xChainge: a platform with a simple user interface for the anonymous and decentralized exchange of assets

Albert Ibragimov, Ilya Vorobyov,
Danil Popov, Arthur Ustimov

xChainge.io
25 October 2017

Abstract

xChainge is a platform with a simple user interface for the anonymous and decentralized exchange of assets, build on the Ethereum blockchain. The platform's users can conduct simple P2P exchanges, create contracts with different terms to conduct complex transactions, and use marketplaces built on a rapid exchange platform that guarantees a transaction speed comparable to that of centralized exchanges. In addition, the platform's users can securely buy and sell real goods and services using a guarantor mechanism. All of the platform's functionality is available from a single window, using xChainge Wallet: a wallet that provides a user experience on par with that of the best mobile banking apps. It does not require verification and enables users to have full control over their funds. The xChainge team's ultimate goal is to create a global marketplace that allows assets to be rapidly exchanged for minimal fees, without the need to trust a third party at every stage of the transaction, including transaction clearing.

DISCLAIMER

THE PURPOSE OF THIS WHITE PAPER IS TO PRESENT THE XCHAINGE PROJECT TO POTENTIAL TOKEN HOLDERS IN CONNECTION WITH THE PROPOSED TOKEN LAUNCH. THE INFORMATION SET FORTH BELOW MAY NOT BE EXHAUSTIVE AND DOES NOT IMPLY ANY ELEMENTS OF A CONTRACTUAL RELATIONSHIP. ITS SOLE PURPOSE IS TO PROVIDE RELEVANT AND REASONABLE INFORMATION TO POTENTIAL TOKEN HOLDERS IN ORDER FOR THEM TO DETERMINE WHETHER TO UNDERTAKE A THOROUGH ANALYSIS OF THE COMPANY WITH THE INTENT OF ACQUIRING XCH TOKENS. NOTHING IN THIS WHITE PAPER SHALL BE DEEMED TO CONSTITUTE A PROSPECTUS OF ANY SORT OR A SOLICITATION FOR INVESTMENT, NOR DOES IT IN ANY WAY PERTAIN TO AN OFFERING OR A SOLICITATION OF AN OFFER TO BUY ANY SECURITIES IN ANY JURISDICTION. THIS DOCUMENT IS NOT COMPOSED IN ACCORDANCE WITH, AND IS NOT SUBJECT TO, LAWS OR REGULATIONS OF ANY JURISDICTION WHICH ARE DESIGNED TO PROTECT INVESTORS. CERTAIN STATEMENTS, ESTIMATES, AND FINANCIAL INFORMATION CONTAINED IN THIS WHITE PAPER CONSTITUTE FORWARD-LOOKING STATEMENTS OR INFORMATION. SUCH FORWARD-LOOKING STATEMENTS OR INFORMATION INVOLVE KNOWN AND UNKNOWN RISKS AND UNCERTAINTIES WHICH MAY CAUSE ACTUAL EVENTS OR RESULTS TO DIFFER MATERIALLY FROM THE ESTIMATES OR THE RESULTS IMPLIED OR EXPRESSED IN SUCH FORWARD-LOOKING STATEMENTS.

THIS ENGLISH LANGUAGE WHITE PAPER IS THE PRIMARY OFFICIAL SOURCE OF INFORMATION ABOUT THE XCHAINGE TOKEN LAUNCH. THE INFORMATION CONTAINED HEREIN MAY FROM TIME TO TIME BE TRANSLATED INTO OTHER LANGUAGES OR USED IN THE COURSE OF WRITTEN OR VERBAL COMMUNICATIONS WITH EXISTING AND PROSPECTIVE CUSTOMERS, PARTNERS, ETC. IN THE COURSE OF SUCH TRANSLATION OR COMMUNICATION SOME OF THE INFORMATION CONTAINED HEREIN MAY BE LOST, CORRUPTED, OR MISREPRESENTED. THE ACCURACY OF SUCH ALTERNATIVE COMMUNICATIONS CANNOT BE GUARANTEED. IN THE EVENT OF ANY CONFLICTS OR INCONSISTENCIES BETWEEN SUCH TRANSLATIONS AND COMMUNICATIONS AND THIS OFFICIAL ENGLISH LANGUAGE WHITE PAPER, THE PROVISIONS OF THIS ENGLISH LANGUAGE ORIGINAL DOCUMENT SHALL PREVAIL. XCHAINGE DOES NOT ALLOW USERS TO AVOID CAPITAL CONTROLS OF ANY KIND AND DOES NOT ALLOW THEM TO INVEST IN ANY FOREIGN ASSETS. PURCHASE OF XCH TOKENS MAY INVOLVE A HIGH DEGREE OF RISK. SEE RISK SECTION IN THE TERMS AND CONDITIONS OF TOKEN GENERATION EVENT (THE "TERMS").

BEFORE TAKING A DECISION TO PURCHASE XCH, MAKE SURE YOU ARE CAPABLE OF PROVIDING REPRESENTATIONS AND WARRANTIES SPECIFIED IN THE RESPECTIVE SECTION OF THE TERMS. THE DISTRIBUTION OF THIS DOCUMENT AND THE OFFERING AND SALE OF XCH TOKENS IN CERTAIN JURISDICTIONS MAY BE RESTRICTED BY LAW, AND THEREFORE,ANY PERSON INTO WHOSE POSSESSION THIS DOCUMENT COMES SHOULD INFORM THEMSELVES ABOUT AND OBSERVE ANY SUCH RESTRICTIONS. ANY FAILURE TO COMPLY WITH THESE RESTRICTIONS COULD RESULT IN A VIOLATION OF THE LAWS OF SUCH JURISDICTION. XCH TOKENS HAVE NOT BEEN REGISTERED UNDER THE U.S. SECURITIES ACT OF 1933 (THE "SECURITIES ACT"), OR WITH ANY SECURITIES REGULATORY AUTHORITY OF ANY STATE OR OTHER JURISDICTION OF THE UNITED STATES. XCH TOKENS SHALL NOT BE OFFERED OR SOLD TO, OR FOR THE ACCOUNT OR BENEFIT OF, A GREEN CARD HOLDER OF THE UNITED STATES OR A UNITED STATES CITIZEN OR PERMANENT RESIDENT OF THE UNITED STATES (TAX OR OTHERWISE), OR TO AN INDIVIDUAL HAVING A PRIMARY RESIDENCE OR DOMICILE IN THE UNITED STATES (TAX OR OTHERWISE), INCLUDING PUERTO RICO, THE U.S. VIRGIN ISLANDS OR ANY OTHER POSSESSION OF THE UNITED STATES. IF YOU ARE ONE OF THE FORESAID, YOU ARE NOT ELIGIBLE TO BUY XCH TOKENS IN ANY FORM AND/OR BY ANY MEANS.

XCH TOKENS SHALL NOT BE OFFERED OR SOLD TO, OR FOR THE ACCOUNT OR BENEFIT OF, A CITIZEN OR PERMANENT RESIDENT OF THE PEOPLE'S REPUBLIC OF CHINA (TAX OR OTHERWISE), OR TO AN INDIVIDUAL HAVING A PRIMARY RESIDENCE OR DOMICILE IN THE PEOPLE'S REPUBLIC OF CHINA (TAX OR OTHERWISE). IF YOU ARE ONE OF THE FORESAID, YOU ARE NOT ELIGIBLE TO BUY XCH TOKENS IN ANY FORM AND/OR BY ANY MEANS.

IT IS YOUR SOLE RESPONSIBILITY TO ENSURE THAT YOUR PARTICIPATION IN THE TOKEN SALE IS NOT PROHIBITED UNDER THE APPLICABLE LEGAL RESTRICTIONS IN YOUR COUNTRY OF RESIDENCE OR DOMICILE.

CONTENTS

1. Introduction

Decentralization is capable of producing a real revolution in the storage and exchange of assets. It allows users to maintain full control over their own funds without the need to trust a third party. A decentralized market has no national borders—within it, users from all over the world can interact.[1] Decentralization improves resistance against random errors, as well as against attacks and attempts at collusion by individual participants.[2] The removal of intermediary parties helps to significantly simplify and expedite interactions between users.[3] As a result, the storage and exchange of assets can become much more secure, straightforward, and effective.

However, at this point the development of the crypto-economy goes against the principles of decentralization in many ways. The majority of solutions for the storage of crypto-assets have significant limitations. They provide access to a very small number of cryptocurrencies and tokens, which are chosen arbitrarily, and some even store private keys and maintain full control over all funds. That said, the greatest problems occur in the exchange of crypto-assets. Currently, the focus is on centralized exchanges which maintain full control over users' assets and can block accounts or transactions at will. Most exchanges have KYC rules, which force users to trust them not only with their assets but with sensitive, personal data as well. As a result, in its current state, the cryptoeconomy not only maintains the disadvantages of the traditional, centralized financial system, but is actually inferior to it from the security standards and customer service point of view. This greatly hinders its development.

The existing partially decentralized solutions for the exchange of assets do not solve the problems described above. They do not store their users' funds, but they still have dedicated servers that are responsible for transaction clearing, which naturally become the single point of failure of the whole system. In addition, such solutions are quite complex and require significant technical knowledge of its users which makes them inaccessible to most people and prevents them from building a significant user base and creating sufficient liquidity for an efficient exchange.

The xChainge team sees the convergence of the traditional financial world and the cryptoeconomy as its mission. We are creating a solution which, in its ease of use, will not be inferior to the interfaces of modern mobile banking applications and financial services; and at the same time, it will allow users to maintain full control over their own funds in the process of storing and exchanging them, without the need to trust a third party. We believe that this decision will contribute to a significant increase in the user base for cryptoassets, as well as their use in everyday operations.

2. Market analysis

2.1. Current problems

2.1.1. Cryptoasset storage

The number of users of cryptoassets is rapidly growing. According to a study at the University of Cambridge, in Q1 2017, there were between 5.8 and 11.5 million active wallets, and between 2.9 and 5.8 million active users. The total number of addresses increases increased fourfold between 2013 and 2016.[4] In 2017, this growth rate has accelerated further. For example, the number of unique addresses in the Ethereum network has increased tenfold since the beginning of the year, reaching nearly 10 million.

At the same time, there is still a huge potential for further growth. There are more than 3.5 billion internet users in the world,[6] and more than 1.2 billion people use mobile banking services. This number may grow to 2 billion by as early as 2020.[7] However, in order for the use of cryptoassets to become more widespread, it is necessary to create new solutions for mass market consumers.

Currently, there are several ways to store one's own cryptoassets; however, these were designed primarily for early adopters, and they do not answer the needs of ordinary users of financial services, who need a simple, secure solution that doesn't require a complicated setup process or technical knowledge.

