

RESEARCH ARTICLE

A Blockchain-Based E-Commerce Reputation System Built With Verifiable Credentials

ÖMER DOĞAN¹ AND HACER KARACAN², (Member, IEEE)

¹Informatics Institute, Gazi University, 06680 Ankara, Turkey

²Computer Engineering Department, Faculty of Engineering, Gazi University, 06570 Ankara, Turkey


Corresponding author: Ömer Doğan (doganomer@gmail.com)

ABSTRACT Reviews and reputation scores of sellers play an important role in decision-making process of potential buyers in an e-commerce system. A trustworthy and reliable reputation system is a crucial component in the e-commerce ecosystem, as buyers rely on it to make informed decisions. In this work, we propose a privacy-preserving decentralized reputation system designed to include countermeasures against some known attacks. Our model is built on two permissioned blockchains, namely Hyperledger Indy and Hyperledger Fabric. Hyperledger Indy provides an infrastructure for implementing verifiable credentials with Zero Knowledge Proof support, which is essential for privacy preservation, while Hyperledger Fabric is a robust platform for implementing smart contracts. One of the key advantages of the proposed approach is the use of verifiable credentials for digital identities of sellers, feedback tokens issued to buyers after performing an e-commerce transaction and discount tokens issued to buyers after feedback submission. This helps to ensure that the feedback and identity information is authentic and tamper-proof, reducing the likelihood of identity-related attacks. Additionally, the collection of feedbacks and application of business rules are implemented as smart contracts on Hyperledger Fabric blockchain. This provides a secure and transparent mechanism for processing feedback, reducing the likelihood of unfair feedbacks. Overall, the proposed approach presents a robust reputation system that can help reduce identity-related attacks and unfair feedbacks. The privacy-preserving nature of the system ensures that sensitive information is protected while still enabling the verification of digital identities. The use of feedback and discount tokens incentivizes buyers to provide accurate and honest feedback, which can help reduce unfair feedbacks and identity-related attacks. Finally, the use of smart contracts ensures transparency and immutability, which enhances the overall reliability of the system.

INDEX TERMS Reputation system, electronic commerce, verifiable credentials, privacy preserving, blockchain, hyperledger.

I. INTRODUCTION

The volume of the e-commerce market has rapidly increased in the recent years, especially with the impact of the COVID-19 pandemic. Accordingly, the need for a reliable and satisfactory e-commerce experience for the buyers has become more and more important. Many factors affect the buying decisions, including quality and price of a product together with the reputation of a seller. Among these, reputation of a seller is built by the cumulative purchasing experiences of the buyers. Reviews and ratings of the buyers form

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

the reputation of the sellers. The formation of reputations helps the prospective buyers decide whether to take part in an e-commerce transaction with a seller or not. This form of transitive trust was formulated as EigenTrust algorithm for reputation management in P2P networks by Kamvar et al. [1].

Many e-commerce sites provide means for buyers to submit reviews and ratings for sellers after completing the shopping. These reviews and ratings are collected and processed by the reputation system of that e-commerce site and a reputation score is calculated per seller. The reviews and reputation scores give buyers some degree of trust about sellers although buyers do not usually know sellers. However, there are many possible or encountered attacks against the

reputation systems, which would reduce the trustworthiness of these systems. Koutrouli et al. had a thorough survey on these attacks and produced a taxonomy of the attacks [2]. This taxonomy includes three main categories: unfair recommendations, inconsistent behaviour and identity management related attacks [2]. However, not all of the attacks classified in these categories are applicable to the topic of this article. The following is the list of attacks that are relevant for an e-commerce reputation system where only buyers send feedbacks for sellers.

Bad-mouthing/Slandering attack is a kind of unfair recommendations attack where an attacker provides false negative feedback about sellers in order to degrade their reputation. This attack is mostly expected to come from a competitor.

Ballot-stuffing/Self-Promotion attack is the opposite of bad-mouthing or slandering attack. In this attack, the aim is to increase the reputation score of a seller by injecting false positive feedbacks to the system. As indicated by Hasan et al., this attack can be performed by two users by repeatedly transacting with each other and then assigning each other positive feedback [3].

Whitewashing/Re-entry attack is an identity management related attack. A seller with a bad reputation exits the system and re-joins using a new identity to start with a fresh reputation. The system is vulnerable to this kind of attack when there is no way of linking the identity of the old seller with the new one.

Sybil attackers create multiple identities in the system so that they can have more influence on the reputation scores. Attackers with multiple identities may use this advantage either for bad-mouthing or for ballot-stuffing.

Traitors/Oscillation attacker may behave properly for some time to be a trusted party, and then later on start deceiving. This has been encountered in eBay, where sellers build trust by participating in many transactions with small amounts, and then cheat buyers on high-priced items [2].

In traditional e-commerce systems, reputation is typically managed by centralized platforms that collect and store data on sellers. However, this approach has several limitations, such as vulnerability to manipulation, lack of transparency, and difficulty in sharing reputation data across multiple platforms. Blockchain technology provides a decentralized and tamper-proof way of managing reputation data, which is transparent, immutable, and can be shared across multiple platforms. This means that sellers can build a trusted reputation profile that can be used across multiple e-commerce platforms, making it easier to establish trust and conduct transactions securely and efficiently. On the other hand, non-blockchain-based reputation systems are centralized, meaning that the reputation data is controlled by a single entity, such as an e-commerce platform, which can be vulnerable to manipulation and censorship.

This research aims to create measures to tackle with the known attacks against reputation systems by modelling a blockchain-based decentralized reputation system. Our

model uses blockchain technology not only for submissions and storing the feedbacks but also for issuing and verification of verifiable credentials.

A. OUR CONTRIBUTIONS

Our work proposes a decentralized reputation system that utilizes verifiable credentials to ensure security and privacy. Verifiable credentials are used as:

- 1) Feedback tokens for buyers, ensuring that only those who have completed a shopping transaction can submit reviews and ratings
- 2) Digital identities of sellers to provide uniqueness for the complete legal lifetime of the seller and on all the e-commerce platforms
- 3) Discount tokens issued to reviewers as an incentive mechanism for feedback submission. E-commerce platforms in the system can accept these tokens to provide discounts or any other kinds of special offers to reviewers.

To the best of our knowledge, we are the first to use verifiable credentials as the tokens for these purposes in an e-commerce reputation system.

Furthermore, we propose using a permissioned blockchain, Hyperledger Fabric, as the main building block of our model, which significantly reduces the need for high resource consumption of public blockchains. Our work also connects two different blockchain platforms, Hyperledger Indy and Hyperledger Fabric, to build a complete reputation system.

B. OUTLINE

In section II, we will analyse existing blockchain-based reputation systems and provide background information about the building blocks of our model. In section III, we will explain all the details of our model. In section IV, we will provide the security aspects of our model. In section V, we will provide the security analysis of our model, especially against the attacks listed before. In section VI, we will provide the performance metrics of our system with the test configurations. Finally, in section VII, we will conclude with a summary of our work.

II. RELATED WORK AND BACKGROUND

Because of the decentralized and immutable nature of the blockchain technology, there have been many researches on using blockchain in reputation systems in the recent years.

A. E-COMMERCE REPUTATION SYSTEMS BASED ON PUBLIC BLOCKCHAINS

There are many researches proposing decentralized blockchain based reputation systems built on public blockchains and cryptocurrencies, such as Bitcoin and Ethereum. Some of these systems focus on preserving the privacy of reviewers.

Sun et al. aimed to prevent some types of attacks by spending “reputation tokens” for sending review scores, which

would have a weight proportional to the tokens spent [5]. Nodes are supposed to earn tokens as long as they create block in the blockchain network. They claimed that this model would preserve the privacy of the reviewer. However, there are no incentives for the reviewers to gain more tokens and to provide reviews. Schaub et al. proposed a more comprehensive privacy preserving reputation system to prevent some types of attacks [6]. The main component of their model is the blinded token issued by the service provider to the buyer to let the buyer submit feedback. Service provider needs to earn and spend coins of the underlying blockchain in order to be able to issue tokens. Owiyo et al. also proposed a model which is very similar to the one proposed by Schaub et al. [7]. However, it is not clear how service providers are supposed to earn coins and ensure that they have enough coins to issue tokens to buyers in both models. Carboni proposed a Bitcoin based reputation system, which depends on Bitcoin payments [11]. Bitcoin addresses are used for preserving privacy of reviewers. Soska et al. proposed a reputation system coupled with a decentralized marketplace called Beaver [16]. Although the proposed solution seems promising against reputation system attacks, it is totally built on decentralized marketplace architecture and cryptocurrency based payments.

On the other hand, some systems do not focus on preserving the privacy of reviewers. Most of these reputation systems are based on Ethereum blockchain. Tamang calculated “Total Endorsement Impact” score in order to prevent some attacks in his model, which is based on Ethereum, a public permissionless blockchain network [8]. Calculation of this score is based on both incoming and outgoing connections of endorsers and endorsees, which may result in unexpected reputation scores for an e-commerce system. Another Ethereum based reputation system is proposed by Dhakal et al., which they named as DTrust [9]. The limitations of DTrust is that it depends on the payments performed on Ethereum and it does not consider preserving privacy of reviewers. Zulfiqar et al. also proposed an Ethereum based reputation system with similar constraints, which they named as EthReview [10]. Wang et al. also proposed an Ethereum based reputation system named ReviewChain [13]. ReviewChain is designed not for e-commerce applications but for supply chain systems built on blockchain. Almasoud also proposed an Ethereum based reputation system for e-commerce marketplaces in his thesis [14]. His model embeds review phase as an inseparable part of e-commerce session and does not consider preserving the privacy of reviewers.

There are also other non-privacy preserving reputation systems based on public blockchain networks other than Ethereum. Ahn et al. proposed a reputation system built on Bitcoin cryptocurrency based payment systems by storing the transactions and the user reviews on the blockchain ledger [4]. The limitation of this system is its dependency on the cryptocurrency based payment system. Buechler et al. also proposed a decentralized reputation system built on Bitcoin network and Ethereum smart contracts, which calculates reputation score with their proprietary reputation algorithm [12].

Ramachandiran proposed two blockchains in his model, one for storing review records and the other for storing buyers and sellers [15]. The second blockchain also keeps records of purchases in conjunction with the buyer and seller records. The redundant storage of information brings an additional cost of synchronization of the records since e-commerce platforms already maintain these records. In addition, privacy of the buyers is not preserved since the buyers are kept with their basic information.

