

Atomic Wallet

WhitePaper v.1.40

atomicwallet.io

CRYP2NOVA

2018

Archived copy · cryp2nova.com

Table of contents

Table of contents **2**

Abstract **4**

Crypto market challenges **4**

Custody risk 4

Regulation 6

Possible falsification and distortion of market data 6

Atomic Wallet product **7**

Asset management 7

Distributed Orderbook (DOB) 7

Atomic Orderbook implementation 8

Order acceptance to the DOB mempool 9

DOB anti spam and fraud protection 10

Trades history blockchain storage 10

Atomic Swaps 12

Atomic Swap technology 12

Atomic Wallet Swap implementation 13

Atomic SDK 15

Additional functionality 16

Immutability and decentralization 16

Atomic Wallet ecosystem 17

Platforms 18

Competitive analysis 18

UI Preview 19

Roadmap 23

Current stage 24

Atomic token **25**

Initial Coin Offering (ICO) 25

Token issuing 25

Token allocation 26

Crowdfunding goals 26

Budget allocation 27

Private sale 27

Public sale 28

Community incentives 29

Client Airdrops 29

Bounties 29

Pre-Sale bounty 29

Archived copy · cryp2nova.com

Post-Sale Bounty 31
Post ICO token circulation 31
AWC tokens on exchanges 31
Token economy 31
Team vesting plan 32

Team **33**
Business 33
Tech 33

Glossary **35**

CRYP2NOVA

Archived copy · cryp2nova.com

Abstract

A brief glance at the emerging market of crypto projects is sufficient to understand the potential of the blockchain as a powerful, advanced technology of the future. Yet, despite its vast prospects, a major part of blockchain-based systems still remains at an entry-level, far from being qualified for a general user. Today, the developers' community is facing a number of unresolved issues preventing a full-scale implementation of the blockchain technology in a vast variety of industries, where it could potentially be applied at a great profit.

Crypto market challenges

Blockchain-powered technology is intent on leading the future of financial markets. Today, however, we still observe extensive obstacles for the development of blockchain-based markets. One of the greatest market challenges is the remaining necessity of trust towards centralized financial services in an otherwise decentralized environment. Third party custody risks affect ecosystem sustainability, bringing vulnerability to manipulative and regulative actions.

Atomic Wallet radically solves problems described above by introducing a fundamentally new platform for custody-free, transparent, immutable cryptocurrency trading. Our platform is the simplest way to connect buyers and sellers within a decentralized framework. Atomic Wallet is a new type of decentralized cross-blockchain exchange.

Custody risk

Satoshi Nakamoto, the creator of the Bitcoin, has presented the world with a revolutionary technology thereby offering significant advantages to any projects which would incorporate it. These advantages, namely, transparency, openness, and independence from trust-based mechanisms, have been explored and utilized over the years by those involved in the field.

Since the early days of Bitcoin, cryptocurrency market has evolved into a sophisticated multi-blockchain phenomenon. According to coinmarketcap.com statistics, cryptocurrency market contains over 1,5K different currencies with exchange turnover of over 14 bln in dollar equivalent daily. In addition to coinmarketcap statistics, we should consider the volumes of intransparent and unregulated peer to peer exchange market (a.k.a. ***Over The Counter*****)** as well.

However, present-day exchange providers managing huge exchange volumes inherit custody risks, which counterposes the ideas of transparency, openness, and independence from trust-based mechanisms.

Archived copy · cryp2nova.com

More than once have major exchanges experienced security breaches. One of the most disruptive failures was the Mt. Gox exchange collapse. It took the market up to a year to recover after the disaster. The list of the publicly known biggest failures for custodian-based centralized crypto exchanges would impress an unprepared spectator:

Date	Amount lost	Exchange
February, 2014	650,000 BTC ($368M)	Mt.Gox
March, 2014	150 BTC ($101k)	bitCoin
March, 2014	896 BTC ($572k)	Flexcoin
July, 2014	3,700 BTC ($2M)	Mintpal
July, 2014	5000 BTC ($1.8M)	Bitpay
January, 2015	7,170 BTC ($1.82M)	BTer.com
January, 2015	3,000 BTC ($777k)	Kipcoin
January, 2015	18,866 BTC ($4.3M)	Bitstamp
March, 2015	150 BTC ($3.2k)	Coinapult
May, 2015	1,500 BTC ($350k)	Bitfinex
January, 2016	13,000 BTC, 3,000,000 Litecoin ($5.8M)	Cryptsy
March, 2016	469 BTC, 5,800 ETH 1,900 Litecoins ($230k)	ShapeShift
May, 2016	250 BTC, 185,000 ETH, 1,900 Litecoin ($2.14M)	Gatecoin
August, 2016	119,756 BTC ($65M)	Bitfinex
October, 2016	2,300 BTC ($2.6M)	Bitcurex
July, 2017	37,000 ETH ($7M)	COINDASH
July, 2017	5,300 ETH ($1M)	Bithumb
August, 2017	1,500 BTC ($500k)	Enigma

On a good note, along the process of evolution, each new failure leads to new knowledge, a portion of which crypto professionals comprehend and evangelise in public nowadays in the following way: *if one doesn't have the keys to his/her crypto assets, they can be gone at any moment and this will be irreversible*.

Archived copy · cryp2nova.com

Regulation

Cryptocurrency market draws attention of customers, media, business, hedge funds and even filmmakers. Unfortunately, regulators do not stay aside and give a lot of their attention to the blockchain market as well.
The fundamental idea behind Bitcoin is a censorship-free currency without a central bank, the immutability of which is to be empowered by the financial incentivisation of the stakeholders. Egalitarian permissionless approach showcased by this cryptocurrency contradicts the regulation created for fiat money markets and so is a subject to scrutiny by the officials.
However, while being at the early stage of the development, it is essential to preserve this approach for the further market development and expansion. For the only way of keeping the promise of the Bitcoin manifest is to carry on developing decentralized immutable solutions.

Possible falsification and distortion of market data

In most mechanisms employed by centralized exchanges, the actual market data is unverifiable and suffers from lack of trust. Traders can be misled by false data, intentionally or unintentionally distributed by centralized operators. In a current market state, manipulation and failure to deliver actual trading data can devolve into severe losses for the investors.
Besides the current real-time market data, the history of trades and orders can be substituted, wiped off or distorted in a similar fashion.
Proper end customer and average investor protection from aforementioned risks appears to be a vital step for further successful market development.

CRYP2NOVA

Archived copy · cryp2nova.com

Atomic Wallet product

The aforestated problems are what the blockchain industry is currently faced with and yet fails to solve. Being on the way to achieving its mass adoption, the industry is expected to solve these issues only with a fundamentally new approach based on the idea of decentralization of digital assets exchange. As a reaction to the current challenges of the industry, Atomic project was created - a convenient and versatile decentralized solution for the custody-free cryptocurrency trading.

Atomic Wallet platform is based on a unique, proprietary engine, specially designed to solve its specific tasks. Therefore, this White Paper contains a large number of technical terms describing certain elements of the platform. Each original term is highlighted in ***bold and italic*** when first encountered in the text: for instance, Atomic Swap. At the end of the paper, a glossary with detailed explanations of the terms is available.

Asset management

Atomic Wallet provides a powerful, in-demand service that allows users to reduce efforts spent on managing ***crypto assets*** and renders it transparent and trustless. To make our platform even more convenient and beneficial for users, the Atomic Wallet team utilizes best UI and security practices thus facilitating use of our platform's functionality to the full range. Essential operations one would like to do with his\her cryptocurrency are:

1. Receive crypto assets to the generated wallet
2. Import assets to the wallet using ***private keys*** of various formats
3. Store private keys in a securely encrypted environment
4. Send assets to other ***addresses***
5. Select ***cryptocurrency node*** to use
6. Select ***blockchain explorer*** to use

Aforestated wallet functionality will be built on the ***SPV (Simplified Payment Verification)*** technology. This allows customers to avoid prolonged blockchain synchronization while preserving the security of so-called ***'full node wallets'***.
The keys are stored in an encrypted manner on the end-user device or a hardware wallet (eg. Ledger, Trezor, etc.) Keys can be backed up with the passphrase for all the listed currencies or with a string format key for each currency.

Distributed Orderbook (DOB)

An ***Orderbook*** is an electronic list of buy-and-sell orders of specific security or financial instruments, organized by price level. The Orderbook lists the number of asset units being bid or offered at each price point, or market depth. It also identifies the market participants behind the buy-and-sell orders, although some might choose to remain anonymous. The Orderbook is dynamic and constantly updating in real time throughout the day.

Archived copy · cryp2nova.com

The approach to the construction of the blockchain exchanges (e.g. Binance, Mt. Gox, Bitfinex etc.) has been copied from fiat operators, like NASDAQ, NYSE, LSE, ending up with failures happening one after another.

