mathematics

MDPI

Article

ARS-Chain: A Blockchain-Based Anonymous Reputation-Sharing Framework for E-Commerce Platforms

Yungui Chen [1,2], Li Feng [3,*], Qinglin Zhao [3], Liwei Tian [1,2] and Lei Yang [1,2]

[1] School of Computer Science, Guangdong University of Science and Technology, Dongguan 523000, China; chenyungui@gdust.edu.cn (Y.C.); tianliwei@gdust.edu.cn (L.T.); yanglei@gdust.edu.cn (L.Y.)
[2] Faculty of Digital Science and Technology, Macau Millennium College, Macao SAR 999078, China
[3] School of Computer Science and Engineering, Faculty of Innovation Engineering, Macau University of Science and Technology, Macao SAR 999078, China; qlzhao@must.edu.mo
* Correspondence: lfeng@must.edu.mo

Abstract: E-commerce platforms incorporate reputation systems that allow buyers to rate sellers after transactions. However, existing reputation systems face challenges such as privacy leakage, linkability, and multiple rating attacks. The feedback data can inadvertently expose user information privacy because they reveal the buyers' identities and preferences, which deters a significant number of users from providing their ratings. Moreover, malicious actors can exploit data analysis and machine learning techniques to mine user privacy from the rating data, posing serious threats to user security and trust. This study introduces ARS-Chain, a pioneering and secure blockchain-driven anonymous reputation-sharing framework tailored for e-commerce platforms. The core of ARS-Chain is a dynamic ring addition mechanism with linkable ring signatures (LRS), where the number of LRS rings is dynamically added in alignment with the evolving purchase list, and LRS link tags are constructed with the LRS rings and item identifiers. Further, a consortium blockchain is introduced to store these anonymous ratings on e-commerce platforms. As a result, ARS-Chain ensures full anonymity while achieving cross-platform reputation sharing, making rating records unlinkable, and effectively countering multiple rating attacks. The experimental results confirm that ARS-Chain significantly enhances user information privacy protection while maintaining system performance, having an important impact on the construction of trust mechanisms for e-commerce platforms.

Keywords: user information privacy; data security; decentralized reputation system; blockchain; linkable ring signatures

MSC: 68Uxx

Citation: Chen, Y.; Feng, L.; Zhao, Q.; Tian, L.; Yang, L. ARS-Chain: A Blockchain-Based Anonymous Reputation-Sharing Framework for E-Commerce Platforms. *Mathematics* **2024**, *12*, 1480. https://doi.org/10.3390/math12101480

Academic Editor: Antanas Cenys

Received: 6 April 2024
Revised: 26 April 2024
Accepted: 6 May 2024
Published: 10 May 2024

1. Introduction

E-commerce is a prevalent feature of modern society, notably in countries like the United States and China, where it constitutes a significant portion of daily consumer purchases [1]. Mainstream e-commerce platforms incorporate reputation systems, which play a crucial role in guiding consumers' decision-making [2]. By enabling users to appraise and critique sellers upon their encounters, these systems provide invaluable perspectives on the quality of products and services. This nurtures trust and mitigates the ambiguities associated with virtual transactions. These assessments serve as instrumental aids for prospective purchasers. However, a notable challenge emerges. Sellers and buyers frequently maintain profiles on several platforms, and the absence of a holistic reputation system that amalgamates feedback from diverse sources hinders a comprehensive grasp of a seller's reliability. This cross-platform reputation synchronization deficit could compromise a consumer's capacity to make astute buying judgments [3]. Therefore, there is a need for a reputation-sharing system based on multiple platforms in the e-commerce industry.

In addition, existing reputation systems face challenges such as privacy breaches, linkability, and multiple rating attacks. Feedback data may unintentionally expose user information privacy as they reveal the buyer's identity and preferences, which can prevent a large number of users from providing their rating. Specifically, malicious actors can use data analysis and machine learning techniques to mine user's private information from rating data [4,5], posing a serious threat to user security and trust. For example, data analysts or hackers can use machine learning techniques to analyze rating data and purchase history, identify specific users' identities, and infer their purchasing preferences and consumption habits. Therefore, it is imperative to design a reputation system that achieves cross-platform reputation sharing while protecting user privacy.

A conventional approach in multi-platform reputation systems involves the deployment of a trusted third-party institution for managing users' reputation data, giving rise to numerous centralization-related issues. Centralized systems, prone to single-point-of-failure problems, are vulnerable to attacks and operational failures [6]. Furthermore, centralized systems' data and authority amalgamation may precipitate power misuse, censorship, and data leakage risks [7]. Simultaneously, the central node's processing capabilities limit the scalability and performance of centralized systems, thereby stunting system advancement [8]. In contrast, decentralized systems provide higher resilience, security, and transparency through distributed architecture [9].

Blockchain technology, specifically consortium blockchain, promises potential solutions to these issues with its inherent advantages in reputation sharing and privacy protection [10]. However, blockchain's anonymity does not guard against linkability and multiple rating attacks. The term "Linkability" refers to the possibility of malicious users linking two pieces of information based on historical rating data. "Multiple rating attacks" occur when a single purchase record is rated in an e-commerce system more than once [11].

1.1. Motivation

In mainstream e-commerce frameworks, enterprises' confidentiality is often compromised, necessitating the revelation of specifics like their business identity and location. With such transparency, consumers can make informed decisions and establish trust with merchants. However, ensuring consumers' privacy is paramount in online transactions. There is growing concern among consumers about the safety of their privacy data. This concern indicates that confidence in online shopping platforms could erode if adequate measures are not in place to protect their privacy. Such concerns are particularly pronounced within reputation mechanisms. Here, potential buyers rely on insights and feedback from previous customers to judge a seller's trustworthiness. If privacy is not maintained, consumers might hesitate to engage with these reputation systems or even refrain from transacting on the platform.

Unlinkability is a higher requirement for privacy protection. In Figure 1, Alice provides ratings after purchasing medications on platforms A and B. These ratings entered the e-commerce reputation system, assessing the seller's service and product quality. However, sellers and malicious actors may mine the potential associations of these ratings through manual or data analysis and machine learning methods. Consequently, consumers might worry about personal information security; people might choose silence and discontinue publishing their evaluations, weakening the e-commerce reputation system.

Given the above, our research aims to devise a solution addressing the following challenges:

Multi-platform Reputation Sharing: Our core objective is enabling reputation sharing across multiple e-commerce platforms. In today's segmented digital marketplace, consumers navigate various independent systems, each with unique reputation mechanisms. The absence of a standard reputation system makes it harder for sellers to build trust and complicates the buying process for consumers. We envisage a unified, comprehensive reputation management approach for multi-platform reputation sharing.

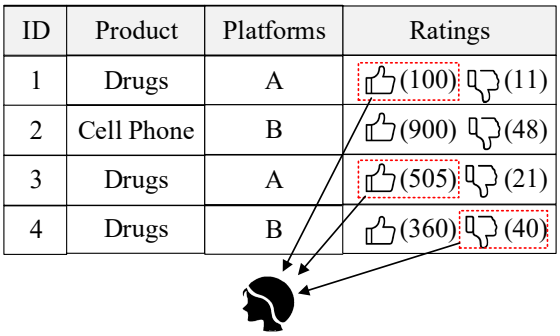

Figure 1. Malicious users can mine the potential associations of ratings through manual or data analysis and machine learning methods.

Full Anonymity and Rating Validity Verification: Full anonymity in the reputation system implies that the user's personal information remains anonymous to unrelated users, platform administrators, and sellers. Ensuring full anonymity presents a challenge to the validity of ratings: how can one ascertain the legitimacy of anonymous users?

Unlinkability: Unlinkability serves as a safeguard to protect users from potential exploitation. We aim to create a system that effectively prevents malicious entities from linking two different pieces of information (rating records) together using historical data, thus safeguarding users from potential targeted attacks.

Prevention of multiple rating attacks: Our system will prevent users from rating repeatedly upon the same purchase record, thereby avoiding the possibility of distorting reputation scores.

It is crucial to note that our architectural framework does not guarantee sellers' privacy. Buyers need access to sufficient information to assess the seller's reputation, mirroring real-world situations.

1.2. Contributions

We propose ARS-Chain, a multi-platform reputation-sharing system based on a consortium blockchain, to address the outlined challenges. E-commerce platforms act as blockchain nodes in ARS-Chain to maintain a distributed ledger through consensus mechanisms. Buyers remain anonymous to sellers, platform administrators, and other users during the evaluation process, utilizing a one-time pseudonym for each evaluation. The system provides unlinkability of evaluation records through one-time pseudonyms, allowing users to participate in evaluations with peace of mind. Furthermore, the system prevents users from repeating their evaluation behavior.

Our research contributes to the body of knowledge in the following ways:

(1) This research proposes ARS-Chain, a novel blockchain-based anonymous reputationsharing system for e-commerce platforms. It is designed to foster reputation sharing among multiple platforms, providing buyers with global reputation data regarding sellers.
(2) This research outlines the design of a new dynamic ring addition mechanism in the linkable ring signatures scheme where the quantity of rings dynamically increases over time. The dynamic ring addition mechanism reduces the LRS group size to a small scale. In addition, the link tags are meticulously constructed using rings and item identifiers. These combined enhancements enable ARS-Chain to achieve full anonymity, unlinkability of rating records, and to resist multiple rating attacks.
(3) This research also involved conducting validity and performance experiments to evaluate the system. The validity experiments demonstrate that ARS-Chain achieves its design goals of anonymity, unlinkability, and prevention of multiple rating attacks. The performance experiments show that the system performs well in terms of runtime, memory consumption, and network overhead under our dynamic ring addition mechanism.

2. Related Work

Early research on reputation systems centered on single-platform or centralized models. Blömer [12] leveraged group signatures in designing a reputation management system specific to a single platform. Bethencourt et al. [13] introduced a unique cryptographic primitive termed 'reputation signature'. The reputation signature allows for the efficient proof and verification of reputation without disclosing the user's identity. Zhai et al. [14] introduced 'AnonRep', a system that integrates cryptographic primitives like verifiable shuffle, linkable ring signatures, and homomorphic encryption to streamline reputation calculation, updating, and verification.

Many researchers introduce decentralized technology or blockchain technology to reputation management. PrivBox [15], a decentralized reputation system, harnesses homomorphic encryption and zero-knowledge proofs to safeguard user privacy during online transactions. It eliminates the need for trusted intermediaries or user groups in processing feedback scores.

Attempts have been made to design reputation-sharing systems suitable for specific scenarios. Grinshpoun et al. [16] unveiled models allowing users to migrate their reputation scores between virtual communities based on trust and similarity metrics. Shen et al. [17] constructed a training model for privacy-preserving support vector machines, allowing reputation score sharing without compromising user identity. Wang et al. [18] utilized blockchain for cross-domain reputation sharing, introducing personalized tags as quality indicators. In our previous work, RS-chain [19] used a trusted execution environment (TEE) to ensure reputation integrity during reputation-sharing processes. Despite these strides, existing solutions often neglect challenges like anonymity, unlinkability, and the threat of multiple rating attacks. RepChain [11] and this paper are the closest in addressing the issues mentioned above while focusing on reputation sharing across multiple platforms.

Researchers have looked into how blockchain-based applications can preserve user privacy. Comparing blockchain-based privacy protection reputation systems with traditional reputation systems, Hasan et al. [20] emphasized the benefits of the blockchain-based privacy-preserving reputation system, including its immutability, transparency, and trustlessness. X. Li et al. [21] presented a blockchain privacy protection system based on ring signatures. Utilizing ring signatures on elliptic curves, the author created a private data storage system that guarantees user identification and data security in blockchain applications. The BPP [22] combined blockchain and public key encryption techniques to achieve secure data sharing, data retrieval, and data access while ensuring the interests of users and the correctness of query results. Han et al. [23] introduced a privacy protection scheme for personal credit score calculation based on zero-knowledge proof, which considered the authenticity verification of multi-dimensional user data and proposed a universal verification platform based on blockchain. Wu et al. [24] proposed an efficient and privacy-preserving traceable attribute-based encryption scheme, which used blockchain technology to ensure the integrity and non-repudiation of data. Casino and Patsakis [25] used a decentralized locality-sensitive hashing classification and a series of recommendation methods to improve the efficiency and accuracy of the reputation system. These studies provided us with inspiration for designing a blockchain-based reputation-sharing framework in terms of privacy protection. However, these works did not address the issue of reputation sharing in multi-platform e-commerce scenarios, which is the main focus of our work.

Our work aims to design a reputation-sharing framework across multiple platforms, providing support for decentralization, anonymity, unlinkability of ratings, and prevention of multiple rating attacks. As shown in Table 1, most existing works only focus on a subset of the design goals. RepChain [11] is the closest to our work, but RepChain uses a combination of techniques such as blind signatures, zero-knowledge range proofs, secure multi-party computation, and consensus hashing, which is far more complex than our work.

Table 1. Brief comparison of repchain and existing work.

Property	Existing Work
Decentralization	[11,15,18–25]
Anonymity	[11–15,17,20,21,23,24]
Unlinkability of Ratings	[11,14]
Prevention of Multiple Rating Attacks	[11,14]
Multi-platform Support	[11,16–19,22]

3. Preliminaries

This section briefly revisits two pivotal technologies: consortium blockchain and linkable ring signatures.

3.1. Consortium Blockchain

A consortium blockchain [26] is a semi-decentralized blockchain architecture maintained by a selected group of nodes, typically organizational or corporate entities, regulated through strict permission controls. Compared to public blockchains, consortium blockchains are suitable for scenarios requiring high trust and permission management, such as supply chain management, financial services, and cross-organizational data exchange. Consortium blockchain F can be defined as an ordered triplet $F = (N, T, P)$, where:

N encapsulates the ensemble of nodes within the network.

T represents the aggregation of transactions.

P denotes a set that spells out permissions or governing rules.

Given its semi-decentralized essence, consortium chains are particularly apt for applications like supply chain management, financial services, and cross-organizational data exchange, aligning seamlessly with the objectives of this research. Within the realm of consortium blockchains, Byzantine Fault Tolerance (BFT) or its pragmatic variant, Practical Byzantine Fault Tolerance (PBFT), often emerge as the consensus algorithms of choice [27].

3.2. Linkable Ring Signatures

Linkable ring signatures (LRS) [28,29] are a fascinating cryptographic scheme that enables users to sign anonymously yet traceably. This system endows a user with the capability to append an anonymous signature amidst a set of users (i.e., a "ring"), all the while ensuring that a singular user does not produce multiple distinct signatures. Unlike classical ring signatures [30], linkable variants possess a salient attribute: should a user sign the same information multiple times, these signatures can be intricately linked. In this work, buyers use LRS to sign ratings when evaluating sellers or products, and the verifiers (sellers or other users) cannot identify the signer from the signature, thus protecting the signer's privacy. Additionally, if the signer makes two ratings based on the same purchase, the second rating will be recognized by the verifier and discarded by the system. LRS primarily includes the following four algorithms:

1. Key Pair Generation Algorithm: A key pair, delineated as (SK, PK), is composed of a private key, SK, intertwined with its public counterpart, PK.

$$(SP, PK) \leftarrow KeyGen() \tag{1}$$

where $KeyGen()$ is the cryptographic key-generating function.