B. E-COMMERCE REPUTATION SYSTEMS BASED ON PERMISSIONED BLOCKCHAINS

The decentralized reputation system proposed by Kugblenu and Vuorimaa is one of the very few permissioned blockchain based reputation systems [21]. It tries to preserve privacy by generating review token at checkout step, which is only a concatenated text composed of ProductID, RetailerID and OrderID. However, there is no signature and cryptographic validation of the token during review submission. Another permissioned blockchain based reputation system proposal is RepChain, which is an anonymous and verifiable reputation system for e-Commerce platforms [40]. RepChain uses blind signatures for preserving privacy of reviewers.

C. OTHER REPUTATION SYSTEMS BASED ON PUBLIC BLOCKCHAINS

There are some other researches related with decentralized reputation systems focusing on areas other than e-commerce. Mendes et al. built a reputation system on blockchain for storing reviews of mobile applications on application stores and processed these reviews on cloud-based systems [17]. Although it looks similar, there are many different characteristics of mobile application reviews and e-commerce reviews. Another application of a decentralized reputation system is proposed for auctions by Omori and Kishigami [18]. Their work is based on Ethereum blockchain; but dedicated to reputations of sellers in auctions. Park et al. proposed a smart-contract based decentralized review system for IoT data marketplaces [19]. Nguyen et al. proposes a blockchain based trust model for evaluating the trustworthiness of reviews from the crowd, such as social media [20].

All the blockchain based reputation systems described above are summarized in table 1. When compared to our model, the listed reputation systems have the following differences:

- Reputation systems based on public blockchains depend on a consensus mechanism, usually proof of work, which is inefficient, has slower transaction times and requires high power consumption compared to permissioned blockchains.
- Reputation systems that don't preserve the privacy of the reviewers fail to prevent unfair feedbacks.
- When compared to reputation systems using blind signatures for privacy preservation, verifiable credentials

TABLE 1. Blockchain based reputation systems.

#	Title	Blockchain Type	Domain	Privacy Preservation
1	[4] A Model for Deriving Trust and Reputation on Blockchain-Based e-Payment System.	Public (Bitcoin)	E-Commerce	No
2	[5] A Privacy-Preserving and Robust Reputation System Based on Blockchain.	Public	General	Yes. Reputation tokens are generated as a reward of mining.
3	[6] A Trustless Privacy-Preserving Reputation System.	Public (any coin based)	E-Commerce	Yes, using blind signatures
4	[7] Decentralized Privacy Preserving Reputation System.	Public (any coin based)	E-Commerce	Yes, using blind signatures
5	[8] Decentralized Reputation Model and Trust Framework Blockchain and Smart contracts.	Public (Ethereum)	General	No
6	[9] DTrust: A Decentralized Reputation System for E-commerce Marketplaces.	Public (Ethereum)	E-Commerce	No
7	[10] EthReview: An Ethereum-based Product Review System for Mitigating Rating Frauds.	Public (Ethereum)	E-Commerce	No
8	[11] Feedback based Reputation on top of the Bitcoin Blockchain.	Public (Bitcoin)	E-Commerce	Yes, using Bitcoin addresses
9	[12] Decentralized Reputation System for Transaction Networks.	Public (Bitcoin and Ethereum)	E-Commerce	No
10	[13] ReviewChain: Smart Contract Based Review System with Multi-Blockchain Gateway.	Public (Ethereum)	E-Commerce	No
11	[14] Smart Contracts for Blockchain-based Reputation Systems.	Public (Ethereum)	E-Commerce	No
12	[15] Using Blockchain Technology To Improve Trust In eCommerce Reviews.	Public	E-Commerce	No
13	[16] Beaver: A Decentralized Anonymous Marketplace with Secure Reputation.	Public (Bitcoin)	E-Commerce	Yes, by the nature of decentralized marketplace.
14	[21] Decentralized Reputation System on a Permissioned Blockchain for E-Commerce Reviews.	Permissioned (Hyperledger Fabric)	E-Commerce	Yes, by generating review token as a text composed of ProductID, RetailerID and OrderID. No signature and cryptographic validation of the token during review submission.
15	[17] A Novel Reputation System for Mobile App Stores Using Blockchain.	Permissioned (Hyperledger Fabric)	Mobile App Stores	No
16	[18] Incorporating Reputation System in Blockchain-Based Distributed Auctions.	Public (Ethereum)	Auctions	No
17	[19] Smart Contract-Based Review System for an IoT Data Marketplace.	Public (Ethereum)	IoT Data Marketplace	No
18	[20] A Blockchain-based trust model for crowd environments.	Not Indicated	Crowd Sourcing	No
19	[40] Anonymous and Verifiable Reputation System for E-Commerce Platforms Based on Blockchain	Permissioned	E-Commerce	Yes, using blind signatures

provide a more structured and attribute based selective disclosure with Zero Knowledge Proof predicates.

D. LITERATURE REVIEWS ON REPUTATION SYSTEMS

In addition to the model proposals, there also exist researches that investigate and compare reputation systems. Bellini et al. analysed both the academic researches and commercial applications on blockchain based reputation systems [22]. Cai and Zhu analysed blockchain based reputation systems with a different perspective. Their focus was the strengths and limitations of blockchain based reputation systems to detect fraudulent reviewers in terms of both objective and subjective information fraud [23]. Hasan et al. had a comprehensive study on reputation systems and created an analysis framework especially for analysing the privacy preserving ones [3]. In addition, their work included comparison of blockchain based reputation systems based on the developed analysis

framework. Andrade, in his thesis, evaluated the blockchain based reputation systems from a technical perspective [24]. Almasoud et al. had a systematic literature review on usage of smart contracts for blockchain based reputation systems [25]. By analysing the gap in the literature, they proposed an Ethereum smart contract-based reputation system. Battah et al. worked on the implementation challenges and possible solutions for blockchain based reputation systems [26]. Similarly, Vandervort discusses the challenges and advantages of reputations systems implemented with Bitcoin transactions [27]. Basili et al. analysed case studies to investigate the effect of reputation systems on the degree of service quality specifically in ridesharing services [28].

E. CENTRALIZED LEDGER DATABASES

Centralized ledger databases and permissioned blockchains are two types of technologies that are designed to manage and

store data in a secure and auditable way. Centralized ledger databases can provide tamper-evidence and non-repudiation features, similar to permissioned blockchains. When decentralization and smart contracts are not needed, centralized ledger databases may be a better option since they provide higher throughput, lower latency and better usability compared to permissioned blockchains. There exist recent researches on the usage of centralized ledger databases when these blockchain features are not required [41], [42], [43], [44]. However, we have not encountered any reputation system proposal that uses centralized ledger databases.

In our reputation system, decentralization is a key feature where no single entity has authority on the ledger data. The ownership of the data is shared by all the participants of the system, including multiple e-commerce platforms and sellers. Our system also utilizes smart contracts feature of the blockchain in order to store feedback data, calculate reputation score and generate discount tokens. Therefore, centralized ledger databases are not considered as an option in our reputation system.

F. TECHNICAL BACKGROUND

This section will provide short background information on the building blocks of the proposed model.

1) BLOCKCHAIN

Blockchain is a distributed ledger technology that stores the records immutably within blocks. Each block is linked to the previous one with the hash of that block. This chain of blocks makes the ledger immutable where any change in a block results in invalidation of all subsequent blocks, as shown in Figure 1.

This chain of blocks structure is based on the Bitcoin paper published by Satoshi Nakamoto in 2008 [29]. Although the proposal was aiming to solve double-spending problem without a trusted third party, it evolved to blockchain technology with a much wider use.

Blockchain networks can mainly be classified into two categories according to who can join the network: public (permissionless) and permissioned blockchains. There is no constraint on the participants of a public blockchain and anyone can join and perform transactions on these networks. On the other hand, permissioned blockchains are controlled by one or more organizations and participants need to be granted to join the network by these controlling organizations. Since the participation to permissioned blockchains is subject to allowance of some controlling organizations, it is usually accepted that there is partial trust amongst the participants rather than no trust.

Since there is no central authority in a blockchain network, nodes agree on valid transactions and the state of the network by using consensus mechanisms. There are various kinds of consensus mechanisms used in blockchain systems with different algorithms. One of the most widely used consensus mechanisms is Proof of Work (PoW), which is the consensus

mechanism of Bitcoin and Ethereum networks. In PoW, validator nodes (miners) need to solve a mathematical problem to be able to add a new block to the chain. Although PoW is a robust and secure consensus mechanism, it is criticized for its high power consumption and high latency when adding a new block to the ledger.

Despite its potential, blockchain technology has not yet been widely adopted across various industries. One of the main reasons for this is the lack of understanding and awareness of how the technology works and its potential use cases. Therefore, there are various researches on the usage of the technology [39]. With the growing interest in blockchain and the increasing number of use cases being developed, it is clear that the potential of this technology is enormous and is likely to shape the future of various industries.

2) SMART CONTRACTS

Smart contracts are pieces of code that automatically run on blockchain networks when triggered by predefined conditions. They are distributed to the network and deployed on the nodes in the network. Therefore, participants of the network agree on how these smart contracts should work. Exactly as the real world contracts do, smart contracts also ensure that the agreement between the parties is fulfilled by running the agreed code.

3) VERIFIABLE CREDENTIALS

Verifiable credentials are digital, cryptographically secured and verifiable versions of paper credentials in the physical world. World Wide Web Consortium (W3C) has made two publications related with the verifiable credentials: Verifiable Credentials Data Model [30] and Verifiable Credentials Use Cases [31]. In the data model publication, W3C defines the verifiable credentials ecosystem and the roles as shown in Figure 2.

As seen in the figure, Issuer creates a verifiable credential dedicated to a subject and transfers it to the Holder. Holder possesses and keeps verifiable credentials provided by Issuers and presents proofs of owning those credentials to Verifiers when needed. Verifiers receive presented proofs from Holders and verifies them through Verifiable Data Registry.

Verifiable credentials can prove the following information when it is presented to the Verifier:

- 1) Issuer of the credential,
- 2) It was issued to the Holder presenting the credential,
- 3) Claims were not tampered with,
- 4) Issuer has not revoked the credential.

4) HYPERLEDGER

Hyperledger is an open-source family of frameworks, tools and libraries, which helps to build enterprise-grade blockchain applications. There are many purpose-built blockchain frameworks under this overarching family.

Hyperledger Fabric is a permissioned blockchain with a modular architecture, which aims to provide a framework for

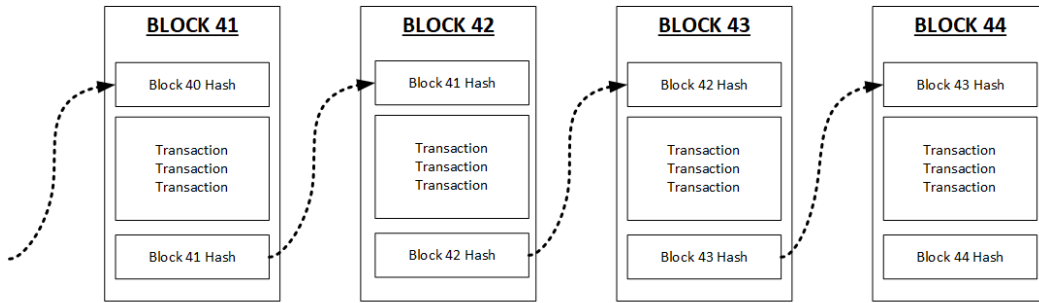


FIGURE 1. Blockchain structure.

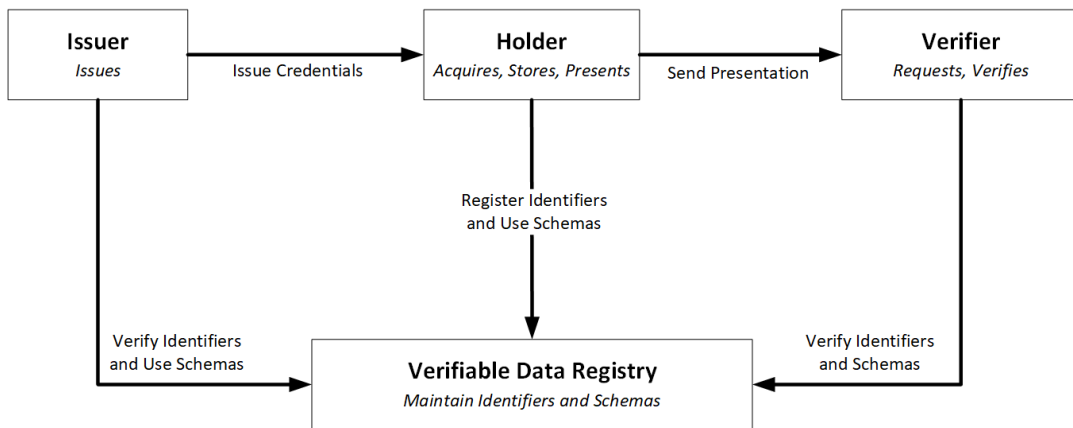


FIGURE 2. Verifiable credentials ecosystem [30].

enterprise applications. It is suitable for a network of participants with partial trust. With this constraint, it has an efficient consensus mechanism that reduces the latency of transactions to an acceptable level for enterprise applications. Hyperledger Fabric supports smart contracts. The implementation of smart contracts in Hyperledger Fabric is named as chaincode.

Hyperledger Indy is a purpose-built permissioned blockchain aimed for verifiable credentials and digital identities. Because of its specific area of use, it does not support asset exchanges and smart contracts. Together with Indy, Hyperledger family has two more components for supporting the verifiable credentials scenarios. Hyperledger Aries is a shared, reusable, interoperable toolkit used for developing digital identity applications. Hyperledger Ursa is a shared cryptographic library. All these Hyperledger frameworks, tools and libraries enable implementation of verifiable credentials data model as standardized by W3C.

5) ZERO KNOWLEDGE PROOF

Zero Knowledge Proofs (ZKP) were first introduced by Goldwasser et al. [32] and defined as those proofs that convey no additional knowledge other than the correctness of the proposition in question. In other words, ZKPs are probabilistic cryptographic techniques that enable a Prover to convince

a Verifier that a statement is valid without having to reveal further information other than the statement. The following properties of ZKP are explained by Groth [33] as follows:

- **Completeness:** If the statement is true, prover will be able to convince verifier that the statement is true.
- **Soundness:** If the statement is false, a malicious prover cannot convince the verifier.
- **Zero-knowledge:** A malicious verifier learns nothing except that the statement is true.

Hyperledger Indy includes ZKP capability and enables holders of verifiable credentials to create ZKPs to prove equality and inequality statements about their credential attributes. For example, it is possible to prove being employed without disclosing employer information or being over age 18 without disclosing date of birth.

III. OUR MODEL

The main goals of our model are to maximize the honest feedbacks from buyers and to minimize fraudulent activities by preventing some major attacks to the reputation system. The principles of our model are built around these goals.

Chang et al. classified the approaches for promoting honest feedbacks for reputation systems into two main categories in their survey [34]:

- 1) Protecting the privacy of recommenders,
- 2) Providing incentives to recommenders (Market-based and Policy-based)

Our model also considers these approaches in order to fulfil the goal of maximizing the honest feedbacks from buyers.

A. PRINCIPLES OF THE MODEL

In order to achieve the identified goals of the model, the following principles are found to be necessary.

- Sellers should uniquely and globally be identified and registered to the system, regardless of the e-commerce platform they are using and whether they have registered/unregistered before.
- System should preserve the privacy of the reviewers. It should not be possible to reveal the information of who provided the feedback for a seller. Therefore, system should not keep any link between the feedback and the owner of the feedback.
- While preserving the privacy of reviewers, system should not allow anyone to send feedback for a seller without involving in an e-commerce transaction with the seller. Therefore, system should only allow feedbacks linked to completed e-commerce activities. In addition, system should prevent submission of multiple feedbacks for a single e-commerce activity.
- Permissions for sending feedbacks should be valid only for a defined period after completing the e-commerce activity. In other words, permissions should have an expiration date.
- Buyers should be encouraged to provide feedbacks for sellers. System should support integrating with incentive mechanisms of the sellers.

B. OVERALL ARCHITECTURE

Our system consists of the following entities:

Buyer: A buyer B purchases some goods or services from a seller S in an e-commerce transaction. B aims to have the best experience from the e-commerce activity. Therefore, B is expected to review the comments and reputation score of S before deciding to purchase from S . After completing a purchase, B is allowed to provide feedback about S . B needs feedback token provided by S or M to be able to give feedback about S . B cannot be linked to her feedback although providing feedback is constrained to completion of a purchase.

Seller: A seller S sells some goods or services online to B . S may either have a store on an online marketplace M or own a dedicated online store. After completion of a purchase, S or M generates feedback token to B , which would be used to provide feedback about S by B .

Marketplace: A marketplace M provides an online platform for sellers to have stores and for buyers to find goods and services to purchase from sellers. Traditionally, a M usually has a built-in feedback system to collect and store feedback from buyers. However, our model externalizes the feedback system from M .

Legal Authority: In our model, a Legal Authority LA is an institute authorized by laws and regulations that is in charge of managing legal processes and records of companies. LA is the only authorized entity to issue digital identities to S . Digital identities issued by LA ensure that S is registered to the system with a unique identity.

Our model is composed of two sub-systems:

1) VERIFIABLE CREDENTIALS SUBSYSTEM

Verifiable Credentials Subsystem VCS enables issuing verifiable credentials and verifying the validity of these credentials.

There are three verifiable credential types in the system:

- Digital identities issued by legal authorities to sellers,
- Feedback tokens issued to buyers as verifiable credentials after completing e-commerce transactions,
- Discount tokens issued to reviewers by the Feedback Collection Subsystem after feedback submissions.

This subsystem is realized by using Hyperledger Indy blockchain together with the supporting tools and libraries, namely Hyperledger Aries and Ursa. During the initial setup of the system, three schemas need to be defined in the Hyperledger Indy blockchain: seller digital identity schema, feedback token schema and discount token schema. Seller digital identity schema should at least have the following fields:

```
{
  "id": "...",
  "type": ["VerifiableCredential", "SellerDigitalIdentity"],
  "issuer": "...",
  "issuanceDate": "...",
  "credentialSubject": {
    "LegalEntityId": "...",
    "Name": "...",
    "URL": "..."
  }
}
```

Feedback token schema should at least have the following fields:

```
{
  "id": "...",
  "type": ["VerifiableCredential", "FeedbackToken"],
  "issuer": "...",
  "issuanceDate": "...",
  "expirationDate": "...",
  "credentialSubject": {
    "SellerLegalEntityId": "...",
    "MarketplaceId": "...",
    "Amount": "..."
  }
}
```

Discount token schema should at least have the following fields:

```
{
  "id": "...",
  "type": ["VerifiableCredential", "DiscountToken"],
  "issuer": "...",
  "issuanceDate": "...",
  "expirationDate": "...",
  "credentialSubject": {
    "SellerLegalEntityId": "...",
    "MarketplaceId": "...",
    "TransactionDate": "...",
    "TransactionAmount": "...",
    "DiscountAmount": "..."
  }
}
```

Having the above fields in the verifiable credentials does not mean that these fields will necessarily be revealed while presenting proof for the credentials. For instance, S or M may want to know whether the amount of the transaction in the discount token is above a certain value or not. TransactionAmount field in the discount token does not need to be disclosed for proving that it is above or below that value. ZKP provides the necessary cryptographic proof mechanisms for the buyer to convince S or M .

2) FEEDBACK COLLECTION SUBSYSTEM

Feedback Collection Subsystem FCS gathers all feedbacks from buyers and calculates reputation scores for sellers. For a buyer to send feedback to this subsystem, the buyer needs to provide the feedback token as the proof of a completed e-commerce transaction. The subsystem verifies the feedback token in terms of validity, expiration, one-time use and seller match constraints. If all checks pass, the subsystem adds feedback to the ledger and calculates the resulting reputation score for the seller.

After saving the feedback, the subsystem issues discount token to the reviewer as the proof of feedback submission. Discount token is an incentive mechanism to encourage buyers to send feedbacks. E-commerce platforms in the system may accept these discount tokens to provide special offers, discount vouchers or other incentive means.

This subsystem is realized by using Hyperledger Fabric blockchain and functions are implemented using chaincodes.

This subsystem acts as the verifier in the Verifiable Credentials ecosystem for seller digital identities and feedback tokens. It verifies and stores the digital identities presented by sellers and feedback tokens presented by buyers. The subsystem also acts as issuer in the Verifiable Credentials ecosystem for discount tokens. Discount tokens are verified by the marketplaces or sellers to provide special offers to the reviewers.

In addition to keeping cryptographically signed presentations of verifiable credentials, the subsystem maintains other linked tables in the ledger in order to support smart contract functions. The logical data model of Hyperledger Fabric ledger state database is shown Figure 3.

