniel, "An analysis of anonymity in Bitcoin using P2P network traffic," in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur. (FC)*. Heidelberg, Germany: Springer, Mar. 2014, pp. 469–485.
- [5] E. Duffield and D. Diaz. *Dash: A Privacy-Centric Cryptocurrency*. Accessed: Nov. 21, 2022. [Online]. Available: <https://github.com/dashpay/dash/wiki/Whitepaper>
- [6] M. C. K. Khalilov and A. Levi, "A survey on anonymity and privacy in Bitcoin-like digital cash systems," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2543–2585, 3rd Quart., 2018.
- [7] D. Yang, J. Gavigan, and Z. Wilcox-O'Hearn, "Survey of confidentiality and privacy preserving technologies for blockchains," R3 Zcash Company. Accessed: Dec. 13, 2022. [Online]. Available: https://z.cash/static/R3_Confidentiality_and_Privacy_Report.pdf-92
- [8] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.
- [9] M. H. U. Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Trust in blockchain cryptocurrency ecosystem," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1196–1212, Nov. 2020.
- [10] S. Ghimire and H. Selvaraj, "A survey on Bitcoin cryptocurrency and its mining," in *Proc. 26th Int. Conf. Syst. Eng. (ICSEng)*, Dec. 2018, pp. 1–6.
- [11] N. P. Patel, R. Parekh, N. Thakkar, R. Gupta, S. Tanwar, G. Sharma, I. E. Davidson, and R. Sharma, "Fusion in cryptocurrency price prediction: A decade survey on recent advancements, architecture, and potential future directions," *IEEE Access*, vol. 10, pp. 34511–34538, 2022.
- [12] X. F. Liu, X.-J. Jiang, S.-H. Liu, and C. K. Tse, "Knowledge discovery in cryptocurrency transactions: A survey," *IEEE Access*, vol. 9, pp. 37229–37254, 2021.
- [13] J. Khangura and J. Arora, "A study on security threats to blockchain & cryptocurrencies," in *Proc. 3rd Int. Conf. Adv. Comput., Commun. Control Netw. (ICACN)*. Dec. 2021, pp. 1560–1564.
- [14] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020.
- [15] B. Hayes, "Anonymous one-time signatures and flexible untraceable electronic cash," in *Advances in Cryptology—AUSCRYPT* (Lecture Notes in Computer Science), vol. 453. Berlin, Germany: Springer, 1990, pp. 294–305.
- [16] P. Fauzi, S. Meiklejohn, R. Mercer, and C. Orlandi, "Quisquis: A new design for anonymous cryptocurrencies," in *Advances in Cryptology—ASIACRYPT* (Lecture Notes in Computer Science), vol. 11921. Cham, Switzerland: Springer, 2018, p. 990.
- [17] I. Osipkov, E. Y. Vasserman, N. Hopper, and Y. Kim, "Combating double-spending using cooperative P2P systems," in *Proc. 27th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2007, p. 41.
- [18] M. H. Miraz and M. Ali, "Applications of blockchain technology beyond cryptocurrency," 2018, *arXiv:1801.03528*.
- [19] T. M. Navamani, "A review on cryptocurrencies security," *J. Appl. Secur. Res.*, vol. 18, no. 1, pp. 49–69, 2023.
- [20] D. Ron and A. Shamir, "Quantitative analysis of the full Bitcoin transaction graph," in *Proc. 17th Int. Conf. Financ. Cryptogr. Data Secur. (FC)*. Heidelberg, Germany: Springer, 2013, pp. 6–24.
- [21] D. D. F. Maesa, A. Marino, and L. Ricci, "Uncovering the Bitcoin blockchain: An analysis of the full users graph," in *Proc. IEEE Int. Conf. Data Sci. Adv. Anal. (DSAA)*, Montreal, QC, Canada, Oct. 2016, pp. 537–546.
- [22] G. Fuchsbaumer, M. Orru, and Y. Seurin, "Aggregate cash systems: A cryptographic investigation of mumblewimble," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 11476. Cham, Switzerland: Springer, 2019, pp. 657–689.
- [23] X. Chen, M. A. Hasan, X. Wu, P. Skums, M. J. Feizollahi, M. Ouellet, E. L. Sevigny, D. Maimon, and Y. Wu, "Characteristics of Bitcoin transactions on cryptomarkets," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage* (Lecture Notes in Computer Science), vol. 11611. Cham, Switzerland: Springer, 2019, pp. 261–276.
- [24] A. Jivanyan, "Lelantus: Towards confidentiality and anonymity of blockchain transactions from standard assumptions," *Cryptol. ePrint Arch.* Accessed: Dec. 19, 2022. [Online]. Available: <https://eprint.iacr.org/2019/373>
- [25] J. Herrera-Joancomartí, "Research and challenges on Bitcoin anonymity," in *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance* (Lecture Notes in Computer Science), vol. 8872, J. Garcia-Alfaro et al., Eds. Cham, Switzerland: Springer, 2015, pp. 3–16.
- [26] Q. Wang, X. Li, and Y. Yu, "Anonymity for bitcoin from secure escrow address," *IEEE Access*, vol. 6, pp. 12336–12341, 2018.
- [27] Y. Liu, X. Liu, C. Tang, J. Wang, and L. Zhang, "Unlinkable coin mixing scheme for transaction privacy enhancement of Bitcoin," *IEEE Access*, vol. 6, pp. 23261–23270, 2018.
- [28] P. Fairley, "Blockchain world—Feeding the blockchain beast if Bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous," *IEEE Spectr.*, vol. 54, no. 10, pp. 36–59, Oct. 2017.
- [29] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *Proc. 25th IET Irish Signals Syst. Conf. China-Ireland Int. Conf. Inf. Communities Technol. (ISSC/CICT)*, 2014, pp. 280–285.
- [30] C. Domingo. (2017). *The Bitcoin vs Visa Electricity Consumption Fallacy*. [Online]. Available: <https://hackernoon.com/the-bitcoin-vsvisa-electricity-consumption-fallacy-8cf194987a50>
- [31] K. Liao, Z. Zhao, A. Doupe, and G.-J. Ahn, "Behind closed doors: Measurement and analysis of CryptoLocker ransoms in Bitcoin," in *Proc. APWG Symp. Electron. Crime Res. (eCrime)*, Toronto, ON, Canada, Jun. 2016, pp. 1–13.
- [32] M. Kiran and M. Stannett. (Dec. 2014). *Bitcoin Risk Analysis*. [Online]. Available: <http://www.nemode.ac.uk/wpcontent/uploads/2015/02/2015-Bit-Coin-risk-analysis.pdf>
- [33] A. Mittal, M. P. Gupta, M. Chaturvedi, S. R. Chansarkar, and S. Gupta, "Cybersecurity enhancement through blockchain training (CEBT)—A serious game approach," *Int. J. Inf. Manag. Data Insights*, vol. 1, no. 1, Apr. 2021, Art. no. 100001.
- [34] A. Batta, M. Gandhi, A. K. Kar, N. Loganayagam, and V. Ilavarasan, "Diffusion of blockchain in logistics and transportation industry: An analysis through the synthesis of academic and trade literature," *J. Sci. Technol. Policy Manag.*, vol. 12, no. 3, pp. 378–398, Jul. 2021.
- [35] A. K. Kar and L. Navin, "Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature," *Telematics Informat.*, vol. 58, May 2021, Art. no. 101532.
- [36] Y. Lu, "The blockchain: State-of-the-art and research challenges," *J. Ind. Inf. Integr.*, vol. 15, pp. 80–90, Sep. 2019.
- [37] L. D. Xu, Y. Lu, and L. Li, "Embedding blockchain technology into IoT for security: A survey," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10452–10473, Jul. 2021.

- [38] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities," *J. Ind. Inf. Integr.*, vol. 15, pp. 21–28, Sep. 2019.
- [39] S. F. Wamba and M. M. Queiroz, "Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities," *Int. J. Inf. Manag.*, vol. 52, Jun. 2020, Art. no. 102064.
- [40] S. Nakamoto. (2019). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: <https://git.dhimmel.com/bitcoin-whitepaper/>
- [41] Y. Lu, "Blockchain: A survey on functions, applications and open issues," *J. Ind. Integr. Manag.*, vol. 3, no. 4, Dec. 2018, Art. no. 1850015.
- [42] H. Yi, "A secure logistics model based on blockchain," *Enterprise Inf. Syst.*, vol. 15, no. 7, pp. 1002–1018, 2019.
- [43] Y. Lu, "Blockchain and the related issues: A review of current research topics," *J. Manag. Anal.*, vol. 5, no. 4, pp. 231–255, 2018.
- [44] E. K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 2, pp. 72–93, 2nd Quart., 2005
- [45] A. Miller and R. Jansen, "Shadow-Bitcoin: Scalable simulation via direct execution of multi-threaded applications," in *Proc. 8th Workshop Cyber Secur. Experimentation Test (CSET)*, Washington, DC, USA, 2015, p. 7.
- [46] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, "Tampering with the delivery of blocks and transactions in Bitcoin," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, Denver, CO, USA, Oct. 2015, pp. 692–705.
- [47] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing attacks on cryptocurrencies," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Jose, CA, USA, May 2017, pp. 375–392.
- [48] G. Wood. *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. Accessed: Dec. 14, 2022. [Online]. Available: <https://gavwood.com/paper.pdf>
- [49] Litecoin. (2022). *Litecoin Wiki*. [Online]. Available: https://litecoin.info/index.php/Main_Page
- [50] Ripple. (2016). *The Cost-Cutting Case for Banks-the ROI of Using Ripple and XRP for Global Interbank Settlements*. [Online]. Available: <http://ripple.com/xrp-portal>
- [51] Tether. (2019). *Tether Whitepaper*. [Online]. Available: <http://bit.ly/2nuc3eG>
- [52] N. T. Courtois, P. Emirdag, and D. A. Nagy, "Could Bitcoin transactions be 100x faster?" in *Proc. 11th Int. Conf. Secur. Cryptogr.*, Vienna, Austria, 2014, pp. 1–6.
- [53] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries," in *Proc. 12th Workshop Econ. Inf. Secur. (WEIS)*, Washington, DC, USA, 2013, pp. 1–21.
- [54] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is Bitcoin a decentralized currency?" *IEEE Security Privacy*, vol. 12, no. 3, pp. 54–60, May/June 2014.
- [55] *Crypto Market Capitalization*. Accessed: Dec. 13, 2022. [Online]. Available: <https://coinmarketcap.com/>
- [56] G. Gutoski and D. Stebila, "Hierarchical deterministic Bitcoin wallets that tolerate key leakage," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* New York, NY, USA: Springer, 2015, pp. 497–504.
- [57] D. Gambetta, "Can we trust trust," in *Trust: Making and Breaking Cooperative Relations*, vol. 13. Oxford, U.K.: Univ. Oxford, 2000, pp. 213–237.
- [58] L. Herskind, P. Katsikouli, and N. Dragoni, "Privacy and cryptocurrencies—A systematic literature review," *IEEE Access*, vol. 8, pp. 54044–54059, 2020.
- [59] E. Badawi and G.-V. Jourdan, "Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review," *IEEE Access*, vol. 8, pp. 200021–200037, 2020.
- [60] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.
- [61] E. Zaghoul, T. Li, M. W. Mutka, and J. Ren, "Bitcoin and blockchain: Security and privacy," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10288–10313, Oct. 2020.
- [62] L.-H. Zhu, B.-K. Zheng, M. Shen, F. Gao, H.-Y. Li, and K.-X. Shi, "Data security and privacy in Bitcoin system: A survey," *J. Comput. Sci. Technol.*, vol. 35, no. 4, pp. 843–862, Jul. 2020.
- [63] T. T. Huynh, T. D. Nguyen, and H. Tan, "A survey on security and privacy issues of blockchain technology," in *Proc. Int. Conf. Syst. Sci. Eng. (ICSSE)*, Jul. 2019, pp. 362–367.
- [64] A. P. Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Math. Found. Comput.*, vol. 1, no. 2, p. 121, 2018.
- [65] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, pp. 1–34, Jul. 2019.
- [66] N. Verma, S. Jain, and R. Doriya, "Review on consensus protocols for blockchain," in *Proc. Int. Conf. Comput., Commun., Intell. Syst. (ICC-CIS)*, Feb. 2021, pp. 281–286.
- [67] R. Longo, A. S. Podda, and R. Saia, "Analysis of a consensus protocol for extending consistent subchains on the Bitcoin blockchain," *Computation*, vol. 8, no. 3, p. 67, Jul. 2020.
- [68] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.
- [69] A. Alshamsi and P. P. Andras, "User perception of Bitcoin usability and security across novice users," *Int. J. Hum.-Comput. Stud.*, vol. 126, pp. 94–110, Jun. 2019.
- [70] M. Fröhlich, F. Gutjahr, and F. Alt, "Don't lose your coin! Investigating security practices of cryptocurrency users," in *Proc. ACM Designing Interact. Syst. Conf.*, Jul. 2020, pp. 1751–1763.
- [71] K. Krombholz, A. Judmayer, M. Gusenbauer, and E. Weippl, "The other side of the coin: User experiences with Bitcoin security and privacy," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Berlin, Germany, 2016, pp. 555–580.
- [72] M. T. Kurbucz, "Predicting the price of Bitcoin by the most frequent edges of its transaction network," *Econ. Lett.*, vol. 184, Nov. 2019, Art. no. 108655.
- [73] I. M. Wirawan, T. Widiyaningtyas, and M. M. Hasan, "Short term prediction on Bitcoin price using ARIMA method," in *Proc. Int. Seminar Appl. Technol. Inf. Commun. (iSemantic)*, Sep. 2019, pp. 260–265.
- [74] S. Lahmiri and S. Bekiros, "Cryptocurrency forecasting with deep learning chaotic neural networks," *Chaos, Solitons Fractals*, vol. 118, pp. 35–40, Jan. 2019.
- [75] L. Alessandretti, A. ElBahrawy, L. M. Aiello, and A. Baronchelli, "Anticipating cryptocurrency prices using machine learning," *Complexity*, vol. 2018, pp. 1–16, Nov. 2018.
- [76] Z. Chen, C. Li, and W. Sun, "Bitcoin price prediction using machine learning: An approach to sample dimension engineering," *J. Comput. Appl. Math.*, vol. 365, Feb. 2020, Art. no. 112395.
- [77] N. Smuts, "What drives cryptocurrency prices? An investigation of Google trends and telegram sentiment," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 46, no. 3, pp. 131–134, 2019.
- [78] A. Mittal, V. Dhiman, A. Singh, and C. Prakash, "Short-term Bitcoin price fluctuation prediction using social media and web search data," in *Proc. 12th Int. Conf. Contemp. Comput. (IC)*, Aug. 2019, pp. 1–6.
- [79] H. Jang and J. Lee, "An empirical study on modeling and prediction of Bitcoin prices with Bayesian neural networks based on blockchain information," *IEEE Access*, vol. 6, pp. 5427–5437, 2017.
- [80] E. Sin and L. Wang, "Bitcoin price prediction using ensembles of neural networks," in *Proc. 13th Int. Conf. Natural Comput., Fuzzy Syst. Knowl. Discovery (ICNC-FSKD)*, Jul. 2017, pp. 666–671.
- [81] M. Saad, J. Choi, D. Nyang, J. Kim, and A. Mohaisen, "Toward characterizing blockchain-based cryptocurrencies for highly accurate predictions," *IEEE Syst. J.*, vol. 14, no. 1, pp. 321–332, Mar. 2019.
- [82] D. Kondor, I. Csabai, J. Szule, M. Pósfai, and G. Vattay, "Inferring the interplay between network structure and market effects in Bitcoin," *New J. Phys.*, vol. 16, no. 12, Dec. 2014, Art. no. 125003.
- [83] M. Sorgente and C. Cibils. *The Reaction of a Network: Exploring the 1270 Relationship Between the Bitcoin Network Structure and the Bitcoin Price*. Accessed: Dec. 11, 2022. [Online]. Available: <http://snap.stanford.edu/class/cs224w-2014/projects/cs224w-27-final.pdf>
- [84] A. van Schetsen, "Impact of graph-based features on Bitcoin prices," M.S. thesis, Dept. Elect. Eng., Delft Univ. Technol., Delft, Netherlands, 2019.
- [85] A. K. Dey, C. G. Akcora, Y. R. Gel, and M. Kantarcioglu, "On the role of local blockchain network features in cryptocurrency price formation," *Can. J. Statist.*, vol. 48, no. 3, pp. 561–581, Sep. 2020.
- [86] S. Ji, J. Kim, and H. Im, "A comparative study of Bitcoin price prediction using deep learning," *Mathematics*, vol. 7, no. 10, p. 898, Sep. 2019.
- [87] U.S. Securities and Exchange Commission. (2017). *Customer Advisory: Beware Virtual Currency Pump-and-Dump Schemes*. [Online]. Available: <https://www.investor.gov/additional-resources/news-alerts/alertsbulletins/investor-alert-public-companies-making-ico-related>

- [88] *Investor Alert: Public Companies Making ICO-Related Claims*, The U.S. Commodity Futures Trading Commission, Washington, DC, USA, 2018.
- [89] T. Shintate and L. Pichl, "Trend prediction classification for high frequency Bitcoin time series with deep learning," *J. Risk Financial Manag.*, vol. 12, no. 1, p. 17, Jan. 2019.
- [90] Y. Peng, P. H. M. Albuquerque, J. M. C. D. Sá, A. J. A. Padula, and M. R. Montenegro, "The best of two worlds: Forecasting high frequency volatility for cryptocurrencies and traditional currencies with support vector regression," *Exp. Syst. Appl.*, vol. 97, pp. 177–192, May 2018.
- [91] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of Bitcoins: Characterizing payments among men with no names," in *Proc. Conf. Internet Meas. Conf.*, Oct. 2013, pp. 127–139.
- [92] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in Bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2013, pp. 34–51.
- [93] E. Androulaki, "Hyperledger fabric: A distributed operating system for permissioned blockchains," 2018, *arXiv:1801.10228*.
- [94] M. M. Chakravarty, S. Coretti, M. Fitz, P. Gazi, P. Kant, A. Kiayias, and A. Russell. *Hydra: Fast Isomorphic State Channels*. Accessed: Dec. 7, 2022. [Online]. Available: <https://eprint.iacr.org/2020/299.pdf>
- [95] L. Schwittmann, M. Wander, C. Boelmann, and T. Weis, "Privacy preservation in decentralized online social networks," *IEEE Internet Comput.*, vol. 18, no. 2, pp. 16–23, Mar. 2014.
- [96] M. Siddula, L. Li, and Y. Li, "An empirical study on the privacy preservation of online social networks," *IEEE Access*, vol. 6, pp. 19912–19922, 2018.
- [97] A. R. Javed, "Future smart cities requirements, emerging technologies, applications, challenges, and future aspects," *Cities*, vol. 129, Oct. 2022, Art. no. 103794.
- [98] N. Puri, V. Garg, and R. Agrawal, "Blockchain technology applications for next generation," in *Blockchain, Artificial Intelligence, and the Internet of Things*. Berlin, Germany: Springer, 2022, pp. 53–73.
- [99] K. Wust and A. Gervais, "Do you need a blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Zug, Switzerland, Jun. 2018, pp. 45–54.
- [100] A. A. Monrat, O. Schelen, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.
- [101] M. R. Islam, M. M. Rahman, M. Mahmud, M. A. Rahman, and M. H. S. Mohamad, "A review on blockchain security issues and challenges," in *Proc. IEEE 12th Control Syst. Graduate Res. Colloq. (ICSGRC)*, Shah Alam, Malaysia, Aug. 2021, pp. 227–232.
- [102] S. K. Dwivedi, P. Roy, C. Karda, S. Agrawal, and R. Amin, "Blockchain-based Internet of Things and industrial IoT: A comprehensive survey," *Secur. Commun. Netw.*, Aug. 2021, Art. no. 7142048.
- [103] B. Zaabar, O. Cheikhrouhou, M. Ammi, A. I. Awad, and M. Abid, "Secure and privacy-aware blockchain-based remote patient monitoring system for internet of healthcare things," in *Proc. 17th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2021, pp. 200–205.
- [104] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on Internet of Things (IoT), internet of everything (IoE) and internet of nano things (IoNT)," in *Proc. Internet Technol. Appl. (ITA)*, Sep. 2015, pp. 219–224.
- [105] A. S. Khan, K. Balan, Y. Javed, S. Tarmizi, and J. Abdullah, "Secure trust-based blockchain architecture to prevent attacks in VANET," *Sensors*, vol. 19, no. 22, pp. 1–27, 2019.
- [106] M. A. Karabulut, A. F. M. S. Shah, and H. Ilhan, "Performance optimization by using artificial neural network algorithms in VANETs," in *Proc. 42nd Int. Conf. Telecommun. Signal Process. (TSP)*, Jul. 2019, pp. 633–636.
- [107] M. A. Karabulut, A. F. M. S. Shah, and H. Ilhan, "A novel MIMO-OFDM based MAC protocol for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 11, pp. 20255–20267, Nov. 2022.
- [108] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical layer security in vehicular networks with reconfigurable intelligent surfaces," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–6.
- [109] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, K. Adhikari, G. Nauryzbayev, X. Li, and R. Kharel, "Toward physical-layer security for Internet of Vehicles: Interference-aware modeling," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 443–457, Jan. 2021.
