Privacy-Preserving Reputation Systems based on Blockchain and other Cryptographic Building Blocks: A Survey

OMAR HASAN and LIONEL BRUNIE, University of Lyon, CNRS, INSA-Lyon, LIRIS, France
ELISA BERTINO, Department of Computer Science, Purdue University, USA

The purpose of a reputation system is to hold the users of a distributed application accountable for their behavior. The reputation of a user is computed as an aggregate of the feedback provided by fellow users in the system. Truthful feedback is clearly a prerequisite for computing a reputation score that accurately represents the behavior of a user. However, it has been observed that users can hesitate in providing truthful feedback because, for example, of fear of retaliation. Privacy-preserving reputation systems enable users to provide feedback in a private and thus uninhibited manner. In this survey, we propose analysis frameworks for privacy-preserving reputation systems. We use these analysis frameworks to review and compare the existing approaches. Emphasis is placed on blockchain-based systems as they are a recent significant development in the area. Blockchain-based privacy-preserving reputation systems have properties, such as trustlessness, transparency, and immutability, which prior systems do not have. Our analysis provides several insights and directions for future research. These include leveraging blockchain to its full potential in order to develop truly trustless systems, to achieve some important security properties, and to include defenses against common attacks that have so far not been addressed by most current systems.

CCS Concepts: • **Information systems** → **Reputation systems**; • **Security and privacy** → *Trust frameworks*; *Distributed systems security*; • **General and reference** → *Surveys and overviews*.

Additional Key Words and Phrases: Anonymity, blockchain, computational trust, privacy, reputation, trustlessness

ACM Reference Format:
Omar Hasan, Lionel Brunie, and Elisa Bertino. 2021. Privacy-Preserving Reputation Systems based on Blockchain and other Cryptographic Building Blocks: A Survey. *ACM Comput. Surv.* 55, 2, Article 111 (September 2021), 37 pages. https://doi.org/10.1145/3490236

1 INTRODUCTION

Reputation systems are an essential tool for determining the trustworthiness of users in environments where there is no pre-established trust in users. Reputation of a *target* user is computed by aggregating the subjective feedback provided by other users, referred to as *source* users. These are users who have previously interacted with the target user and have consequently gained personal experience regarding her actions in the context of the given application. It is expected that actions perceived as legitimate will lead to high positive feedback and thus to an aggregated positive reputation score. Inversely, a target user acting dishonestly will elicit negative feedback resulting in a low aggregated reputation score. Any

Authors' addresses: Omar Hasan, omar.hasan@insa-lyon.fr; Lionel Brunie, lionel.brunie@insa-lyon.fr, University of Lyon, CNRS, INSA-Lyon, LIRIS, F-69621, France; Elisa Bertino, bertino@purdue.edu, Department of Computer Science, Purdue University, IN, 47907, USA.

0360-0300/2021/9-ART111 $15.00
https://doi.org/10.1145/3490236

users concerned about the legitimacy of future actions of a potential transacting partner can consider the computed reputation score of this partner as an indication of her trustworthiness. Reputation systems thus assist in holding users accountable for their actions despite the initial absence of trust in the users.

E-commerce marketplaces and sharing economy based platforms are some popular applications where reputation systems are employed. Sites and mobile applications such as ebay.com, airbnb.com, and uber.com are significant examples. Additionally, systems by Liu et al. [61], Azad et al. [8], Bag et al. [11], and Schaub et al. [79] are some of the academic approaches for managing reputation in e-commerce and retail environments. Let's consider Airbnb (airbnb.com), which is an online marketplace for vacation rentals. The platform enables independent hosts to offer their private lodgings to guests for short stays. The reputation system of the platform plays a critical role since the guests seeking satisfactory accommodations can only rely on the reputation of the hosts and their offerings stemming from reviews by previous guests. Similarly, hosts concerned about lending out their lodgings to well-behaving guests also depend on the reputation system.

Another application that relies on reputation systems is mobile participatory sensing, where users sense various environmental conditions with their mobile devices and submit sensing data to a central entity for analysis. Reputation is used to discourage users from providing corrupted information. Systems by Jo and Choi [52], Ma et al. [63], and Mousa et al. [71] are examples of reputation systems that focus on this application area. A related application area is participatory sensing in Vehicular Adhoc Networks (VANETs), where vehicles collect and upload information about road conditions. Reputation systems by Zhao et al. [97], Lu et al. [62], and Chen et al. [23] aim to hold the vehicles and their owners accountable for submitting false data. One more notable application area, among several others, that relies on reputation systems is the Internet of Things (IoT). Trusting corrupted devices in the IoT can undermine network security [9]. Recent systems by Azad et al. [7, 9] are instances of reputation systems for this application domain.

It has been documented that users may hesitate to provide truthful feedback [68, 77]. Reasons range from fear of retaliation to negative reviews [68, 77] to concerns about revealing sensitive personal information [69]. Returning to the example of Airbnb, we note that its reputation system escrows the feedback until both parties have submitted their opinion. The reason is to prevent tit for tat retribution by the hosts and the guests. However, the truthfulness and the impartiality of user feedback can still be impacted by the personal nature of the reviews [46]. Hiding the identities of the users has been recommended as a solution [46]. Moreover, it has been observed that the lack of anonymity on Airbnb "causes people to feel pressure to post reviews that lean positive" [72].

Privacy-preserving reputation systems are designed to allay the fears of feedback providers by protecting the confidentiality of their individual feedback. The implication is that providing feedback in a private manner encourages the raters to submit honest and accurate feedback. Another approach that privacy-preserving reputation systems take to motivate users to submit their truthful feedback is guaranteeing their anonymity. Operating in an anonymous manner in the system means that a third party is unable to attribute sensitive personal information to the user or to profile the user in the long term. Privacy-preserving reputation systems are therefore an important category of reputation systems for scenarios where user privacy or anonymity needs to be upheld.

The research area of privacy-preserving reputation systems is fairly mature. All academic reputation systems cited above are in fact privacy-preserving. Reputation systems that support user privacy were first proposed in the mid 2000s. Some notable original works include those by Pavlov et al. [75], Kinateder and Pearson [58], and Dingledine et al. [31], among others. However, privacy-preserving reputation systems continue to evolve to cater for emerging application areas, such as Social IoT (Azad et al. [9]), Industrial IoT-enabled retail marketing (Liu et al. [61]), and Intercloud (Dou et al. [34]). Moreover, the advent of

the blockchain technology has recently fueled further research in this area. The use of blockchain as a building block has resulted in privacy-preserving reputation systems that have important novel properties such as trustlessness, transparency, and immutability. For example, Schaub et al.'s [79] system does not require users to trust third parties or any fellow users in order to guarantee their privacy and thus provides trustlessness. This property was absent from prior systems. Another important reason for recent research in the area of privacy-preserving reputation systems is that a number of issues still remain open. As we discuss in Section 8, these issues include lack of important security properties and defenses against common attacks.

We believe that a comprehensive survey is needed to offer a uniform perspective to the rich literature in this area. Moreover, we believe that our survey is timely because of the recent emergence of systems based on blockchain as well as novel systems for emerging application domains. In this survey, we analyze 44 privacy-preserving reputation systems proposed between the years 2003 and 2021 inclusive, while placing emphasis on recent systems based on blockchain.

Reputation systems that support user privacy have always mostly relied on cryptographic building blocks and their combinations to provide strong security guarantees. These building blocks include Secure Multi-Party Computation (SMPC), secret sharing, homomorphic encryption, zero-knowledge proofs, and cryptographic signatures. Blockchain is a recent addition to this arsenal of cryptographic building blocks utilized by privacy-preserving reputation systems. We analyze blockchain-based systems as well as systems based on other building blocks and security mechanisms in this survey.

1.1 Contributions

This survey makes the following contributions:

- Identification of the various dimensions of privacy-preserving reputation systems. An analysis framework that allows for the decomposition and comparison of privacy-preserving reputation systems in a normalized manner.
- Identification of the security requirements of privacy-preserving reputation systems that cut across multiple types of these systems.
- Definition of broad categories of privacy-preserving reputation systems proposed in the literature according to their security mechanisms.
- Fine-grained analysis and comparison of 44 privacy-preserving reputation systems using the proposed analysis frameworks.
- Detailed review of several significant and representative privacy-preserving reputation systems proposed in the literature.
- Discussion of the analysis results, and based on these results, insights and directions for future work in this research area.

1.2 Organization

The rest of the paper is organized as follows. Section 2 proposes an analysis framework that identifies the dimensions and the requirements of privacy-preserving reputation systems. Section 3 defines two broad categories of privacy-preserving reputation systems with respect to their security objectives. Section 4 develops an analysis framework encompassing the various non-privacy related dimensions of reputation systems. Section 5 defines broad categories of the privacy-preserving reputation systems proposed in the literature according to their security mechanisms. Section 6 presents a fine-grained analysis of privacy-preserving reputation systems proposed in the literature according to the frameworks established in Sections 2 through 4. Section 7 describes in greater detail some of the blockchain-based systems. Section 8

discusses the analysis results and relevant insights. Section 9 summarizes the related work and Section 10 concludes the survey.

2 AN ANALYSIS FRAMEWORK FOR PRIVACY-PRESERVING REPUTATION SYSTEMS

In this section, we introduce our analysis framework that identifies the common dimensions and requirements of privacy-preserving reputation systems. The dimensions of the analysis framework regarding security objectives are described in Section 3. We conduct a fine-grained analysis and comparison of privacy-preserving reputation systems proposed in the literature using this framework in Section 6.

Some fundamental concepts in reputation systems are as follows:

Source User (Rater). A user u is said to be a source user or rater of a user t if u has feedback about t in a given context.

Target User (Ratee). When a source user assigns feedback to a user t, or a user q initiates a query to determine the reputation of user t, the user t is referred to as the target user or the ratee.

Querying User (Querier, Inquirer). When a user q initiates a query to determine the reputation of a user t, the user q is referred to as the querying user, the querier, or the inquirer.

Reputation. The reputation of a target user is any function that aggregates the feedback of its source users. In Section 4, we list some possible realizations of the aggregation function.

Our analysis framework is graphically represented in Figure 1.

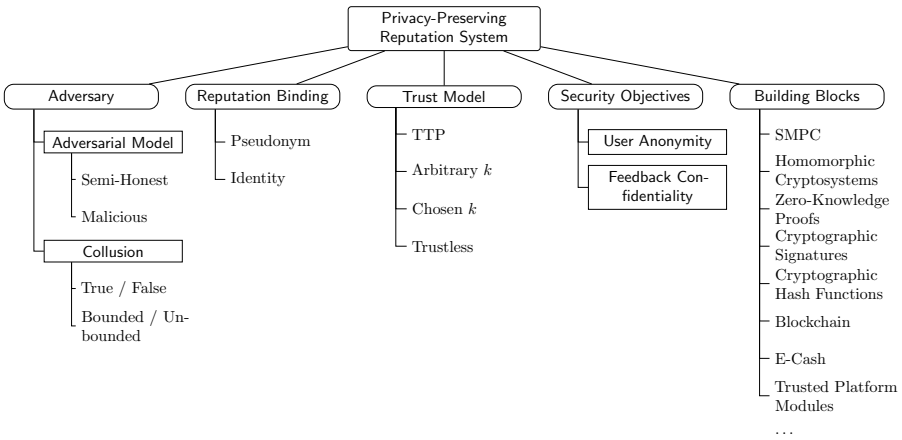

Fig. 1. Analysis framework for privacy-preserving reputation systems.

2.1 Adversary

The goal of a reputation system is to compute the reputation from the inputs of the participants. All participants of the protocol are expected to pursue this and only this goal. An honest participant is one who conforms to this expectation. However, there may exist dishonest participants who have ulterior motives. Those motives may include learning the inputs of other participants, tampering with the output, disrupting the protocol, etc.

2.1.1 Adversarial Model. We list below two standard adversarial models [37] that characterize the behavior of dishonest users. A privacy-preserving reputation system is considered secure under one of these models if it can show correctness and meet its privacy requirements under the given model.

Semi-Honest. In the semi-honest model, the users do not deviate from the specified protocol. In other words, they always execute the protocol according to the specifications. However, the adversary passively attempts to learn the inputs of honest users by using intermediate information received during the protocol execution and any other information that it can gain through legitimate means.

Malicious. Malicious users are not bound to conform to the protocol. Users under a malicious model may deviate from the protocol as and when they deem necessary. They actively attempt to achieve their objectives. A malicious adversary may have either or both of the following objectives: 1) learn the inputs of honest users, and 2) disrupt the protocol for honest users. The reasons for disrupting the protocol may range from gaining illegitimate advantage over honest users to completely denying the service of the protocol to honest users.

2.1.2 Collusion. A dishonest user may act alone or multiple dishonest users may act in agreement to achieve their ulterior motives. The collaboration of multiple dishonest users is referred to as collusion. Privacy-preserving reputation systems either consider that collusion can take place between users or consider that collusion does not take place.

Collusion can be bounded or unbounded. Bounded collusion implies that the number of dishonest colluding participants is limited, for example, by $\frac{1}{2}$ or $\frac{1}{3}$ of all n participants. Unbounded collusion places no limit on the number of dishonest participants who can collude with each other, thus $n-1$ of the participants can be dishonest and collude, except for the one honest participant whose privacy needs to be preserved.

2.2 Reputation Binding

A privacy-preserving reputation system can be either pseudonym-bound or identity-bound.

In a pseudonym-bound system, the reputation of the ratee is associated with her pseudonym. If she changes or creates a new pseudonym, then she looses her reputation. The use of pseudonyms has the drawback that the reputation is not transferable between a ratee's multiple pseudonyms. An additional major drawback is that a dishonest ratee can drop a pseudonym with bad reputation and re-enter the system with a new pseudonym and a fresh reputation. This common attack against pseudonym-bound systems is known as whitewashing.

On the other hand, in an identity-bound system, the reputation of a ratee is bound to her real identity. Even if she changes pseudonyms, she maintains her reputation. This is often made possible by verifying the true identity of a ratee before issuing a new pseudonym.

2.3 Trust Model

The security and privacy guarantees that users receive in a privacy-preserving reputation system often require that they trust certain entities, such as a central authority, or some fellow users in the system. The trust implies a belief by the trusting user that the trusted entity or the trusted fellow users will behave in an expected manner in order to ensure their security and privacy. We identify four different types of trust models that privacy-preserving reputation systems are based on.

Trusted Third Party. A Trusted Third Party (TTP) for a set of users is an entity whom every user in the set trusts completely for certain actions. In this model, all users of the system must trust the designated TTP entities in the system. A user in a system who needs to be fully trusted is also considered as a TTP.

Trust on arbitrary k fellow users. A user in the system is required to place her trust in k different fellow users for the security guarantees, where $k \leq n$, and n is the total number of users participating in the protocol. These k users are selected by the system without taking the user's preferences

into account. Thus from the perspective of the user, the set of trusted users is selected arbitrarily. Generally, only a partial level of trust is required in each of the trusted users in this model.

Trust on chosen k fellow users. In this trust model, a user in the system also places her trust in k distinct fellow users. However, these fellow users are chosen by the user herself. The user may select the trusted users based on the level of their subjective trustworthiness in order to maximize the privacy guarantee. This model requires that a user is able to determine the trustworthiness of fellow users and choose accordingly from a pool of available users.

Note that there is a difference between choosing fellow users for establishing security guarantees versus choosing feedback providers for personalizing the reputation score of the target entity. In the first case, a user chooses fellow users who specifically influence the security and privacy guarantees that she would receive in the reputation system. In the latter case, there is no impact intended on the security guarantees. The "Trust on chosen k fellow users" model addresses choosing k users specifically for the purposes of security in the reputation system.

As an example, consider the systems by Hasan et al. [44] and Gudes et al. [39]. In the system by Hasan et al., the selection of k fellow users is made for preserving privacy. The trust model of this system can thus be classified under the chosen k users category. In contrast, in the system by Gudes et al., even though a user selects a subset of fellow users, the system's trust model cannot be classified as the chosen k users model. The reason being that the selection of users in this latter system is made purely for personalizing the reputation score.

