International Journal of Engineering Insights: (2024) Vol. 2, Nro.1, Regular Paper
https://doi.org/10.61961/injei.v2i1.13

Security aspects in the implementation of blockchain in payment gateway transactions in Ecuador

Kerly Naranjo Paez · Renato M. Toasa

Received: 20 Dec 2023 / Accepted: 24 Feb 2024 / Published: 15 May 2024

Abstract: This paper explores the security aspects involved in implementing blockchain technology in payment gateway transactions within the Ecuadorian context. Blockchain technology offers numerous security benefits such as data security, immutability, decentralization, authentication, and transparency. These features contribute to enhancing the overall security and trustworthiness of payment transactions. The decentralized nature of blockchain reduces the risk of cyber attacks targeting centralized servers, while its immutability ensures the integrity of transactions. Additionally, authentication mechanisms such as digital signatures and smart contracts help ensure that only authorized parties can participate in and validate transactions. Furthermore, blockchain's transparency facilitates auditing and compliance with financial regulations. This paper discusses how leveraging blockchain technology can significantly improve security in payment gateway transactions in Ecuador and provides insights into the potential challenges and opportunities associated with its implementation.

Keywords Blockchain · Payment · Security · Transactions · Ecuador

1 Introduction

1.1 Motivation

Currently, payment gateways have certain limitations in terms of security and efficiency compared to solutions based on blockchain. Payment gateways typically centralize transaction data on servers controlled by the entity operating the gateway. This can be a point of vulnerability, as if these servers are compromised by attackers, there is a risk of financial information and personal data of users being stolen [1].

Traditional payment gateways may be exposed to fraudulent attacks and unauthorized charges. Attackers could exploit vulnerabilities in authentication systems or intercept credit card data to carry out fraudulent transactions [2].

It's important to mention that security in traditional payment gateways has significantly improved over the years, and many companies have implemented robust security measures to protect transactions and user data. However, blockchain technology has the potential to revolutionize the security and efficiency of transactions in payment gateways. Additionally, it offers features such as immutability, transparency, and decentralization that can address some of the challenges mentioned earlier in the context of online transactions [3].

The implementation of blockchain in payment gateways can bring several significant benefits to society [4]. These benefits stem from the unique characteristics of blockchain technology and its ability to enhance security, efficiency, and transparency in online financial transactions. The primary beneficiaries of this proposal are users who make purchases of goods or services online and use their bank cards to complete the order and acquire the goods [5].

In particular, this proposal focuses on Sustainable Development Goal number nine, closely related to innovation, which is considered key to finding a lasting solution that provides security, efficiency, and trust to people when making an online purchase. Additionally, it stimulates innovation in the financial services sector. It can lead to the development of new technological solutions and business models that leverage the security and efficiency features of blockchain.

1.2 Related Works

For the present article, references are taken from various research sources related to the security and pro-

Kerly Naranjo Paez
Universidad Tecnológica Israel
Quito, Ecuador
E-mail: e1726773169@uisrael.edu.ec

Renato M. Toasa
Universidad Tecnológica Israel
Quito, Ecuador
E-mail: rtoasa@uisrael.edu.ec

tection of banking information, as well as documents that detail in-depth fundamental concepts of blockchain and its application in different areas. Initially in [6], the authors describe blockchain as a technology that goes far beyond Bitcoin and cryptocurrencies. Although Bitcoin was the first successful application of blockchain, this technology has a wide range of use cases in various industries and fields. Based on the authors' opinion, this statement leads to further exploration of the proposed topic and uncovering the potential of blockchain in payment gateways. Furthermore, in [7], the author examines how blockchain is transforming business models and provides an overview of the practical applications of this technology. There are also proposals for an electricity billing system based on Ethereum blockchain technology and Google's Firebase mobile application development platform. The system aims to enhance efficiency and transparency in the electricity billing process, leveraging the security and decentralization features of Ethereum and the rapid application development capabilities of Firebase [8]. Finally, in [9], the authors describe a blockchain design solution emphasizing the unique features offered by blockchain, such as decentralization, transparency, and security.

