A Blockchain-based E-Commerce Reputation System Built with Verifiable Credentials

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 relatedattacks. Finally, the use of smart contracts ensures transparency and immutability, which enhances the overall reliability of the system.

**EXISTING SYSTEM**

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 are not preserved since they are kept with their basic information.

**Disadvantages**

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

Proposed System

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.

**Advantages**

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.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL