

SoK: Unifying Definitions of Privacy and Anonymity in Cryptocurrencies and DLTs

GERARD DE ROODE, TNO, The Hague, Netherlands and University of Twente, Enschede, Netherlands
MAARTEN EVERTS, University of Twente, Enschede, Netherlands and Linksight, Utrecht, Netherlands

As interest in the practical use of cryptocurrencies continues to grow, so does the focus on the (perceived) privacy and anonymity of users within this domain. Despite this attention, there is a notable absence of standardized definitions for these terms. This article aims to address this gap by exploring the various interpretations of privacy, anonymity, and related concepts in the context of cryptocurrencies. Drawing from a thorough review of existing literature, we propose practical definitions for both privacy and anonymity. Utilizing these definitions, we introduce an ontology designed to streamline future research, identify knowledge gaps, and facilitate clearer communication in the field.

CCS Concepts: • **Security and privacy** → *Pseudonymity, anonymity and untraceability; Privacy-preserving protocols; Privacy protections*; • **Networks** → **Network privacy and anonymity**;

Additional Key Words and Phrases: cryptocurrency, privacy, anonymity, ontology

ACM Reference format:

Gerard de Roode and Maarten Everts. 2026. SoK: Unifying Definitions of Privacy and Anonymity in Cryptocurrencies and DLTs. *Distrib. Ledger Technol.* 5, 3, Article 29 (May 2026), 14 pages.
<https://doi.org/10.1145/3736656>

1 Introduction

Individual payments are inherently personal; a glimpse into one's bank transactions can reveal significant insights into their life. For example, payments may reveal political preferences, shopping habits, or even specific health problems. However, the increasing digitization of payments means that this information is no longer as fleeting as it once was in the era of physical cash. Initially, the cryptocurrency Bitcoin was lauded for its privacy and anonymity features in popular media. Yet, it is now widely understood that Bitcoin offers, at best, a form of pseudonymity and is generally inadequate for concealing financial trails. Over the years, numerous projects and initiatives have emerged to enhance privacy in the realm of cryptocurrencies and **Distributed Ledger Technologies (DLTs)**. However, comparing these initiatives is challenging due to inconsistent terminology.

More specifically, *privacy* and *anonymity* are closely related concepts that are sometimes hard to distinguish [11]. As a result, these terms are frequently interchanged; some see anonymity as part of privacy (e.g., [1, 19, 44, 48]), some perceive privacy as part of anonymity (e.g., [31]), yet others consider them synonymous (e.g., [2]). On the other hand, some studies also clearly differentiate between them: “one [Privacy] is about hiding the content, and one [Anonymity] is about hiding who is saying it” [11].

Authors' Contact Information: Gerard de Roode, TNO, The Hague, Netherlands and University of Twente, Enschede, Netherlands; e-mail: arne.deroode@tno.nl; Maarten Everts (corresponding author), University of Twente, Enschede, Netherlands and Linksight, Utrecht, Netherlands; e-mail: maarten.everts@utwente.nl.



This work is licensed under Creative Commons Attribution International 4.0.

© 2026 Copyright held by the owner/author(s).

ACM 2769-6480/2026/5-ART29

<https://doi.org/10.1145/3736656>

Given this backdrop, the primary objective of this article is to clarify the definitions in use and to distinguish clearly between privacy and anonymity. To this end, we propose specific definitions for these terms in the context of cryptocurrencies, based on a thorough review of existing literature. Finally, we compile commonly used concepts and terms related to privacy and anonymity in the literature and introduce an ontology that outlines the relationships and definitions among these terms.

2 Proposed Definitions

As noted, no comprehensive or common definition is employed for privacy or anonymity in current literature on cryptocurrencies. Therefore, based on the study we present in this article, we propose definitions for these concepts in this section. To establish these definitions, we have put the common understanding of these concepts (as expressed in dictionary definitions) in the context of cryptocurrencies and studied current literature for the definitions used there. In Section 3.1, we align the common understanding of privacy and anonymity with current literature. Moreover, we highlight the (in)consistencies among literature definitions. As such, Section 3.1 serves as both a background and justification for the definitions presented here, highlighting the variation in existing definitions while providing a rationale for our chosen terms.

2.1 Privacy

Based on the definition from the Cambridge dictionary [13] and the way privacy is used in the literature, the definition of privacy that we propose to be used in the context of DLT systems is as follows:

Definition 2.1. Privacy is the right of a DLT system user to keep secret any data stored or used within the DLT system that pertains to them.

In the discussed literature on cryptocurrencies and DLTs in general, privacy as a right and confidentiality/secretcy are regularly mixed up. Privacy is more often perceived as “the hiding of things,” although, as commonly interpreted, privacy is something that pertains to a person and is about the right to hide things as desired. Consequently, hiding things is a tool to express this right. In available research, privacy is often seen as a property of a system, a technology, or an object (e.g., transaction). However, a system itself does not directly have privacy, nor does a transaction, although they might help to ensure a user’s privacy. As such, we propose to label these systems or objects as *privacy-preserving*, which is a property rather than a right.

This means that privacy is not secrecy, confidentiality, or anonymity; it is a higher-level concept that is about users. However, as already noted above, this definition does not satisfy the use of the term *privacy* in current literature. In many instances, the term privacy in literature should be interpreted as *privacy-preserving*. We propose to explicitly differentiate between privacy as a right, and the ability to ensure that right which is granted through *privacy-preserving* measures. Obviously, various levels of privacy-preservation are possible, still, in general, something that is privacy-preserving contributes to (at least in part) protecting a user’s privacy. Thus, we propose the following definition of *privacy-preserving*.

Definition 2.2. Privacy-preserving is a property of systems, technologies, or objects reflecting their ability to protect the privacy of their users (to some extent).

The dual use of the term privacy in literature, both as defined in Definitions 2.1 and 2.2, could be interpreted as some form of an abuse of notation. This provides basis to allow the use of the term *privacy* in this way. However, such an abuse of notation hinders the discussion on privacy, since it is misaligned with the common understanding of privacy in other disciplines and in daily life. The privacy provided in cryptocurrencies is relevant to multiple parties; users, merchants, developers, regulators, and law enforcement, among others. To enable discussion and clear communication between these parties, which come from different backgrounds and disciplines, aligned

definitions are crucial. The introduced definition aims to contribute to this by providing an alternative to noted abuse of notation.