Trustless. In the trustless model, the users in a system do not need to trust any entities or any fellow users. Thus, this model does not expect users to have pre-existing trust toward fellow users or entities in the system. The users need to rely solely on the underlying algorithms and protocols of the system in order to receive the security guarantees.

However, we note that even though the users do not need to directly trust any entities or users in this model, there may exist a requirement of trustworthiness for the overall correct and secure working of the system. Trustless systems are based primarily on the blockchain technology. As an example, the Bitcoin blockchain requires that a majority of all participants in the system act honestly in order to ensure integrity.

The trustless model may be considered a special case of the "Trust on arbitrary k fellow users" model, where k is at least greater than half of the total number of all participants in the entire system (not just a protocol instance). A blockchain system functions by building consensus among peers. In the case of Bitcoin, if a majority of peers are dishonest, consensus cannot be achieved and the entire system malfunctions. Thus, the breach of the trustworthiness requirement in such systems does not simply threaten the security of a given user but the integrity of the entire system. It is therefore in the collective interest of all honest users in the system to prevent any breach of trustworthiness.

2.4 Building Blocks: Blockchain

In order to achieve their security objectives, privacy-preserving reputation systems utilize various building blocks, which are generally cryptographic in nature. These building blocks include secure multi-party computation, homomorphic cryptosystems, zero-knowledge proofs, blockchain, etc. In this section, we present an overview of blockchain, which has been utilized as a building block by recent privacy-preserving reputation systems. The description of the more traditional cryptographic building blocks can be found in cryptography texts as well as in the extended version of this survey [43] released as a research report.

A blockchain is a distributed data structure that was introduced as the foundation of the Bitcoin cryptocurrency. A blockchain can be considered a public distributed ledger that is composed of a set of blocks linked by cryptographic hashes. The blocks are chronologically ordered. Each block comprises of the record of a set of transactions or operations that have recently taken place between the users. Through an implicit consensus mechanism, all users eventually agree on the state of the public distributed ledger. A new block is proposed for being appended to the blockchain by competing users. The user who wins the right to append the new block by first solving a cryptographic puzzle receives an award in order to incentivize the continuity of the blockchain. This Proof of Work (PoW) mechanism is specific to Bitcoin. However, several other consensus mechanisms have been proposed as well. Examples include Proof of Stake (PoS) used by Ethereum, and Proof of Authority (PoA) used by VeChain. The new block and the user's right to append it are verified by the peers. Only correctly formed blocks are accepted, thus guaranteeing the security of the blockchain.

A blockchain has some important advantages. It stores an immutable record of information, which means that the information once recorded is not modifiable and its integrity and persistence are guaranteed. Additionally, it provides transparency since all information is public and each block of information is appended in an auditable manner. Moreover, it is decentralized since there is no trusted third party or any super nodes involved in its maintenance. Every node in the network is able to verify the integrity of the blockchain as well as compete toward earning the right to append a new block. This decentralization also leads to the property called trustlessness, which enables users to cooperate and collaborate without having to trust each other.

Certain systems, such as Ethereum, build on the principles of blockchain to implement the smart contract technology. A smart contract is a set of programmed rules that are agreed upon by a group of users in advance. The correct execution of the program and the enforcement of the rules is then guaranteed by all nodes in the system who are maintaining the blockchain. Smart contracts allow users who do not have any pre-existing trust in each other to be able to conduct transactions with guaranteed compliance to the mutually agreed upon set of rules. They can rely on the underlying blockchain system to prevent deceitful behavior from any of the parties.

Privacy-preserving reputation systems can benefit from blockchains in multiple ways. A blockchain can be used for its immutability, transparency, and auditability properties to create a reputation system that enables users to verify the integrity of the computation of the reputation scores. The decentralized system by Schiedermeier et al. [80] is an example of such utilization of blockchain. Moreover, a privacy-preserving reputation system can use smart contracts to transparently enforce the rules for updating the reputation of a user. This is the case in the reputation framework for participatory sensing systems by Jo and Choi [52], where a smart contract manages the reputation of a participant user based on their sensing data and the corresponding feedback.

3 SECURITY OBJECTIVES OF PRIVACY-PRESERVING REPUTATION SYSTEMS

We have identified two broad categories of privacy-preserving reputation systems with respect to their security objectives. The goal of the systems in the first category is to preserve the anonymity of the users. The systems in the second category do not aim to hide the identity of the users but focus on preserving the confidentiality of the feedback that the users provide. The two categories of privacy-preserving reputation systems are defined as follows:

(1) **User anonymity-oriented privacy-preserving reputation systems.** The true identity of the users is hidden in these systems. The feedback providers thus remain anonymous. A user is represented in the system by one or more pseudonyms which are unlinkable to her real identity.

This setup allows the user to anonymously carry out transactions with others and submit feedback. The submitted feedback does not need to be confidential since the anonymity of the users prevents the feedback from being linked to them.

(2) **Feedback confidentiality-oriented privacy-preserving reputation systems.** These systems do not attempt to hide the identity of the users beyond assigning each user a single pseudonym. Moreover, these systems do not conceal the act of a user assigning feedback to another user. However, the value of the submitted feedback and any other related information are considered private. This type of systems is necessary since complete anonymity is not always possible due to the nature of real world transactions. For example, even if anonymity is preserved online on an e-commerce site, the exchange of physical items sold and bought through the site would reveal the real identities of the participants. Preserving the confidentiality of the feedback is a practical alternative to enable users to submit truthful feedback without fear of retaliation.

The security objectives of a privacy-preserving reputation system can be further categorized as those fulfilling privacy and those fulfilling integrity or correctness. The privacy objectives are related to hiding information about users, for example, preserving the anonymity of the rater and the ratee. On the other hand, the integrity objectives aim at maintaining the correctness of the functions of the reputation system while preserving the privacy of the users. An example of integrity objectives is preventing a malicious user from manipulating the reputation aggregation function to forge an unmerited good reputation.

Figure 2 graphically represents the classification of the security objectives of privacy-preserving reputation systems. In Sections 3.1 and 3.2, we describe specific security objectives of user anonymity and feedback confidentiality-oriented privacy-preserving reputation systems, respectively. A given reputation system may pursue a few or more of these objectives depending on the stringency of its security requirements.

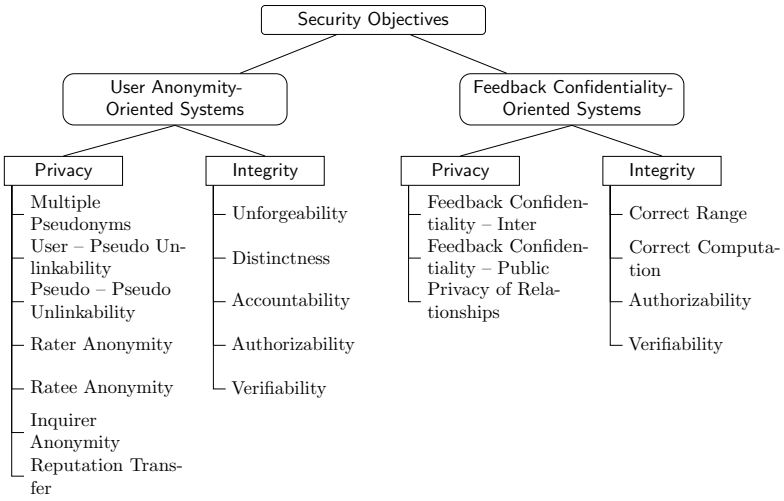

Fig. 2. Security objectives of privacy-preserving reputation systems.

3.1 User Anonymity-Oriented Privacy-Preserving Reputation Systems

3.1.1 Privacy Objectives.

Multiple Pseudonyms. A user is able to assume multiple pseudonyms in the system. As noted by Anwar and Greer [5, 6], the variation in the pseudonyms of a user may be on a per context or a per transaction basis. In the first case, a user may adopt a different pseudonym for each context in the system. For example, a tutor could use different pseudonyms for different subjects in an e-learning system. Alternatively, a user may choose a different pseudonym for each transaction in the system.

User-Pseudonym Unlinkability. User-pseudonym unlinkability implies that the true identity of a user is not linkable to any pseudonym that she uses in the system. Androulaki et al. [4] characterize this requirement as follows: Given a pseudonym P that does not belong to a corrupted party, the adversary can learn which peer owns P no better than guessing at random among all non-corrupted peers that appear consistent with P.

Pseudonym-Pseudonym Unlinkability. Pseudonym-pseudonym unlinkability implies that two different pseudonyms that belong to the same user cannot be linked to each other. The adversary is unable to tell whether two given pseudonyms belong to the same user. Androulaki et al. [4] specify this property as follows: Given two pseudonyms P_1, P_2 that do not belong to corrupted parties, the adversary has no advantage in telling whether P_1, P_2 belong to the same peer or not. This requirement should hold as long as there are at least two non-corrupted peers who appear consistent with both P_1 and P_2 (because if there is only one such uncorrupted peer, clearly both pseudonyms belong to the same one).

Rater Anonymity. A user is able to rate another user without her true identity being revealed. The purpose of rating anonymously is to prevent the adversary from linking the rater to her interaction with the ratee and the rating that she submitted. Schiffner et al. [81] specify this property as follows: A pseudonym P_1 that interacted with a ratee R should not be linkable to the pseudonym P_2 that rated R.

Ratee Anonymity. A user is able to receive a rating without her real identity being disclosed. A ratee may not wish to be associated with her past transactions and ratings since they could influence the ratings for her future transactions. According to Schiffner et al. [81], this property implies that a ratee R can use a different pseudonym for each transaction.

Inquirer Anonymity. A user is able to inquire about the reputation of another user. However, others are not able to learn whose reputation she is querying or even the fact that she is inquiring about another user's reputation. Users wish to query the reputation of other users anonymously in order to prevent the adversary from compiling a profile of their interactions and interests.

Reputation Transfer and Aggregation. A ratee is able to transfer reputation among multiple pseudonyms that she owns without letting the adversary infer associations between these pseudonyms. Consequently, a ratee is able to aggregate the reputation of her multiple pseudonyms into the reputation of one pseudonym.

3.1.2 Integrity Objectives.

Reputation Unforgeability. A ratee is unable to show reputation higher than the cumulative reputation of her pseudonyms. A ratee is also unable to borrow good reputation from another ratee.

Distinctness. It is possible to prove that the reputation of a ratee is an aggregate of votes or feedback from distinct raters while simultaneously hiding the identities of those raters. The advantage of this property is that one or a few dishonest raters are not able to submit multiple votes or feedback (ballot stuffing) for artificially increasing or decreasing the reputation of the ratee.

Accountability. If and only if a user commits a predefined adversarial act, such as ballot stuffing, then her pseudonym becomes linkable to her real identity. This property ensures that anonymous users are still accountable for adversarial actions.

The properties of authorizability and verifiability are discussed in Section 3.3.

3.2 Feedback Confidentiality-Oriented Privacy-Preserving Reputation Systems

3.2.1 Privacy Objectives.

No Inference from Intermediate Information. This property requires that a rating assigned by a rater to a ratee is never revealed to any other party including the ratee. The system must protect the confidentiality of the feedback such that the feedback is neither divulged explicitly nor inferred from any intermediate information gained by the adversary during a reputation query. The system may define the confidentiality of the feedback as deterministic or probabilistic. In the first case, the adversary is unable to learn any information about the feedback. However, in the latter case of probabilistic confidentiality, the amount of information leakage depends on certain variables, such as the number of raters, the reputation score, etc.

No Inference from Public Information. The reputation score of any ratee is by definition public and any other user in the system is authorized to learn this score. The issue is that a dishonest user may use this public information to derive the private feedback of honest raters. For example, in a basic additive reputation system, the adversary simply needs to observe the reputation score before and after the latest rater submits her feedback to learn its value. The requirement of confidentiality of feedback, with no inference from public information, implies that the adversary is unable to learn information about the feedback even from publicly available information.

Privacy of Relationships. A user may have relationships with multiple users in the system. These other users may include fellow users who have rated the same ratees. The relationships between the users could be in various contexts, for example, the context of trust in preserving each others privacy. This requirement implies that information about the relationships of a rater is not revealed during the course of a reputation query. This information includes the amount of trust that the rater has in the fellow users.

3.2.2 Integrity Objectives.

No Out of Range Feedback. A dishonest rater is unable to submit out of range feedback. A dishonest rater may take advantage of the fact that the feedback is confidential and submit out of range feedback in order to mount an attack such as bad mouthing or ballot stuffing. A system enforcing this property does not permit out of range feedback even though the feedback is hidden.

No Incorrect Computations. A dishonest user is unable to carry out incorrect computations. A reputation query may require users to perform certain computations, for example, the summation of some values. This property requires that a dishonest user is unable to submit erroneous results for these computations.

3.3 Integrity Objectives Common to Both Types of Privacy-Preserving Reputation Systems

Authorizability of Ratings. The requirement of authorizability of ratings implies that only the users who have had a transaction with the ratee are allowed to rate her. This property prevents users who have not transacted with a ratee from assigning her feedback and thus possibly reduces the impact of attacks such as bad mouthing and self promotion.

Verifiability by Ratee. The requirement of verifiability by ratee, as identified by Kerschbaum [57], suggests that a ratee R should be able to identify all published feedback linked to her identity and verify that they are related to a recorded transaction and the correct transaction partners. Moreover, a ratee R should be able to identify all published feedback linked to her identity and verify that the inquirer has computed its reputation score according to them.

4 AN ANALYSIS FRAMEWORK FOR REPUTATION SYSTEMS

In this section, we develop an analysis framework that identifies the various non-privacy related dimensions of reputation systems. Since privacy-preserving reputation systems are fundamentally reputation systems, we need to establish a uniform framework to analyze and compare their non-privacy features as well. However, we do not describe these dimensions in detail in this paper since they have been covered extensively by prior works (such as the surveys by Braga et al. [17], Hendrikx et al. [45] and Hoffman et al. [47]). Additionally, the details of these properties can be found in the extended version of this survey [43] released as a research report.

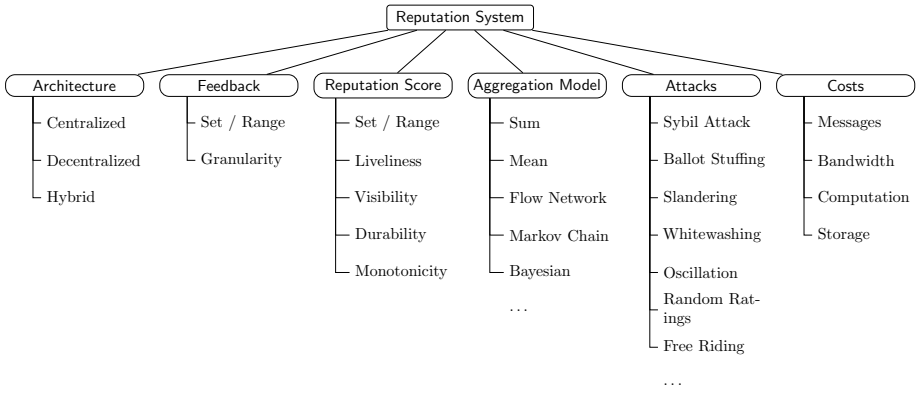

Fig. 3. Analysis framework for reputation systems.

The architecture of a reputation system is one of the key factors in determining how the following activities are conducted: 1) Feedback collection; 2) Feedback aggregation (reputation computation); and 3) Reputation dissemination. The architecture of a reputation system can be centralized, decentralized, or hybrid.

The properties of feedback include the *set or range* that the feedback belongs to, for example, $\{-1, 0, 1\}$, $[0, 1]$. Additionally, the *granularity* of the feedback of a rater reflects either the experience with the ratee for a single given transaction or the cumulative experience over multiple transactions.

The properties of reputation include the set or range of its values, for example, $\mathbb{R}$, $[0, 1]$. Some other properties of reputation are liveliness, visibility, durability, and monotonicity. As noted by Schiffner et al. [81], reputation *liveliness* implies that a reputation system does not offer users the possibility to reach a final state of reputation in which bad behavior no longer damages their reputation. For example, for a reputation score in the set $\mathbb{R}$, there are no minimum and maximum limits, whereas, for a reputation score in the interval $[0, 1]$, the reputation can reach the mininum value of 0 or the maximum value of 1. The *visibility* of a reputation score may be global or local. Global visibility implies that all nodes in the system view the same reputation score of a certain entity. Whereas with local visibility, the reputation score available to a subset of the nodes may be different than elsewhere in the system. Reputation *durability* refers to the transience of a reputation score. Once a reputation score is computed, it may be stored permanently until the reputation changes or may remain transient and require re-computation for every query. *Monotonic* reputation implies that the reputation score increments in only one direction. For example, consider a reputation system in which a ratee can receive integer feedback between 1 and 5 for each transaction, and reputation is considered as the sum of feedback. The reputation in such a system cannot be decremented.

