Blockchain technology: banking system review

Maria Gopkalo

Haaga-Helia University of Applied Sciences
Bachelor's Thesis
2021

Author

Maria Gopkalo

Degree

Bachelor of Business Administration

Report/thesis title

Blockchain technology: banking system review.

Number of pages and appendix pages

37 + 0

Blockchain technology, relative to other popular innovations of a large-scale nature, has appeared recently. However, it quickly gained popularity not only as a new system but also as an opportunity to influence many existing problems in different spheres of human activity, by creating new products based on it. At the moment, opinions about this technology differ.

The purpose of this study is to identify different areas of integration from a technical point of view of the functionality and internal component of the crypto wallet, given the large selection of cryptocurrencies, into a classic bank wallet.

- Determine the technical model of cryptocurrency and crypto wallet, as well as their main format of work
- Determine the technical model of the banking product "online wallet" and make its architecture
- Identify the main technical criteria of the crypto wallet that affect the integration.
- Find different options for implementing a new product in the architecture of a banking enterprise and make models of integration results

However, it's worth noting that this study has some limitations. Due to the novelty of the topic under study and the lack of practical implementation, it seems that most of the discussion will be purely theoretical and illustrative.

Conducting a study and searching for possible options for integrating crypto wallet services made it possible to identify the final version of the architecture of the banking industry, or rather its specific product "online banking".

In this research, the definition and characteristics of the blockchain were studied, the current state in the industry was studied and the feasibility of further implementation was determined. Also, the goal of the work was achieved - an analysis was carried out of whether the blockchain will increase the level of security of banking operations compared to current methods of conducting.

Keywords

Banking, blockchain, bitcoin, Ethereum, transaction, user, buyer, seller.

Contents

1 Introduction

Blockchain technology, relative to other popular innovations of a large-scale nature, has appeared recently. However, it quickly gained popularity not only as a new system, but also as an opportunity to influence many existing problems in different spheres of human activity, by creating new products based on it. At the moment, opinions about this technology differ. Some large investors do not risk investing in it, but other companies are trying to offer more advanced products to the market on its basis. This topic is relevant, as products continue to be created and attract investment, and it is impossible to give an accurate answer to the question of whether these products will be viable for a long time. Given that they are aimed at different areas in which solutions already exist, in one form or rather, the task of integrating this technology into ready-made business models has not been solved. The main need to study this issue is to understand the possibility of implementing this integration from the point of view of the optimal benefit of the company regulating the product in question. The question posed at this time is often attributed to the digital transformation of business. It is necessary to algorithmize the process and clarify whether in the banking industry this is a pivot, or the introduction of new product solutions into the business process?

In 2009, Satoshi Nakamoto published the bitcoin code, and the cryptocurrency was trading at $0.003 per 1,000 units — as of 2017, it has grown by a few hundred thousand times, breaking through the mark of 1800 dollars for 1 unit.

However, the concept and scope of blockchain are much broader than cryptocurrencies. Features of distributed ledger technology allow it to be used in a large number of industries - from file transfer systems in torrent trackers to more reliable copyright protection. for example, in art and elections.

Naturally, blockchain technology has caught the attention of the banking sector. If some central banks are sceptical about the free-floating of the blockchain-based rip, then the technology itself is of great interest. Central banks of developed (USA, UK, European Union) and developing (China, Russia, etc.) At the same time, the largest European banks, led by HSBC, announced the creation of a consortium to develop blockchain-based platforms for internal transactions among themselves; Bank of America together with Microsoft is engaged in the creation of an online blockchain platform

In the banking industry worldwide, there has been a continuous increase in the use of online banking and non-cash payment. Additionally, there is a strong push in the blockchain products industry, and in particular a product such as a crypto wallet, which I am going to consider in this study. The increasing popularity of payment with both classic currency and cryptocurrency raises the question of how to implement their integration into one common product. My research is intended to answer this question.

Vincenzo Morabito – author of one of the most famous books on the blockchain, "Business innovation through blockchain" – defines the technology as a distributed decentralized cipher-protected database, a public repository of information. in which each completed transaction is recorded and becomes known to all participants in the network. Any transaction in the registry is recognized as valid only if it is approved by more than half of the network participants. This means that no single participant in the system or an agent from the outside can conduct a valid transaction without the consent of other users.

A global study of cryptocurrencies conducted by the University of Cambridge in 2017, and updated a year later, shows that the number of active, unique wallet owners is constantly growing. In 2013, the number of users was approximately 3 million people. By 2017, this number had increased almost 2 times, amounting to 5.8 million. The number of active wallets is 11.5 million ciphers (Hileman, 2017).

1.1 Research objectives and research question

The object of the study is the process of integration of two different technologies into a single banking product. On the one hand, blockchain technology and a certain product, such as cryptocurrency, are considered. The object in which this technology will be integrated is a classic banking product: an online wallet. The problem situation of the object of research is the question of choosing the direction of integration.

The subject of the study is the business model of the products and companies under consideration. In this case, it is necessary to consider the object from the point of view of the effective application of blockchain technology in the banking sector. Since the business model includes a large number of additional parts that need to be considered, which are written about later, we will not specify them as separate subjects of research, and we will consider them as a general component.

The purpose of this study is to identify different areas of integration from a technical point of view of the functionality and internal component of the crypto wallet, given the large selection of cryptocurrencies, into a classic bank wallet.

- Determine the technical model of cryptocurrency and crypto wallet, as well as their main format of work
- Determine the technical model of the banking product "online wallet" and make its architecture
- Identify the main technical criteria of the crypto wallet that affect the integration.
- Find different options for implementing a new product in the architecture of a banking enterprise and make models of integration results

There are several options for integrating cryptocurrency into a classic banking service. Additional integration of cryptocurrency and the implementation of the possibility of its use in a classic bank wallet will allow banks to cover more areas, and offer more services to their consumers. This integration will lead to a large additional profit. This study addresses the technical challenge and the need to change the business models of banks wishing to integrate cryptocurrency into their product line.

1.2 Methodology

In this study, I will mainly use the theoretical method of solving the tasks. It will include the following separate areas of work:

- Analysis and generalization of the history of technology development. Search for the main necessary theory among the available online publications on popular resources related to the research topic, as well as written books.
- Search and comparison of the technical component of finished products on the open online resource GitHub. The main programming languages and the main files that allow you to link the algorithms of the product are investigated.
- Search and study of the objects under consideration and their representation using the ArchiMate modelling language. It allows you to cover different layers of architecture, from the point of view of the enterprise.

1.3 Limitations

However, it's worth noting that this study has some limitations. Due to the novelty of the topic under study and the lack of practical implementation, it seems that most of the discussion will be purely theoretical and illustrative.

As will be seen from further investigation, most of the ideas discussed are thoughts or points of view that may seem biased towards one direction or another. With this in mind, it is important to note that this study should not be regarded as the only source of information on the topic under discussion and that readers are strongly encouraged to conduct further research on their own.

In addition to this, it is important to note that this study should be seen as an attempt to raise awareness of the topic as, in the author's opinion, it has great potential for further research.

2 Literature review

In this chapter, I look at cryptocurrency from the technical side. First of all, it is necessary to pay attention to the history of the development of blockchain technology, on which the products in question work. What are the main changes that were a consequence of the current popularity, and the reasons for their occurrence?