The analysis of this solution is closely related to the present work due to the assessment of the needs of implementing blockchain to contribute to the digital transformation of the public sector in Ecuador.
The document is organized as follows: Section 1 includes the Introuction, Section 2 the Methodology, Section 3 the Proposal and Section 4 the Conclusions.

2 Methodology

2.1 Focus

A bibliographic, analytical, and direct observational investigation is conducted aiming to identify and comprehend the techniques and strategies employed by payment gateways, while also devising action plans to address the impacts of attacks and prevent future incidents [10].
The aim is to create a proposal that facilitates the adaptation and integration of blockchain technology to enhance transaction security. This proposal aims to ensure that transactions accurately reflect the corresponding information regarding users' actual consumption, while maintaining immutable real-time data records without the need for intermediaries. The methodology also aims to streamline each stage of the process, ensuring efficiency, profitability, and continuous measurement, while preventing fraud. Additionally, it seeks to provide complete and transparent visibility of the process for all parties involved.

2.2 Analysis

According to the research and methodology described above, the proposal to implement blockchain technology in payment gateways in Ecuador, as well as in any other country, is deemed feasible. The analysis conducted through direct observation method entails detailed observation of the processes involved in online payment transactions to identify potential weak points and security risks. The vulnerabilities and threats detected through this method are described below.

Sensitive data leaks: By observing the data input processes in payment gateways, possible vulnerabilities in the protection of sensitive information, such as addresses and personal data, were revealed. The inadvertent exposure of this data could result in identity theft or financial fraud.

Intermediary attacks: Communication between the user, the payment gateway, and the payment service provider can uncover potential points of vulnerability where attackers could intervene and manipulate information during transmission. This could lead to intermediary attacks, such as data interception or identity impersonation.

Authentication vulnerabilities: When observing the user authentication process, effective mechanisms can be evidenced. Nevertheless, with blockchain, the utilization of decentralized digital identities stored in the blockchain can be implemented, ensuring the integrity and immutability of authentication information.

Software security flaws: When examining the user interaction with the payment gateway interface, it is determined that there may be vulnerabilities in the underlying software, such as security breaches, injections of malicious code, or weaknesses in session management.

Social Engineering Attacks: Observing the interactions between the user and the payment gateway reveals potential social engineering tactics used by attackers to deceive users and obtain confidential information, such as login credentials or credit card details.

This analysis enables proactive steps to be taken to mitigate risks and enhance system security. The proposed implementation of blockchain offers various tools and techniques that can be utilized to improve authentication and mitigate vulnerabilities in this critical security process. By implementing measures such as authentication based on blockchain, multifactor authentication, and decentralized identity management, it is possible to create a more robust authentication system

resistant to attacks. Figure 1 depict the flow of sensitive information in an online payment process.

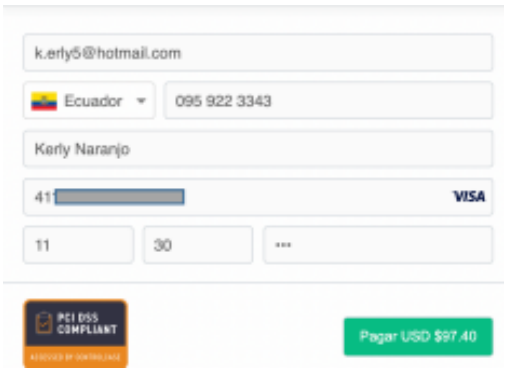

Fig. 1 Interface of a payment gateway ready for data entry and online payment.

Figure 2 shows the metadata generated when a transaction is carried out, allowing us to highlight the low level of security maintained by these processes.

Fig. 2 Recording a successful transaction through a payment gateway.

