Technological Model for Cryptocurrency Payments in E-Commerce

Luis Navarro[1][a], Juan Mansilla-Lopez[1][b] and Christian Cipriano[2][c]
[1]*Universidad Peruana de Ciencias Aplicadas (UPC), Prolongación Primavera 2390, Monterrico, Santiago de Surco, Lima, Perú*
[2]*Cranfield University, College Road Cranfield MK43 0AL, U.K.*

Keywords: Blockchain, Cryptocurrencies, Payment Gateway, Bitcoin, Three-Tier Architecture.

Abstract: The number of cryptocurrency users worldwide increased by 190 % between 2018 and 2020, with Bitcoin being the most widely used. Credit card gateways request the payment of a usage fee, a sales tax that generates cost overruns for the businesses that use it. Likewise, virtual stores are exposed to cybersecurity threats, such as SQL injection and man-in-the-middle, which could affect the integrity and confidentiality of their information. This research proposes a Technological Model for Cryptocurrency payments based on a set of guidelines to develop a virtual store that accepts Bitcoins as a payment method and offers measures that guarantee the security of the integrity and confidentiality of its information. The structure of the model is based on a three-Tier architecture pattern that includes a private Blockchain in which the information of the sales made in the virtual store and of logistics (purchase orders, suppliers, and products) is stored. The model was validated in an online business, evidencing a reduction in the percentage of transaction costs.

1 INTRODUCTION

The purchase of products and services through virtual stores continues to gain popularity with an increase in sellers adopting cryptocurrencies as a means of payment for their sales (Sawarnkatat & Smanchat, 2022). Also, due to their integrity, confidentiality, and transaction speed, cryptocurrencies have seen accelerated growth since the creation of Bitcoin (Gong & Huser, 2019). Thus, its users has grown by 190 % between 2018 and 2020 (Raynor, 2024).

Online payment methods for e-commerce have been constantly evolving since the birth of the Internet. Initially, this was provided by financial services such as credit cards and fund transfers; however, these are subject to regulations and relatively high fees (Sawarnkatat & Smanchat, 2022).

According to (Kim & Kim, 2022), most people who purchase in virtual stores use credit cards. In such cases, payment gateways are used to ensure the integrity and non-repudiation of payments. However, nowadays, due to the increase in the number of credit card terminals, changes in the types of tax deductions, and the growing number of stores that process a large volume of small payments, this has caused problems in the e-commerce market. This has led sellers and consumers to take into consideration the fees associated with electronic payment systems.

According to (Cáceda et al., 2022), e-commerce in Peru had a 55 % growth in 2021. In 2024, credit card payment gateways, such as Culqi, Niubiz, and Mercado Pago, charge average fees of 3.40 % per transaction, in addition to other charges. On the other hand, cryptocurrency payment gateway services charge around 1 % per transaction, with no extra fees, as is the case with Blockonomics. According to (Sawarnkatat & Smanchat, 2022), one of the newest payment methods for digital merchants is with cryptocurrencies. The latter are considered an alternative form of investment assets, as they have high yields and are very secure. An example of this is (Bamert et al., 2013), who designed a vending machine that accepted bitcoins as a means of payment.

Regarding Cryptocurrency regulations in Peru, digital asset providers are required to provide information to the Peruvian Financial Intelligence Unit, which is in charge of analyzing payment transactions to be able to detect money laundering or

[a] https://orcid.org/0009-0007-0711-5782
[b] https://orcid.org/0000-0003-0039-6044
[c] https://orcid.org/0000-0002-5864-658X

Navarro, L., Mansilla-Lopez, J. and Cipriano, C.
Technological Model for Cryptocurrency Payments in E-Commerce.
DOI: 10.5220/0012916800003825

In *Proceedings of the 20th International Conference on Web Information Systems and Technologies (WEBIST 2024)*, pages 25-34
ISBN: 978-989-758-718-4; ISSN: 2184-3252

terrorist financing (El Peruano, 2023). The emergence of cryptocurrencies caused a change in the world and brought benefits, such as not needing institutions to act as intermediaries, which reduces transaction costs. Likewise, they are immutable; for example, if a bank is hacked, it will depend on its backup to recover its information; however, in the case of cryptocurrencies, if a part of its network is altered, the rest of the network will continue to work correctly (Fang et al., 2022).

There are studies such as those by (Kim & Kim, 2022), who, by making use of blockchain features such as public keys, private keys, as well as digital signatures, manage to develop a cryptocurrency payment model that does not make use of a payment gateway or public key certificates. However, there is a risk that their Public Blockchain System of Record for Distributed Transactions will compromise the confidentiality of personally identifiable data. Also, there is the study of (Sawarnkatat & Smanchat, 2022), who proposed a cryptocurrency payment system called NAGA, which was characterized in that buyers paid with one type of cryptocurrency and sellers received another.

On the other hand, e-commerce information is not free from having its confidentiality and integrity compromised. According to (Ehikioya & Olukunle, 2019), data in the different databases and those in transit must be protected from unauthorized persons, such as hackers, who can alter the integrity and steal sensitive company information.