2.1 The market of projects based on blockchain technology and their historical development.

The world saw the technology and the first blockchain-based project, called bitcoin, in the fall of 2008 (the first public appearance on January 9, 2019). Satoshi Nakamoto, the nickname of the creator of this technology, sent a letter to a certain circle of people in which he described the algorithm of his idea (Bitcoin.org, 2021). It was the first significant breakthrough in history, which in the future will greatly change the market of IT projects and forever leave a mark as one of the most widely divided technologies in the views of the public. As it seems to many, the motivation of the creator was the desire to rid the third party as an intermediary in financial matters of two traders. In other words, a feature of bitcoin, a cryptocurrency written based on the blockchain, was the possibility of transferring digital currency without an additional supervisory authority in the person of a bank or other financial institution.

In order to continue, let's define the main mechanism of operation and terms of this technology:

Blockchain is a technology for reliably distributed storage of records of all bitcoin transactions ever made. Blockchain is a chain of data blocks, the volume of which is constantly growing as miners add new blocks with records of the most recent transactions.

The main innovation of this technology is an architecture that provides decentralized (divided among all participants in the process) transactions.
Any transaction is essentially a transfer of ownership. The nature of almost any such operation implies a lack of mutual trust between the participants in the transaction, which requires the presence of a third party in the transaction, which would be guaranteed its execution. The concept of blockchain allows the participants of the system to reach agreements on the transaction without participation and confirmation from the intermediary. Thus, the need for an intermediary disappears, which in theory allows you to change all

spheres of human life, where in one way or another there is an exchange between persons. not having mutual trust.

Blockchain is an information array that has the following characteristics:

· Peer-to-peer decentralized distributed system

· Certain members can make changes

· Digital signature and cryptographic algorithms are used to authenticate, verify the user, and allow them to make changes and track transaction facts

· The structure of the system makes it almost impossible to make changes to already held records (completed transactions)

· The structure of the system leads to the fact that the participants of the system become quickly aware of the fact that someone is trying to make changes to the transactions made.

· Financial transactions are part of the technology

· Direct participants and a wide audience can track transactions

Blockchain is a chain of transaction blocks. The key element is the transaction log, with transactions being the only way to change the state of the ledger. For a transaction to be considered complete and confirmed (consent is required more than half the life of the network participants), its format and signatures must be verified, and in the case of validation it (or a group of transactions) is written to the block.

A block includes a list of transactions and a header that contains its own hash, the hash of the previous block, the hash of the transactions, and additional information. The connection between the blocks due to the presence in each (except the first) hash of the previous one means that it is impossible to make changes to the block without changing the entire chain with first block - you cannot delete any transaction or insert it between already completed. Hash functions and electronic signature are two of the most important elements of the blockchain, providing connectivity and authorization.

Cryptocurrency is basically digital cash. It is both a digital currency and an online payment system in which encryption technologies provide control over the generation of monetary units and confirmation of the transfer of funds, and which works independently of state structures regulating the financial industry. In fact, we can say that cryptocurrency is a means of payment, which at the same time does not have a full set of functions of money, but acts more as digital goods, the cost of which depends on the standards generally accepted among users.

A crypto wallet is a service that provides the ability to store and conduct certain operations with cryptocurrency. It is based on the technology of encrypting information using an identification key that is unique to each user. Wallets for storing cryptocurrency are of 4 types, each of which I will consider in more detail in the future: paper wallet (paper-wallet); software wallet (soft-wallet); hardware wallet (hard-wallet); exchange (exchanges).

Initially, during the advent of the blockchain and bitcoin, a model for regulating this technology and its public use was not developed. The reasons are pretty clear, the technology was developed for humans, and was planned to be synonymous with the word "freedom". However, in fact, after almost 10 years of its worldwide use, it has become clear that it is impossible to do without research in matters of its use in the business environment.

After this proposal, a rather obvious question arises: "What has happened in these 10 years?". The history of blockchain projects is quite extensive to affect all its areas, so I will try to talk about the most important ones related specifically to the cryptocurrency side. This retrospective is aimed at understanding the algorithms of development. Remembering in which direction the progress was moving and having understood its reasons, you can find more arguments for answering the question in which direction it is likely to move on.

According to the unspoken philosophy of technology, all projects based on it are open source in version control systems. Basically, GitHub (GitHub, 2021) is a gravity platform that attracts all developers. The feature of GitHub allows you to identify the creators of the technology, the stack technologies used in the creation of the project, and also provides value to potential investors in the form of understanding risk factors. Since writing the first code on which bitcoin was built, the number of projects on GitHub increased by an average of 8600 per year. In 2016, that figure approached 27,000 (Deloitte, 2021).

The growth of project content has not kept up with the accelerated growth in the number of projects. "When analyzing blockchain repositories and their contents, we noticed that the number of participating organizations is growing rapidly. In 2010, organizations developed less than 1% of all projects. In 2017, their blockchain projects accounted for 11%.

And the latest data on the success of blockchain initiatives of commercial open-source organizations looks promising; among them are some major well-known commercial entities," Deloitte wrote in its study of GH Torrent and GitHub API data. We can notice that the development of projects of this technology occurs in the so-called leaps. This conclusion can be drawn based on the trend towards a strong increase in the number of projects and the popularity of the technology in the short period of time in question. Most often, cultural phenomena that are characterized by leaps can be divided into logically interrelated periods. What periods in the market of blockchain projects can be distinguished?

- Phase 1.0: The emergence of bitcoins and altcoins. Transaction. (2008-2013)

After the first mined cryptocurrency, the formation of bitcoin into the understanding of the public began. The complexity of the technology and the small community that was analyzed above explains the reasons for the low popularity of the blockchain. Initially, the ways of its development were not as multifaceted as now. Using the blockchain only as the basis for electronic currency was an axiom that did not last like a template for a long time. However, although there were few projects, they began their formation.

The first to appear crypto wallets, mainly with a cold storage key, as well as a service for buying and selling bitcoins (exchange) Bitcoin Market. And accordingly, realizing that the cryptocurrency market should not be limited to only elections to one coin, such cryptocurrencies as Litecoin and SwiftCoin were born. And rethinking the blockchain technology and getting rid of the need for mining in 2012 (Medium.com, 2019), Ripple appeared, representing the concept of consensus among network members. At this time, the first online stores that accept bitcoin through anonymous accounts already appeared, and began to gain popularity, a larger exchange that exchanges fiat money for bitcoin - MtGox, when the cost of one Bitcoin began to be equal to about 1 dollar.

- Phase 2.0: The advent of Ethereum. Smart contracts. (2013-2015)

The beginning of this phase has left a big mark on the history of blockchain culture. First, the number of investments in bitcoin projects has increased, mainly in cryptocurrency exchanges Coinbase, Circle and Bitstamp. Secondly, the emergence of a new vision of the world of cryptocurrency and as a result, the creation of Ethereum by a young programmer, Vitalik Buterin. Ethereum is an open source blockchain that supports a modified and improved version of Nakamoto's consensus.