1) **A full client (e.g. Geth for ERC-20 tokens)**
   Is secure and reliable, but inconvenient and difficult to use for the average user. It can only be installed on a computer or server, and it requires a lot of disk space: when fully synchronized, Geth already takes up more than 300GB of disk space[8].Even when the “fast sync” mode is enabled, memory requirements go up to almost 25GB[9]. Other downsides include a complicated interface and lack of built-in functionality to transfer other types of assets.

2) **Thin clients**
   There is a large number of wallets that allow one to store cryptoassets and manage them using a desktop application, browser interface, or mobile application. Despite the fact that these are developed for mass market consumers, the existing solutions are nonetheless significantly inferior from a usability and functionality standpoint for users who are accustomed to mobile banking and mobile apps for transferring money. Almost all of these wallets allow users to store only a limited number of popular cryptocurrencies and tokens.[10] Additionally, the majority of these wallets don't allow users to exchange different assets. The few solutions that do offer this functionality implement it through centralized services, like ShapeShift.

3) **Centralized exchanges**
   Many users store their cryptoassets on large, centralized exchanges. The main advantage of these exchanges is the ability to quickly exchange cryptoassets

with reasonable fees. However, users must sacrifice the security of their funds, as all of these exchanges store their clients' private keys and have full control over their funds. On more than one occasion, this has led to major losses for users, as in the cases of MtGox[11], Bitfinex[12], and BTC-e[13]. Exchanges may also take a long time to verify clients, delay fund withdrawal[14], block accounts without warning[15], and share user data with third parties[16].

Despite the risks of asset lossand other disadvantages, many users continue to store their cryptoassets on centralized exchanges, since there is currently no alternative to conveniently and rapidly exchange them.

2.1.2 Exchange of cryptoassets

The number of transactions involving the exchange of cryptoassets is growing even more quickly than the number of users. Globally, it has been observed that purchases of cryptocurrency with fiat currency have increased several times over[17], while the volume of trades on cryptocurrency exchanges has increased from $100–200 million per day at the start of 2017 to $4–7 billion per day in recent months. The capitalization of cryptoassets has grown since the start of the year by nearly 10 times, exceeding $150 billion.[18]

Simultaneously, the cryptoasset market occupies only a small share of the global financial system, and is almost unnoticeable in contrast to the stock market, the total capitalization of which exceeds $60 trillion[19]; or the forex market, with a daily trading volume in excess of $5 trillion per day.[20] This is due in part to the fact that current cryptoasset exchange methods have significant shortcomings and until solutions for these are found further growth will be limited.

1) **Wallets with built-in exchange functionality**
   Only a few existing solutions, including Jaxx and Exodus, have a built-in asset exchange function; however, this functionality is provided through a third-party, centralized service. Currently, there are no solutions that combine the storage and exchange of assets in a single interface without requiring users to trust a third party.

2) **Centralized exchanges**
   Centralized exchanges allow for the rapid and convenient exchange of cryptoassets; however, as with the storage of funds, users must trust the exchange, which involves elevated risks. In addition to this, large exchanges typically offer a very limited list of cryptocurrencies and tokens for exchange. These are selected arbitrarily and exchanges may delist them at any time, either on their own initiative or under pressure from regulatory agencies. Exchange servers are also often subjected to DDoS attacks, which can result in the exchange being unavailable for many hours. Such a situation may lead to losses for users with active orders on the exchange, since they have no opportunity to change or cancel them.

3) **Partially decentralized exchanges**
   There are also partially decentralized exchanges like EtherDelta and OasisDEX, which allow one to exchange a large assortment of ERC-20 tokens

without verification or the need to entrust one's funds to a third party. Despite this, users of these exchanges are not protected against loss of funds.[21] What's more, the clearing of all transactions is still handled in a centralized manner, creating risks for the sustainable operation of these exchanges. In addition, the use of these exchanges requires some technical knowledge[22], which makes them difficult to use for most consumers. This leads to low liquidity and the inability to implement an effective exchange.

2.2. The xChainge solution

xChainge is a platform with an accessible user interface for the anonymous, decentralized exchange of assets. xChainge allows users to securely and anonymously store any ERC-20 token and conduct P2P on-chain exchanges without middlemen. A key focus of the xChainge team is the creation of a secure, yet simple and convenient solution with an intuitive interface, available on all key platforms (Windows, OS X, iOS, and Android).

In addition, additional functionality is planned for the xChainge platform, which will gradually broaden the platform's capabilities and create a full ecosystem of services, all available from one window:

- A Smart Contract builder, which will allow users to execute complex transactions with a variety of additional conditions, as well as execution prices.
- Platform-based creation of marketplaces for P2P purchases and sales of cryptocurrencies and real-world goods, with the use of a guarantor mechanism.
- Platform-based creation of marketplaces to allow the rapid exchange of tokens between users, in a manner comparable to that of centralized exchanges, while maintaining control of one's own funds.
- The creation of a unified trading system, within which the rapid and decentralized exchange of all orders and transactions will be implemented using distributed processing tokens, without the need to trust a third party at any stage of the transaction.

3. xChainge Wallet

The xChainge Wallet is a central component of the xChainge platform. Users' digital assets are stored within the wallet. Through the single-window interface, all payments and exchange operations can be conducted. Our goal is to make xChainge Wallet a payment center that users will use to conduct everyday transactions with tokens, as well as with other assets in the future.

Key features of the xChainge Wallet:

1) **Security**
   Private keys for users of xChainge Wallet are created and stored on a local device, and are never transferred to any external server. Users maintain complete control over their funds without the need to trust a third party.

2) **Anonymity**
   xChainge Wallet doesn't require users to identify themselves or verify any data. This eliminates discrimination of users and the risk of their personal data being leaked.

3) **Convenience**
   xChainge Wallet will be available for all major platforms (iOS, Android, Windows, and OS X), and will be translated to the most popular languages (see the "Roadmap" section). The xChainge Wallet team focuses heavily on user experience and strives to create a product that is intuitive and straightforward for all users. The team's accomplishments and relevant skills are listed in the "User experience" section.

4) **Availability**
   xChainge Wallet will not charge users a fee for any transfers neither involving ETH, nor any of the ERC-20 tokens.. The only expenses the user will face will be Ethereum network transaction fees. Installing the wallet to store cryptoassets is, naturally, free of charge.

4. P2P exchange platforms

4.1. xChainge on-chain P2P platform

The xChainge on-chain P2P platform will allow users of xChainge Wallet to conduct on-chain exchanges of any ERC-20 tokens directly from the wallet. This P2P exchange format is most relevant for one-time transactions with less liquid tokens that aren't available on popular exchanges, and whose prices are not subject to drastic fluctuations. It can also be used for large, one-time exchange transactions between ETH and popular tokens. xChainge does not charge for P2P exchanges, but users incur a small Ethereum network fee for the processing of the transaction.

To perform an exchange, a user can either submit the order and wait for it to be filled by another participant, or choose an already published offer and conduct the transaction immediately. To publish an order, the user navigates to the P2P exchange portion of xChainge Wallet and selects the option to create an order. Then, the user selects the two assets to be exchanged, enters a desired price, chooses how long the order will be valid, and confirms the input parameters. After this, the order is published in the Ethereum blockchain, making it available to other participants for viewing and responding. To publish an order, as well as to recall it or change its parameters, the user pays a small Ethereum network fee. In order to understand what price to assign to an order, the user can select a quote from one of the major exchanges right in the xChainge Wallet interface. These quotes are displayed as a real-time indicator.

If the user wishes to conduct their transaction based on existing offers, they can also navigate to the P2P exchange portion of xChainge Wallet to view the list of existing offers. Users can filter the offers by selecting tokens they're interested in, as well as setting price and transaction volume restrictions. If one of these options is satisfactory, users can confirm the order and the transaction will be carried out. Its results are published in the Ethereum blockchain. The user pays a small Ethereum network fee for the confirmation of the order.

4.2. Smart contract builder

The smart contract constructor allows for a significant expansion in the functionality of P2P exchanges within the xChainge platform by providing the possibility to create transactions with different terms. With it, users can perform complex transactions. In addition to a price, these transactions can have additional conditions, such as execution time or the consideration of the value of assets that do not participate in the transaction directly. The smart contract constructor will be presented in the form of standard templates. Users need only fill in the required fields and confirm the transaction, without needing any technical knowledge.

4.3. xChainge cross-chain P2P platform

Using the xChainge cross-chain P2P platform, xChainge Wallet users will be able to exchange ETH and ERC-20 tokens for any other cryptocurrencies. Currently, there are no technical solutions that allow such exchanges to be conducted without having to trust the other party. To resolve possible disputes that can arise while conducting exchanges

on the xChainge platform, the mechanism of arbiters is introduced. Arbiters are xChainge users who receive compensation in the form of xChainge tokens (XCH) from the parties in a transaction for resolving conflicts that arise. For transactions using the xChainge cross-chain P2P platform, users must have sufficient balances of XCH in their wallets to pay for the arbiter's services. Arbiters must also maintain an XCH balance in their wallets, which serves as insurance to prevent abuse on their part.

If a user wants to conduct a cross-chain exchange, like selling ETH from one's own xChainge Wallet for BTC, the user first navigates to the appropriate section of the wallet, chooses the two currencies to be exchanged, sets filters for the price and volume of the transaction, and receives a list of offers from other participants. If the user finds a suitable offer, they can respond to it.

If the user doesn't find a suitable offer, they can create their own order. To do this, the user fills out a simple form within the xChainge Wallet interface, specifying the desired exchange parameters, choosing how long the offer will remain valid, and confirming it. As a result, an order is created and recorded in the Ethereum blockchain. It becomes available to other users. The order remains active until another user responds to it or the specified date and time of expiry are reached. The user can also cancel the order before it expires.

Both parties to a transaction can suggest a particular arbiter for the transaction, or use a random search option. If one party agrees to the proffered arbiter, that arbiter is assigned to the transaction. If the parties reject each other's proposals for an arbiter, the arbiter will be chosen randomly. After selecting an arbiter, an amount of XCH tokens corresponding to the arbiter's fee will be frozen in both parties' wallets. The arbiter will be rewarded in XCH tokens. Arbiters may choose their own payment terms, either as a fixed quantity of XCH tokens or a percentage of the transaction volume with a minimum XCH value.

After an arbiter is assigned to a transaction, a temporary 2-of-3 multisignature wallet is created automatically in the xChainge Wallet interface, to which ETH is debited from the account of the user who wishes to sell ETH and buy BTC. The signatures of either both parties or one party and the arbiter are required for the ETH to be transferred into the new wallet. After the ETH is locked in the new 2-of-3 multisignature wallet, the transaction participants agree on a transaction with the other cryptocurrency, which is BTC in this case. Communication between the parties to the transaction can be carried out in any convenient means, through external channels. In particular, the recipient of BTC must provide the address to which BTC will be transferred. After receiving the agreed-upon amount of BTC in accordance with the negotiated terms, the user confirms the withdrawal of ETH from the intermediate wallet on account of the second participant in the transaction, upon which it is terminated. In this case, the arbiter is not involved in the transaction and receives no compensation. The XCH tokens that were locked in both parties' wallets become available once again. For such a transaction, users pay only the Ethereum network fee and the Bitcoin transaction fee that are necessary for the transaction to be completed.