Besides the well-known custody-centric fails, market manipulation through falsification and distortion of market data, unfortunately, happens as well. Howbeit, blockchain establishes new forms of financial products. Adopting new opportunities this technology brings is the most guaranteed way for promising and smart projects to skyrocket. One of the undervalued possibilities is the creation of a completely decentralized and transparent Orderbook.

Atomic Orderbook implementation

Distributed Orderbook (DOB) is a way to represent market offers in a decentralized manner, in accordance with the spirit of blockchain industry.

Atomic DOB is based on a ***BitTorrent protocol***. BitTorrent is a communication protocol for peer-to-peer file sharing ("P2P") which is used to distribute data and electronic files over the Internet.

BitTorrent is one of the most common protocols for transferring large files, such as digital video files containing TV shows or video clips or digital audio files containing songs. Peer-to-peer networks have been estimated to collectively account for approximately 43% to 70% of all Internet traffic (depending on location) as of February 2009. In November 2004, BitTorrent was responsible for 25% of all Internet traffic. As of February 2013, BitTorrent was responsible for 3.35% of all worldwide bandwidth, more than half of the 6% of total bandwidth dedicated to file sharing.

To anticipate a better understanding of how Atomic Swaps will work within the Atomic Wallet we should reveal major principles of the Distributed Orderbook and order matching. In terms of Atomic Wallet Orderbook an order possesses following characteristics:

1. **An *order* is an offer, not a commitment**. By creating an order, customer posts an ad for a future ***trade***. When the time of the trade comes, the customer can avoid processing the transaction if he/she desires so. Maker faces a moderate decrease of his/her current rating in case of rejecting to trade against hi/her own orders.
2. **Order placement doesn't block customers' funds**. Unless the orders have matched between two traders, funds are not being moved. Only after two traders confirm a trade the funds actually move from their wallets.
3. **An order can be executed with multiple trades**. An order can be filled with several trades with an unbounded range of traders (***takers***). Until the order is canceled it stays active in the orderbook and available for trade.
4. **Offline traders cannot trade**. Atomic Swaps require both customer and wallet to be online in order to be processed. In case a customer gets off the Internet or closes wallet application the order becomes invisible for other traders. After the connection is established back the order automatically gets back to demonstration at the orderbook. *In future the protocol will allow offline trading but this function is out of scope for current document*.
5. **Execution is a manual operation**. Atomic Swap technology is known to be the best among others because even within the exchange customer retains control over the private keys. *In*

Archived copy · cryp2nova.com

future the protocol will allow offline trading but this function is out of scope for current document.

6. **Maker is free to reject execution.** Before the start of the swap, maker can change his/her mind for various reasons, such as the amount of trade being less/more than desired or the rating of the counterparty being below the ***maker's*** expectation. The only shortcoming that maker faces is a moderate decrease of his/her current rating.

Order acceptance to the DOB mempool

Atomic DOB is an immutable and decentralized solution created to transmit information about the exchange orders among Atomic wallet users.

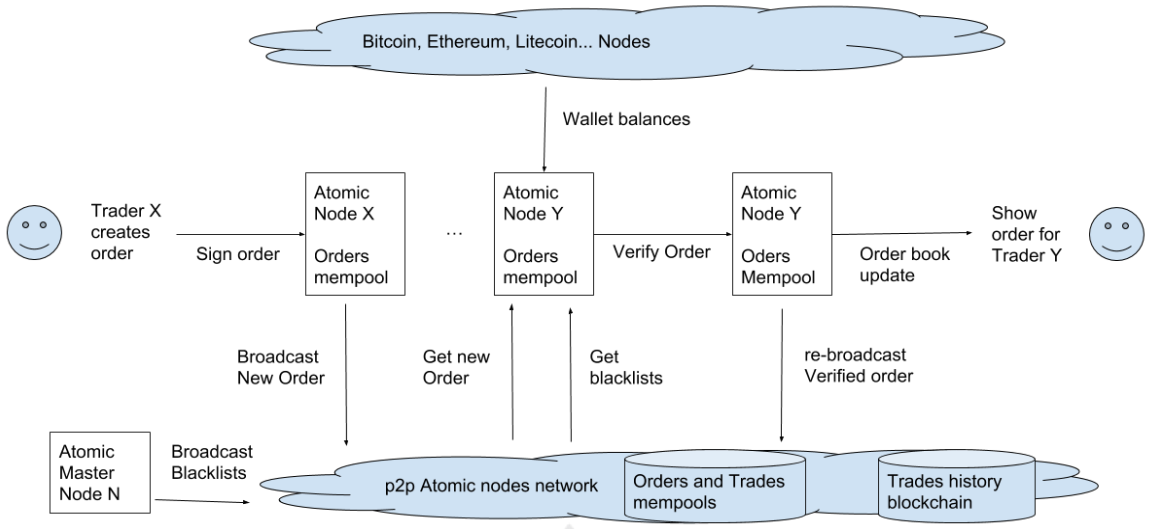
DOB is maintained by the Atomic Wallet clients serving as nodes in the distributed network. When an order is transmitted to the network it first gets verified by all of the Atomic Wallet clients available. All the clients validate following information before submitting it to the ***mempool***:

1. **Data consistency**. All the data should be submitted to the mempool in pre-described by the orderbook protocol format and shouldn't contain ***injections*** nor interfere the dependencies in the orderbook that can appear.
2. **Order Legitimity**. Active nodes from the network analyse the following parameters:
    a. Accordance of the Order ***digital signature*** to the Makers public address in the blockchain appointed in the order
    b. Availability of the amount on the wallet address appointed in the order. Maker cannot stake more than he/she has on the wallet
    c. Absence of the conflict between newly created order and the previously created orders with the same signature
3. **Blacklist screening**. The absence of the orders address in the blacklist of spamming or rarely finishing trades actors.

After necessary checks are processed Atomic Wallet adds Order to the DOB and starts ***seeding*** it with the neighbouring Atomic Wallets.

CRYP2NOVA

Archived copy · cryp2nova.com



Img 1. Order acceptance to the DOB mempool

When an Atomic Wallet receives a new valid block (see Trades history blockchain storage), it removes all the orders executed within the previous time and contained in this block from the mempool.

DOB anti spam and fraud protection

In many ways DOB mempool works as the widely known and high-load production verified Bitcoin Mempool and has a very similar realisation. This ensures us in a high level of attack resistance of the solution and a very unlikely possibility of spam and fraud within the network.

However for the first period of operation Atomic Wallet team leaves itself the right to blacklist fraudulent and spamming actors from the network by blacklisting addresses or public keys by signatures. Centralized nature of such verification should not and will not last for a long time. The complete decentralization of the DOB blacklisting will be finished with the release of decentralized ratings system planned in the Roadmap.

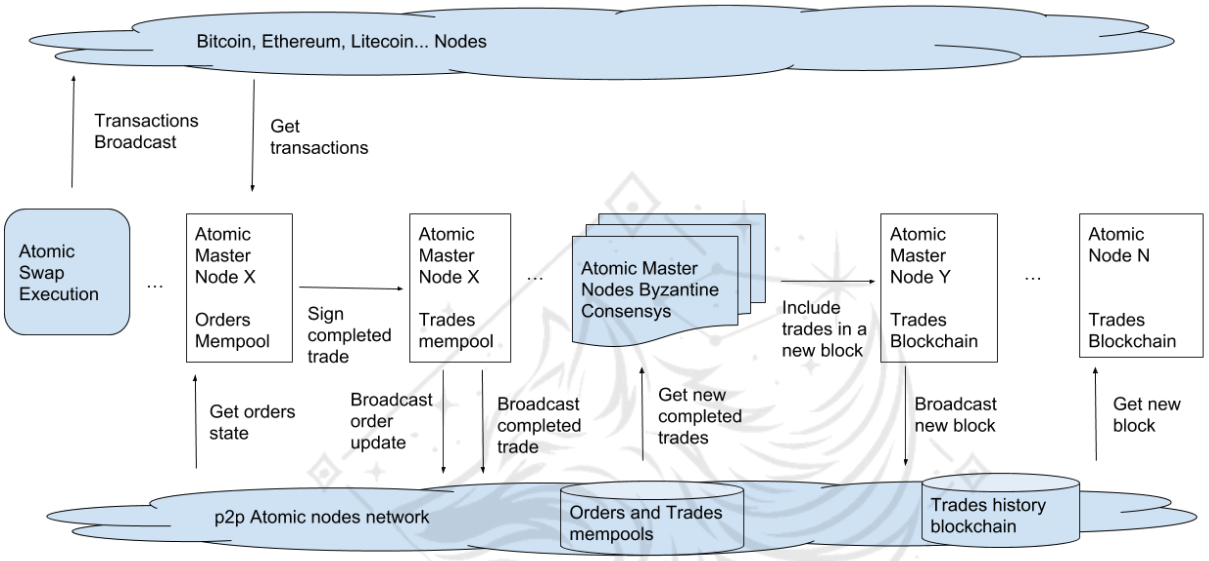
Trades history blockchain storage

Atomic Wallet will use a custom-built ***Byzantine consensus*** algorithm that keeps DOB historical data safe without needing to “mine” blocks, even in the case of a situation where your nodes malfunction or become susceptible to the actions of bad actors. This feature also makes it near impossible for a bad actor to add incorrect data or change the history in Atomic Wallet Blockchain. In case of many compromised nodes, Atomic Blockchain still maintains its fundamental security properties, protecting data. Atomic Wallet Blockchain will update immediately with the addition of every new block.