According to (Tadhani et al.,2024), the SQL Injection (SQLi) attack type seeks to exploit the vulnerability of databases by injecting harmful code into queries, which compromises their confidentiality and integrity. It does this by first attacking web applications by inserting code into the site's input fields to access the database. There is also the Man-in-the-middle threat, which consists of the attacker managing to infiltrate the network and place himself in the communication between a client and a server (Elakrat & Jung, 2018). Thus, the attacker can listen to the information and modify the information between the sender and the receiver.

This research proposes a technological model for payment with cryptocurrencies in electronic stores that is secure and that allows for reducing transaction costs in virtual stores. This consists of a set of guidelines for developing a virtual store that allows accepting cryptocurrency payments through a payment gateway called "Blockonomics". Likewise, it will use KuroNexus, a private blockchain designed by us to store sales and logistics information (products, suppliers, purchase orders).

This article is divided into five sections. Section 2 presents the literature review. Section 3 describes the proposed technological model. Section 4 validates and analyzes the results. Finally, section 5 provides the project's conclusions and recommendations.

2 RELATED WORK

Blockchain has many uses that can be applied to different contexts, such as medicine, e-commerce, and social networks.

2.1 Application of Blockchain in Electronic Commerce

(Miers et al., 2013) propose ZeroCoin, an electronic payment system that is a cryptographic extension of Bitcoin that augments the protocol to allow fully anonymous currency transactions.

(Sawarnkatat & Smanchat, 2022) propose a payment architecture of a system that allows the buyer to pay with a currency and the seller to receive the currency of his choice.

(Eskandari et al., 2018) developed a "point-of-sale" web system that accepted Bitcoin and implemented it in a Cafe called Aunja, in 2014. For its part, (Hu et al., 2019), with the aim of helping remote villages, proposed a payment scheme based on the Ethereum blockchain, which can maintain a record of verifiable transactions in a distributed manner.

(Su et al., 2020) propose a p2p transaction method based on blockchain, which in turn guarantees data privacy and trust between entities. Likewise, a GO programming language was used for validation.

(Kumar et al., 2020) propose "ProdChain", a Blockchain framework with cryptographic processes to reduce the complexity of traceability of e-commerce products and, in turn, ensure financial sustainability.

(Zulfiqar et al., 2021), in order to maintain the integrity of the information regarding the Reviews of certain products on e-commerce platforms proposes EthReview, a resilient Product Review system based on Ethereum that solves the integrity above problem.

(Guan et al., 2020) propose a scheme that integrates blockchain that seeks to solve the need to store and process sensitive data from e-commerce.

(Li et al., 2021), to solve the privacy and integrity problems of supplier reputation systems of e-commerce platforms, propose RepChain, a reputation blockchain-based system that preserves privacy. In addition, it allows access to multi-platform reputation and the creation of private ratings.

To solve chargeback fraud, which consists of canceling credit card payments, and which is harming online sellers, (Liu & Lee, 2022) propose CF-Ledger, an exchange mechanism of Chargeback fraud data that is based on Consortium Blockchain.

2.2 Application of Blockchain for Privacy and Information Security

(Makhdoom et al., 2020), due to the vulnerabilities regarding the information of IoT systems; propose "PrivySharing", an innovative framework based on blockchain, preserves privacy and guarantees the security of the transfer of IoT data in a Smart City environment.

(Hinarejos et al., 2022), to solve security problems in the application of promotional programs, propose a solution based on Blockchain that allows points to be transferred between clients for multiple merchants.

Due to privacy issues in "Online Social Networks", (Frimpong et al., 2023) propose RecGuard, a blockchain-based network system for privacy preservation.

In the medical context, (Szczepaniuk & Szczepaniuk, 2023) present a framework for implementing cryptographic proofs of smart contracts in health systems. According to (Gan et al., 2023), with the growth of Electronic Medical Data, it becomes a problem to find it efficiently in a Blockchain; due to the above, a method for searching for encrypted medical data in a Blockchain with a mechanism is proposed. Likewise, (Miao et al., 2024), to protect medical data on the "Internet of Medical Things", propose a Privacy-Preserving Authentication Management Protocol based on Blockchain.

(Luo et al., 2023), for its part propose RATS, a Blockchain-based system that protects the privacy of transactions in the Blockchain and regulates illegal transactions. Likewise, this allows users to be tracked without affecting the transaction when dealings that can be called suspicious are detected.

Likewise, (Aldweesh, 2023) proposes a framework for E-ticketing that makes use of blockchain. This proposal eliminates the participation of third parties and improves user privacy.

3 TECHNOLOGICAL MODEL

The technological model consists of guidelines for developing a virtual store to reduce transaction costs for the seller by integrating a cryptocurrency payment method. It provides instructions for developing a Blockchain structure, "KuroNexus," designed by us to ensure the integrity of the sales and logistics data.

There are works like (Sawarnkatat & Smanchat, 2022) and (Miers et al., 2013) with their own designed payment systems; in our case, we wanted to contribute with a model that would allow the implementation of an E-Commerce using a payment gateway called "Blockonomics". Being an outsourced service, this gateway reduces the risk of security and regulatory compliance failures.

