Security of Financial Software to Support Cryptocurrency Trading

Julijana Mirčevski[1,*], Nikola B. Popović[1], Mirjana Andrić[2] and Branko Stanojev[3]

[1] *Permanent court expert, Belgrade, Serbia*
[2] *Bank of America Global Technology, London, Great Britain*
[3] *Attorney at law, Belgrade, Serbia*

Abstract

Cryptocurrency trading is becoming a feature of the world's digital commerce in the present time. The software used to carry out financial operations in cryptocurrency trading must have speed and reliability. Successful cryptocurrency trading is unsustainable without secure financial software. The paper analyzes the interdependence of these two close areas as well as possible individual deviations in the functioning of financial software. The elements for controlling cryptocurrency trading software based on the specifics of a real case are discussed.

The introduction of cryptocurrencies into financial, market and social movements in general required a complete change in the security system. In dealing with crypto-currencies, the protection of social institutions (banks, auditors, financial police) is insufficient, but priority must be given to software solutions, mathematical algorithms, and the laws of probability theory. In this sense, business in the domain of cryptocurrencies has significantly improved the methodology, means and technology of protection of all participants of financial transactions in general. The elements for quality control of cryptocurrency trading software are discussed based on the specifics of a real case.

Keywords

cryptocurrency, financial software, reliability and speed, standards in digital commerce

1. Introduction

Financial transactions can be done through various digital forms: cards, mobile phone, etc. When paying with cards, a device called a POS terminal (Point Of Sale) plays an important role. It is a simple electronic device, of relatively small dimensions, equipped with software for processing payment card transactions. Its basic functions are: reading data from the card, forwarding it to the accepting bank and accepting the response of the issuing bank, based on which the payment for the purchase of goods is made. It is used in service and commercial shops. It is the device through which the user accesses the "big black box" that performs financial transactions.

It is useful to return to the basic principles of digital payment at the beginning of the analysis, that is, to observe the process from the general to the individual. Digital trade currently uses the internet as its basic technological infrastructure. Financial software applications require a more detailed understanding of Internet management. The fact is that Google, as a significant participant in the Internet, occupies a huge part of the transaction ecosystem. Google is an intermediary, but by definition also a "controller", and in itself the maximum cybersecurity risk since it controls traffic in the world in accordance with its protocols and especially its interests. Google has a de facto monopoly on the search function. Without an independent / alternative / parallel Internet, there can hardly be a reliable digital trade, but at the moment there is no choice.

The next level of "control" are ISPs (Internet Service Providers). ISPs have the equipment and access to the telecommunications lines needed to connect to the Internet in a given geographic area. ISP is a company that provides individuals and organizations with access to the Internet and other related services (e-mail, domain registration and web hosting, etc.). Services are charged. Does the ISP provide "trusted services"? And here, the primary question is who forms and who chooses the ISP, that is, who is the "best" on the market, by analogy with Google, "which is always the best on the market".

In addition to the technological participants in the management of data flows, there are also participants from the domain of legislation (levels of states and international or supranational organizations) that further complicate the process of data transfer. The term "trust service" is now in very wide use in the world and in our country, and is formalized in a series of laws and regulations. However, if we look at the broader picture, some very serious processes in the field of finance and trade in the world raise doubts about the meaning of the term "trust" [1]. Paper or more precisely virtual gold recalls, whether we like it or not, the early conquest of America

BISEC'22: 13th International Conference on Business Information Security, December 03, 2022, Belgrade, Serbia

[*] Corresponding author.

julijana.mir@gmail.com (J. Mirčevski); nikola.popovic@eunet.rs (N. B. Popović); mirjana_andric@yahoo.com (M. Andrić); stanojev.br@gmail.com (B. Stanojev)

CEUR Workshop Proceedings (CEUR-WS.org)

by Europeans who gave the natives shiny glass balls in exchange for physical gold [2]. In this paper, we do not deal with gold, but the question of "trusted services" remains partially open. For example, does Google as a company really provide trustworthy services? Let's just mention the issue of collecting user personal data and creating a user profile that is formally generated for the purpose of more efficient searching. Regulations and mechanisms for preventing money laundering allow all messages to be intercepted and read! There are too many intermediaries that provide "trusted services" and this opens up a much wider range of issues than just the issue of the correct functioning of software and hardware. opt to use a combination of methods to ensure transparency. The set of GDPR [3] rules recommend a layered application of privacy notices as well as links to different categories of information that must be shown to the data subject. The software tool should avoid information fatigue for the user, but at the same time ensure the effectiveness of information.