Archived copy · cryp2nova.com

Atomic Wallet will gather successful and unsuccessful trades into blocks; the whole block is approved atomically. Each trade is executed separately from the Atomic Wallet Blockchain. Atomic Wallet Blockchain will be used only in the purpose of storing historical data.

As every block includes the hash of the previous block, it is impossible to change one block without the appropriate changes to each of the following blocks. This ensures immutability of the trade log; once a trade is committed, it cannot be retroactively modified or evicted from the log. Similarly, it is impossible to insert a trade in the middle of the log



Img 2. Trades history blockchain storage

Atomic Wallet uses a custom modification of Byzantine fault tolerant consensus to guarantee that in any time there is one agreed version of the blockchain. It is assumed that the environment is decentralized, i.e., any node is allowed to fail or be compromised. Consensus is *authenticated*; consensus validators are identified with the help of public-key cryptography.
To generate a new block and vote upon it, a 3-phase approach is used.

- The consensus algorithm is divided into rounds, the beginning of which is determined by each ***validator*** based on its local clock. For every round, there is a predefined leader validator, which is determined based on the round number, blockchain height and other information from the blockchain state. The leader creates a block proposal and sends it to other validators
- Other validators check the proposal, and if it is correct, vote for it by broadcasting prevote messages to the validators
- If a validator collects prevote messages for the same proposal from a supermajority of validators, it executes transactions in the proposal, creates a precommit message with the resulting data storage state and broadcasts it to the validators
- Finally, if a validator receives precommits from a supermajority of validators for the same proposal, the proposal becomes a new block and is committed to the local storage of the validator

Archived copy · cryp2nova.com

Historical data from the blockchain will be used in the purpose of public actors rating system. Public actor rating will be counted on the basis of the number of successfully finished exchanges. Data is collected with the help of ***blockchain oracles*** from the networks where Atomic Swaps are processed.

Atomic Swaps

A cross-chain is an exchange of cryptocurrencies between users. Basically, party A sends Coin A to party B's Coin B address via blockchain, while party B does the same with Coin B. These actions happen independently on parallel blockchains, in a one-way fashion. Such setup raises the possibility of either of the parties never honoring his/her end of an agreement. One of the ways to solve this issue is involvement of a trusted third party. An atomic cross-chain swap, on the other hand, solves this problem without the need for a third party.

Atomic swaps require each party to arrange a transaction contract. The contracts contain an ***output*** spendable by the the opposite party, but the rules required to collect is are different for each party involved.

Atomic Swap technology

The first party (called the initiator) wishes to trade Coin B for Coin A with the other party (called the participant). The initiator allocates the intended amount of Coin B to a contract and generates a "secret". The secret will later allow the participant to collect the contract output. Until he/she learns the secret, the participant is unable to spend from the initiator's Coin B contract.

The participant creates a contract on the Coin A blockchain in a similar to the initiator fashion. To create the contract, the participant requires a cryptographic hash of the initiator's secret. The initiator could not access this contract without revealing the secret to the participant.

After both parties created their contract, neither of them can collect their coins back until the alloted time expires. The initiator redeems the participant's contract, thereby revealing the secret to the participant. The latter redeems the former's contract using the secret extracted from him/her.

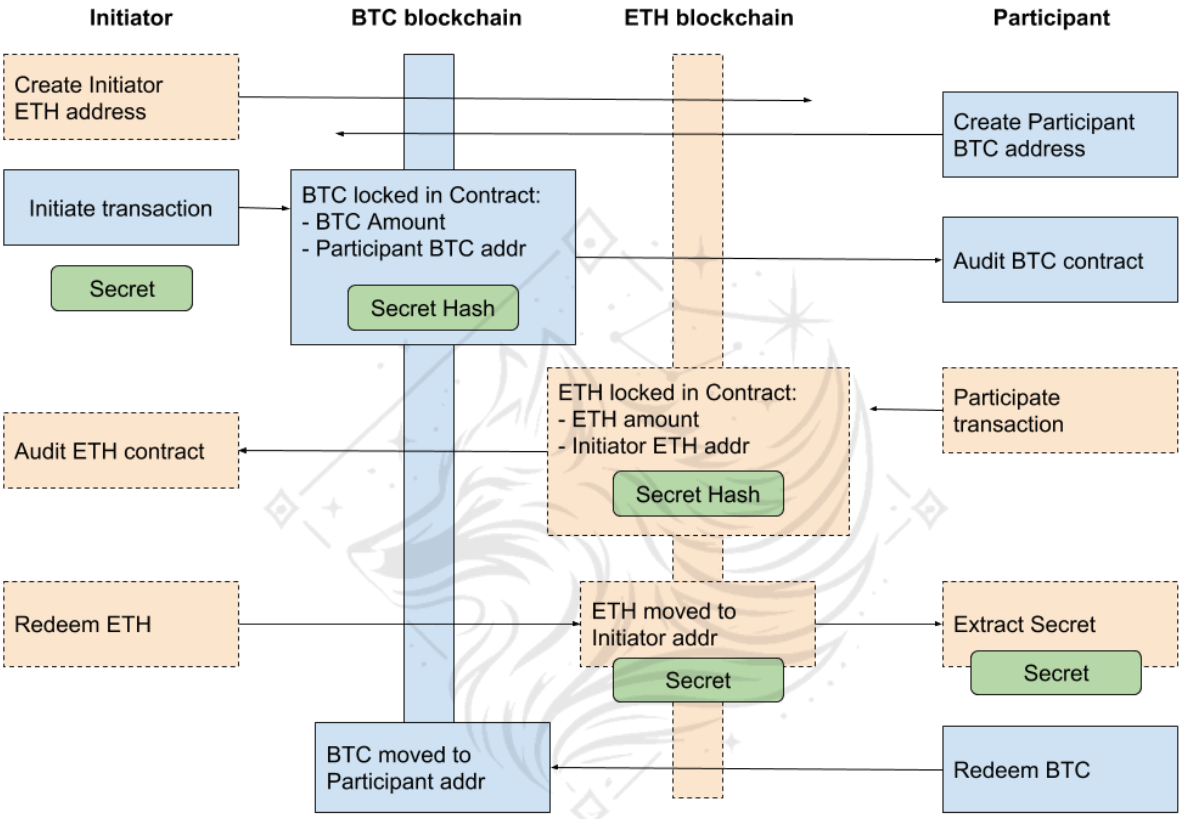
When a certain period of time (typically 1 hour) expires and the participant did not redeem the contract output, it is refunded back to the initiator's wallet. The participant's contract can also be refunded back to the participant, but only after half the period of time that the initiator is required to wait before their contract can be refunded (typically 2 hours).

The initiator can also trade Coin A for Coin B and the procedure will be the same, but with each step performed in the opposite direction on another blockchain.

This procedure is considered atomic (i.e. with a timeout) since it gives each party at least 24 hours to redeem the coins from the opposite blockchain before a refund can be performed.

Archived copy · cryp2nova.com

The image below provides a visual of the steps each party performs and the transfer of data between each party:



Img 3. Atomic Swap execution process

Atomic Wallet Swap implementation

Atomic Wallet has implemented the best solution on the market for both Atomic Swaps and Distributed Orderbook. The process of an order creation and execution is designed as follows:

1. Customer A creates an order for the trade and signs it with the private key. The order inherits following parameters:
   Currency pair. The currency desired to receive and the currency desired to be sold.
   Size. Order size is not to be limited by trading lots but will have a minimum value that will cover current ***network commissions*** for processing a swap.
   Price. The price that is desired to process the trade with.
   Price type. Price can be of a fixed (set in stone) or float type (following the current market rate).

