iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35262

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Optimization of E-Commerce Platform Structure based on Blockchain Technology

Vijayalakshmi C[1], Aruna M[2], Harini T M[3], Krithikaa K[4]
[1]*Associate Professor,* [2, 3, 4]*UG Students, Panimalar Engineering College*

Abstract: ***E-Commerce has become more and more popular because of rich products, fast transactions, and free from time, locations, stores, and so on. However, the disclosure of personal data such as their IDs, addresses, and phone numbers has become a major concern for online activities. The current e-commerce model is at the crossroads of ownership and privacy. To address this, this article creates an enterprise protocol that uses smart personal contracts to protect privacy during the negotiation phase. This protocol allows contracting parties to conduct business without disclosing personal information such as identity, address, and phone number. Furthermore, we employ the zero-knowledge proof to ensure ownership.***
Keywords: BlockChain, Token, Ledger, Smart Contract, Zero-Knowledge Proof, E-commerce, Cryptography, Online Transaction.

I. INTRODUCTION

E-Commerce has grown in popularity as a result of the wide range of products available, the speed with which transactions can be completed, and the lack of time, location, and store constraints. However, internet activities have made the revelation of personal data such as IDs, addresses, and phone numbers a big problem. In fact, it has created a huge "gray industry" that seriously threatens user security and privacy. It's not uncommon for sellers to threaten customers and force them to create, modify, or delete product reviews that are against their will. Meanwhile, online store websites also suffer from malicious, bad reviews or fake praise reviews that degrade the quality of the experience. There is already research and practice on these issues. Janice Tsai and others show that consumers are more likely to pay for privacy protection. Berendt and others propose PET that provides more timely privacy protection and web application trust tools. Li et al. Present a consistent adaptive trust model based on a transaction feedback system that quantifies and compares user credibility in peer-to-peer (P2P) e-commerce communities. Vandervort proposes three different models with which to implement a reputation system based on blockchain technology. However, none of them consider disclosing the privacy of buyers when delivering products. To address privacy concerns when delivering products, a "Private Waybill" was invented to hide consumer information so that private information does not appear on the waybill. Only couriers can obtain recipient information, including identities, addresses, and phone numbers, through authorized devices. While it prevents the disclosure of personal information to some extent, this technology cannot hide addresses, phone numbers, and information about other users from vendors. As far as we know, no existing models protect private information from start to finish. In this article, we tackle this issue by focusing on the trade and certification of collections such as artwork, luxury goods, and limited edition items. These goods are much easier to face privacy concerns in e-commerce as buyers tend to be more likely to protect their private information such as identities or addresses in these transactions. We would like to build a unified platform for collectors' collections and items for exchange, evaluation and certification of their property. Our platform is designed to convey, certify and protect the value of these "collections". We protect users' private information by using blockchain technologies, including private smart contracts and zero-knowledge proof. Specifically, each transaction is represented by a private smart contract that defines the business logic, transaction types, counterparties, underlying assets, price and any other relevant information.

II. RELATED WORKS

Li Xiong, Ling Liu. [1] The peer-to-peer e-commerce community is often viewed as an environment that offers both opportunities and threats. One way to minimize the risks in such an open community is to use community reputation to gauge credibility and predict future peer behavior. This paper presents PeerTrust a consistent adaptive trust model for quantifying and comparing the reliability of partners based on a transaction-based feedback system. The article discusses two main features of the model. First, they introduce three basic trust parameters in calculating the reliability of partners. In addition to the feedback you receive from transactions with other partners, record all transactions made by the feedback source on the creditworthiness assessment form. We suggest that trust models based primarily on feedback from peer-to-peer partners are not accurate and effective. It then introduces two consistent trust factors, the transaction context element and the community context element, in order to align the basic trust

criteria of different contexts and common faces of different e-commerce communities. done how to build trust in the electronic markets by using trusted third parties or intermediates. This does not apply to the peer-to-peer e-commerce community as peers play equal roles and are separate entities, hence neither of them can act as a trusted third party or intermediary.

David Vandervort.[2] Seller rankings from previous buyers are presented to provide information to help new customers make purchasing decisions. However, the purpose of Bitcoin is to hide the buyer-seller relationship at a level of anonymity and prevent buyers from finding or verifying this information. The bitcoin community appreciates this level of anonymity and continues to embrace bitcoin, but buyers and sellers who want to know more about their trading partners want to be known for their strength. Allows for greater transparency. They consider three models by which credit/rating systems can be applied to Bitcoin transactions, and their associated pros and cons. We believe there are technological and social challenges that we all face. The drawback is that Bitcoin stands for the anonymity of the Bitcoin community, and is often referred to as a pseudonym because it is not an absolute asset and is not a way to avoid cumbersome surveillance systems. It is also a hedge against personal user profiles/data mining for large companies like K-Mart.

Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza.[3] Bitcoin was the first widely used digital currency. Although payments are made between aliases, Bitcoin cannot provide strong privacy protection. Payment transactions are recorded in a central register from which a lot of information can be extracted. ZeroCoin (Mears et al., IEEE S&P 2013) addresses some of these privacy concerns by separating payers and transactions. However, it still reflects goals and payouts, and performance is limited. In this article, we will create a fully office-based digital currency with strong privacy features. Our findings benefit from recent advances in zero-sum non-interactive cognitive debate (eg, SNARK). First, we are developing a decentralized anonymous payment method (DApp method). The transaction hides the payer, payee and amount transferred. We provide a formal definition and proof of building safety. Next, we are building ZeroCash, an active example of DApp design. With ZeroCash, transactions are less than 1KB and validation takes less than 6ms. Orders are more efficient than ZeroCash, are not hidden, and do not compete with regular Bitcoin.

Janice Y. Tsai, Serge Egelman, Lorrie Cranor and Alessandro Acquisti.[4] Although online retailers have clarified their privacy practices in their online privacy policies, this information is often not visible to consumers, and consumers rarely read and understand these policies. This article reports on a study to determine whether consumers are becoming more aware of privacy issues in their online buying decisions due to increased exposure to personal information. We have developed an experience that provides clear and concise information about purchasing privacy information from search engines. By providing this information, consumers are more likely to purchase from online retailers that better protect their privacy. This research shows that as personal information becomes more and more available, some consumers may be willing to pay for their purchases from privacy sites. These results suggest that businesses can benefit from data protection.

III. EXISTING SYSTEM

The existing system protocols are instantiated using efficient primitives in cryptography with no trusted third parties. Payments of arbitrary value are conducted directly between parties, or via an intermediate connection that learns neither the participant's identities nor the amount involved. Coupled with a decentralized anonymous payment scheme for funding the channels, they provide for private instantaneous anonymous payments without a trusted bank. They use the idea of lightning networks and address the anonymity problem of payment channels based on the zero-knowledge technology. We design new decentralized logistics platforms that incorporate modern intelligence improvements to improve and accelerate the impact provided by integrating the most recent developments in information technology to multi-modal freight operations. Besides, the platform allows for an implementation that is not affected by scalability issues and is not limited by geographical borders. They also employ IDS and blockchain technology to construct a decentralized logistics platform.

IV. PROPOSED SYSTEM

We make the following contributions, We design a privacy-preserving model for E-commerce based on the private smart contract technology. Our model can provide proof of ownership while protecting users' private information by employing blockchain technologies including private smart contracts and zero-knowledge proof. Specifically, each trade is represented by a private smart contract, which defines the business logic, types of trade, counter parties, underlying assets, price, and any other relevant information from other participants. Besides, we build implementations of the model using two existing blockchain application platforms. We also evaluate the performance and validate the effectiveness and efficiency of the model with experiments. Performance analysis of the blockchain platforms provides further considerations for deploying a usable implementation.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

We employ an escrow protocol to address the problem of dispute. In addition, our model is based on an allowed blockchain which in nature has superior performance efficiency to public chains. We further tap the potential of blockchain and expand it to E-commerce systems based on allowed blockchain. Additionally, we enhance the anonymity of the logistics model to better protect user's privacy.

V. SYSTEM ARCHITECTURE

The entire system mainly consists of 4 modules, which are

1) Central Authority
2) Token Creation
3) Negotiation Phase
4) Delivery Phase

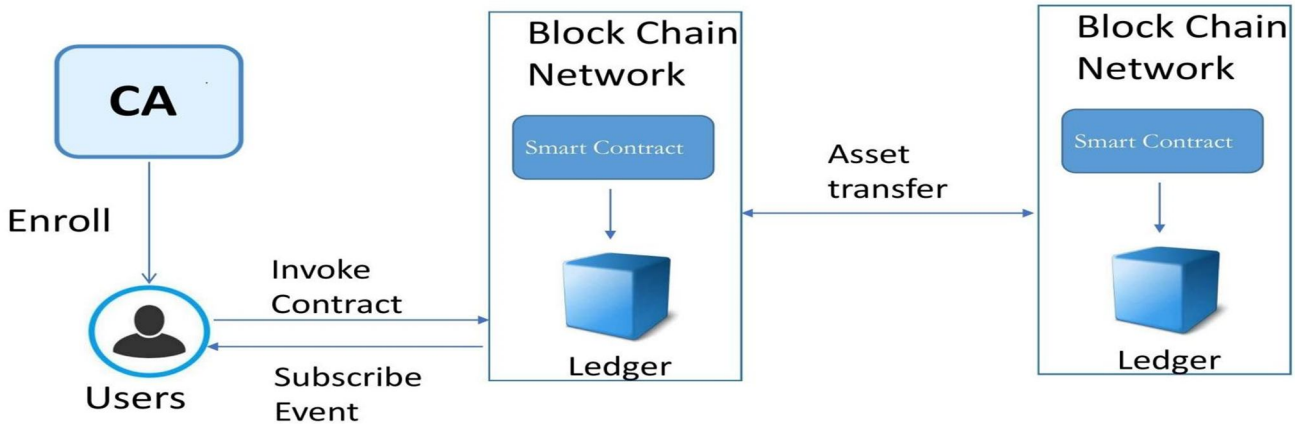


Fig. 1 .Architecture Overview

A. Central Authority

The CA component is in charge of issuing PKI-based certificates to organization members and their users. A root certificate is issued to each member and one enrollment certificate to each authorized user. The Client interacts with the blockchain network and smart contracts. It has to obtain a valid identity certificate from CA before joining the application channel/chains in the network. Both users and intelligent logistics centers act as clients.

B. Token Creation

Thus, Alice has to create a note-contract for the set of collector cards and issue a shielded token for herself. Now Alice owns a CARD token. At the same time, Bob shields some USD tokens by the USD note-contract.

C. Negotiation Phase

Alice establishes a private contract with Bob in a private channel. The private contract specifies the trade of the cards at a specific price in USD between Alice and Bob. The private contract also refers to the cards and USD note- contracts. Besides, the private contract also receives the relevant public keys and payment addresses of the two parties (including the Hash of physical addresses). When Alice initializes the contract, Bob can send to the private contract a transaction indicating acceptance of the terms We assume that the USD must be paid first. After the private contract receives the confirmation transaction, the private contract issues an instruction to Bob to pay the relevant amount of USD to Alice (Bob places the USD tokens into the escrow.USD tokens to a mediator’s payment address by generating the necessary zk-SNARK proof and sends it to the USD note-contract(Miner).

D. Delivery Phase

Alice places the cards into a delivery box that has a unique number. Then Alice sends the delivery box to the intelligent logistics center (suppose the intelligent center is reliable). Transport companies are responsible for inspecting and monitoring the legitimacy of the items. Alice’s client sends the Hash of Bob’s address to this box and sends the number of the box to the private contract. The private contract then sends the number of the delivery box to Bob’s client.

VI. RESULT

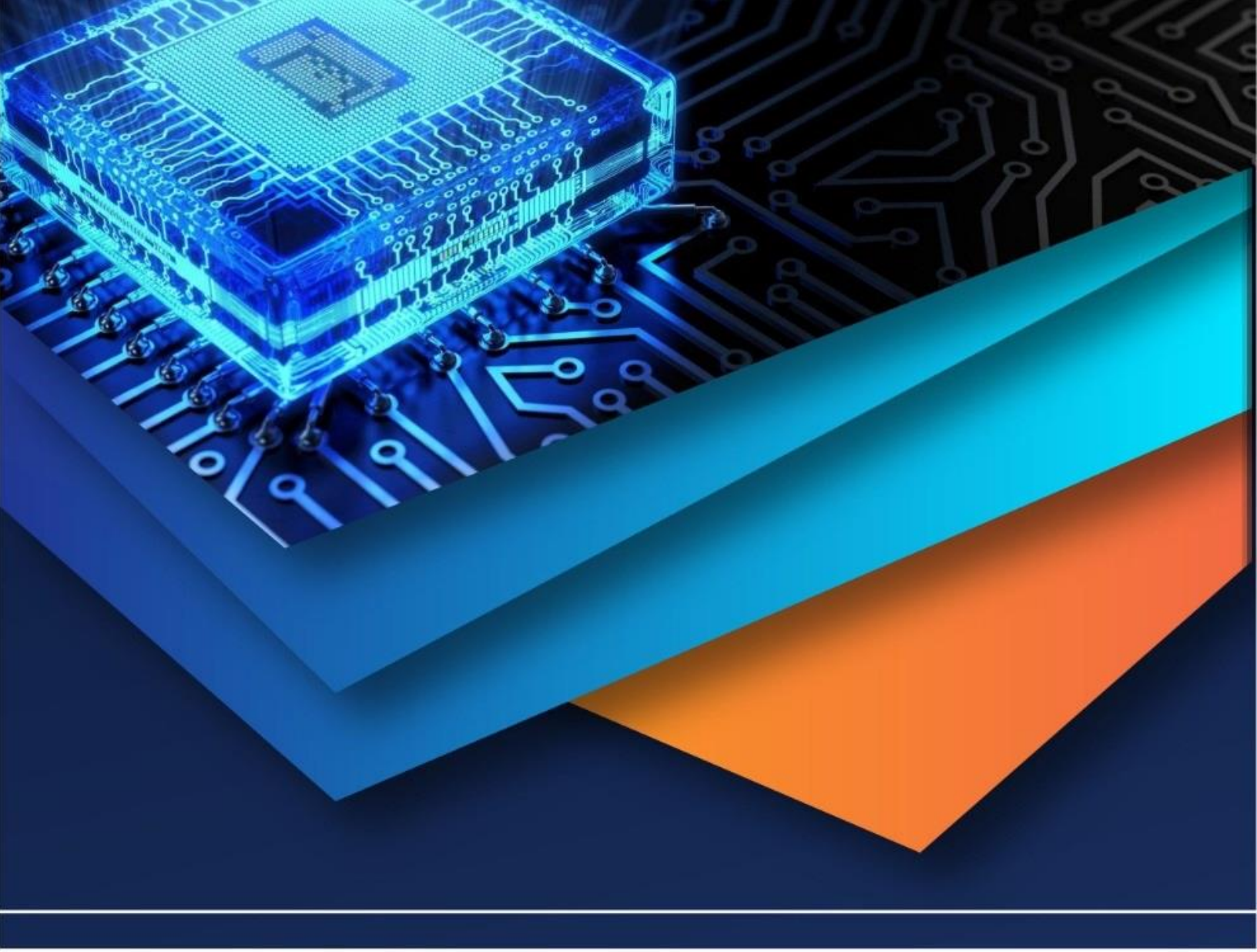
We designed a privacy-preserving model for E-commerce systems based on blockchain technology. To protect users' identities and guarantee proof of ownership, we employ a zero-knowledge proof algorithm called zk-SNARKs. The algorithm allows one party to prove to another party that a given statement is true, without conveying any information apart from the fact that the statement is indeed true by zero-knowledge proof.

VII. CONCLUSION

The designed blockchain application fully optimizes blockchain properties to remodel customer experience with full security. Therefore, it demonstrates the utility and suitability of blockchain applications in e-commerce. Performance analysis of the blockchain platforms provided insights into the model feasibility and further considerations for deploying a usable implementation. In the future, we will implement our logistics chain on blockchain platforms such as IOTA, which is mainly used in the field of IOT, and perform further simulations on the hardware through the Raspberry Pi.

REFERENCES

[1] M. Niranjanamurthy and D. D. Chahar, "The study of e-commerce security issues and solutions," International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 7, 2013.
[2] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The effect of online privacy information on purchasing behavior: An experimental study,"Information Systems Research,Vol.22,No.2,June 2011.
[3] B. Berendt, O. G¨unther, and S. Spiekermann, "Privacy in e-commerce: stated preferences vs. actual behavior," Communications of the ACM, vol. 48, no. 4, pp. 101–106, 2005.
[4] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer e-commerce communities," in E-Commerce, 2003. CEC 2003. IEEE International Conference on. IEEE, 2003, pp. 275–284.
[5] D. Vandervort, "Challenges and opportunities associated with a bitcoinbased transaction rating system," in International Conference on Financial Cryptography and Data Security. Springer, 2014, pp. 33–42.
[6] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman and Matthew Green "Zerocash: Decentralized anonymous payments from bitcoin," in Security and Privacy (SP), 2014 IEEE Symposium on. IEEE, 2014, pp. 459–474.
[7] Rosario Gennaro, Steven Goldfeder and Arvind Narayanan "Threshold-optimal dsa/ecdsa signatures and an application to bitcoin wallet security," in International Conference on Applied Cryptography and Network Security. Springer, 2016, pp. 156–174.
[8] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in International Conference on Financial Cryptography and Data Security. Springer, 2013, pp. 6–24.
[9] N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: trick or treat?" A chapter in Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment, 2017, pp 3-18 from Hamburg University of Technology (TUHH), Institute of Business Logistics and General Management.
[10] Hemantkumar P. Bulsara, Pratiksinh S. Vaghela."Blockchain Technology for E-commerce Industry" in International Journal of advanced Science and Technology,Vol.29,No.5,2020.
[11] Shazia Yasin,Khalid Haseeb,Rashid Jalal Qureshi,"Cryptography Based E-Commerce Security: A Review" in International Journal of Computer Science Issues,9(2),2012.
[12] Uriel Feige,Amos Fiat,Adi Shamir,"Zero-knowledge proofs of identity",in Journal of Cryptology,Springer,1,77-94(1988).
[13] Weiqin Zou,David Lo,Pavneet Singh Kochhar,Xuan-Bach D. Le,Xin Xia,Yang Feng,Zhenyu Chen,Baowen Xu, "Smart Contract Development: Challenges and Opportunities"published in IEEE Transactions on Software Engineering,24 September 2019.
[14] Paul J.Taylor,TooskaDargahi,AliDehghantanha,Reza M.Parizi,Kim-Kwang RaymondChood"A systematic literature review of blockchain cyber security" in Digital Communication and Networks,Volume 6, Issue 2, May 2020, Pages 147-156.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY