Development of modern payment gateways using blockchain technology

Olha Suprun[1,*,†], Oleksandr Provotar[1,†] and Oleh Suprun[1,†]

[1]Taras Shevchenko National University of Kyiv, Volodymyrska Str., 64/13, Kyiv, 01601, Ukraine

Abstract

In the process of research, the features of blockchain technology were considered, namely its use in payment systems. The advantages over centralized systems were investigated and determined. The differences between digital currency and cryptocurrency were analyzed. Options for using cryptocurrency gateways in blockchain wallets and exchanges were presented. As a result of the work, a web system with integrated cryptocurrency payment gateways based on blockchain technology was designed and built. The functionality necessary for real use of the system was implemented: wallet generation, deposit, withdrawal of funds. A clear user interface was created, with the help of which it is possible to conveniently use all the functions of the system. Such system is faster and much more protected comparing to modern web-currency analogs.

Keywords

payment systems, bitcoin, data protection, cybersecurity

1. Introduction

Blockchain is an innovative technology that has numerous applications in various fields such as retail, advertising, energy, supply chains, healthcare, etc. Thanks to blockchain, people have found a way to manage many processes securely and transparently. While blockchain applications can be found in various industries today, the payment and finance industry is at the forefront with the hype that is attracting people towards blockchain technology [1, 2].

Blockchain technology was introduced to store time-stamped records. However, the technology did not gain much attention until it was used to create and exchange a cryptocurrency called Bitcoin. Since then, blockchain has been adopted by numerous industries around the world, and everyone has appreciated its advantages.

Recently, as the world is experiencing a movement of digitalization, the payment industry is using numerous technologies to make payment procedures easier for people [3]. We have moved from accepting payments only in cash to creating a cashless economy. With the adoption of many digital payment methods, people have started using this system of money exchange. Now, with the development of technology, we are moving towards a new system of money transfer - payments through blockchain.

Blockchain payment systems are basically a way of making payments using blockchain technology. But to understand this concept better, we need to delve into the details of blockchain, how it works in payment systems and the various benefits it offers.

2. Blockchain in payments

As the name suggests, blockchain refers to a 'chain of blocks'. Blocks contain a digital record of any transaction or data exchange that takes place using the technology. A blockchain functions as a decentralized and distributed ledger, meaning that there is no central authority responsible for the data.

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

*Corresponding author.

†These authors contributed equally.

o.n.suprun@gmail.com (O. Suprun); a.i.provotar@gmail.com (O. Provotar); oleh.suprun@knu.ua (O. Suprun)

0000-0002-1196-5655 (O. Suprun); 0000-0002-6556-3264 (O. Provotar); 0000-0002-6243-3720 (O. Suprun)

© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

CEUR-WS.org/Vol-4024/paper06.pdf

A “block” has its own cryptographic hash, which is like a unique identifier. Each block contains its own hash, as well as the hash of the previous block, along with the data that connects the blockchain.

The information stored on the blockchain is distributed among the various members of the transaction network, also known as nodes. Whenever a new transaction occurs, a new block is added to the blockchain.

The transaction must be verified by all network nodes in order to add the new block to the blockchain. To verify a transaction, the nodes must reach a consensus using a consensus mechanism. Different blockchain use different consensus mechanisms such as Proof of Work, Proof of Stake, etc. Blockchain offers many advantages such as transparency and security, which is why it is a very suitable technology for the payment and financial industry [4].

2.1. Advantages of blockchain in payments

Blockchain system offers the following benefits in payments. Here are the main ones:

1. Elimination of intermediaries.
2. Transparency.
3. Secure and fast cross-border payments.
4. Automation through smart contracts.

The existing payment system requires intermediaries. To make a payment, it is necessary to go through several intermediaries and authorities, such as a payment gateway, exchange mode, issuer, etc. Even though intermediaries are responsible for maintaining the authenticity of payments, their services:

- are paid;
- increase the time of transaction execution.

Each block contains its own hash, as well as the hash of the previous block, they are chronologically linked. So, no one can tamper with the record on the blockchain, after any change will be visible. Thus, blockchain payment systems provide a high level of security, reliability and transparency to guarantee you that your payments are genuine and safe. Cross-border payments occur when the recipient and the payer live in different countries. Making cross-border payments is very problematic for a very long time.