If, during the process of a transaction, a dispute arises between users that they cannot themselves resolve, either user may enlist the services of the arbiter. The arbiter requests information from both parties. On the basis of this information, the arbiter can

decide to return the ETH from the intermediate 2-of-3 multisignature wallet to its original owner, or transfer it to the second party to the transaction. Communication with the arbiter may take place in any manner convenient to the transaction parties and the arbiter. When the arbiter intervenes in the process of an exchange, they receive compensation for their services. The arbiter's fee will be taken from the party who violated the terms of the transaction.

A scenario is possible in which the arbiter abuses their position and colludes with one of the parties, or is insufficiently qualified and makes a bad decision. For such cases, there is a second-level arbitration mechanism. Either party to the transaction may appeal the arbiter's decision within 24 hours after the transaction is completed. To do so, they must deposit a quantity of XCH (fixed for such cases) which is sufficient to pay for the services of three arbiters chosen at random. These arbiters will consider the arguments submitted by the user, and, if necessary, the decisions made by the arbiter and the other party to the transaction. Second-level arbitration decisions are decided by majority vote and are final. They may not be appealed. If second-level arbitration upholds the initial arbiter's decision, the user who submitted an unfounded protest bears the cost of the arbiters' services. If second-level arbitration upholds the user's protest, the cost of compensation for the user's losses and payment for the arbiters' services is borne by the original arbiter, who will be forbidden to act as an arbiter in the future.

In the future, as a result of developments in cross-chain exchange technology, we expect that direct P2P exchanges between participants will be possible without the participation of arbiters. In the development of this functionality, technical solutions in the final stages of development may be used, such as Raiden Network and Token Swap. As soon as such a solution appears, we plan to implement its functionality in xChainge Wallet, allowing cross-chain exchanges between users to take place directly, without the involvement of guarantors.

4.4. xChainge offline P2P platform

The xChainge offline P2P platform will give xChainge Wallet users the opportunity to buy and sell goods and services with ETH or any ETC-20 token as a means of payment. Online shops can create an xChainge Wallet and install a website extension to allow customers to choose xChainge as a payment method.

To resolve possible disputes in the exchange process, xChainge will introduce a decentralized arbitration mechanism similar to that described above for cross-chain exchanges. However, with the offline exchange, there is an additional complication. Unlike cross-chain exchanges, where information about all transactions can be easily checked to arrive at a definite verdict in the event of a dispute, resolving offline exchange disputes is significantly more complicated. For example, goods may be delivered, but the recipient may claim the goods are fake, while the sender insists that the goods fully meet the description set out in the original offer.

For such situations, the xChainge offline P2P platform includes an additional type of guarantor: a notary. By mutual consent of the parties, they may avail themselves of a notary's services after allocating the necessary quantity of XCH to pay for the service. As in the case of an arbiter, the parties may choose a particular notary, or one may be

selected randomly. The notary can offer a broad range of services, such as confirmation of the existence or authenticity of a product, the fact that a particular operation has been performed, and so on. As the format in which the notary's services are provided cannot be standardized, any price can be set for such services. The notary fees can be divided between users in any way agreed upon in advance. In addition, for every such transaction, the notary must confirm their agreement to act in that role. The notary must also deposit a sufficient quantity of XCH tokens to cover arbitration fees, should this be necessary. Upon confirmation of the notary's involvement in a transaction, a record is created in the Ethereum block chain with a description of all relevant agreements. An intermediate 2-of-4 or 3-of-5 multisignature wallet is created, if confirmation is required by both parties to the transaction. The right of signature for the wallet is held by the parties to the transaction, the notary, and the arbiter (two signatures, in the case of 3-of-5).

The notary agrees in advance with the parties to the transaction concerning the format of any work to be performed. After the service has been rendered, the notary sends a payment request. The request may be agreed to by one or both parties to the transaction, depending on the initial agreements. If a dispute arises between the parties to the transaction and the notary, a decision will be made by the arbiter. The arbiter's decision is final and not subject to appeal. The cost of payment for the arbiter's services will be borne by the party against whom the arbiter's decision was made. If the parties to the transaction are not satisfied with the notary's services, they may appoint a new one by mutual consent, having re-agreed on all terms.

Another difference between offline transactions and cross-chain exchanges is the format of orders for buying and selling goods. It can contain a large amount of information, including characteristics of the goods, as well as graphics, video, and audio files. Recording such a volume of information in the Ethereum blockchain may be impractical or impossible. With this in mind, it will be possible to create requests using IPFS or similar solutions that allow for the distributed storage of large quantities of data. The order itself will not contain all the information about the product; instead, it will contain the hash from a file in distributed storage.

5. Marketplaces for rapid token exchange

P2P-based exchanging of tokens, as described under item 4.1, has natural limitations that occur in any on-chain operations. These are primarily expressed in the form of restricted transaction speeds and liquidity. In order to provide users with the ability to rapidly exchange any ERC-20 tokens, the xChainge platform will introduce centralized clearing nodes (Matchers' nodes). Existing technical solutions—the 0x Protocol, in particular—will be used for prototyping this functionality.

Matcher's nodes are trading platforms that can produce rapid off-chain exchanges of all ERC-20 tokens using the technology of state channels. When a channel is opened with a Matcher's node, the user reserves tokens in their own wallet with which they plan to make transactions. The user also pays a small Ethereum network fee. After that, the user can send the Matcher's node requests to purchase or sell tokens, or to fill requests submitted by other users. The Matcher's node has a direct channel to all connected users, allowing for rapid exchanges between participants to take place. At the same time, the Matcher's node does not have access to the users' funds, ensuring the security of transactions between those users.

A Matcher's node charges a commission in XCH tokens for every transaction processed through it. Each node may determine the amount of this fee independently. We predict that as a result of competition between Matcher's nodes, these fees will be no greater than those charged by existing centralized exchanges. We also plan to create an xChainge API to create opportunities for arbitration between different platforms, helping to create high liquidity. This will contribute to an influx of users from centralized exchanges that provide comparable services in terms of trading conditions, while now being able to maintain full control over their own funds.

The user may at any time sever the channel with the Matcher's node, upon which the user's initial token balance that was reserved when opening the channel will be recalculated according to the results of transactions that were conducted while connected to the node. As with opening a channel, closing it carries a small Ethereum network fee. A user can be simultaneously connected to any number of Matcher's nodes, but a separate reserve is required to open each channel.

Connections and other operations with Matcher's nodes will take place through the xChainge Wallet interface. After navigating to the appropriate section, the user can choose the pair of cryptocurrencies to be exchanged and filter nodes based on their commissions, liquidity, availability, and the size of the XCH deposit, which demonstrates its reliability. The interface and trading functionality will be developed by xChainge, and will be the same for all marketplaces, improving the user experience. From an interface point of view, the marketplaces will resemble traditional, centralized exchanges, with the order books and graphs that users are already familiar with.

6. Innovative open token exchange protocol

6.1. Prerequisites for the development of a new protocol

The xChainge team's global goal is to create a protocol that will allow for fast, affordable transactions without needing to trust a third party at any stage of a transaction. For this, several conditions must exist simultaneously:

1) Users must maintain control over their funds at all times while conducting operations.
2) The exchange of assets must take place without the involvement of intermediaries.
3) Transaction processing must be distributed and have no single point of failure.
4) Transaction processing must be resistant against collusion and fraud from processing nodes.
5) The system must process a volume of transactions per unit time in a manner on par with existing centralized solutions.
6) Transaction processing overhead should be negligible, for any lot size.

At the time of writing, there are no solutions that meet all of the following criteria:

#	Criteria	Centralized exchanges (e.g. Poloniex)	Current DEX (e.g. EtherDelta)	On-chain exchange (e.g. Ethereum)	Off-chain protocols (e.g. 0x)	Simple peer-to-peer network
1	Security of funds	No	Yes	Yes	Yes	Yes
2	Exchange without intermediaries	No	Yes	Yes	Yes	Yes
3	Distributed clearing	No	No	Yes	No	Yes
4	Resistance against node collusion and fraud	No	No	Yes	No	No
5	Rapid transactions	Yes	No	No	No	Yes
6	Affordable transactions	Yes	No	No	No	Yes

Thus, none of the existing solutions can be used effectively to meet our ultimate goal. For this reason, the xChainge team is planning to create a custom protocol that will meet all of these criteria.

6.2. The Ariadna Network

xChainge team plan to develop “The Ariadna Network”. It is a hybrid, distributed network of simple computational nodes with different technical characteristics. The powers of an individual node at any given time depend on a set of measured parameters. The Ariadna Network is built on a proprietary blockchain. Within the Ariadna Network, nodes receive remuneration in the form of fees paid by users for conducting transactions.

Nodes in the Ariadna Network can be any personal computer or server with the network server software installed. All nodes have equal authority.

Authority is periodically transferred from one node to another based on the following parameters:

- Time
- Availability
- Historical availability
- Capacity (computational speed)

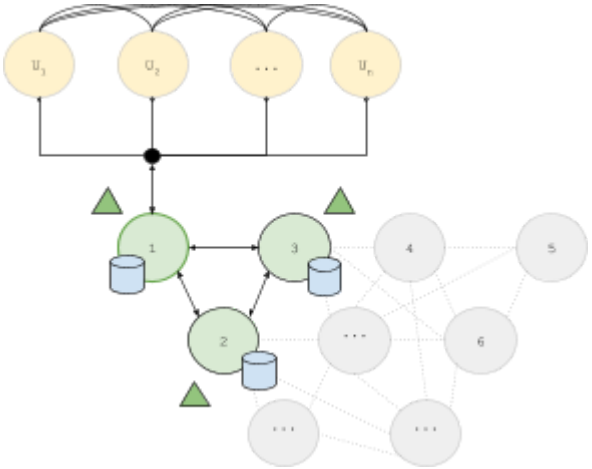
This distribution of powers takes place with the help of a pseudorandom cryptographic method for selecting nodes, eliminating the possibility of predicting the outcome of the process regardless of what actions the nodes themselves do or do not take. This excludes the possibility of influencing the network through collusion among nodes, so long as no more than 50% of the network's processing power is amassed as a result of the collusion.