2. Analysis of possible omissions

Software web tools for financial transactions have been used for many years in domestic financial operations. During that time, the following failures in financial software applications stood out as typical:

- If the text data is entered in Cyrillic, the program accepts the input but "does not see" the Cyrillic text when searching.
- Software applications do not contain built-in priority levels of operations. So it is possible that anyone can read everything and even change the content.
- Duration of operations is limited but not aligned with the limitations of another software service that follows or precedes the downloaded operation (general synchronization problem).
- The duration of the operation is unlimited, so financial transactions made on one day do not reach the recipient's account until the next day or after weekends and holidays
- Servers do not work continuously but only during "working hours"
- Currency exchange is not regulated in the same software service, so it must be "manually" entered or exited in another software service
- "Server crash" results in the inactivity of the website of a bank or other company that performs transfers through a web application, which causes delays in payments, breaking loan repayment deadlines, incorrect interest calculations, and the like.

The problems caused by these omissions are mostly solved individually, and often through court cases. There is no professional agency, association, group of competent individuals who would make a general solution in disputed cases. Analyzes show that similar problems arising from the insufficient security of software applications are also appearing in the world. They are solved in various ways, so it is necessary to make an overview of the relevant world experiences.

According to research published by us, https://www.it-klinika.rs/ [4], 30 financial applications from the domain of the economic sector, banking and insurance were tested. The testing was performed by a "white hat hacker" using the reverse engineering method. On almost all applications, the presence of sensitive data in the source program code has been registered. The data showing that 97% of Android applications did not have binary code protection is particularly worrying. This makes it possible to use the technique of reverse engineering to decompile the source code, modify the program and, by recompilation, put the wrong program into use by the users. A team of researchers from Columbia University found bugs in 306 Android applications [5]. Some of these Android apps have up to 100 million downloads on the Google Play Store.

When we talk about the security of financial software in our country, we mainly mean exposure to virus attacks, and funds are set aside for that type of protection.

Blockchain technology was created in 1991 but it became known only in 2009 with Bitcoin. The text [6] states: "It aimed to be a viable alternative to financial relations that could be made directly between people, without the need for a trust institution, as a bank“. Blockchain technology offers 3 essential conditions to ensure data integrity: security, action traceability and transparency in data handling. Another tool to prevent improper access and change of data blocks is proof-to-work. A blockchain condition in which to create a new data block must wait X minutes (i.e. 10 minutes for Blockchain). Thus, in case of an external attack on the data of one of the blocks, it would be necessary to recreate the following blocks to redo the hash numbers so that they can be identified, and the attack is not noticed. But thanks to proof-to-work, there is no time for it. With Blockchain technology, it is possible to record and track all product-related actions across the entire production chain. From raw material to final consumer, everything is recorded with exceptional security and transparency.".

Everything that has been said is correct, but in the observed case, it is obvious that there is some element of the "production chain" that does not work according to the theory that appears in a huge number of articles on this topic. Blockchain ensures the integrity of a certain chain of data packets, but to what extent and whether it ensures the integrity of the entire chain of transactions.

Is the blockchain technology implemented correctly, who checks it and how? For example, the temporary event of the interruption of the use of payment cards [7] can be understood in a technological sense, but to what extent can a series of already executed transactions be followed - how was the interruption situation processed and explained at the time of interruption. Finally, the interruption of payment itself is carried out at one point, but what happens to the transaction that is being carried out right then. Does the theory take into account working in conditions of unreliable internet, with which we objectively have contact (technological problems, political problems, sanctions, etc.)

3. Reflection on modern digital trade

Companies that register to trade digital currency establish their site in an effort to expertly help anyone interested in buying and selling cryptocurrencies relatively easily and safely. Since that moment, the registered company has established and operationally supports a whole range of services that are common in the international practice of cryptocurrency trading: a crypto machine for buying, a BTC-app for paying with bitcoins, a two-way crypto machine for buying and selling BTC and LTC, buying with cards, network of crypto machines in Serbia, vouchers, management of instant purchases, Wallet. The available set of these services differs from company to company, from the time when the trading process is started, from the environment as well as from the laws of the country in which the company operates.