2. Signature Generation Algorithm: As a ring member, a signer orchestrates the signing operation.

$$\sigma \leftarrow Sign(SK, R, m, T) \tag{2}$$

wherein:

σ stands as the signature.

SK is the signer's private key.

R is the ring, characterized by n public keys $\{PK_1, PK_2, \ldots, PK_n\}$.
m is the message awaiting its signature.
T is the link tag.
Sign() functions as the signing procedure.

3. Signature Verification Algorithm: The outcome of the signature verification function can either be 1, signifying the legitimacy of the signature and the signer's membership in the ring, or 0, denoting its rejection.

$$0 \mid 1 \leftarrow Verify(\sigma, R, m, T) \tag{3}$$

4. Linkability Verification Algorithm: The *Link()* function, assessing linkability, ingests two signatures, σ_1 and σ_2, and exudes a Boolean output, indicating whether these signatures come from the same signer and are based on the same link tag.

$$0 \mid 1 \leftarrow Link(\sigma_1, \sigma_2) \tag{4}$$

4. ARS-Chain Overview

This section presents the system architecture, threat model, and security assumptions.

4.1. System Architecture

ARS-Chain is a reputation-sharing framework designed for multiple e-commerce platforms, consisting of two parts: e-commerce platforms and blockchain, as shown in Figure 2.

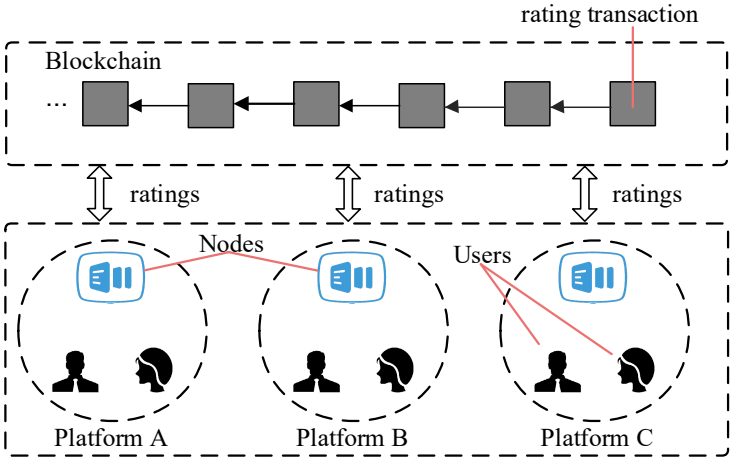

Figure 2. System architecture of ARS-Chain.

The platforms are e-commerce websites that join the ARS-Chain framework, such as Amazon. They provide online services for consumers and merchants. In order to provide more comprehensive reputation queries for users, the e-commerce platforms apply to join the ARS-Chain reputation system from a certificate authority (CA). The CA is an e-commerce business association jointly created by all platforms. The CA generates system parameters and encryption keys for users and platforms.

Users: In ARS-Chain, users are categorized into two main groups: buyers and sellers. Acting as the raters, the buyers enjoy the cloak of privacy conferred by the system. Conversely, the sellers, acting as the ratees, have openly disclosed information. In the ARS-Chain ecosystem, both buyers and sellers have the latitude to navigate freely among multiple platforms. Buyers furnish the system with evaluative feedback concerning the sellers.

Rating: Upon receipt of the merchandise, the buyer finalizes his seller rating. The rating should be a real number between a range [low, high], for the sake of conciseness in this study, dichotomized into two distinct values: "+1" or "−1". After formulating this

assessment, the buyer employs the linkable ring signatures methodology to sign the ratings. These signed messages are then dispatched to the proximate node in the system.

Blockchain Network Configuration: The blockchain in ARS-Chain is a consortium chain, similar to Hyperledger Fabric [31], maintained by several e-commerce platforms. Each block stores rating transactions in the system.

Nodes: Constituted by servers from various platforms, nodes are vested with the responsibility of aggregating ratings uploaded by buyers, and they also participate in the blockchain consensus mechanism. During the consensus-building phase, each node has the potential to become a consensus node. Consensus nodes are tasked with the duty of block packaging. It should be noted that, in order to ensure the security of the consortium blockchain, it is usually required that at least a sufficient number of consensus nodes participate in the consensus process. Considering this, an e-commerce platform needs to provide multiple servers as blockchain nodes.

Consensus protocol: In alignment with industry consensus, as cited in [27], ARS-Chain adopts the Practical Byzantine Fault Tolerance Algorithm (PBFT) as its consensus protocol.

Rating transactions: The nodes use the signature verification algorithm and the linkability verification algorithm of the linkable ring signature to verify the ratings. The ratings that pass the verifications are valid, called rating transactions, which will be packaged into the blockchain.

4.2. Threat Model and Assumptions

The adversaries in the system encompass troublemakers, malicious sellers, malicious buyers, and platform administrators.

(1) Troublemakers: These entities possess an inherent desire to trace sensitive data from other users, such as purchase records of buyers and evaluative feedback given to sellers, and subsequently link these bits of information together.

(2) Malicious Sellers: Upon receipt of negative reviews, these sellers become increasingly inquisitive about the source, prompting them to transform into system adversaries in their quest for identification.

(3) Malicious Buyers: Motivated by excessive admiration or significant disapproval, such buyers might submit redundant ratings.

(4) Platform Administrators: There exists a potential for platform stewards to compromise sensitive platform data for monetary gains [32,33]. While platform investors find such actions deeply concerning, regrettably, these occurrences are not uncommon in reality.

ARS-Chain stands as a system that fosters reputation sharing across multiple platforms. In this ecosystem, the accounts of ratees (sellers) across varying platforms should possess linkability. We postulate that sellers must employ uniform metadata for the registration process when they register on diverse platforms. For corporate sellers, their official registration certificate is deemed viable. ARS-Chain commits to protecting buyer-centric information, sidelining seller privacy—a stance harmonious with prevailing e-commerce platform conventions. We assume that cryptographic tools such as hash functions, key distribution, and signature schemes are secure, and the protection of these tools is beyond the scope of this study. Further, we believe that users are adept at safeguarding their private keys while their public counterparts can be freely disclosed.

5. ARS-Chain System Design

In this section, we elucidate the intricacies of the ARS-Chain system design, encompassing the dynamic ring addition LRS Scheme, link tag construction, and the system's operational workflow.

5.1. Dynamic Ring Addition Mechanism

We propose a dynamic ring addition mechanism for the LRS scheme in the ARS-Chain. The scheme entails dynamically constructed rings to provide buyers anonymity while forestalling duplicate ratings and ensuring execution efficiency. Under this scheme,

buyers are orchestrated into a ring of size n, predicated on their purchasing sequence. As illustrated in Figure 3, each signature ring should comprise j consensus nodes, one buyer, and k sellers. When a buyer acts as a signer to rate a review, the other members in the ring become verifiers of the signature. The ring R can be articulated as follows:

$$R_i^{item\_id} = \{PK_{i1},\ PK_{i2}, \ldots, PK_{ik}, PK_{item\_id}\} \cup CN \tag{5}$$

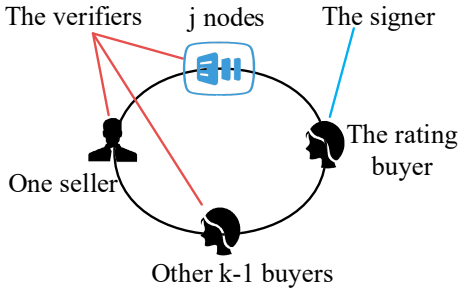

Figure 3. Composition of signature rings in ARS-Chain.