Archived copy · cryp2nova.com

Price margin (optional). This specification is used for the float type prices. A margin is the amount to be put above or below the ***market price***.
Minimal amount (optional). The standard number of units in a trading security. Minimal amount represents the minimal quantity of a blockchain asset as set out by the maker. Minimal amounts are designed to help crypto users with large sums, do so by refraining from performing many small trades within one order.
Wallet address. Public address of the cryptocurrency corresponding to the blockchain asset to be sold. Wallet should contain no less than the amount of the active orders created by this customer.
Signature. To demonstrate the authenticity of digital messages sent to the Atomic Wallet environment (Orderbook and Following order execution), Atomic Wallet uses digital signatures. A valid digital signature gives a recipient a reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message, and that the message was not altered in transit. The Atomic mnemonic seed is used as the private key for signing the messages. With Atomic Wallet signature customers can be identified and rated as more/less efficient partners for Swaps without limiting their privacy and anonymity.

2. The order is sent to all Atomic Wallet users via the proposal of an update to the file distributed and synced among all users.
3. One of the Verification nodes checks the order for legitimacy in terms of Atomic Wallet environment. Verification node creates an updated version of the DOB file wiping off the closed orders and adding new ones.
4. The new version of the DOB file is synchronized along the network once in a minute.
5. Customer B picks the order from the orderbook and decides to trade against it. Customer B indicates the amount he would like to exchange.
6. Customer ’s Atomic Wallet sends a request to the Customer A’s Atomic Wallet. The request for exchange contains the following parameters:
   Amount. The sum desired for a trade.
   Wallet address. The public address in blockchain B which Customer B possesses within the Atomic Wallet.
   Signature. Keys signed by the Customer B.
7. Customer A’s Atomic Wallet confirms the trade after processing several checks:
   a. Sufficiency of the funds on the Customer B’s wallet
   b. Accordance of the amount desired to trade with the order
8. Customer A confirms the trade with the password
9. Customer B’s wallet commences the swap process
   …
   A detailed description of Atomic Swap process can be found at Atomic Swaps paragraph.
   …
10. Customers receive funds to the corresponding addresses.

The implementation of both Atomic Wallet orderbook and the matching procedure requires no blockchain consensus algorithm since the DOB and matching are not built as smart-contracts or onchain solutions. DOB is a distributed file and matching happens on a peer-to-peer basis.

Archived copy · cryp2nova.com

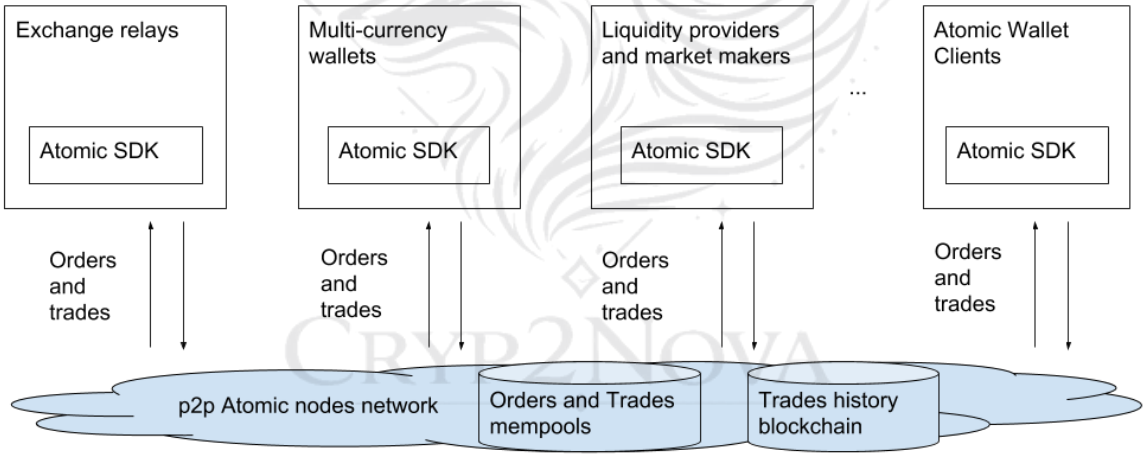
Atomic SDK

Developing even simple applications working with blockchains takes time and money. Creating complex, highly-functional distributed blockchain apps can take a number of highly skilled blockchain developers, thousands of hours for RnD which comes out in millions of USD costs. Following the promise of building a completely decentralized solution Atomic Wallet team will provide the following:

1. Availability to develop applications working with Atomic Wallet DOB and Atomic Swaps code. The protocols will be open and available for integration.
2. Developers SDK to smoothly integrate Atomic Wallet exchange functionality without having to mess with complicated protocols. Atomic Wallet will provide a solution to organizations looking to quickly create and deploy highly functional, custom apps to manage cryptocurrencies with Atomic Software Development Kit (SDK).

Atomic SDK will support following functions:

1. Create order and deploy it to the DOB
2. Confirm order execution
3. Receive order execution status
4. Get list of available orders from the orderbook



Img 4. Atomic SDK ecosystem

With the Atomic SDK, the “heavy lifting” has been done, allowing 3rd party developers to focus resources on figuring out the market needs, building successful user interfaces without worrying about how to make it happen.

Archived copy · cryp2nova.com

Additional functionality

Atomic Wallet adopts various means of exchange. For some occasions, customers might be willing to use non-atomic exchange functionality. Being a custody-free solution, Atomic Wallet implements only instant exchange options. For the convenience of Atomic Wallet users, two instant exchange options are implemented:

1. Shapeshift. ShapeShift is the fastest, most private, and most convenient way to swap digital currencies, with the exchange rate always remaining competitive. Following the Atomic Wallet community vote, ShapeShift was selected as a default option for instant exchanges.
2. Changelly. Popular cryptocurrency exchange providing the ability to instantly and seamlessly exchange over 90 altcoins at the best market rate or to buy them using a bank card. Operating since 2015, Changelly has attracted over 1.5M registered users from around the world. Currently, the service processes more than 15K transactions daily with a monthly turnover of around 60K BTC.
3. Fiat options. Fiat options to be provided to the customers in cooperation with partner services. Integration will be carried in a seamless smooth manner. Atomic will not process fiat operations himself following “do not touch fiat” policy. Early commitments from the partners already received and will be unveiled prior to the public crowdsale. Following options are planned for the implementation: payment cards acceptance, bank wires acceptance, bank wire withdrawals.

Immutability and decentralization

Blockchains are designed to be immutable and decentralized. Atomic Wallet team believes products designed for cryptocurrency assets should be immutable and decentralized as well.
That is why it’s important for Atomic Wallet to be a serverless, immutable solution in all the aspects. All parts of the system operate in a decentralized manner and are not controlled by any company or party:

1. **Atomic Wallet Distribution.** Application is distributed over the BitTorrent network and is supported by the customers.
2. **Asset Management.** Cryptocurrency private keys are stored on the customer side and are not transferred to the server.
3. **Transaction creation.** Transaction is created on the customer-side. The client application handles all the necessary cryptography and transmits it to the node. Customer can appoint any node with open RPC API.
4. **Transaction History.** Transaction history is retrieved from blockchain explorers over the commonly used API requests. Customer can point the block explorer he/she trusts most or deploy own one and use it as source of transaction history.
5. **Orderbook.** Atomic Wallet utilizes own Distributed Orderbook technology. Atomic DOB is based on a BitTorrent protocol and cannot be seized or stopped. DOB is distributed among all the online wallets.
6. **Order execution**. Order execution is processed peer-to-peer and blockchain based. No third party is involved in the transaction processing. The transaction is custody and possible intervention free.

Archived copy · cryp2nova.com

Atomic Wallet ecosystem

The success of the Atomic Wallet is contingent on the participation of a variety of different users. We will briefly give an overview of the key roles that participants can play in the Atomic ecosystem.

1. **Traders**. End-users that hold, convert and transfer blockchain assets.
2. **Blockchain Assets Issuers**. People, companies, communities, organizations or foundations that issue new Smart Tokens, configuring the initial supply, price, CW, and managing the initial issuance of tokens. This also includes creators of Relay Tokens, which can connect any existing ***ERC20 tokens*** to the network.
3. **Cryptowhales**. Traders with the amounts of assets too big to be normally adopted by openmarkets and willing to perform personalized or non-personalized risk-free ***OTC deals***.
4. **Arbitrageurs.** Traders that monitor the Decentralized Orderbook for prices that are inconsistent with an external exchange, and then restore price consistency through arbitrage. Arbitrageurs are organically incentivized to keep prices consistent and hence are important participants in the Atomic ecosystem.
5. **3rd party developers**. Companies or individuals creating services utilizing Atomic Wallet DOB and Atomic Swap code. Developers can build specialized Atomic Wallets, exchange Relays, Decentralized OTC platforms or implement part of the Atomic functionality in their existing services.