As seen in the data model, no information is kept which would help linking buyers to the feedbacks. ID of the feedback token sent by the reviewer is kept in the Feedback-TokenId field in Feedback table. The ID is generated by the reviewer during token creation and it is not known by the issuer of the token. Therefore, it is not possible to link FeedbackTokenId to the reviewer. The aim of keeping FeedbackTokenId is to ensure that feedback tokens are used only once. By this check, the system prevents multiple feedback submissions for a single e-commerce transaction. This data model also ensures that sellers are uniquely registered to the system by their LegalEntityId.

The following smart contracts (i.e. chaincodes) are implemented on the Hyperledger Fabric blockchain:

- **registerSeller:** A prospective seller S of the reputation system invokes *registerSeller* chaincode method and provides its digital identity for registration. The subsystem, through Hyperledger Indy blockchain, verifies that the presented digital identity is valid. If the digital identity is valid, the subsystem extracts information from the presented digital identity and creates or updates seller record in the blockchain.
- **getReputationScore:** Any user can see the reputation score of a seller by invoking *getReputationScore* chaincode method. This method returns the last calculated reputation score.
- **getAllFeedbacks:** Any user can get the list of all feedbacks for a seller within a date interval by invoking *getAllFeedbacks* chaincode method. This method returns the list of individual feedbacks including feedback score and comment.
- **submitFeedback:** A buyer submits feedback by invoking *submitFeedback* chaincode method. Buyer should have already retrieved a feedback token from a seller or a marketplace and should present that token as the proof of completed e-commerce transaction. The subsystem, through Hyperledger Indy blockchain, verifies that the presented feedback token and its signatures are valid and the token has not expired yet. If validated, the subsystem ensures that the reviewed seller is registered in the system and the presented token has not been used before. After all checks are completed, feedback record is added to the blockchain database including feedback date, score and comment details. Reputation score of the seller is calculated and updated in the database. After saving the feedback record, the subsystem issues discount token to the reviewer as the proof of feedback submission.

ZKP can also be applied while reviewers are presenting the discount tokens to e-commerce platforms for some special offers. A marketplace or a seller may want to enforce that the discount token was issued for a feedback that was initiated from that platform. Reviewer can prove that the discount token satisfies this requirement without actually revealing the marketplace and seller information.

Figure 4 depicts the overall network architecture that implements the above subsystems.

As seen in Figure 4, participants of the reputation system compose the blockchain network by providing blockchain nodes. Each participant is composed of two nodes: one node for Hyperledger Fabric blockchain and the other node for Hyperledger Indy blockchain. Integration of these two blockchains is done by smart contracts. Buyers interact with the blockchain through the e-commerce platforms of the marketplaces and the sellers. An independent platform can also be located for the buyers' blockchain interaction.

C. PROCESSES

The whole e-commerce process can be divided into four phases.

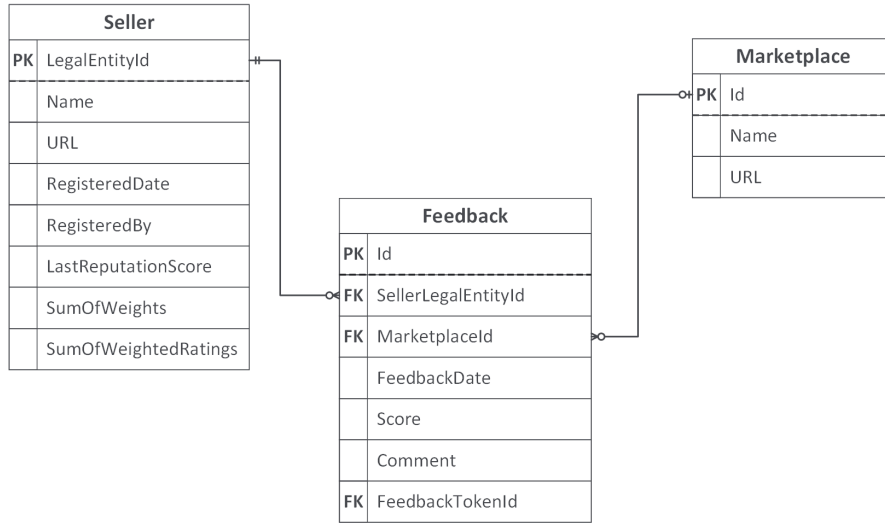


FIGURE 3. Feedback collection subsystem data model.

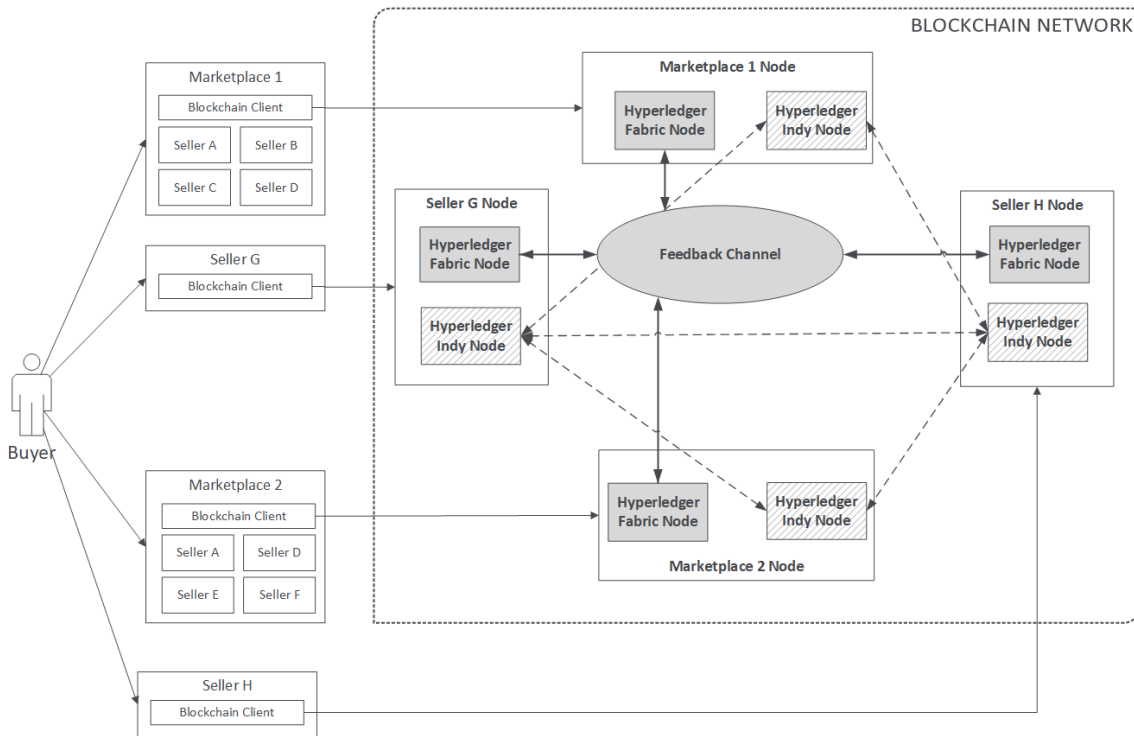


FIGURE 4. Overall network architecture.

- 1) Seller Registration Phase
- 2) Shopping Phase
- 3) Service Delivery Phase
- 4) Feedback Phase

1) SELLER REGISTRATION PHASE

Seller Registration phase has two distinct steps.

Issue Digital Identity is the step where Legal Authority provides digital identity to Seller.

Add Seller to FCS is the step where *S* is registered to *FCS* blockchain after verifying that *S* has a valid Digital Identity.

The sequence diagram in Figure 5 shows a simplified flow of actions for seller registration.

2) SHOPPING PHASE

During the shopping phase, buyer may want to see the overall reputation score or all feedbacks for a seller

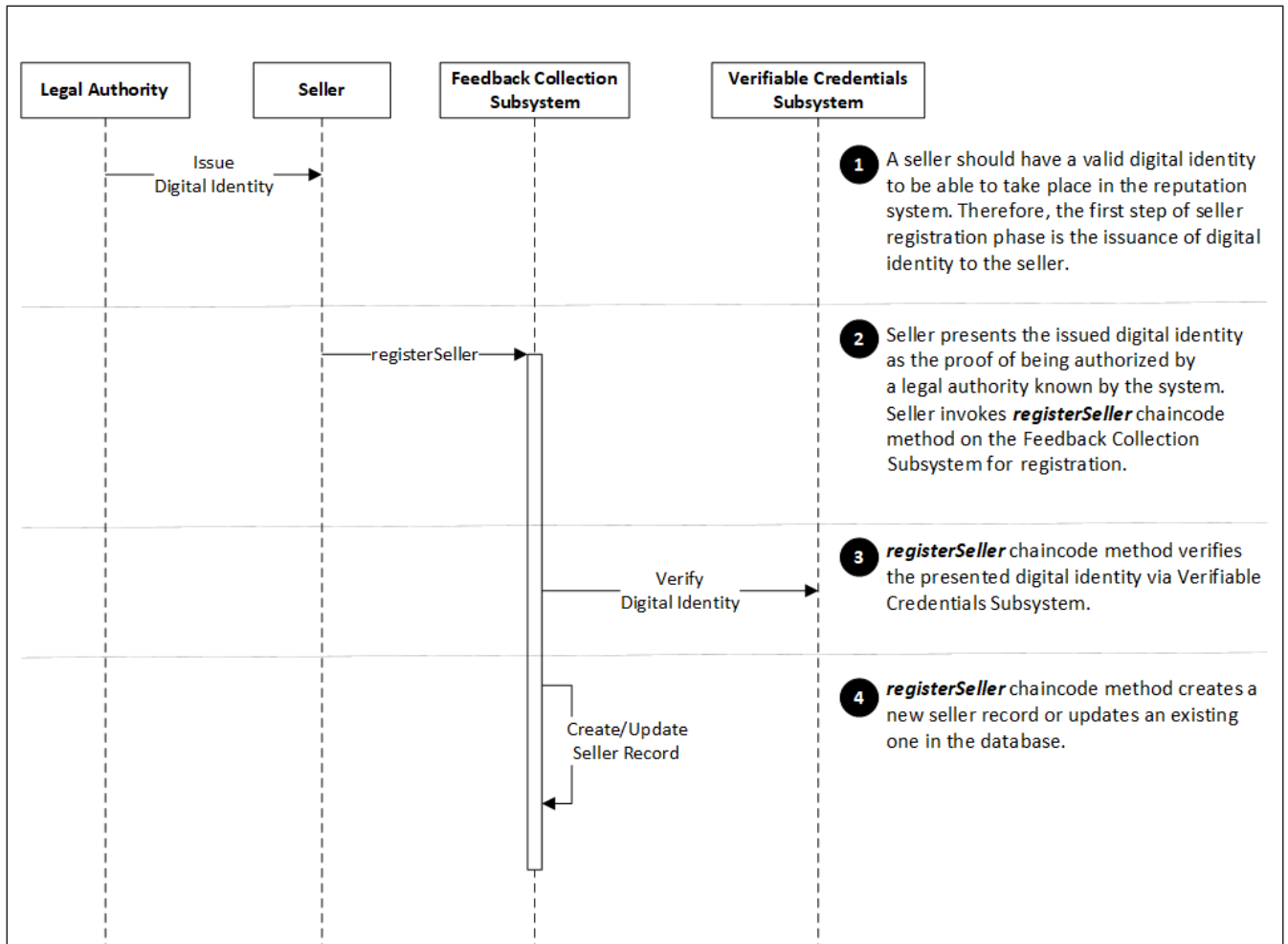


FIGURE 5. Seller registration phase flow of actions.

Algorithm 1 Issue Digital Identity

Ensure: Connection established between *LA* and *S*

- 1: *S* sends credential request to *LA*
- 2: **if** *S* has valid identity records on *LA* **then**
- 3: *LA* issues Digital Identity to *S*
- 4: *S* saves Digital Identity into its wallet
- 5: **else**
- 6: *LA* rejects credential request
- 7: **end if**

by invoking `getReputationScore` and `getAllFeedbacks` chaincode methods. Invocation of chaincode methods can be performed through seller, marketplace or another platform. Buyer can decide whether the seller is trustworthy or not based on the feedbacks and reputation score.

If buyer decides to continue shopping with the seller, the next step is to make payment and wait for the service to be delivered by the seller. After completing the payment, seller or marketplace issues feedback token to the buyer. Buyer may keep the token for some time and prefer to send feedback later as long as the token is still valid.

3) SERVICE DELIVERY PHASE

Service delivery depends on the type of the service provided by the seller. If the seller offers physical items to be delivered to the buyer, service delivery phase may take days or even weeks after the payment. During service delivery, there is no action performed on the system.

4) FEEDBACK PHASE

Buyer can submit feedback for the seller any time after getting the feedback token from the seller/marketplace but before the feedback token expires. Although it is a common practice that feedback is submitted after service delivery phase, it is not a strict constraint in the system. Moreover, service delivery may never happen and in that case, buyer would probably be willing to send negative feedback for the seller.

The sequence diagram in Figure 6 shows a simplified flow of actions for shopping and feedback phases. Service delivery phase is omitted since the system is not involved in that phase.

D. REPUTATION SCORE AND DISCOUNT TOKEN CALCULATION

The main input for the calculation of reputation score for *S* is the ratings provided by *B* as part of the feedback. Reputation

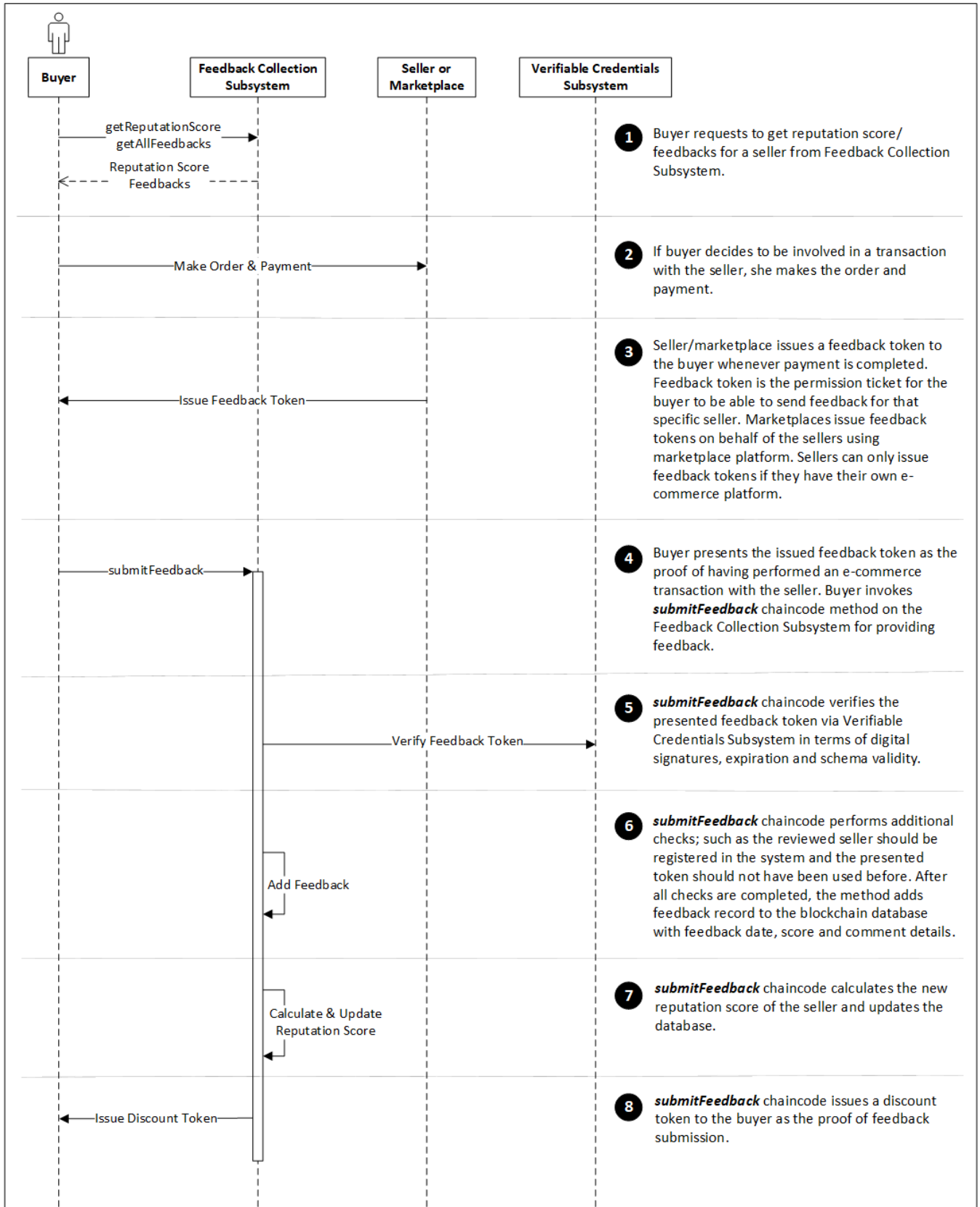


FIGURE 6. Shopping and feedback phases flow of actions.

Algorithm 2 Add Seller to FCS

Require: *S* has a valid Digital Identity

- 1: *S* sends request to *FCS* for registering to the system
- 2: *FCS* checks if *S* has already provided the proof of having Digital Identity from a known *LA*
- 3: **if** no proof is found **then**
- 4: *FCS* requests proof from *S*
- 5: *S* generates proof of having Digital Identity and sends to *FCS*
- 6: *FCS* checks the validity of the proof against *VCS* blockchain
- 7: **if** proof is valid **then**
- 8: *FCS* saves the proof into its wallet
- 9: **else**
- 10: *FCS* rejects seller registration and returns error
- 11: **end if**
- 12: **end if**

- 13: *FCS* calls registerSeller chaincode method
- 14: registerSeller chaincode writes *S* record into *FCS* blockchain

Algorithm 3 Issue Feedback Token

Ensure: Connection established between *S* and *B*

Require: *B* has placed an order on *S*

- 1: **if** Transaction Amount > Min. Threshold **then**
- 2: *S* issues Feedback Token to *B*
- 3: *B* saves Feedback Token into its wallet
- 4: **else**
- 5: *S* does not issue Feedback Token
- 6: **end if**

score of a *S* is calculated by using a weighted average of user ratings based on the following parameters.

1) STALENESS OF PURCHASE

The weighting factor of staleness is calculated by using the following formula.

$P(t) = (1 - 0.02564)^t$ where *t* is the number of days between date of feedback and the date of the delivery of goods or services. This function is an exponential decay function with a decay rate of 2.564%. Decay rate is determined so that the weight of the feedback rating gets close to zero in a six-month period.

2) TRANSACTION AMOUNT

When the weight of feedback ratings for all prices is the same, the system becomes vulnerable to bad-mouthing/slandering. Attackers may provide a lot of unfair feedback ratings when it is possible by purchasing several low price goods or services. Making the weight of feedback ratings dependent on the transaction amount minimizes the impact of such unfair feedbacks. The weighting factor of transaction amount is

Algorithm 4 Submit Feedback

Require: *B* has received Feedback Token from *S*

- 1: *B* sends feedback for *S* to *FCS*
- 2: *FCS* requests proof from *B* for having performed a purchase
- 3: *B* generates proof of Feedback Token from *S* and sends the proof to *FCS*
- 4: *FCS* checks the validity of the proof against *VCS* blockchain
- 5: **if** proof is valid **then**
- 6: *FCS* checks if the same Feedback Token was used before
- 7: **if** Feedback Token was not used before **then**
- 8: *FCS* saves the proof into its wallet
- 9: *FCS* writes feedback into blockchain
- 10: *FCS* calculates and updates reputation score of *S*
- 11: *FCS* sends Discount Token to *B*
- 12: *B* saves Discount Token into its wallet
- 13: **else**
- 14: *FCS* rejects the feedback and returns error
- 15: **end if**
- 16: **else**
- 17: *FCS* rejects the feedback and returns error
- 18: **end if**

calculated by using the following formula.

$$\Psi(A) = \begin{cases} 1 & \text{if } A > \alpha \\ 0 & \text{if } A < \mu \\ A_{normalized} & \text{otherwise} \end{cases}$$

where α is the threshold amount for transactions with a weight factor of 1 and μ is the lower bound for the amount of transactions to have an impact on the reputation score calculation. Weight of transaction amounts lower than α decreases as the amount decreases. When the amount reaches to the lower bound μ value, weight factor becomes zero. $A_{normalized}$ is defined as the normalization of values of *A* between $[\mu - \alpha]$ to $[0-1]$ and calculated with the following formula:

$$A_{normalized} = \frac{A - \mu}{\alpha - \mu}$$

Weighting factor for each rating is

$$w = P(t) \times \Psi(A)$$

Reputation score of *S* is calculated as the weighted average of ratings using the following formula.

$$R_s = \frac{\sum_{i=1}^n w_i \times x_i}{\sum_{i=1}^n w_i}$$

where w_i is the weight factor for each rating, x_i is the rating and *n* is the total number of ratings.

