e-ISSN: 2797-2437

Zero-Knowledge Proof Application in E-Commerce Payment

[1]George Morris William Tangka
[1]*Kun Shan University, Institute of Information Management*
gmwtangka@gmail.com

[2]Ellie Ophelia Delviolin, [3]Hsien-Ming Chou
[2] *Department of Business and Management, Chung Yuan Christian University*
[3] *Department of Information Management, Chung Yuan Christian University*
elly.silaban@gmail.com
chou0109@cycu.edu.tw

Abstract— E-commerce plays a significant role in a country's economic condition. Since the COVID-19 outbreak, it has become more popular, along with concerns about its ability to handle information security. The Zero-Knowledge Proof (ZKP) method could be a possible solution to the e-commerce payment security issue that hampers customer trust. This paper investigates the viability of an online payment framework based on the ZPK method. This method is an upgrade for authentication during the payment process in online shopping. Experiments on customers' perspectives of the payment framework based on the ZKP method were conducted and supported the perceived usefulness, ease of use, trust, control, satisfaction, and loyalty aspects of a better e-commerce website. It allows advantages for both customers and e-commerce and prevents fraud, which will increase the trust level for both sides. zkSNARK speeds up and lowers the cost of the process, but there is a risk of DOS. Future work needs to be done to handle DOS in this method.

Keywords— blockchain, e-commerce, information security, online payment, zero-knowledge proof

I. INTRODUCTION

The rise of urgency in e-commerce popularity has been accompanied by security challenges among digital services. E-commerce is often known as electronic commerce or any business transaction that uses the internet where people purchase and sell gadgets, products, or services. Along with the exchange of products and services, it also includes the flow of capital and data to carry out these transactions. E-commerce has made it simple to identify and purchase from a variety of stores as well as markets that are active and use an online application. [1] People who want to start their own business can choose to join a marketplace like Amazon, Alibaba, etc., or have their system of operations.

Since the COVID-19 outbreak, people's awareness and consideration of how e-commerce, business, and countries' economies are transforming have increased. It is also thrilling how e-commerce gives consumers alternative ways to satisfy their needs. The outbreak is one of the reasons for the many transformations ahead regarding e-commerce. E-commerce, according to economists, is strengthening the price competition in business. Almost all users can now trade, shop, or do other types of commerce from the comfort of their own homes. As a result, it has become much easier to strike a balance between family and work [2].

E-commerce, like other members of the internet world, has its security challenges. The challenges created a trust issue that created a gap in the relationship between customers and

retailers. Security in payment is widely considered by customers. They not only buy things online but also use online payments, including credit cards. People need to feel safe about their payment accounts and prevent false deductions from them.

Blockchain entered the market with amusing technology regarding security in its system [3]. indicate a possible scheme for electronic payment using a blockchain system to execute e-commerce security. It will solve the issue of authenticity in the agreement between customers and retailers, and also integrity during transactions. Despite this, fraudulent users may be able to assemble information and detect personal identities using blockchain systems. To be focused on the issue of securely moving data over the blockchain network, protocols such as Zcash introduced a cryptographic method known as Zero-Knowledge Proof (ZKP) to ensure data secrecy. This method could be a possible solution to the e-commerce payment security issue [4].

The implications of ZKP in the e-commerce trust issue study deserve to be explored further. This study purposed to gain implications as follows: payment framework based on the ZKP method assist better e-commerce website for retailers and customers.

This paper first explores important technology factors and prior research related to the study, then proposes a framework for the payment model using the ZKP method. The next part includes and analyses the whole e-commerce system plan. Finally, the last part concludes this study.

II. LITERATURE REVIEW

During the presence of e-commerce, the merchant must gain customer trust. The reason is that customers cannot be directly involved in the transaction or touch the products physically. Customers are often concerned about whether the system keeps their information safe and accurate payment system that will not take more of their money than it should be. For both concerns, the transaction needs to have high protection and high authentication system.

A. Trust Issue in E-Commerce System

Lazaroiu et al. [5] consider that purchasing intentions of social platform users may be formed by taking into consideration the link between online trust and perceived risk. There is a link between online consumer purchasing intention, social commerce subsequent adoption, consumer trust, and risk variables influencing online consumer choices, based on source trustworthiness features. So, e-commerce needs to have strategies for customer trust. Trust is a mechanism that can be built by people, by developing interactions and time.

Most e-commerce strategies on trust issues include their characteristics, strengths, and identity. But now, trust in information security means that they believe the systems used by the retailer will not disadvantage them. Customers need to be sure that the system will not take more money than their total payment requirement.

