SWAP.ONLINE WHITE PAPER

VERSION 1.0.
February 2019

Vladislav Sopov, vsop@swap.online
Daria Purtova, daria@swap.online

CEO - Alexandr Noxon, noxon@swap.online

CONTENTS

0.1. Swap.online: Abstract

Swap.online is a peer-to-peer (wallet-to-wallet) non-custodial exchange of different cryptocurrencies, utility tokens, and soon to be security tokens. Our two main products are a wallet for storing and exchanging cryptocurrencies without the middlemen and an HTML widget allowing any crypto-project to implement the same functionality and to accept cryptocurrencies on their own site. Both of our products work without a server

Swap.online team was the first ever to perform Atomic Swaps with EOS and USDT (Sep, 2018). We added BTC and ETH blockchains in August 2018. By today LTC, TLOS are also connected to our global cross-chain network. More than 45 projects are already connected and have recommended swap.online to their communities.

0.2. Problems of crypto exchange market

In this chapter, we look into the problems of over-centralization, the excessive participation of third parties in exchanges, the abuse of KYC-AML procedures, as well as the orientation of decentralized services to only one network.

0.2.1. Over-centralization

Over-centralization plays a large role when conducting both transactions within the same blockchain and exchanges between different cryptocurrencies. It is so due to the existence of a single ‘central’ software or a hardware element. Crypto exchanges and wallets use this over-centralization to speed up the process of exchanges, monitor customer behavior, and optimize business processes.

The consequence of centralizing such services is that they become exposed to the decisions made by the authorities of those countries where the service is either registered or deployed. This was greatly illustrated by the litigations [3] made by the US SEC against numerous (local) exchanges, and the problems faced by participants of the Chinese [2] crypto exchange market. Countries that used to be attractive for businesses have become “problematic” in terms of jurisdiction - for example Singapore [5] and Canada [1].

0.2.2. KYC-AML procedures abuse

The KYC/AML policies (Know Your Customer/Anti-money Laundering) as well as the ATF (Anti-Terrorist Financing) obliged cryptocervices to collect data about the identity of its users and their sources of income. Cryptocurrencies, as anonymous or pseudonymous financial systems, are very attractive for laundering and illegal transfer of money. That is why countries like the United States, United Kingdom, South Korea, and the European Union have strict requirements for checking users. In practice, this fact results in significant difficulties with the withdrawal of funds even for law-abiding users who have provided all of the required documents to these centralized services. Some inquiries may be delayed for weeks, even months [6], which is completely unacceptable, considering the volatility of cryptocurrency rates.

0.2.3. Decentralized exchange services focus on one network - Ethereum.

According to the statistics, more than 87% of all operations on the decentralized exchange market are conducted through services that support only ERC-20 tokens, i.e. strictly tied to the Ethereum network. The most popular services - EtherDelta and IDEX support only these type of tokens. On one hand, it is more convenient for exchanges to access only one network, on the other hand, it satisfied the market needs during the ICO bloom period in 2016-2017 when most of the projects issued ERC-20 based tokens. There are a number of problems associated with this circumstance:

- Lack of decentralized services for exchanging Bitcoin despite the fact that BTC dominates the market by more than 50% and is still the most popular cryptocurrency especially for newbies;
- The lack of decentralized exchanges for USDT - a stablecoin with $2 billion capitalization showing high demand among the largest centralized exchanges.
- Lack of decentralized exchanges for coins based on high-tech blockchains such as EOS, Stellar, NEO, etc., although these blockchains are more attractive than Ethereum for the significant part of the community.

0.3. Competitors Overview

Amongst the most popular solutions on the market for a decentralized exchanges are projects based on a single blockchain. A number of promising projects have repeatedly postponed their release date and changed the scope of their product. In addition, most services require additional downloads and installations.

The table below (Figure 1) considers some projects in the field of high-tech decentralized exchanges.

Project	**Web-site**	**Development Stage**	**Weaknesses**
Altcoin.Io	https://altcoin.io	Working	Uncertain product, ‘out-of-the-box white label decentralized exchange’
AirSwap	https://www.airswap.io	Working	ERC-20 tokens only, Metamask, Ledger or Trezor

			are required
0x	https://0x.org/	Working	ERC-20 tokens only
Omega One	https://dark.omega.one	Early Access Program	Uncertain Product, postponed release
Neon Exchange	https://neonexchange.org	Working	NEO and Ethereum blockchains only, Chrome extension required

Figure 1. Selected promising decentralized exchange services (summer-autumn 2018)

Most of our competitors run their decentralized exchanges only on one blockchain. Such services focus on the exchange of assets based on Ethereum blockchain, and were very popular during the period of maximum interest in ICO's with ERC-20 tokens (for example, EtherDelta, ForkDelta, Kyber Network, 0x, Airswap). But evidently, assets based on other blockchains can not be exchanged on these services.

Less common are services with proxy tokens (sidechain bridges) like BitShares, WavesDEX, BinanceDEX. The essence of their decentralization is in an isolated blockchain, the same as in the examples considered in the previous paragraph. Proxy Token is the link between the exchangeable and the target currencies. Money and cryptocurrency of the clients get into such services through affiliate exchanges or special "bridges". Opgfhgfhfgerators of such bridges are a limited number of people called "validators". In this case, the middlemen is not excluded and can act in their own interest. Well known example of such consequences - is the rate fluctuation of BitUSD stablecoin, a unit of payment in BitSharesDEX (Figure 2). Like any stablecoin, its rate must be pegged to one unit of fiat currency (in this case, the US dollar). At the same time, services that use a proxy token provides such a wide field for manipulations, allowing the users to lose more than 30% when depositing and withdrawing their money.

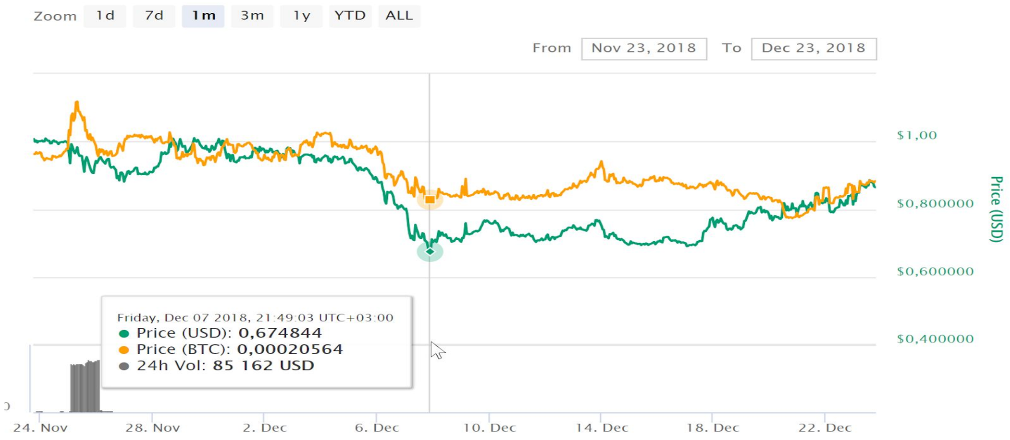


Figure 2. Rate fluctuation of BitUSD stablecoin - possible evidence of manipulations on the affiliate service.