#	Enumeration of powers	Task	Number of authoritative nodes at a given time	Selection criteria
1	Master node (Input/Output channel)	Acceptance of incoming requests, distribution of computations to computing nodes, computation, transmission of results to requesters, comparison of results	== 1	- Time - Availability - Historical availability - Capacity (computational speed)
2	Computing node	Acceptance of requests from the master node, calculation and comparison of results	≥ 2	- Time - Availability - Historical availability - Capacity (computational speed)
3	Authority transfer manager	Transfer of authority between nodes	≥ 3	- Availability - Historical availability
4	Index Holder	Storage of network operation history	∞	All free nodes

6.3. Proof-of-snitch computation testing method

General algorithm

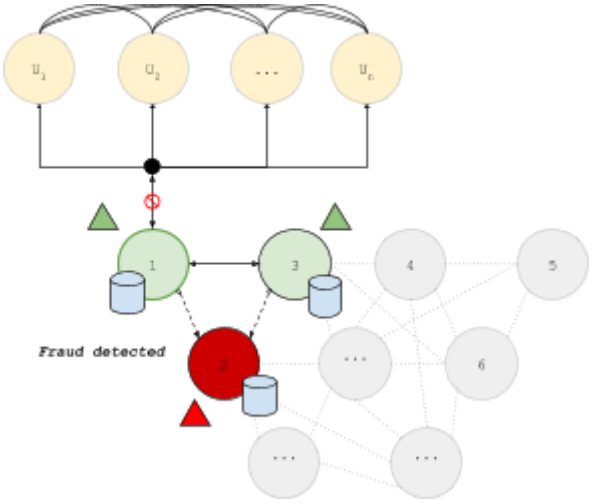
1. Node #1 at time t_0 is the master node, and acts as a gateway for entry of data into the network from nodes U_1 to U_n; that is, the network's users.
2. #1 receives requests, passes them on to subordinate nodes, and begins the calculation.
3. The calculation results are compared between nodes in a round-robin format (every node with every other node).
4. If the same result is obtained by all nodes, the result will be transmitted to the network.

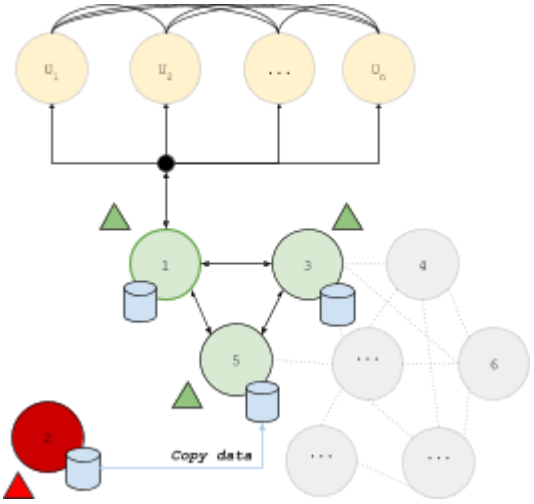


If a single node computes an incorrect result

5. If the result at node #2 is incorrect, it will be removed from the iteration. The correct result from nodes #1 and #3 is transferred to the network; thus, these nodes act as a "snitch" with respect to node #2. After excluding node #2, node #3 connects to the group and receives the calculation history of nodes #1, #3, and #2.

6. To avoid fraud on the part of two affiliated nodes, which could last indefinitely, a "majority check" is used.

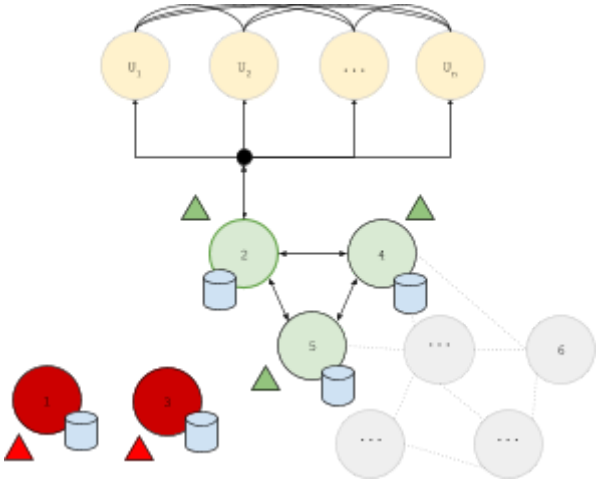


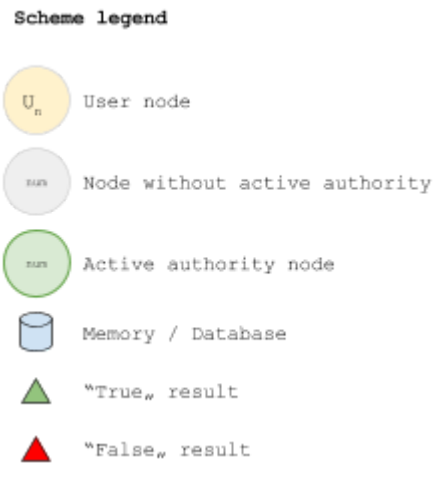


Majority check

7. If nodes #1 and #3, for the duration of their authority, have eliminated more than three nodes, a majority check is executed.

8. Excluded nodes #2, #4, and #5 verify their calculations against the previous requests; should their results be correct, these nodes replace nodes #1 and #3.





7. Target audience and user stories

7.1. Mass market consumers: storage, payments, and transfers

The main target audience of the xChainge platform is people without significant technical skills who are looking for a simple, convenient, and secure solution to store tokens and conduct transactions with them—first and foremost, payments and transfers to other users. Generally, they don't perform these operations very frequently, and they would be limited primarily to ETH and the most popular tokens.

7.2. Owners of illiquid tokens: storage and exchange within the system

A large portion of the existing tokens are not listed on major exchanges, so their liquidity is very limited. These may be tokens from projects that only recently conducted crowdsales and have not yet had time to negotiate with exchanges for the tokens to be listed, or tokens that were delisted from exchanges for one reason or another. xChainge gives owners of such tokens the ability to securely store them and exchange them within the platform for other assets, if needed.

7.3. Guarantor transactions: arbiters and notaries

The guarantor mechanism used for cross-chain and offline exchanges will attract more users to the platform and encourage greater involvement from existing users, since it will provide an opportunity to earn additional income in exchange for services that maintain the platform's operation.

7.4. Marketplace creators: access to a wide user base to receive commission-based income

For marketplace creators, with the help of Matcher's nodes, the xChainge platform will provide access to a wide base of users wishing to exchange their tokens. In addition, no significant investment in the creation of technical solutions is required on their part because xChainge already provides a platform that works out of the box, with a convenient interface.

7.5. Traders: using the platform for trading

The Matcher's node functionality opens up big opportunities for traders, who will have the opportunity to conduct rapid, frequent trades with reasonable commissions. They can also use the xChainge API to conduct arbitrary operations, while still maintaining full control over their own funds. We expect this to lead to a significant influx of traders from centralized exchanges to our platform.

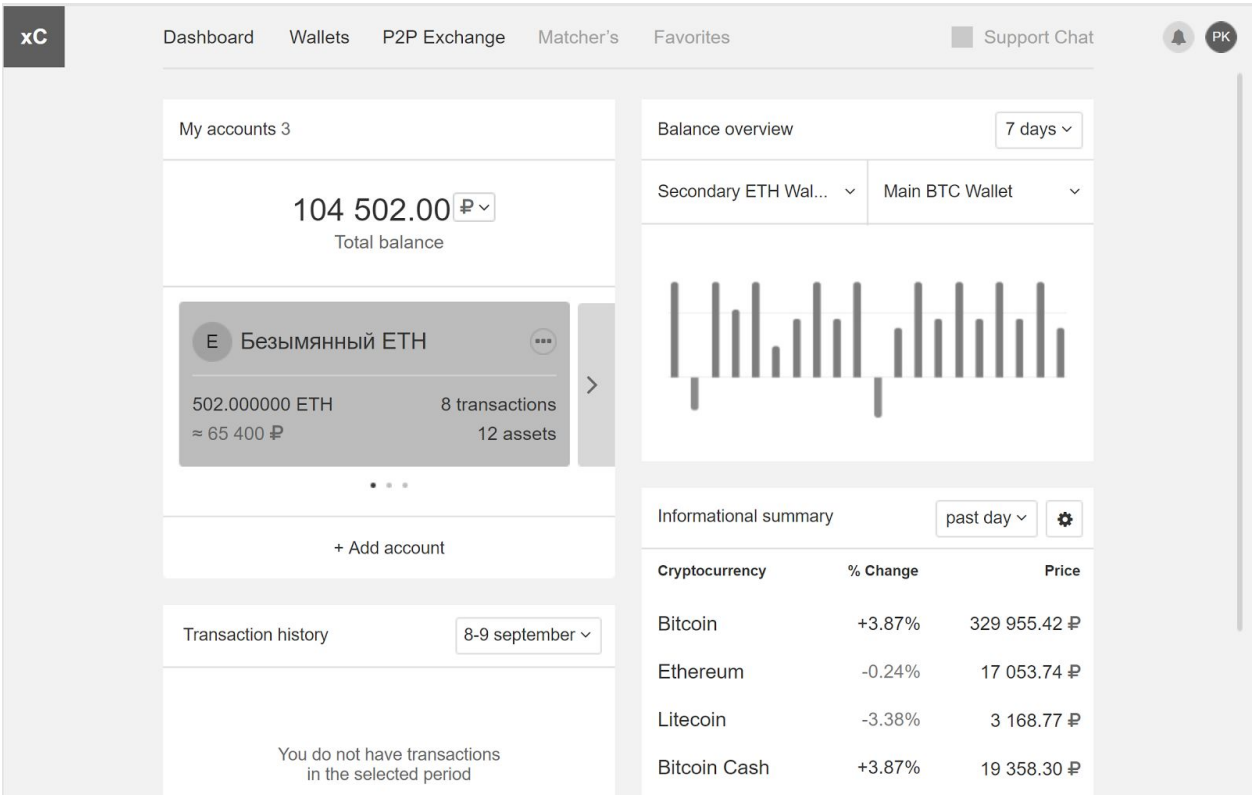
8. User experience

One of xChainge's key priorities is the creation of a maximally convenient and straightforward interface, in order to make the process of storing and conducting transactions with tokens accessible to any user. In this section, we present our work in creating such an interface.