The design of the e-commerce website can help to establish their trust first. A website with a better design can give more positive impressions of a store's trustworthiness and competency, leading to a positive view of the website and the retailer. As a result, customers have more trust in the store. The message of security measurement has been popular on e-commerce websites, but Mohr and Walter [6] prove that those messages do not affect customer trust. Most customers gain trust through recommendations from friends who have previously used the website. Any news about a retailer's data breach also plays a part in building customer trust.

Information security has been a challenge in gaining customer trust for e-commerce. In Kaushik and Gupta review [7], states that all customers must utilize HTTPS during their online shopping.

They also need to choose the best e-commerce platform, keep their admin panel airtight, and have a backup of vital data.

B. E-Commerce Current Payment Model

The popularity of smartphones and credit cards, the development of wireless communications networks, and the spread of online purchasing drive the e-commerce market's continuous rise [8]. As a result of this tendency, purchasing habits are diversifying, as are product sales and delivery methods [3]. The most crucial habit for customers is choosing their payment method. E-commerce will provide many options for customers on their website to make it easier to do online shopping [9].

Sexena et al. [10] mentioned two ways to classify payment methods, credit, and money payment systems. The difference will be in the utilization of direct money. The rise of online payment has been caused by advantages that customers felt. Customers will feel convenient as they will not need to go to ATMs like the previous time. Online payment comes together with a virtual account that can be accessed by customers anytime and anywhere, which will make it easier to track our expenditures. PG (Payment Gateway) is an intermediary system between the merchant and the bank (or card issuer) that allows online payment transactions [3]. First, customers ask for payment information from retailers. Retailers then send a request for payment authorization to PGs. PG will confirm the authorization to a bank (card issuer). After the bank confirmed, PG will allow access to the payment. This authorization can be made if both parties passed the authentication process (Figure 1).

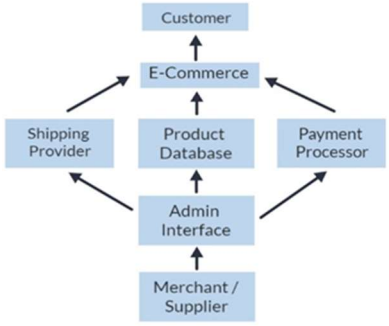

FIGURE 1. CURRENT E-COMMERCE TRANSACTION DESIGN

C. Authentication

The authentication process is essential in an online payment system. It will allow only authenticated users to get control access to the system activity. Users need to match with existing data to be called authenticated users. In the process, users need to provide a unique key that will match the key in the system. This unique key has been transformed day by day, from QR codes to OTP that will be sent to customers' smartphones.

Two-factor authentication is one of the security mechanisms in the authentication process. It uses two or three factors for data proof, like identity validation and logical password. In three-factor authentication, there will be three levels of the process. It will include who we are, something we have, and something we know. First, customers need to do biometric verification like fingerprint or face recognition, then they need to prove their possession like a card or one-

time token. To confirm what customers know, customers need to provide a password or personal id.

D. Zero-Knowledge Proof

ZKP is a cryptographic approach that has been used in blockchain systems [11]. It allows the prover to convince the verifier about the correctness of some data or statements without providing or leaking any additional information [12]. ZKP can be divided into interactive and non-interactive components.

ZoKrates, one of the non-interactive ZKP, is based on the zkSNARK algorithm. First create specific calculations in a human-readable format, then obtain the DSL file containing high-level codes. The DSL file is then compiled into flattened code, an abstraction of restrictions like a circuit, also is compatible with zkSNARK proof systems since it can be turned into Rank-1-Constraint-Systems (R1CS) [13]. ZoKrates, undertakes the phase of preparation to reveal a Common Reference String (CRS), As a result, two public keys are generated: a long verification key and a short verification key. The verification key and contract will be put into the blockchain. Then, the proving key will be handed to each prover. The prover must provide public and private inputs into the generator before creating the zkSNARK proof to calculate the zkSNARK witness that meets the flattening code. Followed by, how zkSNARK proof against the witness and CRS would be calculated (like proving key). The verification key supplied in the verification contract would be used to validate the proof and public inputs. The reported verification result will be used to regulate smart contract identification [14].

Yang and Wenjie [12] succeeded in introducing zkSNARK into the Digital Identity Management Scheme (DIMS). The DIMS effectively forbids the disclosure of ownership between the user entity and distributed ledger characteristics, resulting in identity unlink ability and behavior privacy. The protocol used also implements low-cost and high-throughput authentication operations. This result shows the probability of more applications using ZKP to solve information security issues regarding control access and authorization.