3 Proposal

3.1 Current Payment Gateway Phases

Considering the research among payment gateway providers operating in the country, it has been identified that the operational process of a payment gateway involves a series of phases to facilitate a secure online transaction between a buyer and a seller [11]. These phases are detailed below. Figure 3, shows the current operation of a payment gateway.

Transaction initiation: When a customer decides to make an online purchase, they select the products or services they wish to purchase and proceed to the payment screen.

Choice of payment gateway: The user chooses the payment method they wish to use, such as credit card, debit card, or other methods accepted by the merchant.

Redirection to the payment gateway: Once the payment method is selected, the customer is redirected to the payment gateway screen, where they enter their information to complete the transaction.

Information processing: The payment gateway processes the information provided by the customer and verifies its validity.

Authorization: The payment gateway communicates with the card issuer bank to request authorization and verify if the customer has sufficient funds to make the purchase.

Approval or rejection in the transaction: The card issuer bank or digital wallet provider responds to the payment gateway's authorization request, indicating whether the transaction is approved or rejected.

Transaction confirmation: The payment gateway sends a confirmation message to the merchant's website or application, indicating whether the transaction was successful. If successful, a purchase confirmation is displayed to the customer.

Transaction recording: The payment gateway records the transaction in its system, generating an electronic receipt with details such as the amount, date, merchant, and transaction information.

Settlement and deposit: The payment gateway initiates the settlement process, transferring funds from the customer's account to the merchant. This process may occur immediately or according to a predetermined schedule, depending on the payment gateway and the commercial agreement.

3.2 Blockchain Payment Gateway

The operation of a blockchain payment gateway involves several steps that combine blockchain technology with traditional payment processes [12]. The general components are:

Transaction initiation: The process begins when a customer makes an online purchase and chooses to pay using a payment gateway.

Transaction generation: Once the user selects the payment option, a transaction is generated on the blockchain containing relevant information about the purchase, such as the amount, seller, and buyer.

Digital signature: The buyer digitally signs the transaction using their private key, ensuring the authenticity and integrity of the transaction.