There are a number of models for aggregating feedback to obtain reputation scores. Some common models include sum, mean, flow network, Markov chain, and Bayesian ones. A comprehensive survey of feedback aggregation models (also referred to as reputation computation engines) is provided by Jøsang et al. [53].

Reputation systems can be classified by the attacks that they address and their success in defending against them. Some of the attacks that reputation systems have to contend with include Sybil attack (a single user owning and exploiting multiple identities for malicious purposes), self-promotion or ballot stuffing (improving a ratee's reputation by providing false positive feedback), slandering or bad-mouthing (damaging a ratee's reputation by providing false negative feedback), whitewashing (leaving the system and then re-entering with a fresh reputation), oscillation (cultivating good reputation with the intention to exploit it for malicious purposes), random ratings (submitting randomly generated feedback in order to demonstrate active participation), and free riding (benefiting from the reputation system without providing any contribution). Surveys by Hoffman et al. [47] and Mármol and Pérez [65] describe some of these attacks in detail.

The operations of a reputation system, which include feedback collection, feedback aggregation (reputation computation), and reputation dissemination, incur various computational costs. The costs of these operations can be measured as follows: 1) number of messages exchanged; 2) bandwidth consumed; 3) computational resources consumed; and 4) storage required.

5 CATEGORIZATION OF PRIVACY-PRESERVING REPUTATION SYSTEMS ACCORDING TO THEIR SECURITY MECHANISMS

In this section, we identify broad categories of the privacy-preserving reputation systems proposed in the literature. These categories are based on the general mechanisms that these systems rely on in order to guarantee privacy and other critical security properties, for example, authorizability, verifiability, etc.

We also briefly discuss the contributions of the systems that belong to each of these categories. Each system is further analyzed in depth and compared in Section 6. Five of the listed blockchain-based systems are discussed in detail in Section 7.

Note that these categories are not mutually exclusive and a system may belong to multiple of these categories. For example, the system by Schiedermeier et al. [80] can belong to the category of blockchain-based systems as well as SMPC-based systems. However, we place a system under a single category based on its main novel idea. For example, even though Schiedermeier et al.'s work uses SMPC, the novel idea and the main contribution is rather the use of a blockchain-based public ledger as the sole communication medium between the parties of the SMPC protocol. The blockchain-based protocol provides transparency and verifiability properties that are usually missing from SMPC-only systems. The system by Schiedermeier et al. is therefore categorized as a blockchain-based system.

Article Selection Methodology: In this survey, we have included the systems that we are aware of in this area of research as well as those discovered using the following approach. We searched for articles on Google Scholar published during the period of 2000 to July 2021. The search phrases included the keyword 'reputation' along with one of the keywords 'privacy', 'anonymous', and 'anonymity'. For each relevant article found, we studied its list of references to find other potential systems. Moreover, we also looked at the article's "Cited by ..." list on Google Scholar to discover later relevant papers that cite the given article. All articles that present privacy-preserving reputation systems that we discovered have been included in this survey. We have excluded some articles that present systems similar to those that have been included, for example, articles by the same authors that describe predecessors of their subsequent

systems. We have also excluded short papers (4 pages or less) that do not describe the proposed systems in sufficient detail.

5.1 Blockchain-based Systems

These systems rely on a blockchain or smart contracts as an integral building block for achieving their security objectives. This is one of two categories (the other one being SMPC-based systems, described in the next subsection) that constitute mainly of decentralized systems. Moreover, this is the only category that comprises of systems that can guarantee trustlessness.

Schaub et al. [79] introduced the first blockchain-based trustless privacy-preserving reputation system. The system does not need to rely on trusted third parties, arbitrary trusted nodes, or subjective trust relationships in order to guarantee security. Using blinded tokens issued by service providers, raters anonymously submit feedback, which is recorded on a public immutable blockchain. Issuing a token requires spending the system's cryptocurrency, which provides an incentive to mine and maintain the blockchain and also discourages ballot-stuffing. Bazin et al. [13] present a system, which in addition to protecting rater privacy, enables retrieval of a self-reported reputation score directly from the target service provider. The validity of the reputation score is verifiable and only a constant number of messages need to be exchanged for its retrieval.

Azad et al. [8, 9] propose privacy-preserving reputation systems for online marketplaces and for the Social Internet of Things environment. Self-enforcing computation is a property of their latter system, which implies that the computation process is independent of any trusted third party and it allows verification of the integrity of the scores in an autonomous and public manner. Bag et al. [11] describe a system for computing personalized global reputation of a target, which considers only the feedback from a set of trusted participants. This is done without disclosing the identities of the members of the trusted set and their feedback. The systems by Azad et al. and Bag et al. rely on a public bulletin board for communication, which according to the authors may be realized by a blockchain.

Dou et al. [34] propose a distributed trust evaluation protocol with privacy protection for the Intercloud environment. A distinctive feature of the protocol is that it can continue to function even if some of the feedback providers go offline. Kang et al. [55] devise a blockchain-based scheme for secure data sharing among vehicles in Vehicular Edge COmputing and Networks (VECONs). A reputation system based on a three-weight subjective logic model is employed to manage the trustworthiness of vehicles in terms of the quality of data shared. The anonymity of the vehicles is maintained by allowing multiple pseudonyms. Lu et al. [62] present a privacy-preserving trust model based on blockchain for vehicular adhoc networks. Vehicles can anonymously submit alerts about traffic conditions and neighboring vehicles can provide feedback about the validity of the alerts. The anonymous reputation of a vehicle reflects the feedback received regarding its contributions. Owiyo et al. [74] propose a decentralized privacy-preserving reputation system based on blockchain that is claimed to provide low transaction overheads.

Jo and Choi [52] describe a blockchain-based privacy-preserving reputation framework for participatory sensing systems. The system includes a smart contract that manages the reputation of participants based on their sensing data and the corresponding feedback. The smart contract and the underlying blockchain enable transparency and public auditability of the reputation scores. Liu et al. [61] present an anonymous reputation system for retail marketing in the Industrial Internet of Things environment. The system, which also uses smart contracts on a Proof of Stake blockchain as a building block, is able to provide transparency and public verifiability under the malicious adversarial model. Schiedermeier et al. [80] describe a protocol for holding referendums in trustless networks, which can also serve as a reputation protocol. The protocol combines SMPC with a blockchain as the unique channel for communication

between the parties. The protocol ensures transparency, that is, maintaining a public trace of all operations performed and the information exchanged among the participants. Moreover, any participant is able to autonomously verify the correctness of the outcome of the referendum.

Zhao et al. [97] propose a privacy-preserving reputation system that takes advantage of blockchain technology in the resource-constrained environment of mobile crowdsensing. The global reputation scores are updated by a smart contract based on the average of all feedback. The system overcomes the challenge of user dynamics, that is, frequent user turnover, by including a delegation protocol. Zhang et al. [95] present another privacy-preserving reputation management scheme for mobile crowdsensing that is based on blockchain. The well-known Eigentrust distributed reputation computing algorithm is adapted in this system such that participant privacy is preserved. Dimitriou [28] develops a blockchain-based fully decentralized privacy-preserving reputation system. The participants can change pseudonyms as frequently as they wish, yet they can maintain user-pseudonym and pseudonym-pseudonym unlinkability, while being able to aggregate reputation among those pseudonyms. The system provides fully trustless operations, except for the user registration operation that relies on the trustworthiness of an entity called the Registrar, which may be composed of a single server or a decentralized set of nodes. However, the Registrar is trusted only for ensuring uniqueness of user identities and for reputation soundness.

5.2 SMPC-based Systems

These systems use feedback score as direct evidence from witnesses to compute a reputation score. Their goal is to obfuscate the feedback score of the witnesses from the querier as well as from fellow witnesses. These systems use Secure Multi-Party Computation to achieve their goal. The reputation systems in this category focus primarily on feedback confidentiality as their security objective. Decentralization is one of the key advantages of SMPC-based systems over systems in the categories discussed next that are mostly centralized.

Pavlov et al. [75] introduced SMPC-based privacy-preserving reputation systems by proposing a number of protocols for decentralized additive reputation systems. Two of their protocols are secure under the semi-honest and the malicious adversarial models, respectively. The protocols draw their strength from witness selection schemes, which guarantee the inclusion of a certain number of honest witnesses as participants. Gudes et al. [39] and Gal-Oz et al. [35] present several schemes that augment their Knots reputation system [36] with privacy-preserving features. A defining characteristic of the Knots reputation model is the notion of subjective reputation. The reputation of a target member is computed by each querying member using a different set of feedback, thus the reputation is subjective for each querying member. Nithyanand and Raman's system [73] complements an SMPC mechanism for privacy with a fuzzy technique and an Ordered Weighted Average (OWA) operator in order to compute local as well as global reputation scores.

Hasan et al. [44] present a system that operates under the more demanding malicious adversarial model and offers the chosen k trust model (discussed in Section 2.3) instead of the usual arbitrary k trust model for privacy preservation. Dimitriou and Michalas [29, 30] describe a decentralized privacy-preserving scheme that is formally shown to be resistant to collusion against up to $n-1$ malicious participants. Dolev et al. [32, 33] propose SMPC-based reputation schemes that are more efficient than the previous ones in terms of the number of messages exchanged. Their schemes privately compute reputation scores with a communication overhead of $O(n)$ messages, where n is the number of participants in the protocol. Clark et al. [25] present a dynamic privacy-preserving decentralized reputation system. They specifically address the problem of the dynamicity of the nodes in a network. Nodes may frequently leave along with their feedback, which then becomes unavailable for reputation computation in a decentralized manner.

Clark et al. propose a privacy-preserving reputation information delegation protocol to counter this problem. Bakas et al. [12] propose an SMPC-based privacy-preserving decentralized additive reputation system, which is the first one to practically utilize Functional Encryption (FE), an emerging cryptographic building block that permits selective computations on encrypted data.

5.3 Token-based Systems

These systems are a type of privacy-preserving reputation systems in which a cryptographic token is issued to a pseudonymous user participating in a transaction. The token is implemented using a blind signature or another scheme. The token is issued either by a central entity (called the bank in the system by Androulaki et al. [4]) or directly by the ratee to the rater (as in the system by Kerschbaum [57]). A variation of the following approach is then employed in order to credit the ratee with a reputation point while preserving the privacy of the token depositing user. The token is deposited by the user to an account maintained by the central entity using a different pseudonym or even their real identity. The blinded nature of the token unlinks the user from the initial pseudonym while assuring the central entity of the legitimacy of the deposit. The number and the value of the tokens deposited reflect the reputation of the ratee. An advantage of user anonymity-oriented token-based systems over SMPC-based systems is the ability of users to assume multiple pseudonyms.

The system by Androulaki et al. [4] addresses the difficulties outlined by Dingledine et al. [31] for building reputation systems in anonymous user networks. Androulaki et al.'s system achieves: 1) unlinkability between a pseudonym and the identity of its user; 2) no double-awarding or forging of a token; 3) no false accusations of forgery; and 4) non-transferability of reputation, that is, a user cannot borrow reputation from another user. The system by Kerschbaum [57] builds on the blinded token idea to achieve feedback confidentiality while enforcing the property of verifiability. Schiffner et al. [81, 82] improve upon Androulaki et al.'s work by introducing systems that support the properties of liveliness and non-monotonicity.

Zhang et al. [93] propose a reputation system that preserves the privacy of feedback providers and resists Sybil attacks. The system is based on the Camenisch and Lysyanskaya (CL) signature scheme. Busom et al. [19] describe a privacy-preserving reputation system based on Chaum-Pedersen blind signatures that allows users to anonymously submit text feedback about a target entity. Fellow users can in turn anonymously endorse a text feedback that they find helpful. The system thus encourages honest feedback. Moreover, the system offers a privileged status for users who earn sufficient endorsements thus also incentivizing feedback submission.

5.4 Proxy-based Systems

These systems aim to maintain privacy through the use of a trusted third party as a proxy between the raters and the reputation querier. The proxy may forward the anonymized feedback scores to the querier or the proxy may compute the aggregated reputation and only report that to the querier. Additionally, the querier and the raters may interact directly. However, in this case, a rater is generally issued an anonymous identity or an encryption key by the proxy to protect their privacy. The proxy may be composed of one or several central entities. Usually, the architecture of these systems comprises of one to three central entities that are considered not to collude with each other in order to guarantee security. The proxy may be considered partially or fully trusted.

Ries et al. [78] propose an approach for privacy-preserving computation of trust. A key contribution of this approach is that in addition to computing reputation based on encrypted private feedback, the querier can also evaluate the trustworthiness of the raters. Petrlic et al. [76] propose a reputation management

system that focuses on privacy (anonymity in reputation retrieval, and anonymity in rating) as well as robustness (authorization, authentication, integrity, and accuracy). A semi-honest Reputation Provider (RP) entity serves as an intermediary between the raters and the service providers. The RP manages the reputation of the service providers and helps enforce some of the above listed security objectives.

Mousa et al. [71] present PrivaSense, a privacy-preserving reputation system for mobile participatory sensing applications. The system implements a sequence of registration and authentication phases orchestrated by independent central servers that ensure participants' anonymity and improve the system's resilience against Sybil and replay attacks. Ma et al. [63] propose a privacy-preserving reputation management system for edge computing enhanced mobile crowdsensing. The architecture comprises of a Central Manager (CM), a Reputation Manager (RM), and a Central Authority (CA). Participants submit sensing data in homomorphic encrypted form. The encrypted deviation of a participant's data from the aggregated result is computed and the RM updates reputation according to the deviation.

5.5 Signature-based Systems

Inspired by cryptographic digital signatures and group signature schemes, Benthencourt et al. [15] propose a new cryptographic framework called signatures of reputation. In a scheme based on this framework, the verification of the signature of a user reveals her reputation instead of revealing her identity. This is in contrast to a conventional signature scheme where the verification of the signature of a user results in the confirmation of the identity of the user associated with the corresponding public key.

Guo et al. [40] build upon the notion of signatures of reputation to propose a fine-grained attribute-based privacy-preserving reputation system. The system enables users to rate each other's attributes instead of real identities. The signature verification process provides authenticity of the reputation value of a user for a given attribute. Bethencourt et al.'s system is improved by the work of Anceaume et al. [3] and Lajoie-Mazenc et al. [60], who implement non-monotonic signature-based reputation systems. Whereas, Bethencourt et al.'s system only supports monotonic reputation.

Chen et al. [23] present a privacy and reputation-aware announcement scheme for vehicular adhoc networks where vehicles can report road conditions. The scheme is based on the Boneh-Boyen-Shacham (BBS) short group signatures. The scheme overcomes the problem of having to establish a secure channel for reputation score retrieval in prior systems.

5.6 Transitory Pseudonym-based Systems

Transitory pseudonym-based systems aim to obfuscate a user's identity by assigning them multiple short-term pseudonyms. The focus is on how to make the multiple pseudonyms of a user unlinkable with the user as well as with one another. Moreover, how to transfer reputation from one pseudonym to another while preventing observation and profiling is also addressed.

One of the first systems in this category is RuP (Reputation using Pseudonyms) by Miranda and Rodrigues [70]. In their system, a user is identified by a certified pseudonym that is valid only for a predefined time slot. The certified pseudonyms are issued by a TTP called Pseudonym Certification Authority (PCA). However, the link between the real identity of the user and the pseudonym is hidden from the PCA as well. The system also includes a scheme based on blind signatures that allows a user to transfer their reputation associated with an old pseudonym to a new one, without disclosing the link between them or their real identity. Another early work in this category is by Steinbrecher [84]. Their system enables simultaneous use of multiple pseudonyms by a user and permits them to regularly change their pseudonyms to achieve anonymity. To prevent an adversary from linking new and old pseudonyms,

the system suggests using a set of non-colluding trustworthy third parties who make incremental changes to the pseudonym of the user.