Automation through smart contracts is a great advantage, especially for people running businesses and companies [5]. When writing smart contracts, you can mention all the requirements that need to be met to transfer the payment. Once the required data is verified, the payment is automatically made to the relevant person. For example, let’s say a company hires a content creator to deliver a certain product. The person will be automatically paid when he finishes and provides his requirements, regardless of what is required under the agreement.

2.2. Principles of operation in the blockchain system

Blockchain payment systems are not very complicated to work with. Let’s take an example of how a cross-border payment would be made through the Stellar Blockchain payment system. The example of a transfer on the Stellar network is shown in Figure 1.

2.3. Options of using blockchain in payments

As discussed earlier, cross-border payments using traditional payment methods are secure, but very expensive and slow. There are numerous intermediaries in the system, which leads to commissions ranging from 3 to 20% of the transfer amount.

Decentralized payment systems conduct transactions:

- faster;

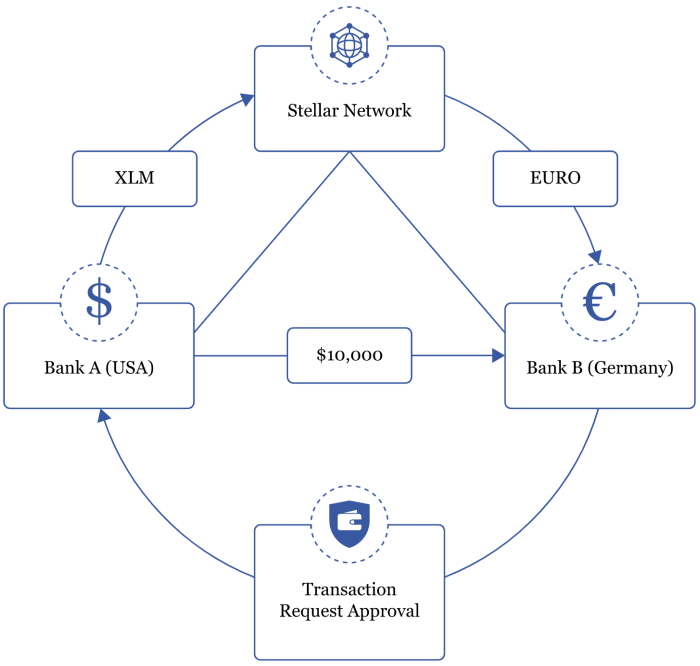

Figure 1: Example of a transfer on the Stellar network.

- cheaper;
- without the need for third-party permissions.

Banks like Westpac are partnering with Ripple to implement low-cost cross-border blockchain payment systems. Many banks and companies are planning to implement blockchain payment systems in their businesses to make secure and fast cross-border payments.

Trade finance refers to the financial activities related to international trade. Trade finance deals with a huge amount of paperwork related to payment records and invoices, amounts credited, etc. These procedures are time-consuming as multiple copies of the same paperwork are required for multiple uses, and there is also the possibility of errors when filling out documents manually, which can lead to complete unusability of the documentation.

With the help of blockchain payment systems, trade finance documents can become more manageable because:

1. No manual effort is required to record payment details, invoices, and bills.

2. A single document can be accessed by all participants, as blockchain payment systems work as a distributed ledger.

3. The possibility of manual errors will be eliminated, as information about all payments made through a blockchain payment system will be stored directly on the blockchain.

3. The difference between digital currency and cryptocurrency

Quite often, cryptocurrency is identified with digital currency, but this is wrong, since there are fundamental differences between cryptocurrency and digital currency that you need to know.

Digital currency is money used to make payments over the Internet. They exist only in virtual form and have no real equivalent. But they can be sent, received and exchanged in the same way as fiat money, so they have all the classic monetary characteristics. With their help, you can pay for goods in online stores, make utility payments, pay for mobile and Internet, as well as other services. Digital wallet funds can be sent and received around the world.

Cryptocurrency is a type of digital money that is considered a more reliable tool for data exchange. Cryptography ensures the accuracy of protocols and algorithms created and analyzed to transmit data without modification and destruction. Cryptocurrency is based on blockchain technology, and everything that happens on its network cannot be controlled by any regulators.

3.1. Digital currencies

Digital currencies or electronic money are monetary balances recorded electronically on a stored value card or remotely on a server. The Bank for International Settlements defines electronic money as "stored value or prepaid payment mechanisms for making payments through point-of-sale terminals, direct transfers between two devices, or open computer networks such as the Internet." Electronic money is typically associated with so-called smart cards issued by companies such as Mondex and Visa Cash.

Electronic money is a floating claim that is not tied to any specific account. Examples of electronic money include bank deposits, electronic funds transfers, payment processors, and digital currencies.

The term "stored value card" means that the funds and/or data are "physically" stored on the card in the form of binary encoded data. With prepaid cards, the data is stored on the card issuer's computers. Typical stored value cards include: prepaid phone cards, gift cards, employee pay cards, loyalty cards, travel cards.

Electronic money can also be stored on (and used via) mobile phones or on an online payment account. The most common and widely used mobile subsystems are Google Wallet and Apple Pay. The rapid adoption of electronic money has led to government regulatory activity.

Electronic currencies can be divided into soft and hard currencies. Hard electronic currencies are those that only support irreversible transactions. It is impossible to change a transaction even in the event of a legitimate error. They are more focused on cash transactions. Examples for hard currencies are: Western Union or KlickEx. On the other hand, soft electronic currencies are those that allow for the reversal of payments in the event of fraud or disputes. Examples are PayPal and credit cards.

In other words, digital accounts and wallets can be considered like bank account balances.

3.2. Cryptocurrencies

Cryptocurrencies are a type of digital currency. Cryptocurrency is an asset used as a medium of exchange. It is considered secure because it is based on cryptography.

One of the main goals of cryptography is communication and how to protect it. It creates and analyzes algorithms and protocols so that no information is changed or interrupted during a conversation by third parties. Cryptography is a combination of a large number of different sciences, with mathematics as the basis. It is mathematics that gives rigor and reliability to algorithms and protocols.

Cryptocurrencies use blockchain and a decentralized ledger system. This means that no supervisory authority controls the actions on the network. This happens in the space of all users.

3.3. Key differences between digital currency and cryptocurrency

lthough cryptocurrency is a type of digital currency, there are significant differences between them:

- Structure. Digital currency is centralized; transactions are controlled by servers belonging to a group of people in such a system. Cryptocurrency is decentralized in structure; rules are dictated by the majority of participants in the crypto community.
- Anonymity. To use digital currency, you need to pass identification, present scanned identity documents, and wait for their confirmation. Using cryptocurrency does not require such actions. Although cryptocurrency cannot provide complete anonymity either, since transactions in them are recorded and tracked.
- Transparency. Digital currency is opaque, it is impossible to see information about other people's money transfers to their wallet address. Cryptocurrency is transparent, and user transactions are entered into a publicly available blockchain.

- Transaction management. Each digital currency system has a central authority that deals with resolving problems, canceling transactions in disputed situations, freezing wallets at the request of the authorities. Cryptocurrency is controlled by the crypto community, which approves changes to the ledger.
- Regulatory framework. Most states have developed legal statuses for digital currencies, while defining them in legislation. As for cryptocurrencies, only a few developed countries have created a legislative framework, while the rest of the world has not yet defined the official status of cryptocurrencies.

Most of the differences can be viewed as both advantages and disadvantages.

In a centralized system, there is a group of people responsible for the state of the entire system. If you make a mistake in a transaction, you can submit a request to the company and rely on a successful outcome. You cannot do this in a decentralized system.

On the other hand, centralized networks store a lot of confidential information about users. This data can be lost, corrupted, or handed over to law enforcement at the request of a court. Decentralized networks do not have these problems.

The same applies to the cancellation of a transaction. If a centralized system can be revoked, you can make changes to the transaction on the blockchain. At the same time, this opens up space for fraudulent actions.

4. Areas of payment gateways usage

Cryptocurrency payment gateways should enable the implementation of a business decision to accept cryptocurrency transactions as payment from customers in exchange for goods or services. These systems should accept payments from any country and emphasize security due to the blockchain-based nature of cryptocurrencies.

When a customer makes a transfer of funds using cryptocurrency as payment, the transaction often passes through the payment gateway at a fixed rate and is automatically converted to a traditionally defined fiat currency so that the buyer can avoid the volatility of the cryptocurrency markets. However, some cryptocurrency payment gateways do not automatically transfer cryptocurrency to fiat currency, allowing the merchant to hold the digital coins for as long as they wish, typically inside a cryptocurrency wallet.