Our system does not keep all the individual ratings for the sake of efficiency. In order to recalculate the new reputation score when a new rating is received, the system keeps W_t and

X_t where W_t is the sum of all weights and X_t is the sum of all weighted ratings. When a new rating is received, R_s is calculated as follows:

$$R_s = \frac{X_t + w \times x}{W_t + w}$$

where x is the new rating value and w is the weighting factor of the new rating.

Discount token is provided to Buyer B by Seller S or Marketplace M as an incentive mechanism for B to provide feedback. The amount of the discount should not be a fixed amount but rather be dependent on the same parameters used in the calculation of the reputation score. Therefore, calculation of discount amount includes the weight factor w .

In addition to w , we need to set a ratio r of the total transaction amount for calculating the discount amount. Hence, the amount of the discount is calculated with the following formula:

$$D = A \times w \times r$$

r can be adjusted by each S so that S has the flexibility to determine how much discount they will provide.

IV. SECURITY OF THE MODEL

This section provides security aspects of the proposed model.

A. PRESERVING PRIVACY

As stated in section II-F5, the proposed model uses ZKP algorithms to preserve the privacy of Buyers. ZKP algorithms provided by Hyperledger Indy are based on the same cryptographic primitives as Identity Mixer (idemix) Cryptographic Library developed by IBM. Idemix is built from a blind signature scheme that supports multiple messages and efficient zero-knowledge proofs of signature possession. The digital signature scheme mainly utilized in idemix is Camenisch-Lysyanskaya (CL) signature scheme that is used to issue credentials [36]. CL Signature allows a user to prove that she has a signature without disclosing the underlying credentials using ZKP. A user can prove that an issuer has given a credential to the user and also can hide or reveal some or all of the attributes of the credential by using a ZKP which shows that she knows a signature of the issuer for the credential. Another feature of CL Signature Scheme is that it supports signing multiple messages, m_1, m_2, \dots, m_L , where L is the number of messages. For this specific digital identity case, it corresponds to signing multiple attributes in a single credential. CL Signature Scheme has the following algorithms [37].

GenerateKey(l_n) \rightarrow (P_k, S_k): On input l_n , outputs a (P_k, S_k) public-private key pair, where l_n denotes the length of the RSA modulus n .

Message Space: Let l_m be a parameter. The message space is the set $\{(m_0, m_1, \dots, m_{L-1}) : m_i \in \pm\{0, 1\}^{l_m}\}$

Sign($(m_0, m_1, \dots, m_{L-1}), S_k$) \rightarrow δ : On input $(m_0, m_1, \dots, m_{L-1})$ and private key S_k , outputs a signature δ .

Verify($(m_0, m_1, \dots, m_{L-1}), \delta, P_k$) \rightarrow *success/fail*: On input message $(m_0, m_1, \dots, m_{L-1})$, signature δ and public key P_k , the algorithm verifies the validity of δ on $(m_0, m_1, \dots, m_{L-1})$. If valid, the algorithm outputs success. Otherwise, it outputs fail.

The protocol for issuing a credential, presenting proof and verification of the proof can be summarized as follows [38]:

- 1) Issuer determines a credential schema S . Credential schema definition includes the number l of attributes in a credential, the indices $A_h \subset \{1, 2, \dots, l\}$ of hidden attributes, the non-revocation credential attribute number l_r , cryptographic signature type, the public key P_k , the non-revocation public key P_r . Issuer publishes the credential definition to the blockchain ledger.
- 2) Holder gets the credential schema from the blockchain ledger and sets the hidden attributes.
- 3) Holder requests a credential from issuer.
- 4) Issuer sets the attributes, including credential index (used for non-revocation) and issues credential C to Holder. In addition, Issuer adds the index to the accumulator for non-revocation.
- 5) Verifier sends proof request ε to Holder. Proof request includes credential schema S and disclosure predicates D . The predicates for attribute m and value V can be of form $m = V$, $m < V$, or $m > V$. Some attributes may be asserted to be the same: $m_i = m_j$.
- 6) Holder checks if she holds credentials satisfying credential schema S and gets non-revocation witness from the blockchain ledger.
- 7) Holder creates a proof P that she has a non-revoked credential satisfying the proof request ε and sends it to verifier.
- 8) Verifier verifies the proof.

B. COMPARISON TO X.509 CERTIFICATES

The process of issuance of digital identity and X.509 certificates is very close in the sense that:

- A set of attributes is signed digitally,
- The digital signature cannot be forged,
- Digitally signed credential is cryptographically bound to a secret key.

However, the signature scheme used in Hyperledger Indy provides efficient zero-knowledge proofs of the possession of a signature and the corresponding attributes without disclosing the signature and attribute values themselves. When X.509 certificate is used, all attributes have to be disclosed to verify the signature. This results in that all usages of the same certificate can be linked to each other. With signatures in Hyperledger Indy, it is not possible to link proofs to original credentials.

V. SECURITY ANALYSIS

A security analysis of the proposed model is performed in two dimensions. First, the model is analysed based on some information security aspects. Then, the model is evaluated

in terms of how it provides protection against some known reputation system attacks.

A. INFORMATION SECURITY ASPECTS

Analysis against information security aspects include privacy of identities, unlinkability of credentials and integrity of stored feedback data.

1) IDENTITY PRIVACY

Identity Privacy requires that other entities cannot identify the real identity of the actor who is presenting credentials. In our model, there are two cases where privacy of credential holder identity is ensured: For feedback tokens, identity of the reviewer is kept private and for discount tokens, identity of the seller and marketplace is kept private.

As explained in section IV-A, our model uses ZKP so that identities of entities are not disclosed when proofs are presented to the verifiers. In addition to ZKP, another mechanism to enhance privacy protection is the usage of link secrets for preventing correlation of credentials. Link secret is a blinded cryptographic commitment to a secret value only known to the holder itself. During credential issuance, link secret is sent to the issuer as a blind attribute, which makes the identifier of the holder unknown to the issuer. The issuer's method of individually signing every claim, which includes the blinded link secret, enables selective disclosure. This means that the issuer has no knowledge of the actual value of the link secret, while the holder is able to prove ownership of their credentials to a verifier without revealing any persistent identifier. In unblinded form, the link secret is not shared with issuers, verifiers, or other parties. It is not possible for a malicious party to use multiple different blinded link secret values to derive the link secret, but it is possible for the holder to prove to a verifier that the same link secret was included in each credential. By the usage of ZKP and link secrets, privacy of the holder identity is ensured in the proposed model.

2) DATA INTEGRITY

Data Integrity requires that data is accurate, consistent, reliable and it has not been altered or tampered with in an unauthorized manner. The proposed model uses a permissioned blockchain, which has the following mechanisms to ensure the integrity of feedback data.

Blockchain in the proposed model employs a consensus protocol that requires participating nodes to agree on the validity of transactions before they are added to the ledger. This consensus mechanism ensures that all nodes have a consistent view of the data stored on the ledger, and any attempts to manipulate the data will be detected and rejected by the network. It also uses digital signatures to provide authentication and ensure that only authorized participants can submit transactions to the network. This mechanism protects the network from unauthorized access and prevents malicious actors from tampering with the data. In addition, it provides end-to-end encryption to secure data in transit and at rest. This ensures that data is protected from unauthorized

access, interception, or modification, providing an additional layer of security and ensuring the integrity of the data.

B. PROTECTION AGAINST KNOWN ATTACKS

The proposed model provides countermeasures for some known attacks against reputation systems.

1) BAD-MOUTHING/SLANDERING

One of the motivations of bad-mouthing and slandering attack is lowering the reputation of a competitor [3], [6], [23]. Many researches show that limiting users to send feedback for sellers only if they were involved in a transaction is a way of tackling bad-mouthing or slandering attacks [2], [6], [23]. An attacker would need to contribute to the sales of a competitor seller to be able to send negative feedbacks. Our model enforces reviewers to have feedback tokens in the form of verifiable credentials to be able to send feedbacks. Feedback tokens are issued only after the completion of an e-commerce transaction. Therefore, feedbacks are one-to-one linked to involved transactions, which helps reducing bad-mouthing and slandering attacks.

2) BALLOT-STUFFING/SELF-PROMOTION

Similar to the prevention of bad-mouthing and slandering attacks, limiting feedback submission to only users involved in transactions is also a countermeasure for ballot-stuffing and self-promoting attacks. For the sellers who have stores in marketplaces, they cannot inject feedbacks for themselves without taking part in transactions since marketplaces issue feedback tokens on behalf of sellers. Therefore, feedback tokens help reducing ballot-stuffing and self-promoting attacks, too. However, for the sellers who have their own e-commerce platforms, there is no way of preventing sellers from issuing fake tokens that will allow submitting positive feedbacks for themselves. As Chang et al. revealed in their survey of approaches for promoting honest recommendations, protecting the privacy of reviewers is a major factor for collecting fair feedbacks [34]. Disclosure of reviewer information may result in unfairly high positive feedbacks [35]. Privacy preserving feature of our model helps reducing dishonest positive feedbacks.

3) WHITEWASHING/RE-ENTRY

One way of preventing whitewashing and re-entry attacks is binding the record of a seller to a real world identity [2], [6], [22]. Requiring digital identities issued by legal authorities ensures that sellers have legal entity identifiers associated with their records in the system. Therefore, exiting from the system and re-joining does not reset previous feedbacks and reputation score.

4) SYBIL ATTACKS

Similar to the prevention of whitewashing and re-entry attacks, digital identities bound to legal entity identifiers prevent creation of multiple identities for a single seller. Sellers are distinguished by their real world identifiers. Obtaining

multiple digital identities from legal authorities does not result in creation of multiple identities in the system.

5) TRAITORS/OSCILLATION

As stated by Hasan et al., this attack can be reduced by considering weights for the feedback scores according to the ages of feedbacks while calculating reputation score [3]. Reputation score calculation algorithm in our model weights the ratings depending on their ages and the amount of transactions. Therefore, the algorithm in our model helps reducing oscillation attacks.

VI. PERFORMANCE EVALUATION

Our reputation system can work together with the existing e-commerce platforms and allows integration with the system through REST APIs. When our reputation system is integrated with an e-commerce platform, it brings some overheads as a trade-off of providing security and privacy by using blockchain. In this section, we provide an evaluation of the system in terms of feasibility of integrating it with e-commerce systems. We have created two servers running on one of the cloud service providers in order to test the latency and blockchain block sizes based on various test cases.

VCS Server runs all the Docker containers needed for Verifiable Credential Subsystem. It is a Linux server running Ubuntu 20.04 LTS version with 16GB RAM and 4vCPUs. Its main duty is to provide a Hyperledger Indy blockchain network with agents used to communicate with the blockchain. It runs the following Docker containers:

- Four containers for establishing a Hyperledger Indy blockchain network.
- One container for monitoring the Hyperledger Indy blockchain network.
- Four containers for agents representing *B*, *S*, *LA* and *FCS* to communicate with the blockchain network.