Anceaume et al. [2] propose a privacy-preserving distributed reputation mechanism. The system allows users to themselves generate pseudonyms in order to achieve anonymity. They introduce the concept of mailboxes, which are agents that replicate anonymous feedback, in order to provide resistance against network dynamicity and user misbehavior. Christin et al. [24] present IncogniSense, another improvement on the RuP scheme, which is claimed to achieve better protection against reputation manipulation and reduce the cryptographic overhead for the client.

5.7 Other Systems

In this category, we include systems that propose unique approaches and therefore cannot be placed in the above defined categories.

Kinateder and Pearson [58] introduced one of the earliest privacy-oriented decentralized reputation systems. The system requires a Trusted Platform Module (TPM) chip at each agent, which enables an agent to demonstrate that it is a valid agent and a legitimate member of the system without disclosing its true identity. This permits the agent to provide feedback anonymously. Bo et al. [16] present a privacy-preserving reputation system, which offers incentives to users for feedback submission. A user who anonymously submits feedback can also anonymously receive a discount token (an incentive) from the ratee. The architecture of the system comprises of a Card Issuer (CI) entity and a Registration Center (RC) entity that are responsible for issuing smart cards and anonymous identities to users, respectively.

6 FINE-GRAINED ANALYSIS AND COMPARISON OF PRIVACY-PRESERVING REPUTATION SYSTEMS

In this section, we conduct fine-grained analysis of privacy-preserving reputation systems in the literature according to the frameworks established in Sections 2 through 4. The analysis is presented in the form of Tables 1 through 6. The tables also permit side by side comparison of the systems.

We have analyzed 44 privacy-preserving reputation systems in depth and summarized their properties in the given tables. We report information about the systems as gleaned from the articles. In case of multiple variants of a system presented in the same article, we have selected the variant that provides the strongest security guarantees. The systems are grouped in the tables according to the category of their security mechanisms. The categories are ordered by the number of included systems and then alphabetically. Under each category, the systems are ordered chronologically to allow observation of the evolution of the systems.

Table 1 identifies the fundamental characteristics of each reputation system according to the analysis framework developed in Section 4. The architecture of the systems and the properties of their feedback and reputation are presented.

Table 2 and Table 3 present the security related fundamentals of user anonymity and feedback confidentiality-oriented systems, respectively. In accordance with the analysis framework for privacy-preserving reputation systems formulated in Section 2, the properties reported include the adversarial model, the extent of collusion resistance, reputation binding, the trust model, and the main security building blocks. Multiple adversarial models are listed if a scheme uses different adversarial models for different entities, for example, semi-honest for the server, and malicious for the users. We note strong collusion resistance if t out of the n users in the protocol must collude to breach security, where $t < n$, and t is variable. For example, $t = \frac{1}{2}n$, or $t = \frac{1}{3}n$. Alternatively, we note partial collusion resistance if a constant number of colluding entities, for example, two partially trusted colluding servers, are able to

breach security. Multiple trust models are noted for the systems that rely on different models for their different security properties. The aggregation model is stated as open where the system is not constrained to one specific function.

The details of the security objectives of user anonymity and feedback confidentiality-oriented systems are presented in Table 4 and Table 5, respectively. As discussed in Section 3, the security objectives of privacy-preserving reputation systems include those aiming to enforce privacy and those targeting integrity or correctness.

The robustness of the reputation systems against common attacks listed in Section 4 is summarized in Table 6.

7 BLOCKCHAIN-BASED PRIVACY-PRESERVING REPUTATION SYSTEMS

In this section, we describe in greater detail some of the blockchain-based privacy-preserving reputation systems in the literature. We focus on their security mechanisms as well as their use of blockchain. Moreover, we highlight salient features that require further explanation or those that are not evident from the analysis in Section 6.

7.1 Schaub et al. 2016

Schaub et al. [79] design a reputation system for real-world e-commerce applications. It is therefore assumed that a customer c's real identity will be disclosed to the service provider SP during a transaction. Instead of complete anonymity, the system emphasizes user anonymity specifically for the feedback submission stage. The system requires unlinkability of the rater to the rating, unlinkability of the rating to the transaction, and unlinkability of the rating to other ratings by the same rater. These properties ensure that c can submit a rating without identification by the SP, and thus achieve user anonymity for feedback submission.

In order to receive a rating from a customer, the service provider SP is required to spend a certain amount of coins of the native cryptocurrency of the system. This approach is advantageous in a number of ways. It discourages the ballot stuffing attack, since the SP will need to spend coins proportional to the number of artificial ratings. Moreover, the cryptocurrency allows the system to incentivize mining its blockchain by rewarding the creation of new blocks with coins. The service providers can either mine the coins themselves or they may acquire the coins on open market from other miners. The system thus ensures the continuity of the blockchain through incentivized mining, which in turn also ensures the trustlessness property of the system.

A customer c can compute the reputation of a service provider SP by aggregating the ratings about the SP available in the public blockchain of the system. The ratings are aggregation function agnostic. Therefore, any aggregation function of the customer's choosing can be used for computing the reputation. Moreover, the user can consult text reviews submitted along with the numerical ratings. If the reputation is acceptable, c generates a one time private/public key pair specifically for the transaction with SP.

After the transaction has taken place, c asks SP for a blinded token authenticating the transaction. SP can issue a token to c if SP has at least n coins available on her address on the blockchain. The n coins are necessary, since this amount will be deducted from SP upon submission of a rating by the customer. c then verifies the token and unblinds it, breaking the link between herself and the transaction. When c wishes to rate SP, she broadcasts a message containing SP's address, the unblinded token, and her rating. A miner of the blockchain who creates a new block then verifies and includes this rating in the block, which is eventually appended to the blockchain.

Table 1. Fundamentals.

		Feedback		Reputation					
System	**Architecture**	**Set / Range**	**Granularity**	**Set / Range**	**Liveliness**	**Visibility**	**Durability**	**Non-Monotonicity**	**Aggregation Model**
Blockchain-based Systems									
Schaub et al. 2016	D	$\mathbb{Z}$	S	$\mathbb{R}$	●	G	○	●	Open
Bazin et al. 2017	D	$\mathbb{Z}$	S	$\mathbb{R}$	●	G	●	●	Open
Azad et al. 2018	D	$\{-,+\}$	S	$\mathbb{Z}$	●	G	○	●	Beta reputation
Bag et al. 2018	D	$\{0,1\}$	M	$[1,10]$	○	L	○	●	Mean
Dou et al. 2018	D		S			G	●		Weighted mean
Kang et al. 2018	H	$[0,1]$, multi-criteria	M	$\mathbb{R}$	●	G	●	●	Subjective logic
Lu et al. 2018	C	$\{-1,0,1\}$, $[0,1]$	S	$\mathbb{R}$, $[0,1]$	●	G	●	●	Polynomial
Owiyo et al. 2018	D		S			G	●		Open
Jo and Choi 2019	H	$\{-1,1\}$	S	$\mathbb{R}$	○	G	○	●	Sum
Liu et al. 2019	C	$[1,10]$	S	$\mathbb{N}$	●	G	●	○	Sum
Schiedermeier et al. 2019	D	$\{-1,1\}$	S	$\mathbb{Z}$	●	G	●	●	Sum
Zhao et al. 2019	C	$[0,1]$	S	$[0,1]$	●	G	●	●	Mean
Azad et al. 2020	D	$\{-1,1\}$	S	$\mathbb{Z}$	●	G	●	●	Weighted sum
Zhang et al. 2020	D	$[0,1]$	M	$\mathbb{R}$	●	G	●	●	Weighted sum
Dimitriou 2021	D		M	$\mathbb{Z}$	●	G	●	●	Sum
SMPC-based Systems									
Pavlov et al. 2004	D	$\mathbb{R}$	M	$\mathbb{R}$, $[0,1]$	●	L	○	●	Sum, beta reputation
Gudes et al. 2009	D	$\mathbb{R}$	M	$\mathbb{R}$	●	L	○	●	Weighted sum, mean
Nithyanand and Raman 2009	D	$\mathbb{R}, \{0,1\}$	M	$\mathbb{R}$	●	L	○	●	Ordered weighted average
Gal-Oz et al. 2010	D	$\mathbb{R}$	M	$\mathbb{R}$	●	L	○	●	Weighted sum, mean
Hasan et al. 2013	D	$[0,1]$	M	$\mathbb{R}$, $[0,1]$	●	G	○	●	Sum, mean
Dimitriou and Michalas 2014	D	$\mathbb{Z}$	M	$\mathbb{Z}$	●	G	○	○	Sum
Dolev et al. 2014	D	$\{1,2,\ldots,10\}$	M	$\mathbb{R}$	●	L	○	●	Weighted mean
Clark et al. 2016	D	$[0,v_{max}]$	M	$[0,v_{max}]$	●	L	○	●	Mean
Bakas et al. 2021	D	$\{n^1,n^2,\ldots,n^k\}$	M	$\mathbb{Z}$	●	L	○	●	Sum
Token-based Systems									
Androulaki et al. 2008	C	$\{0,1\}$	S	$\mathbb{Z}$	○	G	●	○	Sum
Kerschbaum 2009	C	$\{0,1\}$	S	$[0,1]$	●	G	●	●	Beta reputation
Schiffner et al. 2009	C	$\{-1,1\}$	S	$\mathbb{Z}$	●	G	●	●	Sum
Schiffner et al. 2011	C	$\{-,+\}$	S	$\mathbb{R}$	●	G	●	●	Open
Zhang et al. 2014	H		S	$\mathbb{R}$	●	G	●	●	Open
Busom et al. 2017	C	Text	S		●	G	●	●	Union
Proxy-based Systems									
Ries et al. 2011	C	$\{0,1\}$	M	$[0,1]$	●	L	○	●	Beta reputation
Petrlic et al. 2014	C	Vector, $\{0,1\}$	S	$\mathbb{Z}$	●	G	●		Sum
Mousa et al. 2017	C	$\{-1,0,1\}$, $[0,1]$	S	$[0,1]$	●	G	●	●	Bounded sum
Ma et al. 2018	C	$[0,1]$	M	$[0,1]$	●	G	●	●	Weighted mean
Signature-based Systems									
Bethencourt et al. 2010	H	$\{0,1\}$	S	$\mathbb{Z}$	●	G	●	○	Sum
Guo et al. 2013	C	$\{-1,1\}$	S	$\mathbb{Z}$	●	G	●	●	Sum
Lajoie-Mazenc et al. 2015	H	$\{-,+\}$, $\mathbb{Z}$	S	$\mathbb{R}$	●	G	●	●	Open
Chen et al. 2016	C		S	$\{0,1,\ldots,m\}$		G	●		Time discount function
Transitory Pseudonym-based Systems									
Miranda and Rodrigues 2006	C		S		●	G	●	●	Open
Steinbrecher 2006	C		S		●	G	●	●	Open
Anceaume et al. 2013	D	$[0,1]$	S	$[0,1]$	●	G		●	Beta reputation
Christin et al. 2013	C		S		●	G	●	●	Open
Other Systems									
Kinateder and Pearson 2003	D	$[0,1]$	S	$\mathbb{R}$	●	L	○	●	Open
Bo et al. 2007	H		S		●	G	●	●	Open

Legend

C – D – H	Centralized – Decentralized – Hybrid	●	Property satisfied
S – M	Single – Multiple	○	Property not satisfied
G – L	Global – Local		Property not specified or not applicable

Table 2. User Anonymity-Oriented Systems – Security Fundamentals and Building Blocks.

System	Adversarial Model	Collusion Resistance	Reputation Binding	Trust Model	Building Blocks
Blockchain-based Systems					
Schaub et al. 2016	M	●	P	Trustless	Okamoto / Chaum blind signatures, PoS blockchain
Bazin et al. 2017	M	●	P	A-k, TTP	Merkle trees, blind signatures, non-interactive zero-knowledge proofs, blockchain
Dou et al. 2018	SH, M	●	P	A-k, TTP	Additive homomorphic encryption, verifiable secret sharing, blockchain for feedback storage
Kang et al. 2018	SH, M	◒	I	A-k, TTP	Elliptic curve digital signatures, blockchain, smart contracts
Lu et al. 2018	SH, M	◒	I	TTP	Merkle trees, digital certificates, blockchain
Owiyo et al. 2018	SH		P		SMPC, blind signatures, blockchain
Jo and Choi 2019	SH, M	◒	I	TTP	Group signatures, blind signatures, blockchain, smart contracts
Liu et al. 2019	M	●	I	A-k, TTP	PS signature, bulletproof system, non-interactive zero-knowledge proofs, PoS blockchain, smart contracts
Dimitriou 2021	SH, M	●	I	Trustless, TTP	Pedersen commitments, blockchain, zkSNARK proofs
Token-based Systems					
Androulaki et al. 2008	SH, M	●	I	A-k, TTP	E-cash, anonymous credential system, blind signatures
Schiffner et al. 2009	SH, M	●	I	A-k, TTP	E-cash, cryptographic signatures, one-show credentials
Schiffner et al. 2011	SH, M	●	I	A-k, TTP	Symmetric key encryption, homomorphic encryption, DC-Net, Diffie-Hellman key exchange
Zhang et al. 2014	SH, M	●	I	TTP	Bilinear maps, Camenisch and Lysyanskaya (CL) signatures, Pedersen commitment, non-interactive zero-knowledge proofs
Busom et al. 2017	SH, M	●	I	TTP	Chaum-Pedersen zero-knowledge proofs, Chaum-Pedersen blind signatures, verifiable secret sharing, oblivious transfer
Proxy-based Systems					
Petrlic et al. 2014	SH, M	◒	I	TTP	Paillier additive homomorphic encryption, zero-knowledge proofs
Mousa et al. 2017	SH, M	◒	I	TTP	Digital certificates
Signature-based Systems					
Bethencourt et al. 2010	SH, M	◒	I	TTP	Homomorphic encryption, selective-tag weakly CCA-secure encryption, zero-knowledge proofs, one-time signatures
Guo et al. 2013	SH, M	◒	I	TTP	Boneh-Boyen signature scheme, homomorphic encryption, selective-tag encryption, Groth-Sahai non-interactive proofs
Lajoie-Mazenc et al. 2015	SH, M	●	I	A-k, TTP	Verifiable secret sharing, non-interactive zero-knowledge proofs, anonymous proxy signatures, SXDH commitments
Chen et al. 2016	SH, M	◒	P	TTP	Boneh-Boyen-Shacham (BBS) short group signature scheme
Transitory Pseudonym-based Systems					
Miranda and Rodrigues 2006	SH, M	◒	I	TTP	Cryptographic signatures, blind signatures
Steinbrecher 2006	SH, M	◒	I	TTP	Identity management, cryptographic credentials, cryptographic signatures
Anceaume et al. 2013	M	●	I	A-k, TTP	Overlay network, Distributed Hash Tables (DHTs), cryptographic commitments
Christin et al. 2013	SH, M	◒	I	TTP	Cryptographic signatures, blind signatures
Other Systems					
Kinateder and Pearson 2003	SH, M	◒	I	TTP	Trusted Platform Module (TPM), cryptographic signatures
Bo et al. 2007	SH, M	◒	I	TTP	Smart cards, cryptographic signatures, hash chain, zero-knowledge proof of possession

Legend

SH – M	Semi-Honest – Malicious
I – P	Identity – Pseudonym
A-k – C-k – TTP	Arbitrary k – Chosen k – Trusted Third Party
●	Strong resistance to collusion
◒	Partial resistance to collusion
○	Weak or no resistance to collusion
	Collusion resistance not specified or not applicable

In addition to ballot stuffing, the system also offers resistance against bad mouthing. In order to submit a feedback about SP, a real transaction needs to take place and its cost needs to be paid to the service provider. It is therefore not possible for an adversary to submit frivolous negative feedback about the service provider without incurring a cost. A Sybil attack is not feasible for either the customer or the service provider since owning multiple addresses in the system does not provide any apparent adversarial advantage. The system is also fairly immune to free riding because (other than potentially generating some network traffic) consulting the blockchain for computing the reputation of a service provider does not directly draw any resources from the raters or the ratee. Moreover, the system is robust against out of range feedback since feedback is public and is verified by miners before integration into the blockchain.