1. Swap Online: the idea and technology

At the moment Swap Online offers two conceptual products: 1) Swap.Widget - a solution for projects to accept cryptocurrencies on their websites directly, without intermediaries; and 2) a decentralized multi currency wallet with a built-in cross-chain exchange powered by atomic swap technology.

1.1. Swap.Widget - a solution for exchanging Bitcoin and other cryptocurrencies within a clients project.

After major legal issues will be resolved, Blockchain, as a global financial network, will allow every entrepreneur to get access to the global market, and cross-chain solutions will play an essential part. Businesses will be interested in receiving payments in Bitcoin with its huge community, as well as in stablecoins that will advance in terms of legal recognition.

The easiest way for a project to access this market is by issuing their own token, and exchanging it for BTC and USDT directly on their website. An excellent technological solution for this is Swap.Widget, which will allow to exchange any token with any of the world's key blockchains. This way of business tokenization is safe, adaptive, and beneficial for all parties.

1.1.1. Bitcoin and USDT: unavailable Klondike

In 2017 during the high popularity of classical ICO schemes, the vast majority of these projects accepted just Ethereum. This is due to a number of reasons, such as: the simplicity of the technical solution, the convenient interaction of smart contracts executed by the Ethereum Virtual Machine, the popularity of Ethereum tokens, and the relatively high speed of transactions. However, those schemes have a number of inevitable flaws:

- A high level of dependance on the rate of Ethereum in a cryptocurrency market that is highly volatile. Thus, a startup that collected $1 million in Ethereum in May 2018 would have to reduce its budget in six months by 5 times, which in most cases forces to spend these funds as soon as they are collected;
- Bitcoin is still the dominant cryptocurrency, recognized in many countries as the most legitimate mean of circulation;
- For beginners in the Cryptocurrency trade, it is more complicated to purchase Ethereum than Bitcoin.
- In case of Bitcoin and altcoins simultaneous failure stablecoins become the most profitable means of payment for both businesses and customers.

Note that in this situation Ethereum can be replaced by any other currency, but the point will remain the same: any program that is tied to only one blockchain and does not include stablecoins becomes extremely vulnerable.

So in order for projects that have their own token to start accepting payments, there solution should have the following features:

- Work with different blockchains in addition to the Ethereum network;
- Work with stablecoins and first of all with USDT;
- Quick installation, developability, simple integration with any sort of project.

1.1.2. Swap.Widget: accepting cryptocurrency and stablecoins on any website.

At the end of November 2017 the idea was formulated of how the payments in Bitcoins can be accepted in a decentralized mode through atomic exchanges using bitcoin.js. A decentralized application interacts with the payer through a special type of time-limited cryptographic payment - HTLC (for more details, see 1.2.2) - which allows the payer to receive tokens, and the seller (for example, the application team) to receive the payment in cryptocurrency. Thus , the b2b-implementation of atomic swaps gave the idea which started Swap.Online.

The end-user solution in this business field of Swap Online is Swap.Widget - an HTML widget that allows to accept cryptocurrencies. The back-end of Swap.Widget is a javascript code. It can be built-in to any website and allows to accept payments in both Bitcoins and USDT, exchanging them for tokens of the project. For the buyer, it is somewhat similar to the payment gateways of traditional financial systems. Swap.Widget, is a completely decentralized solution, that does not store assets and is only a mean of interaction between the buyer and the seller.

So for teams that are issuing tokens, some of the advantages of Swap.Widget are:

- Quick access to exchanges. As of today, projects have to use exchanges that require them to go through massive and time-consuming verification procedures;
- Low cost solution in comparison with the average price for listing tokens;
- No transaction fees via Swap.Widget;
- No need to trust centralized services with the customers' money and the project’s assets.

For ‘end’ users purchasing tokens, the following benefits of Swap.Widget are important:

- The variety of cryptocurrencies that are accepted. Bitcoin and USDT are already connected, new blockchains are being tested and will be added soon;
- Accepting stablecoins guarantees a more accurate financial forecast;

- Funds go directly to the team, bypassing centralized services. This allows the requirements for the nature and amount of cash inflows to be as flexible as possible;
- The ability to exchange rare, over-the-counter assets.

The abovementioned allows us to define Swap.Widget as a highly adaptive solution. It is suitable for ICO, STO schemes and any other forms of interaction between blockchains of the buyer, seller and regulator that may become popular in the future.

1.2. Swap.Wallet - a cross-chain wallet

An important function of swap.online service is - storing, sending and receiving cryptocurrencies of different blockchains. Additional installations and downloads are not required - a multi-currency wallet is created automatically when the main domain - https://swap.online is loaded. The technologies of atomic swap and HTLC are used for the exchange.

1.2.1. Technology: atomic swaps.

The idea of atomic swaps was introduced in 2013. The commercial implementation followed only four years later and was demonstrated by one of the developers from the Komodo Platform team in September 2017. At that time swaps were performed between the blockchains of Bitcoin, Litecoin, and Decred. Those exchanges work with Hashed Timelock Contracts.

HTLC is a smart contract in which the cryptocurrency is locked, and it can only be received at a predetermined address, by presenting the secret to the corresponding hash within a certain time period. When creating the contract, only the hash of the secret is known, and the secret itself is not yet publicly available.

By creating two symmetric HTLC’s on different blockchains, you get a fairly simple atomic swap mechanism. One smart contract is created by Alice on the Bitcoin network; The beneficiary of this contract is Bob’s Bitcoin address. Bob creates exactly the same smart contract on the Ether network, where the beneficiary is Alice’s address. One of the parties holds the secret, but both parties known the hash of this secret, and with this hash both smart contracts are created. _Which party keeps the secret is not important. The important thing is that the one who knows the secret creates a contract with an increased time lock frame.

HTLC features - both contracts are symmetrical, the party that has presented the secret is the first to get the cryptocurrency. For example, Alice presents the secret to Bob's smart contract which is on the Ether network. The Smart Contract calculates the hash of the secret — and if everything matches — it sends ETH to Alice's address, pre-wired into the Smart Contract.
Since all operations in blockchain are public, the secret is immediately revealed to Bob. In Alice's smart contract, bitcoins are locked with the same hash, so after Bob presents the revealed secret he immediately receives his Bitcoins. It is important to do it in time, while the

time lock is valid.
If for some reason Alice does not reveal her secret, Bob can safely take back his Ether after the expiration of the time lock. At the same time, Alice cannot get Bob’s Ether from a smart contract by presenting the wrong secret, because it doesn’t match the hash and the smart contract will not release Ether.

Any atomic swap has two stages.

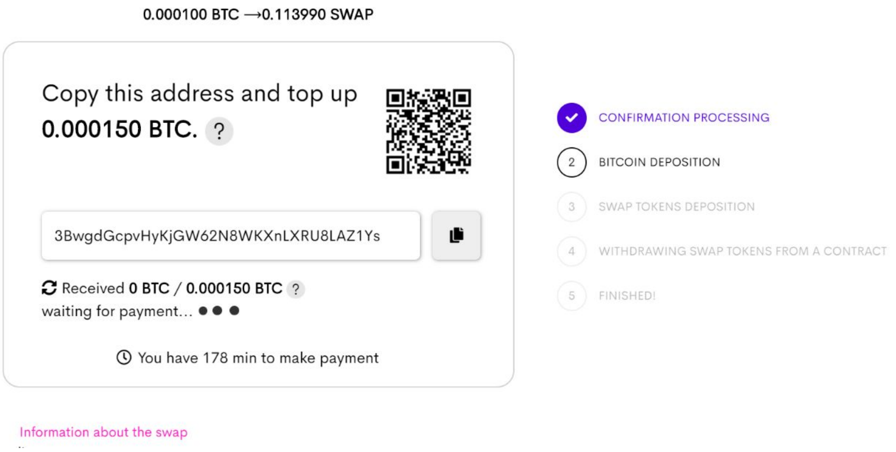
The first stage is “order matching”, the process when to parties agree on an exchange. To be precise, this is a necessary step that must occur before an atomic swap begins. How this step is executed differs projects from one another. The protocols for the “handshake” procedure before starting a swap are completely different - some use centralized services, some sidechain, others decentralized order-books.

Swap.online, in the first version of its protocol, uses IPFS pubsub, a fully decentralized messaging protocol. Each order created by the market maker is translated into the message channels which market takers are subscribed to. It’s like a loud announcement: “I am ready to change my 10 Bitcoins for your 100 Ethers”.

After subscribing to the message channels, the market taker sees orders as soon as they are available. In order for a market maker’s order to be visible - he must constantly post messages about its relevance to the channel, therefore the market maker needs to be always online in order to make deals. This inconvenience is eliminated by Swap.online professional trading solution (bot), which can work with orders independently.

But this does not bring any inconvenience, because in any case exchanges with HTLC protocol requires the transactions to be signed in real time. And the Market Taker can accept the order at any time.

Once the market taker accepts one of the advertised orders by signing the acceptance message, both parties start creating the HTLC contracts on their blockchains and complete the transaction using the protocol described above.



0.000100 BTC →0.113990 SWAP

Copy this address and top up **0.000150 BTC.** ?

3BwgdGcpvHyKjGW62N8WKXnLXRU8LAZ1Ys

Received **0 BTC / 0.000150 BTC** ?
waiting for payment... ● ● ●

You have 178 min to make payment

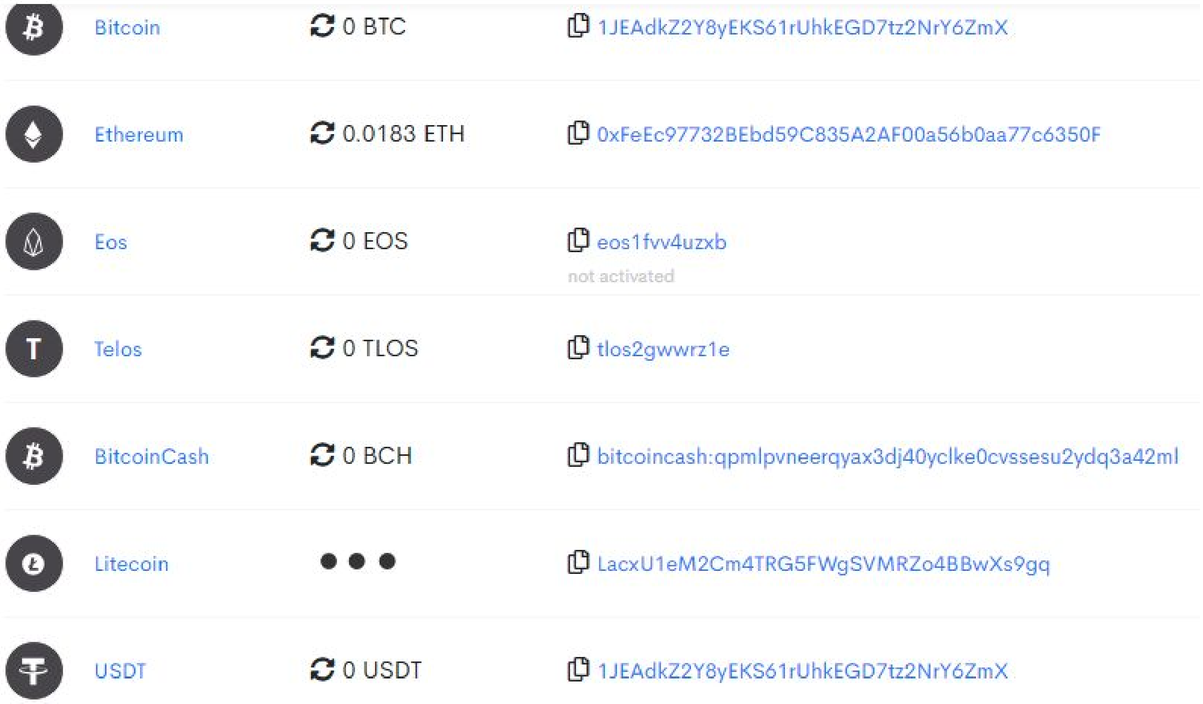
1. ✓ CONFIRMATION PROCESSING
2. BITCOIN DEPOSITION
3. SWAP TOKENS DEPOSITION
4. WITHDRAWING SWAP TOKENS FROM A CONTRACT
5. FINISHED!

Information about the swap

Figure 3. Swap.online user sees all the steps of atomic swap.

1.2.2. Secure private keys.

To confirm operations, the service generates a set of public keys (one for each blockchain, i.e. an unlimited number of ERC-20 tokens are available to the user under one public key, see Figure 4) and private keys associated with them. The address in the Ethereum network assigned to the user is used for identifying him/her by our resource.

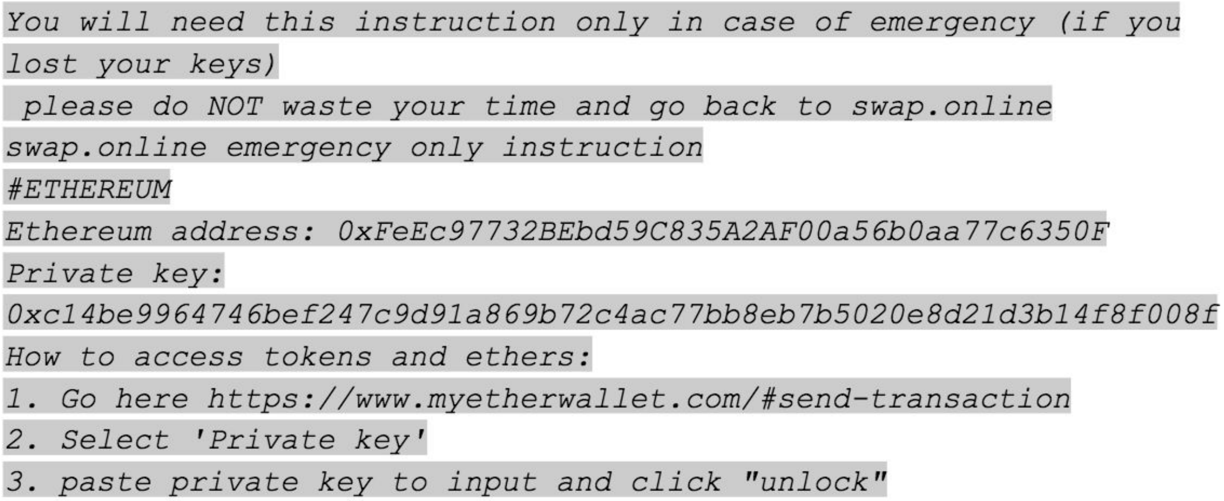


Bitcoin	0 BTC	1JEAdkZ2Y8yEKS61rUhkEGD7tz2NrY6ZmX
Ethereum	0.0183 ETH	0xFeEc97732BEbd59C835A2AF00a56b0aa77c6350F
Eos	0 EOS	eos1fvv4uzxb not activated
Telos	0 TLOS	tlos2gwwrz1e
BitcoinCash	0 BCH	bitcoincash:qpmlpvneerqyax3dj40yclke0cvssesu2ydq3a42ml
Litecoin	● ● ●	LacxU1eM2Cm4TRG5FWgSVMRZo4BBwXs9gq
USDT	0 USDT	1JEAdkZ2Y8yEKS61rUhkEGD7tz2NrY6ZmX

Figure 4. A set of public keys, generated by the user using swap.online.

Since swap.online does not store users' keys or their funds, it is the users full responsibility to keep a backup copy of their keys. They are warned about this matter. In the first version of the wallet the backup copy of the keys are downloaded as a .txt file and can be used both to restore access to the account initially opened on Swap.online and to import it from another service. As shown in Figure 5, the file with keys contains instructions for opening and importing accounts in case of an emergency.

One of the features of swap.online wallet is it can quickly create and access an account on EOS.IO network. The difficulties with registration and creating an account on this blockchain leads to the fact that users who want to purchase these tokens turn to centralized exchanges. Swap.online allows even a beginner to do it in a matter of minutes.



```
You will need this instruction only in case of emergency (if you
lost your keys)
 please do NOT waste your time and go back to swap.online
swap.online emergency only instruction
#ETHEREUM
Ethereum address: 0xFeEc97732BEbd59C835A2AF00a56b0aa77c6350F
Private key:
0xc14be9964746bef247c9d91a869b72c4ac77bb8eb7b5020e8d21d3b14f8f008f
How to access tokens and ethers:
1. Go here https://www.myetherwallet.com/#send-transaction
2. Select 'Private key'
3. paste private key to input and click "unlock"
```

Figure 5. A backup copy of the keys and instructions for using them: this document is generated for each user of Swap.online and covers the blockchains of Ethereum, Bitcoin, EOS, etc.

Which technological solutions allow us to talk about Swap.online's special approach to securing private keys?

- The requirement to save the file with the backup keys when replenishing the wallet;
- Swap.online extension for Google Chrome is isolated and is immune to DNS attacks and script injection;
- A special software solution - Keychain - allows you to store keys in an isolated location that is inaccessible even for the operating system. Keychain was developed by our colleagues from Array.Io, who tell in detail about its features here [4]. At first, this function will be available only to investors from the white list.

1.2.3. Atomic swaps with USDT and EOS: swap.online technological innovations.

USD Tether, as one of the most popular and trusted stablecoin has been drawing the attention of the Cryptocurrency community for a long time already. Being a “replacement” for the dollar for jurisdictions and situations in which the use of fiat currencies is impossible, he quickly gained $2 billion in capitalization and became the most popular currency on centralized exchange services. In addition, the Omni Layer protocol, within which the USDT operates, is a unique “second layer” solution. By working with Omni Layer, projects are able to release their own assets into the Bitcoin network.

Komodo Platform developers were interested in a decentralized exchange of USDT, but their solution covered only the ERC-20 version of the USDT, which accounts for about 3% of the total turnover of this currency. Thus, their solution rather misled the USDT users than made the exchange easier. In September 2018 Swap Online team presented a solution of atomic swap with USDT which is a 200-line code. The technical description of this solution is in Appendix 2.

The EOS.IO project, developed by the teams of Graphene, BitShares and SteemIt, attracted the attention of the cryptocurrency community long before the official release of the Mainnet, which followed in the summer of 2018. This blockchain (often called EOS by the name of its token) is used for hosting decentralized applications, which should excel Ethereum. In commercial terms, the following EOS features are most attractive:

- high network bandwidth;
- no transaction fees;
- High level of developability, due to the use of the C ++ language instead of Solidity;
- system scalability;
- high level of decentralization.

Considering this, the issues of integrating the EOS.IO blockchain and organizing sustainable interaction with other well-known blockchains will inevitably come up on the agenda of the world's leading cross-chain projects. Now the storage and exchange of EOS tokens is carried out through centralized exchanges or services tied only to this blockchain, but atomic swaps are the most promising solution. Technical details of atomic swaps with EOS are described in Appendix 3.

2. Swap.online: the progress and perspectives for 2019

On September 1 2018, Swap.online was released on the minnet and we consider this date as the official launch of the project. Therefore, on September 1 2019 we will be able to sum up the annual results. We will track the development of the project according to the following criteria:

- **Swap.Widget: quantity of projects that have implemented this solution.**
- **Swap Wallet: quantity of blockchains and forks added, quantity of swaps.**

2.1. Swap.Widget: Plans

Swap.Online has been developing Swap.Widget since July 2018.

- The working version of the widget was presented and tested in November 2018;
- Today Swap.Widget can accept payments in USDT and Bitcoin;
- based on the knowledge from swap wiki, a demo service was developed where any interested project can test the functionality of the swap widget

For example, you can buy the token of online gambling service Funfair (ERC-20: FUN) directly on the projects website: https://demo.Swap.online/iframe/?url=https%3A%2F%2Ffunfair.io.

The Swap.Widget button that offers to purchase project's tokens can be organically integrated into the functionality of any website. After clicking the button the user can select a cryptocurrency to buy the tokens with, the amount of tokens to buy, the wallet address from which the purchase will be paid for; and the current dollar equivalent will be displayed as well.

Thus, the Swap.Widget product is fully ready for USDT and Bitcoin, other blockchains are under development, an active marketing campaign is in progress.

The goal for 2019: at least 144 implementations of Swap.Widget.

2.2. Swap.Wallet - cross-chain wallet: plans

The MVP of the multi-currency decentralized online wallet from Swap.online was developed in July-August 2018. The alpha testing of the transactions was conducted in July 2018 on the testnet (https://testnet.swap.online). The first blockchains were Bitcoin and Ethereum. After that the development of the wallet went in two directions:

- connecting new blockchains, including those of terra incognita in relation to atomic exchanges;
- Integration of new ERC-20 tokens since it is the main tool for financing of blockchain startups. The teams that participated were satisfied with the listing capabilities of Swap.online and shared their feedback about our service with their community on social medias.

So far, progress has been made in both areas:

- USDT stablecoin was added in August 2018. In September - EOS and Gemini USD (just in a week after the currency was released on the mainnet), Litecoin and Bitcoin Cash were added in October, Telos in November. Such a variety of blockchains is unique for a decentralized exchange.
- First ERC-20 tokens were added in September 2018, they are: ARN by Aeron Project, YUP by Crowdholding, and LEV by Leverj. More than 45 tokens were listed in November with a total community of about 200 thousand people and capitalization exceeding 300 Mln US dollars, including stablecoin DAI by Maker DAO - a world's top project.

First swaps between Bitcoin and Ethereum were performed on the testnet https://testnet.swap.online in June 2018. And new blockchains are gradually being integrated into atomic swaps.

At the time of publication, swap.online exchange capabilities have reached the following progress:

- Over 110 trade pairs are constantly and reliably operating;
- The first ever atomic swap with the full version of USDT;
- The first ever atomic swap with EOS;
- “Smart order book” - shows only those orders that can be taken with the current balance;
- A constantly evolving trading bot that can place and receive orders, analyze the order book, etc.

Goals for 2019:

- To add 50% of the existing blockchains (including all fair and recognized forks) to swap.online atomic swap mechanisms(most of these projects have already reached an agreement with Swap.Online).
- To diminish the turnover of CEXs and Ethereum-pegged DEXs by 10 per cent.
- To reach the monthly volume of 1 million dollars of all transactions that are going through Swap.Online wallets

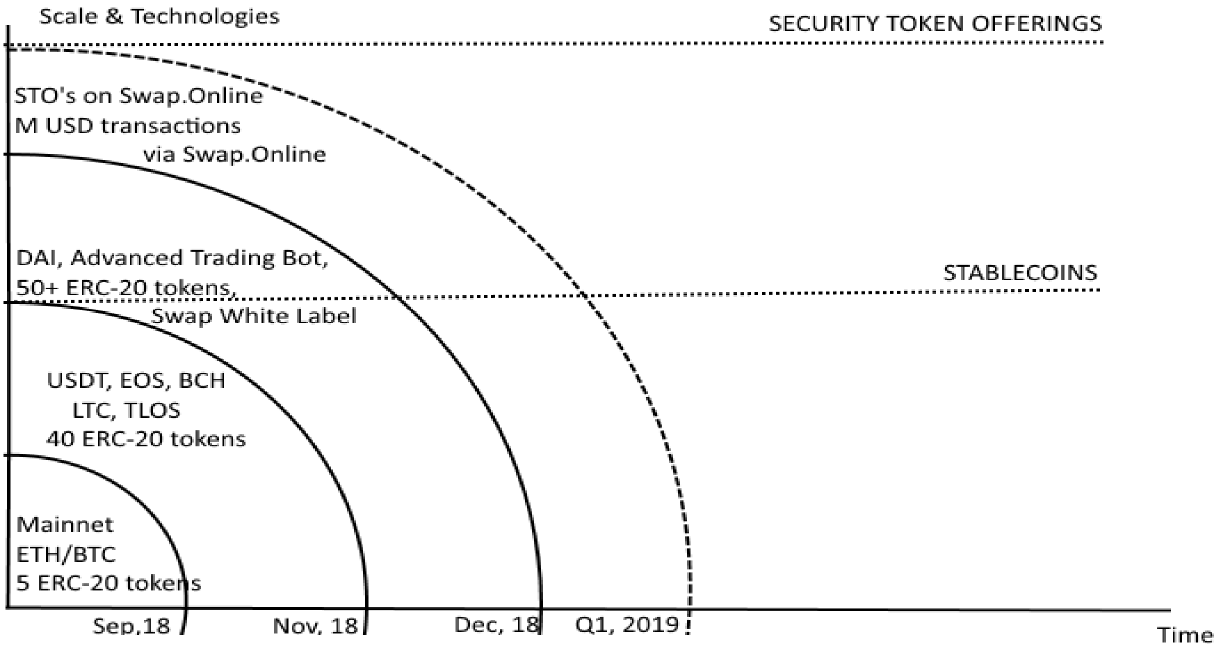


Figure 6. Swap.online roadmap.

3. Swap.online: monetization and legal aspects

3.1. Tokens of crypto-exchange services: examples and method of utilization.

Crypto-exchanges have set up a progressive trend in the blockchain community by distributing their own tokens. These tokens are available for mass purchasing and are considered as an understandable tool for project monetization. Although, the functionality of such tokens may vary in different cases.

Examples of popular tokens associated with cryptocurrency exchange services are Binance Coin (ERC-20: BNB), Kyber Network Crystal (ERC-20: KNC) and Bancor Network Token (ERC-20: BNT).

The most common functions of such tokens are: to create preferences in trading with the exchanges that have issued these tokens, the participation of tokens in technological processes of the exchange, and to cover the service and miners fees with these tokens. In 2018 it became more common to manipulate the rates of these exchange tokens for example by transactional mining or occasionally burning these tokens, that would lead to the increase of their price by reducing their total supply. Lastly, Binance offers to use its tokens for investing into partner projects.

3.2. Swap.online Community Token (ERC-20: SWAP): a mean to account the contribution to the project

According to the examples from chapter 3.1, the most common functions of tokens issued by exchange services are the coverage of fees and securing the network performance. At the same time the interest for the token and its price increase as the demand for the services rises, thus the token holders get "dividends" from the success of the project. At the moment SWAP token serves as a mean for accounting the contribution to the project. SWAP is already used as a reward for the contributors of the project. 10 to 100 percent of the reward is paid in tokens. Most of the contributors of the project consider the rate of 1 SWAP=1 USD. The company Swap Online OÜ itself does not sell SWAP tokens at the moment.

3.3. Equity and tokens: get a share in Swap.online via blockchain.

Given the undefined and extremely dynamic legal status of cryptocurrencies, tokens of any blockchain projects cannot yet be considered as a full-fledged form of ownership of an equity-share in a company, despite the assurance made by the tokens issuers. However, the nature of blockchains -decentralized systems that are resistant to all sorts of scams and abuses - are great for these purposes. In Swap.online, we are developing a mechanism that will maximize the potential of the blockchain as an institutional and technological design for acquiring equity. Here we stick to the following views:

- the acquisition of equity through tokens may be anonymous, but identity proof should empower the acquirer;
- Purchasing the equity with tokens must be legal and from the purchaser side as well. This leads to the need to consider different options for interaction, taking into account the different principles of cryptocurrency regulation;
- The number of SWAP tokens acquired by the user should directly correlate with the share of equity in the company.

3.4. Legal expertise of the project and token

In August 2018, before launching swap.online on the mainnet, lawyers from Bright Law Firm (Tallinn, Estonia) gave a qualified legal assessment to the project and its SWAP tokens. In the evaluation process, experts were asked the following questions:

- Can the Swap.Online token constitute a security within the meaning of the Securities Market Act?
- Is the sale of Swap.Online tokens taxable with the value added tax?
- Can requirements of the Money Laundering and Terrorist Financing Prevention Act apply to activities of Swap.Online?

The Bright Law Firm experts gave an explicit negative answer to all three questions:

- Due to the fact that the “token of swap.online project does not give its holder the right to make decisions, vote, and income expectations” the swap.online token is not a security in accordance with article 2 of the Securities Market Act;
- Swap.online token can be considered as a virtual currency. In accordance with paragraph “e” of Part 1 of Article 135 of the VAT Directive, the Swap.online token cannot be subject to VAT;
- Swap.online service does not create keys for the user itself, does not store them, and does not enter into legal relations with users. Thus, Swap.online does not provide wallet services for storing virtual currency in the sense described in Section 10 of Article 3 of the Money Laundering and Terrorist Financing Prevention Act, and therefore cannot consider itself bound by the provisions of this Law in the relevant part.

Therefore, we can say with confidence that the acquisition and storage of SWAP tokens, as well as the use of swap.online as a service, will not involve large legal procedures and will not attract the interest of tax and financial regulatory authorities.

3.5. License proceedings

The controversial and dynamic status of cryptocurrency in the legal field of most countries of the world poses a complex issue for obtaining licenses for financial and technological start-up teams. Some projects decide not to obtain legal status in one or another country, that on the one hand allows to avoid tax and legal difficulties, but on the other - have a negative impact on the credibility of the project, that in this case exists only in the form of a website.

Swap.online has passed all the registration and licensing procedures. The project is registered as Swap Online OÜ with the registration number 14477421 at Harju maakond, Tallinn, Kesklinna linnaosa, Tartu mnt 83-701, 10115, which is officially recorded in Estonian Register of Economic Activities. The license number FVR 000299 from July 26, 2018 issued by the Eesti Politsei- ja Piirivalveamet in relation to the “Financial Services” subject of field.

Appendix - Technical Details

Appendix 1 . Decentralized order book based on libp2p

TBA

Appendix 2. Atomic Swaps on USDT: Technical Details

To carry out the Omni transaction, a user needs to create a regular Bitcoin transaction -transfer of 546 satoshi (minimum) with an additional output storing payload using the OP_RETURN op-code. An example of such a transaction. The payload is a mandatory part of any Omni transaction, as it is a sequence of bytes containing all the necessary information about the transaction. Here is the example on bitcoinjs.js: https://gist.github.com/caffeinum/f64a51ce55d5ac9075bb2f5f2f439c0d)

Let us consider what information is stored in the payload itself:

●transaction marker — 4 bytes, the mandatory part of any Omni payload is always equal to 0x6f6d6e69 — ASCII code omni. If the first 4 bytes of the sequence are not equal to 0x6f6d6e69, then this sequence is not a payload of Omni.

●version — 2 bytes, an analog version of the transaction in Bitcoin. For the described algorithm to work, version 0 is used, or that is the same as 0x0000.

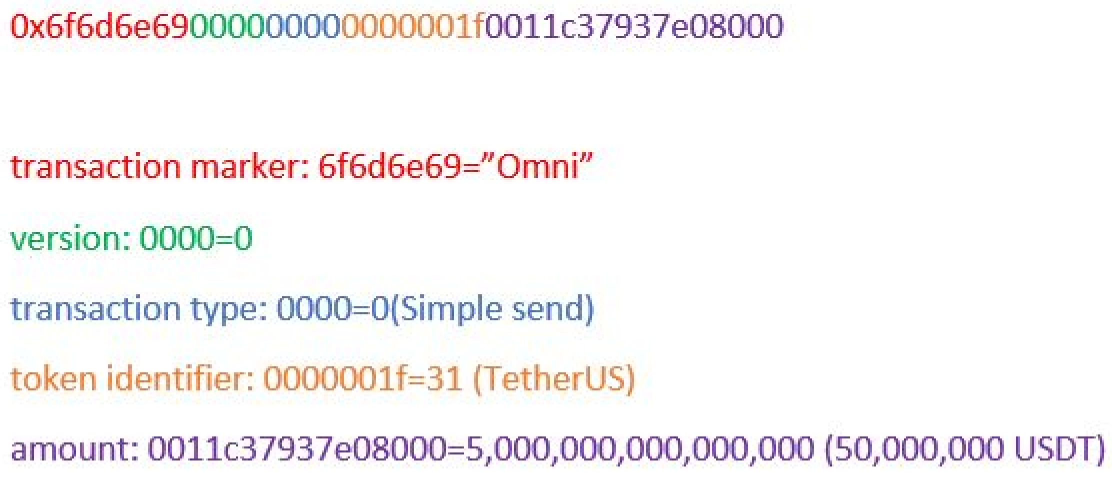
●transaction type — 2 bytes, transaction type, for an atomic swap it is sufficient to use only "Simple send" transactions, as simple send is the usual sending of omni currency from its address to the address of the recipient. Simple send corresponds to the transaction type code 0, that is, the next 2 bytes 0x0000. Other possible types of transactions exist in Omni.

●token identifier — 4 bytes, identifier of the currency used. For example TetherUS has the identifier 31 or 0x0000001f. All tokens created by the Omni protocol at this time can be seen via the following link.

●amount — 8 bytes, for a transaction of type Simple send, this is the amount of the sent currency.

As you can see, payload does not store the addresses of senders and recipients of the transactions, these addresses are determined by the Bitcoin transaction in which the payload output was detected. By scanning inputs, the Omni protocol determines who makes the transfer by finding the output of the corresponding address from among the inputs of the transaction p2pkh.

Thus, for a transfer from Alice to Bob of, for example, 50,000,000 USDT, we need to create a Bitcoin transaction where one of the inputs will refer to the p2pkh output corresponding to the Alice's address. It is also important that this entry be the first in this transaction (the index of this entry in the received transaction would be is minimal or none at all). One of the outputs of this transaction should be the output of p2pkh to Bob's address, and another output must have been one of the outputs with the following payload:



0x6f6d6e69000000000000001f0011c37937e08000

transaction marker: 6f6d6e69="Omni"

version: 0000=0

transaction type: 0000=0(Simple send)

token identifier: 0000001f=31 (TetherUS)

amount: 0011c37937e08000=5,000,000,000,000,000 (50,000,000 USDT)

Figure 7. Omni Transaction Payload.

Suppose that Alice and Bob are willing to make an inter-blockchain exchange of cryptocurrencies. Alice wants to exchange the units of any Omni currency, for example USDT (the given currency has the currency identifier # 31 in the Mainnet, then in the text we will only talk about this currency of the Omni protocol, since it is the most popular at the moment, but the algorithm below will work for any currency of the Omni protocol as well) for b units of a cryptocurrency working on another blockchain. (Omni works on top of the Bitcoin blockchain, of course, according to the algorithm below it is possible to exchange USDT for Bitcoins, but due to their work on one and the same blockchain, this exchange can be done in a different, more efficient way).

Also, suppose, that:

A — blockchain of Bitcoin.

B — the blockchain of the cryptocurrency for which TetherUS is being exchanged.

a — the sum of USDT, which Alice wants to exchange.

b — the sum of the cryptocurrency of the adjoining blockchain B, to which Alice wants to exchange her a USDT.

That’s how the transaction is created:

1) Bob generates a random value secret.

2) Bob calculates the secretHash by performing the following operation: secretHash = RIPEMD160 (secret)

3) Bob creates and sends an HTLC transaction sealed by secretHash

4) Bob sends Alice a secretHash value, and a hash of the hrlc transaction he created in the previous paragraph in order for Alice to make sure that the correct HTLC transaction is actually present in the B blockchain.

5) Alice received from Bob the secretHash and hash of the HTLC-transaction Bob created, and is convinced that such a transaction is really present in the B blockchain, and that this is indeed a HTLC-transaction sealed by the secretHash value.

6) using the received secretHash, Alice creates the following transaction and translates it into the Bitcoin blockchain:

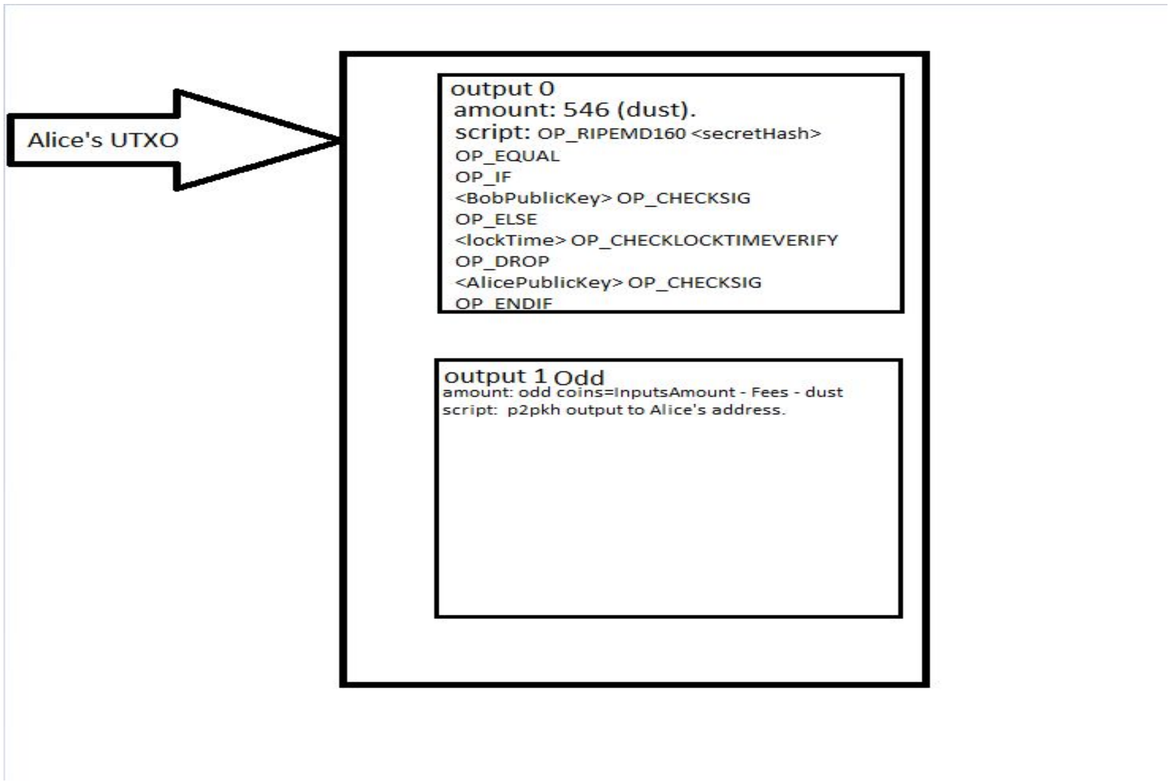

Alice's UTXO
output 0
amount: 546 (dust).
script: OP_RIPEMD160 <secretHash>
OP_EQUAL
OP_IF
<BobPublicKey> OP_CHECKSIG
OP_ELSE
<lockTime> OP_CHECKLOCKTIMEVERIFY
OP_DROP
<AlicePublicKey> OP_CHECKSIG
OP_ENDIF
output 1 Odd
amount: odd coins=InputsAmount - Fees - dust
script: p2pkh output to Alice's address.

Figure 8. Alice UTXO.

Let us call such a transaction financing_tx. In fact, it is almost an ordinary Bitcoin HTLC transaction that is used in atomic swap with the only difference that in the amount field, 546 satoshi is the minimum number of Bitcoins that can be at the output of the transaction, below this value, Bitcoin counts the transaction as dust and does not conduct it.

7) Alice creates a transaction according to the following scheme:

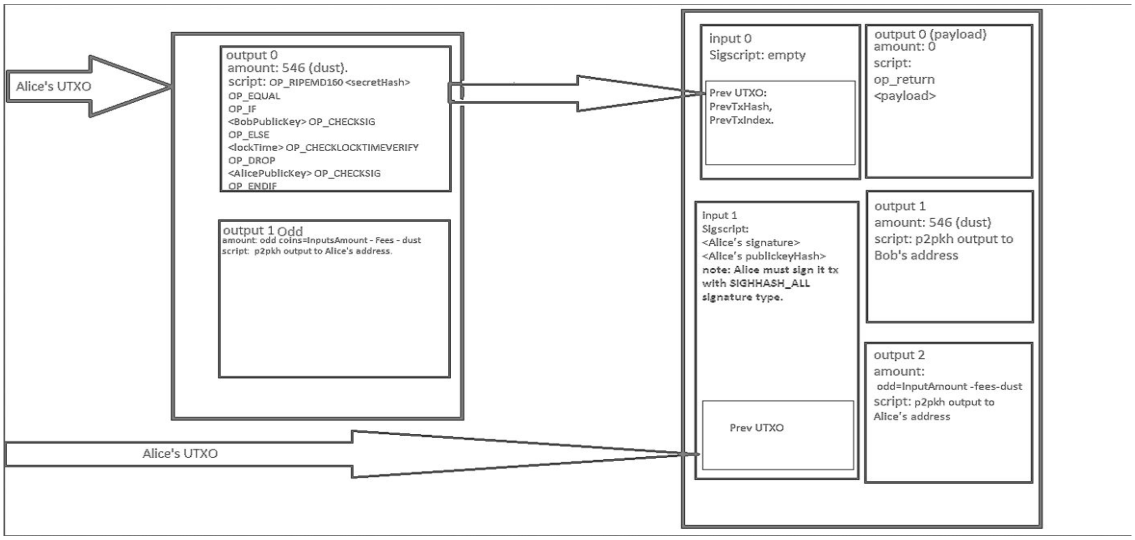


Figure 9. Alice creates transaction

Let us call this transaction redeem_tx. Alice creates such a transaction with two inputs: the first is the input referencing the output of funding_tx, which contains the HTLC script. Alice does not sign this script, that is, the SigScript field remains completely empty. The second input is the input referring to any unspent exits of Alice, the main condition is that at this output stage there are enough Bitcoins to pay the transaction fee, and this entry is signed by Alice with her private key with the signature type SIGHASH_ALL (that is, she signs the entire transaction except for SigScript fields on the inputs transaction, which makes this transaction immutable. The outputs of the same transaction are the elementary Simple Send and a TetherUS from Alice to Bob (details of what Simple Send, payload is and how it works can be found in another section).

8) Alice sends Bob the redeem_tx created in the previous paragraph and the one she signed herself.

9) Bob got the redeem_tx sent by Alice, checks it, just looks through the inputs and outputs, making sure that this is really a transaction that Alice should have created using the real algorithm. After that, Bob signs the transaction with his private key and provides the secret value in the SigScript of the corresponding redeem_tx entry.

10) Bob sends the signed redeem_tx transaction to the blockchain, thereby transferring the TetherUS currency from Alice to himself. Note — before carrying out this step, we still need to check that Alice's address has the necessary amount of TetherUS.

11) Alice looks through blockchain A and gets the value secret and uses it in the B blockchain to transfer the funds using the HTLC transaction Bob created in point 3. The exchange ends here.

Stating the obvious: naturally the timelock value used by Bob when creating the HTLC-transaction must be significantly longer than the timelock that Alice uses, since her HTLC transaction should be spent earlier than the HTLC created by Bob. This is necessary so that Bob cannot manage to spend both HTLC.

Appendix 3. Atomic Swaps on EOS: Technical Details

EOS uses a WebAssembly virtual machine to run smart contracts. The “eosio.token” is smart contract that enables different tokens including SYS tokens. Users will need to create an account to interact with EOS smart contracts. The Swap Online team prepared scripts and instruction for this, which can be found here. Users can also use the “Register” button on the Swap.online website and pay in BTC for account creation. The user also has the function to interact with EOS smart contracts though the EOS endpoint via eosjs library that is imported at Swap.online. It is also possible to interact with the special contract for atomic swaps in order to exchange BTC to EOS using the Swap.online orderbook.

When the user agrees to make a peer-to-peer atomic swap with the owner of EOS tokens, then they have to prefund the HTLC Bitcoin script. Then the owner of EOS will be notified and will send funds to the swap smart contract. In order to withdraw the EOS funds from the smart contracts, the user will have to reveal their secret from the HTLC script in the same transaction. Then the owner of EOS will notified and will withdraw the BTC using the given secret.

Every swap in the smart contract has a period of time when users can withdraw the funds and reveal their secret. That period is twice as less as the period of HTLC to ensure that the EOS owner will have enough time to withdraw their Bitcoins from the HTLC.

If you will not reveal your secret during this period of time, then the EOS owner will be able to get a refund and the opposing user’s reputation on Swap.online will be decreased. If the EOS owner will not create a swap when they prefunded the HTLC script, then their reputation will be decreased.

The smart contract has actions that mutate the state of a contract. Single transactions can have multiple actions. The swap contract has the create, deposit, refund, withdraw and refund actions. When the EOS owner creates swap they send two actions in a single transaction: create and deposit. The swap contract immediately sees that it received EOS token and creates an open swap that is available for withdraw by revealing the secret key. When the user withdraws funds from the swap, they send a withdraw action with their secret key in the argument. When the EOS owner wants to get a refund after the safe period of time, they send a refund action. The code of the smart contract account has the permission to transfer funds to the user.

Disclaimer

YOU UNDERSTAND, ACKNOWLEDGE AND ACCEPT THAT BLOCKCHAIN APPLICATIONS AND PROTOCOLS ARE GENERALLY STILL IN AN EARLY DEVELOPMENT STAGE AND THEREFORE OF EXPERIMENTAL NATURE. YOU THEREFORE UNDERSTAND THAT THE CONTENTS ARE PROVIDED TO YOU ‘AS IS’ AND WITHOUT WARRANTIES OR REPRESENTATIONS OF ANY KIND EITHER EXPRESSED OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, EACH OF SWAP ONLINE PARTIES DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF ANY KIND IN CONNECTION WITH THE TOKENS, THE CONTENT, NON-INFRINGEMENT, AND FITNESS FOR ANY PARTICULAR PURPOSE, USEFULNESS, AUTHORITY, ACCURACY, COMPLETENESS AND/OR TIMELINESS.

The Site and the Content may experience sophisticated cyber-attacks, unexpected surges in activity, or other operational or technical difficulties, which may hinder the use of the Content or affect or even cause faults or failures in the conversion of Tokens. You agree not to hold Bancor accountable for any related losses.

Trading and investing in cryptocurrencies (also called digital or virtual currencies, crypto assets, altcoins and so on) involves substantial risk of loss and is not suitable for every investor. The valuation of cryptocurrencies and futures may fluctuate, and, as a result, clients may lose more than their original investment. The highly leveraged nature of futures trading means that small market movements will have a great impact on your trading account and this can work against you, leading to large losses or can work for you, leading to large gains.

If the market moves against you, you may sustain a total loss greater than the amount you deposited into your account. You are responsible for all the risks and financial resources you use and for the chosen trading system. You should not engage in trading unless you fully understand the nature of the transactions you are entering into and the extent of your exposure to loss. If you do not fully understand these risks you must seek independent advice from your financial advisor.

Swap.online services (including SWAP token) are still in its infancy and may not act as it is envisaged. Functionality of the token and the website may change as it develops

Exchange transactions of cryptographic tokens include the interaction of the hosting provider, carrier, and others. Swap.online minimizes, but does not completely eliminate the risks associated with the actions of third parties and disclaims any responsibility for their actions.

Swap.online does not guarantee the execution of orders available on the website.

Swap.online warns about the possibility of an attack in order to seize any of the domains associated with the website and is not responsible for its consequences.

References

1. *Alexandre A.* Judge Rules in Favor of Canadian Bank in Dispute With Crypto Exchange. URL: https://cointelegraph.com/news/judge-rules-in-favor-of-canadian-bank-in-dispute-with-crypto-exchange .
2. *Graham L.* As China Cracks Down, Japan is Fast Becoming the Powerhouse of The Bitcoin Market. URL: https://www.cnbc.com/2017/09/29/bitcoin-exchanges-officially-recognized-by-japan.html .
3. *Marks H.* The SEC Kills Crypto Exchanges. URL: https://hackernoon.com/the-sec-kills-crypto-exchanges-3dc9e3e87651 .
4. *Ređić E., Petukhova Y.* Keychain Security. URL: https://github.com/arrayio/array-io-keychain/wiki/KeyChain-security#three-security-layers-of-keychain .
5. *Yi S.B.* Singapore's First Bitcoin Trial Begins, With Dispute on Trades Allegedly Reversed Wrongfully. URL: https://www.straitstimes.com/business/singapores-first-bitcoin-trial-begins-with-dispute-on-trades-allegedly-reversed-wrongfully .
6. *Zykov D.* Atomic Exchange Protocol from Swap. URL: https://medium.com/saturn-black/atomic-exchange-protocol-from-swap-8967e70dd750 .