CRYP2NOVA

Archived copy · cryp2nova.com

Platforms

Atomic Wallet team is focused on bringing truly decentralized experience to all the customers on all the platforms. Atomic Wallet technology is created with the idea of omni-channel product which customer can access from any device he\she has.
Atomic Wallet supports the following platforms at the moment:

- Microsoft Windows
- MacOS
- Ubuntu
- Debian
- Fedora

Within the development further platforms are to be supported as well:
Web

- Javascript web based application

Mobile

- iOS
- Android

Browser plugin

- Chrome
- FireFox

Competitive analysis

Feature	Bitfinex	0x	Etherdelta	Exodus	Altcoin.io	Airswap.io	BarterDEX	Atomic
Exchange assets	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Immutable solution	No	No	No	Yes	No	No	?	Yes
Private key on device	No	Yes	No	Yes	?	Yes	Yes	Yes
Cross chain Atomic swap	No	No	No	No	Yes	No	Yes	Yes
Decentralised orderbook	No	No	Yes	No	Yes	No	Yes	Yes
User friendly interface	Yes	No	Yes	Yes	Yes	Yes	No	Yes
Banking card acceptance	No	No	No	No	No	No	No	Yes
Instant centralized exchange	Yes	No	No	Yes	No	No	No	Yes

Archived copy · cryp2nova.com

UI Preview

Atomic Wallet is created to make day-to-day cryptocurrency usage more secure while bringing the best customer experience to our clients. Following are the example screenshots from the interface of the Atomic Wallet Alfa Version.

1. Home screen (Wallet)



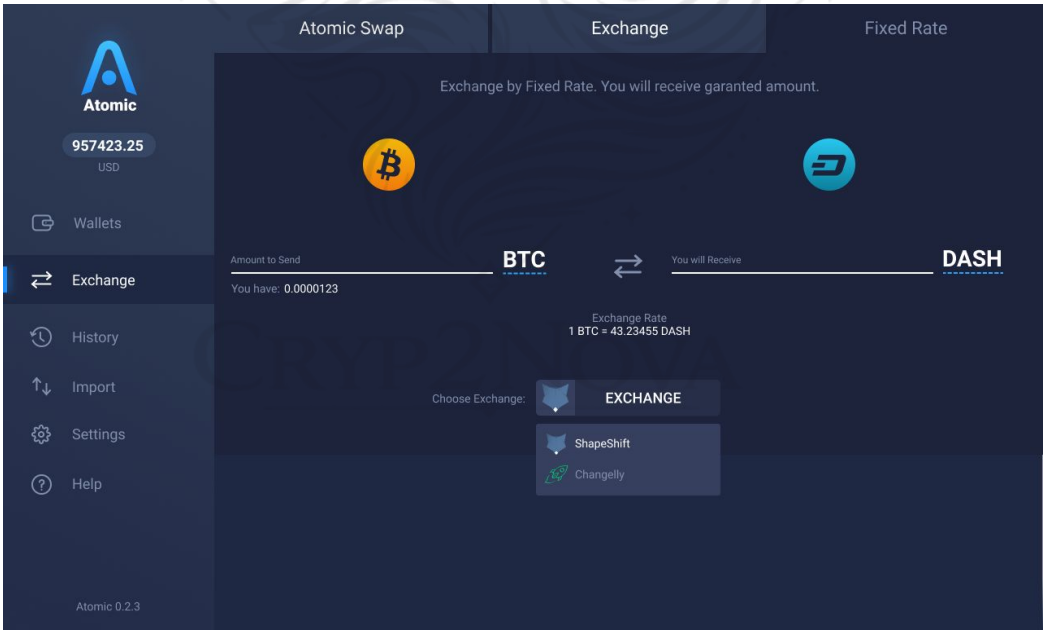
Img 5. Atomic Wallet User Interface. Wallets overview.

Archived copy · cryp2nova.com



Img 6. Atomic Wallet User Interface. Blockchain assets display settings.

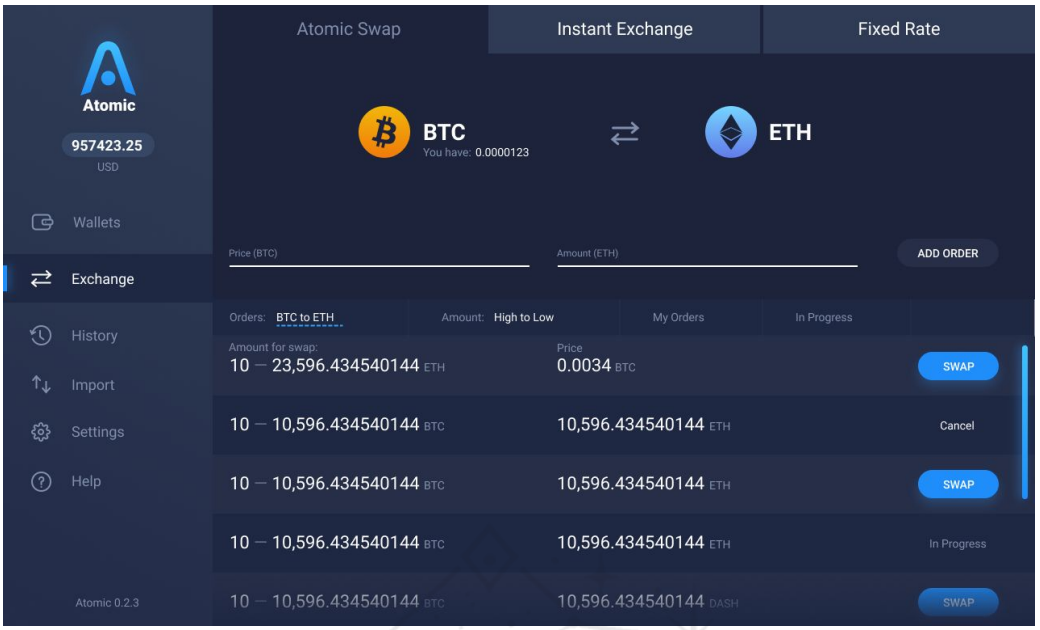
2. Exchange.



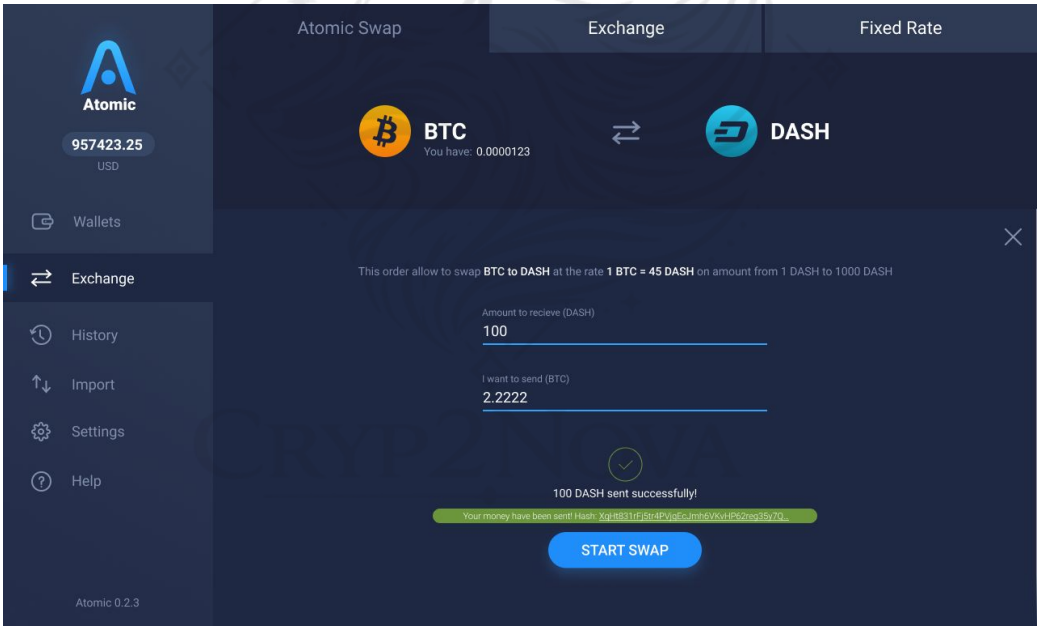
Img 7. Fixed rate exchange via partnering instant exchange service

Archived copy · cryp2nova.com

3. Exchange. Performing an Atomic Swap



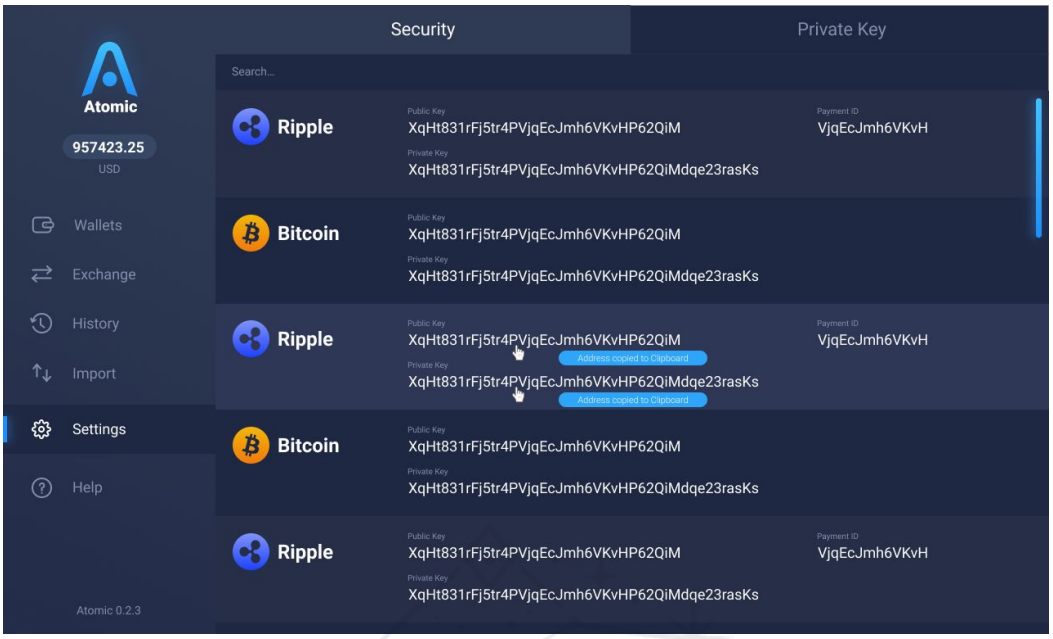
Img 8. Atomic Wallet Distributed Orderbook display.



Img 9. Takers execution process.

Archived copy · cryp2nova.com

4. Security.



Img 10. Private key management

CRYP2NOVA

Archived copy · cryp2nova.com

Roadmap

April 2018 - Alpha release

- Ethereum and Bitcoin asset management
- 200+ token assets support
- Integrated instant exchange service

May 2018 - Beta Version release

- Litecoin asset management
- First pair for Atomic swaps
- Distributed Orderbook over torrent protocol v. 1.0

June 2018

- ERC20 token swaps
- Lightning network implementation
- Multi-language UI
- 26 new assets in the wallet
- 4 new assets in the atomic exchange

July 2018

- Crypto against fiat conversion options integration
- 8 new assets in the wallet
- 4 new assets in the atomic exchange
- Atomic exchange users ratings
- Finish of the token sale
- Custom nodes and block explorers usage

August 2018

- Web wallet
- Mobile wallet for Android
- Mobile wallet for iOS
- 8 new assets in the wallet
- 4 new assets in the atomic exchange

September 2018

- User chat in the wallet (trollbox)
- Hardware wallet integration (Trezor, Ledger)
- 8 new assets in the wallet
- 4 new assets in the atomic exchange

October 2018

- dApps browser
- 8 new assets in the wallet
- 4 new assets in the atomic exchange

Archived copy · cryp2nova.com

Current stage

As of now, Atomic Wallet is a functioning ecosystem. For an Alpha version our team has delivered a Desktop application supporting:

1. Asset management for BTC, ETH, DCR, LTC and 200+ ERC20 tokens
2. Main net atomic swap exchange (https://twitter.com/atomicwallet/status/964207905686749184)
3. Import, export of the private keys
4. Exchange assets via instant exchange services (Changelly, ShapeShift)
5. Backup with 12 words passphrase

The product is available for download at www.atomicwallet.io.

Archived copy · cryp2nova.com

Atomic token

Atomic Wallet will issue own token, called the AWC (Atomic Wallet Coin). A strict limit of 100M AWC will be created, never to be increased. AWC will run natively on the Ethereum blockchain with ERC20.

Type: ERC20 Token
Ticker: AWC
Full name: Atomic Wallet Coin
Decimals: 8
Total supply: 100,000,000 AWC
Open Contract Source Code
Token economy and premises to following price growth is described in a special charter.

Initial Coin Offering (ICO)

Token issuing

A ***smart contract*** based on the Ethereum network is written for the effective implementation of the Atomic ICO project. On the day of the ICO launch, the Atomic team will publish the smart contract, which will initialize the issuing of AWC-tokens based on ethereum in accordance with the ERC20 standard.

The contract will support following functionality:

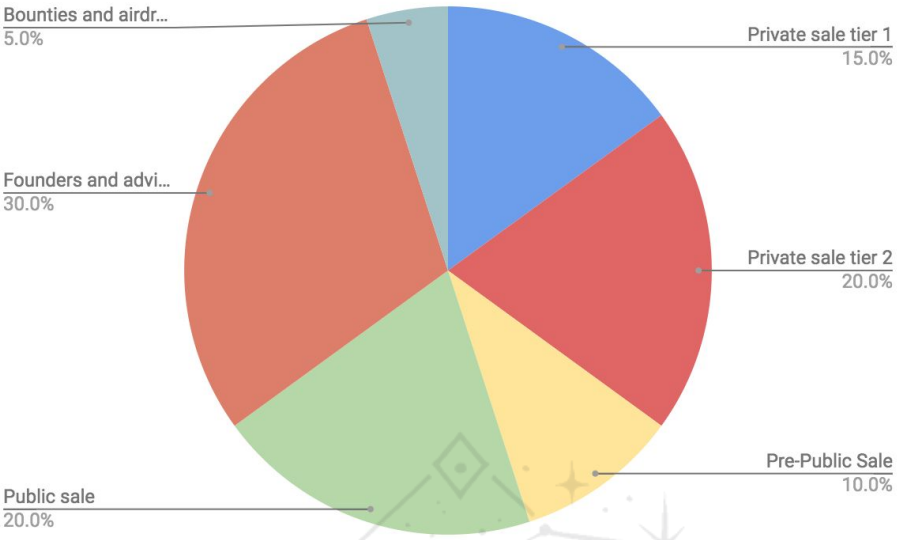
1. Crowdsale management
2. AWC tokens issuance (standart ERC20)
3. AWC tokens transmittance

The main function of the crowdsale part of the contract is to regulate the price of the token. Additionally, this smart contract will keep records of the AWC-tokens provision to investors' community and to founders.

The source code of the smart contract for the release of AWC-tokens can be found here: https://github.com/Atomicwallet.

Archived copy · cryp2nova.com

Token allocation



Img 11. Token allocation plan pie-chart

Round	Stage	Tokens	Percent	Token price	Total
1	Private sale tier 1	35,000,000	15%	TBD	
2	Private sale tier 2	30,000,000	20%		
3	Pre-Public Sale	30,000,000	10%		
4	Public sale	20,000,000	20%		
5	Founders and advisors	30,000,000	30%		
6	Bounties and airdros	5,000,000	5%		

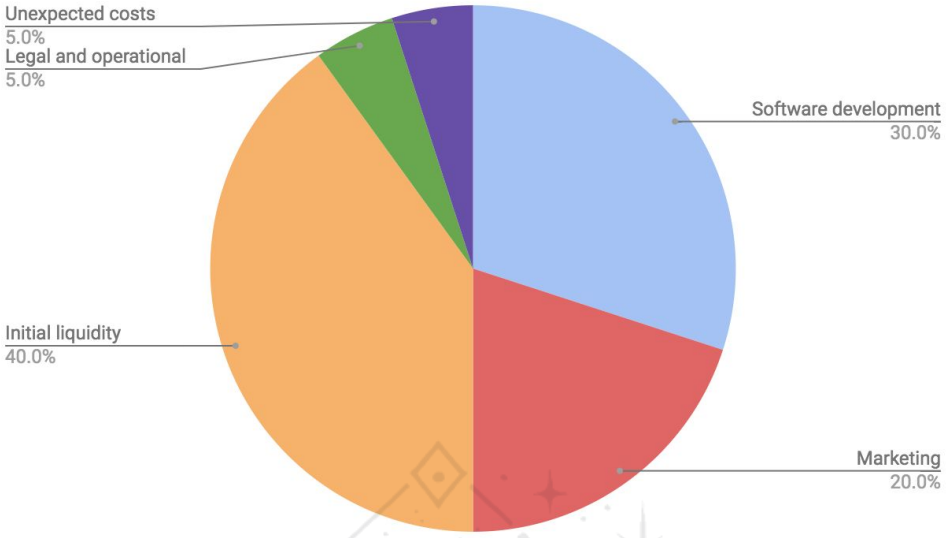
Crowdfunding goals

The following amounts are alloted for meeting intended goals, lowering possible risks, as well as filling market with liquidity.

A minimum of $5,000,000 is required for the successful implementation of the Atomic project. The maximum amount upon which any emissions of tokens will terminate is TBD.

Archived copy · cryp2nova.com

Budget allocation



Img 12. Budget allocation plan pie-chart

The budget is planned to be apportioned in the following way:

- Team: 30% of budget. This amount of financing allows for the rollout of the AWC solution, including the necessary adjustments to and development of the existing service.
- Marketing: 30% of budget. Marketing will focus on expanding awareness and adoption of the Atomic and the Atomic Swaps technology among users and companies. This also includes the growth and maintenance of the world-wide community.
- Initial liquidity: 30%. This financing part is intended for the initial market making program. The funds left after the program ends will be transferred to repurchase AWC-tokens from the market.
- Legal and Operational: 5% of budget. Consists of AWC legal, security, accounting and other associated administration costs.
- Contingency: 5% of budget. A set-aside for unforeseen costs.

Private sale

Prior to the launch of the AWC tokens release, we will invite potential investors to pass the Investor Questionnaire consisting of the following items:

1. Description of the investor's objectives, which they hope to achieve by taking part in the Atomic project
2. Information on the source of invested funds
3. Contacts
4. Amount of planned investments

Based on the acquired data, a White List will be compiled, consisting of persons allowed to invest.

Atomic Wallet is open to all investors ready to contribute at least $100,000.

Archived copy · cryp2nova.com

In order to prevent the possible centralization of tokens in single hands, the maximum investment threshold of $1 million has been determined.

Token allocation between Private and Public Sales is a subject to change in case of significant market changes and drastic increase/decrease of interest from potential investors. Prior to changes in Token allocation Atomic Wallet team will initiate discussion with private round investors.

Investing in Atomic Wallet will be available only to individuals and companies who have passed ***KYC procedure***.

Public sale

The crowdsale will start on October 1, 2018.

The maximum possible number of issued tokens is 100,000,000. This amount of emission is possible only on condition that all investments are collected to the maximum allowable amounts of 1,000,000, and a hard cap is reached.

The minimum number of tokens to be issued is set to 25,000,000. This amount of emission is possible only on condition that all investments are collected with minimum allowable amounts of 100,000, and the minimum amount necessary for the development of the project is achieved.

Due to the instability of the ETH with respect to USD, the price for one AWC-token in ETH will be refined several days prior the ICO. The final starting price will be determined on the day of the ICO.

Atomic Wallet team preserves it's right to skip crowdsale stage in case necessary funds are raised on the private sale stage. Final solution regarding crowdsale to be published here: https://github.com/Atomicwallet.

CRYP2NOVA

Archived copy · cryp2nova.com

Community incentives

Client Airdrops

Early adopters of Atomic Wallet will be granted with the AWC tokens. To receive tokens, first customers should:

1. Subscribe for the waiting list to become a beta tester
2. Receive the magnet link for download
3. Download the application and install it on the computer
4. Create a Wallet and transfer funds on it
5. Claim tokens by leaving an e-mail in the application form
6. Wait for the token distribution dates (on the end of each week)
7. Receive tokens on the same address used in Atomic Wallet

Customer airdrops will cultivate the amount of first users and help Atomic Wallet team create active token advocating community.

Tokens allocated to the airdrop program: **2%**

Bounties

One of the key goals of Atomic Wallet marketing strategy is to ensure as much market penetration as possible. This point is crucial due to the existence of the “chicken and egg” problem considering the establishment of new financial markets.

By doing a bounty campaign, Atomic Wallet strives to achieve a number of goals, such as brand-awareness, testing, development community involvement, security improvements, orderbook fulfillment. Bounty program and Airdrops are an integral part of a marketing and promotional strategy for Atomic Wallet.

Bounty hunters are required to join the Atomic Wallet Telegram chat.

The bounty program is divided into the pre-sale and post-sale periods,mostly for the convenience of the crowdsale investors as well as for the preservation of token distribution transparency .

Pre-Sale bounty

Pre-sale bounty starts on 1st June, together with the launch of private Alpha testing, and finishes a week before the public crowdsale ends. Pre-sale bounty program will include the following tracks:

1. **Atomic Swap Evangelism**
   Atomic Wallet team will be looking for people who believe in and are willing to tell the world about the Atomic Swaps technology and to promote our decentralized solutions. Evangelists’ task is spreading the word of our product around the globe. Evangelists will be chosen on the basis of a contest to participate in which candidates should apply on the Atomic Wallet website with a motivation letter and their vision of the future work. The candidates will be assessed in accordance with their knowledge in cryptocurrencies, their passion and drive,

Archived copy · cryp2nova.com

community prominence, location and native language. Successful candidates will receive monthly compensation for their work in AWC tokens.
Tokens allocated to program: **0.3%**

2. **Currency list enhancement**
   Atomic Wallet has an open API for currency integration. Scope of works for adding a new cryptocurrency normally includes two major tasks: integration of a currency into the wallet and development of Atomic Swap contract and client library.
   To receive the reward developer should follow the steps:
   a. Pick up a currency from the list on Atomic Wallet website
   b. Develop an integration of a currency into the wallet or develop an Atomic Swap contract code with client library
   c. Create pull request to the Atomic Wallet github repository
   d. Successfully pass Atomic Wallet employees code review and testing
   e. Wait for the development to be released into production
   f. Claim the reward

   Tokens allocated to program: **0.6%**
3. **Ethical hacking and vulnerability scan**
   Ethical hacking or penetration testing will be carried on Atomic Wallet systems with the permission of Atomic Wallet team in order to determine its vulnerabilities and weaknesses. It is an essential process of testing and validating information security posture and maturity. The results of ethical hacking will be used to proceed with preventive and corrective countermeasures that can mitigate the risk of a cyber attack.
   To receive the reward ethical hacker should:
   a. Report the found vulnerability to the Atomic Wallet team over an e-mail.
   b. Do not enclose publicly or in any other way the vulnerability to third parties
   c. Wait for the development mitigating the vulnerability to be released into production
   d. Claim the reward

   Tokens allocated to program: **0.3%**
4. **Content production**
   Audio, Video and Text content will be granted with bounties in case they meet several requirements:
   a. Content is unique
   b. Content is created for Atomic Wallet only
   c. Content has received minimal traction

   Content can be submitted in any language. Non-English content will be warmly welcomed.
   Tokens allocated to program: **1.5%**
5. **Bug bounty**
   Atomic Wallet team will be looking for bug reports clearly and concisely identifying problematic issues with the cryptocurrency software or platform.
   To receive the reward tester should:
   a. Be a part of the testing team
   b. Report the found bug to the Atomic Wallet team over an e-mail.
   c. Do not enclose publicly or in any other way the bug to third parties
   d. Wait for the development mitigating the bug to be released into production

Archived copy · cryp2nova.com

e. Claim the reward.

Tokens allocated to program: **0.3%**

Post-Sale Bounty

After the token sale has ended, all bounties will still apply. However, the amount of the compensation can change with time. The funds to support bounties will be allocated from the crowdfunding budget in accordance with the expenditure.

Post ICO token circulation

AWC tokens on exchanges

Next stage will start in a month after the ICO. The AWC tokens will become "transferable", meaning that the holder can utilize them.

Token economy

AWC token will be used to pay for different fees on Atomic Wallet platform, including but not limited to:

- Listing new assets in Atomic Wallet
  Each cryptocurrency, foundation or token will be able to purchase integration within the Atomic Wallet for the AWC-tokens. The price of integration will be 100,000 AWC-tokens.
- Listing new assets in Atomic swap exchange
  Each cryptocurrency, foundation or token will be able to purchase integration within the Atomic Wallet swap exchange market for the AWC-tokens. The price of integration will be 150,000 AWC-tokens.
- Highlights and featurings in Atomic Wallet interfaces
  Each cryptocurrency, foundation or token will be able to purchase promotion within the Atomic Wallet GUI for the AWC-tokens. The price of integration will be determined in each particular case AWC-tokens.
- Atomic swap usage
  For the swaps exceeding 1 BTC since the end of 4Q 2018 users will be obliged to have at least 0.5 AWC token on the same Ethereum address with the one used by the Atomic Wallet.
- Increasing atomic swap rating
  Each customer will receive a public rating which will influence his/her position in Atomic Wallet Orderbook GUI. The rating will be determined on the basis of successfully completed swaps and the volume of trades. To boost his/her experience customer will be able to increase rating by paying in AWC-tokens. The rating mechanics will be announced in 3Q 2018.

All services paid in AWC token will be sold with a significant discount or sold only for AWC tokens. Tokens received for the abovementioned services will be burned until we destroy 50% of all the AWC.

Archived copy · cryp2nova.com

Team vesting plan

We have a solid team led by Paul Sokolov and Konstantin Gladych, with both traditional fintech and cryptocurrency experience. We have a track record of successful startups under our belt. To preserve team dedication to the project we developed a vesting plan for our key team members:

- Initial release - 25%
- After 1 year - 25%
- After 2 year - 25%
- After 3 year - 25%

We believe that the plan specified above will help the team successfully drive the Atomic Wallet product adoption and AWC token price.

CRYP2NOVA

Archived copy · cryp2nova.com

Team

Business

- **Konstantin Gladych**, CEO, PhD in data science with 3 years solid experience in blockchain and cryptocurrencies, 10 years in IT. Konstantin is well-known as the co-founder and ex-CEO of https://changelly.com/, biggest cryptocurrency instant exchange with over 2 millions active customers monthly and $0.5bln in monthly turnover. Konstantins interests are: decentralization, custody-free solutions, p2p exchangers. https://www.linkedin.com/in/gladkos/, https://twitter.com/gladkos

- **Paul Sokolov**, Chief product officer, has three years experience in blockchain, 10 years in fintech, 2 years of which in COO position at top-20 cryptocurrency exchange. Certified banking cards security and business expert. Launched over 6 successful projects within last five years (https://guarda.co, https://chainthis.com, https://changenow.io). Paul's interests are: cryptocurrency exchanges, wallets, smart contracts, financial inclusion. https://www.linkedin.com/in/sokolovpaul/

- **Charlie Shrem**, Strategic Advisor and Visionary, is an American entrepreneur and bitcoin advocate. In 2011 he co-founded the now-defunct startup company BitInstant, and is a founding member of the Bitcoin Foundation, formerly serving as vice chairman.
https://twitter.com/charlieshrem

- **Simon Yu**, Advisor, CEO and cofounder at https://www.stormx.io/ project, micro-tasks application to earn cryptocurrency for millions of users. Raised $32M in token sale, advised by Bill Shihara (Bittrex), Anthony Di Iorio (Jaxx), Charles Hoskinson (Cardano/ADA) and others.

- **Simon Dixon**, Advisor, CEO of online investment platform BnkToTheFuture.com who have invested over US$250m in FinTech companies, like BitFinex, Bitstamp, Kraken, BitPay, ShapeShift, Exodus and over 40 others. https://twitter.com/simondixontwitt
https://www.linkedin.com/in/simondixonbankingreform/

Tech

- Ilia B., CTO, Co-Founder, expert in blockchain, security and highload. Has 6+ years of experience in highload projects' development, 4+ years of experience in blockchain development. Designed and launched cryptocurrency billing system last year.

- Roman L., Project manager, in web development since: 2006. https://github.com/memphys
Blockchain experience: building Block Explorer, working with RPC protocols of multiple currencies, developed mobile light wallet, developed atomic swap for ETH\BTC, developed web light wallet, working multiple exchanges API and markets data (cryptocompare, coinmarketcap etc.)

- Alexandr D., Backend Developer, in development since: 2013. https://github.com/remedge
His Blockchain experience is: building Block Explorer, developed mobile light wallet, working with RPC protocols of multiple currencies, working multiple exchanges API and markets data (cryptocompare, coinmarketcap etc.)

Archived copy · cryp2nova.com

- Denis K., Backend Developer, in web development since: 2013. https://github.com/altingfest
His Blockchain experience is: building Block Explorer, working with RPC protocols of multiple currencies, built web light wallet, Working multiple exchanges API and markets data (cryptocompare, coinmarketcap etc.)

- Alexey K., Full Stack Developer, in development since 2014. https://github.com/waterelder
His Blockchain experience is: building High load Block Explorer, Working with RPC protocols of multiple currencies, development of mobile light wallet, working multiple exchanges API and markets data (cryptocompare, coinmarketcap etc.)

- Denis K., Full-stack developer, has 3 years experience in frontend development and 1 year experience in backend development. Also has a strong background in math. Participated in 20 projects that were successfully launched.

Archived copy · cryp2nova.com

Glossary

Crypto asset - a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets.

Private keys - a private key in the context of Blockchain is a secret number that allows crypto assets to be spent. Every Crypto asset wallet contains one or more private keys, which are saved in the wallet file. The private keys are mathematically related to all Crypto asset addresses generated for the wallet.

Addresses - an identifier of alphanumeric characters, that represents a possible destination for a Crypto asset payment. Addresses can be generated at no cost by any user of Crypto asset.

Cryptocurrency node, Full node wallet - any computer that connects to the Blockchain network is called a node. Nodes that fully verify all of the rules of Bitcoin are called full nodes. Full nodes download every block and transaction and check them against Blockchain consensus rules.

Blockchain explorer - a block chain browser (also called "block explorer") is a program or web site that lets users search and navigate a blockchain. Uses include: checking address balances, tracking coin transfer histories, watching for transaction acceptance, monitoring the network hash rate and other statistics.

SPV (Simplified Payment Verification) - a method for verifying if particular transactions are included in a block without downloading the entire block. The method is used by some lightweight Blockchain clients. Thin clients don't verify the preceding blocks, they use the number of confirmations (whether they are valid or not) as a measure of the likelihood of a block chain reorganization producing a new longer fork which excludes the transaction.

Full node wallet - a full node is a program that fully validates transactions and blocks. Almost all full nodes also help the network by accepting transactions and blocks from other full nodes, validating those transactions and blocks, and then relaying them to further full nodes. It’s possible and safe to run a full node wallet to support the network and use its wallet to store your Crypto assets, but one must take the same precautions you would when using any Crypto asset wallet.

Orderbook - an order book is an electronic list of buy and sell orders for a specific security or financial instrument, organized by price level. An order book lists the number of assets being bid or offered at each price point, or market depth. It also identifies the market participants behind the buy and sell orders, although in some cases participants choose to remain anonymous (most likely for crypto markets).

BitTorrent protocol - a communication protocol for peer-to-peer file sharing ("P2P") which is used to distribute data and electronic files over the Internet.

Order - in means of the current document an order is an investor's declaration of willing to purchase or sell a crypto asset. Orders are typically placed over the phone or online. Orders fall into different available types which allow investors to place restrictions on their orders affecting the price and time at which the order can be executed.

Archived copy · cryp2nova.com

Trade - trade is a basic economic concept involving the buying and selling of goods and services, with compensation paid by a buyer to a seller, or the exchange of goods or services between parties.

Taker - a taker is an individual or company that must accept prices in a market and takes liquidity from the makers. A Taker hits previously created order from the orderbook.

Injections - an exploitation of a computer bug that is caused by processing invalid data. Injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution. The result of successful code injection can be disastrous, for example by allowing computer worms to propagate.

Signature - a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).

Seeding - an uploading of already downloaded content for others to download from. A peer, a computer that is connected to the network, becomes a seed when having acquired the entire set of data it tries to download. This data consists out of small parts so that seeds can effectively share their content with other peers, handing out the missing pieces. A peer deliberately chooses to become a seed by leaving the upload task active when content is downloaded.

Byzantine consensus - a dependability of a fault-tolerant computer system, particularly distributed computing systems, where components may fail and there is imperfect information on whether a component is failed. In a "Byzantine failure", a component such as a server can inconsistently appear both failed and functioning to failure-detection systems, presenting different symptoms to different observers.

Validator - a special role for active consensus participants maintaining consensus in Byzantine networks. While not all the nodes in the blockchain network may be actively involved in the consensus algorithm Validator nodes do.

Blockchain oracles - an application for a delivery of data to the blockchain and delivery of the data itself.

Market price - current price at which an asset or service can be bought or sold. The economic theory contends that the market price converges at a point where the forces of supply and demand meet.

Network commissions - a fee that spenders may include in any Blockchain transaction. The fee may be collected by the miner who includes the transaction in a block.

ERC20 (223) tokens - a technical standard used for smart contracts on the Ethereum blockchain for implementing tokens. It defines a common list of rules that an Ethereum token has to implement, giving developers the ability to program how new tokens will function within the Ethereum ecosystem.

OTC deals - crypto assets traded in some context other than on a formal exchange such as the Poloniex, Binance, Kraken. The phrase "over-the-counter" can be used to refer to Crypto assets that trade via a dealer network as opposed to on a centralized exchange.

Archived copy · cryp2nova.com

Smart contract - a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.

KYC procedure - the Know Your Client form is a standard form in the investment industry that ensures investment advisors know detailed information about their clients' risk tolerance, investment knowledge and financial position.
KYC forms protect both clients and investment advisors. Clients are protected by having their investment advisor know what investments best suit their personal situations. Investment advisors are protected by knowing what they can and cannot include in their client's portfolio.

Archived copy · cryp2nova.com