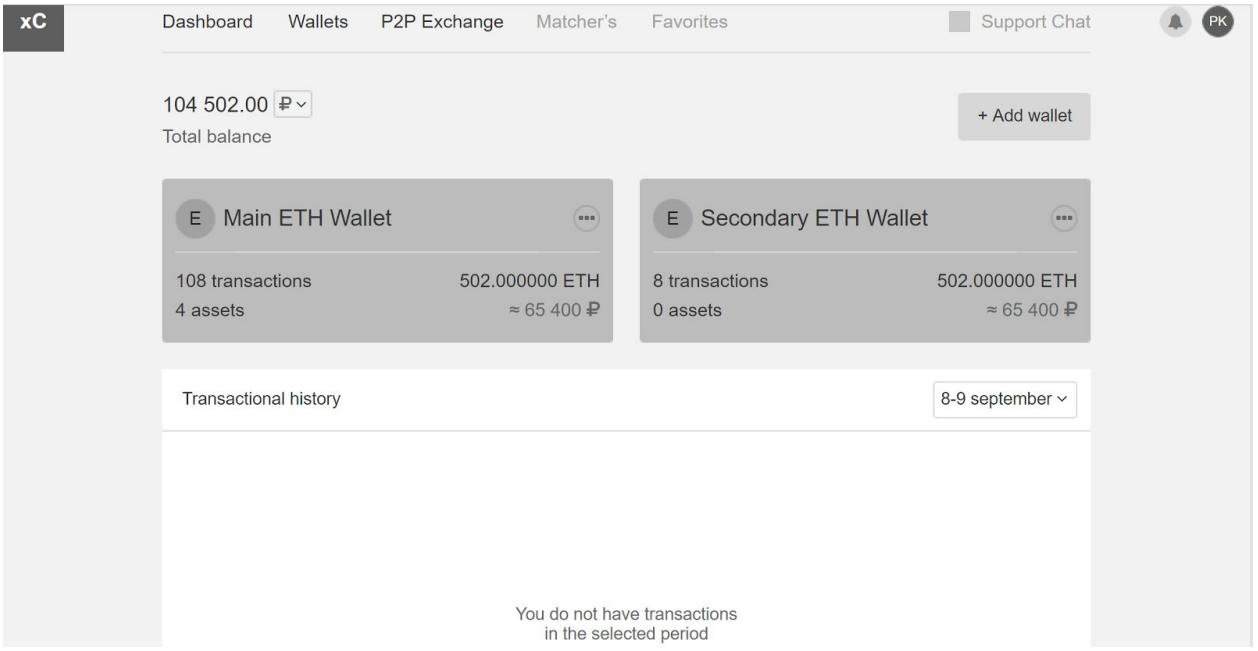
Below is a **prototype** of the interface, reflecting our vision in terms of functionality and a general visualization of the solution in development. The **prototype presented here is in no way a standalone or independent design project**; rather, it serves as a fundamental basis for creating a design in the near future.

8.1. The xChainge Wallet interface

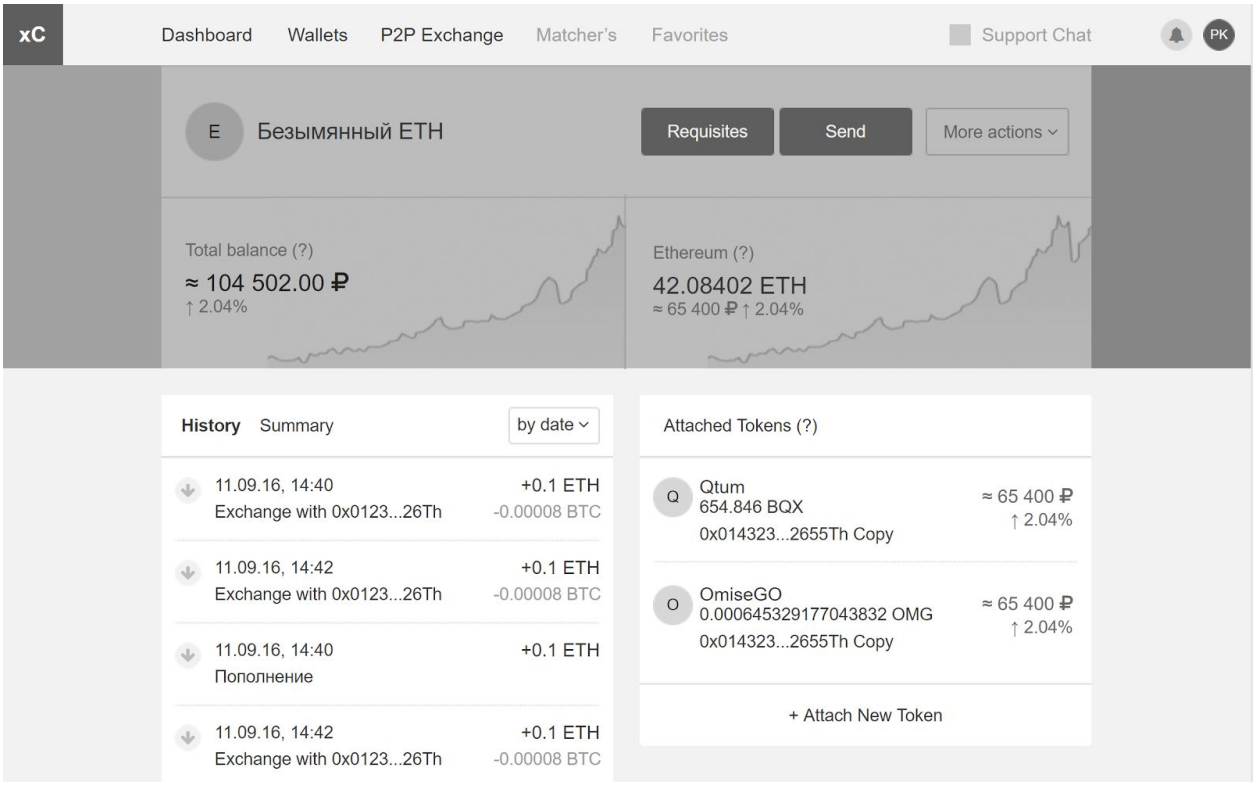
Upon entering the wallet, the user is presented with the Dashboard, which aggregates basic information about the user's accounts, changes in them, recent transactions, and exchange rates for major cryptoassets. The menu allows the user to quickly navigate between sections of the wallet to conduct various operations.



The Wallets tab provides the user with more detailed information about their wallets, as well as allowing the user to perform further actions with them. The user can create as many accounts as they wish, to use for various transactions. The creation of a new account occurs instantly upon selecting the corresponding option. Users can assign names to their accounts in order to make navigating between them easier.

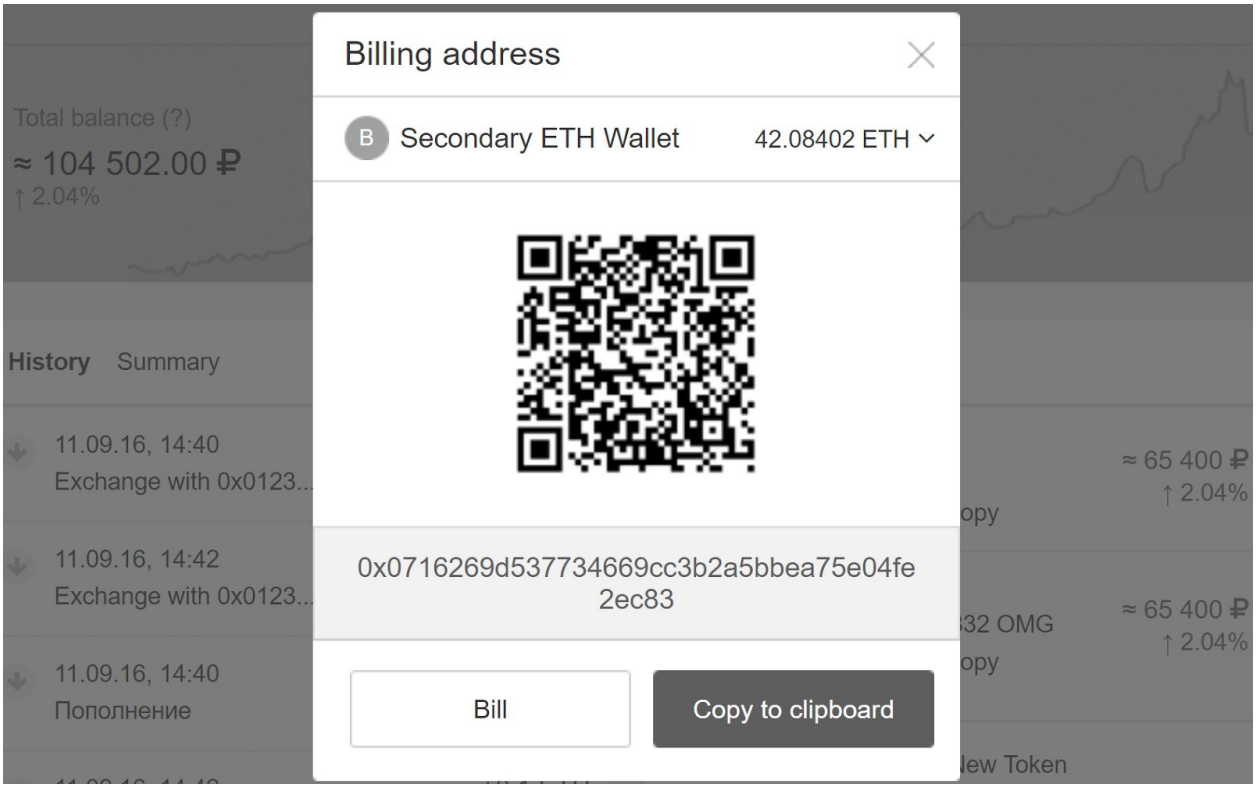


For each account, more detailed analytics are available, including a complete list of conducted transactions, currently held assets, and other information. Accounts can be topped up or used for payments and transfers.



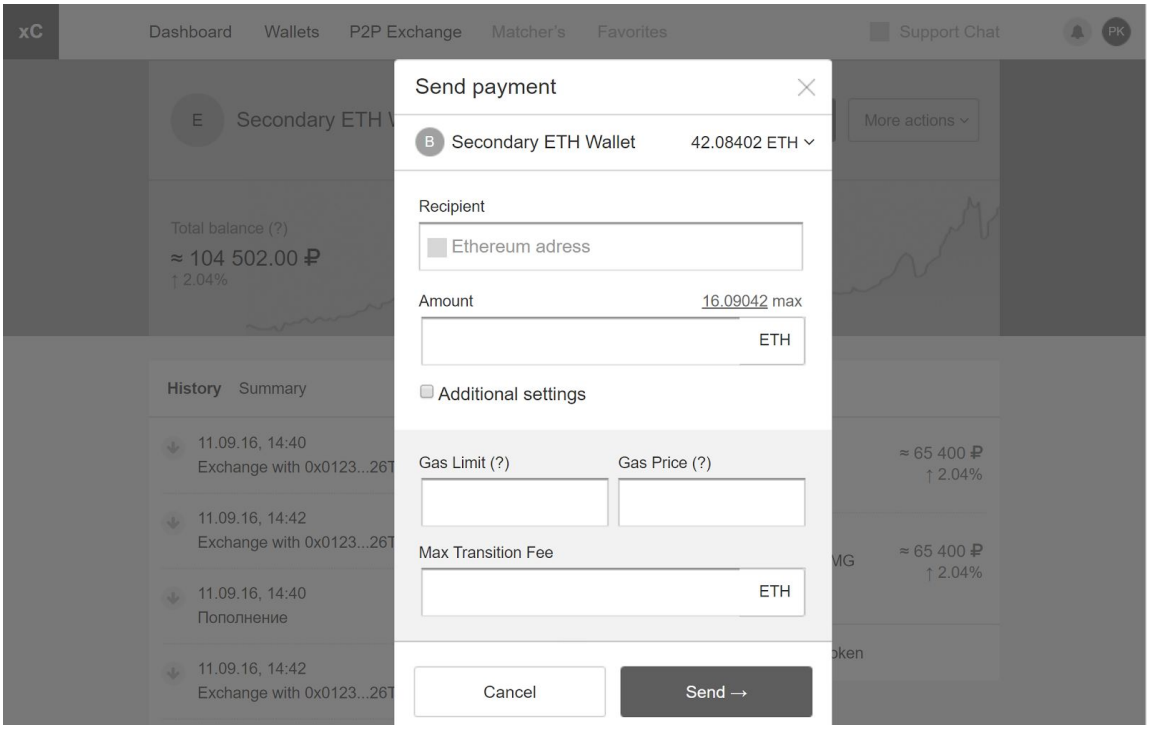
8.2. Replenishment, payments, and transfers

To replenish a wallet, the user can select which account is to receive funds and then replenish it from an external wallet using its address or QR code, or by sending its address to another user.