Ethereum provides a platform for creating decentralized applications. Buterin distinguished Ethereum from the Bitcoin blockchain by enabling a feature that allows people to record other assets, such as slogans, as well as contracts. The new feature has extended the functionality of Ethereum from cryptocurrency to a platform for developing decentralized applications.

With the advent of new blockchain technology, programming languages such as Solidity, Serpnet, etc. They support algorithms for writing smart contracts. This has accelerated the growth of new projects, allowing developers to create networks within the blockchain with their own hands and with greater speed. By this time, a stronger altcoin appears on the cryptocurrency market - XRP, developed by Ripple. Cooperation with large banks allowed this cryptocurrency to sit on the second line in the exchange index of cryptocurrencies, indisputably second only to Bitcoin. In 2014, blockchain R3 technology was formed.

The Force Consortium is also created with more than 40 legacy financial companies to implement blockchain technology. The R3 blockchain platform called Corda has a strong presence in the financial sector, which signals the success of the project. In 2015, two important events take place:

First, the American financial agency FinCEN fined Ripple Labs $ 700,000 for selling the XRP cryptocurrency without prior registration with them. This information will be useful for further acquaintance with the joint work of state banks and cryptocurrencies.

Second, the world's largest open source nonprofit, the Linux Foundation, is launching Hyperledger; a set of tools to help people create blockchain projects. This, in turn, shows us that the world is fully ready to transfer knowledge about the development of blockchain projects. In the future, such steps will develop into more global university approaches to the study of blockchain.

- Phase 3.0: Applications. (2016-2021)

One of the most famous projects working on the third generation blockchain is Cardano. The company focuses on solving 4 major problems that blockchains of the world face today: (Swan, 2017)

1. Scalability
2. Compatibility
3. Stability
4. Management

There are many other companies trying to solve the problem with the first two generations of blockchain.

Among the leading companies besides Cardano, Stellar, Zilliqa and EOS, however, even more can be found as the competition is really fierce. Cardano claims to be the 3rd generation of blockchain, solving problems with scalability and compatibility.

2018 was the year of icing, and now we are entering the year of blockchain adoption. An internet giant like AliBaba, Amazon, Google, Facebook, etc. have already started working on projects with blockchain technology. Recently, Facebook announced the launch of its own cryptocurrency. The EOS cryptocurrency is attracting $4 billion in the largest ICO ever. Many believe that in the future it will replace Ethereum due to advanced technology and high transaction speed.

According to Forbes, the world's largest annual blockchain conference in 2018 is attended by 4,000 people. Nearly 15% of financial companies today use blockchain.

2.2 Cryptocurrency as a decentralized monetary unit.

The decentralization of the blockchain ensures its stability - even if some of the nodes fail for some time, the system will still continue to function. The essence of decentralization and distribution is that each network participant has on his hard disk a complete copy of the current registry, which makes it impossible to compromise it.

When carrying out a transaction, information about itis fed to the input, and a hash is generated at the output, which is recorded in the hash amount. Thus, if at least one bitis tried to change in the block, all participants in the system (nodes) will be notified of this.

In the last paragraph, the terminology of cryptocurrency was mentioned. In this paragraph, I will look at this digital currency in more detail to understand the model of its operation. As mentioned earlier, a cryptocurrency is a set of code based on a specific blockchain technology. For example, Bitcoin, as a currency, is registered in the record log of the bitcoin blockchain. Blockchain as a chain of transaction blocks is a distributed, public and shared registry or record book containing transaction data. The journal is updated by miners and tracked by everyone, but not controlled by anyone. It is like a giant a public spreadsheet that is periodically updated and confirms the uniqueness of digital money transfer operations. (Bitcoin.org, 2021)

This algorithm shows the first, lower level of the stack of technologies necessary for the full functioning of the cryptocurrency. In total, there are three levels of the blockchain technology stack. The middle layer of the stack is a protocol – a software package that transfers funds by making transactions in the blockchain (journal of records). The third level is the scheme of the currency itself. It is important to understand that the overall structure of any modern cryptocurrency system is formed by all three levels (blockchain, protocol and currency). Each coin is both a currency and a protocol, it can have its own distributed ledger of records or use the distributed blockchain of Bitcoin. Another example: the Litecoin cryptocurrency uses the Litecoin protocol, which works with the Litecoin blockchain – in fact, it is a clone of Bitcoin, in which some functions are slightly changed. A separate blockchain means that the coin has its own decentralized ledger of records with the same structure and format as Bitcoin's distributed ledger. Other protocols, such as Counterparty, have their own currency (XCP), but use the Bitcoin blockchain, that is, XCP transactions are recorded in the distributed ledger of bitcoin records.

The main paradigm of the many current companies that own information, such as Facebook, Google or any banks, is centralization. All user data is stored on their servers.

Due to the trend of increasing the cost of information, in parallel with it, the risk of using such products increases. Blockchain and the mechanism of operation of cryptocurrency solve this problem with decentralization. However, in the decentralization model, there is an obvious question: if there is no regulatory body, how to avoid problems associated with similarity in the information flow of data?

For example, two addresses in the system ending in the same way. Cryptography theory will help answer this question. Blockchain technology has two keys, private and public. They are the main regulators of both user relations and from a technological point of view. you have a private password for conducting operations with cryptocurrency. It is unique for each user and is provided by the program. On its basis, based on the algorithms prescribed in the code of the blockchain technology, a public address is generated. It, in turn, is necessary so that you can interact with its owner. What happens at the time of sending "money" (here and in the future the word money can be used as a description of digital currency / cryptocurrency)? When making a payment, the private key is used to "sign" the transaction. In the future, this transaction is automatically sent to other accounts in the blockchain chain, which allows you to maintain full transparency in the system. In order for this process to take place according to the rules, a consensus algorithm was developed. It is used by legal cryptocurrencies.

The main algorithms are:

1. Proof of work

Proof of work is a system protection protocol. Anyone who wants to write a block to a database must perform a certain difficult-to-compute task built on the principle of a one-way function. The calculation process takes a long time, while the receiving party quickly checks the result.

The first proof-of-work system was demonstrated by Adam Beck in 1997 - it was the Hash cash system, which was used to reduce the number of spam and DoS attacks. Before sending the message, a certain mark was added to the header, which can only be confirmed by a complete redraw. Thus, some time passed before sending each message, which significantly reduced the number of messages that can be sent out during the day (hash calculations that reduces the number of people sent per day from totals to 1750). Validation of calculations on the receiving side is fast - due to a one-time calculation of SHA-1 with a pre-prepared label.

A possible proof-of-work vulnerability exists at the theoretical level - it has not yet been confirmed. In the theory of algorithms, there is a hypothesis that the time to find a solution and the time to check the truths of the solution are approximately equal, but so far this problem is not close to solving and is included in the list of seven millennium tasks.

2. Proof of Stake

Proof-of-stake is a proof-of-work protection protocol in which it is necessary to confirm as evidence the storage of a certain amount in the account. The system will select a miner with a large amount of funds on the account, while the probability of this choice does not depend on the power of its process. Therefore, the energy costs in this transaction are every minute. In order to undermine the reliability of the system, one of the participants must collect in his hands more than 50% of all the funds of the system, which is very costly.

Proof-of-stake has more advantages over proof-of-work. The main thing is lower time costs (there is no need for lengthy calculations), but this does not eliminate possible problems. There is also no evidence of effectiveness in protecting against the risks arising in cryptocurrencies.