Table 3. Feedback Confidentiality-Oriented Systems – Security Fundamentals and Building Blocks.

System	Adversarial Model	Collusion Resistance	Reputation Binding	Trust Model	Building Blocks
Blockchain-based Systems					
Azad et al. 2018	SH, M	●	P	A-k	Homomorphic encryption, non-interactive zero-knowledge proofs, public bulletin board (may be implemented by a blockchain)
Bag et al. 2018	M	●	P	A-k	SMPC, homomorphic encryption, zero-knowledge proofs, Schnorr signature protocol, public bulletin board (may be implemented by a blockchain)
Schiedermeier et al. 2019	M	●	P	A-k	SMPC, secret sharing, homomorphic encryption, blockchain
Zhao et al. 2019	SH, M	●	P	TTP	SMPC, additive secret sharing, blockchain, smart contracts
Azad et al. 2020	M	●	P	A-k	SMPC, homomorphic encryption, zero-knowledge proofs, public bulletin board (may be implemented by a blockchain)
Zhang et al. 2020	M	●	P	A-k, TTP	SMPC, Eigentrust algorithm, blockchain, smart contracts, verifiable secret sharing
SMPC-based Systems					
Pavlov et al. 2004	M	●	P	A-k	SMPC, Pederson verifiable secret sharing scheme, discrete-log commitment, zero-knowledge proofs
Gudes et al. 2009	SH	◒	P	A-k	SMPC
Nithyanand and Raman 2009	SH	◒	P	A-k	SMPC, Paillier additive homomorphic encryption
Gal-Oz et al. 2010	SH	●	P	A-k	SMPC, semantically-secure public-key encryption, homomorphic encryption
Hasan et al. 2013	M	●	P	C-k	SMPC, Paillier additive homomorphic encryption, non-interactive zero-knowledge proofs
Dimitriou and Michalas 2014	M	●	P	A-k	SMPC, Paillier additive homomorphic encryption, non-interactive zero-knowledge proofs
Dolev et al. 2014	M	●	P	A-k	SMPC, Paillier additive homomorphic encryption, Polhig-Hellman commutative encryption, ElGamal encryption
Clark et al. 2016	SH	●	P	C-k	SMPC, secret sharing, digital signatures
Bakas et al. 2021	SH	●	P	A-k	SMPC, Multi-Input Functional Encryption (MIFE), Trusted Execution Environment (TEE)
Token-based Systems					
Kerschbaum 2009	SH, M	◒	I	A-k, TTP	Homomorphic encryption, cryptographic pairings, zero-knowledge proofs
Proxy-based Systems					
Ries et al. 2011	SH, M	◒	P	TTP	Homomorphic encryption, zero-knowledge proofs
Ma et al. 2018	SH	◒	P	TTP	Somewhat-homomorphic encryption, cloud

Legend

SH – M	Semi-Honest – Malicious
I – P	Identity – Pseudonym
A-k – C-k – TTP	Arbitrary k – Chosen k – Trusted Third Party
●	Strong resistance to collusion
◒	Partial resistance to collusion
○	Weak or no resistance to collusion
	Collusion resistance not specified or not applicable

As our analysis in Section 6 shows, the limitations of the system include the inability to guarantee ratee anonymity, reputation transfer, distinctness, and accountability. Moreover, the system does not offer strong countermeasures against ballot stuffing, slandering, and whitewashing attacks. No countermeasures are offered against the oscillation and random ratings attacks.

7.2 Bag et al. 2018

Bag et al. [11] present PrivRep, a privacy aware decentralized and personalized reputation system for electronic marketplaces. The system computes a personalized reputation score of a business entity by taking into account only the trust scores from a set of personally trusted users. This is done so with disclosing neither the identities of participants in the trusted set nor their trust scores.

The architecture of PrivRep comprises of the raters, the marketplace, and a Public Bulletin Board (PBB). Although, not explicitly stated by the authors, the public bulletin board described in the paper lends itself well to implementation by a blockchain. In a more recent paper [9] by the same authors, they do describe a blockchain as "essentially a public bulletin board with distributed data storage and computing power", which "hence can be used in our system to realize the PBB".

Table 4. User Anonymity-Oriented Systems – Security Objectives.

	Privacy							Integrity				
System	**Multiple Pseudonyms**	**User-Pseudo Unlinkability**	**Pseudo-Pseudo Unlinkability**	**Rater Anonymity**	**Ratee Anonymity**	**Inquirer Anonymity**	**Reputation Transfer**	**Unforgeability**	**Distinctness**	**Accountability**	**Authorizability**	**Verifiability**
Blockchain-based Systems												
Schaub et al. 2016	●	●	●	●	○	●	○	●	○	○	●	●
Bazin et al. 2017	●	●	●	●	○	●	○	●	○	○	●	●
Dou et al. 2018	○	●		●	○	○	○	●	○	○	●	○
Kang et al. 2018	●	●		●	●	○	○	●	○	●	○	○
Lu et al. 2018	●	●	●	●	●		○	●	○	●	○	○
Owiyo et al. 2018	●	●	●	●	○	○	○	●	○		●	●
Jo and Choi 2019	○	●	○	●	○	○	○	●	○	●	○	●
Liu et al. 2019	○	●		●	○			●		●	●	●
Dimitriou 2021	●	●	●	●	●	○	●	●	○	○	●	●
Token-based Systems												
Androulaki et al. 2008	●	●	●	●	●	●	●	●	○	●	○	○
Schiffner et al. 2009	●	●	●	●	●	●	●	●	○	●	●	○
Schiffner et al. 2011	●	●	●	●	●	●	●	●	○		●	○
Zhang et al. 2014	●	●	●	●	○	○		●		●	●	
Busom et al. 2017	●	●	●	●	○		○	●			●	
Proxy-based Systems												
Petrlic et al. 2014	●	●	●	●	○	●	○	●			●	●
Mousa et al. 2017	●	●	●		●	○	●	●		○	●	○
Signature-based Systems												
Bethencourt et al. 2010	●	●	●	●	●		●	●	●			
Guo et al. 2013	●	●	●	●	●			●				
Lajoie-Mazenc et al. 2015	●	●	●	●	●	●	●	●	●		●	●
Chen et al. 2016	●	●	●	●	○		○	●		●	○	○
Transitory Pseudonym-based Systems												
Miranda and Rodrigues 2006	●	●	●	○	●	○	●	●	○	○	○	○
Steinbrecher 2006	●	●		○	●	○		●	○		●	
Anceaume et al. 2013	●	●	●	●	○	○		●	○	○	●	●
Christin et al. 2013	●	●	●	○	●	○	●	●			●	
Other Systems												
Kinateder and Pearson 2003	●	●	●	●	●	○		●	○	●	○	○
Bo et al. 2007	●	●	●	●	○	○	○		○		○	○

Legend

●	Property satisfied
◒	Property partially satisfied
○	Property not satisfied
	Property not specified or not applicable

Table 5. Feedback Confidentiality-Oriented Systems – Security Objectives.

	Privacy			Integrity			
System	**Confidentiality (Intermediate Info)**	**Confidentiality (Public Info)**	**Privacy of Relationships**	**Correct Range**	**Correct Computation**	**Authorizability**	**Verifiability**
Blockchain-based Systems							
Azad et al. 2018	●	◒		●	●	●	●
Bag et al. 2018	●	◒	●	●	●	○	●
Schiedermeier et al. 2019	●	○		◒	●	◒	●
Zhao et al. 2019	●	●		◒	●	●	
Azad et al. 2020	●	○	○	●	●	○	●
Zhang et al. 2020	●	○	○	●	●	●	○
SMPC-based Systems							
Pavlov et al. 2004	●	○		●	●	○	○
Gudes et al. 2009	●	○	◒	●	●	○	○
Nithyanand and Raman 2009	●	○		●	●	○	○
Gal-Oz et al. 2010	●	○	◒	●	●	○	○
Hasan et al. 2013	●	◒	○	●	●	○	○
Dimitriou and Michalas 2014	●	◒		●	●	○	○
Dolev et al. 2014	●	○		●	◒	○	○
Clark et al. 2016	●	○	○	●	●	○	○
Bakas et al. 2021	●	○		●	●	○	○
Token-based Systems							
Kerschbaum 2009	●	◒		●	●	●	●
Proxy-based Systems							
Ries et al. 2011	●	◒		●	●	○	○
Ma et al. 2018	●	●		◒	●	●	○

Legend

●	Property satisfied
◒	Property partially satisfied
○	Property not satisfied
	Property not specified or not applicable

The feedback providers homomorphically encrypt their rating scores and publish them on the public bulletin board. The feedback providers also publish non-interactive zero-knowledge proofs to demonstrate that the encrypted rating scores lie within the correct range. The reputation engine, which is operated by the owner of the marketplace, runs a SMPC protocol to compute personalized reputation scores. The reputation engine considers feedback from only personally trusted sources. The feedback providers do not learn whether their submitted scores are included or discarded in the computation of a particular reputation score. The set of trusted participants is constituted by the reputation engine.

The system is shown to be secure under the malicious adversarial model. The adversary may collude with up to $\Delta - 2$ users, where Δ is the number of trusted feedback providers in the protocol. Δ is less than n, which is the size of the set of all feedback providers in the protocol. Privacy is guaranteed if there are at least 2 honest users who provide different feedback. The trust model in this system is arbitrary k.

Table 6. Countermeasures Against Common Attacks.

System	Sybil Attack	Ballot Stuffing	Slandering	Whitewashing	Oscillation	Random Ratings	Free Riding
Blockchain-based Systems							
Schaub et al. 2016	●	◒	◒	◒	○	○	●
Bazin et al. 2017	●	◒	○	●	◒	○	○
Azad et al. 2018	◒	◒	◒	◒	○	○	○
Bag et al. 2018	◒	◒	○	○	○	○	○
Dou et al. 2018	◒	○	○	◒	◒	○	○
Kang et al. 2018	●	◒	◒	◒	●	○	○
Lu et al. 2018	●	◒	●	●	●	●	
Owiyo et al. 2018	○	◒	◒	○	○	◒	○
Jo and Choi 2019	●	●	◒	●	○		
Liu et al. 2019	●	◒	○	○	○	○	○
Schiedermeier et al. 2019	◒	◒	○	○	○	○	○
Zhao et al. 2019	○	◒	◒	○	○	○	●
Azad et al. 2020	○	○	○	◒	○	○	○
Zhang et al. 2020	◒	●	●	○	●	○	◒
Dimitriou 2021	●	●	○	●	○	○	○
SMPC-Based Systems							
Pavlov et al. 2004	○	◒	◒	○	○	○	○
Gudes et al. 2009	◒	◒	◒	○	○	○	○
Nithyanand and Raman 2009	◒	◒	◒	○	○	○	○
Gal-Oz et al. 2010	◒	◒	◒	○	○	○	○
Hasan et al. 2013	○	○	○	○	○	○	○
Dimitriou and Michalas 2014	○	○	○	○	○	○	○
Dolev et al. 2014	○	◒	◒	○	○	◒	○
Clark et al. 2016	○	○	○	○	○	○	○
Bakas et al. 2021	○	○	○	○	○	○	○
Token-based Systems							
Androulaki et al. 2008	●	○	◒	◒	○	●	○
Kerschbaum 2009	●	◒	◒	●	○	○	●
Schiffner et al. 2009	●	○	◒	●	○	●	○
Schiffner et al. 2011	●	◒	◒	●	○	◒	○
Zhang et al. 2014	●		●	●	○	◒	○
Busom et al. 2017	●	●	◒	◒	○	◒	○
Proxy-based Systems							
Ries et al. 2011	◒	◒	◒	○	○	◒	○
Petrlic et al. 2014	●	◒	◒	●	●	◒	○
Mousa et al. 2017	●	●	●	●	◒	●	●
Ma et al. 2018	○	●	●	○	●	●	●
Signature-based Systems							
Bethencourt et al. 2010	●	●	●	◒	◒	●	●
Guo et al. 2013	●		◒	◒	◒		
Lajoie-Mazenc et al. 2015	●	◒	◒	●	○	○	○
Chen et al. 2016		◒	○	◒	◒	○	○
Transitory Pseudonym-based Systems							
Miranda and Rodrigues 2006	●	○	○	◒	○	○	
Steinbrecher 2006		○	○		○	○	
Anceaume et al. 2013	●	●	◒	●	◒	◒	○
Christin et al. 2013	●	●	●	●	○	●	
Other Systems							
Kinateder and Pearson 2003	◒	◒	○	◒	○	○	○
Bo et al. 2007	●	○	◒	○	○	○	○

Legend

●	Strong or explicit countermeasures
◒	Partial or implicit countermeasures
○	Weak or no countermeasures
	Countermeasures not specified or not applicable

The Δ users in a protocol are selected by the reputation engine. The privacy of the users depends on that set of Δ users.

In terms of limitations, the system does not fully guarantee that the adversary is unable to infer user feedback from publicly available information, such as the reputation score. Furthermore, the system does not provide authorizability of ratings. The system provides partial resistance to Sybil and ballot stuffing attacks since the reputation engine is able to select trusted feedback providers for the computation of reputation. However, the system offers no defenses against the slandering, whitewashing, oscillation, random ratings, and free riding attacks.

7.3 Jo and Choi 2019

Jo and Choi [52] present BPRF, a blockchain-based privacy-preserving reputation framework for participatory sensing systems. The system has two concurrent goals: 1) protecting the privacy of users who submit sensing data; and 2) ensuring data trustworthiness by managing the reputation of users in the context of the reliability of the data submitted. A participating user is able to submit a sensing report anonymously and in an unlinkable manner. However, fellow users (e.g., those in the same location) can independently observe the environment and can then submit feedback about the veracity of the sensing report. The architecture of BPRF comprises of a smart contract on a blockchain that manages the reputation of a participant user based on their sensing data and the corresponding feedback. A reliable sensing report earns the participating user a reward token, whereas a disputed one earns a penalty token. Reputation values of users are transparently managed by the smart contract and are thus publicly auditable.

Although, the reputation is managed by a smart contract on a decentralized blockchain, the system overall has a hybrid architecture due to the inclusion of centralized trusted parties, such as the application servers and a trace server. An application server employs a group signature algorithm to maintain groups corresponding to different reputation levels. Membership of a user in a group represents association with the reputation of that group. Group signatures are used for a group member to send sensing reports without revealing identity, yet demonstrating reputation. Reputation is not transferable between members of different groups.

Reputation is identity-bound because users are authenticated using a PKI. If they exit and re-enter the system, they can be recognized and re-assigned their existing reputation. This mechanism provides strong resistance against Sybil attacks and whitewashing. BPRF considers the users to operate under the malicious adversarial model. However, the majority of users is considered to be honest. Moreover, the relaxed semi-honest model is assumed for the servers and they are required not to collude with each other. An application server and the trace server may collaborate to reveal the identity of a misbehaving user, thus providing accountability. The system provides protection against out of range feedback since a trusted application server receives feedback directly.

A limitation of the system is that it does not allow a user to assume multiple pseudonyms. This may be problematic for the privacy of the past activity of the user if her single pseudonym gets linked to her identity. Consequently, the system does not offer pseudonym-pseudonym unlinkability and reputation transfer. Additionally, the system does not provide ratee anonymity, inquirer anonymity, distinctness, and authorizability. As discussed above, the system is robust against several common attacks. However, it does not guarantee strong protection against slandering and oscillation attacks. It is not evident whether the system provides any countermeasures against random ratings and free riding attacks.

7.4 Liu et al. 2019

Liu et al. [61] propose a reputation system that preserves user anonymity in a retail marketing environment. The architecture of the system comprises of: retailers whose reputation is managed by the system; consumers who transact with the retailers and provide rating scores; an Identity Management entity (IDM) that issues unique identities and credentials to the retailers and the consumers; and a Proof of Stake (PoS) blockchain.