2.1.1 Anonymity. Definitions of anonymity have also been shown to vary in recent research. However, compared to privacy there is more agreement on what anonymity is and what it is not, which is likely due to it being a more descriptive term. We propose to take the definition of anonymity presented in [38] as the definition to be used for anonymity in DLT. This definition is also the basis for multiple other recent studies, which provide further fine-grained notions of anonymity [4].

Definition 2.3. Anonymity is the state of being not identifiable within a set of subjects, the anonymity set.

The relation between anonymity and privacy is such that to enable privacy protection, anonymity may be a measure to achieve some level of privacy-preservation. Moreover, anonymity can be used as an indicator to assess the level of privacy-preservation that a system provides to a user.

3 Definitions in (Current) Literature

Privacy and anonymity are interpreted in different ways in recent literature¹ on cryptocurrencies and DLTs; no comprehensive and common definition is employed for either. Moreover, privacy is often not defined when used in literature on DLTs. In this section, we discuss available definitions leading to the definition proposed in the previous section, despite the fact it has already been suggested that no “unified formal privacy definition” exists [22]. Availability and adoption of good definitions can aid communication about these topics and will allow for better comparison between technologies. In this section we show our analysis of the definitions of privacy and anonymity from included studies. In our analysis, we gathered privacy and anonymity definitions from all included papers and subsequently looked for common factors in these definitions. We then extracted what we call “definition aspects.” A “definition aspect” is a facet of a privacy or anonymity definition that occurs in some of the included papers. Based on the definition aspects we group the included studies and thereby show how the studies include different though also partially overlapping aspects in their definitions.

3.1 Literature Analysis Results

In our analysis, we also included dictionary definitions of these concepts. We included these to represent the common understanding of these concepts in a wider scope, to be able to compare this with interpretation in the field of DLT research. Moreover, we included privacy and anonymity interpretations from Monero [18, 41, 43] and Zcash [8, 47] as found in their corresponding whitepapers and documentation, to represent the view on these concepts from the perspective of the privacy-centric DLT community. The results of the analysis are summarized in Tables 1 and 2. In these tables, the included studies are grouped. The dictionary references are in bold, and the Monero and Zcash references are underlined to highlight these specifically.

The results of our literature analysis are shown in Tables 1 and 2. When a study is shown in a specific row in a table, that means that the study incorporated that definition aspect in their definition of privacy (or anonymity for the anonymity table) explicitly or implicitly. Any given study can be mentioned in multiple rows in the table, when the definition from that study includes multiple aspects. Multiple studies include no explicit definition of privacy or anonymity. For some of these studies we were able to extract their interpretation of privacy and/or anonymity through the way these concepts were discussed or implicitly defined. Using columns of the table, we differentiate between explicit definitions and implicit definitions. In essence, an implicit definition comes down to our interpretation of the meaning that a study attributes to privacy or anonymity.

¹We included papers on privacy and anonymity in DLTs published since 2019, and selected a few key studies from before this period.

Table 1. Privacy Definitions in Current Literature

Definition aspect	Explicit definition	Implicit definition
A user's right to control their data	[This study], [13, 20, 34, 47]	[11, 14, 23, 24, 28, 41]
Hiding the identity of users (senders/receivers)	[26, 43]	[1, 3, 8, 39, 44]
Hiding links among addresses and/or transactions	[48]	[5, 37]
Hiding of certain (on-chain) data (e.g., transaction data)	[18, 24, 26, 30, 31]	[8, 11, 28, 37, 39, 40, 44]
Anonymity	[48]	[1, 2, 8, 24, 37, 39, 44]
Not defined	[1–6, 8, 11, 14–16, 19, 23, 25, 28, 29, 32, 33, 37, 39, 40, 43, 44–46, 49]	

Bold references are from the dictionary, and underlined definitions are from Monero and Zcash documentation. The implicit definition column contains studies that, according to our interpretation, imply these definitions' aspects in their discussion of privacy.

Table 2. Anonymity Definitions in Current Literature

Definition aspect	Explicit definition	Implicit definition
Unidentifiable in a set	[This study], [2, 4, 34, 37, 38]	[4, 17, 39]
Any entity indistinguishable from any other entity	[3, 4]	[31]
Name not known	[12]	[11, 26]
Hiding identity of users (senders and receivers)	[17, 24, 30, 40, 43]	[1, 8, 11, 14, 39]
Unlinkability of transactions/addresses to user identities	[17, 43]	[1, 3, 4, 8, 26, 28, 48]
Taint-resistance	[33]	
Privacy		[2, 31, 39]
Not defined	[1, 5, 6, 8, 11, 14–16, 18, 19, 20, 23, 25, 26, 28, 29, 31, 32, 39, 41, 44–46, 47, 48, 49]	

Bold references are from the dictionary, and underlined definitions are from Monero and Zcash documentation. The implicit definition column contains studies that, according to our interpretation, imply these definitions' aspects in their discussion of anonymity

When a concept is not defined in a study, that study is placed in the “Not defined” row. Sometimes we were able to extract an implicit definition, then the study is still included in the “Not defined” row, since there is no actual definition, just our understanding of the interpretation in that study.

3.2 Findings

Through our analysis of definitions in current literature, as shown in the tables, we obtained multiple insights regarding privacy and anonymity definitions and interpretations, which are discussed in this section.

- *Lacking definitions.* As is obvious from both tables, quite often the literature on privacy and anonymity in DLT does not (explicitly) define privacy and anonymity, though often these papers still make numerous claims about these concepts. The majority of the included studies do not provide explicit definitions, even though they are discussing these ill-defined concepts. This shows that the meaning of these concepts is assumed to be clear, while from our analysis it appears there is no such common ground.

