Features of the development of information systems for working with blockchain technology

M G Gorodnichev, E G Kukharenko, T U Salutina, M S Moseva and A M Kukharenko

Moscow Technical University of Informatics and Communication, Moscow, Russia

E-mail: m.g.gorodnichev@mtuci.ru, e.g.kukharenko@mtuci.ru, m.s.moseva@mtuci.ru, a.m.kukharenko@mtuci.ru

Abstract. This article is devoted to the development of an information system for conducting financial transactions on a cryptocurrency exchange based on blockchain technology. The paper provides a brief overview of the underlying technology, the advantages and disadvantages are identified, the design of the information system and user interface is carried out.

1. Introduction

The main prerequisite for the emergence of modern cryptocurrencies is the active development of Internet commerce. All monetary transactions are carried out with the participation of financial institutions, which act as intermediaries for electronic payments. The need for third-party participation requires additional costs for conducting user transactions. All transactions through financial institutions can be canceled, which creates additional risks and inconveniences when conducting online trading [1].

The first and most popular alternative at the moment is Bitcoin. Bitcoin is a cryptography-based payment system that allows users of this system to make money transactions directly without the participation of a third party.

The main technological innovation is Blockchain technology. Blockchain technology is a record of all bitcoin transactions in chronological order. The block chain is the same for all users and is stored in each node of the Bitcoin peer-to-peer network. The blockchain is necessary to create guarantees of uniqueness of each bitcoin transaction, which prevents the problem of double spending.

The problem of double spending is an attempt to make two different transactions for the same unit of currency. Thus, the possibility of endless cryptocurrency copying is suppressed.

The key point in creating a cryptocurrency is the development of a special algorithm that can solve the problem of “double spending” without the participation of third parties - financial institutions.

2. Protection of personal data in the Bitcoin network

One of the most pressing issues in the field of conducting bitcoin transactions is the protection of personal data of users of the Bitcoin network. The private key of a bitcoin wallet is the only resource that allows you to access your bitcoin assets. It is important to understand that the loss of a private key leads to the complete loss of all its bitcoin assets without the possibility of restoring a private key. This problem must be solved by backing up your private keys [2].
It is worth noting that users in the bitcoin network are uniquely identified using a unique account number, which allows anonymous transactions. The only thing that connects the network user to transactions is the number of the bitcoin wallet.

3. The possibilities and disadvantages of Bitcoin
The technologies on which the Bitcoin network operates have a set of the following functions [3]:

- Decentralized storage of the database of all user transactions within the Bitcoin network;
- Protection against unauthorized changes in transaction data;
- Ensuring transparency of interaction between network participants;
- The absence of a third party when conducting user transactions.

Bitcoin was the first successful electronic currency based on Blockchain technology, which could not but lead to the appearance of significant shortcomings in attempts to introduce it:

- Loss of a private key from a bitcoin wallet entails a complete loss of their accumulations;
- There is no way to recover a lost private key from a bitcoin wallet; This problem can be solved by backing up the private key on electronic media or on paper.
- Very low transaction speed. Validation and creation of a record in a decentralized transaction database (Blockchain) can take up to several minutes due to the constantly growing technical requirements for new calculations. The growth of the transaction database leads to an increase in transaction time. Soon, a transaction may take from 5 hours;
- Bitcoin code is open, if a loophole in the code is detected, it will be exploited by cybercriminals, which can lead to system damage and a significant drop in the Bitcoin exchange rate;
- If at the location of the attackers there will be more than 50% of the computing power of the Bitcoin network, they will be able to rewrite the rules for all network users, which can lead to the destruction of the system.
- Transactions in the Bitcoin network are not anonymous. There is a possibility that a person can be identified by the public key.

Also, the cryptocurrency Bitcoin has a sufficient number of disadvantages, because of which it will be very difficult for Bitcoin to become an international financial instrument:

- High cryptocurrency volatility;
- The system is designed in such a way that it is not profitable to invest in cryptocurrency in the long term;
- Bitcoin is very difficult to regulate, which can create certain problems for legal organizations;
- There are no common cryptocurrency exchange points.

4. Trading strategy
Developing an automated trading system for trading on a cryptocurrency exchange is an extremely complex process, which begins with the selection of the right trading strategy. It should be best suited to the current market situation. A trading strategy should have a clear logic and subsequent empirical verification. The development of a model of a profitable trading strategy is based on a conceptualization of each step, rigorous testing and debugging. One of the main requirements of a trading strategy is choosing the right moment to create a sell order or purchase for the further sale of cryptocurrency [4].

