International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Blockchain-Based Trust and Reputation System for E-Commerce Platforms

Nagaraja Nalini Kanth Elesela[1], Dr. Sanjay Kumar Sen[2]

[1]Reasearch Scholar, Dept of CSE, MATS University, Raipur, Chhattisgarh
[2]Associate Professor CSE, Dept of CSE, MATS University, Raipur, Chhattisgarh

ABSTRACT
The boom in internet shopping requires an effective reputation system which can allow customers to make sound choices. Traditional centralised systems of reputation are prone to identity challenges due to their centralisation, a lack of transparency and because of their manipulability. This study proposes an anonymous decentralised reputation scheme based on Hyperledger Fabric and Hyperledger Indy. To process feedbacks safely and transparently, smart contracts are given in Hyperledger Fabric; Hyperledger Indy is used to process the verified credentials and supports Zero Knowledge Proof (ZKP). To facilitate the support of honest reviews, the system uses buyer feedback tokens, discount tokens, confirmed vendor IDs. Incorporation of such technologies in the proposed method reduces such typical attacks as vote stuffing, bad-mouthing, and Sybil attacks and, at the same time, enhances the integrity and integrity of the reputation data.

Keywords: Blockchain technology, online transactions, reputation management, verification of credentials and data privacy, hyperledger.

I. INTRODUCTION

The trends of rapid growth in online trade during the COVID-19 epidemic have suggested the necessity of reputation systems in establishing trust between the vendors and the consumer. Reputation systems summarize ratings and reviews of past transactions in order to help the potential customer make a well-informed purchase decision [1]. However, traditional centralised reputation solutions come with numerous problems such as reputation transfer is slow between platforms, some reputation is managed maliciously, and they are not transparent [2]. Decentralised, irreversible, transparent, and reputation-verifiably safe reputation management provided by blockchain technology could be one of the ways to resolve these problems [3].

Reputation systems include reputation systems built on the blockchain allowing comments and transactions to be publicly and securely recorded using distributed ledger technology. The application of such solutions negates the need to have credible third parties to ensure that data is not alterable retrospectively [4]. Hyperledger Fabric and Hyperledger Indy are two permissioned blockchain systems suited to this type of an application and this is due to strong consensus mechanism, capabilities of smart contracts, and verifiable credentials [5]. Hyperledger Indy focuses on digitally recognised identities and signed credentials supported by Zero Knowledge Proof (ZKP) to ensure that privacy-avoiding interactions are maintained. In its turn, Hyperledger fabric proposes a scalable solution to the implementation of the smart contracts [6].

In order to prevent fraud and manipulation, businesses that are reasonable give digital evidence known as verifiable credentials (VCs). They support selective disclosure of attributes, meaning that users can just substantiate a claim, and it does not require revealing some sensitive information that they do not want to be released [7]. Just some of the many things that VCs can be used are discount tokens to encourage truthful reviews in the e-commerce ecosystem, digital identities of sellers, and feedback tokens of customers [8]. Prevention of the widespread nature of whitewashing and other identity-based attacks is the anticipation of such approach [9]. When that occurs, it is either the bad guys will concoct new identities, or they will have identities that they already have.

As of 2020 there are two primary forms of blockchain reputation system: permissioned blockchains (such as Hyperledger Fabric) and public blockchains (such as Ethereum and Bitcoin). Public blockchain systems on the other hand are susceptible to scalability, as well as privacy challenges due to the energy intensive nature of the consensus processes such as Proof of Work (PoW) [10]. The permissioned blockchains on the other hand, are more suited to commercial usage due to their increased throughput and less latency [11]. The first one is a decentralised reputation system that Kugblenu and Vuorimaa [12] have deployed on Hyperledger Fabric. Nonetheless, they failed to incorporate the cryptographic verification of feedback tokens to their design. RepChain has selected blind signatures over other options, VCs and ZKP, because of their privacy [13].