Cryptocurrency payment gateways tend to offer lower fees than traditional credit card payment systems. Some of these tools can be easily customized and provide their own dashboards to help track all payments. Bitcoin is the most commonly supported cryptocurrency used in transactions with these systems, however, gateways should provide the ability to pay in alternative cryptocurrencies such as Ether, Litecoin, XLM and any other popular currencies. Cryptocurrency payment gateways can integrate with e-commerce platforms, point of sale systems, shopping cart software, billing and accounting solutions, etc. To qualify for inclusion in the “Cryptocurrency Payment Gateway” category, a product must:

- Accept and process cryptocurrency payments;
- Connect transaction systems to e-commerce solutions;
- Securely store cryptocurrencies or exchange them for fiat currencies;
- Encrypt transaction information using blockchain technology.

4.1. Blockchain wallets

A blockchain wallet is a cryptocurrency wallet that allows users to manage various types of cryptocurrencies - for example, Bitcoin, Ethereum, and others. A blockchain wallet helps someone exchange funds easily. Transactions are secure because they are cryptographically signed. The wallet can be accessed from web devices, including mobile, and the user’s privacy and identity are preserved. So, a

blockchain wallet provides all the features needed for safe and secure transfers and exchange of funds between different parties [6, 7].

This is very similar to the process of sending or receiving money through PayPal or any other gateway used for traditional currency transfers, but instead you use cryptocurrency. Examples of blockchain wallets are Electrum, Blockchain.info, MetaMask. There are many more based on your needs and the security you need.

Traditional banking systems pose several challenges for carrying out any transactions. On the one hand, transactions are often slow. On the other hand, any transaction must go through an intermediary, like a bank, i.e. a central point of failure. And there are problems with keeping track of all accounts and balances; data can be compromised, manipulated, or even corrupted across multiple systems where accounts and balances are maintained. Blockchain wallets reduce or completely eliminate these problems.

Here are some features of Blockchain wallets:

- Easy to use. It's just like any other software or wallet you use for your daily transactions;
- Secure. It's just a matter of protecting your private key;
- Enable instant, seamless, and non-intermediate transactions across regions;
- Low transaction fees. The cost of transferring funds is significantly lower than traditional banks;
- Enable transactions between multiple cryptocurrencies. This allows you to easily convert one currency to another.

Hot wallets are online wallets that allow you to quickly transfer cryptocurrencies. They are available online. Examples include Coinbase and Blockchain.info. Cold wallets are offline digital wallets where transactions are signed offline and then revealed online. They are not backed up in the cloud online; they are backed up offline for a high level of security. Examples of cold wallets include Trezor and Ledger. Hot wallets store private keys in the cloud for fast transfer. Cold wallets store private keys on separate hardware that is not connected to the internet or the cloud, or they are stored on a paper document. Hot wallets are easily accessible over the internet 24/7. They can be accessed via a desktop computer or mobile device, but if hacked, there is a risk of irreparable theft. In cold wallets, the transaction method helps protect the wallet from unauthorized access (hacking and other online vulnerabilities).

A software wallet is a program that is downloaded to a device; it can be a desktop or mobile device, or it can be a web wallet that can be accessed online. Breadwallet, Jaxx, and Copay are popular software wallets.

Desktop wallets are cold wallets where your private keys are stored on cold servers (on your desktop). You can take your wallet offline, do some offline transactions, and then bring it back online. In case your main server goes down, a cold server, basically your desktop, is used as a backup server. These wallets can be downloaded from any computer, but they can only be accessed from the system they are installed on, so you want to make sure that the machine you are downloading the wallet to is safe (has a backup and is in a safe place). These wallets are definitely cost-effective. Electrum is one of the most popular desktop wallets.

Web wallets are another type of hot wallet that works on the internet. Users can access these wallets from any device. It can be a tablet or computer, or you can access it from a mobile browser. The private keys are stored online and managed by a third party. For example, GreenAddress is a Bitcoin wallet that is available online, has an Android app, is available on desktop, and is also available on iOS.

Mobile wallets are similar to online wallets, except that they are designed for mobile phone use and accessibility only. These wallets have a user-friendly interface that helps in making transactions easily.

4.2. Cryptocurrency exchanges

Cryptocurrency exchanges are platforms that facilitate the trading of cryptocurrencies against other assets, including digital and fiat currencies. Essentially, cryptocurrency exchanges act as an intermediary between buyers and sellers and make money through transaction fees and commissions [8].