- *Misaligned definitions.* It also quickly becomes clear that interpretations vary widely. For example, while some studies see privacy as pertaining to users, others interpret privacy as the visibility of certain types of information. Moreover, while there is agreement that anonymity has to do with the identity and identifiability of users, nuances differ as to whether anonymity is about the users themselves or objects (e.g., transactions) being linkable to them. Definitions are also conflicting sometimes, which becomes clear in the mingling of privacy and anonymity in current literature.
- *Interchanging privacy and anonymity.* The tables show that sometimes anonymity is seen as an aspect of privacy, while even sometimes privacy is seen as part of anonymity. This highlights interpretations of these concepts are sometimes conflicting, and that some see them as equivalent while others do not. Interchanging privacy and anonymity also happens in the content of several studies. For example, in [2] a four-tier system is introduced to further specify anonymity. Another study [39] refers to the same system although there it is used to indicate levels of privacy. A second example can be seen in [4] and [5]. By choosing unlinkability and indistinguishability, [4] is very similar to [5] which was published much earlier. The earlier study [5] uses unlinkability and indistinguishability as notions of privacy and uses these to quantify privacy of Bitcoin users. Amarasinghe et al. [4] generalize some of the principles presented in [5] and applies these to anonymity rather than privacy. However, the approach in [4] is similar to [5]: formal definitions are provided and game-based definitions of the used notions are introduced in [5].
- *Common understanding.* As appears from the previous notes, there is not yet a common understanding of privacy and anonymity in the scientific DLT community that discusses these concepts. Dictionaries base their definitions of concepts on public understanding, which is analyzed by lexicographers through spoken and written texts. Thereby, a dictionary definition should represent the general understanding of a concept. We included the dictionary definitions of privacy and anonymity in bold in the tables. Arguably, the meaning of these concepts in the context of DLTs should not be too far from dictionary definitions, to avoid misunderstandings when crossing the border of the DLT community. Currently, privacy is often not interpreted as a right of a user. While the dictionary does interpret it as a right of a person, many studies perceive privacy to be about hiding some type of information. In the DLT privacy and anonymity literature, anonymity is seldom interpreted to be specifically about the name of a user, which is the dictionary interpretation. Generally, in the DLT literature, it is interpreted to be about the identity of the user, and specifically about the distinguishability of that identity. This can be seen as an application of the dictionary definition to the DLT context, where the name of a user is represented by some identity. However, this application of the general understanding to the DLT context has not been made explicit thus far.
- *Privacy-centric community definitions.* To represent the perspective of the privacy-centric community on privacy and anonymity, we included definitions from Monero and Zcash. The Cryptonote whitepaper [43], which outlines the theory behind Monero, uses a privacy definition from another study which entails hiding the links between user identities and their transactions. Their anonymity interpretation is rather similar: all senders must be equiprobable (untraceability) and all given two transactions it is impossible to determine whether they were sent to the same user (unlinkability). As such, links between identities of senders/receivers and their transactions must be hidden. In other public sources on Monero, privacy is also about hiding certain data [18], although privacy is also said to be about users [41]. The paper on Zerocash [8] (the protocol that is implemented in Zcash) does not explicitly define privacy. However, implicitly it is interpreted as anonymity, hiding certain transaction data, and hiding user identities. Anonymity is not explicitly defined either, but seems to refer to linking transactions to identities and hiding senders and receivers. Other Zcash sources do explicitly define privacy as a right of users [20, 47]. It appears that even within the privacy-centric DLT community, there is no clear agreement on what privacy does (not) entail. Moreover, the differentiation between privacy and anonymity in these discussions is unclear.
- *Privacy versus privacy-preservation.* In many studies, including the Monero [43] and Zcash [8] papers, privacy is interpreted not as a right but as the hiding of certain information. According to our view, hiding

information can be a way to enforce privacy; it enables a user to control what information they reveal. Thereby, hiding information can be seen as a form of privacy-preservation. However, privacy itself is *the right* of the users to control what information they reveal, as is also supported by multiple of the included studies. Distinguishing privacy and privacy-preservation helps to discuss privacy across disciplines, since it separates two interpretations of privacy that are both common.

- *Anonymity framework.* Amarasinghe et al. [3] stress that “an acceptable framework to model anonymity in the context of cryptocurrencies” is something to be developed and would greatly contribute to understanding and evaluating the performance of cryptocurrencies in this regard. In that same work, Amarasinghe et al. do provide multiple ways to parameterize anonymity, which do not yet provide such a framework which lay the ground-work for their next study [4]. In that next study, a “*fine-grained, formal* qualitative model of anonymity” is introduced. The models uses two notions to characterize anonymity: *indistinguishability* and *unlinkability*. The study furthermore creates a formal model of an adversary and an anonymity game (which is designed like security games in cryptography). These are subsequently used to devise anonymity notions based on parameterized adversary characteristics and an adversary goal which is (breaking) indistinguishability or unlinkability. This leads to a sophisticated formal model of anonymity, which can be used to evaluate the anonymity of cryptocurrencies by analyzing which of the anonymity notions is satisfied (i.e., which anonymity game does (not) result in adversary success).

Based on the tables and our findings, we conclude that unequivocal definitions should be introduced and interpretations aligned. The discussed literature confirms there is no common definition of privacy or anonymity, although there is more agreement on the latter. No agreement on terminology poses a problem since it becomes hard to compare results or develop a common ground for evaluation of systems that enhance privacy or anonymity. Ideally, the introduced definitions should bridge the gaps between the general understanding of privacy and anonymity and the interpretations of these concepts in DLT literature. We introduced such definitions in Section 2, to serve as a common ground for discussion and evaluation of studies and technologies regarding privacy and anonymity, and unify researchers in their approach to these concepts.

Our privacy definition improves ambiguity by separating privacy (as a right) and privacy-preservation. It includes the “privacy as a right” interpretation which is taken both in the dictionary and in some privacy-focused literature and statements from the privacy-focused DLT community. Moreover, it gives way to the interpretation of “privacy as hiding certain data” by labeling this as privacy-preservation, which distinguishes this from privacy itself while acknowledging the close connection that “hiding data” has with privacy.

The anonymity definition proposed in this study also overlaps with some current literature, which has already built further on this definition. Moreover, the chosen definition unifies the other definition aspects. Identifiability is a common theme in most definition aspects of anonymity that we observed in literature, and our proposed definition is based on this common theme. We applied this to the DLT setting, in which identifiability of a user among a set of users is the topic of interest, when anonymity is considered. Finally, the chosen interpretation is widely accepted for the “anonymity in networks”-setting, which is similar to the cryptocurrency setting.

4 Privacy- and Anonymity-Related Concepts in Cryptocurrencies

There are several other terms that are often used in combination with anonymity and privacy in the context of DLT systems, which are briefly discussed below. We will not provide an overview as thorough as we did for privacy and anonymity, however we do base our definitions on interpretations from current literature as much as possible. This overview can serve as a frame of reference when discussing privacy and anonymity in cryptocurrencies using these terms. We propose a common understanding of these concepts, aimed at improving in particular cross-discipline communication. As a part of improving the common understanding of these anonymity and privacy-related concepts in the context of cryptocurrencies, we also highlight the relations between these

concepts, for which we use a structured figure. First, in Section 4.1, we propose definitions for the terms that are often used, which is followed by a visual ontology in Section 4.2 that shows the relations between the concepts.