3.1 Architecture of the Technological Model

3.1.1 Architecture Pattern

The technological model makes use of a Three-Tier architecture pattern, which consists of decomposing the applications into three levels or layers so that each one presents a different level of responsibility. The presentation layer is responsible for system presentation, the business layer handles the business logic and processes requests from the presentation layer, finally, the data layer is responsible for data storage.

3.1.2 Technologies

The technologies used in the model will be described to justify their selection. These will be separated by layers according to the architecture mentioned above.

For the presentation layer, we used:

- **Angular.** According to (Oriols & Gomez, 2018), this framework allows web application development in the client section using HTML and JavaScript. It allows the development of SPA (Single Page Application) web applications. This is an improvement to Multi- Page Web Applications (MPA) in that the client will no longer request entire web pages but only the necessary information. For the business layer, we used:

- **NodeJS.** According to (Brown, 2014), NodeJS provides a framework for building a web server. This can be easy to implement and configure, unlike Apache or Microsoft's Internet Information Services, which can take several years to master. We decided to use it to develop our APIs.

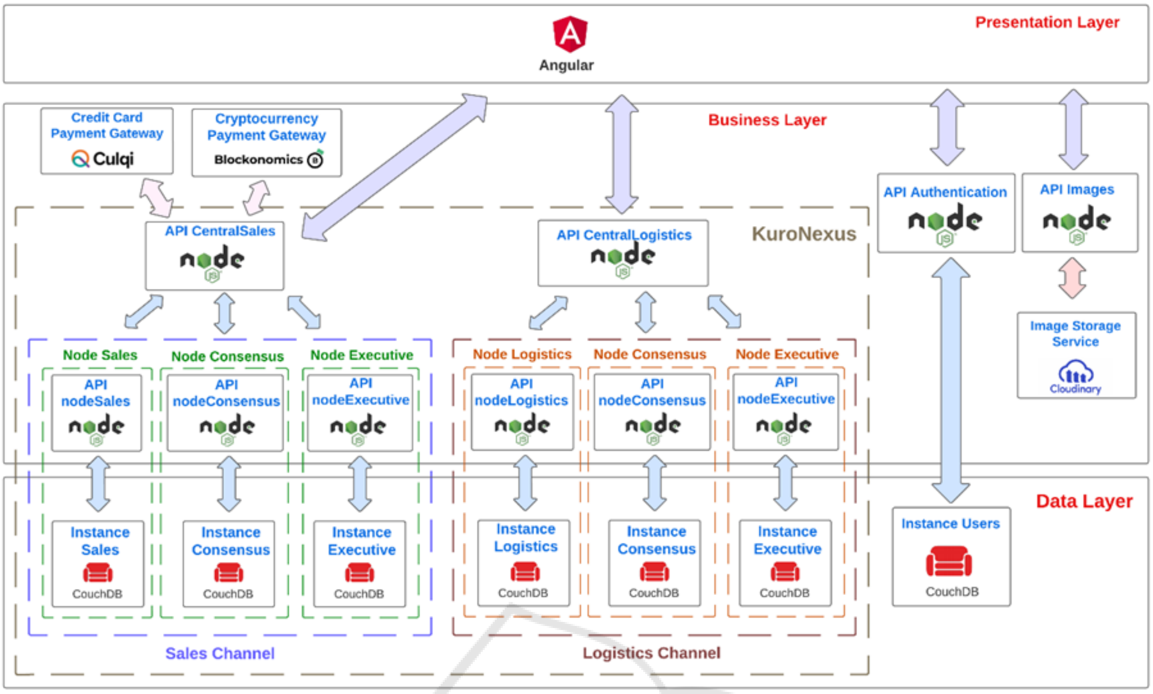


Figure 1: Physical Architecture of the Technological Model.

- **Cloudinary.** This service helps to store images and videos thanks to an API. In addition, it allows users to retrieve images thanks to URLs with a static part and a variable part that would be the name of the images.

- **Culqi.** This model includes a credit card payment method, and for that, we use this payment gateway. It was chosen because it charges a commission rate of 3.44% plus extra charges and delivers the sales deposit about two days later.

- **Blockonomics.** It allows virtual stores to accept payments with bitcoin. We decided to use it because it charges only 1% commission per sale and for its security features.

For the data layer, we used:

- **CouchDB.** It is a NoSQL database that stores information in JSON documents. The latter makes it immune to SQL injection attacks. In addition, it allows access to documents through the web browser (Chrome, etc.). According to (Brown, 2012), it is fault tolerant and generally self-sufficient; likewise, its storage has a flexible nature format that differentiates it from other databases.