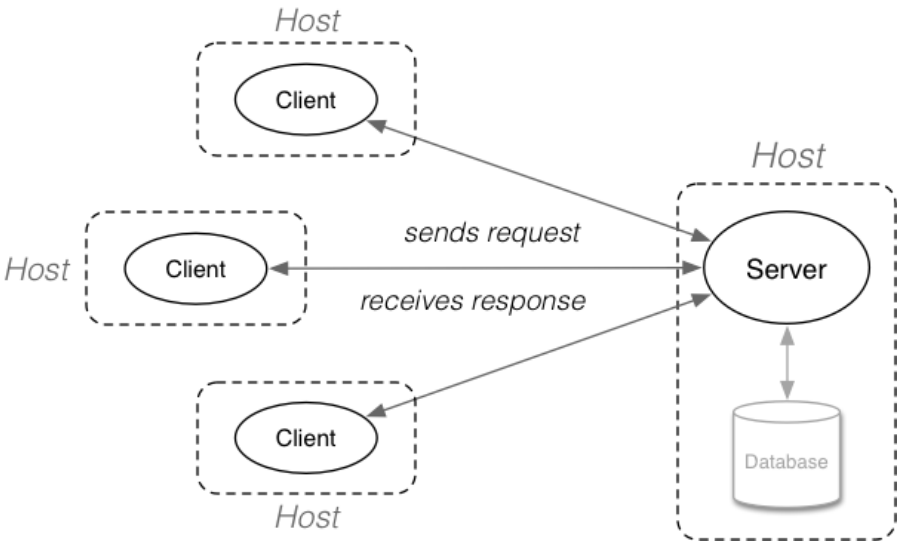

Figure 2: Client-server architecture.

Centralized cryptocurrency exchanges act as a 3rd party between a buyer and a seller. Since they are managed and controlled by a company, centralized exchanges offer greater reliability. Approximately 90% of all crypto transactions go through centralized exchanges.

Decentralized cryptocurrency exchanges (DEXs) allow users to perform peer-to-peer transactions without the need for a third party or intermediary. Due to some of the problems associated with centralized exchanges, some users prefer decentralized exchanges. However, decentralized exchanges do not facilitate the trading of fiat currencies for cryptocurrencies.

Centralized exchanges offer novice investors a familiar, user-friendly way to trade and invest in cryptocurrencies. Unlike using crypto wallets and peer-to-peer transactions, which can be complicated, users of centralized exchanges can log in to their accounts, view their account balances, and make transactions through apps and websites.

They also offer an added level of security and reliability when it comes to transactions and trading. By facilitating transactions through a sophisticated centralized platform, centralized exchanges provide a higher level of convenience.

However, centralized exchanges are run by companies that are responsible for maintaining their customers. Large exchanges typically hold billions of dollars, making them a target for hackers and theft. An example of such an incident is Mt. Gox, which was once the world's largest cryptocurrency exchange until it reported the theft of 850,000 bitcoins, leading to its shutdown Unlike peer-to-peer transactions, centralized exchanges often charge high transaction fees for their services and convenience, which can be especially high when trading large amounts.

5. Description of the developed system

The goal of developing the system is to facilitate the execution of financial transfers, the acceptance of digital payment methods, namely cryptocurrencies, for any user around the world. In order to proceed with the implementation of the system itself, it is necessary to fulfill the necessary design conditions: determine the features of the system, describe the interaction options and provide a physical representation of the architecture.

The basis of the system is a client-server architecture, which will ensure maximum client relief, transfer of the computational load to the database server (SQL server), as well as significant strengthening of data security - both from malicious and erroneous changes. The general scheme looks as follows, as shown in Figure 2.

The starting point will be the user's login to the system and creation of a payment request, the final