Herein, *item_id* denotes the item number, i represents the ith signature ring under the item number *item_id*, PK_{item_id} is the public key of the seller of the item numbered *item_id*, and the set $\{PK_{i1}, PK_{i2}, \ldots, PK_{ik}\}$ encompasses the public keys of the k buyers of the item numbered *item_id*. CN represents a collection of the consensus nodes' public keys, defined as follows:

$$CN = \{PK_{N1},\ PK_{N2}, \ldots, PK_{Nj}\} \tag{6}$$

The consensus nodes are j nodes $\{N1, N1, \ldots, Nj\}$.

The dynamic ring addition LRS scheme, as illustrated in Figure 4, shows that with n = 100 and j = 10, the number of buyers within the ring, denoted as k, is evaluated as $k = n - j - 1 = 89$. In this model, the purchasers of the item numbered *item_id* are allocated into distinct signature rings based on the purchase order: buyers 1 to 89 formulate ring 1, buyers 90 to 178 formulate ring 2, and so on. The benefit of the dynamic ring addition LRS scheme is that it divides large-scale e-commerce transactions into smaller signature rings, thereby reducing the computational overhead within the ring.

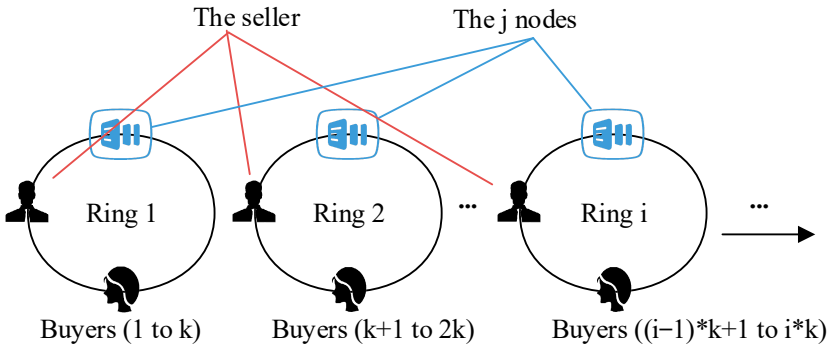

Figure 4. Dynamic ring addition LRS scheme.

5.2. Link Tag Construction

Link tag [29,34] in LRS addresses issues within ring signatures, such as double-spending or repeated signing. The system can identify whether the same entity has signed multiple times by employing link tags, thereby thwarting malicious activities. The computation formula for the link tag is delineated as follows:

$$Link\ tag = hash\left(R_i^{item\_id} \middle| item\_id\right) \tag{7}$$

where $R_i^{item\_id}$ is a collection of public keys from n members as defined in Section 5.1, and *item_id* denotes the item identifier. The *item_id* is constituted of the platform name and an internal number. For instance, the *item_id* for a product with ASIN code "*B08L8KC1J7*" on Amazon can be represented as "*Amazon-B08L8KC1J7*". The ASIN code is a unique identifier generated for each product by Amazon, autonomously created by the Amazon system without the need for seller input. The uniqueness of $R_i^{item\_id}$ and *item_id* culminates in the uniqueness of the link tag, wherein the system will detect multiple signatures under the same *item_id* by the same entity.

Regarding cases of repurchase, as long as the time interval between two purchases is sufficiently long, the buyer will appear in two distinct rings for the same item. Due to the difference in link tag, both ratings will still be regarded as valid by the LRS system. An extreme scenario is when a buyer purchases the same item twice within a short time and can only provide one rating.

5.3. Workflows

As illustrated in Figure 5, the ARS-Chain system's workflows encompass a collection of sub-processes involving multiple stakeholders, including buyers, sellers, and consensus nodes.

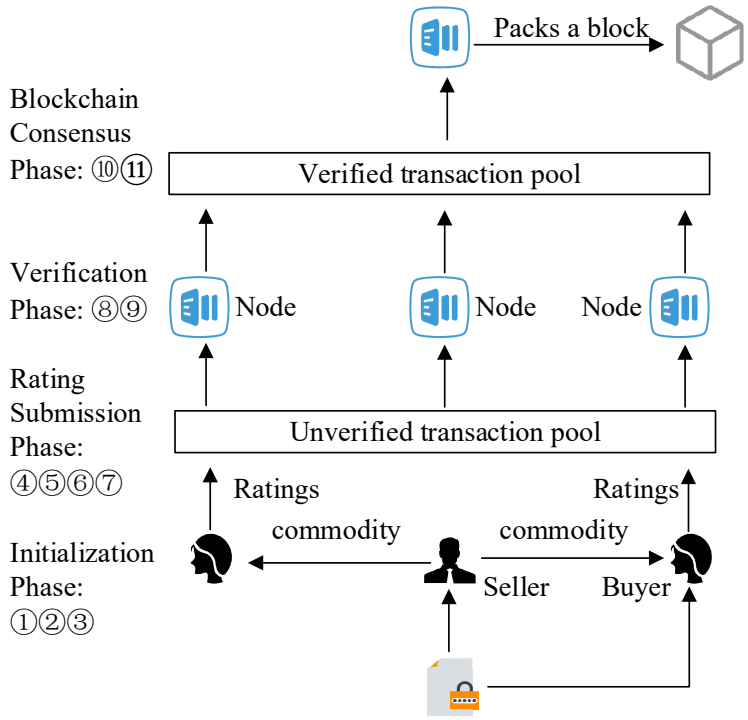

Figure 5. The ARS-Chain's workflows.

Initialization Phase:

① Key Generation: Each buyer x generates a pair of private and public keys (SK_x, PK_x) based on the the *KeyGen()* algorithm.

② Dynamic Ring Formation: The system constructs a ring $R_i^{item\_id}$ for the product identified by *item_id*, where *i* is the ring identifier. According to the definition in Section 5.1, the ring $R_i^{item\_id}$ consists of *k* buyers, *j* consensus nodes, and a seller.

③ Generation of One-time Pseudonyms: One-time pseudonyms are meaningless to the members within the ring and do not serve as inputs for the *Verify()* and *Link()* functions. The one-time pseudonym acts as a part of the rating information *m* to identify the rater, denoted as "*from*". Its calculation method is as follows:

$$from = hash(PK_x|timestamp) \quad (8)$$

Rating Submission Phase:

④ Rating Creation: Upon receipt of the product, the buyer generates the rating m.

⑤ Link Tag Construction: The buyer utilizes $R_i^{item\_id}$ and *item_id* to generate the link tag (T).

$$T = hash\left(R_i^{item\_id} \middle| item\_id\right) \tag{9}$$

⑥ Signing: Buyer x employs private key SK_x, $R_i^{item\_id}$, and T to sign the rating m. T will be used as part of the signature data structure for future verification.

$$\sigma \leftarrow Sign\left(SK_x, R_i^{item\_id}, m, T\right) \tag{10}$$

⑦ Transaction Upload: The buyer uploads the transaction TX to the attached blockchain nodes. At this time, the transactions have not been verified by the nodes, and are placed into the local unverified transaction pool by the nodes. TX is the data format after m has been signed, represented as:

$$TX = (item\_id, i, m, \sigma) \tag{11}$$

Verification Phase:

⑧Transaction Legitimacy Verification: The consensus nodes verify the legitimacy of the collected transaction TX. A return of 1 from *Verify()* indicates the signature's legitimacy, passing the verification.

$$0|1 \leftarrow Verify\left(TX.\sigma, TX.m, R_i^{item\_id}, item\_id\right) \tag{12}$$

⑨Transaction Linkability Check: According to $TX.item\_id$ and $TX.i$, the consensus nodes scan all rating transactions generated based on the same $R_i^{item\_id}$, executing *Link()* to check the linkability of TX with other transactions.

$$0\,|\,1 \leftarrow Link(TX\_now.\sigma, TX\_others.\sigma) \tag{13}$$

Here, *TX_now* represents the transaction to be checked, while *TX_others* represents other rating transactions generated based on the ring $R_i^{item\_id}$. A consistent return of 0 from all calls to *Link()* indicates no repeated ratings by the same user under the same link tag, passing the check.