- [110] K. M. Awan, M. Nadeem, A. S. Sadiq, A. Alghushami, I. Khan, and K. Rabie, "Smart handoff technique for Internet of Vehicles communication using dynamic edge-backup node," *Electronics*, vol. 9, no. 3, pp. 1–20, 2020.
- [111] O. A. Saraereh, A. Ali, I. Khan, and K. Rabie, "Interference analysis for vehicle-to-vehicle communications at 28 GHz," *Electronics*, vol. 9, no. 2, p. 262, Feb. 2020.
- [112] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, K. Adhikari, X. Li, M. Quiroz-Castellanos, and R. Kharel, "Reconfigurable intelligent surfaces-enabled vehicular networks: A physical layer security perspective," 2020, *arXiv:2004.11288*.
- [113] T. Rana, A. Shankar, M. K. Sultan, R. Patan, and B. Balusamy, "An intelligent approach for UAV and drone privacy security using blockchain methodology," in *Proc. 9th Int. Conf. Cloud Comput., Data Sci. Eng.*, Jan. 2019, pp. 162–167.
- [114] A. S. Shah and M. A. Karabulut, "Optimization of drones communication by using meta-heuristic optimization algorithms," *Sigma J. Eng. Natural Sci.*, vol. 40, no. 1, pp. 108–117, 2022.
- [115] M. A. Karabulut, A. F. M. Shah, M. B. Islam, and M. E. Rana, "OFDMA based UAVs communication for ensuring QoS," in *Applications of Artificial Intelligence and Machine Learning (Lecture Notes in Electrical Engineering)*, vol. 925. Singapore: Springer, 2022, doi: 10.1007/978-981-19-4831-2_27.
- [116] D.-T. Do, T.-T.-T. Nguyen, C.-B. Le, M. Voznak, Z. Kaleem, and K. M. Rabie, "UAV relaying enabled NOMA network with hybrid duplexing and multiple antennas," *IEEE Access*, vol. 8, pp. 186993–187007, 2020.
- [117] I. Rasheed, M. Asif, A. Ihsan, W. U. Khan, M. Ahmed, and K. M. Rabie, "LSTM-based distributed conditional generative adversarial network for data-driven 5G-enabled maritime UAV communications," *IEEE Trans. Intell. Transp. Syst.*, early access, Jul. 14, 2022, doi: 10.1109/TITS.2022.3187941.
- [118] S. AlJubayrin, F. N. Al-Wesabi, H. Alsolai, M. A. Duhayyim, M. K. Nour, W. U. Khan, A. Mahmood, K. Rabie, and T. Shongwe, "Energy efficient transmission design for NOMA backscatter-aided UAV networks with imperfect CSI," *Drones*, vol. 6, no. 8, pp. 1–14, 2022.
- [119] M. Sarfraz, "Capacity optimization of next-generation UAV communication involving non-orthogonal multiple access," *Drones*, vol. 6, no. 9, pp. 1–15, 2022.
- [120] A. F. M. S. Shah, "Architecture of emergency communication systems in disasters through UAVs in 5G and beyond," *Drones*, vol. 7, no. 1, pp. 1–16, Dec. 2022.
- [121] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2241–2263, Apr. 2019.
- [122] A. Douglas. (2018). *IBM Applies for Blockchain Patent to Address Drone Fleet Security*. Accessed: Feb. 3, 2020. [Online]. Available: <https://www.commercialdroneprofessional.com/ibm-applies-for-blockchain-to-address-drone-fleet-security/>
- [123] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies," in *Proc. IEEE Symp. Secur. Privacy*, Feb. 2015, pp. 104–121.
- [124] D. R. Figueiredo, J. K. Shapiro, and D. Towsley, "Using payments to promote cooperation in anonymity protocols," Dept. Comput. Sci., Citeseer. Accessed: Dec. 11, 2022. [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.4.500&rep=rep1&type=pdf>
- [125] X. Gao, G. D. Clark, and J. Lindqvist, "Of two minds, multiple addresses, and one ledger: Characterizing opinions, knowledge, and perceptions of Bitcoin across users and non-users," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, May 2016, pp. 1656–1668.
- [126] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "CoinShuffle: Practical decentralized coin mixing for Bitcoin," in *Computer Security—ESORICS (Lecture Notes in Computer Science)*, vol. 8713. Cham, Switzerland: Springer, 2014, pp. 345–364.
- [127] E. Ben-Sasson, "ZeroCash: Decentralized anonymous payments from Bitcoin," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2014, pp. 459–474.
- [128] C. Garman, M. Green, and I. Miers, "Accountable privacy for decentralized anonymous payments," in *Financial Cryptography Data Security (Lecture Notes in Computer Science)*, vol. 9603. Berlin, Germany: Springer, 2017, pp. 81–98.