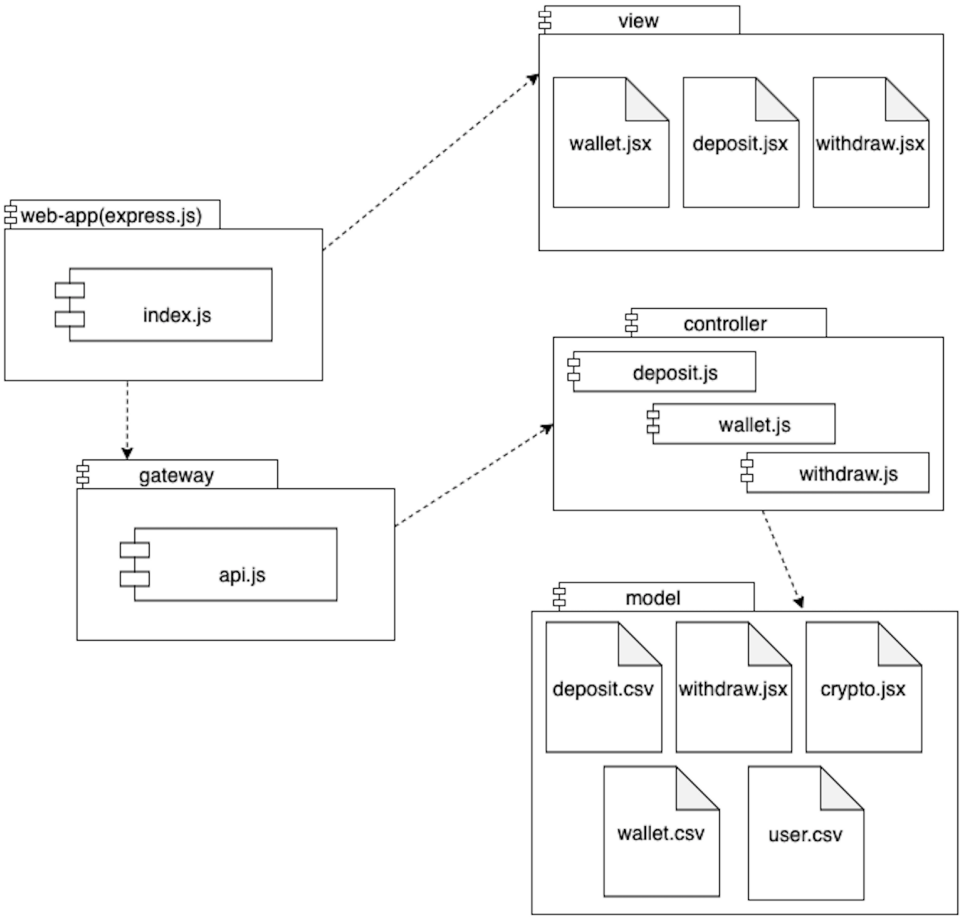

Figure 3: Component diagram.

point will be the result of the request execution, either successful transaction execution, or errors that occurred during the work. The user's interaction with the system occurs step by step:

- creation of a request;
- agreement on the terms;
- provision of payment details (such as: transfer amount, recipient, and other upon request);
- execution of the payment by the system itself;
- obtaining the result of the work;
- updating the balances in the database.

After describing the behavior, it is necessary to present the physical structure of the project, namely to determine which components are needed to create a payment system. We will illustrate these requirements in the form of a component diagram, which is presented in Figure 3.

The main module index.js, which is an instance of the imported Express.js module for implementing the software framework, namely creating the server part of the web application.

The gateway section contains the api.js module, which is responsible for routing requests in the system. The logic for executing requests is performed by controllers that are distributed to perform separate purposes: deposit, withdrawal and account information (balances, transaction history). Models contain the logic for storing and processing transaction data. Views display the data that is passed to them, according to the type of operations. All views are implemented using the React framework.

The main idea of the development is to create a separately functioning payment system for processing all necessary operations of the cryptocurrency exchange, and integrate them into the client part of the entire project. The system supports functionality in the context of more than one cryptocurrency, and

allows the use of BTC, ETH, LTC, EOS, XLM, BNB, USDT (ERC20). Provides convenient integration of new currencies in the future.

Stellar uses public-key cryptography to ensure the security of every transaction: every Stellar account has a key pair consisting of a public key and a secret key. The public key is public - it is needed by other people to identify your account and confirm that you authorized the transaction, it is like an email address. However, the secret key is private information that confirms that you are the owner of the account and grants access to it, it is like a password and should never be shared with anyone.

Any action that is performed on Stellar - such as sending payments or making buy/sell offers - is called a transaction. To submit a transaction to the network, you need to combine it into a transaction, which is a group of 1 to 100 transactions, accompanied by some additional information, such as which account is making the transaction and a cryptographic signature to verify the authenticity of the transaction.

Transactions are atomic, meaning that if any operation in the transaction fails, all of them fail. Let's say you have 100 lumens and you make two payment transactions of 60 lumens each. If you make two transactions (each with one operation), the first will succeed and the second will fail because you don't have enough lumens. You'll be left with 40 lumens. However, if you group the two payments into one transaction, they won't be able to go through, leaving all 100 lumens in your account.