Two of the main advantages of this protocol - an attack on the system is very expensive, and if any participant still conducts it, then he himself will suffer significantly from this, because will disrupt the stability of the system. Arguments against - the method gives motivation to accumulate funds on separate accounts, which calls into question decentralization; in the case of the formation of a small pool of participants concentrated in their hands most of the means, this group can impose its conditions of functioning system.

Proof-of-stake consensus. Only the participants with the largest share in the system take part in the creation of blocks. Active participation in the blockchain system gives the right to generate new blocks. Blocks are created on a principle close to what is valid for proof-of-work, except that hash operations occur on a limited search scope (search space), rather than a computationally demanding unlimited search scope.

The reasons for the appearance of cryptocurrency vary, and in this regard, various kinds of tokens have appeared, which, accordingly, differ in matters of economy.

1. Currencies Coin is the most popular type of cryptocurrency. They allow you to make purchase and sale operations on many services that are not involved in the blockchain infrastructure.
2. Platforms Coins are tokens tied to the platform, allowing you to develop cryptocurrency. I'll take a closer look at them in the next paragraph. The most popular such currency is Ethereum.

3. Cryptocurrency Exchanges - in-exchange tokens. They are created to help new coins get start-up investments from users of the exchange, while not exposing them to great risk. These "coins" are also liquid outside the linked exchange.
4. Utility Tokens - in fact, these are some analogues of shares. These tokens are limited in emission and are related to utility. The app to which you are bound. After the ICO, tokens continue to play the role of an investment product, which makes them model-like to shares.
5. Security Tokens are security tokens that have a certain value, depending on the overall market. They are issued during the ICO and are intended for investors. Based on these tokens, investors further divide the profits, receive dividends, etc.
6. Crypto Commodities - the term is used to describe a tradable or fungible asset associated with a specific product. The service or application offered by the service can create and integrate tokens into its product, which can be an internal currency. Such tokens are not used in markets or exchanges.
7. Stable Coins - "Stable tokens" are cryptocurrencies whose volatility is minimized due to the peg to a particular stable asset, for example, the dollar or gold.

2.3 Analysis of the technical component of cryptocurrency.

The main purpose of my research is to analyze the options for integrating cryptocurrency as a new currency into the classical banking system. And since I am considering the technological side of integration, the question of the mechanism of operation of cryptocurrency is important. At the moment, after several years of development of the industry, the process of creating a new cryptocurrency and its further support has become very simplified. There are three main levels of the blockchain technology stack, which I already mentioned in the last paragraph:

1. The main blockchain platform is the highest level, on the basis of which cryptocurrency algorithms are based.
2. The cryptocurrency protocol and client are the second layer that determines all the processes and operations that are possible on the basis of the blockchain platform.
3. Cryptocurrencies are directly the shell itself.

In fact, most cryptocurrencies can be combined into a single "family tree" and trace that many cryptocurrencies have a basic single "ancestor", which is the bitcoin blockchain. However, speaking about the simplicity of creating a new cryptocurrency, it is impossible not to mention specialized blockchain platforms that allow you to create tokens. One of the most popular such platforms, which I mentioned above, is Ethereum. The second place is occupied by the Waves platform. There are also platforms such as NEM, Nxt, EOS, KickICO and others. Each of them has its own internal algorithm that allows you to determine its uniqueness.

Just like in Waves, a token in Ethereum is a digital asset created inside the platform, with the only difference that the process of issuing a token is more complex, but at the same time more flexible.

The process of creating tokens also requires writing a smart contract. And due to the fact that the integration of this smart contract into different services, exchanges and crypto wallets is a technical process that requires automation, the question arose of minimizing the connection time due to the diverse technology stack. It was then that the Ethereum team came up with the standards used to create tokens.

Ethereum Request for Comments (ERC) is a recommendation for writing smart contracts. There are now two main standards for tokens. ERC-20 and ERC-721. The first is suitable for most solutions. ERC-20 describes all the basic needs of the parties imposed on the token, and is constantly supplemented with new rules and recommendations, which makes the work of developers of new coins simpler and more understandable. There is also a more advanced version of the standard – ERC-223, which allows you to return tokens from a smart contract sent there by mistake. It also allows you to reduce the cost of processing requests that the smart contract carries out. In fact, in the near future the ERC-20 standard will absorb all the functionality of ERC-223. The ERC-721 standard, in turn, can be used to confirm the ownership of unique handmade things, collectible values. It is also realistic to use the token as membership in a closed club, voting, confirmation of asset ownership rights.

Of course, in addition to using open source and creating a fork of a ready-made token, or creating on the basis of an integration platform, examples of which I gave above, there is another option for creating a cryptocurrency. Creating a cryptocurrency based on your own unique blockchain solution is the most difficult option, but this option is used if the project team is going to introduce a new cryptocurrency as a new major player in the market.
Also, when writing a cryptocurrency, an encryption algorithm for this cryptocurrency is added to the program code.

Algorithms are different, and I will consider the most basic of them. They are the most necessary link connecting mining with cryptocurrency: it is these algorithms that the mining equipment deciphers, while receiving as a reward. This part is included in the second level of the technology stack.

- Bitcoin uses the SHA-256 algorithm. Due to the complexity of deciphering this algorithm, standard mining methods are not able to develop the necessary power. For decryption, equipment is used - ASIC (application specific integrated circuit - integrated circuit of special purpose)
- Ethereum - DaggerHashimoto. The platform's official account describes the following principle of creation: "The benefit of creating specialized hardware for the algorithm should be as small as possible, ideally to such an extent that even in an economy where ASICs are developed, acceleration is small enough that users on ordinary computers still find it marginally profitable to extract them with spare processor power."
- Ripple (XRP cryptocurrency) - ECSDA. Used as early as 1999 by banks for a faster and more secure method of making transactions.

- DogeCoin - Scrypt. Previously, this algorithm was a great alternative when ASICs were developed only for SHA256. However, soon Scrypt-ASIC appeared, and this algorithm also became inaccessible to most miners.

From all of the above, it can be understood that a big difference in the technology stacks of cryptocurrencies can be a big problem when integrating. However, here a completely logical question arises, how are these tokens added to crypto wallets and exchanges? If we compare the process of using cryptocurrency with ordinary money in terms of technology, then the obvious conclusion is the complexity of blockchain technology before the classical structure. Based on this information, it is already possible to assume different options for integrating the crypto wallet into the banking industry, which confirms the feasibility of studying the hypothesis.

As I wrote above, the cryptocurrency market begins to be a kind of tree, the roots of which are blockchain platforms, such as bitcoin, Ethereum or waves, and the cryptocurrency acts as branches: different variants of tokens with their own innovative solutions grow from the bottom.

2.4 Technological model of crypto wallets.

Above, I looked at cryptocurrency, both from the point of view of the average user, and the main technology on which the cryptocurrency is based. Now the logically arising question arises, how to use cryptocurrency as conveniently as possible as a monetary unit. Digital money cannot simply exist without a certain service called a crypto wallet. This is either a program or an encrypted record of the user's account. The program has a user-friendly interface that combines a lot of functionality, and can be used on different digital media. The process of conducting transactions is as follows: the program connects to the blockchain network recorded in the cryptocurrency algorithm and confirms its legitimacy. Essentially, it does one of the consensus tasks, and then it enters transaction data into the ledger.