3.1.3 Architecture Description

In Figure 1, you can see the technological model distributed by layers. In the presentation layer, the Angular file controls the visual part. In the business layer, you will find the API: “Authentication”, responsible for processing information related to user registration and login; and the API "Images", responsible for uploading images to the image server. There is also KuroNexus, which consists of a decentralized structure based on Hyperledger Fabric due to its use of channels and digital certificates for authentication. It is made up of the APIs: “CentralSales” and “CentralLogistics”, as well as the "Logistics" and "Sales" channels. The API “CentralSales” communicates with the APIs of the Culqi and Blockonomics payment gateways to process information related to purchases. On the other hand, it also communicates with a channel "Sales" for the storage and retrieval of information (related to customer sales) in blockchain nodes. The "Sales" channel consists of 3 nodes, each containing an API and a database instance, such as the APIs: “nodeSales” and the “Sales Instance”. The "Logistics" channel works similarly, only that the information you work with is related to products, suppliers, and purchase orders.

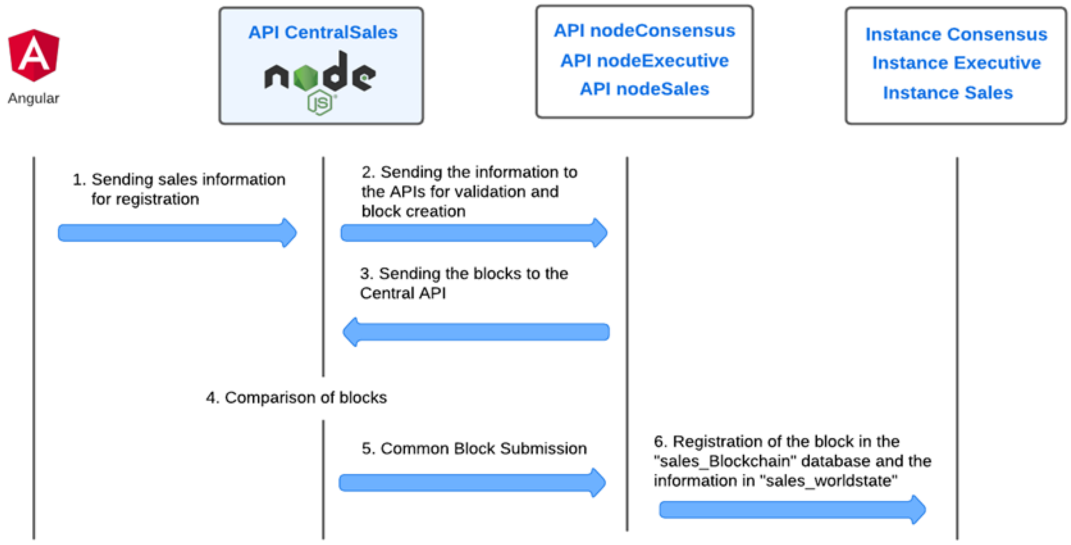

Angular
API CentralSales
node JS
API nodeConsensus
API nodeExecutive
API nodeSales
Instance Consensus
Instance Executive
Instance Sales
1. Sending sales information for registration
2. Sending the information to the APIs for validation and block creation
3. Sending the blocks to the Central API
4. Comparison of blocks
5. Common Block Submission
6. Registration of the block in the "sales_Blockchain" database and the information in "sales_worldstate"

Figure 2: Central API - Information processing.

3.2 Development, Security and Hosting Guidelines for APIs and Databases

3.2.1 API

The APIs will be developed using node.js and Express. API Keys will be implemented as a security measure. For the APIs: “CentralSales” and “CentralLogistics”, a digital certificate will be implemented as an additional authentication method so that they can be verified by the APIs of the channels assigned to them. Finally, the servers where the APIs are located must have a TLS certificate configured to make secure connections with clients. In this case, a hosting service called “Render” will provide these certificates when deploying the APIs.

3.2.2 Databases

CouchDB database instances will be created to prevent Inject SQL attacks. The instances will be created and deployed using a "Railway" service. It is recommended that restrictions be configured so as not to be maliciously altered by unauthorized users.

3.3 Modules and Components of the E-Commerce

This section will cover the model's modules and components. Each module covers a set of functionalities or features, such as the Authentication module, which covers the registration and login functionalities.

3.3.1 KuroNexus Blockchain Module

This Blockchain structure is based on the use of Hyperledger Fabric channels. It has 2 Central APIs: “CentralSales” and “CentralLogistics”. Likewise, it will have 2 channels: “Sales Channel” and “Logistics Channel”. Next, what the Central APIs are, and their details will be defined, then what the channels are for this module will be explained.

- **Central APIs.** This structure contains 2 APIs: “CentralLogistics” and “CentralSales”. These are responsible for receiving the request from the presentation layer and then making requests to the nodes’ APIs. When the presentation layer requests information from the nodes, the Central APIs will consult the Consensus Node or the Executive Node. In the scenario that the presentation layer sends information (Recording a sale, for example) to be registered in the nodes' databases, they will first send the information to the Central API, then it will send the transaction to the three nodes, who will validate the transaction. Once validated, each one will create a block and send it as a response to the Central API which will compare the 3 blocks. If the three blocks do not match, an email will be sent to the “Service Manager” or a person in charge indicating the error. If at least two blocks are equal, the Central API will send the common block to the three nodes for registration in their databases. The block will be saved in the “Blockchain” database, and the transaction will be saved in the “Worldstate” database. All the above helps to identify and prevent possible Man-in-the-Middle (MitM) attacks, as well as possible problems with inconsistencies in database information. An example of this is found in Figure 2.