Most often, trade is enabled within 5 different cryptocurrencies (Bitcoin, Ethereum, Litecoin, Bitcoin Cash and Tether), and powerful foreign companies also have more digital currencies in circulation. It is necessary that business technology is constantly improved.

The operations of cryptocurrency trading companies are regulated by the Law on Digital Assets (Official Gazette of RS No. 153/2020), according to which, in accordance with the definition of Article 5 of Article 2 and Article 3 of the Law, such a company is a provider of services related to digital assets. Sites such as: https://ecd.rs, https://teslacryptocap.com/, are functional platforms for trading digital assets that, in accordance with the definition of Article 11 of Article 2 of the Law on Digital Assets, organize cryptocurrency trading. On these software platforms, it is possible to join people interested in buying and/or selling cryptocurrencies, as well as exchanging one cryptocurrency for another. Transactions take place in accordance with the applicable rules and in a manner that leads to the conclusion of the contract.

Well-known foreign companies for this type of trading are: IQ Option, eToro, Binance, Coinbase

4. Actions and measures to improve the security of software applications in the field of financial transactions

In the case of payment or trade via the Internet, it is necessary to ensure the undeniability of the transaction. It is not enough to "trust" that a transaction has been carried out, it is necessary for the recipient of the transaction message to confirm without a doubt that the transaction has been fully carried out. This means that every financial program for payments or trade must necessarily use a parallel communication channel that confirms the execution of the transaction. For example, when we pay an invoice electronically through the bank, we will receive a confirmation of payment from the other party in a shorter or longer time. An example is mobile telephony, where the confirmation usually arrives within 24 hours. But there are smaller amounts that are not so interesting. Larger amounts, especially cross-border transactions, require a much longer time. For example, some banks, for reasons of "control", allow the collection of a foreign check in 45 or more days. Cryptocurrency trading software, if it wants to function in the mix of banks and control institutions, must be equipped with significantly more complete and efficient mechanisms for confirming the non-repudiation of execution. Control institutions slow down the flow of money and it costs money, but it is reasonable to assume that this slowdown brings some of the intermediaries a lot of profit. This is a serious contradiction, since it turns out that it would be necessary to check the messages of a billion people to find a few hundred or thousands of terrorists. This is not a logic we can accept without serious reservation.

The criteria that must be met in order for electronic transactions to be secure are the following:

- Ensuring the privacy of communication,
- Protection of secrecy and confidentiality of data,
- Protection of sensitive and personal information from intentional and unintentional disclosure,
- Ensuring data integrity,
- Detection of unauthorized modification of data in transmission

In order to meet the above criteria, software applications must provide the following processes: Authentication means a programmatic procedure for verifying the identity of a user (person, application or device) that requires access to a system or network, Authorization includes the process of checking whether a person or entity is legally authorized for the rights it requests Non-repudiation of a transaction consists of procedures to eliminate the possibility that the initiator of the transaction denies sending the message.

It is necessary for the digital platform to introduce software support for authentication standards. The software systems of several companies that operationally support cryptocurrency trading own their digital platforms on the rs or io domain and provide the specified required security functions. For this purpose, the ECD system application uses hash functions in order for the system to realize the authentication of requests sent by a specific identified user. The hash function, according to a certain algorithm, generates a series of characters that result in a unique transaction identification code. When talking about authentication standards, it is useful to mention that certain countries impose restrictions on authentication capacity [1, 2]. In the chapter "Import and Export Control Laws" [8], the author explains in detail the problem of transfer of software technologies, i.e. algorithms, and the reasons for restrictions. These are long-known restrictions, but users are persistently told about the maximum protection of their digital money. In addition, system software ie. operating systems, development software as well as software that is purchased from the original manufacturer or intermediary has limitations in the laws of more technologically developed countries [9]. Trade in digital money is done over the Internet, so the rules of operation and protection are provided by those who are technologically strongest, that is, those who manage the Internet.

The term "Cryptocurrency wallet" also introduces the term "trust", for example [10]: "Embedding support for a cryptocurrency wallet is essential for a crypto exchange. All the crypto tokens/coins will be stored in the user's wallet. Developing a wallet solution with enhanced security will help in the development of trust between users and your cryptocurrency exchange.

We repeat that it is a multifactorial problem that cannot be accepted at the technological level. In technology, reliability is ensured by a multiple safety factor (in construction, by incorporating several times the amount of concrete and iron, etc.).

The "maximum security" of storing and generally working with cryptocurrencies is limited by the local laws of the countries in which the headquarters of security firms are located. The applied protection algorithms must be aligned with local normative acts that regulate the export and import of technologies related to the protection of communications and data. The fact that an algorithm is patented for a user in cryptocurrency trading means nothing - it all depends on what is actually implemented in a software system.

5. On the application of software quality standards

In the observed case, an incident occurred that clearly indicates a problem in the software through which digital money trading was performed. In a formal sense, it can be expected that an entrepreneur who performs cryptocurrency trading services uses the correct software in accordance with the valid regulations of the Republic of Serbia and the corresponding foreign and domestic regulations used for the domain of banking services. The observed omission is of such a nature that there is reasonable doubt as to whether the software has passed quality control. In software quality control, it is necessary to follow control procedures in accordance with international and national standards. In the observed case, the supplied software subsequently demonstrated a defect (is it the only one?). deliver, so the question arises as to how the results of the initial quality control, ie the behavior of the software in the time domain, are monitored. What complicates the analysis is the assessment that it may not even be a programmer's fault. Namely, the question is whether the software over time remains in the same (initial) operational state in which the application started? It is useful to note that, in addition to the common view of software and hardware as fixed structures, they are in fact dynamic structures. Operating systems are frequently updated (most often in the form of improved protection etc.) and sporadically cause problems. It also updates the development software used to create cryptocurrency trading software, among others. For example, the Python programming language in version 10.3 cannot be installed under the Windows operating system if the operating system version is below version 8. At the same time, the same version of the programming language, together with all its libraries, can be installed without problems on Linux. From a purely software point of view, cryptocurrency trading software projects work with extensive function libraries (for example Microsoft Base Cryptographic Provider), or software libraries used in the development of applications and depending on the applied programming language. For example, in the text [11], a table of frequently used software components in the development of applications for working with cryptocurrencies is given in Table 1.

It is especially important to emphasize that digital currency trading applications are primarily oriented towards WEB technology (programming languages PHP, JavaScript, etc.), which is known for its security "holes". Browsers are also software components that are literally continuously updated (in the visible and invisible domains). To what extent all those components passed quality control is an important question, since the influence of the market is disproportionately present here.

Table 1
Software components for work with cryptocurrencies

Mobile App Development	React Native, Flutter, Xamarin
Web App Development	Node.JS, Nest.js, Next.js, Angular, React.JS, PHP
Back-end Development	MongoDB, MySQL, AWS, Fire-base

There is no reason to believe that software components have serious flaws, but practice shows that there is no reason to believe that they do not.

6. Quality control in a complex software/hardware environment

Analysis of international standards for software quality control [12] and other documents in the field of control indicates that not all features of interest are covered. For example, on page 11 [12] it is written: "4.2.2.1 Time behavior - Degree to which the response and processing times and throughput rates of the product or system, when performing its functions, meet requirements.

4.2.2.2 Resource utilization - Degree to which the amounts and types of resources used by a product system, when performing its functions, meet requirements."

In the first point called "Time behavior", the maintenance of the response time of the product or system is observed, but not the functional changes over time, i.e. the assumption is that the product is static in terms of functional characteristics. The second point, Resource utilization, talks about "the degree and type of resources that meet (initial) requirements". Trading in digital currency or assets in general is done in direct contact with the (external) environment, which is dynamic in nature. New system participants appear, some disappear, some change software systems, etc. Despite the fact that the criteria for participation in traffic are sufficiently clearly defined (message formats, messages, etc.), practice shows the possible presence of anomalies.

International standards are concentrated on one product (software or any other system) viewed as an individual entity. However, how to control the quality of "compound software" actually a software system consisting of "local software(s)" interacting with "external software". As far as we have established so far, "quality control" is not foreseen in this case. When trading in digital assets or money, this procedure is not implied. Even checking external software would be an act of attacking foreign software. Legal Restrictions clearly indicate that external, actually independent software certainly does not fit into something that is subject to quality standards. The user can only trust that it will not be stolen by someone with higher access powers. When the basic software uses or communicates with several external software and in addition to the defined work protocols, there is no sufficient control - checking the synchronization of their work and the results of data processing. For example, there is a known problem of losing time synchronization on personal computers due to the aging of devices, this as a technical aspect is not considered in quality control since it is "understood" that all participants in the trade are equipped with correct devices.