Earlier I mentioned that there are several types of crypto wallets. Now let's consider them in more detail. As you can see, an important detail in the work of the wallet is the connection with the blockchain. And one of the criteria for dividing crypto wallets into types is by the way they communicate with the blockchain system.

1. Hot wallet (hot wallet, or hot storage) - In the case of hot storage, constant communication with the system is maintained. This increases the speed of transactions, but at the same time increases the vulnerability to hacker attacks.
2. Cold wallet - Another way to integrate with the system in which there is no constant connection. In contrast to the first type, it is better protected from hacker attacks.

The next criterion I'd like to consider is the format of key storage.

1. Paper wallet - The very first and easiest way to store private keys. I'm talking about it to understand the technical possibilities, or rather the fact that you don't have to have an account in services that provide the ability to use cryptocurrency to use it. And the obvious fact of such a wallet is a cold kind of storage.
2. Software wallet - The same kind of wallet that is developing very much now, and which I have repeatedly mentioned. In a software wallet, as the author of the book "About Cryptocurrency" says, the private key is encrypted with a password on a computer or in an application, and it becomes possible to receive and send money through this application without the inconvenient import and execution function, as in offline wallets. Software wallets, like ordinary online products, can be used in three different ways:
   -an application on the computer.
   -application on your smartphone.

-web version of the application.

3. Most crypto wallets support the first two methods, and some and all three. For example, such popular crypto wallets that are recommended by the official website of Bitcoin developers, (Vigna et. all, 2017) Bither, Electrum and BitPay. I will consider some of the crypto wallets in more detail later. Software wallets come with both cold storage and hot.
4. Hardware wallets are compact gadgets, similar to a USB drive, for storing cryptocurrencies. A high degree of security is achieved due to the fact that private access keys are stored on this device in encrypted form. Several levels of protection, including a pin code, make it reliable .. The most popular hardware wallets are Ledger Nano, Trezor. (Blockchain.com, 2021) Like a paper wallet, a hardware wallet has a cold kind of data storage. Using a hardware wallet to conduct transactions involves connecting to a computer. In theory, a hardware wallet can be called a bank card in the world of cryptocurrency. It is a physical object that requires special equipment to use. However, compared to bank cards, data it is not copied or duplicated, and cannot be hacked without a direct connection to it.
5. Cryptocurrency Exchange - The exchange provides the ability to exchange various kinds of tokens, if there is technical support of course, including popular state currencies, such as Russian rubles, US dollars or European euros. The main work is carried out through the browser, without the need for additional integration of wallets. The exchange allows you to create an internal account and store data on it.

3 Research analysis and results

I looked at different variants of the crypto wallet to further understand which ones can be integrated into the banking system and in what way. In the last chapter, much attention was paid to the theory of cryptocurrency, and what technical characteristics it consists of. I mentioned encryption standards and algorithms. On crypto wallets, these parameters also have great attention.

First, the standardization of cryptocurrency allows you to highlight crypto wallets, which have only a certain range of tokens at their disposal. As an example, we can highlight the popular crypto wallet MyEtherWallet (MEW), which allows you to dispose of only the cryptocurrency of the ERC-20 standard, or rather written on the basis of the Ethereum blockchain. This fact allows me to draw the following conclusion: the technical architecture and business model of many crypto wallets differ, which leads to the allocation of unique features among them and a more customized approach to the issue of integration. If we consider the issue of introducing a crypto wallet into a bank from the point of view of a consulting project, the obvious fact is that a different integration model is suitable for different banks.

Now let's go directly to the analysis of the functionality of crypto wallets. Many of the applications have at their disposal capabilities similar to the capabilities of banking products. A simple search made it possible to find a large number of crypto wallets. I chose several of them the most popular and actively developing in order to analyze their functionality.

Above, I mentioned the difficulty of integrating the ability to work with a certain currency into a wallet, therefore, different wallets have a unique list of cryptocurrencies that they support.

Product	**Functionality**	**Platform**	**Cryptocurrency Support**
Crypterium	Purchase / Exchange Receive / Send Real-time value tracking Online payment by phone	IOS	BTC (Bitcoin) ETH (Ethereum) LTC (Litecoin) CRPT (Crypterium)
Blockchain	Receive / Send Buy / Sell / Exchange Two-factor authentication	IOS Android Web	BTC, ETH, BCH (Bitcoin cash)
Coinbase	Purchase / exchange (via exchange) Receiving / sending (via the exchange) Storage Real-time value tracking	IOS Android	BTC, BCH, ETC (Ethereum Classic), ETH, LTC + ERC-20 tokens
Trust Wallet	Purchase / Exchange Receive / Send Two-factor authentication	IOS Android	BTC + ERC-20, ERC-721 and ERC-223

The obvious fact is a fairly common set of functionalities in products, but there are several innovations in this area that I would like to talk about.

First, as you can see, companies are trying to implement two-factor authentication. The application, the idea of the main product of which is safe, improves this particular area of responsibility.

Secondly, the Crypterium product has the ability to pay online via card / phone (contactless payments - NFC technology) in places where Google / Apple pay is accepted. The payment mechanism takes place through the automatic exchange of cryptocurrency for USD (dollar) / EUR (euro). This fact allows us to draw a conclusion about the possibilities of introducing popular functionality, which has long been integrated into banking products.

This stage of the study was implemented by assessing the theoretical part of the technical component and the model of operation of individual parts of the overall product (blockchain technology; cryptocurrency; crypto wallet) and further modeling the architecture of these parts using the ArchiMate program.

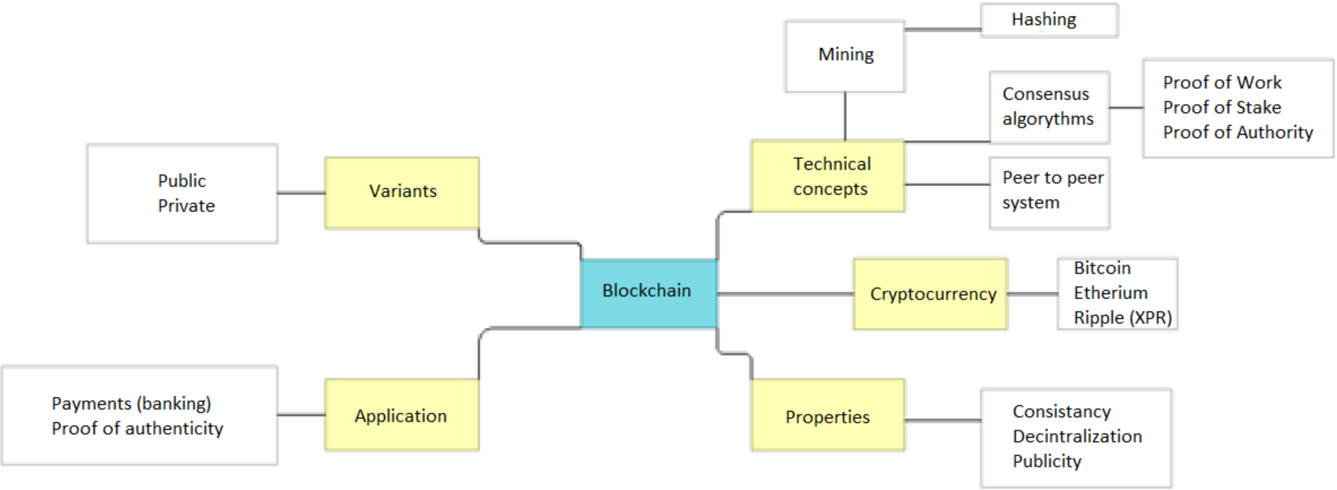

Figure 1 - General model of the blockchain

Having understood the general model of the blockchain, I created a general architecture of blockchain technology. This is the first step in the study of the architecture of the crypto wallet.

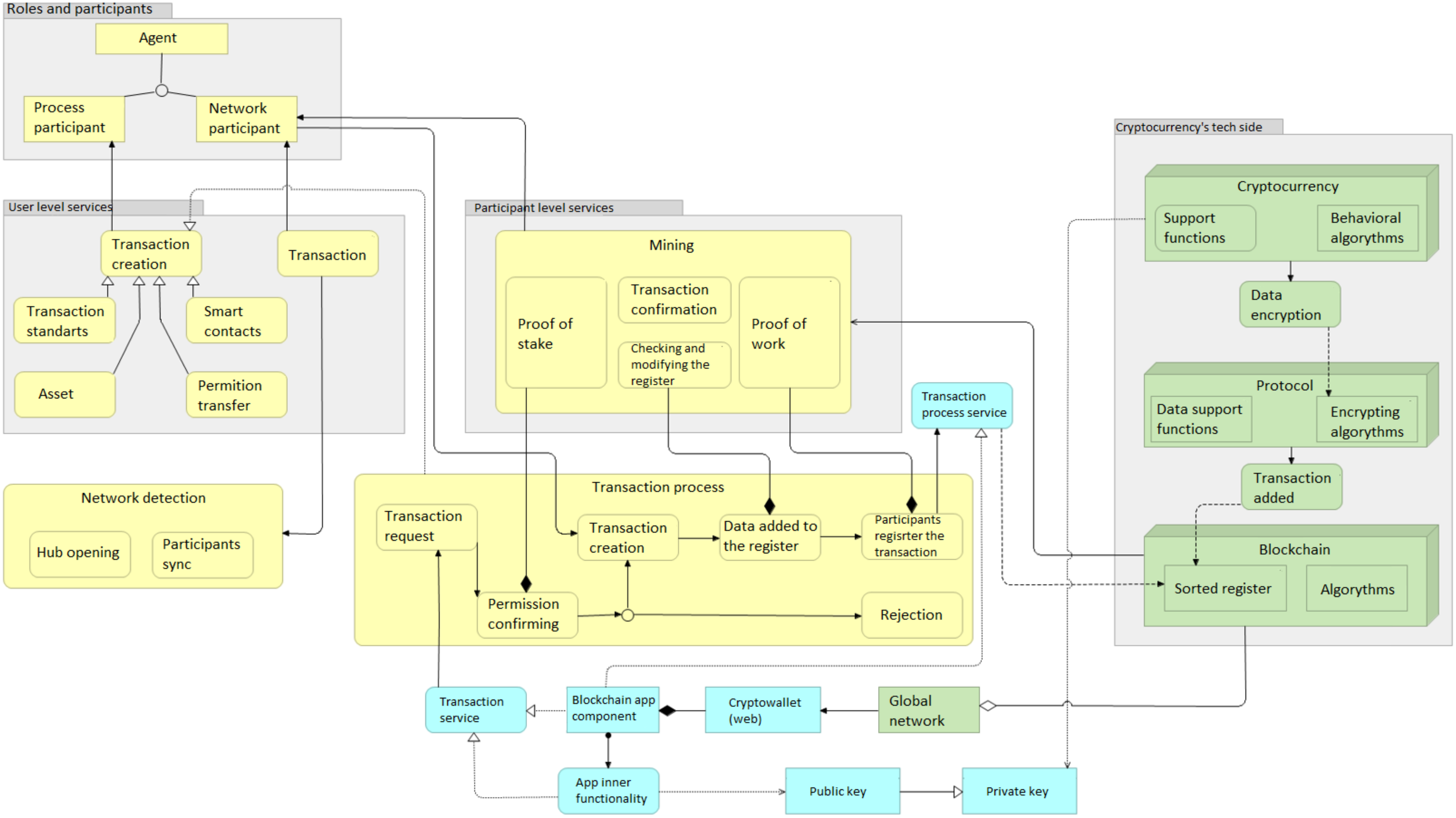
Roles and participants
Agent
Process participant
Network participant
User level services
Transaction creation
Transaction
Transaction standarts
Smart contacts
Asset
Permition transfer
Network detection
Hub opening
Participants sync
Participant level services
Mining
Proof of stake
Transaction confirmation
Checking and modifying the register
Proof of work
Transaction process service
Transaction process
Transaction request
Transaction creation
Data added to the register
Participants regisrter the transaction
Permission confirming
Rejection
Cryptocurrency's tech side
Cryptocurrency
Support functions
Behavioral algorythms
Data encryption
Protocol
Data support functions
Encrypting algorythms
Transaction added
Blockchain
Sorted register
Algorythms
Transaction service
Blockchain app component
Cryptowallet (web)
Global network
App inner functionality
Public key
Private key

Figure 2 - General architecture of the blockchain

The group "technical layer of cryptocurrency" shows the already considered three-layer model: blockchain - protocol - cryptocurrency. After researching the open-source code of crypto wallets such as "Coinbase" and "Blockchain" and "Trust Wallet", I found similarities in writing a system of connections with a common blockchain system. First, the connection is established directly, based on which cryptocurrencies the crypto wallet works with. It can be both Ethereum, Bitcoin, and other blockchains. Secondly, crypto wallets have a document with a list of cryptocurrencies and the storage of their identification number. By accessing this document, the application gains access to the common database of blockchain transactions, where it can participate as an intermediary for conducting operations.

The next stage is a detailed consideration of the architecture of the crypto wallet.