Each transaction also requires a small fee. Like the minimum account balance, this fee is to discourage spam and prevent people from overloading the system. This base fee is very small - 100 stroops per transaction, where stroops equals $1 * 10^{-7}$ XLM - and it is charged for each transaction in the transaction. For example, a transaction with two transactions would cost 200 stroops.

The proposed system is able to perform the following actions:

- Create an account;
- Operations and transactions;
- Sending a payment (withdraw);
- Receiving a payment (deposit).

6. Conclusions

The integration of Bitcoin-based payment systems within web applications developed using the React framework represents a significant interdisciplinary convergence between decentralized financial technologies and modern front-end software engineering. Bitcoin, as the most established cryptocurrency, alongside with other crypto-systems offers unique advantages including cryptographic trust, resistance to censorship, and independence from centralized financial institutions. These attributes align closely with current trends in digital sovereignty and user-centric financial control. React, on the other hand, offers a component-based architecture and a robust ecosystem conducive to building dynamic and responsive interfaces. Its modular design and compatibility with state management libraries and API integrations make it a compelling choice for implementing real-time payment flows and interacting with blockchain infrastructure.

However, while the technical feasibility of such integrations is increasingly evident, their practical deployment introduces a range of complexities. These include, but are not limited to, the volatility of cryptocurrency markets, scalability limitations of the Bitcoin network, regulatory uncertainties across jurisdictions, and challenges in ensuring usability and accessibility for non-specialist end users. Moreover, the environmental and ethical considerations surrounding proof-of-work consensus mechanisms remain areas of critical inquiry and ongoing debate within the broader scientific and policy communities.

Nevertheless, recent advancements - such as second-layer scaling solutions like the Lightning Network and the increasing availability of developer tools and APIs - are gradually mitigating many of these limitations. These developments not only enhance transaction speed and reduce fees but also pave the way for broader adoption of cryptocurrency in mainstream web applications. When combined with the flexibility and responsiveness afforded by modern JavaScript frameworks like React, a new paradigm of decentralized, user-friendly financial applications becomes increasingly attainable.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] L. Al-Abbasi, W. El-Medany, Blockchain security architecture: A review technology platform, security strength and weakness, in: 2nd Smart Cities Symposium (SCS 2019), Bahrain, 2019, pp. 1–5. doi:10.1049/cp.2019.0190.

[2] Z. Hu, Y. Khokhlachova, V. Sydorenko, I. Opirskyy, Method for optimization of information security systems behavior under conditions of influences, International Journal of Intelligent Systems and Applications 9 (2017) 46–58. doi:10.5815/ijisa.2017.12.05.

[3] M. Zaliskyi, et al., Model building for diagnostic variables during aviation equipment maintenance, in: International Scientific and Technical Conference on Computer Sciences and Information Technologies, 2022, pp. 160–164. doi:10.1109/CSIT56902.2022.10000556.

[4] P. K. Kaushal, A. Bagga, R. Sobti, Evolution of bitcoin and security risk in bitcoin wallets, in: 2017 International Conference on Computer, Communications and Electronics (Comptelix), Jaipur, India, 2017, pp. 172–177. doi:10.1109/COMPTELIX.2017.8003959.

[5] Z. Hu, S. Gnatyuk, T. Okhrimenko, S. Tynymbayev, M. Iavich, High-speed and secure PRNG for cryptographic applications, International Journal of Computer Network and Information Security 12 (2020) 1–10. doi:10.5815/ijcnis.2020.03.01.

[6] H. Takahashi, U. Lakhani, High secure mobile wallet for token transfer using escrow account on PoA voting blockchain, in: 2023 IEEE 12th Global Conference on Consumer Electronics (GCCE), Nara, Japan, 2023, pp. 478–480. doi:10.1109/GCCE59613.2023.10315485.

[7] N. Marchenko, O. Nechyporuk, O. Suprun, O. Martynova, O. Suprun, M. Melnyk, Methods of designing adaptive systems of multilevel monitoring and diagnosis for recognition and forecasting of technological condition of complex technical objects, in: 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2021, pp. 290–293. doi:10.1109/ATIT54053.2021.9678591.

[8] Y.-F. Wen, C.-M. Huang, Stability analysis of market-making mechanisms for decentralized cryptocurrency exchanges, in: 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dublin, Ireland, 2024, pp. 299–301. doi:10.1109/ICBC59979.2024.10634337.