Blockchain Consensus Phase:

⑩Transaction Broadcast: Transactions that pass *Verify()* and *Link()* are regarded as legitimate transactions, placed into the transaction pool, and then broadcasted to other peers.

⑪ Block Generation and Linkage: Consensus nodes, adhering to the PBFT consensus protocol, reach a consensus to package the rating transactions into a new block and append the new block to the end of the blockchain. At this juncture, the seller's reputation score is updated, and the buyers view the reputation score based on multi-platform global data.

6. Validity Analysis

This section analyzes whether the ARS-Chain system meets the design goals we proposed in Section 1.1.

Multi-platform Reputation Sharing: ARS-Chain achieves this goal by storing reputation data in a consortium blockchain maintained by multiple platforms.

Full Anonymity and Evaluation Validity Verification: ARS-Chain uses linkable ring signature technology to achieve the signer's anonymity to the seller, platform administrators, and other members within the ring. In addition, as shown in Section 5.3, the system generates a one-time pseudonym for the user during the initialization phase. This helps to achieve the signer's anonymity to outsiders. We conducted validity experiments in Section 7.2 to test this design goal.

Unlinkable Rating Records: ARS-Chain ensures that the identity presented by the user in each rating is different by introducing one-time pseudonyms, thus ensuring that rating records are unlinkable. It should be noted that the linkability in LRS and the unlinkability in our design goals are not contradictory. The unlinkability in the design goals refers to the unlinkability between two different purchase records, while the linkability in LRS refers to the linkability between two ratings of the same purchase record.

Preventing Multiple Rating Attacks: ARS-Chain achieves this goal through our novel dynamic ring addition LRS scheme and link tag construction method. As shown in Table 2, two legitimate ratings are based on different link tags. Conversely, two ratings based on the same link tag will be considered as multiple rating attacks. When the system detects repeated ratings, the second rating will be discarded. In addition, the experiments (Section 7.2) shows that ARS-Chain effectively prevents multiple rating attacks.

Table 2. The value of the link tag(T) based on different rating situations.

Situation	$R_i^{item\_id}$ and *item_id*	Link Tag (T)
two ratings based on different products	different $R_i^{item\_id}$ / different *item_id*	different T
two ratings based on repurchase records	different $R_i^{item\_id}$ / same *item_id*	different T
two ratings based on a purchase record	same $R_i^{item\_id}$ / same *item_id*	same T

Preventing Multiple Rating Attacks: ARS-Chain achieves this goal through our novel dynamic ring addition LRS scheme and link tag construction method. As shown in Table 1, two legitimate ratings are based on different link tags. Conversely, two ratings based on the same link tag will be considered as multiple rating attacks. When the system detects repeated ratings, the second rating will be discarded. In addition, the experiments (Section 7.2) shows that ARS-Chain effectively prevents multiple rating attacks.

Sybil attacks: In ARS-Chain, the blockchain stores reputation information and does not compete for control over user accounts with e-commerce platforms. We assume that e-commerce platforms can resist Sybil attacks through measures such as real-name authentication, and ARS-Chain is responsible for anonymizing real-name accounts during the process of reputation data being put on the blockchain.

7. Experiments and Evaluation

The primary algorithms encompassed within the framework of LRS consist of three pivotal components: signature generation, signature verification, and linkability verification. To assess the performance metrics of these algorithms, we conducted empirical evaluations in three areas: runtime, memory consumption, and signature size. Both runtime and memory consumption are indicative parameters for gauging the computational burden imposed on user hardware. The signature constitutes a seminal factor contributing to blockchain network communication overhead. Recognizing that the performance of LRS is intricately correlated with the LRS group size, our experimental framework was judiciously executed under both large-scale (100–5000 members) and small-scale (<100 members) LRS group sizes. It should be pointed out that the dynamic ring addition LRS scheme described in Section 5.1 transforms the large-scale group size LRS, corresponding to large-scale e-commerce transactions, into small-scale group size LRS, corresponding to small-scale e-commerce transactions. In actuality, the LRS within ARS-Chain operates under the small-scale group size condition.

7.1. Experimental Setup

Parameters Configuration. Unsigned blockchain transactions (the rating from buyer to seller) are delineated as follows:

const m = {
timestamp: "May-19-2023 08:17:35 AM +UTC",

from: "0x1114c78d5de672996d812dc2e1a05b5f33eacdfb",
to: "0x000000d40b595b94918a28b27d1e2c66f43a51d3",
value: "+1"
};

In this structure, the "timestamp" signifies the initiation time of the blockchain transaction, which concurrently serves as the moment at which the buyer rates the seller. The "from" field represents the rater's one-time pseudonym. Adopting this one-time pseudonym obfuscates the evaluator's identity, impeding malicious actors from tracking evaluations. Furthermore, the 'to' field distinctly identifies the seller, while the 'value' parameter denotes the appraisal score. Given the structural confines of our model, this score is rigorously limited to the binary choices of "+1" or "−1".

The item identifier is configured as a string similar to "*Amazon-B08L8KC1J7*", representing a product from Amazon.

Hardware Specifications. For the empirical analysis, we conducted our experiments on a machine equipped with an Intel® Core™ i5-7300HQ CPU @ 2.50 GHz, 8.0 GB of memory, running Windows 10.

Experimental Framework. Our experimental framework is implemented in two programming languages, PureScript and JavaScript, each catering to distinct aspects of the LRS algorithm. More specifically, the framework is partitioned into the following modules: (1) PureScript Component: This segment takes on the onus of actualizing the core logic of the LRS algorithm, encompassing key pair generation, message signing, signature verification, and linkability verification. The code for this module is encapsulated in approximately 300 lines of PureScript statements and further augmented by a plethora of PureScript library references. (2) JavaScript Component: This section serves as interface calls and benchmarking. The JavaScript component consists of about 400 lines of code.

7.2. Validity Experiments

As described in Section 1.1, the design goal of ARS-Chain is to achieve anonymity, unlinkability and prevent multiple rating attacks while sharing reputation across multiple platforms. We introduce the validity experiments in this section.

In LRS, *Verify()* returns "*true*" to indicate that the signature is valid, i.e., the signer belongs to the signature ring, and *Link()* returns "*true*" to indicate that the two signatures are signed by the same signer under the same link tag, i.e., the system detects that the user rated multiple times. As shown in Table 3, ARS-Chain correctly judged the legitimacy of the users and successfully detected the multiple ratings. When the system detects multiple ratings, the second rating will be discarded, thus avoiding the multiple rating attack. The experiments show that ARS-Chain effectively achieves legitimacy verification and prevents multiple rating attacks.

Table 3. Results of *Verify()* and *Link()* based on different rating situations.