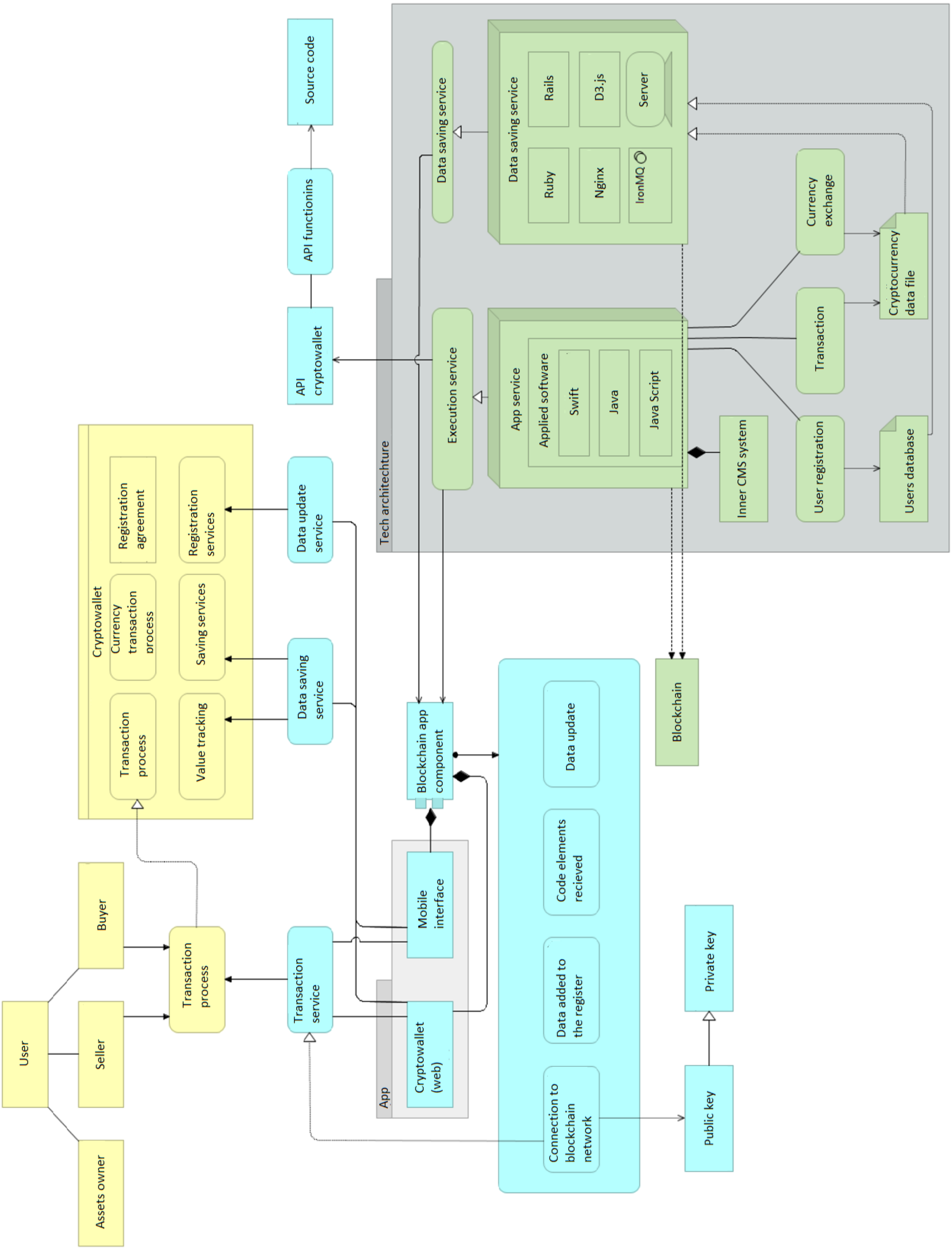

Figure 3 - Crypto wallet architecture

3.1 Business Level

In making the architecture, I only added the processes that I directly discuss in this study. I note that the processes and functions of the product are much more than presented in the model. The user of the product can act as both a buyer and a seller.

The main process on the basis of which I plan to further consider integration options is to conduct a transaction (transfer of funds from one participant to another).

3.2 Application Tier

The application layer discusses the main services (application functionality) that were identified in the last paragraph. Note that only two types of interfaces are shown here: "web application" and "mobile interface". I didn't consider the hardware wallet, because I only look at the implementation of the technology at the level of online applications, as an additional service to online banking. Another important point is the component of blockchain applications. I singled out this general structure, since this is in the longer term a way to build a large architecture of products based on blockchain technologies, which I considered in the first chapter.

3.3 Technical level

The main stack of technologies used by developers of crypto wallet applications is indicated on this chart. I want to note the importance in the use of professional databases, since this application has primarily the nature of storing information. That is why I divided the nodes (the performer of key operations in the technological layer) into two parts. The second, the application server, includes all the information on the application code that allows it to work. It also has a direct algorithm for working with the blockchain.

As I mentioned above, databases store information on connecting to the distributed registry, and an algorithm for performing this process has been developed in the application program code. This means that these two parts work interconnectedly.
In addition, I would like to note the existence of an API for connecting to the general cryptocurrency network. For example, a crypto wallet such as Blockchain has its own API, on the basis of which companies can implement their own crypto wallet product. They offer the introduction of such services as: registry data: "Requesting JSON data for blocks and transactions"; query algorithms; Web sockets, which provide real-time information about the occurrence of new transaction data in the registry to update information. This information is important because it allows you to get another additional way to introduce a new product into the banking architecture.

And the last model I'd like to consider at this point shows the most recent level in this architecture: the transaction process model.

This model shows the user's relationship to the product and its application layer. And also, in this model I have considered in more detail the process of conducting a transaction. It is executed after the event that the buyer "submitting an application to perform the transaction" implements. In fact, this is a technical transfer of currency from one account to another.

However, within this process, there are still participants, other members of the network, who at the technical level confirm the possibility of conducting a transaction. The main problem point in this process is the last two stages. I have considered in detail the internal functionality of several cryptocurrencies, and some of them require manual confirmation of the receipt of the transaction, for example, "MyEtherWallet". Or rather, the funds will not be credited to the user's account, if he does not add the data from the confirmed transaction to his wallet on his own.

3.4 Integration of crypto wallet technology into the classical banking system.

3.4.1 Technical architecture of the banking industry.

The architecture of the banking enterprise in this study will be described at the most basic level, without unnecessary additional elements. I will be referring to the diagrams I have shown earlier.

Product - online banking is the main product, which will be the main element taking in additional technical functionality. It allows you to implement the following two processes: registration and conduct of a transaction (similar to the functionality of a crypto wallet). Note that as in the models, products and business processes in the banking industry there are much more, but they are not valuable for this stage of research.

The process of conducting a transaction through a banking service is similar in technical component to blockchain technology and crypto wallet architecture. When performing the process, users have sent a request through the web interface to the bank's database, where all information about the user's account is stored. In this case, the third party confirming the possibility of performing the transaction is directly the bank.

However, the difference in this process between the two technologies in question is that the bank stores information about the user's funds directly, without additional factors. That is, there is a normal check for the difference in the cost of performing a transaction. In the blockchain, this algorithm works differently. At the technical level, it is not checked that the user has a certain amount of funds, but first of all there is a check for the existence of these funds in the common database, or rather the blockchain registry.

3.4.2 Options for the introduction of crypto wallet services into the banking system.

As I wrote above, the implementation options will vary from the requirements and business opportunities. I will try to suggest the most possible options in terms of implementation. All subsequent reflections are based on the above study of the business functions and technical requirements of both integration items.

First of all, consider the most obvious option for introducing technology into the bank's architecture: creating your own additional layer of technology that works with cryptocurrency.

There is no change in the business layer of the architecture in this integration option. Major changes will occur at the application level and the technical layer. From the user's point of view, he gets the opportunity to work with cryptocurrencies. This feature at the application level will be provided in the same way as the usual functionality of a banking product. The "online banking" application will be the main web interface in this case (without the introduction of an additional application).

The main difficulty of this implementation from the point of view of a single structure is the issue of security. The encryption algorithms of the crypto wallet and internal data are different from banking. Therefore, it will be difficult to integrate new user data into a common database. And of course, in this case, there can be no question of anonymity when using the functionality provided by blockchain technology.