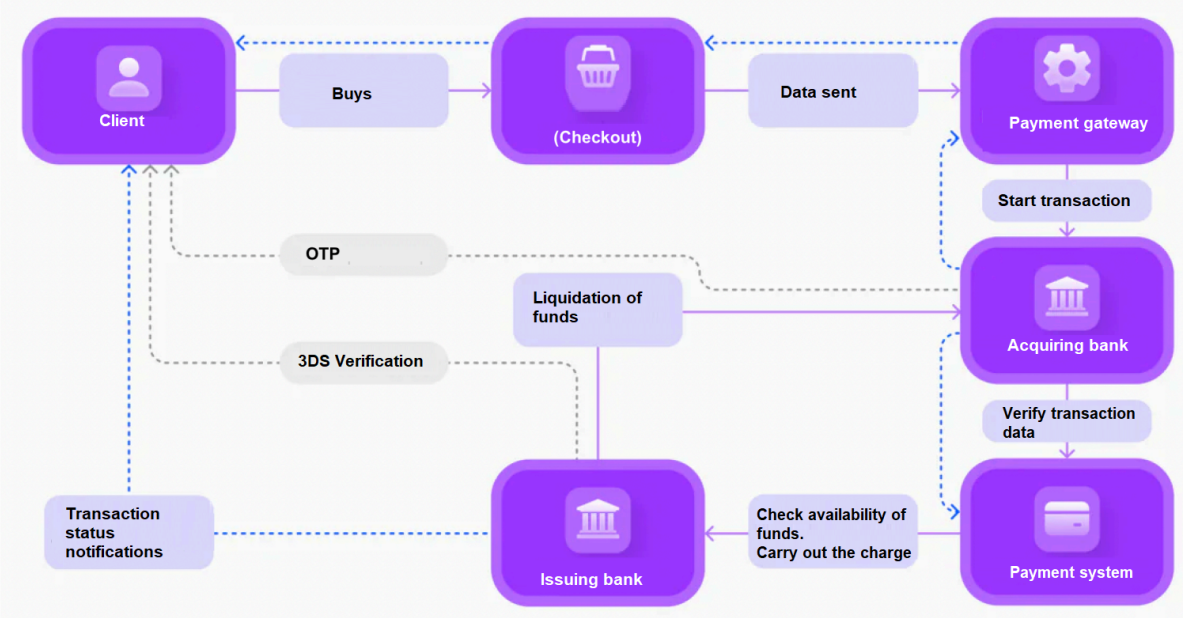

Fig. 3 Operation of an online payment gateway.

Transaction validation: The transaction is transmitted to the blockchain network, where it is validated by network nodes using consensus algorithms. Nodes verify the validity of the transaction and its compliance with the predefined rules of the blockchain.

Inclusion in a block: Once validated, the transaction is included in a block along with other pending transactions. This block is then added to the existing blockchain, creating an immutable record of the transaction.

Payment confirmation: After the block has been added to the blockchain, the transaction is considered confirmed, and the payment process is completed. Confirmation can take several minutes or more, depending on the speed and capacity of the blockchain network used.

Merchant notification: Once the transaction is confirmed, the seller is notified that the payment has been successfully made, and authorization is granted for the delivery of the product or service to the buyer.

Permanent record: The transaction is recorded on the blockchain permanently, providing a transparent and verifiable record of all transactions conducted.

The operation of a payment gateway with blockchain security involves the generation, signing, validation, inclusion, and confirmation of transactions in the blockchain, providing a secure, transparent, and efficient way to process online payments. Figure 4 shows the Payment flow of a blockchain gateway.

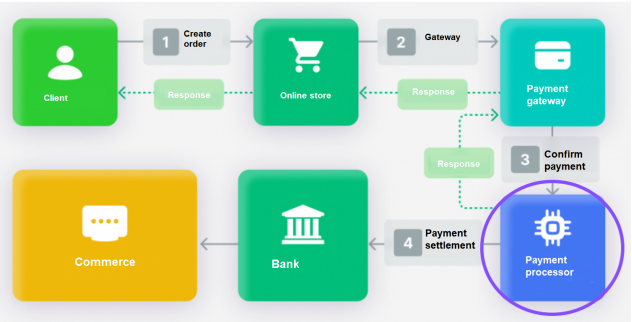

Fig. 4 Payment flow of a blockchain gateway.

3.3 Proposal Structure

A payment gateway plays a crucial role in the online purchasing process, ensuring that financial information is transmitted securely, transactions are authorized, and funds are transferred appropriately between the involved parties. Below is the proposal for the adaptation and implementation of blockchain aimed at securing the transaction process of e-commerce businesses, focusing on data security fundamentals using blockchain technology. Every event or modification of data is written as a new block in a chain, thus creating a certified, settled record, ensuring its integrity and availability [13]. Additionally, if the content is encrypted, reliability is ensured. Figure 5 illustrates the stages comprising the current proposal that will enable the achievement of the objective.

It is proposed to utilize smart contracts and a decentralized network to ensure payment integrity and re-

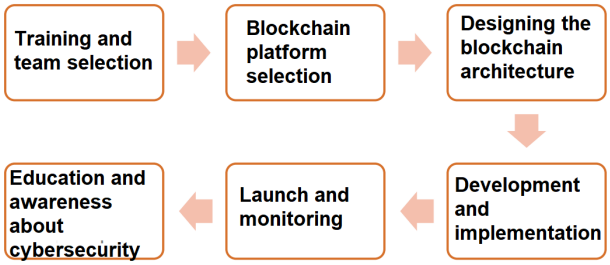

Fig. 5 Proposal designed for blockchain implementation.

duce risks associated with fraud and data manipulation. Additionally, the aim is to eliminate unnecessary intermediaries and streamline settlement processes. This implementation will benefit both merchants and consumers, providing a more secure and reliable payment experience.