- **Channels.** The structure will have two channels: “Sales Channel” and “Logistics Channel”. Each one will have a minimum of 3 nodes. Each of these will be composed of an API and a CouchDB instance with their respective databases, as can be seen in Figure 3.

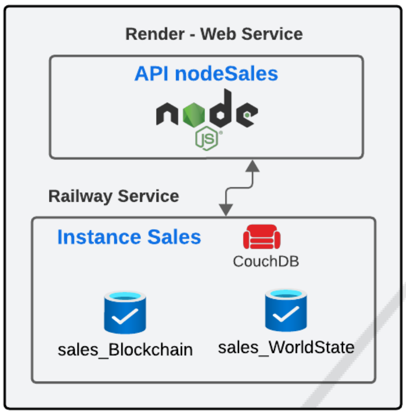


Figure 3: Node Sales.

As mentioned in the previous point, the API of each node will oversee the validation of the transactions it receives from the "Central API" and create the blocks that will return them as a response. The node instances will have “worldstate” and “blockchain” databases, an example of this is the sales node which will have “sales_worldstate” and “sales_blockchain” instances. The “worldstate” database is made up of arrangements of specific information, in the case of “sales_worldstate” it will store sales arrangements. Likewise, the “blockchain” database will store blocks sequentially with information about changes in the “Worldstate” database. As seen in Figure 1, the “Sales Channel” contains three nodes: “Consensus Node”, “Executive Node” and the “Sales Node”. For its part, the “Logistics Channel” contains three nodes: “Consensus Node”, “Executive Node” and the “Logistics Node”. The "Sales node" contains the “nodeSales” API and a “Sales Instance” that stores sales-related information. This instance has two databases: “sales_worldstate” and “sales_blockchain”. The “Logistics Node” consists of the “nodeLogistics” API and a “Logistics Instance”, this instance will store the information of suppliers, purchase orders and products. The instance has 2 databases: “logistics_worldstate” and “logistics_blockchain”. Finally, the "Consensus Node" and the "Executive Node" are the same in both channels; they have their own API and database instances. These instances will store all the previously mentioned databases: “sales_worldstate”, “sales_blockchain”, “logistics_worldstate” and “logistics_blockchain”.

3.3.2 Authentication Module

This module covers the "Login" and "User Registration" functionalities. These require using a "Users" database instance containing the "Users_Commerce" database containing user information, such as username, password, name, email, and role. The module's functionalities will be described in greater detail below:

- **User Registration.** Allows the user to register to purchase items in the virtual store. To register data, the following will be requested: Name, Username, Email and Password. Then you will receive a message with a special code in your email. Once the code has been entered and accepted by the system, you will be redirected to the home page of the virtual store.
- **Login.** Allows users to log in to the virtual store using their username and password. This can be logged using a JSON Web Token (JWT) approach, where the API will provide the user's browser with a token to authenticate on the e-commerce pages.

3.3.3 Payment Processing Module

The credit card payment process requires using a Credit Card payment gateway (such as Culqi). If you use this service, the presentation layer and the “CentralSales” API will be programmed to implement this payment method. The Cryptocurrency payment process requires using a Cryptocurrency payment gateway (such as Blockonomics). The presentation layer (the Angular file) and the “CentralSales” API must be programmed to implement the following payment process:

1. The customer fills his shopping cart.
2. The customer clicks Pay, then is redirected to a “Payment Options” page.

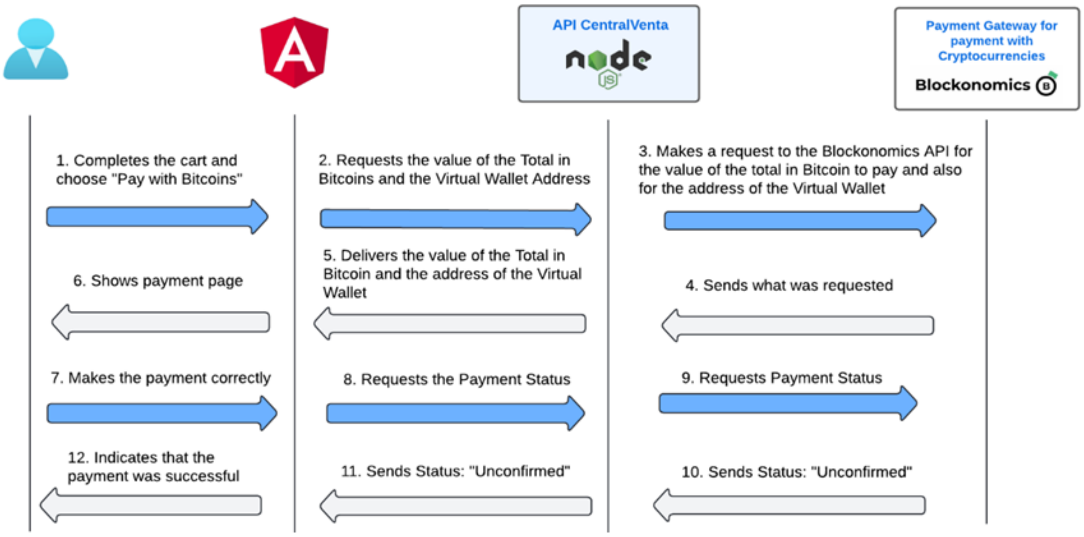

API CentralVenta
node
Payment Gateway for payment with Cryptocurrencies
Blockonomics
1. Completes the cart and choose "Pay with Bitcoins"
2. Requests the value of the Total in Bitcoins and the Virtual Wallet Address
3. Makes a request to the Blockonomics API for the value of the total in Bitcoin to pay and also for the address of the Virtual Wallet
4. Sends what was requested
5. Delivers the value of the Total in Bitcoin and the address of the Virtual Wallet
6. Shows payment page
7. Makes the payment correctly
8. Requests the Payment Status
9. Requests Payment Status
10. Sends Status: "Unconfirmed"
11. Sends Status: "Unconfirmed"
12. Indicates that the payment was successful

Figure 4: Central API - Information processing.

3. The customer clicks on “Pay with Bitcoin”, so they will be redirected to a “Verify Payment” page which contains a QR, the amount to pay in bitcoins, and a box with a message that says, “Processing Payment”. Additionally, a timer will appear, so if it reaches 0 and no payment has been made, the transaction is canceled, and you are redirected to the home page.
4. The customer makes the payment, then the message in the box will change its message: “Payment made successfully”, then they will be redirected to the home page, likewise, they will be able to see their purchase in “My Orders”.

The payment process at the frontend and backend level will follow the logic in Figure 4.

3.3.4 Sales Management Module

It consists of a section in which the seller can trace the purchases of all users of the virtual store. This section will obtain its information from the “Sales Channel”. On the other hand, it is recommended to implement a section or page in which the seller will list all users with the “Customer” role. Likewise, you can block or unblock your account activity to stop it if suspicious behavior is observed.

3.3.5 Logistics Management Module

It will include sections allowing you to manage (list, register, and modify) information on purchase orders, suppliers, and products.

3.3.6 Website Monitoring Module

It is important to track the components of a Blockchain structure to guarantee its correct functioning. Therefore, the creation of a "Website Monitoring" page is proposed in which administrators will be able to view the availability of the virtual store components, such as the "Central APIs", the node APIs, the "Authentication" API. ", the "Images" API and the database instances. If all the components (APIs and database instances) of the Sales channel nodes are operational, a message will appear at the top: “Sales Channel operational perfectly”. The same will happen with the “Logistics Channel”. If all the components of the website are operational, a box will appear that mentions “Website Operating perfectly”.

3.4 Development Process

The development will follow 4 phases:
The first phase is to request business requirements, such as Product Information, images, and videos, if necessary.

The second phase consists of the development of CouchDB instances and their respective databases for the sales and logistics channels. Likewise, a “Users” instance is created in which the credentials of the virtual store users will be saved.
The third phase consists of the development of the system APIs. To do this, first the generation of the public and private key of the Certification Authority will be carried out. Then two digital certificates are created as a Javascript object, one for the “CentralSales” API and another for the

“CentralLogistics” API. This is to authenticate with the APIs of the nodes as an extra layer of security apart from the API Key. Next, the development of the central APIs and the node APIs is carried out, so that they follow the previous logic mentioned. Also, the development of the “Authentication” API will be carried out, in which POST routes will be created for login, registration and email verification. Likewise, GET routes will be established to obtain information from users. Finally, a PUT route will be created to modify the user's status ("Active" or "Blocked"). Subsequently, the “Images” API will be developed, in which a POST route will be created to receive the image file and upload it to the Cloudinary storage service.

Finally, phase 4 consists of developing the components and services in Angular for the creation of the e-commerce pages.

4 VALIDATION AND ANALYSIS OF RESULTS

The validation was carried out in a company dedicated to the import and sale of car accessories, such as Covers, Steering Wheel Covers, Cool Seats, among others. The construction of the virtual store followed the previously mentioned guidelines.

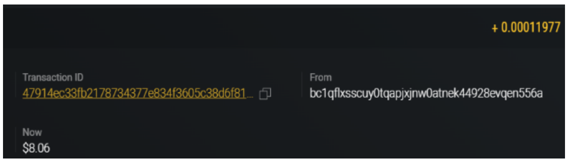
The improvement verification was carried out in the Context of "Transaction Costs", by comparing commissions for using credit card and cryptocurrency payment gateways. Additionally, we calculated the Block Time and compared it with others blockchain networks.

4.1 Verification of Improvement in the Context of "Transaction Costs"

To carry out this verification, in the case study business, a comparison of "Transaction Costs" (Commissions) was carried out for the use of payment gateways that allow payment methods with Credit Card (Culqi) and Bitcoin (Blockonomics).