4.1 Definitions

Transaction Privacy. Existing literature on privacy and anonymity in cryptocurrencies regularly mentions transaction privacy [15, 17, 19, 23, 26, 32, 37, 44, 48, 49]. Definitions in current literature are mostly about transaction privacy-preservation, rather than privacy. They mention methods such as hiding addresses or amounts, which prevent linkage and clustering of transactions. Therefore, we propose a definition of transaction privacy-preservation based on definitions of transaction privacy (from current work): the extent to which transaction properties like addresses and amounts can be hidden. Transaction privacy-preservation supports user privacy in cryptocurrencies by enabling the user to hide information about them that is embedded in transactions.

Accountability. Within the context of cryptocurrencies *accountability* is the extent to which a cryptocurrency user can be held accountable for their transactions. To hold a user accountable, it must be possible to identify activity as belonging to a specific user. Current literature relates cryptocurrency use to criminal transactions and concludes that accountability is necessary such that when a user does something malicious this is detectable and can be penalized [14, 19, 37]. It is also mentioned that to achieve this some traceability is required [19, 30, 37].

Accountability is also often mentioned in relation to coin mixing protocols (e.g., [30, 44, 48]). In such systems, accountability means that the mix provider or system can be held accountable for their actions, and dishonesty will be registered by the system and result in a penalty or public reputation loss. Thereby, accountable mixes are safer to use and will be less likely to result in loss of funds.

(In)distinguishability. Throughout current work various types of indistinguishability are presented, the most comprehensive definition thereof is provided in [3, 4, 38]. As such, we propose to use a definition for indistinguishability based on these: in the context of cryptocurrencies indistinguishability means that an entity cannot be distinguished from any entity of the same type. This works well with definitions for coin- [3], profile- [3, 5], ledger- [1, 40], or mix-address [30] indistinguishability when these are the entities to distinguish, and the definition in [34].

Furthermore, in [23] a unique variant of distinguishability is mentioned. This study shortly mentions distinguishability of various techniques that are used to improve privacy-preservation. For example, CoinJoin transactions may easily be distinguished from other transactions.

Confidentiality. This is another often-used term in relation to privacy and anonymity in cryptocurrencies. Many of the considered studies interpret confidentiality specifically as the hiding of transaction amounts (e.g., [1–3]). Some studies have a more general interpretation, where confidentiality refers to hiding some (private) (transaction) data [1, 16]. Even when confidentiality is not discussed, Confidential Transactions are often mentioned as a privacy-preserving technique. This technique, which was introduced in Monero, relates to confidentiality in that it enables hiding of transaction amounts. In this work, we propose to define confidentiality in the context of cryptocurrencies as the hiding of otherwise public data such as transaction data (e.g., sender/receiver addresses or amounts) using cryptographic techniques. We restrict it to cryptographic techniques to discern it from confusion techniques. Moreover, we propose a rather general definition such that the term, which is quite general in itself, can also be used for describing the hiding of things other than transaction amounts.

Immutability. Immutability is also regularly used in relation to privacy and anonymity in cryptocurrencies. It does not affect privacy or anonymity directly, but causes (public) data to be persistent. In combination with transparency, it is detrimental to privacy-preservation; once information is made public on a cryptocurrency blockchain, that cannot be reversed (without detection). Existing literature provides the following notes on

immutability (also coined tamper-resistance [26]): it is mentioned that the blockchain is an append-only ledger [15] that cannot be modified without detection [16, 19, 37]; and immutability comes from the need of verification and traceability of changes [19].

We stay in line with existing definitions. Immutability is the impossibility to modify or delete data after it has been appended to a cryptocurrency ledger. Immutability is usually implemented and enforced with the use of hash functions.

Transparency. This often-used term in literature on cryptocurrency privacy-preservation refers to the public visibility of the data that is generated within the cryptocurrency system. More specifically, some cryptocurrencies use a ledger in which all transactions are publicly visible and readable, although the level of transparency varies among cryptocurrencies. Several studies note that transparency is at odds with privacy-preservation [15, 16, 26, 37, 39, 40, 44, 46] and anonymity [31, 33], since transparency provides an adversary with a lot of data to attack the privacy of users. It is also noted that transparency is required for accountability [49] and transparency provides auditability [48]. Finally, [30] mentions that transparency causes Bitcoins to not be fully equal since the history of coins can be compared, essentially preventing full fungibility. This also goes for many other coins that follow a similar design.

Linkability. In current literature, (un)linkability is an often-used term with varying interpretations (e.g., [1, 6, 23, 27, 30, 31, 39, 40]). In the context of cryptocurrencies, it refers to the ability to link entities to each other; for example, linking transactions or addresses that belong to the same user or linking identities to addresses [24]. Conversely, unlinkability means an adversary cannot extract the relation between two entities [3]. Three types of linkability are mentioned most often:

- Transaction linkability [26, 37, 48]: An adversary can link (at least) two transactions that belong to the same user.
- Address linkability [17, 32, 45]: An adversary can link (at least) two addresses that belong to the same user.
- Input-output linkability: In Bitcoin-like cryptocurrencies, the links between transaction inputs and outputs are easily observed; mixing protocols like CoinJoin aim to break this link [3, 46]. When external unlinkability is achieved, an observer cannot know what inputs and outputs are related. Internal unlinkability is achieved when the mixing service does not know the input-output relationship either [15, 19, 32, 44]. Finally, when both internal and external unlinkability is realized full unlinkability is reached [22].

Transaction- and address unlinkability together are characterized as activity unlinkability in [5]. In [15], linkability is also used to refer to connecting transactions to users who participated in them. Finally, some variants of unlinkability are used, such as value unlinkability and metadata unlinkability, which entail that transactions cannot be linked based on these properties [4].

Linkability is also connected to distinguishability; when transactions are pairwise indistinguishable it becomes impossible to link them to each other [33]. This also goes for currency units, which ties into our definition of fungibility.

In conclusion, based on [38] and the above, we propose to define linkability as the extent to which entities in a cryptocurrency can be linked together, where entities can be users, transactions, and so on. On the other hand, unlinkability then entails that two entities are no more related than they would be when they occurred outside of the cryptocurrency system.

Finally, it should be noted that many Bitcoin-like cryptocurrencies inherently suffer from linkability, since transactions are linked to previous transaction by design [34]. This also enables traceability.