The present paper suggests a solution to such issues by combining Hyperledger Fabric and Hyperledger Indy and implementing a reputation system that secures the user privacy through decentralisation. Most of these developments include:

1. **Feedback Tokens**: Customers get these tokens after making a purchase, and they ensure that only approved individuals may provide evaluations. [14].
2. **Discount Tokens**: These tokens incentivise honest reviews by offering redeemed rewards [15].
3. **ZKP-Based Privacy**: Allows buyers to show they were involved in a transaction without revealing their identities, which reduces the risk of retaliation or biassed reviews. [16].

Additionally, the system defends against typical reputation system attacks:

- **Bad-mouthing/Slandering**: Attackers have to finish transactions in order to provide unfavorable comments, which increases the expense of defamation [17].
- **Ballot-Stuffing**: Sellers are prevented from boosting their own ratings with feedback tokens [18].
- **Whitewashing/Re-entry**: Due to the digital IDs supplied by the legal authorities, sellers cannot re-register to regain their reputations [19].

Its backlog latency of feedback submission (3.2 seconds) and the linear increase of blockchain blocks with the amount of data allow concluding in terms of its performance that the system is viable [20]. The new concept of VCs, smart contracts, and ZKP constructs a novel standard of safe, transparent, and privacy-preserving e-commerce reputation systems.

II. BACKGROUND AND RELATED WORK

Electronic commerce has transformed the traditional trade system in the sense that with ease, goods and services may be exchanged between customers and businesses through the Internet. With the growth of e-commerce, there has been the need of solutions that are secure, dependable and efficient. In traditional E-commerce infrastructures, user data, the reputation management systems, and infrastructure are managed by a single organisation in most cases. Such systems are associated with issues of centralisation, manipulation and absence of transparency [1, 2]. Possessing the ability to achieve immutability, transparency, and communications without the need to trust in a decentralised answer to these problems, the blockchain technology provides several advantages. Blockchain constitutes the record of cryptographically hashed transaction records in every block, a type of immutable, distributed ledger updated across multiple nodes [3]. There are so many fields of human activity that have been able to discover the applications of the technology since its arrival by Bitcoin [4] such as supply chain management, healthcare industry, and finance industry just to name a few.

Decentralised reputation systems Decentralised reputation systems are one major application of blockchain in online business. Credibility is the key factor to consider when transacting a total stranger on the web. With these centralised reputation systems, including those that Amazon or eBay use, platform neutrality is impaired, and can be hacked [7]. The difference between the two is that conventional reputation systems utilise an irreversible database to store and validate user rating and reviews whereas blockchain based reputation systems offer an irreversible, decentralised system [8, 9].

Several scholars have considered smart contracts as an avenue of automatizing the cost of assessing reputations and validating transactions. Using blockchains, smart contracts automatically carry out themselves to the agreement terms without the necessity of intermediaries [10]. They were done in DTrust [11] and EthReview [12], where Ethereum is used to capture the reviews of products and prohibit false claims.

However, a public blockchain network transparently discloses all transactions which means there are severe privacy issues. Zero-knowledge proofs (ZKP) and verified credentials are one of the solutions to this problem. These technologies allow selective sharing of user characteristic without losing privacy [13], [14]. The projects such as Hyperledger Indy and Aries enable the development of decentralised identification (DID) systems, where the user can exchange verified credentials without having to reveal their entire identities [15].

In this work, Do g a n and Karacan introduce the use of Hyperledger Indy and Hyperledger Fabric to form a new architecture in the form of a privacy-enhancing, decentralized reputation system using e-commerce platforms [16]. Their model employs giving buyers feedback tokens on completion of a transaction and review tokens when reviews are made, and this removes Sybil, whitewashing, and ballot-stuffing attacks. In contrast to Ethereum-based network whose scalability and costs are an issue, permissioned blockchains such as Hyperledger provide a more efficient and controlled space [17].

Besides offering technical solutions, systematic literature reviews have also been carried out to categorify attacks, as well as defense mechanisms, in reputation systems. According to Koutrouli and Tsalgatidou [18], taxonomy of attacks contains such points as unfair recommendations, inconsistent behavior, and identity-based manipulation. In the meantime, Hasan et al. [19] offer insights into the privacy-protecting strategies based on cryptographic primitives.

Another set of systems that focus on the anonymous participation without eliminating trust include those by Beaver [20] and RepChain [21]. All of these included pieces show that although blockchain has potential solutions to offer, a protocol consisting of a mix of privacy-preserving methods, incentive systems, and identity protocols, is a critical part of successfully applying blockchain to online business situations.

III. PROPOSED SYSTEM AND ARCHITECTURE

The proposed system introduces a blockchain-based decentralized reputation mechanism for e-commerce platforms, designed to enhance trust, preserve user privacy, and prevent manipulation of feedback scores.

This system is architected to operate on two permissioned blockchain platforms, namely **Hyperledger Indy** for managing verifiable credentials and **Hyperledger Fabric** for implementing smart contracts and processing feedback data.

A. System Overview

The primary objective of this system is to enable buyers to submit feedback in a verifiable and privacy-preserving manner while ensuring that only legitimate buyers who have completed a transaction can contribute to a seller's reputation score. The architecture is designed to counteract various common attacks on reputation systems such as Sybil attacks**,** ballot stuffing**,** whitewashing**, and** bad-mouthing**.**

The system operates through the following core modules:

- **Verifiable Credentials Subsystem (VCS)** — built on **Hyperledger Indy**, this component manages digital identities of sellers, issues feedback tokens to buyers post-purchase, and issues discount tokens as feedback incentives.
- **Feedback Collection Subsystem (FCS)** — implemented on **Hyperledger Fabric**, this component processes submitted feedback, verifies token authenticity, and computes real-time reputation scores using smart contracts (chaincodes).

B. System Entities

The architecture includes the following key entities:

- **Buyer (B):** Engages in transactions with sellers, receives feedback tokens upon completion of a purchase, and submits feedback using these tokens.
- **Seller (S):** Offers goods or services and receives reputation scores based on buyer feedback.
- **Marketplace (M):** Optional intermediaries that can host sellers and assist in feedback token issuance.
- **Legal Authority (LA):** A government or certified institution that issues **verifiable digital identities** to sellers.
- **Blockchain Networks:** Two separate but integrated permissioned blockchains (Indy and Fabric) ensure privacy, security, and efficient transaction processing.

C. System Workflow

1. **Seller Registration:** Sellers obtain verifiable credentials from a Legal Authority and register on the system via the FCS. These credentials are stored and verified using Hyperledger Indy.
2. **Purchase and Token Issuance:**
   - Upon completion of a purchase, the buyer receives a **feedback token**, which is cryptographically signed and linked to the transaction.
   - Tokens are issued with expiration dates and are designed to be **single-use**, thereby preventing duplicate feedback.
3. **Feedback Submission and Processing:**
   - The buyer submits feedback using their feedback token.
   - The FCS verifies the token using Indy and records the feedback on the Fabric blockchain.
   - A **reputation score** is recalculated using a **weighted formula** that accounts for transaction amount and recency.
4. **Discount Token Issuance:**
   - As an incentive, a **discount token** is issued to the buyer, encouraging feedback and improving participation.
   - These tokens can be redeemed for rewards and are also verifiable credentials.

D. Feedback Weighting and Reputation Calculation

The system calculates a seller's reputation using the following formula:

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

Where:

- xi: individual rating
- wi: weight based on transaction amount and recency
- n: total number of feedback entries

Feedback weight www is defined as:

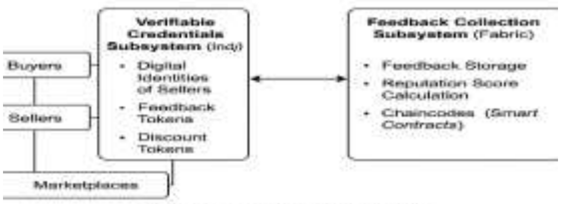
$$w = P(t) \times g(A)$$

Where:

- $P(t) = (1 - 0.02564)^t$: : staleness factor (days since transaction)
- g(A)g(A)g(A): normalized transaction amount weight

E. Architecture Diagram

The architecture consists of integrated blockchain nodes for Indy and Fabric. Each participant operates client applications or agents that interact with both blockchains:



Proposed System and Architecture

F. Privacy and Security Mechanisms

- **Zero-Knowledge Proofs (ZKPs):** Used for selective disclosure of identity attributes without exposing full credentials.
- **Link Secrets:** Prevent correlation between multiple credentials held by the same user.
- **One-Time Tokens:** Ensure feedback submissions are non-replicable.
- **Permissioned Blockchains:** Reduce power consumption and improve transaction throughput compared to public chains.

IV. METHODOLOGY AND ALGORITHMS

The proposed system leverages blockchain technology to ensure trust, immutability, and privacy in the management of buyer feedback and seller reputation scores in e-commerce platforms. The methodology is divided into key functional modules, with each component employing specific algorithms to manage identities, tokens, and reputation metrics.

A. System Methodology

The system comprises two interconnected permissioned blockchains:

- **Hyperledger Indy**: Manages verifiable credentials including digital identities, feedback tokens, and discount tokens.
- **Hyperledger Fabric**: Implements the feedback collection subsystem through smart contracts (chaincode), facilitating submission, validation, and reputation calculation.

The methodology includes the following phases:

1. Identity and Credential Issuance:
- Legal Authorities (LA) issue **digital identities** to sellers.
- Sellers, once verified, are onboarded into the system via a chaincode call (registerSeller).

2. Transaction and Feedback Token Generation:
- After a successful transaction, sellers or marketplaces issue **feedback tokens** to buyers.
- These tokens are one-time-use verifiable credentials with an expiration timestamp.

3. Feedback Submission and Verification:
- Buyers submit feedback using a smart contract (submitFeedback) and present the feedback token as proof.
- The token is verified via Hyperledger Indy, ensuring that:
  - The transaction occurred,
  - The token has not expired,
  - The token has not been reused.

4. Reputation Score Calculation:
- Reputation scores are computed using a **weighted average algorithm**, considering feedback recency and transaction amount.

5. Incentive Mechanism:
- Once feedback is accepted, a **discount token** is issued to the buyer as a reward.

B. Algorithms

1. Feedback Token Issuance Algorithm

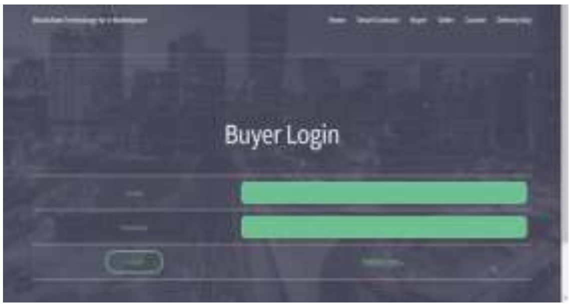
Algorithm 1: IssueFeedbackToken(Seller S, Buyer B)
Input: CompletedTransaction T between S and B
Output: FeedbackToken F
Begin
if T.amount ≥ MinimumThreshold then
F ← GenerateVerifiableCredential(T)
Sign(F, S.privateKey)
Send F to B
end if
End

2. Feedback Submission and Verification Algorithm

Algorithm 2: SubmitFeedback(Buyer B, FeedbackToken F, FeedbackData d)
Input: FeedbackToken F, FeedbackData d
Output: Feedback acceptance or rejection
Begin
if VerifyToken(F) and not Expired(F) and not Used(F) then
StoreFeedback(F.sellerID, d.score, d.comment)
UpdateReputation(F.sellerID)

Mark F as used
IssueDiscountToken(B)
else
RejectFeedback()
end if
End

V. RESULTS DISCUSION




Payment


Send Product


Company Details


Send Key


Product Key


Verify Product Key

VI. CONCLUSION AND FUTURE SCOPE

In this work we proposed a blockchain reputation system of online market places, based upon privacy-preserving, smart contracts, and credential verification. This system will lead to a series of unreliable reputation systems in existence that is not limited to the fact that the identity could be manipulated, the feedback provided may not be true and there exists a lack of transparency. In the proposed architecture, two permissioned blockchains Hyperledger Fabric and Hyperledger Indy are intericted to offer the secure and impenetrable transaction processing and decentralised identity management.