The issue of quality control of "software complex" is not covered by any international regulations or recommendations. The term "International Information Security" is not new, but it has not yet been introduced into the domain of digital commerce. Regulations and standards refer to "observed software of a single manufacturer". Since the software complex is created by the nature of things by the inclusion of products from several "software manufacturers", the matter is significantly more complicated. For example, the latest worldwide automotive "supply chain" crisis shows that replacing components is not a simple matter at all. The problem of "chips" for electronics in cars, although it initially seemed simple, created a series of new problems, one of which is checking the compatibility of chips from different manufacturers. The same or in reality much more complicated thing is with the "complex software" that uses the "services" of different software, but not only (individual) software, but also the system of services (one can also say a chain of services). For example, paying for the services of buying digital currency requires the service of at least one but essentially more banks. Banks' response times differ both in terms of time and method of message exchange. The bank as an intermediary has its own inertia, which is conditioned by technology, but also by many other reasons of an economic nature, that is, reasons of the bank's business policy. Do banks use reliable software systems, do they use "proven libraries" in software development? Which and what kind of software each individual bank uses cannot be known. Checking these queries is not possible in practice because it would amount to a violation of regulations. It means that the user and financial operators only have at their disposal "trust in the bank", which is basically a religious attitude and not a technological one.

Blockchain technology in itself is not controversial, i.e. the theoretical basis is probably correct enough. The key problem is in the application i.e. when blockchain technology starts to be applied in the "production chain", but without knowing what is applied in the "accessible" or "peripheral" part of the production chain. Namely, in the text [7] it is said: financial relations that could be made directly between people, without the need for a trust institution, as a bank. The fact is that intermediaries appear in digital currency trade, and what technology is used in that "intermediary" part of the "production chain" remains unknown. Only the intermediary or intermediaries can be "trusted" to use reliable technology. Blockchain is valid for "directly between people", which is in contradiction with intermediaries who make money from the services of the intermediary service.

With API I, a note from the text [13] is useful, which says: "You can also implement other APIs that complement your crypto currency API to help build a better project. Consider security features like email verification or phone verification a priority for many crypto currency-based projects.". Also, for example for "Binance API" it says: "The API is easy to implement, with relatively few issues or bugs, and thus the low likelihood of requiring additional troubleshooting."

The author of the mentioned quotes is Emma Jager - Google alumna, which warns us that people with more (big) experience in this field know that there are problems in APIs as well. In our environment, claims that we have a large number of IT experts are largely overshadowed by the fact that even 25% of the total number of experts have a secondary education. It is also useful to note the trend expressed in text [11]:

"The demand for cryptocurrency exchange apps will continue to rise with the growing trading volumes worldwide. In such a scenario, launching a high-end crypto exchange app is a far better choice than thinking of ways to mine bitcoin tokens. By being an intermediary and handling transactions efficiently, an entrepreneur can earn enormously."

Developing software for crypto exchange can earn more money than "mining" which requires significant investment, which means that software with potentially problematic features will be mass generated.

7. Process flow on a concrete example

A company engaged in the provision of services related to digital assets for a fee, in the territory of the Republic of Serbia, performs transactions, purchases and sales of virtual currencies. The processes are carried out "online" through the website, i.e., the digital platform.

On the site, the Rules of Business are highlighted, as well as all other instructions that users should follow, in order to buy virtual currencies for a number of dinars or to be paid a certain number of dinars for the sale of virtual currencies. Transactions are processed by a software application, so that everything is automatically transferred, namely money to a bank account when selling virtual currencies, or virtual currency to a specialized digital "wallet" - when buying virtual currencies.

The user is regularly registered on the site, which means that he has attached personal documents, that he is personally identified, that he is in the records of the digital currency trading company. Also, the user voluntarily accepted the merchant's business rules in the field of selling and buying virtual currencies published on the digital platform - the merchant's website.

In accordance with the Business Rules, a Contractual relationship is established between the User and the trading company. The contractual relationship is always established at the User's initiative by creating an order for the purchase (or sale) of virtual currencies, which is considered as giving an Offer to conclude a contract. If the Order is created in accordance with the instructions given on the website, it is considered that the Offer has been accepted by the trader's company. After that, the software application informs the user that the order has been successfully sent, that is, that the offer has been accepted. Then, the trader approaches the fulfillment of his obligation, i.e., sending money, in cases where the User sells virtual currencies, i.e., sending virtual currencies, in cases when the User buys virtual currencies.