FCS Server runs all the Docker containers needed for Feedback Collection Subsystem. It is a Linux server running Ubuntu 20.04 LTS version with 16GB RAM and 4vCPUs. Its main duty is to provide a Hyperledger Fabric blockchain network with deployed chaincodes. It runs the following Docker containers:

- Five containers for each of *LA*, *S* and *FCS*: two containers for two peers, two containers for chaincodes and one container for certificate authority.
- Three containers for Orderer nodes.

Although the message exchanges related with the Verifiable Credentials take place on various phases of e-commerce process, they have very close latency values regardless of the case. Table 2 lists these message exchanges with the average latency values observed in the tests. These latency values are used to calculate overall overhead of the system during specific e-commerce processes.

Seller Registration Phase does not intervene with the other e-commerce activities and is totally isolated from purchasing transactions and feedback submissions. Therefore,

TABLE 2. Verifiable credentials message exchanges.

Message Exchange Type	Cases	Average Latency
Issue Credential	Digital Identity(<i>LA</i> to <i>S</i>) Feedback Token(<i>S</i> to <i>B</i>) Discount Token(<i>FCS</i> to <i>B</i>)	172ms
Request Proof	Digital Identity(<i>FCS</i> to <i>S</i>) Feedback Token(<i>FCS</i> to <i>B</i>) Discount Token(<i>S</i> to <i>B</i>)	115ms
Send Proof	Digital Identity(<i>S</i> to <i>FCS</i>) Feedback Token(<i>B</i> to <i>FCS</i>) Discount Token(<i>B</i> to <i>S</i>)	165ms

TABLE 3. Seller registration phase metrics.

#	Step	Average Latency
1	Issue Digital Identity	172ms
2	Request Proof of Digital Identity	115ms
3	Send Proof	165ms
4	Verify Digital Identity and Add Seller to Blockchain	2437ms
	Total	2889ms

TABLE 4. Get feedbacks of a seller.

Feedback Size	Response Time
1KB	180 ms
2KB	250 ms
3KB	218 ms
4KB	276 ms
8KB	227 ms
16KB	241 ms
26KB	269 ms
32KB	301 ms
66KB	214 ms
132KB	440 ms
176KB	382 ms
264KB	562 ms
440KB	810 ms
768KB	1496 ms
1034KB	2109 ms

any latency in the Seller Registration Phase does not have an impact on these e-commerce activities. However, since this phase brings extra steps, we still provide the metrics related with this phase.

Shopping Phase includes *S* issuing Feedback Token to *B* after an order is created in the system with a purchasing transaction. However, issuing Feedback Token is not part of purchasing transaction and does not extend the duration of the transaction. When a purchasing transaction is completed, a message is placed into the Message Queue of the system and the message is handled asynchronously without interrupting the transaction. When the message is processed, issuing Feedback Token to *B* lasts 172ms, as depicted in Table 2. Another possible user activity during Shopping Phase is retrieving feedbacks of a specific *S* in order to have an idea about the performance of *S*. We tested the function for getting feedbacks of an *S* with varying sizes of feedbacks stored in the blockchain. Table 4 shows the varying response times depending on the size of feedbacks stored.

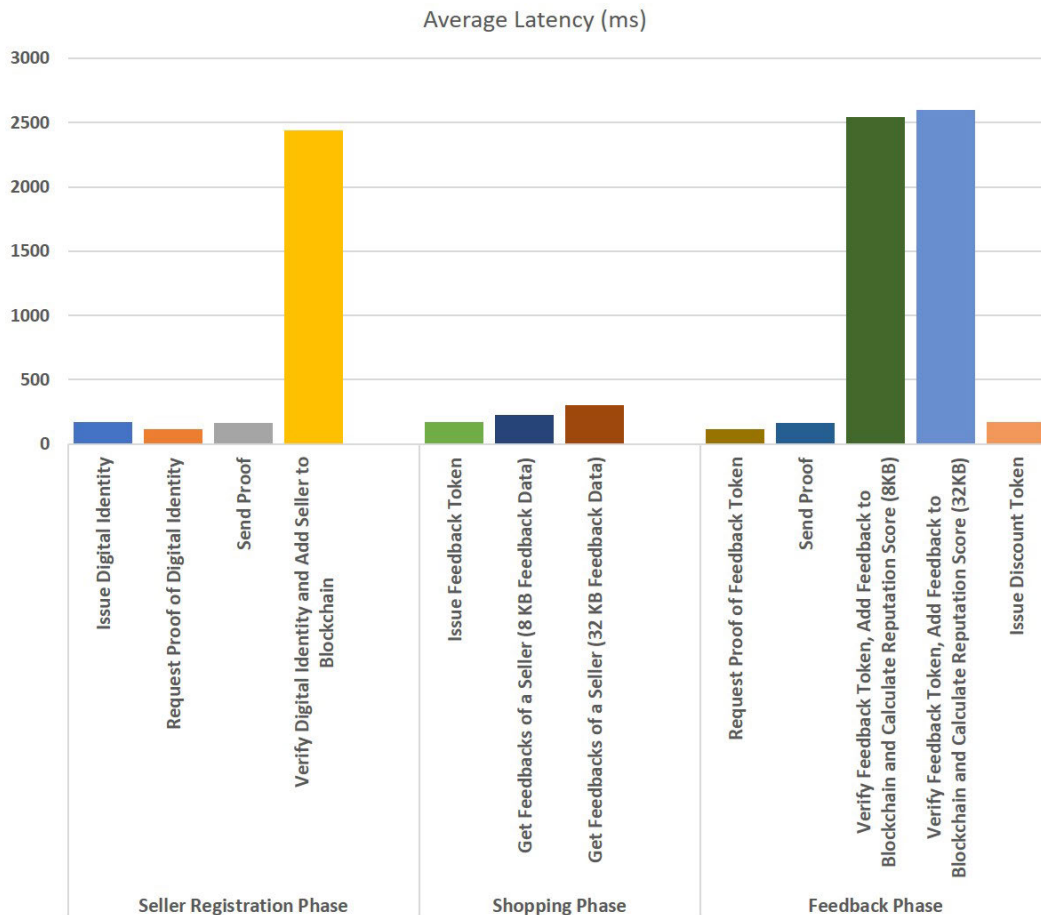


FIGURE 7. Average latency of each step.

TABLE 5. Feedback phase metrics.

#	Step	Average Latency
1	Request Proof of Feedback Token	115ms
2	Send Proof	165ms
3	Verify Feedback Token, Add Feedback to Blockchain and Calculate Reputation Score	2540ms
4	Issue Discount Token	172ms
	Total	2992ms

As seen in Table 4, response time increases as the size of the stored feedback records increases, which is an expected behaviour. However, even the response time of the test with approximately 1MB of feedback for only one seller does not exceed 2.1 seconds. The observed response times for getting feedback records from blockchain are evaluated as acceptable.

Feedback Phase includes all steps related with the submission of feedbacks by *B* for an *S* to the *FCS* in order to store them in the blockchain. It is a prerequisite for this phase that *B* should have already received Feedback Token from *S*.

We tested Step 3 of Feedback Phase in more details with varying sizes of feedback messages submitted by *B*

TABLE 6. Verify feedback token, add feedback to blockchain and calculate reputation score.

Feedback Size	Message	Response Time	Block Size Created on Blockchain
125B		2471ms	6K
250B		2518ms	6K
500B		2519ms	7K
1KB		2577ms	8KB
2KB		2504ms	10KB
4KB		2502ms	14KB
8KB		2540ms	22KB
16KB		2648ms	38KB
24KB		2548ms	54KB
32KB		2599ms	70KB

As seen in Table 6, size of the feedback message does not have a significant impact on the response time of feedback submission function. However, the size of the block created on Hyperledger Fabric blockchain increases as the size of the feedback message increases, which is an expected behaviour.

The overall impact of our system on each phase of the e-commerce process can be seen in Figure 7. As seen in the figure, issuance of the credentials, proof requests and sending proofs have very little latency. The highest latency impact

comes with the steps that involve credential verification and adding data to blockchain.

VII. CONCLUSION

In this paper, we have presented a blockchain-based privacy preserving reputation system focusing on the e-commerce market. The system is composed of two main modules each with a specific purpose, aimed at achieving the overall objective of privacy preserving, immutable and secure reputation system. The first module of the proposed system is the Verifiable Credentials Subsystem, which aims to provide an end-to-end verifiable credential issuance and verification infrastructure. The second module is the Feedback Collection Subsystem, and its purposes are receiving feedbacks from buyers after verifying that they hold a valid feedback token, calculating reputation score using our genuine algorithm and issuing discount tokens on behalf of sellers and marketplaces.

Building the system on top of blockchain technology implicitly brings decentralization, immutability and security on the infrastructure layer. We have chosen a permissioned blockchain, namely Hyperledger Fabric, with efficient consensus mechanism, which provides a high performant platform compared to public blockchains. Integration of verifiable credentials as digital identities of the sellers, proofs of performed e-commerce transactions and proofs of feedback submissions make our model an innovative reputation system. Using Hyperledger Indy blockchain for the implementation of verifiable credentials provides a robust system and brings additional capabilities such as Zero Knowledge Proofs. ZKPs enable our system to present the verifiable credentials securely and protect the privacy of buyers, which encourages users to send honest feedbacks. Security analysis (V-A) of the system proves that the system provides privacy of reviewer identities and integrity of the feedback data. Limiting feedback submissions only to purchasing users is an effective protection against bad-mouthing and ballot stuffing attacks. Another measure of our reputation system for honest feedbacks is the discount tokens issued in consequence of feedback submissions. Binding legal identities of sellers to digital identities prevents identity related attacks, such as whitewashing and Sybil attacks. Having all these features, our reputation system provides security measures for the attacks listed in section V-B against reputation systems.

We have also developed a software system of the proposed model and deployed on servers hosted on a cloud provider. We have evaluated the performance of the system using various test cases. The results of the tests show that it is quite feasible to apply and integrate the proposed system into the existing e-commerce ecosystem.

For future work, we consider to focus on possible interoperability issues of our reputation system with multiple real world e-commerce systems. Although our experiments show that the developed prototype is feasible from the performance point of view, the diversity of existing e-commerce systems would require to deal with new challenges during integration. Another area for future work is linking the reviews to prod-

ucts in the purchase as well as sellers. This additional link information would display the linked products with their prices and help buyers decide whether there are any suspicious products with extremely low prices.