A product “Wheel Insurance” was chosen with a sale price of 8.09 USD, in which, if a purchase was made with the credit card payment method (VISA), the “Culqi” gateway It would have taken an amount of 0.57 USD (due to commission and VAT), which represents 7.05% of the total sale.

Regarding the Bitcoin payment gateway (Blockonomics), the purchase was made with the cryptocurrency payment method following the process stated in the subsection 3.3.3. As can be seen in Figure 5, the gateway did not take any commission regarding the sale price. The "Blockonomics" payment gateway sends all income to the business's virtual wallet. At the end of the month, the service charges 1% of each transaction.



+ 0.00011977

Transaction ID
47914ec33fb2178734377e834f3605c38d6f81...

From
bc1qflxsscuy0tqapjxjnw0atnek44928evqen556a

Now
$8.06

Figure 5: Receiving the deposit in the virtual wallet.

Likewise, it does not take commissions for the first 20 transactions for new service users (Blockonomics). On the other hand, if several transactions were made until transaction number 21 was reached, the gateway would take a commission of 1% concerning to the sale price, which would be 0.08 USD, as shown in Figure 6.

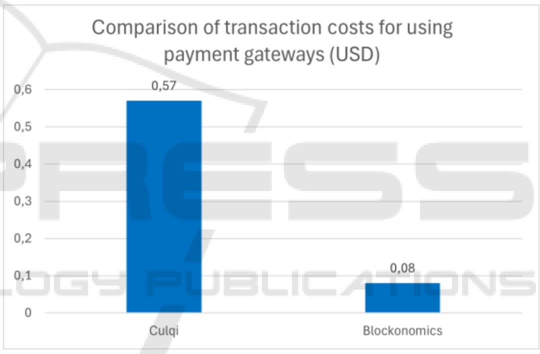


Figure 6: Comparison of transaction costs for payment gateways for transactions 21 or more.

4.2 Verification of Improvement of the Block Time

In this performance context, the block time refers to the time required for a block to be created and added to the blockchain. We retrieved the block time of a set of transactions in the e-commerce to get the average Block Time for our model:

- Registration of a supplier: 1338 milliseconds
- Registration of a product: 1321 milliseconds
- Registration of a sale: 1615 milliseconds

From the above, the average block time was 1425 milliseconds. Considering that Ethereum has a Block Time of 12 seconds (YCHARTS, 2024), we got an improvement of 88.1%. Also, BTC has a block time of 10 minutes (BitInfoCharts, 2024), thus confirming greater efficiency on the part of our system.

5 CONCLUSIONS AND RECOMMENDATIONS

This research proposes a technological model for the payment of electronic commerce with cryptocurrencies with a set of guidelines for its architecture and components. The model was validated using a case study with a company dedicated to the import and sale of car accessories. Following the defined guidelines, a virtual store was developed that allowed comparing the transaction costs of using payment gateways with credit cards and cryptocurrencies. In the storage context, we calculated the Block Time to analyze and compare its performance in comparison with other blockchain network. With all the above, the following conclusions were obtained:

- The use of payment gateways for cryptocurrencies is economically convenient because the commissions charged to the business are lower compared to those charged through credit card payment gateways.

- Using multiple nodes for information processing (block creation) is useful for identifying and preventing Man-in-the-middle attacks.

- The block time of our system was lower compared to public blockchain networks such as Ethereum and Bitcoin, making it a good choice for an e-commerce context.

Likewise, there are the following recommendations:

- These guidelines serve as an initial implementation for a Blockchain-oriented e-commerce for both payment processing and information storage, which can be improved with enhancements that fit business requirements.

- Multi-factor authentication can be implemented to increase privacy for login.

- Consider enough cryptocurrencies to take advantage of volume transaction fees.

- Increase the decentralization of information by seeking to increase the Blockchain nodes and assign them to trusted entities/roles that are independent of each other.

6 RECOGNITIONS

The authors would like to thank the Research Directorate of the Peruvian University of Applied Sciences for their role in supporting this research. Likewise, we would like to emphasize the work made by Juan Mansilla-López for providing his guidance and experience in the writing of this work.

REFERENCES

Aldweesh, A. (2023). BlockTicket: A framework for electronic tickets based on smart contract. *PLOS ONE*.

Bamert T, Decker C, Elsen L, Wattenhofer R, Welten S, & IEEE Communications Society. (2013). Have a snack, pay with Bitcoins in peer-to-peer computing. *IEEE*.

BitInfoCharts. (2024). Bitcoin (BTC) price stats and information. Retrieved August 12, 2024, from https://bitinfocharts.com/bitcoin/

Brown, M. C. (2012). Getting started with CouchDB. *O'Reilly*.

Brown, E. (2014). Web Development with Node and Express. *O'Reilly Media, Inc*.

Cáceda Salazar, H., Bravo Tejeda, F., Cáceda Salazar, H., Valle Escalante, E., Galván, S., Gálvez, F., Triveño, M., Valle Salazar, R., & Montalván Velaochaga, B. (2022). Reporte Oficial de la Industria E-Commerce en Perú. *CAPECE*.