Traceability. This entails tracing activity back to its origin and is also said to be equal to sender anonymity [3, 4, 26]. As such, in cryptocurrencies, traceability is the extent to which transactions can be traced back to their sender, while the opposite (full untraceability) means all possible senders are equiprobable [39].

Traceability is clearly related to (transaction) linkability [31, 34]; transactions can only be traced when they are linkable to their history. In fact, in many blockchain-based systems, each transaction references previous transactions, causing inherent linkability and thereby traceability. Traceability is countered by breaking input–output links in transactions using privacy-preserving technologies like ring signatures and mixing protocols [30, 40]. Such technologies decrease linkability, and thereby decrease traceability.

Fungibility. Another regularly mentioned fundamental property of currency systems [4, 15] is fungibility. We endorse a definition based on [31]: any two value units (e.g., dollars or bitcoins) should be “pairwise indistinguishable.” Fungibility will ensure that the currency units have the same value, when a unit is uniquely identifiable (for example through its visible history as in Bitcoin-like cryptocurrencies) it may be blocklisted by some, thereby decreasing its value. As such, the transparency, linkability, and traceability, as encountered in many cryptocurrencies, is detrimental to fungibility. As it is defined here, fungibility is the same as coin indistinguishability [3], which was mentioned earlier.

Decentralization. This is one of the core ideas around which DLT systems are built. Decentralization in the context of cryptocurrencies means there is no central party for governance or management and execution of transactions and other functions in the currency system. To operate, ledgers are mostly transparent and distributed, communication happens in a peer-to-peer fashion, and consensus is reached using a dedicated distributed consensus protocol (of which blockchain is often a key component). This provides resistance to centralized security risks (single point of failure) and can improve fairness (everyone can contribute and participate) and even privacy (no central authoritarian party that may misuse (transaction) data). On the other hand, decentralization often means openness and public data which provides adversaries with a broad attack surface.

Obfuscation. Different types of obfuscation have in common that they hide an entity among other entities of the same type and make the relations between entities unclear. After obfuscation an adversary cannot distinguish their target entity anymore. Mixing services exemplify this: CoinJoin combines inputs from different users, resulting in multiple indistinguishable equal-valued outputs. As a result, each of the separate inputs is (somewhat) obfuscated since it cannot be known which output belongs to the input thus obfuscating the input–output relationship within a transaction [2, 30, 37]. Ring signatures achieve a similar result [23]. Obfuscation may also obscure the link between an input and a previous output [34], for example through centralized mixing services (pool mixing) [23, 32].

Furthermore, some cryptocurrency systems aim to obfuscate IP-addresses of its participants using technologies like I2P and TOR [27, 31]. Users can also try to obfuscate their cryptocurrency activity by creating new addresses for each of their activities (like receiving and sending funds) [5].

Based on the above, we propose to define obfuscation as “hiding an entity (such as an address or transaction) and its relations among other entities of the same type.”

Identifiability. Some studies mention identifiability in the context of cryptocurrency privacy-preservation [3, 17, 48], referring to linking activity to real-world identities. This may be achieved by aggregating traceability information, clustering addresses and transaction, and possibly even linking this to exchange information. Identifiability is related to profile distinguishability: when a user can be profiled, the adversary learns information about the user that can help to identify them. Taint resistance and traceability are similarly related to identifiability: when looking at a coin, being able to trace it back through previous transactions may provide information on the current ownership [3]. In [44], identifiability is referred to as identity privacy. In conclusion, identifiability is the extent to which entities or events in a cryptocurrency system can be linked to a user’s real-world identity.

Deniability. Deniability is the ability of a cryptocurrency user to deny they participated in certain activity or own a certain entity [1, 3, 39]. Of course, a user could always deny such claims, however when a system provides deniability it means an adversary cannot prove (using information from the system) the opposite: “plausible

deniability” [1, 34, 40]. (Plausible) Deniability may be provided through techniques that break linkability and traceability; for example, CoinJoin transactions allow a participant to plausibly deny that a certain output of that transaction is theirs [39]. Rinberg and Agarwal [40] also relate deniability to fungibility in Monero, it notes that when for all transaction outputs it can be denied whether they are spent or not, then they are fungible since they cannot be distinguished from each other. Logically, deniability prevents accountability; no one can be held accountable for a transaction if they can plausibly deny it is theirs.

Persistency. Persistency, which is sometimes mentioned (e.g., [1] and [48]) is similar to immutability: data cannot be changed or removed after it has been included in the cryptocurrency ledger (it is tamper-resistant and will persist). Persistency emphasizes that the data remains forever in the system, while immutability emphasizes the tamper-resistance of that data. Since cryptocurrency ledgers often combine transparency and persistency, adversaries are provided with a lot of public data to use for attacking the privacy of users.

Auditability. Throughout current literature the terms auditability and auditable are used with varying meaning. Some studies propose to enable government-like parties to audit transactions (which includes de-anonymization) to be able to trace illicit money flows and hold criminals accountable [3]. On the other hand, Herskind et al. [24] state there are proposals to make the tracing of transactions auditable, such that not just anyone can trace but only authorized parties. Another recent study states that Bitcoin-like transactions are auditable by default since they are persistent and public [48]. Auditability is therefore related to persistency and transparency. Auditability is closely related to accountability; to hold anyone accountable for transactions, it must be possible for transactions to be audited. In line with existing literature, we propose to define auditability as the extent to which it is possible for a party external to the cryptocurrency system to investigate the source and history of funds used in a certain transaction.

Taint(-Resistance). Since the input to a new transaction refers to an output of a previous transaction (in a UTXO-model cryptocurrency), some information is transferred from that output to the new transaction input, which is called taint in cryptocurrency literature. Thus, for any address A that holds some coins, those coins are tainted by all inputs to the transactions that transferred these coins to address A. For example, when one of these inputs to one of these transactions was previously associated with illicit activity, this information (and the illicitness) is carried over to the coins in address A because that input taints the coins in address A. The concept of taint and taint resistance was introduced by [33]. Subsequently, tools (e.g., [35]) have been developed to do taint analysis and compute taint values (which indicates the strength of a connection between two addresses through taint). Taint resistance is the extent to which taint can be prevented, such that no information is carried over from address to address through transactions. As such, Herskind et al. [24] define taint resistance as “an attacker’s inability to link a transaction’s source with its destinations, given the source is tainted.” Therefore, unlinkability is a method to achieve taint resistance. Moreover, Amarasinghe et al. [3] relate taint resistance to identifiability, traceability, and fungibility. Obviously, when coins are tainted differently that means they can be distinguished and fungibility decreases as a result. Traceability is a requirement for taint analysis, when previous transactions cannot be found then an address is untainted. Finally, taint can be used to fingerprint and profile users, which decreases anonymity.