- [129] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "P2P mixing and unlinkable Bitcoin transactions," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2017, pp. 1–15.
- [130] S. Meiklejohn and R. Mercer, "Möbius: Trustless tumbling for transaction privacy," *Proc. Privacy Enhancing Technol.*, vol. 2018, no. 2, pp. 105–121, Apr. 2018.
- [131] T. Ruffing and P. Moreno-Sanchez, "ValueShuffle: Mixing confidential transactions for comprehensive transaction privacy in Bitcoin," in *Financial Cryptography Data Security (Lecture Notes in Computer Science)*, vol. 10323. Cham, Switzerland: Springer, 2017, pp. 133–154.
- [132] A. Saxena, J. Misra, and A. Dhar, "Increasing anonymity in Bitcoin," in *Financial Cryptography Data Security (Lecture Notes in Computer Science)*, vol. 8438. Berlin, Germany: Springer, 2014, pp. 122–139.
- [133] T. E. Jedusor. *Mimblewimble*. Accessed: Dec. 21, 2022. [Online]. Available: <https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt>
- [134] G. Betarte, M. Cristiá, C. Luna, A. Silveira, and D. Zanarini, "Towards a formally verified implementation of the MimbleWimble cryptocurrency protocol," 2019, *arXiv:1907.01688*.
- [135] J. Groth, "On the size of pairing-based non-interactive arguments," *Cryptol. ePrint Arch.* Accessed: Dec. 9, 2022. [Online]. Available: <https://eprint.iacr.org/2016/260>
- [136] J. H. Ziegeldorf, R. Matzutt, M. Henze, F. Grossmann, and K. Wehrle, "Secure and anonymous decentralized Bitcoin mixing," *Future Gener. Comput. Syst.*, vol. 80, pp. 448–466, Mar. 2018.
- [137] E. Fujisaki and K. Suzuki, "Traceable ring signature," in *Public Key Cryptography—PKC (Lecture Notes in Computer Science)*, vol. 4450. Berlin, Germany: Springer, 2007, pp. 181–200.
- [138] X. Hou and C. H. Tan, "On fair traceable electronic cash," in *Proc. 3rd Annu. Commun. Netw. Services Res. Conf.*, 2005, pp. 39–44.
- [139] N. Van Saberhagen. *Cryptonote V 2.0*. Accessed: Dec. 14, 2022. [Online]. Available: <https://cryptonote.org/whitepaper.pdf>
- [140] M. Moser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, and N. Christin, "An empirical analysis of traceability in the Monero blockchain," in *Proc. 18th Privacy Enhancing Technol. (PETS)*, 2018, pp. 143–163.
- [141] D. A. Wijaya, J. Liu, R. Steinfeld, and D. Liu, "Monero ring attack: Recreating zero mixin transaction effect," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./ 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 1196–1201.
- [142] D. A. Wijaya, J. Liu, R. Steinfeld, D. Liu, and T. H. Yuen, "Anonymity reduction attacks to Monero," in *Information Security and Cryptology (Lecture Notes in Computer Science)*, vol. 11449. Cham, Switzerland: Springer, 2019, pp. 86–100.
- [143] A. Kumar, C. Fischer, S. Tople, and P. Saxena, "A traceability analysis of Monero's blockchain," in *Computer Security—ESORICS (Lecture Notes in Computer Science)*, vol. 10493. Cham, Switzerland: Springer, 2017, pp. 153–173.
- [144] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science)*, vol. 576, J. Feigenbaum, Eds. Berlin, Germany: Springer, Aug. 1991, pp. 129–140.
- [145] B. Bunz, S. Agrawal, M. Zamani, and D. Boneh, "Zether: Towards privacy in a smart contract world," *IACR Cryptol.*, vol. 2019, p. 191, Jan. 2019.
- [146] G. Kappos and A. M. Piotrowska, "Extending the anonymity of Zcash," 2019, *arXiv:1902.07337*.
- [147] E. Daniel, E. Rohrer, and F. Tschorsch, "Map-Z: Exposing the Zcash network in times of transition," in *Proc. IEEE 44th Conf. Local Comput. Netw. (LCN)*, Oct. 2019, pp. 84–92.
- [148] C. Ganesh, C. Orlandi, and D. Tschudi, "Proof-of-stake protocols for privacy-aware blockchains," in *Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science)*, vol. 11476. Cham, Switzerland: Springer, 2019, pp. 690–719.
- [149] S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan, "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies," *Proc. Privacy Enhancing Technol.*, vol. 2018, no. 4, pp. 179–199, 2018.
- [150] S. Meiklejohn and C. Orlandi, "Privacy-enhancing overlays in Bitcoin," in *Proc. 2nd Workshop Bitcoin Res.*, Jan. 2015, pp. 127–141.



A. F. M. SHAHEN SHAH (Senior Member, IEEE) received the B.Sc. degree in electronics and telecommunication engineering from Daffodil International University, Bangladesh, in 2009, the M.Sc. degree in information technology from the University of Dhaka, Bangladesh, in 2011, and the Ph.D. degree in electronics and communication engineering from Yildiz Technical University, Turkey, in 2020. He worked as an Assistant Professor with the Department of Electrical and Electronics Engineering, Istanbul Gelisim University, Turkey, from 2020 to 2021. He also worked in the industry for ten years, where he held a higher management position. Since 2021, he has been working as an Assistant Professor with the Department of Electronics and Communication Engineering, Yildiz Technical University. He is the author of a book. He has published a good number of research papers in international conferences and journals. His current research interests include wireless communications, artificial intelligence, and cross-layer design. He is a Life Member of the Institution of Engineers, Bangladesh (IEB). He has been a TPC member of several IEEE conferences and a regular reviewer for various IEEE journals. For his Ph.D. work, he won a Gold Medal at the 32nd International Invention, Innovation and Technology Exhibition (ITEX 2021). He is currently serving as an Editor for the *Open Transportation Journal* (Bentham) and an Associate Editor for the *Journal of Cyber Security Technology* (Taylor & Francis).

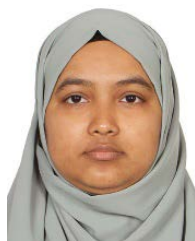


MUHAMMET ALI KARABULUT (Member, IEEE) received the B.Sc. degree in electrical and electronics engineering from Mustafa Kemal University, Hatay, Turkey, in 2010, and the M.Sc. and Ph.D. degrees in electronics and communication engineering from Yildiz Technical University, Istanbul, Turkey, in 2015 and 2021, respectively. He was a Research and Teaching Assistant at the Department of Electronics and Communication Engineering, Yildiz Technical University,

from 2013 to 2021. He has been working as an Assistant Professor with the Department of Electrical and Electronics Engineering, Kafkas University, Turkey, since 2022. His research interests include digital communication, cooperative communication, and MAC protocols for vehicular ad hoc networks.



A. F. M. SUAIB AKHTER (Member, IEEE) received the Ph.D. degree from the Department of Computer and Information Engineering, Sakarya University, Turkey, in 2021. He is currently working as a Lecturer with the Sakarya University of Applied Sciences. He is also involved in several projects related to distributed systems and the Internet of Things (IoT). His research interests include blockchain technology, the IoT, wireless communications, vehicular ad hoc networks, intelligent vehicles, network security, distributed systems, and machine learning. He is also serving as an Associate Editor for the *Journal of Cyber Security Technology* (Taylor & Francis) and a guest editor for many special issues of different journals.



NAZIFA MUSTARI (Graduate Student Member, IEEE) received the B.Sc. degree in mathematics from the University of Dhaka, Bangladesh, in 2017. She is currently pursuing the M.Sc. degree in electronics and communication engineering with Yildiz Technical University, Turkey. Her current research interests include wireless communications, blockchain, and cross-layer design.



AL-SAKIB KHAN PATHAN (Senior Member, IEEE) received the B.Sc. degree in computer science and information technology from the Islamic University of Technology (IUT), Bangladesh, in 2003, and the Ph.D. degree in computer engineering from Kyung Hee University, South Korea, in 2009. He is currently a Professor with the Department of Computer Science and Engineering, United International University (UIU), Bangladesh. In his academic

career so far, he worked as a Faculty Member at Independent University, Bangladesh, from 2020 to 2021; Southeast University, Bangladesh, from 2015 to 2020; International Islamic University Malaysia (IIUM), Malaysia, from 2010 to 2015; BRACU, Bangladesh, from 2009 to 2010; and NSU, Bangladesh, from 2004 to 2005. He has served as the General Chair, an Organizing Committee Member, and a Technical Program Committee Member in numerous international conferences/workshops like INFOCOM, GLOBECOM, and ICC. He was awarded the IEEE Outstanding Leadership Award for his role in IEEE GreenCom 2013 Conference. Among various editorial roles, he is also serving as the Editor-in-Chief for *International Journal of Computers and Applications* and *Journal of Cyber Security Technology* (Taylor & Francis); an Associate Editor for *Connection Science* (Taylor & Francis); an Editor for *Ad Hoc and Sensor Wireless Networks* (Old City Publishing) and *International Journal of Sensor Networks* (Inderscience Publishers); a guest editor for many special issues of top-ranked journals, and an editor/author for 32 books.



KHALED M. RABIE (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in electrical and electronic engineering from The University of Manchester, in 2011 and 2015, respectively. He is currently a Reader with the Department of Engineering, Manchester Metropolitan University (MMU), U.K. He worked as a part of several largescale industrial projects and has published more than 200 journals and conference papers (mostly IEEE). His current research interest

includes designing and developing next-generation wireless communication systems. He is a fellow of the U.K. Higher Education Academy (FHEA) and

a Fellow of the European Alliance for Innovation (EAI). He serves regularly on the technical program committee (TPC) for several major IEEE conferences, such as GLOBECOM, ICC, and VTC. He has received many awards over the past few years in recognition of his research contributions, including the Best Paper Awards at the 2021 IEEE CITS and the 2015 IEEE ISPLC, and IEEE Access Editor of the Month Award, in August 2019. He is also serving as an Editor for IEEE COMMUNICATIONS LETTERS, an Editor for *IEEE Internet of Things Magazine*, an Associate Editor for IEEE ACCESS, and an Executive Editor for the *Transactions on Emerging Telecommunications Technologies* (Wiley).



THOKOZANI SHONGWE (Senior Member, IEEE) received the B.Eng. degree in electronic engineering from the University of Swaziland, Swaziland, the M.Eng. degree in telecommunications engineering from the University of the Witwatersrand, South Africa, and the D.Eng. degree from the University of Johannesburg, South Africa. He is currently an Associate Professor of telecommunications and the Head of the School of Electrical and Electronic Engineering, University

of Johannesburg. His research interests include digital communications, visible light communications (VLC), and security.

...