Ehikioya, S. A., & Olukunle, A. A. (2019). A Formal Model of Distributed Security for Electronic Commerce Transactions Systems. International *Journal of Networked and Distributed Computing*.

El Peruano. (2023). Decreto Supremo que amplía la lista de los sujetos obligados a proporcionar información a la Unidad de Inteligencia Financiera UIF - PERÚ. *El Peruano*.

Elakrat, M. A., & Jung, J. C. (2018). Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network. *Nuclear Engineering and Technology*.

Eskandari, S., Clark, J., & Hamou-Lhadj, A. (2018). Buy your Coffee with Bitcoin: Real-World Deployment of a Bitcoin Point of Sale Terminal. *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress*.

Fang, F., Ventre, C., Basios, M., Kanthan, L., Martinez-Rego, D., Wu, F., & Li, L. (2022). Cryptocurrency trading: a comprehensive survey. *Financial Innovation*.

Frimpong, S. A., Han, M., Boahen, E. K., Ayitey Sosu, R. N., Hanson, I., Larbi-Siaw, O., & Senkyire, I. B. (2023). RecGuard: An efficient privacy preservation blockchain-based system for online social network users. *Blockchain: Research and Applications*.

Gan, C., Yang, H., Zhu, Q., Zhang, Y., & Saini, A. (2023). An encrypted medical blockchain data search method with access control mechanism. *Information Processing & Management*.

Gong, Y., & Huser, R. (2019). Asymmetric tail dependence modeling, with application to cryptocurrency market data. *Annals of Applied Statistics*.

Guan, Z., Wang, N., Fan, X., Liu, X., Wu, L., & Wan, S. (2020). Achieving Secure Search over Encrypted Data for e-Commerce. *ACM Transactions on Internet Technology*.

Hinarejos, M. F., Ferrer-Gomila, J. L., & Barcelo, A. J. (2022). A Secure Solution for a Blockchain-Based Consortium Promotional Scheme. *IEEE*.

Hu, Y., Manzoor, A., Ekparinya, P., Liyanage, M., Thilakarathna, K., Jourjon, G., & Seneviratne, A. (2019). A Delay-Tolerant payment scheme based on the ethereum blockchain. *IEEE*.

Kim, S. I., & Kim, S. H. (2022). E-commerce payment model using blockchain. *Journal of Ambient Intelligence and Humanized Computing*.

Kumar, G., Saha, R., Buchanan, W. J., Geetha, G., Thomas, R., Rai, M. K., Kim, T. H., & Alazab, M. (2020). Decentralized accessibility of e-commerce products through blockchain technology. *Sustainable Cities and Society*.

Li, M., Zhu, L., Zhang, Z., Lal, C., Conti, M., & Alazab, M. (2021). Anonymous and Verifiable Reputation System for E-Commerce Platforms Based on Blockchain. *IEEE*.

Liu, D., & Lee, J. H. (2022). CFLedger: Preventing chargeback fraud with blockchain. *ICT Express*.

Luo, M., Zhou, J., & Yang, P. (2023). RATS: A regulatory anonymous transaction system based on blockchain. *Journal of Parallel and Distributed Computing*.

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*.

Miao, J., Wang, Z., Wu, Z., Ning, X., & Tiwari, P. (2024). A blockchain enabled privacy-preserving authentication management protocol for Internet of Medical Things. *Expert Systems with Applications*.

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous distributed e-cash from bitcoin. *IEEE*.

Oriols, M. B., & Gómez Gutiérrez, J. A. (2019). El gran libro de Angular: 100 ejercicios prácticos. *ALFAOMEGA – MARCOMBO*.

Raynor de Best (2024). Number of identity-verified cryptoasset users from 2016 to November 2023. https://www.statista.com/statistics/1202503/global-cryptocurrencyuser-base/.

Sawarnkatat, D., & Smanchat, S. (2022). NAGA: multi-blockchain based decentralized platform architecture for cryptocurrency payment. *International Journal of Electrical and Computer Engineering.*

Su, X., Liu, Y., & Choi, C. (2020). A Blockchain-Based P2P Transaction Method and Sensitive Data Encoding for E-Commerce Transactions. *IEEE*.

Sun, Q., Dong, M., & Tan, A. (2022). An order allocation methodology based on customer repurchase motivation drivers using blockchain technology. *Electronic Commerce Research and Applications*.

Szczepaniuk, H., & Szczepaniuk, E. K. (2023). Cryptographic evidence-based cybersecurity for smart healthcare systems. *Information Sciences*.

Tadhani, J. R., Vekariya, V., Sorathiya, V., Alshathri, S., & El-Shafai, W. (2024). Securing web applications against XSS and SQLi attacks using a novel deep learning approach. *Scientific Reports*.

YCHARTS (2024). Ethereum Average Block Time. https://ycharts.com/indicators/ethereum_average_block_time.

Zulfiqar, M., Tariq, F., Janjua, M. U., Mian, A. N., Qayyum, A., Qadir, J., Sher, F., & Hassan, M. (2021). EthReview: An Ethereum-based Product Review System for Mitigating Rating Frauds. *Computers & Security*.