Situation	Results of *Verify()*	Results of *Link()*
Legal and illegal users rate the same product	First signature: true Second signature: false	Linkability of two signatures: false
A legal user rates the same product twice	First signature: true Second signature: true	Linkability of two signatures: true
A legal user rates two different products	First signature: true Second signature: true	Linkability of two signatures: false
Different legal users rate the same product	First signature: true Second signature: true	Linkability of two signatures: false

7.3. Performance Evaluation under Large-Scale LRS Group Size

The numbers of participants (n) in experiments under the large-scale LRS group size are 100, 200, 400, 800, 1200, 1600, 2400, 3200, and 5000, respectively.

The runtimes of signature generation, signature verification, and linkability verification algorithms increase with the number of participants, exhibiting an approximately linear relationship, as shown in Figure 6. The runtimes of signature generation and verification are very close to each other and much larger than the runtimes of linkability. This indicates that signature generation and verification processes involve more computation, while the linkability verification algorithm is relatively simple.

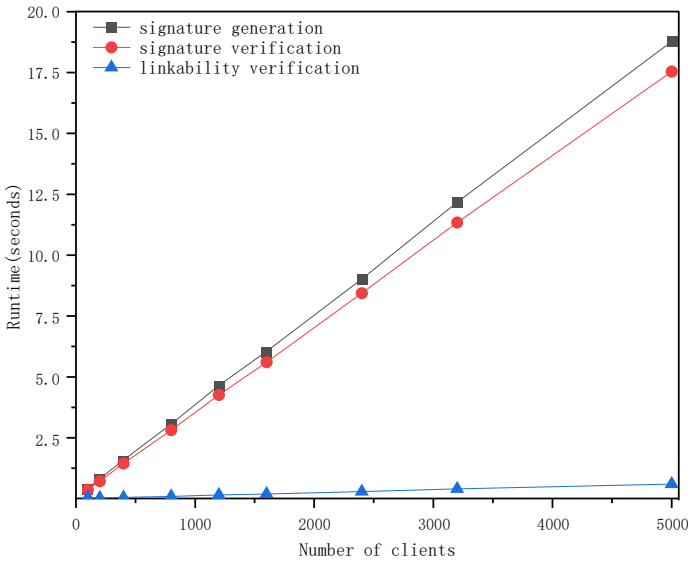

Figure 6. Algorithm runtime with different numbers of participants.

As can be discerned from Figure 7, several noteworthy patterns emerge in memory consumption across the three algorithms. In the signature generation algorithm, memory usage escalates as the number of participants increases; however, the trajectory of this increase does not strictly adhere to a linear pattern. In stark contrast, the memory utilization for the signature verification algorithm demonstrates considerable fluctuation across varying participant counts, defying any conspicuous systematic trend. For the linkability verification algorithm, it is apparent that the memory overhead is markedly lower compared to the other two algorithms, an attribute that may be due to its relative algorithmic simplicity.

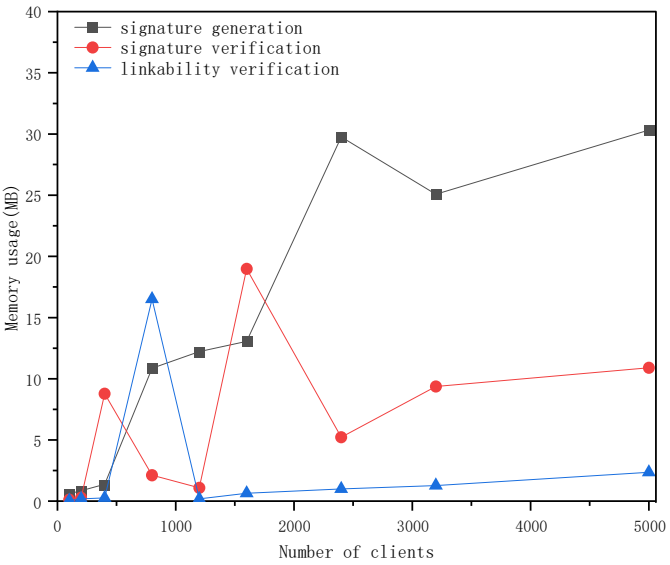

Figure 7. Algorithm memory consumption with different numbers of participants.

Viewed holistically, the hierarchy of memory consumption from highest to lowest aligns well with the algorithms' inherent code complexities. It is sequenced as follows: signature generation, signature verification, and linkability verification. Additionally, each algorithm manifests episodic spikes in memory usage, which are subsequently followed by a decrement. This oscillatory behavior could potentially be correlated with the garbage collection and optimization mechanisms intrinsic to the node.js runtime environment.

The signature constitutes a seminal factor contributing to blockchain network communication overhead. Figure 8. shows a linear correlation between the signature size (y) and the number of participants (n). Mathematically, the best-fit function for the signature size (y) and the number of participants (n) can be expressed as follows:

$$y = 0.1884 * n + 0.3808 \tag{14}$$

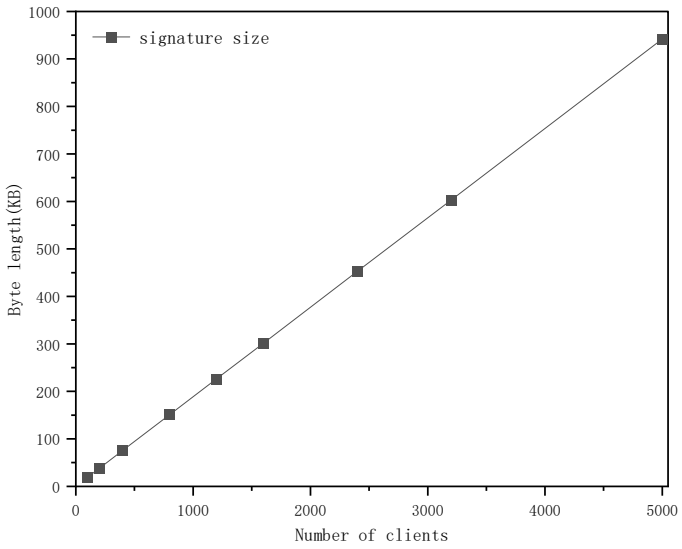

Figure 8. Signature size with different numbers of participants.

Given these findings, managing the number of ring participants is necessary to ensure operational efficiency.

7.4. Performance Evaluation under Small-Scale LRS Group Size

In light of the observations presented in Section 7.3, it becomes evident that large-scale LRS group size not only elongates the algorithm's runtime but also inflates the communication overhead within the blockchain network. As a direct countermeasure, we introduce the dynamic ring addition mechanism described in Section 5.1. The dynamic ring addition mechanism reduces the LRS group size to a small scale. In this section, we test the system performance when the LRS group size is small (less than 100).

Table 4 unequivocally elucidates that when the group size is curtailed to under 100, the signature size and the algorithmic runtime exhibit an incremental ascent in correlation with increasing group size. Although memory consumption generally trends upwards, it demonstrates a degree of irregularity, potentially attributable to the idiosyncrasies of the runtime environment's memory garbage collection mechanisms. With a group size restricted to fewer than 100, all 3 performance metrics remain within the bounds of reduced overhead. Considering the ubiquitous flood-fill propagation characteristic inherent in blockchain systems, it is necessary to limit the byte size of transactions to be sufficiently small. We surmise that fixing the group size to less than 50 is optimal.

Table 4. Performance metrics correlation with group size under 100.