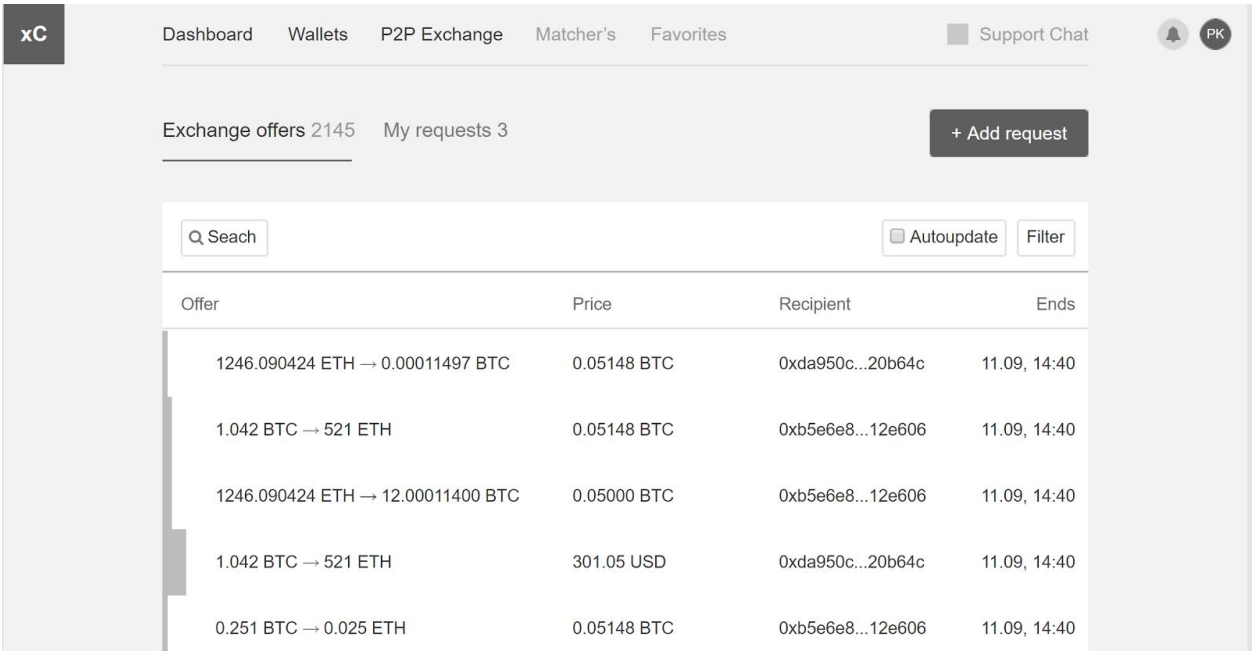
When making a transfer or payment, the user can also select the account from which the amount will be debited, as well as specifying the recipient and the amount. The Gas Limit, Gas Price, and Max Transaction Fee parameters can be left at their defaults or selected manually.

If the user makes frequent payments or transfers to a particular address, it can be entered into the address book and assigned a name. Later, the user can quickly select it as a recipient when conducting transactions, without the need to search for and verify the recipient's wallet address every time.

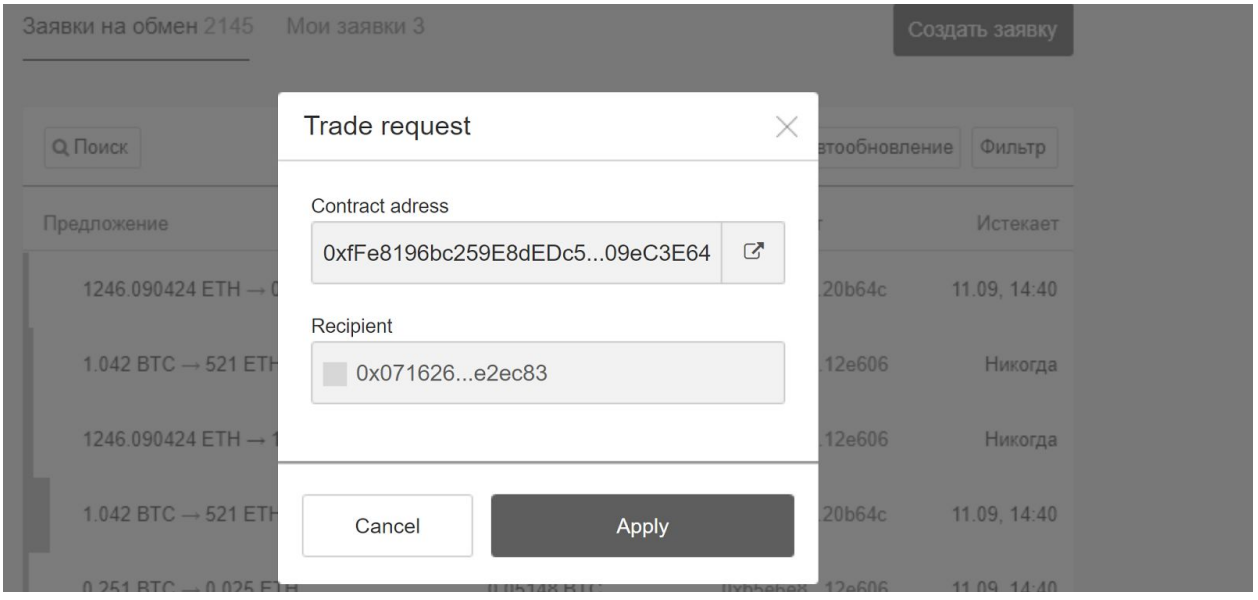


8.3. P2P asset exchange

For P2P asset exchange, users can navigate to the corresponding section, where available offers from other participants are displayed directly. These offers can be filtered by selecting a pair of assets to exchange, a price range, and a transaction volume.

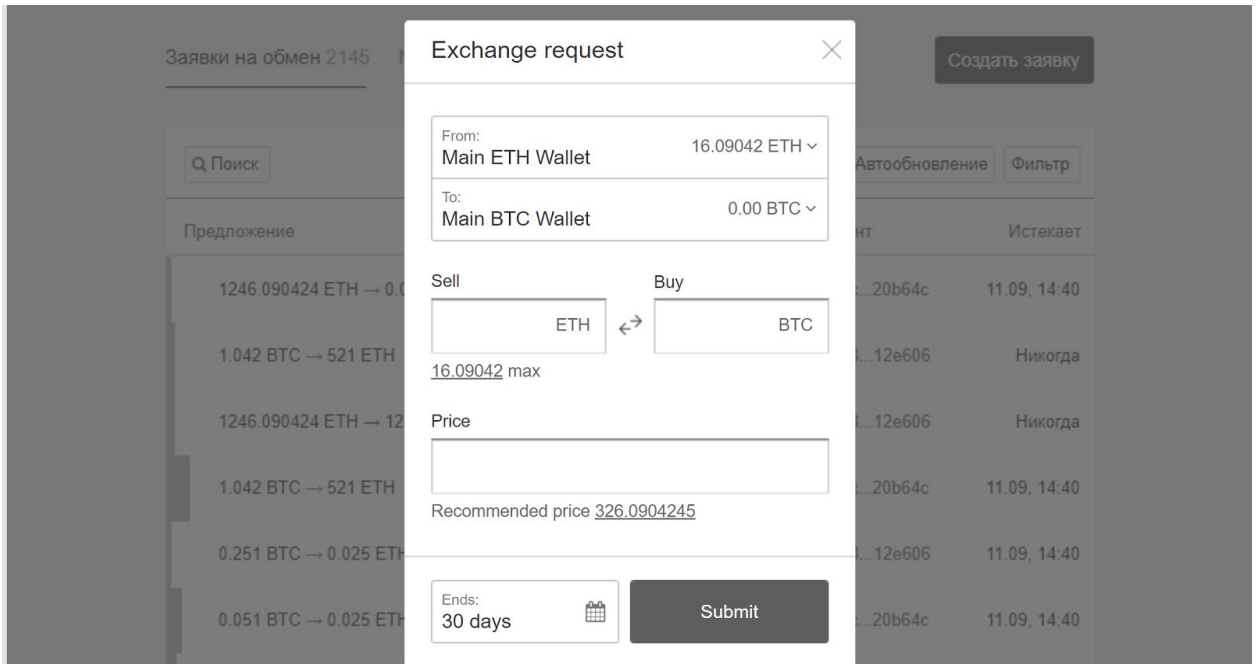


If users find a suitable offer for the exchange, they can select it and confirm the transaction, after which it will be conducted automatically.



If users don't find a suitable offer, they can create their own by choosing the pair of assets to exchange, which account(s) will participate in the exchange, the price, and the period during which the offer will be valid. When specifying a price, users can see recommended values, which are updated in real time based on quotes from a popular exchange. Users can also manually select a specific exchange to take quotes from as a

benchmark. After users confirm an order, the order is published and becomes available to all participants in the network.



The application interface is not simply an attempt to make the product appear visually attractive. It is a clear, robust system that takes into account user interests and structurally combines solutions from users and developers. In developing the interface, we familiarized ourselves with the banking products from leading financial companies in Russia, Europe, and the USA. After a detailed study, we discovered general trends in the design of banking products which are familiar to users, and incorporated these into the design.

The minimal, concise design emphasizes a well-thought-out UX which has been validated in focus group testing. For example, the upper part of the screen always contains an intuitive menu with all of the key options of the product; upon navigating to a particular section (e.g. the dashboard or active wallet), the user sees a graphical layout that facilitates the perception of financial information. In addition to the more traditional solutions, we also used some more innovative ones: for example, regardless of the number of wallets in use, the user can easily understand the total value of their assets. Furthermore, wallets contain an assortment of functions which are helpful to users:

- the ability to monitor changes in operations and growth of a currency
- the ability to create and send invoices independently
- the ability to, and ease of, importing and adding any wallet, as well as adding and removing tokens of interest.

Even though the interface we've created is unique in its accessibility, to engage users in the material, users will be led through a tutorial with a full virtual tour when first using the product. Tips will be attached to all complicated, technical elements.

9. xChainge Token

The xChainge Token (XCH) is an ERC-20, Ethereum-based token with a number of functions in the xChainge platform:

1) Formation of interim Matcher's node deposits
2) Payment of commissions to users when using Matcher's nodes
3) Formation of interim guarantor deposits
4) Payment of guarantor commissions for cross-chain and offline exchanges

Before the start of the crowdsale, 23,529,412 XCH tokens will be generated. A portion of the tokens may be destroyed as a result of the crowdsale; more detailed information on this can be found in section 12. Further issuing of tokens is not anticipated.

There are two principle, long-term drivers of value growth for XCH tokens:

1) An increase in the volume of token operations on the xChainge platform and outside it
2) An increase in the share of tokens reserved in xChainge platform users' deposits, not actively being circulated

The increase in the volume of XCH token operations will occur due to:

- An increase in the volume of transactions processed by Matcher's nodes, and the amount of XCH commission tokens required to execute them
- An increase in the volume of cross-chain and offline P2P marketplace transactions, within which all guarantor payments will be made in XCH tokens

The increase in the share of XCH tokens reserved in xChainge platform users' deposits will occur due to:

- An increase in the number of Matcher's nodes which store deposits in XCH
- An increase in the number of participants and transactions in cross-chain and offline P2P marketplaces, which require deposits for transactions
- An increase in the number of guarantors in cross-chain and offline P2P marketplaces, which require deposits for the provision of services

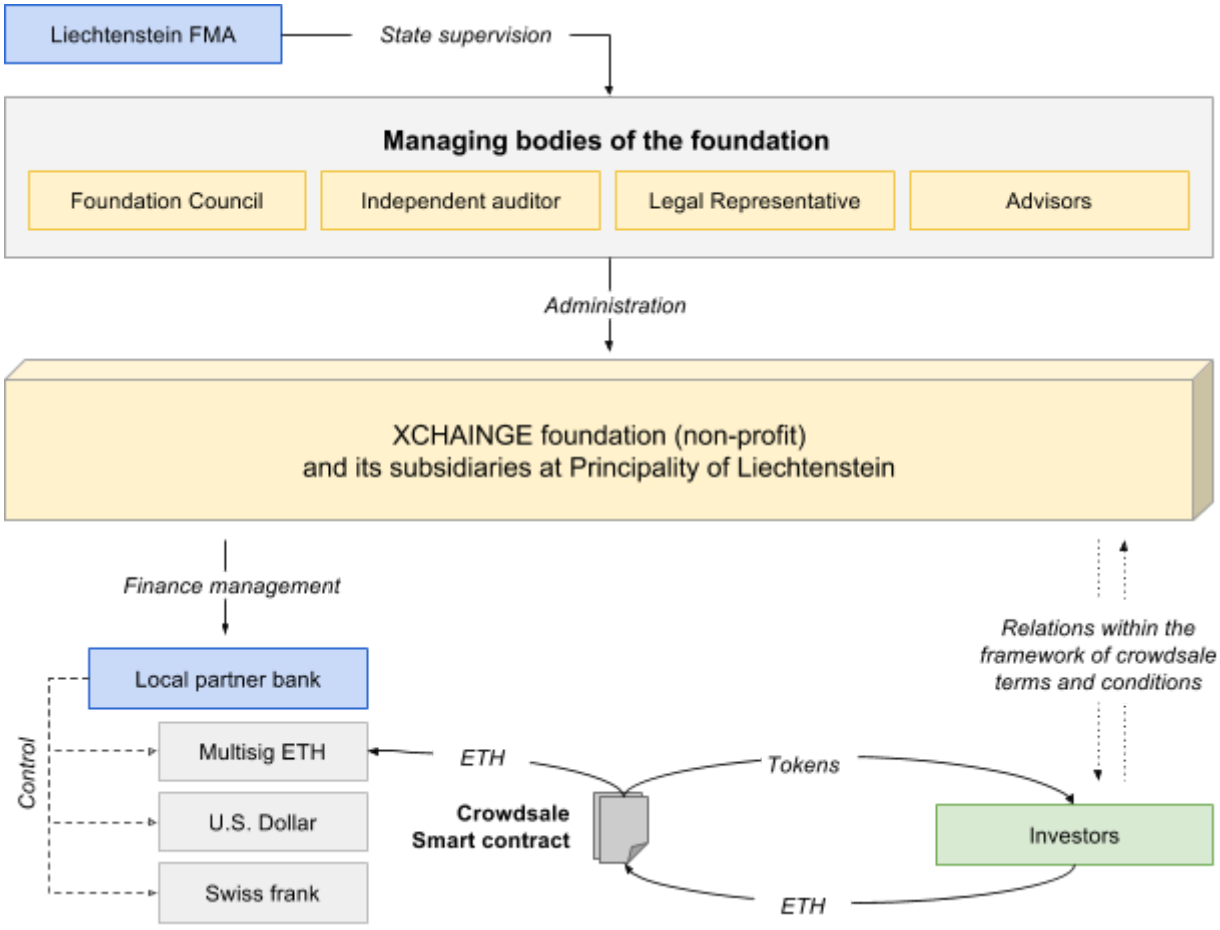
10. Governance

The ICO project is currently under negotiation with the Financial Market Authority (FMA) of Liechtenstein.

FMA
Finanzmarktaufsicht Liechtenstein

For the development and design of the xChainge platform, a non-profit XCHAINGE Foundation will be created; it and its subsidiaries will be based in Liechtenstein. The XCHAINGE Foundation will make key decisions regarding platform development, as well as supervising the collection of funds for development in the context of the crowdsale. The XCHAINGE Foundation will function in full compliance with the laws of Liechtenstein, and will engage in regular reporting in accordance with the requirements of the Financial Market Authority of Liechtenstein. An independent auditing company will be involved in the reporting process.

The highest governing body of the XCHAINGE Foundation is the Foundation Council, which will include the founders of xChainge, advisors, independent directors, and representatives from Liechtenstein regulatory agencies. The composition of the XCHAINGE Foundation Council will be determined and published on the xChainge website before the beginning of token sales.



The xChainge team pays particular attention to legal issues. In connection with the current situation, many tokens fall under the definition of a security. In practice, this means the delisting of tokens from centralized exchanges, the inability to list new

tokens, and penalties from government authorities in respect to the issuers and owners of tokens. xChainge tokens (XCH) do not entitle you to a share in the assets of the Foundation or its subsidiaries. They do not give you the right to vote for the adoption of administrative decisions, nor do they give you the right to receive passive income or a guaranteed redemption value of the token from the issuer. The token is intended for use within the xChainge system. Utility status of xChainge token is under negotiation with the Financial Market Authority of Liechtenstein.

11. Roadmap

The first version of the product is a wallet for ERC-20 tokens; the possibility of a decentralized exchange for them is currently in development. We plan to release the first version in Q1 2018 with full English and Russian localizations. In the future, we also plan to localize the product in other languages[1].

The main stages of xChainge platform development are as follows:

Q1 2018 — v. 0.0.1
- Release of xChainge Wallet for Windows
- Launch of a decentralized P2P exchange platform for ERC-20 tokens

Q2 2018 — v. 0.0.2
- Introduction of the digital transaction constructor in the wallet functionality
- Release of xChainge Wallet for iOS and macOS

Q3 2018 — v. 0.0.3
- Launch of Matcher's node functionality for Windows
- Launch of a P2P decentralized cross-chain exchange platform

Q4 2018 — v. 0.0.4
- Launch of a decentralized P2P exchange platform for real assets
- Release of xChainge Wallet for Android

Q1 2019 — v. 0.1.0.
- Launch of Matcher's functionality for macOS
- Closed testing of the Ariadna Network and the proof-of-snitch protocol

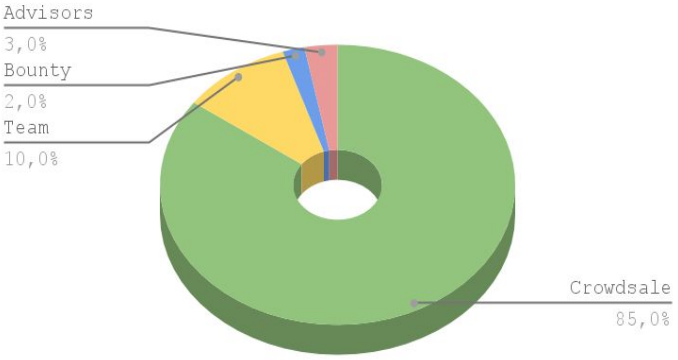
Q2 2019 — v. 0.1.0.
- Launch of the Ariadna Network

[1] In the future, the xChainge team plans to localize its product in Chinese, Spanish, German, French, Portuguese, Japanese, and Korean. Additional localizations may also be possible with the help of community members or external contractors.

12. XCH token crowdsale

In total, 23,529,412 XCH tokens will be issued. They will be distributed as follows:

- 85% distributed to crowdsale buyers
- 10% for the use of the team
- 3% for the use of project advisors
- 2% for participants in the bounty campaign



The xChainge crowdsale will be conducted from 1 December to 25 December using the Dutch auction model, similar to Raiden Network. The initial value of an XCH token will be equal to 0.05 ETH at the start of the crowdsale, and will continuously decrease while the auction is being conducted. Time-dependent token value decrease parameters will be included in the smart contract and published on the xChainge site before the start of the crowdsale. The parameters will remain unchanged for the duration of the crowdsale. The hard cap is 20 000 000 XCH tokens.

A Dutch auction allows each user to independently determine the maximum price for which they are willing to buy tokens. If a user wishes to buy at least n XCH tokens at a price no greater than y ETH per XCH token, they submit an amount to the xChainge crowdsale smart contract equal to $m = n \cdot y$ ETH. The variable y is defined as the auction price at the time of the transaction. If the final auction price x ETH per XCH token is equal to y, the smart contract converts m ETH into n XCH tokens and sends these tokens to the user. If the final auction price $x < y$, the smart contract converts m ETH into $k = \frac{m}{x}$ XCH tokens and sends these tokens to the user. $k > n$; i.e., the user receives more XCH tokens at a lower price than was initially planned.

In our opinion, the Dutch auction model is the most objective way to assess the value of the token and distribute tokens to crowdsale participants. The first time a similar model was applied to a crowdsale was for Gnosis; however, it attracted a significant amount of criticism, because it had a fiat currency hard cap that was quickly reached. As a result, less than 10% of all tokens in the project were allocated to crowdsale participants. Setting the hard cap in terms of the number of tokens sold provides for a more fair, uniform distribution of tokens.