Any trading strategy should include risk management tools when entering the market. A typical way to control risks is to strictly adhere to a certain price range, which prevents severe losses that may occur in the current market situation.
A trading strategy may include the ability to control profits, which protects not actualized profits generated during the period of conducting transactions on orders. After the development of a trading strategy and its implementation in the software, there is a stage of testing and optimization of a trading strategy in real trading. A stage of developing a special environment for testing a trading strategy is possible, which is a very non-trivial task. It is difficult to design and develop a test environment in the right way. Thus, it makes sense to test and optimize a trading strategy in real cryptocurrency exchanges. Software testing in real markets should be carried out under the close attention of the developer to quickly identify problems in the software or to identify vulnerable revenge in the trading strategy [5].

Optimization of a trading strategy is a continuous process that continues until the developer abandons the chosen strategy. The market is constantly changing, and the trading system must be adapted to such variability. The key point in optimizing a trading software is to see gaps in a trading strategy using real trading on a cryptocurrency exchange as an example.

Trading on a cryptocurrency exchange through software is in most cases a complex and difficult to predict process. Clear recommendations and rules do not exist. With such trading, it is very important to actively monitor the state of the market and the behavior of the trading software [6].

When developing a software tool for trading on a cryptocurrency exchange, you need to choose trading exchanges that have an API for programmatic interaction. API is a set of software functions for interacting with the exchange through external software tools. The API is used by programmers to develop algorithms for cryptocurrency exchanges.

When trading on a cryptocurrency exchange, first you need to study the available strategies and choose the most suitable one for yourself. In the process of use, the selected strategy can be changed and modernized depending on the situation on the cryptocurrency exchange [7].

5. Cryptocurrency exchange scalping strategy design
Scalping on a cryptocurrency exchange is a high-frequency cryptocurrency trade with opening and closing orders for short periods of time, so that a small profit from each transaction pours out after a lapse of time into a fairly large profit.

To trade on the cryptocurrency exchange using the scalping trading strategy, a software tool will be used to monitor the state of the exchange, creating orders for the purchase and sale of cryptocurrency at a favorable rate in order to profit from cryptocurrency speculation accounts. To begin with, it is necessary to think over the most basic functions that a software tool for algorithmic trading should perform and think over the algorithm for buying cryptocurrency on the exchange.

The software tool creates a warrant for the purchase of cryptocurrency at a lower market price for a fixed percentage of interest. If after a certain period of time the purchase order is not executed, then a decision will be made to cancel the order and a new order will be created taking into account changes in the cryptocurrency exchange rate on the exchange.

When using the scalping strategy when buying and selling cryptocurrency, almost no forecast is made on the further course of the cryptocurrency. Transactions are made instantly. To sell cryptocurrency for fiat money, an approach similar to that used when buying cryptocurrency is used.

The main objective of the sale is the sale of cryptocurrency at a price several percent higher than the price for which the cryptocurrency was originally purchased.

Before selling cryptocurrencies, the presence of purchase orders is initially checked. If they are not, then the software starts selling the cryptocurrency that was purchased earlier [8].

6. Application architecture
In order to ensure the possibility of working with developed applications from all possible operating systems that have a browser and a graphical interface, it was decided to develop a system for trading on the cryptocurrency exchange in the form of a Web application running on a client-server architecture.

Client-server architecture involves the interaction of two or more software tools that are located on different computers. The client application will be a web browser that will send certain requests to the
server computer with the corresponding server software package to perform certain financial transactions on various cryptocurrency exchanges.

Server computers will run a software server enclosed in packages from the Django Framework. The software package running on the Django server will analyze the cryptocurrency rates on cryptocurrency exchanges and make appropriate trading decisions. Transferring application components of the software to the server side reduces the requirements for the configuration features of client software, but increases the requirements for performance and security of client data on the server side.

7. Application Partitioning Logic

To ensure the reduction of time spent on the development of complex software tools, it is often necessary to use ready-made solutions for organizing software components. Following a certain design pattern allows you to develop certain software constructs, which will allow the developer to communicate more easily with each other, referring to common terms, and reduce the number of architectural errors in the software being developed.

If a developer who is familiar with development patterns begins to parse the program code of an application developed according to well-known development patterns, then it will be much easier for a developer to understand the basic logic of the software.

Using the Django Framework for development, you must adhere to a strict separation of the parts of the software. Following certain development patterns and dividing the logic of the software into separate parts, you can make changes to each individual part of the software without affecting the rest of its parts.

The development of software based on this separation of the parts of the software is based on the use of a design pattern called “Model-View-Control” or “Model-View-Template”.

In this development pattern, “Model” refers to the presentation of the rules for interacting with databases and accessing them. The term “Presentation” refers to the logic by which the data requested by the user will be visually presented. The term “Management” refers to a component of a software tool that is responsible for processing data, implementing business logic, and choosing the appropriate “presentation”.

Each component of the software tool works independently of other components, which reduces the number of errors in the software tool, provides the ability to more easily scale, test, and debug software components.

The principle of the application, the operation of which is based on the pattern "Model-Presentation-Management":

- The client sends a request to the server and asks to provide the html page of the web application with a certain content;
- The control module sends a request to the database access control module to obtain the requested data;
- The “Model” block sends to the control unit the requested data;
- In order to transfer data to the client, the “Management” module must select a specific presentation model, for this a request is made to the “Presentation” module;
- The "Views" block answers the request and transmits the page template in html format;
- The "Management" block returns to the client a page in html format with the requested data.

8. Prototype GUI Program

For convenient work with a software tool for conducting automated trading on a cryptocurrency exchange, you must have a graphical interface with a minimum number of software tool controls for successful conclusion of trade transactions. The graphical interface of the trading software is presented below.

The software tool with this graphical interface works according to an algorithm that corresponds to the cryptocurrency exchange scalping strategy.
The presented graphical interface provides the user with auxiliary information for convenient monitoring the status of glasses on the cryptocurrency exchange and quotes of courses. It is possible to view the operations performed in the form of a table.

![Figure 1. Software GUI.](image)

9. Conclusion
As part of this work, a detailed study of the principles of the Blockchain technology was conducted, an analysis of cryptocurrency exchanges was conducted, and cryptocurrency trading techniques were studied and described in detail [9].

A prototype software was implemented. The development of the prototype relied on a detailed design part, which included mock-ups of graphical interfaces of the software, a description of the development stages and trading algorithms on which the work of the software for conducting automated trading on the cryptocurrency exchange is based.

The task of cryptocurrency price forecasting, based on market analysis and quotation trends, is an extremely non-trivial task and for the most part, cryptocurrency prices are poorly technical. To analyze cryptocurrency quotes, an analysis method using exponential smoothing was used, which did not show positive results when trying to use it in algorithmic trading to conclude trading transactions. The cryptocurrency exchange scalping trading strategy is most effective [10].

Reference
[1] Buldin I D, Gorodnichev M G, Makhrov S S and Denisova E N 2018 Next generation industrial blockchain-based wireless sensor networks Proc. Wave Electronics and its Application in Information and Telecommunication Systems, WECONF (Saint-Petersburg, Russia)
[2] AlMallohi I A I, Alotaibi A S M, Alghafees R, Azam F and Khan Z S 2019 Multivariable based checkpoints to mitigate the long range attack in proof-of-stake based blockchains ACM Int. Conf. Proc. 3 118-22
[3] Pal O, Alam B, Thakur V and Singh S 2019 Key management for blockchain technology ICT Express
[4] Aras S T, Kulkarni V 2017 Blockchain and its applications — A detailed survey *Int. J. Compt. Appl.* **180** (3) 0975-8887

[5] Lin I-C and Liao T-C 2017 A survey of blockchain security issues and challenges *Int. J. Netw. Secur.* **19** (5) 653-9

[6] Lewko A and Waters B 2011 Unbounded HIBE and attribute-based encryption *Advances in Cryptology - EUROCRYPT* **6632** 547-67

[7] Lei A, Cruickshank H, Cao Y, Asuquo P, Chibueze P, Ogah A and Sun Z 2017 Blockchain-based dynamic key management for heterogeneous intelligent transportation systems *IEEE Internet Things J.* **4** (6)

[8] Billings J, Image-Based Proof of Work Algorithm for the Incentivization of Blockchain Archival of Interesting Images, University of Colorado Denver

[9] Huckle S, Bhattacharya R, White M and Beloff N 2016 Internet of Things, blockchain and shared economy applications *Procedia Comput. Sci.* **58** 461-6

[10] Borrows M, Harwich E and Heselwood L 2017 The Future of Public Service Identity: Blockchain, report of M/s Accenture 1-13