Pseudonymity. It “is the use of pseudonyms as IDs” [38]. If a DLT system user uses a pseudonym (e.g., a string of random characters), then the pseudonym identifies that user. Pseudonymity somewhat improves the anonymity of cryptocurrency users, although whenever pseudonyms can be coupled to identities in some way the advantage is lost.

4.2 Relations between Concepts

Based on the definitions and relations between these definitions as discussed in the past section, we created an ontology graph of privacy- and anonymity-related concepts in cryptocurrencies (see Figure 1). This provides a

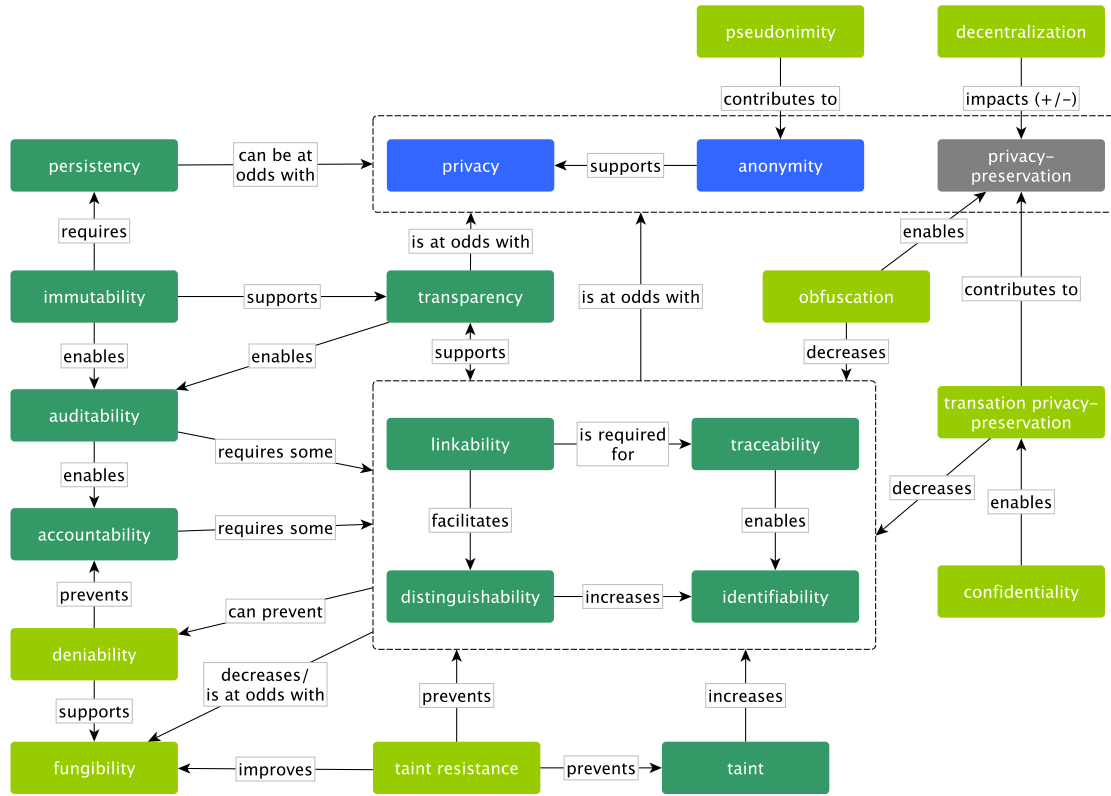


Fig. 1. Ontology of privacy-related concepts in the context of DLTs.

visual representation of how the concepts relate to each other, with short descriptions of the relations on the connecting edges.

The natural (and obvious) tension between concepts supporting privacy (light green) and the concepts related to accountability/traceability on the other hand (dark green) is clearly shown in this figure. This tension is in essence the challenge of finding a balance between the needs of a society (transparency, solving crimes) and the needs of the individual (privacy). This topic is very relevant in the context of **Central Bank Digital Currencies (CBDCs)**. And there are possibilities to marry individual privacy and accountability using technological advances, specifically in the context of *permissioned* blockchains. Some approaches build upon the foundations of Zerocash/Zcash [8] and add additional zk-SNARK circuits for additional accountability and regulatory control. In [21] the authors build upon Zerocash and zk-SNARKs to support privacy-preserving policy enforcement to guarantee regulatory compliance. Similarly, Bontekoe et al. [10] also build upon the Zerocash approach to allow fully anonymous transactions for small (aggregated) amounts and auditable transactions for larger amounts. Other approaches focus on auditability [9, 36], accountability with high-throughput [42], or high-complexity policy enforcement [7].

5 Conclusion

In this study, we extensively explored the literature concerning privacy and anonymity within the realm of cryptocurrencies. Our aim was to understand how these concepts are currently defined and to propose standardized definitions for use in both cryptocurrency-specific and broader DLT research. Additionally, we identified and clarified several other terms that are pertinent to discussions of privacy and anonymity in this context. The outcome

of this research serves as a frame of reference for future studies on privacy or anonymity in cryptocurrencies and CBDCs. We specifically welcome our work to be used as a basis for a framework that can be used for a systematic analysis of cryptocurrency projects, DLTs, and CBDC proposals with respect to their privacy-preserving properties. Specifically, we would like a more technical and/or formal definition of privacy to be developed, perhaps in line with or the game-based definition of anonymity of [4]. Such a definition can then be used as the basis for a framework for the comparison of both “traditional” and privacy-focused cryptocurrencies in a fair way.

A limitation of the current work is that the proposed definitions are based mostly on definitions from cryptocurrency-related research. Additional research is required to see whether the definitions can indeed also be applied to non-cryptocurrency-focused DLTs.

References

- [1] Ghada Almashaqbeh and Ravital Solomon. 2022. SoK: Privacy-preserving computing in the blockchain era. In *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*, 124–139. DOI: <https://doi.org/10.1109/EuroSP53844.2022.00016>
- [2] N. Alsalamy and B. Zhang. 2019. SoK: A systematic study of anonymity in cryptocurrencies. In *2019 IEEE Conference on Dependable and Secure Computing (DSC)*, 165–174. DOI: <https://doi.org/10.1109/DSC47296.2019.8937681>
- [3] Niluka Amarasinghe, Xavier Boyen, and Matthew McKague. 2019. A survey of anonymity of cryptocurrencies. In *Australasian Computer Science Week Multiconference (ACSW '19)*. ACM, New York, NY, Article 2, 10 pages. DOI: <https://doi.org/10.1145/3290688.3290693>
- [4] Niluka Amarasinghe, Xavier Boyen, and Matthew McKague. 2021. The cryptographic complexity of anonymous coins: A systematic exploration. *Cryptography* 5, 1 (2021), 10. DOI: <https://doi.org/10.3390/cryptography5010010>
- [5] Elli Androulaki, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2013. Evaluating user privacy in Bitcoin. In *Financial Cryptography and Data Security*. Ahmad-Reza Sadeghi (Ed.), Springer, Berlin, 34–51.
- [6] A. Averin, A. Samartsev, and N. Sachenko. 2020. Review of methods for ensuring anonymity and de-anonymization in blockchain. In *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 82–87. DOI: <https://doi.org/10.1109/ITQMIS51053.2020.9322974>
- [7] Christian Badertscher, Mahdi Sedaghat, and Hendrik Waldner. 2023. Fine-Grained Accountable Privacy via Unlinkable Policy-Compliant Signatures. *Cryptology ePrint Archive*, Paper 2023/1070. Retrieved from <https://eprint.iacr.org/2023/1070>
- [8] E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. 2014. Zerocash: Decentralized anonymous payments from Bitcoin. In *2014 IEEE Symposium on Security and Privacy*, 459–474. DOI: <https://doi.org/10.1109/SP.2014.36>
- [9] Dmytro Bogatov, Angelo De Caro, Kaoutar Elkhyaoui, and Björn Tackmann. 2021. Anonymous transactions with revocation and auditing in Hyperledger Fabric. In *20th International Conference on Cryptology and Network Security (CANS '21)*. Mauro Conti, Marc Stevens, and Stephan Krenn (Eds.), Lecture Notes in Computer Science, Vol. 13099, Springer, 435–459. DOI: https://doi.org/10.1007/978-3-030-92548-2_23
- [10] Tariq Bontekoe, Maarten H. Everts, and Andreas Peter. 2022. Balancing privacy and accountability in digital payment methods using zk-SNARKs. In *19th Annual International Conference on Privacy, Security and Trust (PST '22)*. IEEE, 1–10. DOI: <https://doi.org/10.1109/PST55820.2022.9851987>
- [11] Danny Bradbury. 2014. Anonymity and privacy: A guide for the perplexed. *Network Security* 2014, 10 (2014), 10–14. DOI: [https://doi.org/10.1016/S1353-4858\(14\)70102-3](https://doi.org/10.1016/S1353-4858(14)70102-3)
- [12] Cambridge. 2021. Anonymity. In *Cambridge English Dictionary*. Cambridge University Press. Retrieved from <https://dictionary.cambridge.org/dictionary/english/anonymity>
- [13] Cambridge. 2021. Privacy. In *Cambridge English Dictionary*. Cambridge University Press. Retrieved from <https://dictionary.cambridge.org/dictionary/english/privacy>
- [14] Sherman S. M. Chow, Kim-Kwang Raymond Choo, and Jinguang Han. 2021. Editorial for accountability and privacy issues in blockchain and cryptocurrency. *Future Generation Computer Systems* 114 (2021), 647–648. DOI: <https://doi.org/10.1016/j.future.2020.08.039>
- [15] Mauro Conti, E. Sandeep Kumar, Chhagan Lal, and Sushmita Ruj. 2018. A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials* 20, 4 (2018), 3416–3452.
- [16] Yuchong Cui, Bing Pan, and Yanbin Sun. 2019. A survey of privacy-preserving techniques for blockchain. In *Artificial Intelligence and Security*. Xingming Sun, Zhaoqing Pan, and Elisa Bertino (Eds.), Springer International Publishing, Cham, 225–234.
- [17] Dominic Deuber, Viktoria Ronge, and Christian Rückert. 2022. SoK: Assumptions underlying cryptocurrency deanonymizations. *Proceedings on Privacy Enhancing Technologies* 3 (2022), 670–691. DOI: <https://doi.org/10.5653/popets-2022-0091>
- [18] The Cryptonote Developers. 2023. Monero (GitHub ReadMe). Retrieved from <https://github.com/monero-project/monero/blob/ac02af92867590ca80b2779a7bbeafa99ff94dcb/README.md>

- [19] Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. 2019. A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications* 126 (2019), 45–58. DOI: <https://doi.org/10.1016/j.jnca.2018.10.020>
- [20] Zcash Foundation. 2023. Home—Zcash Foundation—Our Mission. Retrieved December 21, 2023 from <https://zfnf.org/>
- [21] Christina Garman, Matthew Green, and Ian Miers. 2016. Accountable privacy for decentralized anonymous payments. In *20th International Conference on Financial Cryptography and Data Security (FC '16)*, Revised Selected Papers. Jens Grossklags and Bart Preneel (Eds.), Lecture Notes in Computer Science, Vol. 9603, Springer, 81–98. DOI: https://doi.org/10.1007/978-3-662-54970-4_5
- [22] Daniel Genkin, Dimitrios Papadopoulos, and Charalampos Papamanthou. 2018. Privacy in decentralized cryptocurrencies. *Communications of the ACM* 61, 6 (May 2018), 78–88. DOI: <https://doi.org/10.1145/3132696>
- [23] Simin Ghesmati, Walid Fdhila, and Edgar Weippl. 2022. User-Perceived Privacy in Blockchain. Cryptology ePrint Archive, Paper 2022/287. Retrieved from <https://eprint.iacr.org/2022/287>
- [24] L. Herskind, P. Katsikouli, and N. Dragoni. 2020. Privacy and cryptocurrencies—A systematic literature review. *IEEE Access* 8 (2020), 54044–54059. DOI: <https://doi.org/10.1109/ACCESS.2020.2980950>
- [25] Loren Jolly. 2022. Ensuring the protection of privacy of cryptocurrency users: An impossible task? In *Law and Technology in a Global Digital Society: Autonomous Systems, Big Data, IT Security and Legal Tech*. Georg Borges and Christoph Sorge (Eds.), Springer International Publishing, Cham, 105–120. DOI: https://doi.org/10.1007/978-3-030-90513-2_6
- [26] Aisha Zahid Junejo, Manzoor Ahmed Hashmani, and Abdullah Abdulrehman Alabdulatif. 2020. A survey on privacy vulnerabilities in permissionless blockchains. *International Journal of Advanced Computer Science and Applications* 11, 9 (2020), 130–139. DOI: <https://doi.org/10.14569/IJACSA.2020.0110915>
- [27] N. Khan and M. Nassar. 2019. A look into privacy-preserving blockchains. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, 1–6. DOI: <https://doi.org/10.1109/AICCSA47632.2019.9035235>
- [28] Lyudmila Kovalchuk, Roman Oliynykov, Yurii Bespalov, and Mariia Rodinko. 2022. *Methods of Ensuring Privacy in a Decentralized Environment*. Springer International Publishing, Cham, 1–32. DOI: https://doi.org/10.1007/978-3-030-95161-0_1
- [29] Merve Can Kus and Albert Levi. 2022. Investigation and application of differential privacy in Bitcoin. *IEEE Access* 10 (2022), 25534–25554. DOI: <https://doi.org/10.1109/ACCESS.2022.3151784>
- [30] M. C. Kus Khalilov and A. Levi. 2018. A survey on anonymity and privacy in Bitcoin-like digital cash systems. *IEEE Communications Surveys & Tutorials* 20, 3 (2018), 2543–2585. DOI: <https://doi.org/10.1109/COMST.2018.2818623>
- [31] J. Lee. 2019. Rise of anonymous cryptocurrencies: Brief introduction. *IEEE Consumer Electronics Magazine* 8, 5 (2019), 20–25. DOI: <https://doi.org/10.1109/MCE.2019.2923927>
- [32] Y. Li, W. Susilo, G. Yang, Y. Yu, X. Du, D. Liu, and N. Guizani. 2019. Toward privacy and regulation in blockchain-based cryptocurrencies. *IEEE Network* 33, 5 (2019), 111–117. DOI: <https://doi.org/10.1109/MNET.2019.1800271>
- [33] Sarah Meiklejohn and Claudio Orlandi. 2015. Privacy-enhancing overlays in Bitcoin. In *Financial Cryptography and Data Security*. Michael Brenner, Nicolas Christin, Benjamin Johnson, and Kurt Rohloff (Eds.), Springer, Berlin, 127–141.
- [34] Malte Möser. 2022. *Cryptocurrency Privacy in Practice*. Ph.D. Dissertation. Princeton University.
- [35] M. Möser, R. Böhme, and D. Breuker. 2013. An inquiry into money laundering tools in the Bitcoin ecosystem. In *2013 APWG eCrime Researchers Summit*, 1–14. DOI: <https://doi.org/10.1109/eCRS.2013.6805780>
- [36] Neha Narula, Willy Vaquez, and Madars Virza. 2018. zkLedger: Privacy-preserving auditing for distributed ledgers. In *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI '18)*. USENIX Association, Renton, WA, 65–80. Retrieved from <https://www.usenix.org/conference/nsdi18/presentation/narula>
- [37] Li Peng, Wei Feng, Zheng Yan, Yafeng Li, Xiaokang Zhou, and Shohei Shimizu. 2021. Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks* 7, 3 (2021), 295–307. DOI: <https://doi.org/10.1016/j.dcan.2020.05.008>
- [38] Andreas Pfizmann and Marit Köhntopp. 2001. Anonymity, unobservability, and pseudonymity—A proposal for terminology. In *Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability*. Hannes Federrath (Ed.), Springer, Berlin, 1–9. DOI: https://doi.org/10.1007/3-540-44702-4_1
- [39] Chaitanya Rahalkar and Anushka Virgaonkar. 2021. Summarizing and analyzing the privacy-preserving techniques in Bitcoin and other cryptocurrencies. arXiv:2109.07634. Retrieved from <https://arxiv.org/abs/2109.07634>
- [40] Roy Rinberg and Nilaksh Agarwal. 2022. Privacy when Everyone is Watching: An SOK on Anonymity on the Blockchain. Cryptology ePrint Archive, Paper 2022/985. Retrieved from <https://eprint.iacr.org/2022/985>
- [41] Monero Core Team. 2023. About Monero—Monero—Secure, Private, Untraceable. Retrieved December 21, 2023 from <https://www.getmonero.org/resources/about/>
- [42] Alin Tomescu, Adithya Bhat, Benny Applebaum, Ittai Abraham, Guy Gueta, Benny Pinkas, and Avishay Yanai. 2022. UTT: Decentralized Ecash with Accountable Privacy. Cryptology ePrint Archive, Paper 2022/452. Retrieved from <https://eprint.iacr.org/2022/452>
- [43] Nicolas Van Saberhagen. 2013. CryptoNote v 2.0. Retrieved from <https://www.getmonero.org/resources/research-lab/pubs/cryptonote-whitepaper.pdf>
- [44] D. Wang, J. Zhao, and Y. Wang. 2020. A survey on privacy protection of blockchain: The technology and application. *IEEE Access* 8 (2020), 108766–108781. DOI: <https://doi.org/10.1109/ACCESS.2020.2994294>

- [45] Philipp Winter, Anna Harbluk Lorimer, Peter Snyder, and Benjamin Livshits. 2023. Security, privacy, and decentralization in Web3. arXiv:2109.06836. Retrieved from <https://arxiv.org/abs/2109.06836>
- [46] Tianjiao Yu and Chunjie Cao. 2020. Privacy protection in blockchain systems: A review. In *Data Processing Techniques and Applications for Cyber-Physical Systems (DPTA '19)*. Chuanchao Huang, Yu-Wei Chan, and Neil Yen (Eds.), Springer, Singapore, 2045–2052.
- [47] Zcash. 2023. Zcash: Privacy-Protecting Digital Currency—Features—Privacy. Retrieved December 21, 2023 from <https://z.cash/>
- [48] Tianyu Zhao and Tao Zhang. 2021. Revisiting anonymity and privacy of Bitcoin. In *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1275–1280. DOI : <https://doi.org/10.1109/TrustCom53373.2021.00175>
- [49] Saide Zhu. 2021. *Privacy Preservation & Security Solutions in Blockchain Network*. Ph.D. Dissertation. Georgia State University. DOI : <https://doi.org/10.57709/23973698>

Received 29 December 2023; revised 12 March 2025; accepted 18 April 2025