III. PROPOSED METHOD

The proposed payment framework includes three parties, the merchant, the customer, and the blockchain system [15]. This also will involve the ZKP method during the process. The following is the steps for processing payments based on the purposed model as in Figure 2:

1. The system will assert the profile of customers using two hash functions that contain tokens. One is the order validity created by the e-commerce website system, and the other is account

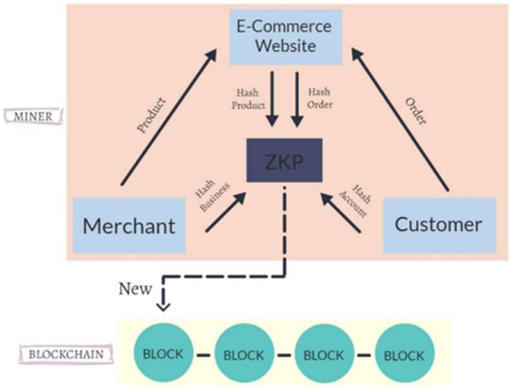

FIGURE 2. PROPOSED E-COMMERCE PAYMENT MODEL

validity by the blockchain system.
2. If an e-commerce site's product validity is verified, the system will assert the merchant profile using two hash functions (product and business validity) that contain tokens.
3. If the factor validity is verified, the customer gains a report of factor validity and unique code. The customer needs to click the "pay" button that includes the unique code access to request payment to the system, which contains the transaction ledger.
4. The Blockchain system deducts the balance of the customer's account.
5. Blockchain transmits the result of payment to customers and notification of a delivery request to the merchant.
6. The merchant delivers products as requested to the customer.
7. After pick-up and get the products, the customer needs to click "confirm arrival" in the website system that also contains the same unique code as the previous process.
8. The system raises the balance of the merchant's account, then transmits payment results to the merchant.

The whole process can be assessed as in order. The process will continue into the third step only if the profile assessment in the second step is valid. The unique code in the third step only can be formed if the profile assessment in the third step is verified.

IV. Customer Perspectives Experiment

For testing customer perspectives on the proposed payment system framework, the researcher collected twenty participants to fill out an anonymous questionnaire. The participants consist of women and men from different countries that ever done online shopping on some e-commerce websites. Participants also need to be above 18 years old and agree to contribute to the experiment.

A. The Design

The questionnaire will be analysed to evaluate our implications in the study. In this experiment, the hypothesis considers the validity of a better e-commerce website that uses the ZKP method on its online payment model by improving customers' perceived usefulness, ease of use, trust, control, satisfaction, and loyalty [16] [17]. All parts consist of two five-point Likert scale questions that used the first point as strongly disagree and the fifth point as strongly agree.

B. Analysis and Findings

The researcher conducted a one-sample t-test and evaluated customers' perspectives. The questionnaire-based data indicate a good fit for the test. For all aspects (perceived usefulness, ease of use, trust, control, satisfaction, and loyalty), the two-sided P-value shows $p < 0.001$. The results in Table 1 shows that customers' perspectives on the online payment framework proposed, supports the research hypothesis.

V. Results and Discussion

The whole process in online payment model using ZKP method will provide a secure and trustworthy system that prevents losses for both customers and the e-commerce side. Here will be the advantages that can be gained from these processes:

1. The merchant is only allowed to send the products after verification of the customer's profile. It will make them feel safe delivering the products.

2. The merchant is allowed to get the account balance after the product has arrived in the customer's hand. It will prevent fraud from a merchant that gains the money without the customer having their purchased product.

TABLE 1. T-TEST MEASUREMENT

Item	t	df	Significance Two-Sided P	Mean Difference
A1	24.658	19	<0.001	4.000
A2	18.420	19	<0.001	3.750
B1	29.947	19	<0.001	4.050
B2	23.106	19	<0.001	3.850
C1	16.905	19	<0.001	3.800
C2	15.119	19	<0.001	3.550
D1	22.134	19	<0.001	3.800
D2	21.326	19	<0.001	3.750
E1	27.568	19	<0.001	4.000
E2	25.667	19	<0.001	3.850
F	23.269	19	<0.001	3.950

3. Both merchant and customer will have the exact number of financial transactions based on valid data in the blockchain system. It will prevent the possibility of overpaid and online scams that take customers' money more than it should be.
4. The ZKP method in the blockchain system does not allow data leaking or any additional information to both merchants and customers about each other

VI. CONCLUSION AND SUGGESTION

Data secrecy in a blockchain system may be achieved by employing ZKP protocols. It allows e-commerce to overcome the information security challenge and gain trust from the customer, even though they are newcomers when they use it on their website. The researcher believe that some e-commerce companies do not use their website but have their business site in the marketplace, so choosing a marketplace that uses a secure protocol will also be important for them.