Through the digital platform-site, the specific user created an order for the purchase of virtual currencies of the type "Ethereum" for the amount of 100,000.00 (one hundred thousand) dinars. The epilogue of the created order is such that they were sent/transferred to the user's digital wallet by the Merchant. Virtual currency "Ethereum" in the amount of 0.27135122 units of the same (equivalent to the value of 100,000.00 dinars at that moment). However, the dinar amount of RSD 100,000.00 was not paid. The financial operator, in this particular case the money transfer service "iPay", did not forward the reserved money from the User's account to the Merchant's bank account, but returned it to his bank account.

This case is a consequence of incorrect functioning of the financial software of organizations in the trade chain. The "iPay" service has an explanation that it is an "electronic error". The Merchant is seeking a final epilogue and possible compensation in a court case.

8. Concluding considerations

Financial service providers depend on customer trust, privacy and risk management. It is imperative to protect sensitive data deposited by customers from cyber-attacks and data breaches. A solution that includes enterprise risk management (ERM) capabilities is required. Such a solution provides protection not only for the company from potential business impacts of the crisis, but also protection for shareholders, customers and the industry as a whole from any ill effects and ripples. In particular, risk should be reduced in complex environments. Complex environments, data and software can make software finance applications more prone to vulnerabilities and increase security risk. There are software tools that can provide security for even the most complex configurations of digital trading, including cryptocurrency trading. If the speed of development is maximized, agile processes give developers speed, but then it is usually difficult to insert enough security processes without slowing down development. Special tools are needed that can help maximize speed while minimizing risk with. Since the trade in cryptocurrencies is enormously increasing and accelerating, the number of financial software applications in modern system software environments that function on the web or in the cloud is increasing to that extent.

References

[1] BullionStar, Infographic: London Gold Market, 2016. URL: https://www.bullionstar.com/blogs/bullionstar/infographic-london-gold-market/.

[2] Daliborka Kiković, Nova Akropola: Konkvistadori, 2017. URL: https://www.nova-akropola.rs/konkvistadori/.

[3] European Data Protection Board, Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, 2020. URL: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-062020-interplay-second-payment_en/.

[4] IT klinika, Finansijske android aplikacije prepune ranjivosti, 2022. URL: https://www.it-klinika.rs/blog/finansijske-android-aplikacije-prepune-ranjivosti.

[5] S. RAMASUBRAMANIAN, Columbia University team finds bugs in several Android apps, 2020. URL: https://www.thehindu.com/sci-tech/technology/columbia-university-team-finds-bugs-in-android-apps/article32581423.

[6] D. Rocha, R. Almeida, S. Martins, Blockchain and Data Integrity in Computer System Validation, 2017. URL: https://fivevalidation.com/blockchain-and-data-integrity-in-computer-system-validation/.

[7] ECD.rs, Trenutno je onemogu'ena kupovina platnim karticama , 2017. URL: https://ecd.rs/servisne-informacije/trenutno-je-onemogucena-kupovina-platnim-karticama.

[8] J. L. Grama, Legal and Privacy Issues in Information Security, Jones & Bartlett Learning, 2020.

[9] M. Learn, Restrict the use of certain cryptographic algorithms and protocols in Schannel.dll, 2022. URL: https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/restrict-cryptographic-algorithms-protocols-schannel.

[10] P. Rupareliya, How to Build a Cryptocurrency Exchange App, 2018. URL: https://medium.com/swlh/how-to-build-a-cryptocurrency-exchange-app-d463d3e0ccb3.

[11] A. Gromenko, How to Create Your Own Cryptocurrency App: Everything You Need to Know, 2021. URL: https://code-care.com/blog/cryptocurrency-app-development/.

[12] I. O. for Standardization, S. Technical Committee ISO/IEC JTC 1, Information technology. Subcommittee SC 7, systems engineering, Systems and Software Engineering: Systems and Software Quality Requirements and Evaluation (SQuaRE): System and Software Quality Models, ISO, 2011.

[13] E. Jagger, Best Crypto Currency APIs, 2022. URL: https://www.abstractapi.com/guides/best-crypto-currency-apis.