The design goals of the system include: 1) Bounded confidentiality – Even though a rating score provided by a consumer is kept private, the consumer is unable to submit a rating score that falls out of a predefined range. 2) Conditional anonymity – The anonymity of a consumer is guaranteed for operations such as providing a rating score. However, the IDM is able to retrieve the true identity of a consumer in case of misbehavior. 3) Unforgeability – Consumers are unable to forge credentials issued by the IDM and rating tokens issued by retailers. 4) Confined unlinkability – An adversary cannot observe whether two valid rating scores for two different retailers are from the same consumer. Yet, the rating scores can be linked to the consumer in case she submits multiple scores for the same transaction. 5) Transparency – Rating score submission and reputation computation is transparent and publicly verifiable.

The system operates as follows: Retailers and consumers must register themselves with the IDM using their true identity. The IDM issues anonymous identity credentials to consumers upon registration. A consumer can then transact with a retailer using their anonymous credential and an anonymous payment channel. After the transaction, the retailer issues an anonymous rating token to the consumer. The IDM constitutes a committee of retailers for the rating generation and verification process. The consumer chooses a rating and encrypts it using the public keys of the committee members. The consumer then constructs a zero-knowledge proof of correctness of the rating score. Additionally, the consumer constructs zero-knowledge proofs of possession of a valid credential and a valid rating token. The committee of retailers receives the encrypted rating score and the corresponding zero-knowledge proofs. After verifying its correctness, the committee is able to aggregate the newly submitted rating with the reputation score of the target retailer, while maintaining its confidentiality. The system also enables the committee to detect repeat ratings (ballot stuffing). The committee notifies the IDM in case of misbehavior, which in turn can reveal the identity of the misbehaving consumer.

The rating generation, verification, and aggregation operations take place on the PoS blockchain through smart contracts. This allows the system to provide transparency and public auditability. In order to breach confidentiality, either all committee members or the slot leader (the participant who creates a block on the chain for a given time slot) must collude. A user needs to trust the committee of retailers. Therefore, the arbitrary k trust model applies. Additionally, the IDM is a centralized trusted third party. The system is secure under the malicious adversarial model.

As a limitation, this user anonymity-oriented system does not allow users to hold multiple pseudonyms. Moreover, rater anonymity is not offered. The properties of inquirer anonymity and feedback distinctness are not evident either. Apart from strong resistance to Sybil attacks and partial resistance to ballot stuffing, the system does not provide countermeasures against any of the other attacks that have been analyzed.

7.5 Schiedermeier et al. 2019

Schiedermeier et al. [80] describe a protocol for holding referendums in trustless networks. The protocol is a secure multi-party computation protocol assisted by a blockchain that serves as a public communication channel among the participants. A referendum protocol can serve as a reputation protocol where the subject of the referendum is considered to be the ratee and the voters are considered to be the raters.

The key objectives of the protocol are as follows: 1) confidentiality of the votes; 2) transparency, that is, maintaining a public trace of all operations performed and the information exchanged among the participants; 3) outcome verifiability, that is, any participant is able to autonomously verify the correctness of the outcome of the referendum; and 4) immutability of proceedings, that is, all published information regarding the execution of an instance of the protocol is persisted and accessible permanently.

The participants of the protocol comprise of: 1) an initiator who initiates a referendum and defines its parameters such as the referendum subject and the list of voters (identified by their public keys); 2) voters, who submit their votes; and 3) workers, who perform intermediate computations for the execution of the protocol. In order to vote, a voter generates n secret shares of her vote, which are homomorphically encrypted with the public keys of the n workers, respectively. The shares are published on a blockchain to be retrieved by the workers. After the expiration of the voting phase, each worker aggregates the shares encrypted with her key. The worker does not gain access to the private votes because she does not have access to a sufficient number of decrypted shares of any voter. The intermediate results are also placed on the blockchain by the workers. Any querier can then aggregate the intermediate results to determine the final result.

The protocol is analyzed to be secure against a number of threats posed by malicious adversaries. Considering that the protocol uses a t out of n secret sharing scheme, collusion would be possible between up to $t-1$ workers. The authors discuss some heuristics for minimizing the risk of collusion. The initiator of the protocol authorizes the pseudonymous users that participate in the referendum. The protocol therefore provides partial resistance to Sybil attacks and ballot stuffing. An arbitrary set of workers need to be trusted by a voter. Therefore, the arbitrary k trust model applies. Other aspects of the protocol (such as, information storage on the blockchain) are trustless.

A limitation of this protocol is that the adversary may use publicly available information such as the vote total to infer individual votes. This is particularly a problem when the number of voters is low. Furthermore, the protocol takes some measures to ensure the correct range for votes as well as authorizability. However, these properties are not fully guaranteed. Additionally, the protocol does not defend against any of the analyzed common attacks except the Sybil and ballot stuffing attacks, for which partial countermeasures are included.

8 DISCUSSION

The fine-grained analysis and comparison of privacy-preserving reputation systems carried out in this survey, according to the proposed analysis frameworks, reveal a number of insights into this area of research, which are discussed below. We label each of the identified major future research directions with a unique ID (given as Di). Moreover, we summarize these research directions in Table 7.

Our first observation relates to the utilization of blockchain by privacy-preserving reputation systems. We note that the advent of the blockchain technology has provided a fresh impetus to research on privacy-preserving reputation systems. A majority of the systems published since 2016 utilize blockchain as one of the building blocks. We found 15 privacy-preserving reputation systems that are blockchain-based. In contrast, we discovered only 6 systems developed since 2016 that do not utilize blockchain. The reasons for the adoption of blockchain are evident. For example, in the case of Schaub et al.'s [79] system, using blockchain enables the system to provide the property of trustlessness, which was not offered by any prior systems. Another example is the system by Schiedermeier et al. [80], which is able to guarantee transparency and immutability by employing a blockchain. These properties are mostly absent in pre-blockchain systems.

Despite the successful application of blockchain, we do note that the development of non-blockchain-based privacy-preserving reputation systems still holds importance (D1). We can cite a couple of reasons. Firstly, blockchain can be an expensive building block to rely on in terms of the resources consumed. The computing cycles and the network bandwidth spent, and more worryingly the carbon footprint of popular blockchain-based systems such as Bitcoin, remain a significant concern [85]. Secondly, certain applications do not benefit as much as others from the decentralization and the trustlessness that blockchain offers. One such application is mobile participatory or crowdsensing. We note that two (Ma et al. [63] and Mousa et al. [71]) of the six non-blockchain-based privacy-preserving reputation systems since 2016 that have been analyzed are for this application area. They both employ a centralized architecture due to the nature of the application, which collects reports from mobile users and centralizes the data for subsequent analysis. We acknowledge that at least three (Zhang et al. [95], Jo and Choi [52], and Zhao et al. [97]) of the blockchain-based systems included in the survey also target the participatory sensing application area. These systems benefit from the smart contract functionality of blockchain technology to transparently manage the reputation of participants. However, we can observe that all three systems employ centralized TTPs in their architecture and thus do not take full advantage of the decentralization and trustlessness properties of blockchain.

Our above observations lead us to another notable and perhaps undesirable trend. Fully decentralized systems have existed since before blockchain. A key advantage that blockchain is able to offer in addition to decentralization is trustlessness. However, we observe that among all the blockchain-based systems analyzed, only one system (Schaub et al. [79]) benefits from this novel trust model to propose a fully trustless privacy-preserving reputation system. The system by Dimitriou [28] is another one that is primarily trustless, but it relies on a TTP for one of its operations. Other blockchain-based systems do benefit in part from the trustlessness of blockchain, but end up proposing hybrid trust models that include arbitrary k trusted users, chosen k trusted users, or TTPs. We believe that one of the future directions in this area of research is to leverage the blockchain technology to its full potential and build truly trustless systems (D2).

Next, we look at the success of the surveyed systems in guaranteeing the security of users. As discussed earlier in Section 3, the objectives of security include privacy and integrity. We first address user anonymity-oriented systems. Figure 4 shows the 12 identified individual security objectives of user anonymity-oriented systems and the portion of the 26 systems included in the literature that fulfill each of these objectives.

In terms of privacy properties, we can observe that all the systems guarantee user-pseudo unlinkability (26 systems). This is to be expected since this is a vital goal of user anonymity-oriented systems. Moreover, a high majority of the systems enable multiple pseudonyms (23 systems), pseudo-pseudo unlinkability (21 systems), and rater anonymity (22 systems). This is another positive sign indicating success of the systems toward providing strong privacy to the users. On the other hand, we note that much fewer systems aim for guaranteeing ratee anonymity (14 systems) and inquirer anonymity (7 systems). These properties have been ignored by a large number of the systems even though these are important properties for the privacy of roles other than the raters. We can identify inclusion of these objectives in future privacy-preserving reputation systems as another direction of research (D3). Reputation transfer and aggregation is another property that is offered by some systems but not provided by most others. We believe that this is an important property for long term sustainable privacy in the system and should thus be given priority as well (D4).

Moving to the properties of integrity, we are pleased to observe that almost all systems (25) enforce unforgeability, an essential property for the correct functioning of the user anonymity-oriented systems. Unfortunately, the assessment is not as bright for the rest of the integrity properties. There are 9 or less systems implementing the properties of either distinctness, accountability, or verifiability. The property of

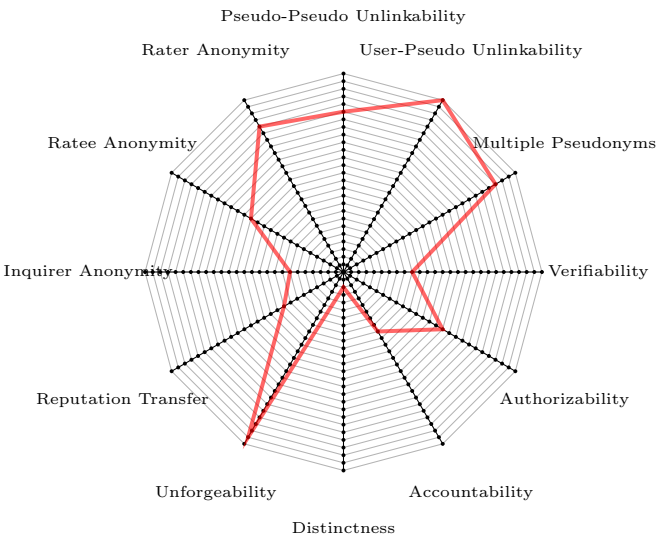

Fig. 4. The number of user anonymity-oriented systems (out of a total of 26) that fully satisfy the given security objectives. Note: there are no systems that partially satisfy the objectives.

authorizability is offered by only 15 of the systems that we have analyzed. This is a worrisome figure since we believe that authorizability must be a critical feature for all privacy-preserving reputation systems. Absence of this property can allow an adversary to take unfair advantage of anonymity and mount attacks such as ballot stuffing and slandering. The somewhat encouraging news is that if we consider only the subset of systems since 2016, we can observe that 8 out of the 12 systems offer authorizability. Thus, the trend is moving favorably toward including authorizability and should continue to do so (D5).

We now discuss the feedback confidentiality-oriented systems and their success in enforcing the listed security objectives. Figure 5 shows the 3 privacy objectives and the 4 integrity objectives of feedback confidentiality-oriented systems and the fraction of the 18 systems that satisfy those objectives.

Considering the privacy objectives, we observe that all systems ensure that feedback confidentiality is maintained even if the adversary has access to intermediate information revealed during the execution of the protocols. This is the primary privacy objective of feedback confidentiality systems. Therefore, this property is the minimum expectation from any system. In contrast, we observe that less than half of the systems can guarantee to some degree that an adversary will be unable to infer the feedback values from publicly available information, which includes the computed reputation scores. However, this issue is generally of concern when the number of participants is low. Therefore, even if future systems do not ensure this property, they should take measures to either warn users when their privacy is at risk or prevent execution of protocol instances with few participants (D6). The property of privacy of relationships concerns a subset of the systems that rely on relationships between users for privacy preservation. We observe that only 3 systems are able to satisfy this property to some extent. Future systems should protect the privacy of relationships in addition to the confidentiality of feedback (D7).

Looking at the integrity objectives, we appreciate that almost all systems fully enforce correct computation as well as guarantee that submitted feedback will respect the correct range. This is a reassuring trend since these two properties imply that systems are able to produce correct reputation scores despite

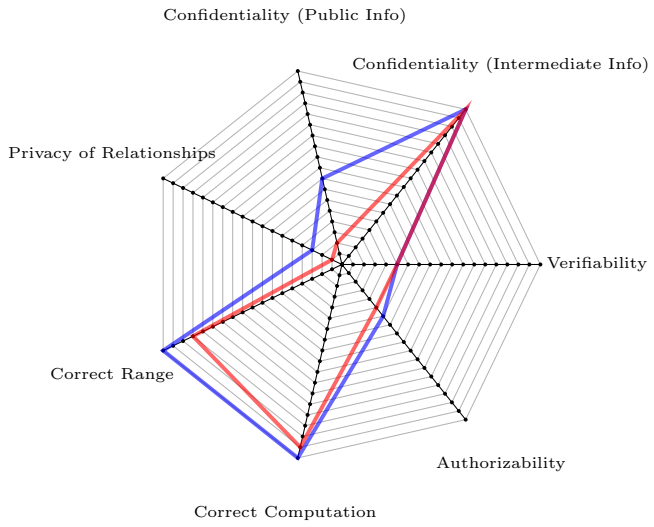

Fig. 5. The number of feedback confidentiality-oriented systems (out of a total of 18) that satisfy the given security objectives. Blue line: fully or partially satisfied. Red line: fully satisfied.

the confidentiality of the feedback values. Regrettably, similar to user anonymity-oriented systems, the feedback confidentiality-oriented systems also largely ignore the properties of authorizability (6 systems) and verifiability (5 systems). Even if we consider recent feedback confidentiality-oriented systems since 2016, we observe that only 4 out of the 9 systems fully satisfy the property of authorizability. As we argued earlier, this is an important property. Therefore, future work on feedback confidentiality-oriented privacy-preserving reputation systems should focus on its inclusion (D8).

Lastly, we discuss the systems in terms of their countermeasures against common attacks as analyzed in Table 6. Figure 6 shows the number of the 44 systems that propose defenses to the 7 listed attacks. We observe that the number of systems implementing countermeasures against these attacks is fairly low all across the board. This is particularly true for systems that propose strong countermeasures. A majority of the systems shows some level of resistance to the Sybil attack (32 systems), ballot stuffing (31 systems), slandering (29 systems), and whitewashing (25 systems). Defenses against other attacks are mostly overlooked: oscillation (12 systems), random ratings (15 systems), and free riding (7 systems). The figures are starkly lower when we consider only systems that offer strong countermeasures. For example, no more than 9 systems implement strong countermeasures against any of the following attacks: ballot stuffing, slandering, oscillation, random ratings, and free riding.

Moreover, Table 6 reveals that only two systems (Mousa et al. [71] and Benthencourt et al. [15]), out of the 44 systems analyzed, provide somewhat comprehensive resistance to the attacks. However, both these systems employ TTPs in their architecture. None of the systems with a fully decentralized architecture or with less intrusive trust models offers resistance to the full range of attacks. Table 6 further shows that there is no noticeable improvement in recent systems toward offering better resistance to these attacks.

There is clearly more work that needs to be done in the area of privacy-preserving reputation systems in terms of defenses against attacks other than breach of privacy. Privacy-preserving reputation systems are fundamentally reputation systems and their overall success thus relies on countering their basic challenges as well. One possible reason for the non-inclusion of robust protection against common attacks is that

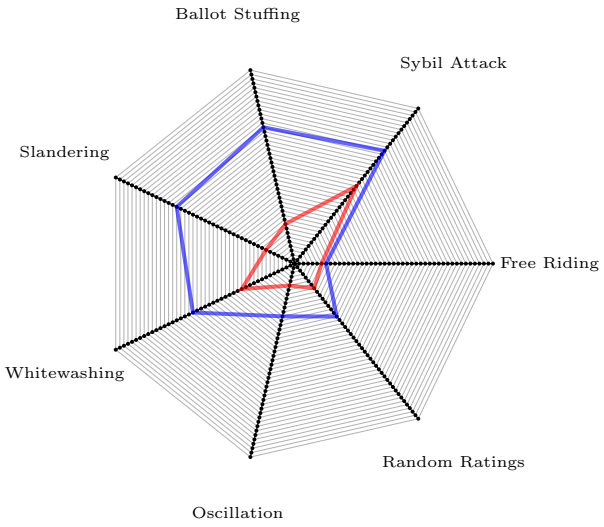

Fig. 6. The number of systems (out of a total of 44) that propose countermeasures for the listed attacks. Blue line: strong or partial countermeasures. Red line: strong countermeasures.

anonymity and privacy add further obstacles to preventing attacks such as ballot stuffing, slandering, random ratings, free riding, and others. An adversary may exploit the anonymity and privacy offered by a system to mount these attacks while simultaneously foregoing accountability. From these observations, an evident direction for future research in the area is designing systems that provide comprehensive protection against the broad range of attacks faced by reputations systems (D9). This is particularly true for decentralized systems, none of which were found to offer comprehensive countermeasures.