This paper designates a position of sustainability in business and smart-economy in the future that has high authentication system to satisfy society's needs. Based on zkSNARK, the method has a much faster and low-cost method. But this requires a trusted setup that allows DoS to happen. Improvements in this area are needed to make the zkSNARK-based blockchain scale for the demands of future use cases. It could be achieved by repeatedly creating key-value pairs in the token to be used by different users while also reducing the redundancy by optimizing attribute token logic.

REFERENCES

[1] C.-C. Chou, Journal of Industrial and Production Engineering, vol. 38, no. 4, pp. The impacts of information technology and e-commerce on operational performances: A two-stage dynamic partial adjustment approach, 2021.

[2] M. Basit, A. Bhatti, H. Akram, A. U. Khan, S. M. R. Naqvi and M. Bilal, "E-commerce trends during COVID-19 Pandemic," International Journal of Future Generation Communication and Networking, vol. 13, no. 2, pp. 1449-1452, 2020.

[3] S. I. Kim and S. H. Kim, "E-commerce payment model using blockchain," Journal of Ambient Intelligence and Humanized Computing, vol. 13, p. 1673–1685, 2020.

[4] X. Sun, F. Richard Yu, P. Zhang, Z. Sun, W. Xie and X. Penh, "A Survey on Zero-Knowledge Proof in Blockchain," IEEE Network, vol. 35, pp. 198-205, 2021.

[5] G. Lazaroiu, O. Negurita, I. Grecu, G. Grecu and P. C. Mitran, "Consumers' Decision-Making Process on Social Commerce Platforms: Online Trust, Perceived Risk, and Purchase Intentions," Frontiers in Psychology, vol. 11, no. 890, 2020.

[6] H. Mohr and Z. Walter, "Formation of Consumers' Perceived Information Security: Examining the Transfer of Trust in Online Retailers," Information System Frontiers, vol. 21, pp. 1231-1250, 2019.

[7] D. Kaushik, A. Gupta and S. Gupta, "E-Commerce Security Challenges: A Review," International Conference on Innovative Computing & Communication , pp. 1-4, 2020.

[8] B. Purwandari, S. Alam Suriazdin, A. Nizar Hidayanto, S. Setiawan, K. Phusavat and M. Maulida, "Factors Affecting Switching Intention from Cash on Delivery to E-Payment Services in C2C E-Commerce Transactions: COVID-19, Transaction, and Technology Perspectives," Emerging Science Journal, vol. 6, 2022.

[9] L. Qian and S. Mimi, "Discussion on Payment Application in Cross-border E-Commerce Platform from the Perspective of Blockchain," EDP Sciences, 2021.

[10] S. Sexena, S. Vyas, B. S. Kumar and S. Gupta, "Survey on Online Electronic Paymentss Security," Amity International Conference on Artificial Intelligence, pp. 746-751, 2019.

[11] D. Anand, S. Gracia Villar, H. Moaiteq Aljahdali and D. Mohanty, "Blockchain Interoperability: Towards a Sustainable," Sustainability, vol. 14, no. 913, 2022.

[12] X. Yang and L. Wenjie, "A zero-knowledge-proof-based digital identity management scheme in blockchain," Computer & Security, vol. 99, 2020.

[13] M. Harikrishnan and V. Lakshmy, "Secure Digital Service Payments using Zero Knowledge Proof in Distributed Network," International Conference on Advanced Computing & Communication Systems, pp. 307-312, 2019.

[14] M. u. Rehman, A. Lakhan, Z. Hussain, F. Hussain Khoso and A. Ahmed Arain, "Cyber Security Intelligence and Ethereum Blockchain Technology for E-commerce," International Journal of Emerging Trends in Engineering Research, vol. 9, 2021.

[15] H. Al-Aswad, W. M. El-Medany, C. Balakrishna, N. Ababneh and K. Curran, "BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation," ARAB JOURNAL OF BASIC AND APPLIED SCIENCES, vol. 28, 2021.

[16] H. M. Chou, "A Smart-Mutual Decentralized System for Long-Term Care," Applied Sciences, vol. 12, no. 7, p. 3364, 2022.

[17] C.-C. Tu, K. Fang and C.-Y. Lin, "Perceived Ease of Use, Trust, and Satisfaction as," JOURNAL OF COMPUTERS, vol. 7, 2012.