And at this stage, the question arises how to add to the banking product line the possibility of using cryptocurrency without violating the "blockchain philosophy".

3.4.3 Creating a new crypto wallet

In this case, a new product is created, which is a separate part of the component of banking applications.

The algorithm for supplementing the technical layer is not much different from the previous version considered. However, a strong change is visible at the application level. The user, in comparison with the previous point, interacts with two applications. Both of them should be integrated with a single system in which general information about the user and transactions conducted through both the classical system and the blockchain is recorded.

This option allows you to use a single database of user accounts. However, it is quite complex in terms of programming a new application and is much more susceptible to external attacks.

Hence the next question arises, whether it is possible to introduce the possibility of using blockchain technology and working with cryptocurrency in another way. A method that will be essentially similar to the new crypto wallet, but at the same time be part of the component of banking applications, which allows you to connect the databases of individual applications into a single whole. This question can be answered by the mentioned functionality in the last chapter - the Crypto Wallet API.

3.4.4 Using the API

This option allows the bank to implement a ready-made boxed crypto wallet solution, changing the visual and external characteristics of the existing product. The choice of solutions presented on the market and its further implementation in the architecture will allow the bank to obtain algorithms for performing requests and working with the blockchain technology network and already integrated cryptocurrencies.

Then the main disadvantage would be the limitation in innovations. The bank will have to adapt to changes in the API of the original product and work only with those assets that are technically supported by this company. However, this allows you to get query algorithms and add already encrypted information to the database, while not violating the principles of the blockchain.

To implement this implementation, it is necessary to add an additional layer of applications at the program level in the external part, allowing users to interact with the functionality of blockchain applications. And connect it via API to the selected ready-made crypto wallet. The registration process in the service remains directly on the bank, and the user database is also not embedded in external services.

However, in this case, the bank does not have direct access to the transactions of its user, their implementation takes place just through the API. This implementation option is excellent for banks that are not major players in the market but have great user potential for implementing the technology and working with the new emerging market of crypto payments.

4 Conclusion

Conducting a study and searching for possible options for integrating crypto wallet services made it possible to identify the final version of the architecture of the banking industry, or rather its specific product "online banking".

In this research, the definition and characteristics of the blockchain were studied, the current state in the industry was studied and the feasibility of further implementation was determined. Also, the goal of the work was achieved - an analysis was carried out of whether the blockchain will increase the level of security of banking operations compared to current methods of conducting. The result is that it will increase, especially in the field of account management, servicing deposits and credit lines - and it is easier to implement everything in practice since the bank needs only its own private blockchain for this without interconnection with other banks and the Central Banks. For the corporate sector, there is no one-sided answer primarily due to the lack of regulation of smart contracts and problems in their codes.

Accordingly, the blockchain is compared according to these criteria with the current tools for performing banking operations - relational centralized databases (for storing information on deposits and loans) and SWIFT for translations.

Blockchain produces results that are superior to others in providing security.

First, due to the electronic signature, user identification is uniquely carried out - it can be compromised only by stealing the key.

Secondly, access control and shielding in the blockchain is also at a high level - the technology allows you to share roles in the system (operator, auditor, ordinary user). Thus, in order not to allow everyone to participate, for example, in confirming transactions.

Thirdly, the blockchain has a high level of cryptographic protection, since the blocks consist of hash sums, and the hash sum cannot uniquely determine the subject of the transaction and other inputs.

The fourth advantage of the blockchain is the most important compared to conventional databases and SWIFT - transactions are formed into blocks that are almost impossible to change. This allows for close-to-perfect logging, as without authorized action, no one will be able to delete transactions, which provides a high level of transparency and much easier to audit, as nothing can be hidden.

Based on the foregoing, it can be concluded that when identifying the necessary criteria, there is a different way of introducing a new technology that meets the needs. I note that I integrated the crypto wallet into the banking industry with ready-made functionality and service, which was identified as a result of theoretical research.

However, a bank that is going to use the technology can add a new structure, functionality, technology stack and other necessary parameters. The format of interaction of banking algorithms of the technical layer and the application layer with the technical side of the blockchain technology remains unchanged.

The considered implementation options offer companies a ready-made solution and an answer to the question of what additional layers of architecture need to be introduced into the banking structure. Different directions have their positive aspects and, accordingly, disadvantages. The choice of one or another option depends on the criteria of necessity set by the bank.

References

Dr Garrick Hileman, Michel Rauchs. GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY // Cambridge Centre for Alternative Finance. – M., 2017

Bitcoin.org. 2021. [online] Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 11 October 2021].

GitHub. 2021. *GitHub: Where the world builds software*. [online] Available at: <https://github.com/> [Accessed 11 October 2021].

Deloitte Insights. 2021. *Evolution of blockchain technology*. [online] Available at: <https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html> [Accessed 26 October 2021].

Mining of bitcoin and other coins, built on the PoW algorithm. [online] Available at: <https://medium.com/@muhammadnoor/a-very-brief-history-of-blockchain-technology-blockchain-history-2019-3c9f9857e085> [Accessed 26 October 2021].

Melanie Swan, Blockchain. Scheme of the new economy. – M.: Izdatelstvo Olimp-Biznes, 2017. 1-I'm the head. Blockchain: The Foundation for Cryptocurrencies

Bitcoin.org. 2021. Choose your wallet - Bitcoin. [online] Available at: <https://bitcoin.org/ru/choose-your-wallet> [Accessed 3 November 2021].

Paul Vigna, Michael Casey. The era of cryptocurrency. How Bitcoin and Blockchain Are Changing the Global Economic Order. – M.: Izdatelstvo

Mann, Ivanov and Ferber, 2017.

- Crypterium. 2021. *The Crypto Wallet with Unlimited Features | Home Page | Crypterium*. [online] Available at: <https://crypterium.com/> [Accessed 3 November 2021].

- Blockchain.com. 2021. *Blockchain.com - The Most Trusted Crypto Company*. [online] Available at: <https://www.blockchain.com/wallet> [Accessed 15 November 2021].

- 2021. [online] Available at: <https://wallet.coinbase.com/> [Accessed 18 November 2021].

- Trust Wallet. 2021. *Best Cryptocurrency Wallet | Ethereum Wallet | ERC20 Wallet | Trust Wallet*. [online] Available at: <https://trustwallet.com/> [Accessed 18 November 2021].

- Blockchain.com. 2021. *Blockchain.com Explorer | BTC | ETH | BCH*. [online] Available at: <https://www.blockchain.com/api> [Accessed 24 November 2021].

- Blockchain.com. 2021. *Blockchain.com Explorer | BTC | ETH | BCH*. [online] Available at: <https://www.blockchain.com/api/blockchain_api> [Accessed 24 November 2021].

- Blockchain.com. 2021. *Blockchain.com Explorer | BTC | ETH | BCH*. [online] Available at: <https://www.blockchain.com/api/q> [Accessed 25 November 2021].

- Blockchain.com. 2021. *Blockchain.com Explorer | BTC | ETH | BCH*. [online] Available at: <https://www.blockchain.com/api/api_websocket> [Accessed 25 November 2021].