Table 7. Future Research Directions.

ID	Description
D1	The development of non-blockchain-based privacy-preserving reputation systems still holds importance and should continue in parallel with the development of blockchain-based systems.
D2	The blockchain technology should be leveraged to its full potential in order to build truly trustless systems.
D3	User anonymity-oriented systems should aim for guaranteeing ratee anonymity and inquirer anonymity.
D4	Reputation transfer and aggregation among pseudonyms should be given priority by user anonymity-oriented systems.
D5	The property of authorizability has been incorporated by a higher percentage of user anonymity-oriented systems in recent years than in the past. This trend of providing authorizability should continue.
D6	Future systems that do not prevent inference of feedback values from publicly available information, must take measures to either warn raters or prevent execution of protocol instances when their privacy is at risk.
D7	Feedback confidentiality-oriented systems should protect the privacy of relationships in addition to the confidentiality of feedback.
D8	Future work on feedback confidentiality-oriented privacy-preserving reputation systems should focus on the inclusion of the property of authorizability.
D9	Privacy-preserving reputation systems should be designed such that they provide comprehensive protection against the broad range of common attacks.

9 RELATED WORK

The Systematization of Knowledge (SoK) paper by Gurtler and Goldberg [41], which appeared after the initial submission of our survey, provides a systematic review of privacy-preserving reputation systems. Our survey is more up to date as it covers the literature published until July 2021, whereas the SoK covers articles until the year 2019. The analysis framework established in our survey is more fine-grained as it enables us to analyze and compare the user anonymity-oriented systems on 33 different parameters and the feedback confidentiality-oriented systems on 28 different parameters, whereas the SoK identifies 19 general parameters for analysis and comparison. Our analysis framework includes vital parameters such as the adversarial model, the trust model, the countermeasures against common attacks, etc. that are not addressed in the SoK. Another major difference is that the SoK does not focus on blockchain-based privacy-preserving reputation systems and thus includes neither a discussion of the important development of the new trustless model, nor the coverage of at least 10 blockchain-based systems [9, 34, 52, 55, 62, 74, 80, 95, 97] that are analyzed in detail in our survey.

Bellini et al. [14] author a survey on blockchain-based distributed trust and reputation management systems. The survey defines uniform taxonomies for blockchain and for systems aimed at managing trust and reputation. Several recommendations are given for the utilization of blockchain in the context of trust and reputation management. In contrast to the work by Bellini et al., our survey focuses specifically on privacy-preserving reputation systems based on blockchain as well as other cryptographic building blocks.

Butun and Österberg [21] and Butun [20] present a review of distributed access control approaches for blockchain-based systems toward securing the IoT, and a study of privacy and trust relations in IoT from the user point of view, respectively. Butun and Österberg address the applicability of blockchain solutions to providing security and privacy in IoT networks. Several reputation-based distributed access control systems are analyzed as part of this review. Butun's study includes a user survey that gauges the sensitivity of various personal identification features for users. Neither of these two papers specifically covers privacy-preserving reputation systems.

A survey by Chang et al. [22] studies approaches for promoting honest feedback in reputation systems, which include protecting the privacy of the feedback providers as well as providing them incentives. The work is focused in large part on the latter category, that is, providing incentives. However, four privacy oriented systems (Pavlov et al. [75], Hasan et al. [44], Gudes et al. [39], and Kinateder and Pearson [58]) are also analyzed and compared.

Tran et al.'s position paper [86] on the challenges and opportunities of privacy-preserving reputation management in fully decentralized systems includes a summary of the systems in this category.

The survey by Michalas et al. [66] addresses privacy in decentralized additive reputation systems. Michalas et al. identify and analyze the vulnerabilities of privacy-preserving reputation systems in the semi-honest and the malicious adversarial models. The survey covers three sets of decentralized additive reputation systems (from Pavlov et al. [75], Hasan et al. [44], and Dolev et al. [32]). In comparison, our survey aims to provide a broader perspective of the area of privacy-preserving reputation systems.

Hoffman et al. [47] present a survey of attack and defense techniques for reputation systems. The survey describes a number of challenges that reputation systems face and techniques that can resolve those challenges. However, their survey does not address the issue of privacy in reputation systems. A survey by Mármol and Pérez [65] also analyzes threat scenarios for reputation systems. Their survey does not cover privacy-preserving reputation systems either.

An extended version of the current survey has been released as a research report [43]. The extended version includes detailed descriptions of the non-privacy related dimensions of reputation systems listed

in Section 4 as well as of building blocks other than blockchain. Moreover, the extended version discusses in detail some systems in the literature for each of the categories identified in Section 5.

10 CONCLUSION

In this survey, we presented an in-depth analysis of a broad range of privacy-preserving reputation systems. We proposed an analysis framework that decomposes privacy-preserving reputation systems according to the following dimensions: the nature of the adversary, reputation binding, the trust model, the security objectives of the system, and the building blocks utilized. Additionally, we identified the security requirements of privacy-preserving reputation systems that cut across multiple types of such systems. It is observed that there are two main types of privacy-preserving reputation systems: 1) systems that preserve the anonymity of the users, and 2) systems that don't necessarily preserve the anonymity of the users but preserve the confidentiality of their feedback. We noted that the security-related requirements can be further subdivided into privacy requirements and integrity requirements. We also presented an analysis framework that covers the fundamental elements that are common to all reputation systems. The following elements were identified for this framework: the architecture of the system, the properties of the feedback, the properties of the reputation, the feedback aggregation model, the attacks addressed, and the reputation query costs.

We conducted a fine-grained analysis and comparison of 44 privacy-preserving reputation systems using our analysis frameworks. We established several categories of systems according to their security mechanisms and classified the privacy-preserving reputation systems according to these categories. Our detailed comparison of privacy-preserving reputation systems in a normalized manner using our analysis frameworks reveals the differences between the systems in the literature as well as their chronological evolution. The survey presented detailed descriptions of a number of blockchain-based systems, which included the first trustless decentralized system by Schaub et al. [79] as well as more recent systems. We discussed the details of their protocols and security approaches as well as highlighted their individual strengths and other salient features.

Our fine-grained analysis, comparison, and discussion led to the identification of a number of insights into this area of research. We observed that the advent of the blockchain technology has provided a fresh impetus to research on privacy-preserving reputation systems. A majority of the systems published since 2016 that are listed in this survey utilize blockchain as one of the building blocks. However, we also noted that one of the future directions is to leverage the blockchain technology to its full potential and build truly trustless systems. We looked at the success of the surveyed systems in guaranteeing the security of users. It was observed that a high majority of both anonymity-oriented and feedback confidentiality-oriented systems are able to guarantee their respective essential privacy and integrity properties. However, there are also many properties that have been mostly ignored. We identified authorizability as one of the important properties that needs to be addressed by systems in the future. Lastly, analyzing the systems in terms of their countermeasures against common attacks, we observed that designing systems that provide comprehensive protection against a broad range of attacks is an evident direction for future research in the area.

ACKNOWLEDGMENTS

We thank the anonymous reviewers and our fellow researchers Rémi Canillas and Sonia Ben Mokhtar for their valuable suggestions that have helped us improve this work.

REFERENCES

[1] Ahmed S Almasoud, Farookh Khadeer Hussain, and Omar K Hussain. 2020. Smart contracts for blockchain-based reputation systems: A systematic literature review. *Journal of Network and Computer Applications* 170 (2020), 102814.

[2] Emmanuelle Anceaume, Gilles Guette, Paul Lajoie-Mazenc, Nicolas Prigent, and V Viet Triem Tong. 2013. A privacy preserving distributed reputation mechanism. In *2013 IEEE International Conference on Communications (ICC)*. IEEE, 1951–1956.

[3] Emmanuelle Anceaume, Gilles Guette, Paul Lajoie-Mazenc, Thomas Sirvent, and Valérie Viet Triem Tong. 2014. Extending Signatures of Reputation. *Privacy and Identity Management for Emerging Services and Technologies, IFIP Advances in Information and Communication* 421 (2014), 165–176.

[4] Elli Androulaki, Seung Geol Choi, Steven M. Bellovin, and Tal Malkin. 2008. Reputation Systems for Anonymous Networks. In *Proceedings of the 8th Privacy Enhancing Technologies Symposium (PETS 2008)*.

[5] Mohd Anwar and Jim Greer. 2006. Reputation Management in Privacy-Enhanced E-learning. In *Proceedings of the 3rd Annual Scientific Conference of the LORNET Research Network (I2LOR-06)*. Montreal, Canada.

[6] Mohd Anwar and Jim Greer. 2008. Enabling Reputation-based Trust in Privacy-Enhanced Learning Systems. In *Proceedings of the 9th International Conference on Intelligent Tutoring Systems*. Montreal, Canada.

[7] Muhammad Ajmal Azad, Samiran Bag, and Feng Hao. 2017. M2m-rep: Reputation of machines in the internet of things. In *Proceedings of the 12th international conference on availability, reliability and security*. 1–7.

[8] Muhammad Ajmal Azad, Samiran Bag, and Feng Hao. 2018. PrivBox: Verifiable decentralized reputation system for online marketplaces. *Future Generation Computer Systems* 89 (2018), 44–57.

[9] Muhammad Ajmal Azad, Samiran Bag, Feng Hao, and Andrii Shalaginov. 2020. Decentralized self-enforcing trust management system for social Internet of Things. *IEEE Internet of Things Journal* 7, 4 (2020), 2690–2703.

[10] Mahmoud M Badr, Wesam Al Amiri, Mostafa M Fouda, Mohamed MEA Mahmoud, Abdulah Jeza Aljohani, and Waleed Alasmary. 2020. Smart parking system with privacy preservation and reputation management using blockchain. *IEEE Access* 8 (2020), 150823–150843.

[11] Samiran Bag, Muhammad Ajmal Azad, and Feng Hao. 2018. A privacy-aware decentralized and personalized reputation system. *Computers & Security* 77 (2018), 514–530.

[12] Alexandros Bakas, Antonis Michalas, and Amjad Ullah. 2021. (F) unctional Sifting: A Privacy-Preserving Reputation System Through Multi-Input Functional Encryption. In *Secure IT Systems: 25th Nordic Conference, NordSec 2020, Virtual Event, November 23–24, 2020, Proceedings 25*. Springer, 111–126.

[13] Rémi Bazin, Alexander Schaub, Omar Hasan, and Lionel Brunie. 2017. Self-reported verifiable reputation with rater privacy. In *IFIP International Conference on Trust Management*. Springer, 180–195.

[14] Emanuele Bellini, Youssef Iraqi, and Ernesto Damiani. 2020. Blockchain-based distributed trust and reputation management systems: a survey. *IEEE Access* 8 (2020), 21127–21151.

[15] John Bethencourt, Elaine Shi, and Dawn Song. 2010. Signatures of reputation: Towards trust without identity, In Proceedings of the Fourteenth International Conference on Financial Cryptography and Data Security (FC '10). *FC*, 400 – 407.

[16] Yang Bo, Zhou Min, and Li Guohuan. 2007. A Reputation System with Privacy and Incentive. In *Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'07)*.

[17] Diego De Siqueira Braga, Marco Niemann, Bernd Hellingrath, and Fernando Buarque De Lima Neto. 2018. Survey on computational trust and reputation models. *ACM Computing Surveys (CSUR)* 51, 5 (2018), 1–40.

[18] Sonja Brangewitz, Alexander Jungmann, Ronald Petrlic, and Marie Christin Platenius. 2014. Towards a flexible and privacy-preserving reputation system for markets of composed services. In *Proceedings of the 6th International Conferences on Advanced Service Computing (SERVICE COMPUTATION)*.

[19] Nuria Busom, Ronald Petrlic, Francesc Sebé, Christoph Sorge, and Magda Valls. 2017. A privacy-preserving reputation system with user rewards. *Journal of Network and Computer Applications* 80 (2017), 58–66.

[20] Ismail Butun. 2017. Privacy and trust relations in internet of things from the user point of view. In *2017 IEEE 7th annual computing and communication workshop and conference (CCWC)*. IEEE, 1–5.

[21] Ismail Butun and Patrik Österberg. 2020. A Review of Distributed Access Control for Blockchain Systems towards Securing the Internet of Things. *IEEE Access* (2020).

[22] Junsheng Chang, Liquan Xiao, and Weixia Xu. 2018. A Survey of Approaches for Promoting Honest Recommendations in Reputation Systems. In *CCF National Conference on Computer Engineering and Technology*. Springer, 179–191.

[23] Liqun Chen, Qin Li, Keith M Martin, and Siaw-Lynn Ng. 2016. Private reputation retrieval in public–a privacy-aware announcement scheme for VANETs. *IET Information Security* 11, 4 (2016), 204–210.

[24] Delphine Christin, Christian Roßkopf, Matthias Hollick, Leonardo A Martucci, and Salil S Kanhere. 2013. Incognisense: An anonymity-preserving reputation framework for participatory sensing applications. *Pervasive and mobile Computing* 9, 3 (2013), 353–371.
[25] Michael R Clark, Kyle Stewart, and Kenneth M Hopkinson. 2016. Dynamic, privacy-preserving decentralized reputation systems. *IEEE Transactions on Mobile Computing* 16, 9 (2016), 2506–2517.
[26] Sebastian Clauß, Stefan Schiffner, and Florian Kerschbaum. 2013. k-Anonymous Reputation. In *ASIA CCS 2013*. ACM.
[27] Daniel Cvrcek, Vaclav Matyas Jr., and Ahmed Patel. 2005. Evidence processing and privacy issues in evidence-based reputation systems. *Computer Standards & Interfaces* 27 (2005), 533 – 545.
[28] Tassos Dimitriou. 2021. Decentralized Reputation. In *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*. 119–130.
[29] Tassos Dimitriou and Antonis Michalas. 2012. Multi-party trust computation in decentralized environments. In *2012 5th International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 1–5.
[30] Tassos Dimitriou and Antonis Michalas. 2014. Multi-party trust computation in decentralized environments in the presence of malicious adversaries. *Ad Hoc Networks* 15 (2014), 53–66.
[31] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2003. Reputation in P2P Anonymity Systems. In *Proceedings of the Workshop on Economics of Peer-to-Peer Systems*.
[32] Shlomi Dolev, Niv Gilboa, and Marina Kopeetsky. 2010. Computing multi-party trust privately: in O (n) time units sending one (possibly large) message at a time. In *Proceedings of the 2010 ACM Symposium on Applied Computing*. 1460–1465.
[33] Shlomi Dolev, Niv Gilboa, and Marina Kopeetsky. 2014. Efficient private multi-party computations of trust in the presence of curious and malicious users. *Journal of Trust Management* 1, 1 (2014), 8.
[34] Yi Dou, Henry CB Chan, and Man Ho Au. 2018. A distributed trust evaluation protocol with privacy protection for intercloud. *IEEE Transactions on Parallel and Distributed Systems* 30, 6 (2018), 1208–1221.
[35] Nurit Gal-Oz, Niv Gilboa, and Ehud Gudes. 2010. Schemes for privately computing trust and reputation. In *IFIP International Conference on Trust Management*. Springer, 1–16.
[36] Nurit Gal-Oz, Ehud Gudes, and Danny Hendler. 2008. A Robust and Knot-Aware Trust-Based Reputation Model. In *Proceedings of the Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM 2008)*.
[37] Oded Goldreich. 2004. *The Foundations of Cryptography - Volume 2*. Cambridge University Press.
[38] Michael T Goodrich and Florian Kerschbaum. 2011. Privacy-enhanced reputation-feedback methods to reduce feedback extortion in online auctions. In *Proceedings of the first ACM conference on Data and application security and privacy*. 273–282.
[39] Ehud Gudes, Nurit Gal-Oz, and Alon Grubshtein. 2009. Methods for Computing Trust and Reputation While Preserving Privacy. In *Proceedings of the 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security*.
[40] Linke Guo, Yuguang Fang, and Lingbo Wei. 2013. Fine-grained privacy-preserving reputation system for online social networks. In *2013 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE, 230–235.
[41] Stan Gurtler and Ian Goldberg. 2021. SoK: Privacy-Preserving Reputation Systems. *Proc. Priv. Enhancing Technol.* 2021, 1 (2021), 107–127.
[42] Liming Hao, Songnian Lu, Junhua Tang, and Aixin Zhang. 2008. A low cost and reliable anonymity scheme in p2p reputation systems with trusted third parties. In *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*. IEEE, 1–5.
[43] Omar Hasan, Lionel Brunie, and Elisa Bertino. 2020. *Privacy preserving reputation systems based on blockchain and other cryptographic building blocks: A survey*. Technical Report. University of Lyon, CNRS, INSA-Lyon, LIRIS, UMR5205. https://hal-cnrs.archives-ouvertes.fr/hal-03034994/document (HAL Id: hal-03034994).
[44] Omar Hasan, Lionel Brunie, Elisa Bertino, and Ning Shang. 2013. A decentralized privacy preserving reputation protocol for the malicious adversarial model. *IEEE Transactions on Information Forensics and Security* 8, 6 (2013), 949–962.
[45] Ferry Hendrikx, Kris Bubendorfer, and Ryan Chard. 2015. Reputation systems: A survey and taxonomy. *J. Parallel and Distrib. Comput.* 75 (2015), 184–197.
[46] Erica Ho. 2015. Why you should think twice before trusting Airbnb reviews. https://mashable.com/2015/05/18/airbnb-reviews/
[47] Kevin Hoffman, David Zage, and Cristina Nita-Rotaru. 2009. A Survey of Attack and Defense Techniques for Reputation Systems. *Comput. Surveys* 41, 4 (December 2009).
[48] Kuan Lun Huang, Salil S Kanhere, and Wen Hu. 2012. A privacy-preserving reputation system for participatory sensing. In *37th Annual IEEE Conference on Local Computer Networks*. IEEE, 10–18.