REFERENCES

- [1] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in P2P networks," in *Proc. 12th Int. Conf. World Wide Web (WWW)*, 2003, pp. 640–651.
- [2] E. Koutrouli and A. Tsalgatidou, "Taxonomy of attacks and defense mechanisms in P2P reputation systems—Lessons for reputation system designers," *Comput. Sci. Rev.*, vol. 6, nos. 2–3, pp. 47–70, May 2012.
- [3] O. Hasan, L. Brunie, and E. Bertino, "Privacy preserving reputation systems based on blockchain and other cryptographic building blocks: A survey," INSA-Lyon, Univ. Lyon, Lyon, France, Tech. Rep. CNRS-LIRIS-UMR5205, Nov. 2020.
- [4] J. Ahn, M. Park, H. Shin, and J. Paek, "A model for deriving trust and reputation on blockchain-based e-payment system," *Appl. Sci.*, vol. 9, no. 24, p. 5362, Dec. 2019.
- [5] S. Sun, Y. Liu, and G. Guo, "A privacy-preserving and robust reputation system based on blockchain," in *Proc. IEEE Int. Conf. Parallel Distrib. Process. Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom)*, Dec. 2019, pp. 634–639.
- [6] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," *ICT Systems Security and Privacy Protection*. Cryptology ePrint Archive, 2016, pp. 398–411.
- [7] E. Owiyo, Y. Wang, E. Asamoah, D. Kamenyi, and I. Obiri, "Decentralized privacy preserving reputation system," in *Proc. IEEE 3rd Int. Conf. Data Sci. Cyberspace (DSC)*, Jun. 2018, pp. 665–672.
- [8] S. Tamang, "Decentralized reputation model and trust framework blockchain and smart contracts," Uppsala Univ., Dept. Inf. Technol., Uppsala, Sweden, Tech. Rep., 2018.
- [9] A. Dhakal and X. Cui, "DTrust: A decentralized reputation system for e-commerce marketplaces," Wuhan Univ., Wuhan, China, Tech. Rep., Apr. 2019.
- [10] M. Zulfiqar, F. Tariq, M. U. Janjua, A. N. Mian, A. Qayyum, J. Qadir, F. Sher, and M. Hassan, "EthReview: An Ethereum-based product review system for mitigating rating frauds," *Comput. Secur.*, vol. 100, Jan. 2021, Art. no. 102094.
- [11] D. Carboni, "Feedback based reputation on top of the Bitcoin blockchain," *CoRR*, vol. abs/1502.01504, pp. 1–10, Feb. 2015.
- [12] M. Buechler, M. Eerabathini, C. Hockenbrocht, and D. Wan, "Decentralized reputation system for transaction networks," Univ. Pennsylvania, Philadelphia, PA, USA, Tech. Rep., 2015.
- [13] K. Wang, Z. Zhang, and H. S. Kim, "ReviewChain: Smart contract based review system with multi-blockchain gateway," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (Smart-Data)*, Jul. 2018, pp. 1521–1526.
- [14] A. Almasoud, "Smart contracts for blockchain-based reputation systems," Faculty Eng. Inf. Technol., Univ. Technol. Sydney, Ultimo NSW, Australia, 2020.
- [15] R. Ramachandiran, "Using blockchain technology to improve trust in e-commerce reviews," Univ. Maryland, College Park, MD, USA, Tech. Rep., May 2018.
- [16] K. Soska, A. Kwon, N. Christin, and S. Devadas, "Beaver: A decentralized anonymous marketplace with secure reputation," *IACR Cryptol. ePrint Arch.*, vol. 2016, p. 464, Aug. 2016.
- [17] G. S. Mendes, D. Chen, B. M. C. Silva, C. Serrao, and J. Casal, "A novel reputation system for mobile app stores using blockchain," *Computer*, vol. 54, no. 2, pp. 39–49, Feb. 2021.
- [18] R. Omori and J. Kishigami, "Incorporating reputation system in blockchain-based distributed auctions," in *Proc. IEEE 8th Global Conf. Consum. Electron. (GCCE)*, Oct. 2019, pp. 1115–1117.
- [19] J.-S. Park, T.-Y. Youn, H.-B. Kim, K.-H. Rhee, and S.-U. Shin, "Smart contract-based review system for an IoT data marketplace," *Sensors*, vol. 18, no. 10, p. 3577, Oct. 2018.
- [20] M. Nguyen, Q. Bai, and J. Yu, "A blockchain-based trust model for crowd environments," in *Proc. Australas. Comput. Sci. Week Multiconf. (ACSW)*, Feb. 2020, pp. 1–7.
- [21] C. Kugblenu and P. Vuorimaa, "Decentralized reputation system on a permissioned blockchain for e-commerce reviews," in *Proc. 17th Int. Conf. Inf. Technol.-New Gener. (ITNG)*, 2020, pp. 177–182.

- [22] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-based distributed trust and reputation management systems: A survey," *IEEE Access*, vol. 8, pp. 21127–21151, 2020.
- [23] Y. Cai and D. Zhu, "Fraud detections for online businesses: A perspective from blockchain technology," *Financial Innov.*, vol. 2, no. 1, Dec. 2016, Art. no. 20.
- [24] G. Andrade, "Technical analysis of reputation systems based on blockchain technologies," Hochschule Angewandte Wissenschaften Hamburg, Hamburg, Germany, Tech. Rep., 2019.
- [25] A. S. Almasoud, F. K. Hussain, and O. K. Hussain, "Smart contracts for blockchain-based reputation systems: A systematic literature review," *J. Netw. Comput. Appl.*, vol. 170, Nov. 2020, Art. no. 102814.
- [26] A. Battah, Y. Iraqi, and E. Damiani, "Blockchain-based reputation systems: Implementation challenges and mitigation," *Electronics*, vol. 10, no. 3, p. 289, Jan. 2021.
- [27] D. Vandervort, "Challenges and opportunities associated with a Bitcoin-based transaction rating system," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer, 2014, pp. 33–42.
- [28] M. Basili and M. A. Rossi, "Platform-mediated reputation systems in the sharing economy and incentives to provide service quality: The case of ridesharing services," *Electron. Commerce Res. Appl.*, vol. 39, Jan. 2020, Art. no. 100835.
- [29] S. Nakamoto. (Mar. 2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [30] M. Sporny, D. Longley, and D. Chadwick. (Nov. 2019). *Verifiable Credentials Data Model 1.0*. [Online]. Available: <https://www.w3.org/TR/vc-data-model>
- [31] N. Otto, S. Lee, B. Sletten, D. Burnett, M. Sporny, and K. Ebert. (Sep. 2019). *Verifiable Credentials Use Cases*. [Online]. Available: <https://www.w3.org/TR/vc-use-cases>
- [32] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems," in *Proc. 17th Annu. ACM Symp. Theory Comput.*, 1985, pp. 291–304.
- [33] J. Groth, "Short pairing-based non-interactive zero-knowledge arguments," in *Advances in Cryptology—ASIACRYPT 2010*. Berlin, Germany: Springer, 2010, pp. 321–340.
- [34] J. Chang, L. Xiao, and W. Xu, "A survey of approaches for promoting honest recommendations in reputation systems," in *Computer Engineering and Technology*. Singapore: Springer, 2019, pp. 179–191.
- [35] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system," in *The Economics of the Internet and E-Commerce (Advances in Applied Microeconomics)*. Bingley, U.K.: Emerald (MCB UP), vol. 11, Oct. 2002.
- [36] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in *Security in Communication Networks*, vol. 2576, S. Cimato, G. Persiano, and C. Galdi, Eds. Berlin, Germany: Springer, 2003, pp. 268–289.
- [37] J. Camenisch, "Specification of the identity mixer cryptographic library," IBM Res., Zürich, Switzerland, Res. Rep. 99740, Apr. 2010.
- [38] M. Lodder and D. Khovratovich, "Anonymous credentials 2.0," Tech. Rep., p. 12.
- [39] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Informat.*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.
- [40] M. Li, L. Zhu, Z. Zhang, C. Lal, M. Conti, and M. Alazab, "Anonymous and verifiable reputation system for e-commerce platforms based on blockchain," *IEEE Trans. Netw. Serv. Manage.*, vol. 18, no. 4, pp. 4434–4449, Dec. 2021, doi: 10.1109/TNSM.2021.3098439.
- [41] D. L. Fekete and A. Kiss, "A survey of ledger technology-based databases," *Future Internet*, vol. 13, no. 8, p. 197, Jul. 2021, doi: 10.3390/fi13080197.
- [42] X. Yang, Y. Zhang, S. Wang, B. Yu, F. Li, Y. Li, and W. Yan, "LedgerDB: A centralized ledger database for universal audit and verification," *Proc. VLDB Endowment*, vol. 13, no. 12, pp. 3138–3151, Aug. 2020, doi: 10.14778/3415478.3415540.
- [43] M. J. Amiri, T. Allard, D. Agrawal, and A. E. Abbadi, "PRVer: Towards private regulated verified data," OpenProceedings.org, Tech. Rep., 2022, doi: 10.48786/EDBT.2022.40.
- [44] X. Yang, S. Wang, F. Li, Y. Zhang, W. Yan, F. Gai, B. Yu, L. Feng, Q. Gao, and Y. Li, "Ubiquitous verification in centralized ledger database," in *Proc. IEEE 38th Int. Conf. Data Eng. (ICDE)*, Kuala Lumpur, Malaysia, May 2022, pp. 1808–1821, doi: 10.1109/ICDE53745.2022.00181.



ÖMER DOĞAN was born in Denizli, Turkey, in 1980. He received the bachelor's degree in electrical and electronics engineering and the master's degree in software management from Middle East Technical University (METU), Ankara, in 2003 and 2015, respectively. He is currently pursuing the Ph.D. degree in management information systems with Gazi University, Turkey. He has been a software professional, since 2001, in various areas of software development, including blockchain systems.



HACER KARACAN (Member, IEEE) was born in Erzurum, Turkey, in 1980. She received the bachelor's degree from the Department of Computer Education, Middle East Technical University (METU), Ankara, in 2002, and the master's and Ph.D. degrees from the Cognitive Science Department, METU, in 2005 and 2007, respectively. She started her academic career as a Research Assistant with the Department of Cognitive Science, METU, in 2002. During her Ph.D. studies, she was a Visiting Researcher with the University of Rochester, USA. She is currently a Professor with the Computer Engineering Department, Gazi University, where she has been a Faculty Member, since 2007. Her research interest includes artificial intelligence methods to gain data insights. She is particularly interested in understanding data flow patterns and potential causal factors in cyber security problems.