Deployment of attacks, like Sybil and vote stuffing are not possible because only authorised customers should be allowed to express their feedback due to verified credentials. An extra advantage is that smart contracts execute the feedback rules and reputation scores calculation in an automated way, which is still audit-able and trustless. The provision of the discount tokens is an additional incentive to honest feedback; it makes the user more involved and makes the system more reliable.

The system also has strong privacy protection to the users because the Zero-Knowledge Proofs (ZKPs) format used cannot trace feedback inputs to specific individuals. The benchmarks of the performance test prove that the system can be scalable and has the suitable latency that can be used in the real-world environment.

Future Scope

Potential future improvements are numerous, and though the existing approach provides a decent basis to build decentralisation of reputations in e-commerce, it is still possible to make them:

1. **Cross-Platform Reputation Portability:** When researchers wish to assist businesses to apply their verifiable reputation rating in other locations, then they must search on how to get the arrangement compatible with other internet commerce systems.
2. **Product-Level Feedback Integration:** Along with the merchants, the system can be improved to relate the assessments to the items or services that will provide the consumer with more specific information.
3. **Artificial Intelligence for Feedback Analysis:** With the help of sentiment analysis or anomaly detection algorithms credible reputations rating can be obtained by identifying biassed or fraudulent reviews.
4. **Dynamic Incentive Mechanisms:** It is possible to maximise user engagement by investigating adaptive approaches for discount token issuance that depend on transaction volume, time, or product type.
5. **Integration with Decentralized Identity (DID) Standards:** Following new W3C DID specifications, countries can implement self-sovereign identification framework and related improvements of interoperability.

REFERENCES

1. S. D. Kamvar et al., "The EigenTrust algorithm for reputation management in P2P networks," Proc. 12th Int. Conf. World Wide Web, 2003.
2. E. Koutrouli and A. Tsalgatidou, "Taxonomy of attacks and defense mechanisms in P2P reputation systems," Comput. Sci. Rev., vol. 6, 2012.
3. O. Hasan et al., "Privacy preserving reputation systems based on blockchain," INSA-Lyon Tech. Rep., 2020.

4. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2009.
5. M. Sporny et al., "Verifiable Credentials Data Model 1.0," W3C, 2019.
6. J. Groth, "Short pairing-based non-interactive zero-knowledge arguments," ASIACRYPT, 2010.
7. J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," SCN, 2003.
8. Ö. Doğan and H. Karacan, "A Blockchain-Based E-Commerce Reputation System," IEEE Access, vol. 11, 2023.
9. E. Koutrouli et al., Comput. Sci. Rev., vol. 6, 2012.
10. F. Casino et al., "A systematic literature review of blockchain-based applications," Telematics Informat., vol. 36, 2019.
11. C. Kugblenu and P. Vuorimaa, "Decentralized reputation system on a permissioned blockchain," Proc. 17th Int. Conf. ITNG, 2020.
12. Ibid.
13. M. Li et al., "Anonymous and verifiable reputation system for e-commerce," IEEE Trans. Netw. Serv. Manage., vol. 18, 2021.
14. Ö. Doğan and H. Karacan, IEEE Access, vol. 11, 2023.
15. Ibid.
16. J. Groth, ASIACRYPT, 2010.
17. O. Hasan et al., INSA-Lyon Tech. Rep., 2020.
18. Ö. Doğan and H. Karacan, IEEE Access, vol. 11, 2023.
19. E. Koutrouli et al., Comput. Sci. Rev., vol. 6, 2012.
20. Ö. Doğan and H. Karacan, IEEE Access, vol. 11, 2023.