[49] Yasir Hussain, Huang Zhiqiu, Muhammad Azeem Akbar, Ahmed Alsanad, Abeer Abdul-Aziz Alsanad, Asif Nawaz, Izhar Ahmed Khan, and Zaheer Ullah Khan. 2020. Context-aware trust and reputation model for fog-based IoT. *IEEE Access* 8 (2020), 31622–31632.

[50] Roslan Ismail, Colin Boyd, Audun Josang, and Selwyn Russell. 2004. Private Reputation Schemes for P2P Systems. In *Proceedings of the Second International Workshop on Security in Information Systems (WOSIS'04)*.

[51] Roslan Ismail, Colin Boyd, Audun Josang, and Selwyn Russell. 2004. Strong Privacy in Reputation Systems. In *Proceedings of the 4th International Workshop on Information Security Applications (WISA'03)*.

[52] Hyo Jin Jo and Wonsuk Choi. 2019. BPRF: Blockchain-based privacy-preserving reputation framework for participatory sensing systems. *Plos one* 14, 12 (2019), e0225688.

[53] Audun Josang, Roslan Ismail, and Colin Boyd. 2007. A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems* 43, 2 (March 2007), 618 – 644.

[54] Carlos Aparecido Serrato Júnior. 2020. *A Privacy Preserving System to Consult Public Institutions Records*. Master's thesis. Universidade de Coimbra.

[55] Jiawen Kang, Rong Yu, Xumin Huang, Maoqiang Wu, Sabita Maharjan, Shengli Xie, and Yan Zhang. 2018. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal* 6, 3 (2018), 4660–4670.

[56] Benjamin Kellermann, Stefanie Pötzsch, and Sandra Steinbrecher. 2011. Privacy-Respecting Reputation for Wiki Users. In *IFIP International Conference on Trust Management*. Springer, 223–239.

[57] Florian Kerschbaum. 2009. A verifiable, centralized, coercion-free reputation system. In *Proceedings of the 8th ACM workshop on Privacy in the electronic society (WPES'09)*. ACM, New York, NY, USA.

[58] Michael Kinateder and Siani Pearson. 2003. A Privacy-Enhanced Peer-to-Peer Reputation System. In *Proceedings of the 4th International Conference on Electronic Commerce and Web Technologies*.

[59] Michael Kinateder, Ralf Terdic, and Kurt Rothermel. 2005. Strong Pseudonymous Communication for Peer-to-Peer Reputation Systems. In *Proceedings of the 2005 ACM symposium on Applied computing*.

[60] Paul Lajoie-Mazenc, Emmanuelle Anceaume, Gilles Guette, Thomas Sirvent, and Valérie Viet Triem Tong. 2015. Efficient distributed privacy-preserving reputation mechanism handling non-monotonic ratings. *hal.archives-ouvertes.fr* (2015).

[61] Dongxiao Liu, Amal Alahmadi, Jianbing Ni, Xiaodong Lin, and Xuemin Shen. 2019. Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain. *IEEE Transactions on Industrial Informatics* 15, 6 (2019), 3527–3537.

[62] Zhaojun Lu, Wenchao Liu, Qian Wang, Gang Qu, and Zhenglin Liu. 2018. A privacy-preserving trust model based on blockchain for VANETs. *IEEE Access* 6 (2018), 45655–45664.

[63] Lichuan Ma, Xuefeng Liu, Qingqi Pei, and Yong Xiang. 2018. Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing. *IEEE Transactions on Services Computing* 12, 5 (2018), 786–799.

[64] Félix Gómez Mármol, Joao Girao, and Gregorio Martínez Pérez. 2010. TRIMS, a privacy-aware trust and reputation model for identity management systems. *Computer Networks* 54, 16 (2010), 2899–2912.

[65] Félix Gómez Mármol and Gregorio Martínez Pérez. 2009. Security threats scenarios in trust and reputation models for distributed systems. *computers & security* 28, 7 (2009), 545–556.

[66] Antonis Michalas, Tassos Dimitriou, Thanassis Giannetsos, Nikos Komninos, and Neeli R Prasad. 2012. Vulnerabilities of decentralized additive reputation systems regarding the privacy of individual votes. *Wireless Personal Communications* 66, 3 (2012), 559–575.

[67] Antonis Michalas and Nikos Komninos. 2014. The lord of the sense: A privacy preserving reputation system for participatory sensing applications. In *2014 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 1–6.

[68] Nolan Miller, Paul Resnick, and Richard Zeckhauser. 2005. Eliciting informative feedback: The peer-prediction method. *Management Science* 51, 9 (2005), 1359–1373.

[69] Tehila Minkus and Keith W Ross. 2014. I know what you're buying: Privacy breaches on ebay. In *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 164–183.

[70] Hugo Miranda and Luis Rodrigues. 2006. A Framework to Provide Anonymity in Reputation Systems. In *Proceedings of the Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*.

[71] Hayam Mousa, Sonia Ben Mokhtar, Omar Hasan, Lionel Brunie, Osama Younes, and Mohiy Hadhoud. 2017. Privasense: Privacy-preserving and reputation-aware mobile participatory sensing. In *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. 38–47.

[72] Molly Mulshine. 2015. After a disappointing Airbnb stay, I realized there's a major flaw in the review system. https://www.businessinsider.com/why-airbnb-reviews-are-a-problem-for-the-site-2015-6

[73] Rishab Nithyanand and Karthik Raman. 2009. Fuzzy Privacy Preserving Peer-to-Peer Reputation Management. Cryptology ePrint Archive, Report 2009/442.
[74] Erick Owiyo, Yong Wang, Eunice Asamoah, Domnic Kamenyi, and Isaac Obiri. 2018. Decentralized privacy preserving reputation system. In *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)*. IEEE, 665–672.
[75] Elan Pavlov, Jeffrey S. Rosenschein, and Zvi Topol. 2004. Supporting Privacy in Decentralized Additive Reputation Systems. In *Proceedings of the Second International Conference on Trust Management (iTrust 2004)*. Oxford, UK.
[76] Ronald Petrlic, Sascha Lutters, and Christoph Sorge. 2014. Privacy-preserving reputation management. In *Proceedings of the 29th Annual ACM Symposium on Applied Computing*. 1712–1718.
[77] Paul Resnick and Richard Zeckhauser. 2002. Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. *The Economics of the Internet and E-Commerce. Michael R. Baye, editor. Volume 11 of Advances in Applied Microeconomics* (2002), 127–157.
[78] Sebastian Ries, Marc Fischlin, Leonardo A Martucci, and Max Muuhlhauser. 2011. Learning whom to trust in a privacy-friendly way. In *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 214–225.
[79] Alexander Schaub, Rémi Bazin, Omar Hasan, and Lionel Brunie. 2016. A trustless privacy-preserving reputation system. In *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 398–411.
[80] Maximilian Schiedermeier, Omar Hasan, Lionel Brunie, Tobias Mayer, and Harald Kosch. 2019. A transparent referendum protocol with immutable proceedings and verifiable outcome for trustless networks. In *International Conference on Complex Networks and Their Applications*. Springer, 647–658.
[81] Stefan Schiffner, Sebastian Clauß, and Sandra Steinbrecher. 2009. Privacy and Liveliness for Reputation Systems. In *Proceedings of the Sixth European Workshop on Public Key Infrastructures, Services and Applications (EuroPKI'09)*. 209 – 224.
[82] Stefan Schiffner, Sebastian Clauß, and Sandra Steinbrecher. 2011. Privacy, liveliness and fairness for reputation. In *International Conference on Current Trends in Theory and Practice of Computer Science*. Springer, 506–519.
[83] Affaf Shahid, Umair Sarfraz, Muhammad Waseem Malik, Muhammad Sohaib Iftikhar, Abid Jamal, and Nadeem Javaid. 2020. Blockchain-Based Reputation System in Agri-Food Supply Chain.. In *AINA*. 12–21.
[84] Sandra Steinbrecher. 2006. Design Options for Privacy-Respecting Reputation Systems within Centralised Internet Communities. In *Security and Privacy in Dynamic Environments*.
[85] Christian Stoll, Lena Klaaßen, and Ulrich Gallersdörfer. 2019. The carbon footprint of bitcoin. *Joule* 3, 7 (2019), 1647–1661.
[86] Ngoc Hong Tran, Leila Bahri, and Binh Quoc Nguyen. 2017. Privacy-Preserving Reputation Management in Fully Decentralized Systems: Challenges and Opportunities. In *The Joint International Symposium on Artificial Intelligence and Natural Language Processing*. Springer, 207–215.
[87] Muhammad Habib ur Rehman, Khaled Salah, Ernesto Damiani, and Davor Svetinovic. 2020. Towards blockchain-based reputation-aware federated learning. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 183–188.
[88] Marco Voss, Andreas Heinemann, and Max Muhlhauser. 2005. A Privacy Preserving Reputation System for Mobile Information Dissemination Networks. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM)*.
[89] Xinlei Wang, Wei Cheng, Prasant Mohapatra, and Tarek Abdelzaher. 2013. Enabling reputation and trust in privacy-preserving mobile sensing. *IEEE Transactions on Mobile Computing* 13, 12 (2013), 2777–2790.
[90] Liang Xiao, Yuzhen Ding, Donghua Jiang, Jinhao Huang, Dongming Wang, Jie Li, and H Vincent Poor. 2020. A reinforcement learning and blockchain-based trust mechanism for edge networks. *IEEE Transactions on Communications* 68, 9 (2020), 5460–5470.
[91] Adamu Sani Yahaya, Nadeem Javaid, Rabiya Khalid, Muhammad Imran, and Nidal Naseer. 2020. A blockchain based privacy-preserving system for electric vehicles through local communication. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.
[92] Qussai Yaseen and Yaser Jararweh. 2021. Building an Intelligent Global IoT Reputation and Malicious Devices Detecting System. *Journal of Network and Systems Management* 29, 4 (2021), 1–17.
[93] Keli Zhang, Zhongxian Li, and Yixian Yang. 2014. A Reputation System Preserving the Privacy of Feedback Providers and Resisting Sybil Attacks. *International Journal of Multimedia and Ubiquitous Engineering* 9, 2 (2014), 141–152.
[94] Mingwu Zhang, Yong Xia, Ou Yuan, and Kirill Morozov. 2016. Privacy-friendly weighted-reputation aggregation protocols against malicious adversaries in cloud services. *International Journal of Communication Systems* 29, 12 (2016), 1863–1872.

[95] Wenjing Zhang, Yuchuan Luo, Shaojing Fu, and Tao Xie. 2020. Privacy-Preserving Reputation Management for Blockchain-Based Mobile Crowdsensing. In *2020 17th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 1–9.

[96] Zonghua Zhang, Jingwei Liu, and Youki Kadobayashi. 2010. STARS: a simple and efficient scheme for providing transparent traceability and anonymity to reputation systems. In *Data Privacy Management and Autonomous Spontaneous Security*. Springer, 170–187.

[97] Ke Zhao, Shaohua Tang, Bowen Zhao, and Yiming Wu. 2019. Dynamic and privacy-preserving reputation management for blockchain-based mobile crowdsensing. *IEEE Access* 7 (2019), 74694–74710.

[98] Zhili Zhou, Meimin Wang, Ching-Nung Yang, Zhangjie Fu, Sunmin Xin, and QM Jonathan Wu. 2021. Blockchain-based decentralized reputation system in E-commerce environment. *Future Generation Computer Systems* (2021).

APPENDIX

A ADDITIONAL LITERATURE

There are a number of other works that are noteworthy in the context of privacy-preserving reputation systems. Some early works include those by Ismail et al. [50, 51], Voss et al. [88], and Kinateder et al. [59], which presented decentralized systems, and those by Cvrček et al. [27], and Hao et al. [42], which discussed approaches for supporting multiple pseudonyms.

Mármol et al. [64] describe TRIMS, a privacy-aware trust and reputation model in the multi-domain scenario where the identities of the users may be different among domains. Zhang et al. [96] present STARS, a software component that can be added on to a reputation system for providing privacy. Kellermann et al. [56] present a privacy-preserving reputation system for wiki users. Goodrich and Kerschbaum [38] introduce a reputation system that prevents inference of private feedback from reputation scores despite immediate publishing of the scores. Clauß et al. [26] discuss the concept of a k-anonymous reputation system. Brangewitz et al. [18] present a reputation system for markets of composed services that preserves the privacy of consumers who rate the services. Zhang et al. [94] describe a privacy friendly reputation aggregation protocol for rating cloud services. Badr et al. [10] propose a system based on the work by Liu et al. [61] that allows drivers to anonymously rate parking service providers.

A number of works have addressed privacy-preserving reputation in participatory sensing applications. These works include those by Huang et al. [48], Wang et al. [89], and Michalas and Komninos [67]. These systems aim at computing the reputation scores of participating users while maintaining their anonymity.

In recent years, a notable number of reputation systems have been developed in the context of edge computing. In addition to the privacy-preserving systems discussed above in this survey, there are some non-privacy-preserving ones such as those by Hussain et al. [49], Rehman et al. [87], Xiao et al. [90], and Yaseen and Jararweh [92]. These systems primarily employ reputation management to discourage malicious behavior by user devices and edge nodes.

Several non-privacy-preserving reputation systems have also been recently proposed. Júnior [54] designs a reputation scoring system for data processors that reflects their conformance to the prevalent legal framework for processing of private personal data. Shahid et al. [83] present a blockchain-based reputation system in agri-food supply chain for the purpose of maintaining the credibility of the trading entities. Yahaya et al. [91] describe a system for matching Electric Vehicles (EVs) with charging stations based on location and reputation. Although the system protects EV location privacy, the reputation information appears to be shared on a blockchain in a non-private manner. Almasoud et al. [1] develop a system called FarMed that uses smart contracts and artificial intelligence for reputation computation. Zhou et al. [98] propose a blockchain-based decentralized reputation system for the e-commerce environment that resists unfair ratings and collusion, as well as incentivizes users to rate each other.