Group Size	Signature Size (KB)	The Runtime of Sign() (s)	The Runtime of Verify() (s)	The Runtime of Link() (s)	Memory Usage of Sign() (MB)	Memory Usage of Verify() (MB)	Memory Usage of Link() (MB)
10	2.25	0.0783	0.0521	0.0017	0.6633	0.4267	0
20	4.14	0.1172	0.0827	0.0029	0.32	0.0833	0
30	6.03	0.1503	0.1186	0.0041	0.2067	0.09	0
40	7.91	0.1909	0.1535	0.0054	0.33	0.1367	0.0267
50	9.79	0.2273	0.1859	0.0067	0.3967	0.13	0.0167
60	11.68	0.2687	0.2215	0.0082	0.3533	0.0867	0.02
70	13.56	0.3113	0.257	0.009	0.52	0.0967	0.02
80	15.44	0.3443	0.291	0.0101	0.5267	0.0967	0.03
90	17.32	0.3841	0.3308	0.0115	0.5967	0.1233	0.0367
100	19.2	0.4217	0.3627	0.013	0.6067	0.12	0.0467

8. Discussion

8.1. Waiting Time for LRS Ring Generation

As discussed in Section 5.1, the generation of a signature ring is based on the buyer list of a particular commodity, which includes one seller, j consensus nodes, and k buyers. The ring generation time will correspondingly increase when the commodity is less prevalent.

We denote $h_{\mathrm{i}}(t)$ as the popularity of the ith commodity at time t, where the popularity of a commodity is generally an indicator of its appeal or sales velocity. $T(h_{\mathrm{i}})$ represents the time required for this commodity to form a LRS ring independently. We can infer that there exists a functional relationship between $T(h_{\mathrm{i}})$ and $h_{\mathrm{i}}(t)$, as follows:

$$T(h_{\mathrm{i}}) = \frac{a}{h_{\mathrm{i}}(t) + b} \tag{15}$$

In situations where the popularity of a single commodity is insufficient to form a LRS ring within a reasonable time frame, we consider combining the buyers of N commodities to form a LRS ring. Assuming H(t) represents the total popularity of these N commodities at time t, then:

$$T(H(t)) = \frac{a}{\sum_{i=1}^{n} h_{\mathrm{i}}(t) + b} \tag{16}$$

This approach will significantly reduce the waiting time for forming a LRS ring.

8.2. Performance Optimization

In Section 7, performance experiments were conducted regarding the LRS group size under large-scale and small-scale scenarios. The experimental results show that the algorithms' runtime and signature size exhibit a linear relationship with the group size. Thanks to the dynamic ring addition mechanism (described in Section 5.1), ARS-Chain achieves the optimal state of runtime and memory consumption by increasing the number of rings, but the signature size is still the bottleneck of the system. We propose the following methods to address the issue of excessive signature size:

1. SBFT Consensus Protocol: SBFT [35] protocol adopts threshold signature technology and collector technology, modifying P2P broadcasting across the network to message collection through a collector. Once the collector collects a certain number of signatures, aggregation is performed, followed by the dissemination of the aggregated signature by the collector, thereby reducing the message complexity to a polynomial level. The SBFT protocol effectively addresses the issue of oversized signatures, significantly reducing network communication overhead.

2. Optimized Signature Size LRS: Beullens et al. [36] proposed a logarithmic-size LRS, while Subhra Mazumdar et al. [37] introduced a constant signature size LRS. These variants provide technical support for LRS with a large number of members.

8.3. Technical and Economic Barriers That May Be Encountered during Integration

In the process of integrating ARS-Chain with existing e-commerce platforms, we are facing several technical challenges and economic barriers. Firstly, the scalability issue of blockchain is a key factor. Currently, the transaction processing speed of ARS-Chain may not meet the demands of large-scale e-commerce platforms, and sharding technology [38] could be a solution. Sharding divides the blockchain network into multiple smaller segments, each handling a portion of transactions, thereby improving the overall processing speed. Additionally, when integrating ARS-Chain, we must also consider economic barriers. This includes the initial technological investment, operational costs, and potential market resistance. To overcome these barriers, we propose the following: (1) Establishing partnerships with e-commerce platforms to jointly develop and maintain ARS-Chain, sharing the costs. (2) Reducing operational costs by enhancing the efficiency of ARS-Chain and minimizing resource consumption. (3) Through flexible design, enabling ARS-Chain to adapt to e-commerce platforms of different scales and needs, enhancing market competitiveness.

9. Conclusions and Future Work

This paper proposes ARS-Chain, a blockchain-based anonymous reputation-sharing system for e-commerce platforms. ARS-Chain utilizes a novel dynamic ring addition mechanism in the LRS scheme where the number of LRS rings increases over time based on the purchase list. In addition, we propose a practical method for constructing link tags with the LRS rings and item identifiers.

ARS-Chain addresses the critical challenges of enabling reputation sharing across platforms while protecting buyers' privacy through anonymity and unlinkability of ratings. It prevents multiple rating attacks through the link tag mechanism. The experimental results confirm that ARS-Chain achieves its design goals, and the dynamic ring addition mechanism ensures the system's performance.

The anonymous reputation systems have profound impacts on both social and ethical levels. Socially, they can promote more honest and transparent communication, but may also lead to a lack of accountability and misuse. Ethically, such systems could affect individual privacy rights and fairness. Therefore, future research should focus on how to balance anonymity with a sense of responsibility, ensuring that the design and implementation of these systems protect users' rights while promoting the overall well-being of society.

For future work, we plan to extend our framework to support more complex and diverse reputation models, such as multi-dimensional, multi-faceted, and multi-level reputation. We also intend to explore the possibility of applying our framework to other domains that require anonymous and secure data sharing, such as healthcare, social networks, and IoT. Furthermore, we aim to conduct more comprehensive experiments and evaluations to demonstrate the effectiveness and efficiency of our framework in real-world scenarios.

Author Contributions: Conceptualization, Y.C., L.F. and Q.Z.; methodology, Y.C. and L.F.; software, Y.C. and L.F.; validation, Y.C., L.T. and L.Y.; formal analysis, Y.C. and Q.Z.; investigation, Y.C., Q.Z. and L.F.; resources, Y.C. and L.F.; writing—original draft preparation, Y.C. and Q.Z.; writing—review and editing, L.F., L.T. and L.Y.; supervision, L.F. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Key Research and Development Program of China (2023YFB2703800) and the Science and Technology Development Fund, Macau SAR (0093/2022/A2, 0076/2022/A2, and 0008/2022/AGJ), Department of Education of Guangdong Province (2021ZDZX1075, 2022ZDJS146), Guangdong University of Science and Technology (GKY-2022KYZDK-12, GKY-2022CQTD-4).

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Statista-Research-Department. E-Commerce in the United States—Statistics & Facts. 2023. Available online: https://www.statista.com/topics/2443/us-ecommerce/ (accessed on 15 March 2024).
2. Huang, N.; Sun, T.; Chen, P.-Y.; Golden, J. Social Media Integration and E-Commerce Platform Performance: A Randomized Field Experiment. 2017. Available online: https://ssrn.com/abstract=2969670 (accessed on 15 March 2024).
3. He, Y.; Zhang, C.; Wu, B.; Yang, Y.; Xiao, K.; Li, H. A cross-chain trusted reputation scheme for a shared charging platform based on blockchain. *IEEE Internet Things J.* **2021**, *9*, 7989–8000. [CrossRef]
4. Nassar, A.; Kamal, M. Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. *J. Artif. Intell. Mach. Learn. Manag.* **2021**, *5*, 51–63.
5. Sabir, B.; Ullah, F.; Babar, M.A.; Gaire, R. Machine learning for detecting data exfiltration: A review. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–47. [CrossRef]
6. Huang, J.; Kong, L.; Dai, H.-N.; Ding, W.; Cheng, L. Blockchain-based mobile crowd sensing in industrial systems. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6553–6563. [CrossRef]
7. Allen, S.; Čapkun, S.; Eyal, I.; Fanti, G.; Ford, B.A.; Grimmelmann, J.; Juels, A.; Kostiainen, K.; Meiklejohn, S.; Miller, A. *Design Choices for Central Bank Digital Currency: Policy and Technical Considerations*; National Bureau of Economic Research: Cambridge, MA, USA, 2020.
8. Nasir, M.H.; Arshad, J.; Khan, M.M.; Fatima, M.; Salah, K.; Jayaraman, R. Scalable blockchains—A systematic review. *Future Gener. Comput. Syst.* **2022**, *126*, 136–162. [CrossRef]
9. Asante, M.; Epiphaniou, G.; Maple, C.; Al-Khateeb, H.; Bottarelli, M.; Ghafoor, K.Z. Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Trans. Eng. Manag.* **2021**, *70*, 713–739. [CrossRef]
10. Xu, M.; Chen, X.; Kou, G. A systematic review of blockchain. *Financ. Innov.* **2019**, *5*, 27. [CrossRef]
11. Li, M.; Zhu, L.; Zhang, Z.; Lal, C.; Conti, M.; Alazab, M. Anonymous and verifiable reputation system for E-commerce platforms based on blockchain. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 4434–4449. [CrossRef]
12. Blömer, J.; Juhnke, J.; Kolb, C. Anonymous and publicly linkable reputation systems. In Proceedings of the Financial Cryptography and Data Security: 19th International Conference, FC 2015, San Juan, Puerto Rico, 26–30 January 2015; Revised Selected Papers; pp. 478–488.
13. Bethencourt, J.; Shi, E.; Song, D. Signatures of reputation. In Proceedings of the Financial Cryptography and Data Security: 14th International Conference, FC 2010, Tenerife, Spain, 25–28 January 2010; Revised Selected Papers 14; pp. 400–407.
14. Zhai, E.; Wolinsky, D.I.; Chen, R.; Syta, E.; Teng, C.; Ford, B. Anonrep: Towards tracking-resistant anonymous reputation. In Proceedings of the 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16), Santa Clara, CA, USA, 16–18 March 2016; pp. 583–596.
15. Azad, M.A.; Bag, S.; Hao, F. PrivBox: Verifiable decentralized reputation system for online marketplaces. *Future Gener. Comput. Syst.* **2018**, *89*, 44–57. [CrossRef]
16. Grinshpoun, T.; Gal-Oz, N.; Meisels, A.; Gudes, E. CCR: A model for sharing reputation knowledge across virtual communities. In Proceedings of the 2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology, Milan, Italy, 15–18 September 2009; pp. 34–41.
17. Shen, M.; Tang, X.; Zhu, L.; Du, X.; Guizani, M. Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. *IEEE Internet Things J.* **2019**, *6*, 7702–7712. [CrossRef]
18. Wang, L.-E.; Ma, S.; Sun, Z. Blockchain-Based Reputation Sharing for High-Quality Participant Selection of MCS. *Secur. Commun. Netw.* **2023**, *2023*, 6120860. [CrossRef]
19. Chen, Y.; Feng, L.; Liang, H.; Yao, S.; Tian, L.; Yuan, X. RS-chain: A decentralized reputation-sharing framework for group-buying industry via hybrid blockchain. *Clust. Comput.* **2022**, *25*, 4617–4632. [CrossRef]
20. Hasan, O.; Brunie, L.; Bertino, E. Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey. *ACM Comput. Surv. (CSUR)* **2022**, *55*, 1–37. [CrossRef]
21. Li, X.; Mei, Y.; Gong, J.; Xiang, F.; Sun, Z. A blockchain privacy protection scheme based on ring signature. *IEEE Access* **2020**, *8*, 76765–76772. [CrossRef]
22. Zhang, S.; Yao, T.; Arthur Sandor, V.K.; Weng, T.-H.; Liang, W.; Su, J. A novel blockchain-based privacy-preserving framework for online social networks. *Connect. Sci.* **2021**, *33*, 555–575. [CrossRef]
23. Han, Y.; Chen, H.; Qiu, Z.; Luo, L.; Qian, G. A Complete Privacy-Preserving Credit Score System Using Blockchain and Zero Knowledge Proof. In Proceedings of the 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 15–18 December 2021; pp. 3629–3636.
24. Wu, A.; Zhang, Y.; Zheng, X.; Guo, R.; Zhao, Q.; Zheng, D. Efficient and privacy-preserving traceable attribute-based encryption in blockchain. *Ann. Telecommun.* **2019**, *74*, 401–411. [CrossRef]
25. Casino, F.; Patsakis, C. An efficient blockchain-based privacy-preserving collaborative filtering architecture. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1501–1513. [CrossRef]
26. Yao, W.; Deek, F.P.; Murimi, R.; Wang, G. SoK: A Taxonomy for Critical Analysis of Consensus Mechanisms in Consortium Blockchain. *IEEE Access* **2023**, *11*, 79572–79587. [CrossRef]
27. Wu, X.; Jiang, W.; Song, M.; Jia, Z.; Qin, J. An efficient sharding consensus algorithm for consortium chains. *Sci. Rep.* **2023**, *13*, 20. [CrossRef]

28. Liu, J.K.; Wei, V.K.; Wong, D.S. Linkable spontaneous anonymous group signature for ad hoc groups. In Proceedings of the Information Security and Privacy: 9th Australasian Conference, ACISP 2004, Sydney, Australia, 13–15 July 2004; Proceedings 9; pp. 325–335.
29. Odoom, J.; Huang, X.; Zhou, Z.; Danso, S.; Zheng, J.; Xiang, Y. Linked or unlinked: A systematic review of linkable ring signature schemes. *J. Syst. Archit.* **2023**, *134*, 102786. [CrossRef]
30. Rivest, R.L.; Shamir, A.; Tauman, Y. How to leak a secret. In Proceedings of the Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, 9–13 December 2001; Proceedings 7; pp. 552–565.
31. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Eurosys '18: Proceedings of the Thirteenth Eurosys Conference, Porto, Portugal, 23–26 April 2018.
32. Song, H.; Li, J.; Li, H. A cloud secure storage mechanism based on data dispersion and encryption. *IEEE Access* **2021**, *9*, 63745–63751. [CrossRef]
33. Theodouli, A.; Arakliotis, S.; Moschou, K.; Votis, K.; Tzovaras, D. On the design of a blockchain-based system to facilitate healthcare data sharing. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1374–1379.
34. Ren, Y.; Guan, H.; Zhao, Q. An efficient lattice-based linkable ring signature scheme with scalability to multiple layer. *J. Ambient. Intell. Humaniz. Comput.* **2022**, *13*, 1547–1556. [CrossRef]
35. Gueta, G.G.; Abraham, I.; Grossman, S.; Malkhi, D.; Pinkas, B.; Reiter, M.; Seredinschi, D.-A.; Tamir, O.; Tomescu, A. SBFT: A scalable and decentralized trust infrastructure. In Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Portland, OR, USA, 24–27 June 2019; pp. 568–580.
36. Beullens, W.; Katsumata, S.; Pintore, F. Calamari and Falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In Proceedings of the 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, Republic of Korea, 7–11 December 2020; pp. 464–492.
37. Mazumdar, S.; Ruj, S. Design of anonymous endorsement system in hyperledger fabric. *IEEE Trans. Emerg. Top. Comput.* **2019**, *9*, 1780–1791. [CrossRef]
38. Wang, J.; Wang, H. Monoxide: Scale out blockchains with asynchronous consensus zones. In Proceedings of the 16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19), Boston, MA, USA, 26–28 February 2019; pp. 95–112.