The crowdsale will end in the presence of one of two conditions:

- The amount of requests in ETH becomes equal to the maximum number of tokens available for distribution in the crowdsale times the current auction price x.
- If this first condition is not reached by 23:59 GMT, 25 December, the auction price will reach 0.005 ETH, after which the crowdsale will be terminated and all orders will be executed at a price of 0.005 ETH. Tokens not sold in the crowdsale will be destroyed. Similarly, tokens designated for members of the team,

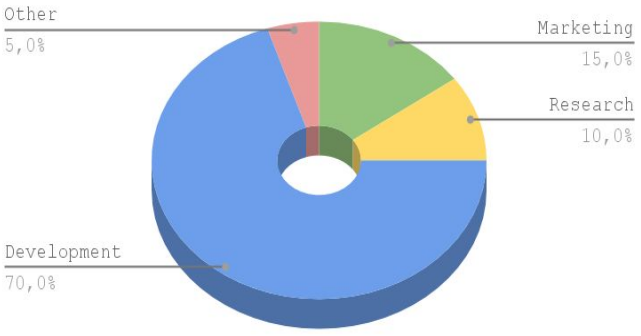
advisors, and participants in the bounty program will be destroyed in proportion to the unallocated portion of tokens.

XCH tokens distributed in the context of the crowdsale and bounty campaign will be available to users within 10 days after the end of the auction, with no restrictions on their further use. The team's tokens have a two-year vesting period and will be released in equal installments of 25% every 6 months. Advisors' tokens have a three-month vesting period. We expect that XCH tokens will begin being traded on decentralized exchanges like EtherDelta as soon as they have been credited to the crowdsale participants. They will also be listed and become available on a few large centralized exchanges soon after the crowdsale.

All funds collected in the crowdsale will be placed into a multisig wallet under the supervision of a bank in the territory of the Principality of Liechtenstein. The bank partner will be announced before the start of the crowdsale. At the end of the crowdsale, the funds will be under the control of the supervisory council of the XCHAINGE Foundation, and will be allocated to the project team gradually within the agreed timetable of the product's development.

The expected distribution of the funds collected in the crowdsale is as follows:

- 70% to the development of the product, including payroll and general expenses
- 15% to marketing and promotion of the product among users
- 10% to academic research on fundamental tasks
- Other expenses, including legal expenses, will not exceed 5%



If the amount collected in the crowdsale amounts to less than 10,000 ETH, all funds will be returned to investors, as these resources may not be sufficient to facilitate development as described above.

13. Team, advisors and partners

13.1. Team

The xChainge founders' company has unique experience in the creation and development of investment companies, financial products, and marketing solutions. All team members have experience in upper management and investment and asset management in hundreds of millions of dollars.

The core team of founders and early investors are shareholders in the company Aktivo is a leader in the Russian market of collective investments in commercial real property. There are also two private venture capital investors.

The founders and early investors are as follows:

- Albert Ibragimov, *co-founder and CEO*
  Key roles: operations management, information security, development management
  Experience more than 10 years of experience in web development and software engineering
  Nornickel, Kaspersky Lab, Workle, Asteros
  LinkedIn **Github**

- Danil Popov, *early investor, co-founder*
  Key roles: product development, marketing strategy, PR
  Experience: marketing director and co-founder of the crowd-investing company Aktivo; general director of Multiways advertising agency
  LinkedIn

- Artur Ustimov, *early investor, co-founder*
  Key roles: strategic development, partnership network
  Experience: operational director and co-founder of crowd-investing company Aktivo, commercial department of Unilever
  LinkedIn

- Egor Klimenko, *early investor, co-founder*
  Key roles: raising capital, strategy
  Experience: general director and co-founder of crowd-investing company Aktivo, managing partner at NRG Capital, director of SARS Capital
  LinkedIn

- Andrey Balakirev, *early investor*
  Key roles: internal auditing
  Experience: more than 10 years in leadership positions with SNS Group (FMCG distribution), managing partner of Pallada retail network, private investor since 2011

- Sergey Skachidub, *early investor*
  Key roles: internal auditing

Experience: general director of TIUSOM (exclusive distributer of British American Tobacco in Russia), managing partner of the Pallada **retail network,** private investor since 2011

Operations team

- Albert Ibragimov, *CEO*
  see "Founders and early investors" section

- Evgeny Shakhmaev, *software architect / back-end developer*
  Experience: more than 5 years of experience developing server-side web applications, including requirements analysis and creation of high-level architecture. Experience in the development of Smart Contracts for the Ethereum platform.
  Worked at Zvooq, Informatica, Fujitsu GDC
  LinkedIn Github

- Konstantin Mazurov, *front-end developer*
  Experience: former CTO of AppInWeb, more than 3 years of experience developing automation systems. Extensive expertise working with big data, optimization of business processes, integration of internal corporate systems with third-party solutions of any complexity.

- Aleksandr Zhulin, *head of design*
  Experience: 10 years of experience in interface design, graphic design, branding, printing, and art direction. Winner of awards in international and Russian graphic design competitions.
  Behance

- Kirill Bedraty, *product manager*
  Experience: More than 3 years of experience in managing IT projects: building project development strategies, KPI planning, process control development.
  LinkedIn

- Konstantin Dolzhenko, *UI/UX lead*
  Experience: 10 years of experience in development and design of informational and commercial products. Project implementation for Tinkoff Credit Systems, QIWI, Art. Lebedev Studio

- Linar Molotov, *head of system modeling*
  Experience: employed by graduate school of business (MBA) of Kazan Federal University, patent holder for complex systems quantitative indicator forecasting methodology
  LinkedIn

- Ilya Vorobyov, *head of analytics*
  Experience: founder of Chain Media, 5 years of experience in strategy and analytics at MegaFon, Unilever, 3M.
  LinkedIn

- Polina Lysenko, *Head of support*
  Experience: administrative director of Front Office business space, project manager for Novosibirsk Oblast Youth Initiative Support Agency.
  LinkedIn

13.2. Advisors

- PhD, Natalya Tokareva
  Experience: Senior researcher at the Laboratory of Discrete Analysis in the Sobolev Institute of Mathematics, associate professor at Novosibirsk State University, researcher at the Algoritmics Laboratory of Novosibirsk State University, team leader of the CRYPTO-group
  Research interests: symmetric cryptography, Boolean functions and discrete mathematics.
  Personal page; Math-Net; ResearchGate; dblp; Scopus

- PhD, Anastasiya Gorodilova
  Experience: Researcher at Sobolev Institute of Mathematics, assistant professor at Novosibirsk State University and NSU Specialized Educational Scientific Center
  Research interests: Boolean functions for cryptography, APN functions, cryptography, combinatorics, algebra.
  ResearchGate; dblp; **Scopus**

- Alexey Oblaukhov
  Experience: Researcher at Novosibirsk State University, lecturer at Novosibirsk State University and NSU Specialized Educational Scientific Center.
  Research interests: blockchain technologies, cryptography, and discrete mathematics.
  ResearchGate; **Mathnet ; Springer**

On 30 october 2017, negotiations concerning the participation of five potential project advisors in the following areas took place:

- Blockchain development
- Cybersecurity and network architectures
- Legal support
- Exchange system design

This section will be updated on 5 November 2017.

13.3. Partners

Science:

- The CRYPTO Group
  Cryptography and cryptanalysis scientific group of the Mechanics and Mathematics department of the Novosibirsk State University and Sobolev Institute of Mathematics.

- Master's degree programme "Master in Cryptography„
  Master in Cryptography from Novosibirsk State University is an innovative programme designed to involve young researchers in the field of modern cryptography and bring them onto a high professional level in this area. The programme covers all basic aspects of cryptography and cryptanalysis and provides deep theoretical and practical background in this field. Professionals in cryptography will be invited to deliver lectures.

Legal:

- **Juricon**

  Juricon Treuhand Anstalt was established in 1976, though its history goes back to 1955. The highly qualified team at Juricon is composed of 15 employees, including lawyers and economists with international experience. Juricon Treuhand Anstalt became one of the six founding members of IAG, Integrated Advisory Group, in 1989. Today, the association includes more than 100 members from Europe, North and South America, and Asia.

- **Actusag**

  An international consulting company specializing in tax consultation and financial planning.

- **Audina**

  Founded in August 1985 in the Principality of Liechtenstein by a group of lawyers, Audina Treuhand AG has been operating successfully for over a quarter of a century as a diversified firm and independent trust company.

14. Conclusion

The xChainge team believes that the ability to freely exchange assets is an important factor in the development of society, and an inalienable right of every human being. For millennia, exchange has contributed to the growth of people's welfare, even despite the strong centralization and myriad artificial restrictions.

The trustless, decentralized, peer-to-peer exchange of assets may signal the beginning of a grand, new chapter in the development of society; however, it currently remains confined to small groups of technologically advanced crypto enthusiasts.

We hope that xChainge's solution will help to make it accessible and familiar to anyone.

15. References

[1]https://medium.com/@FEhrsam/why-decentralized-exchange-protocols-matter-58fb5e08b320
[2]https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
[3]https://twitter.com/vitalikbuterin/status/916926487172968448
[4]https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf
[5]https://etherscan.io/chart/address
[6]http://www.internetlivestats.com/internet-users/
[7]https://www.juniperresearch.com/press/press-releases/mobile-banking-users-to-reach-2-billion-by-2020
[8]https://etherscan.io/chart/chaindatasizefull
[9]https://etherscan.io/chart2/chaindatasizefast
[10]https://www.cryptocompare.com/wallets/#/overview
[11]http://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy/mt-gox-files-for-bankruptcy-hit-with-lawsuit-idUSBREA1R0FX20140228
[12]http://fortune.com/2016/08/03/bitcoin-stolen-bitfinex-hack-hong-kong/
[13]http://fortune.com/2017/07/27/btc-e-digital-currency/
[14]https://themerkle.com/poloniex-users-suffering-from-frozen-accounts-suspended-withdrawals-and-disabled-markets/
[15]https://support.bittrex.com/hc/en-us/articles/115002187632-Statement-on-disabled-accounts
[16]https://news.bitcoin.com/germanys-largest-bitcoin-exchange-hands-over-customer-data-voluntarily/
[17]https://coin.dance/volume/localbitcoins
[18]https://coinmarketcap.com/charts/
[19]https://data.worldbank.org/indicator/CM.MKT.LCAP.CD
[20]http://www.bis.org/publ/rpfx16fx.pdf
[21]https://hackernoon.com/how-one-hacker-stole-thousands-of-dollars-worth-of-cryptocurrency-with-a-classic-code-injection-a3aba5d2bff0
[22]https://www.reddit.com/r/EtherDelta/comments/6hrxjw/etherdelta_guides_for_first_time_users/