3.4 Proposal validation

The proposal was carried out with the support and assessment of two specialists in the field of data security and cybersecurity. The experts believe that a proposal to implement blockchain in payment gateway transactions is a valuable idea. Blockchain technology offers several advantages that could significantly enhance the security, transparency, and efficiency of transactions in payment gateways. However, it is important to note that the successful implementation of blockchain in payment gateways will require careful planning, development, and collaboration among various stakeholders. Additionally, challenges such as scalability, interoperability, and regulation need to be addressed to ensure the long-term success of this proposal. In conclusion, although there are challenges to overcome, the application of blockchain in payment gateway transactions has the potential to generate significant value for the industry and users. The experts validated indicators such as: impact, applicability, conceptualization, relevance, technical quality, feasibility, and relevance, through a scale of 1 - 5, with an average score greater than 4 considered positive, thus validating the proposal and its future implementation in real scenarios.

4 Conclusions

The theoretical foundations on security and blockchain uncovered during the research development enable us to appraise the proposal as it provides a high level of confidence by drawing upon expert sources and books delving into the application of blockchain across various areas beyond the realm of Bitcoin.

The vulnerabilities and threats detected in the flow of a bank transaction through a payment gateway have allowed us to understand that currently, companies providing this service face significant challenges and possibilities of being attacked due to handling sensitive and valuable user information in e-commerce. By designing a proposal that promotes the implementation of blockchain as a security technique in the online payment transaction process, we have paved the way for enhancing security and trust in digital commerce. This proposal not only offers an innovative and effective solution to address security challenges in online transactions but also paves the way for increased adoption and acceptance of blockchain technology in the financial and commercial sectors.

Conflict of interest

The authors declare that they have no conflict of interest.

References

1. M. Di Pierro, "What is the blockchain?" *Computing in Science & Engineering*, vol. 19, no. 5, pp. 92–95, 2017.
2. Sumanjeet, "Emergence of payment systems in the age of electronic commerce: The state of art," in *2009 First Asian Himalayas International Conference on Internet*. IEEE, 2009, pp. 1–18.
3. D. S. W. Khan, "Cyber security issues and challenges in e-commerce," in *Proceedings of 10th international conference on digital strategies for organizational success*, 2019.
4. S.-I. Kim and S.-H. Kim, "E-commerce payment model using blockchain," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 3, pp. 1673–1685, 2022.
5. Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, and A. Seneviratne, "A delay-tolerant payment scheme based on the ethereum blockchain," *IEEE Access*, vol. 7, pp. 33 159–33 172, 2019.
6. D. Tapscott and A. Tapscott, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin, 2016.
7. W. Mougayar, *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons, 2016.
8. K. M. Hlaing and D. E. Nyaung, "Electricity billing system using ethereum and firebase," in *2019 International Conference on Advanced Information Technologies (ICAIT)*. IEEE, 2019, pp. 217–221.
9. A. R. Ramos Rodríguez, "Análisis de pertinencia de una soluciÓn de diseño de bloques de seguridad en transacciones descentralizadas para el gobierno electrónico ecuatoriano." Master's thesis, Quito, Ecuador: Editorial UISRAEL, 2023.
10. N. Galí Espelt and J. A. Donaire, "Direct observation as a methodology for effectively defining tourist behavior," *© e-Review of Tourism Research (eRTR), 2010 (Enter 2010 Short papers), vol. 1, 5 p.*, 2010.

11. M. A. Hassan, Z. Shukur, and M. K. Hasan, "An efficient secure electronic payment system for e-commerce," *computers*, vol. 9, no. 3, p. 66, 2020.
12. U. Bodkhe, P. Bhattacharya, S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, "Blohost: Blockchain enabled smart tourism and hospitality management," in *2019 international conference on computer, information and telecommunication systems (CITS)*. IEEE, 2019, pp. 1–5.
13. I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Computing and Applications*, pp. 1–16, 2022.

License