Online.io

White Paper

Version 1.8
July 2018

Disclaimer

The purpose of this White Paper is to present Online.io and OIO (pronounced OYO) tokens to prospective investors in connection with the upcoming Token sale.

The information set forth in this White Paper may not be exhaustive and does not imply any elements of a contractual relationship. It aims at providing relevant and effective information to potential token holders with the intent to help them decide whether and when to purchase OIO tokens.

The content of this White Paper is not binding for Online.io Blockchain Technologies ("the Company"); furthermore, the Company reserves its right to adjust, add or remove sections and content within this White Paper for any reason and at any time before, during and after the sale of OIO tokens by posting the amended White Paper on the website.

This paper should not be considered a solicitation for investment and it is not composed in accordance with, nor is it subject to, laws or regulations of any jurisdiction, which are designed to protect the investors. Moreover, this White Paper does not constitute an investment, legal, tax, regulatory, accounting or other advice, and it does not aim at being considered the sole basis for any evaluation of a transaction regarding the prospective acquisition of the OIO tokens. Prior to acquiring the OIO tokens, the prospective client should consult his/her own legal, investment, tax, accounting and other advisors to evaluate the potential benefits, burdens and other consequences of such investment.

The OIO token is a utility token and not a digital currency, security, commodity, or any other kind of financial instrument. Hence, it has not been registered under the Securities Act of 1933, the securities laws of any state of the United States of America or the security laws of any other country, including the securities laws of any jurisdiction where a potential token holder is a resident.

The OIO tokens are not intended for sale or use in any jurisdiction where the sale or use of digital tokens may be prohibited by the laws governing the respective jurisdiction. Also, the OIO tokens will not be sold or distributed, or otherwise resold by their holders to citizens of, natural or legal persons with their residence or place of incorporation in any country or territory where deals with digital tokens are prohibited or in any manner restricted by the applicable laws or regulations of that jurisdiction. If such purchases are made, the person responsible for the acquisition shall bear the risks and negative consequences for acting in an unauthorized or fraudulent way. The company reserves its right to refuse or cancel OIO token purchase requests at any time at our discretion when the information provided by the client in the KYC (Know Your Client) procedure is not detailed enough, inaccurate or misleading.

The company does not carry any business activities, nor does it offer or distribute OIO tokens in Singapore, in People's Republic of China or in other countries or territories where there are restrictive laws or regulations, or the Company must be registered or licensed with any applicable governmental authorities in respect to transactions with digital tokens.

Each prospective holder of OIO tokens is reminded that this White Paper is presented to him/her on the basis that he/she is the person entitled to make investments. Moreover, it is prospective token holders that bear the ultimate responsibility to determine if he/she can legally purchase the OIO tokens in his/her jurisdiction and whether the prospective token holder can then resell the OIO tokens to another person in any given jurisdiction.

Certain statements, forecasts and financial information included in this White Paper represent forward-looking statements. Such affirmations take into consideration certain known and unknown risks and uncertainties, which may lead to actual events or results being materially different from the estimates or the future results expected by the forward-looking statements.

The White Paper is conducted in the English language and this version is to remain the primary official source of information about the project. The information contained in the English version will be translated into other languages, and it may happen that in the course of the translation process some of the information contained in the English language version may be lost, corrupted or misinterpreted. The accuracy of such alternative versions cannot be guaranteed. In case of any conflict or inconsistencies between the translations in other languages and the official English language version, the provisions and statements of the English language original document shall prevail.

Contents

Abstract

This white paper outlines first off challenges faced by internet users in nowadays Internet of Things: security, privacy and ad scamming, secondly a shift in digital advertising providing untamed potential, as well as the business and technical specifications of the Online.io project aimed to capitalize on this potential.

1. What is Online.io platform?

1.1. Vision

Our ultimate goal is to reinvent the World Wide Web experience by placing people's privacy as our top priority, thus offering a more secure, non-trackable, without malware and ad free Internet.

1.2. Mission

Government agencies and big Internet companies that shall remain unnamed thrive on tracking your every move! Only together we can put a STOP to this!

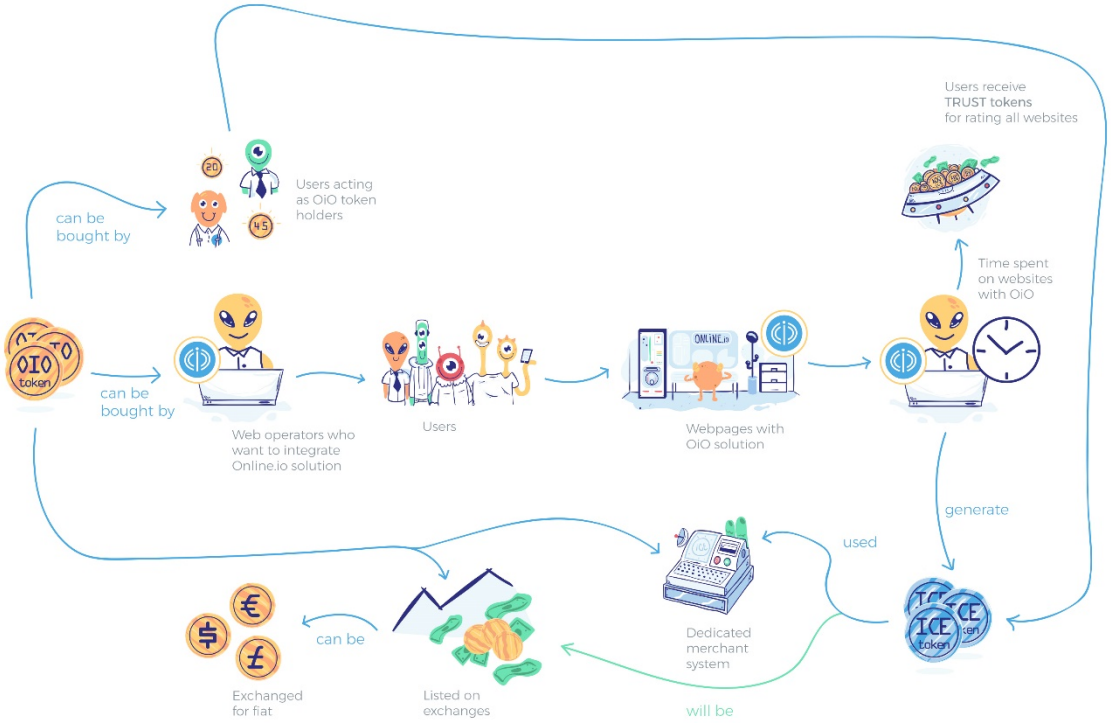
Nowadays websites are full of ads that try to sell you something they think you need by creating an unfriendly and irritating browsing experience. Also, lots of them have hidden malware, scammy ads or mining scripts.

Online.io platform aims at making a groundbreaking change of the Internet, by revolutionizing the browsing experience and making it faster, non-trackable, without malware and ad free.

Website operators gain a significant amount of revenues from ads, which can be changed by implementing our solution based on the highly scalable, transparent and fully accountable Blockchain technology, which will ensure they get fair remuneration based on the number of visitors, time spent on their pages and the interaction with the site, creating a more suitable environment for quality, as opposed to spammy cash driven webpages.

A new website rating system will be developed for the community and you as part of this community will decide on the quality of the websites you visit. This will lower the time and stress spent on click bait pages and you'll have more time for valuable pages.

1.2.1. Ecosystem overview



1.3. Context & Objectives

When people hear about "Blockchain", they think about Bitcoin, the world's first cryptocurrency, which aims at changing the global economy. However, Blockchain, Bitcoin's underlying technology is poised to disrupt other sectors as well. Starting last year there was a huge hype around the Blockchain technology stack and especially Ethereum-based start-ups developed to impact more common areas of our day-to-day routine and not only the banking and financial sectors (where paying intermediaries fees are no longer required). Blockchain technology started to be used for activities such as grocery shopping, online marketplace, paying for your dream house, car, holiday, etc.

The advertising industry is yet another sector that is going to be reshaped by the Blockchain technologies, which accordingly to market experts could be the most groundbreaking change within the industry since the emergence of smartphones and social media.

Considering that over 40% of world's population has Internet access, the advertising business enjoys a large source of data, and in recent years, their focus has been on big data. However, evolving capabilities and changing regulatory prospects will affect how advertisers connect and engage customers in the near future.

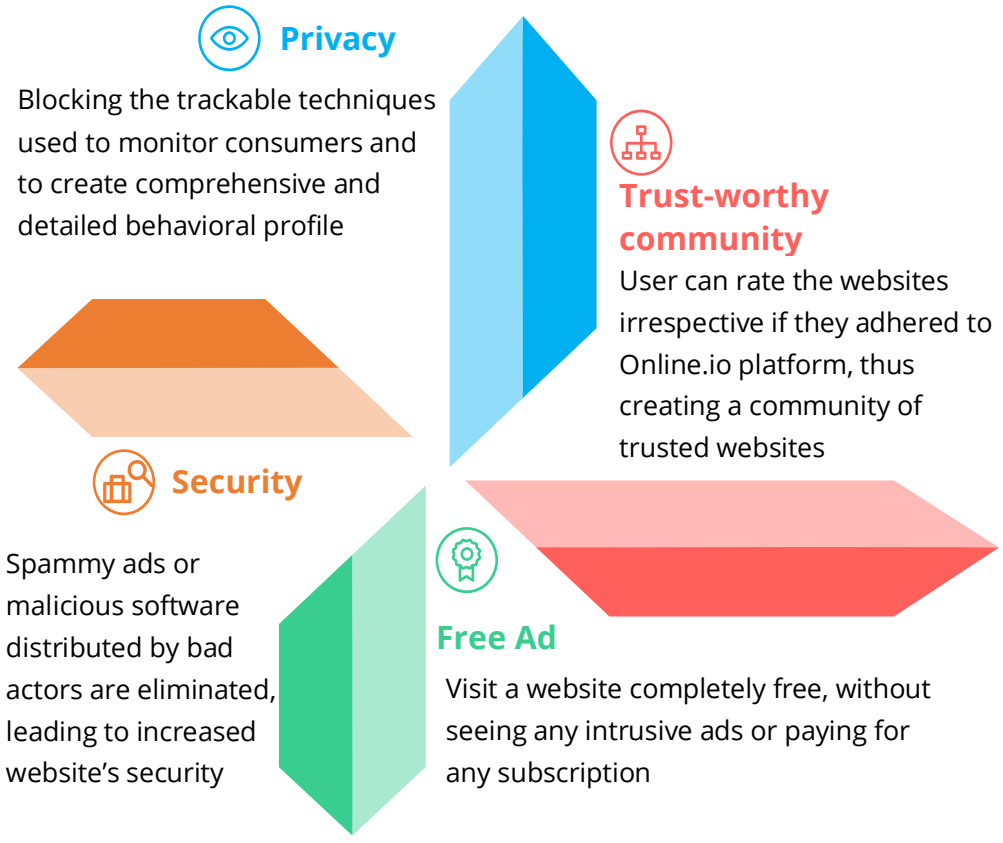
Recent studies regarding users experience with digital ads revealed that more and more consumers seem consistently unhappy with digital advertising for three main reasons: security, privacy and fighting annoyance from intrusive ad formats.

Online.io is implementing a decentralized ecosystem which combines all necessary features for a faster, safer, and more private Internet browsing. Moreover, through the Online.io platform developed by using the most advanced Blockchain technology, both internet end users and website operators will benefit alike.

Enhanced Online experience for Internet users. Bypassing digital advertisements means faster webpage loading time and a more enjoyable browsing experience due to removal of disturbing ad formats. According to a 2016 survey, 91% of consumers appreciated that digital ads were more intrusive than two years ago, while 81% of them stated that they have closed a browser or exited a webpage because of pop-up ads.

Also, Online.io offers an enhanced protection of consumer data first off due to added security of Blockchain technology which will eliminate demographic and behavioral profiling from being collected and used without prior consent. As internet users are able to rate each website according to their experience, this will lead to the creation of a ranking of trust-worthy websites.

1.3.1. Features for internet end user



More satisfied consumers, higher ranked webpages, and a new and profitable revenue stream for website operators. By implementing the Online.io solution, the website operators will offer their visitors a cleaner version of their webpage. This will consistently enhance the browsing experience since the focus will be on the website's content and quality, without any disruption from intrusive ad formats.

Furthermore, the websites and visitors will benefit from the highest security level, since the spammy ads and malicious software distributed by bad actors are eliminated.

In nowadays society, internet users are becoming increasingly aware of the fact that the second they start using the Internet, their behavior is being tracked and used to create a "profile" which is then sold to companies for advertising and other purposes. Since, hard-to-detect tracking techniques are used, even very sensitive information is often collected including financial data, which rises privacy concerns among both users and authorities. Online.io solution comes to meet such threats to visitor's privacy and to help website operators adhere to the latest regulation changes (i.e. GDPR EU regulation) by blocking the online tracking practices, which gives the user the opportunity to browse the Internet without having the feeling of being monitored and stalked.

Website operators may consider that by using the Online.io solution, their revenues might be downsized since they are no longer monetizing on the ads posted, but in fact the Online.io solution will unlock an untamed potential of revenue stream. The website owners will have financial benefits even without embedding advertisements, by capitalizing on the time spent by the visitors on their webpages.

Since the visitors will be able to rate the websites based on their experience, the ad free, secure, private webpages will definitely enjoy a higher ranking, which in turn will attract more visitors and consequently more revenues for their owners generated as Online.io tokens.

By using the Online.io solution, the browsing experience is upgraded for end users and website operators alike. While the former enjoy a faster, ad free, more secure, and private Online experience, the latter keep their website protected from bad ads and malicious software, while rewards accrue based on the time spent by visitors on their websites.

Online.io is created on the Ethereum platform, thus the Online.io tokens can be used for any financial operations within the ecosystem. Furthermore, the Online.io platform is designed by using a new consensus algorithm, Proof-of-Online. As opposed to the other already known proof of concepts, the one used by Online.io does not require massive hardware resources which consume large quantities of natural resources. Our ecosystem is designed to generate ICE tokens based on the number of visitors on websites that integrated our solution. Furthermore, it is optimized for minimum Gas consumption on the Ethereum platform.

2. Token Generation Event Overview

2.1. Purpose of the Token Generation Event

Online.io is offering to the potential clients of its platform the right to pre-purchase its own OIO tokens through a Token Generation Event that is projected to start on June 15th, 2018.

OIO tokens will be distributed in direct correspondence with the amounts paid by the potential clients during the Token Generation Event.

The design and implementation of the Online.io Token Generation Event has been prepared in accordance with industry's best practices. Hence, the potential contributors benefit from the enhanced levels of security and are also reassured that the distribution of tokens will be performed according to the smart contract conditions used by Online.io.

The funds received during the pre-sale and the public Token Generation Event for the OIO tokens will remain unused until the distribution of OIO tokens to token holders.

2.2. Summary of the Token Generation Event

The team at Online.io has been intensively working on bringing this idea to life since June 2017. The next step in developing our platform and thus creating an enhanced online experience will be to release beta versions for several modules in Q3 2018, latest in early Q4 2018. Our vision is to continually develop the platform thus keeping it in line with the latest technology developments.

In order to fund the development of the Online.io project, we plan to organize a public Token Generation Event aiming to attract investors, who are willing to support our goal: creating a faster, ad-free, more secure and private Internet experience.

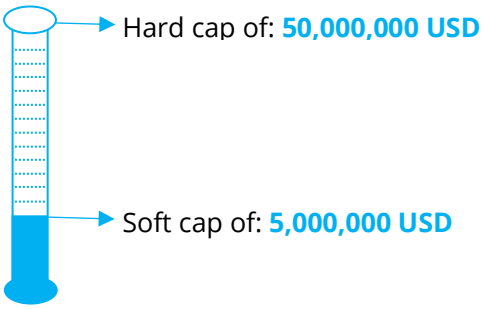
Prior to the opening of public Token Generation Event for the Online.io platform, we are offering pre-sale opportunities of OIO tokens, with bonuses awarded in token ranging between 5% and 25%, depending on the investment's value.

Further details of the Token Generation Event and the potential benefits of OIO tokens ownership are provided in this Whitepaper. The binding terms and provisions of the OIO Token Sale will be outlined in the Terms & Conditions provided at https://online.io/ (the "Website").

2.2.1. Token Generation Event characteristics

The public Token Generation Event planned to commence of June 15th, 2018, is characterized by the following:

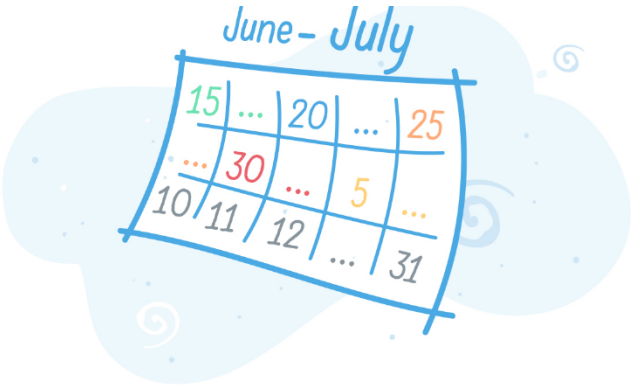
- ✓ Maximum number of tokens: **2,500,000,000**
- ✓ OIO token price: **0.04 USD**
- ✓ Payment methods accepted: **Ethereum, Bitcoin, Litecoin, Bitcoin Cash, Bitcoin Gold, Dash, Eth. Classic**
- ✓ Adjustable distribution: **Unsold and unallocated tokens will be destroyed**
- ✓ Further token issuances: **No, only a single token issue for the Token Generation Event**



2.2.2. Bonuses

In the first day of launching the Token Generation Event, namely June 15th, 2018, a 25% bonus will be granted in OIO tokens. Following the launch day, the below scheme of bonuses will be awarded:

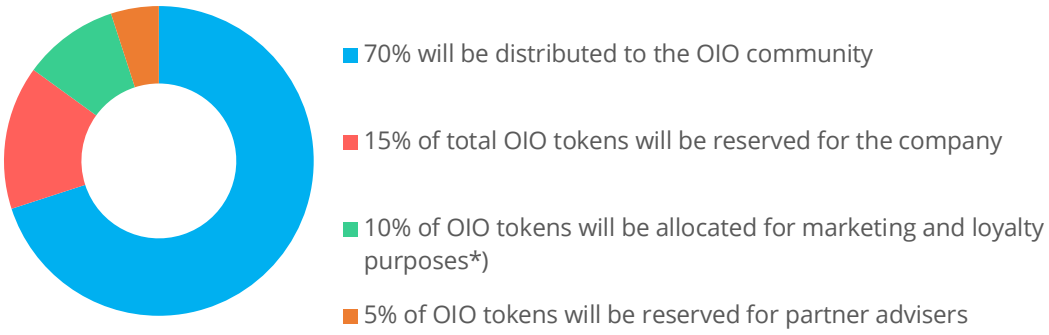
June 15th - June 19th - 25% bonus
June 20th - June 24th - 20% bonus
June 25th - June 29th - 15% bonus
June 30th - July 4th - 10% bonus
July 5th - July 9th - 5% bonus
July 10th - July 31st - no bonus



* there will be a base price for the OIO token, but investors will receive a bonus in accordance to the above mentioned timeline. Investors will be able to withdraw their tokens without the bonus tokens at the end of the Token Generation Event or when all tokens are sold. The OIO tokens received as bonus will be eligible for withdrawal only after 90 days.

The OIO token price will not suffer any modifications, but the investors will receive a bonus in accordance to the above-mentioned scheme. Investors will be able to withdraw their corresponding OIO tokens, without the bonus one, at the end of the Token Generation Event or immediately after the all the tokens are sold. The OIO tokens received as bonus will be eligible for withdrawal only after 90 days.

2.2.3. Distribution of tokens



*) The percentage of 10% includes also the tokens rewarded as referral

3. Market Overview

In today's interconnected society characterized by increased capability of everyday devices to connect to other devices and people through the internet infrastructure, the high degree of connectivity raises a myriad of consumers' privacy and data security concerns.

The advertising industry enjoyed a negative attention both from the large public and the authorities because of its less transparent practices of online tracking and behavioral profiling. Following technological developments, online tracking became increasingly sophisticated, thus it is no longer limited to the "cookies" installed on the user's devices in order to monitor websites a user visits, but it can track real-time data accessed by a user and triangulate that with information stored about that user's location, financial data, health records, etc. These results are then complied into complex and rather comprehensive consumers' profiles that are sold to digital advertising companies for better targeting their promotional campaigns.

Very sensitive information is often collected thus violating consumer privacy. Moreover, the consumers do not have access to the data collected about them and consequently cannot correct any inaccuracies.

The Internet of Things provides a handful of opportunities for cybercrimes aiming at gathering data regarding intellectual property, confidential personal information, financial data, etc. Consequently, the cybersecurity market is on a continuous upward trend, being driven by cybercrime. Since, there is a dramatic rise in cyber-attacks, creation of malware software both for PCs, laptops, but also for smartphones and tablets, both the companies and the end users are becoming increasingly focused on safeguarding their personal data and thus enhancing the cyber security.

3.1. Advertising market

The media work is changing at a rapid pace, given the developments in technology (i.e. expansion of mobile telephony, faster mobile broadband adoption, and high degree of interconnectivity seen recently), users' preferences and behavior and business models.

According to 2016 statistics, around 46% of the population had access to internet – the equivalent of over 3.5 billion of people online – the number is growing very fast.

Hence to thrive in such an interlinked environment, the media and entertainment companies have upgraded their products offering with more developed advertising formats, more sophisticated video and more consumer centric targeting tools.

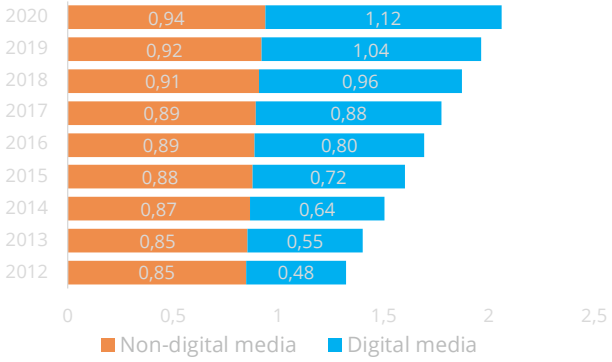
In 2017, the media and entertainment industry is estimated to have reached over USD 1.7 trillion in revenues, accounting for approximately 2.5% share in global GDP. The main driving force behind the industry's revenues in a greater extent, but also behind the consumer spending is the digital media.

As the market continued to be fueled by the transition from traditional to digital media, in the last years, the advertisers gradually directed their budgets towards online advertising, as they benefit from increased availability of consumer data and improving software for data algorithms to track down consumers' preferences and thus creating better tailored ads.

Consequently, according to recent reports and statistical data, is estimated that 2017 marked the year when digital media spending equaled that for global non-digital media for the first time in history. Digital media was the fast-growing entertainment and media (M&E) segment, with a historical 5-year annual growth rate of 13.1% as compared to growth rate of 1.1% recorded by the non-digital segment.

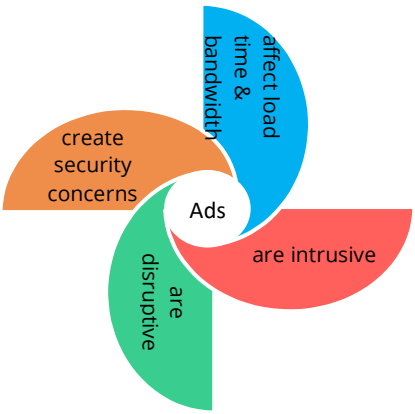
By 2020, the trend is expected to remain the same, digital media continuing to be the driver of the M&E industry registering 8.3% growth rate by 2020, while the non-digital media is forecasted to remain relatively flat, with a growth rate of only 1.4%.

Media and entertainment industry revenues
(2012 – 2020, trillion USD)



*) Digital media is defined by digital advertising, broadband, over-the-top transactional and subscription digital video, satellite radio subscription spending, digital recorded music downloads, digital recorded music streaming subscriptions, digital out-of-home advertising, consumer magazine digital circulation spending, daily newspaper digital circulation spending, electronic consumer books, digital learning materials, online video games, mobile video games
Source: McKinsey, Global Media Report 2016

Big data dominated the advertising trends in the last decade, with Google being the first in paid search advertising and Facebook reigning in display advertising. Essentially, these two Internet giants account for 60-70% market share in digital advertising. In the recent years the online advertising attracted some negative attention for being not that transparent with its practices.



With respect to consumers' experience, the latest research regarding the consumers' opinions revealed that they are becoming less and less tolerant to the barrage of unnecessary, unwanted, irrelevant ads' messages.

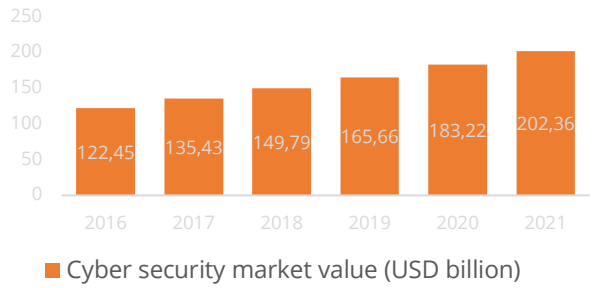
Various surveys concerning the people's attitude to online advertisements exhibited the following top concerns:

Therefore, considering the way the consumers' perceptions are evolving, the future of online advertising is looking increasingly tenuous.

3.2. Cyber security market

The increasingly dependency on technology and internet in today's society has a twofold effect: on one side new business models and revenue streams were created, but it also revealed new gaps and opportunities for the cyber-attacks, which became more complex being carried on with more sophisticated malware software. The cyber attackers are trying to gather valuable and sensitive data like intellectual property, personal information, health records, financial data, by gaining data access through the use of advanced ransomware techniques.

Statistically, the cyber security market is valued in 2016 at over USD 120 billion, being estimated to surpass USD 200 million by 2021.



Source: Statista, Size of the cyber security market worldwide, from 2016 to 2021 (in USD billion)

Only in 2017, more that 978 million adults in 20 countries globally were exposed to cyber security attacks. Financially wise it is estimated that those who were the victims of cybercrime globally lost over USD 170 billion.

In the future, the cybersecurity market value is expected to increase exponentially driven by the cybercrimes. According to a vulnerability assessment, 76% of the websites were found to have vulnerabilities that can by exploited by cyber-attacks.

Cyber security market specialists consider that Blockchain technology can help companies improving cyber defense, since it can secure and avoid deceitful activities through the consensus algorithm and detect data tampering based on its characteristics of transparency, auditability, data encryption and operational resilience.

4. Blockchain current and future evolution

Each distributed system needs a consensus algorithm to validate transactions. Over the last few years the Proof-of-Work algorithm has dominated, not to say was the only one used. As the cryptocurrency ecosystem evolves — the race to create a better consensus algorithm began.

The current year can become the year of competition between different mining algorithms / strategies. The following strategies are currently most widely known:

Proof-of-work (PoW) - (Reference #2). Coins are distributed based on the work performed by the user to demonstrate his input on processing transactions and doing work for the whole infrastructure. This is the group of algorithms that provides slow calculation of some result and fast verification of this result. This helps to ensure that miners have to perform some complex computations on their hardware to find a block, but Blockchain network users that confirm this block don't need to perform such computations and can easily check that result is correct using low resources.

Proof-of-stake (PoS) – (Reference #3). Coins are distributed based on the user's previous investments. The more investments a user has the more coins he will receive.

Proof-of-elapsed time (PoET) - (Reference #4) is a relatively new concept. Coins are distributed based on the proof that the user was doing some specific action for a rather long period of real time. Proof of time algorithm was invented by Intel and it is mainly associated with their hardware platform that provides very fast consensus model. It generates random numbers (wait time) on miner's nodes and then chooses the node with the lowest number. So, it works like a lottery but

with more complex algorithm designed to provide more optimizations. Intel promises that this algorithm cannot be broken by external actions and provides honest consensus model. This makes PoET perfect for private Blockchain when you need performant distributed storage and don't want to force your hardware to make complex computations. The only minus is the restriction on Intel's platform (Sawtooth Lake).

The proof-of-elapsed time has not become popular and well adopted yet. But in the near future it may be intensively developed. Future adoptions may not be the exact algorithm designed by Intel, but rather some variations of the concept.

5. Online.io platform

5.1. Context Overview

A malicious software is an application that was created for a particular bad purpose. Most existing applications are created for normal purposes while some applications have hidden features which are not doing what is expected, but in fact their purpose is to find, steal or destroy files, track any data or just annoy the user. This started a long time ago: the first computer virus was called Elk Cloner and was first found on a Mac in 1982. Over 10 years ago a new kind of malware appeared and it was called Adware. It was distributed through security holes in Windows XP and Internet Explorer. Adware can also use security holes in Java and Flash player or even in JavaScript. But why do developers create adware? The main reason is monetization, of course. Any Adware capable of embedding paid advertisements brings its owners huge income. Starting from pop-up ads, embedded browser toolbars, search hijacking, etc.

How can we stop any kinds of malware from being created? We can stop / alter monetization and make creating malware less attractive!

5.2. Features for end user

5.2.1. Free the Internet

Problem: Historically, users had to pay a visible or hidden fee to browse the Internet, the most popular methods of payment currently in use are Advertising, Ecommerce and Subscription. There are no/or at least next to none/truly free sites currently operating, even Wikipedia asks for donations from its users' base.

Solution: By integrating Online.io solution, websites will now have a completely new revenue stream based on time spent by their visitors on their webpages, that will not require any form of payment from the end user.

5.2.2. Security

Problem: Most of the websites on the Internet are full of ads and lots of them are also infected with malware. In order to capitalize on their websites, the operators will also appeal to promoting ads, and hence they put their webpages and consequently their visitors to the risk of being the victims of bad ads, or other types of malware software.

Solution: Online.io platform will integrate a custom anti-malware and ad-blocking solution that will be made available to end users, so they can enjoy a better experience on all websites. Mass adoption of this solution also has the benefit of putting pressure on website operators to use our system making it more popular and robust.

5.2.3. Privacy

Problem: There is money in customers profiling. Huge companies (think Google and Facebook) invest massively in tracking users across a myriad of websites and actions so they can profile users to better sell to them ads, products or even information. This has the added downside that a person now becomes a set of numbers and will tend to live in an information bubble, you only see the information the companies think you want, the products they think you need, the ads they think you will click on.

Solution: Online.io will integrate a tracking script blocker that will severely disrupt the ability of companies to track and profile real people.

5.2.4. Quality

Problem: The current incentive for websites is to attract users to them by any means necessary this usually involves using tricks and immoral methods (i.e. clickbait, spam, phishing). On its own a system that allows website operators to monetize attention and also provide a clean browsing experience does not really address the issue of quality and will no doubt lead to websites that appeal to the lowest common denominator being remunerated greatly for shady tactics.

Solution: Online.io will integrate a voting platform that will allow users to voice their opinions on the quality of the websites they visit, warning them if websites they are about to visit are deemed low quality.

5.3. Online.io Ecosystem

5.3.1. Desktop Browser Extensions

- ✓ Extensions for all the major browsers will contain the ad blocker, tracking script blocker, anti-malware as well as a web wallet.
- ✓ The voting system will also be included in the extensions allowing users to rate on all websites, not just the ones using our solution.

5.3.2. Mobile Applications

- ✓ Mobile applications will function as a wallet, ad blocker, tracking script blocker, anti-malware.

5.3.3. Wallet

- ✓ Our wallet will work on all major operating systems and browsers.
- ✓ Mobile phones and tables will have one app for wallet, ad blocker, tracking script blocker, anti-malware.
- ✓ Desktop operating systems will have dedicated app wallets.
- ✓ The wallet will be integrated in the desktop browser extensions.
- ✓ The wallet will feature advanced security including but not limited to:
  - Two-factor authentication;
  - Fingerprint and face recognition;
  - Second device;
  - Passphrase + pin;
  - Automatic wallet encryption;

- Vault option (you have a set amount of time to cancel your payments before they go through).

5.3.4. Marketplace

Earned a lot of ICE? You may wish to spend it for getting some products or services. In the marketplace you can find all the places where you can pay with the ICE token.

5.3.5. Merchant System

You can accept payment in multiple cryptocurrencies and receive the funds either in fiat or in ICE. Opting to receive the funds in ICE will come with a 0% commission guaranteed, while fiat payments will have a 3% commission. Best market rates will be applied for all payments using multiple exchanges.

5.3.6. Other

- ✓ Plugins for all major ecommerce shopping solutions (Shopify, Magento, Prestashop, Opencart, WooCommerce, WHMCS, etc.);
- ✓ API SDK for custom integrations.

5.4. Smart Contracts & Workflows components

5.4.1. Three Types of Coins

- ✓ **Online Ethereum token (OIO)**. OIO Tokens are the key element in the ecosystem. The web operators will be required to stake OIO Tokens in order to use our technology and mine ICE tokens. (through Proof-of-Stake and Proof-of-Online algorithms).
- ✓ **ICE Ethereum token (ICE)**. The purpose of the ICE coin is to be used for micropayments and daily use.
- ✓ **Trust token (TST)**. Exists only within the private Blockchain. It is used for stimulating users to rank websites and for ranking gamification.

*) Tokens are described in detail later.

5.4.2. What is an Online master-node?

A master-node will be used to secure the network and will receive the information from a collection of private nodes. The master node is an Ethereum contract which keeps token balances.

5.4.3. What are Private-nodes?

Private nodes are controlled by the network operators and will process and count the number of online users on each website every minute.

Each week the private node aggregates all usage statistics for Websites and makes a transaction to all webmasters to receive the appropriate token amount.

5.4.4. Prerequisites for a User to be Counted

- ✓ Must pass a Turing test (Cloudflare + our custom verifications);
- ✓ The visit must last more than 1 minute;
- ✓ It should be counted (stored to the private node) every minute, once per minute.

5.4.5. Work with the Browser Addon

When a user visits a website that is using the Online.io platform, he will be notified by a tooltip informing him why this website is not running any ads. Through this, he can also install a browser addon that can be used as a wallet and protection.

When you install the addon, it will work also as a tracking blocker on any other site that is not using the Online.io solution. At the same time, this will help the Online.io platform to learn how to block new types of ads while also improving its ability to classify users as real or not.

5.4.6. Use Cases and Roles

Online.io solution is designed for the following types of users:

- ✓ Visitor. The Internet end user who is browsing the web for his own needs.
- ✓ Webmaster. The one who owns a website and wants to monetize on the time spent by his visitors on the webpageby earning the ICE tokens.
- ✓ Infrastructure Operator. The organization which maintains guardian, security rules and token issuing procedures.

5.5. Online.io Financial Model

5.5.1. Online Token (OIO)

The Online tokens (OIO) are generated once and sold at the Token Generation Event.

Out of the maximum number of tokens generated, 15% of the OIO will be reserved for 1 year by the company and will not be available for sale during that time.

After the Token Generation Event the OIO tokens will be available on various exchanges.

The purpose of the OIO tokens is to bootstrap the development of Online.io platform.

The OIO tokens will also function as a proof of stake and generate ICE Tokens, 20% of all generated ICE Tokens will be distributed to OIO token holders who keep their tokens on a special wallet.

The website operators that implement the Online.io solution will have to possess OIO tokens to be able to receive ICE tokens based on the time spent by their visitors on their webpages. The OIO tokens required to manage the websites, will be kept on an Ethereum smart contract.

5.5.2. ICE Token (ICE)

A fixed number of ICE tokens will be generated every week and will be distributed as follows:

- ✓ 40% to OIO token holders;
- ✓ 20% founder rewards for future developments of Online.io solution and marketing and partnership purposes;
- ✓ 40% to website operators:
  - The system will calculate a score for each website based on the TRUST RATING and number of visits (See “Mining - Proof of Online” 5.6.1);
  - Each website will receive ICE tokens amounting to the percentage of score from the total pool.

After the OIO Token Generation Event and after some time since the first production of ICE tokens, they will be available on various exchanges.

ICE tokens are mined based on the time spent by end users on websites attached to the ecosystem.

Do we issue them infinitely? The ICE token is unlimited, but the issued amount is reduced by 2.5% each month for 10 years. After 10 years, the number of ICE tokens generated per year remains fixed.

Ecosystem features

Our benefits	
Mission	Internet without ads, trackers and malware.
Mineable	ICE Tokens will be mineable.
Mining algorithm	Proof of Stake, Proof of Online.
Inflation model	Unlimited ICE token issuance.
Blockchain visibility	Private Blockchain for intermediate state TRUST tokens and public Blockchain for the ICE tokens.
Public Blockchain	Ethereum
JavaScript guardian stack	Vanilla JavaScript
Ecosystem features	1. Web, PC and Mobile compatible wallets with multiple securing methods. 2. PC, Mobile, Chrome & Firefox extensions that will block ads, trackers and malware. 3. Ecommerce plugins for popular platforms like opencart, prestashop, whmcs, etc. 4. Instant payments for those who use Online.io wallet.

5.5.3. Trust Token (TST)

The Trust token is kept in the private Blockchain, due to Gas costs and is not publicly available.

End users will receive TST tokens for actions that allow the system to determine the quality of the websites they visit (voting, reviewing).

TST tokens will also be able to be burned to allow users to get rewards for them:

- ✓ Increase their rank making their ratings and reviews more important;
- ✓ Badges;
- ✓ Achievements;
- ✓ Skins;
- ✓ Custom titles;
- ✓ Prizes.

TST tokens will not be listed on exchanges or traded in any way to prevent websites from increasing their rank artificially.

TST rewards will be fixed per action.

5.6. Online.io Technical Specifications

5.6.1. Mining – Proof of Online

The basis of rewards for website operators will be the Proof-of-Online which is a number that quantifies how many minutes users spend on each website.

Websites will have a script embedded on them (for example http://online.io/script.js?site=site_id)

The webserver on http://online.io will be a Node.js cluster hosted behind Cloudflare.

The combination of Cloudflare's protection and our own custom implemented solution in the cluster will count real people online (multiple sessions from the same user at the same time will count as one).

The webserver will store each website's stats.

Every week each website's visits will be converted to ICE tokens after a period of 7 days (visits for 1-7 of the month will be paid on the 14th, etc.).

Example:

- ✓ Website http://example.org has on average 1000 visits per day for an average session duration of 5 minutes, this translates to 5000 minutes per day or 35000 minutes per week.
- ✓ http://example.org will get a score of: score = 35000 * TRUST RATING
- ✓ http://example.org will receive ICE tokens amounting to score/SUM(score of all websites) * ICE Coins generated this round (77 million)
- ✓ If http://example.org has a TRUST RATING OF 1 and the sum of all website's score is 1.000.000 then example.org will get 35.000 / 1.000.000 * 77.000.000 = 2.695.000 coins this round.

5.6.2. Trust Rating

Users will be able to rate a website from 1 to 5 stars, 5 stars representing the highest quality websites, 1 star representing the lowest quality websites.

The number of stars will initially be converted to Trust Rating simply by dividing them by 5 (i.e. 5 stars will represent a trust rating of 1, 2.5 stars will represent a trust rating of 0.5, 1 star will represent a trust rating of 0.2).

By default, websites with no ratings will have a Trust Rating of 0.5 (equivalent of 2.5 stars).

In the future, the Trust Rating formulae will probably evolve to include many more factors.

5.6.3. Platform Architecture

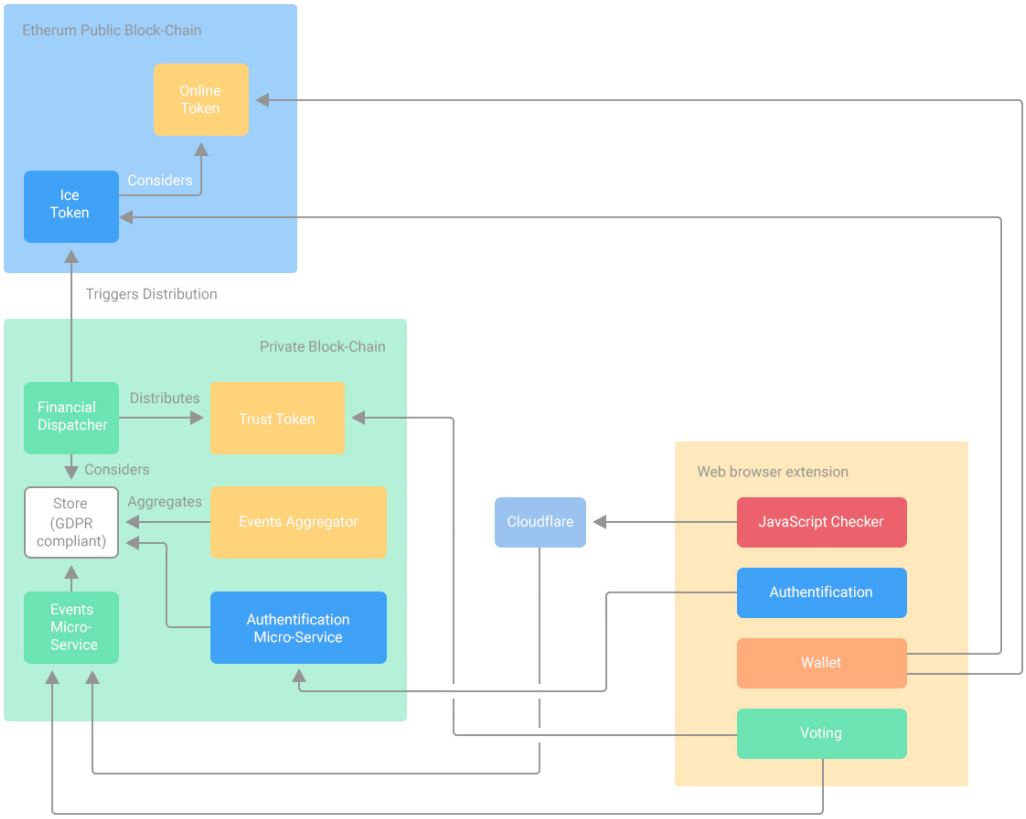
5.6.3.1. Data Flow

The following infrastructure keeps the websites secured with the Online.io code:

Components diagram

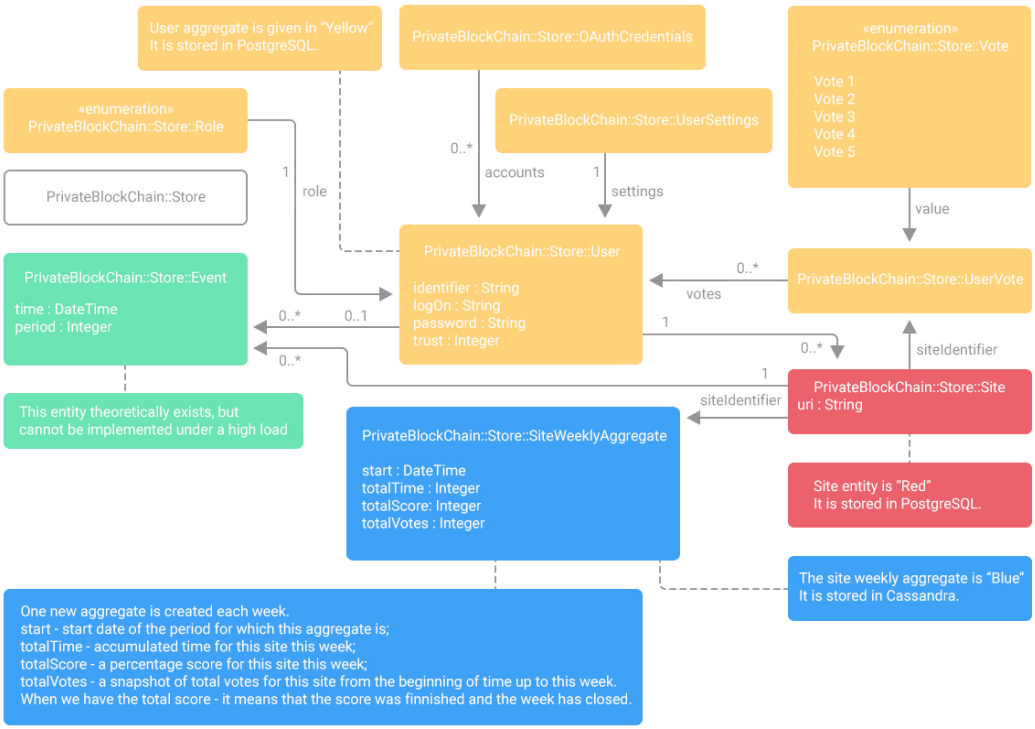
5.6.3.2. Financial Subsystem, Private Blockchain

Online.io private Blockchain is a clustered replicated storage. It stores users' statistics for each website - information about users who have spent more than 1 minute per session and number of total minutes spent. ICE tokens are issued based on the time users spend online. The scheme for issuing all ICE tokens is given on the following components diagram:



The JavaScript guardian does all necessary checks and passes data to the Events microservice to be kept in the Store. When the time comes, the Events aggregator builds intermediate calculations based on these events. The Financial dispatcher periodically triggers ICE token and Trust token to distribute token values based on the aggregated data.

The Store has entities as described on the class diagram below:

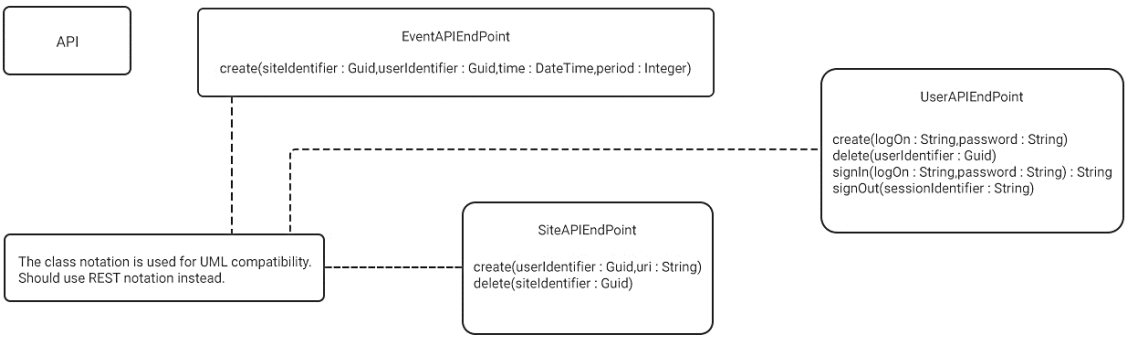


The Event belongs to some website and may belong to some User. The Event theoretically exists but we do not want to track all events under high-load conditions. We track the SiteWeeklyAggregate instead, which accumulates all events.

The User can be authenticated by his logOn and password or OAuthCredentials. A User has a Role, UserSettings, and a collection of UserVote entries. The website belongs to some User and has a unique uri.

For a website there may exist a lot of SiteWeeklyAggregate entries. Each SiteWeeklyAggregate is created for one website per one week. It has the start date, and totals for time, score and votes. Score total is calculated based on time and votes.

The Events and Authentication microservices (API microservices) contain business logic from the class diagram below:



5.6.3.3. Private Nodes

It's clusterized master backend hosted on Cloudflare with the following functionality:

- ✓ Receiving users' statistics (linked with website key) from private nodes, calculation generated units per-website.
- ✓ Weekly conversion of website units to the ICE token by specified rules.
- ✓ Sending ICE token to website wallets (via smart contract in public Blockchain) for websites that have reached required number of generated units.
- ✓ Users' identification (checks that user isn't a robot, includes Cloudflare functionality + custom checks).

5.6.3.4. Master Node & Public Blockchain

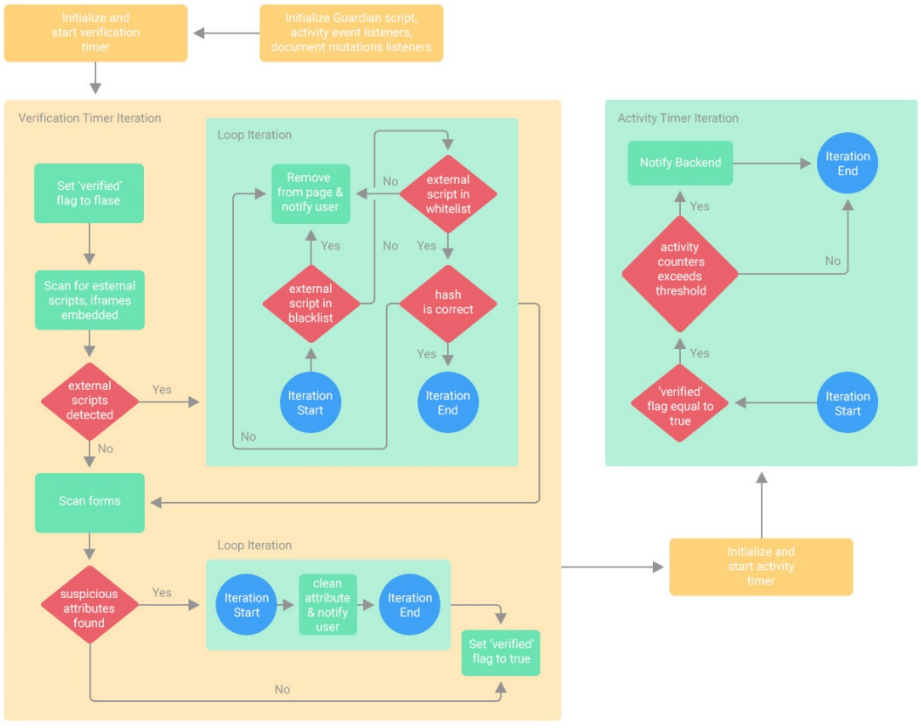
All OIO and ICE tokens are kept in the Ethereum Blockchain. The contract master node receives transactions from the private node and distributes ICE token accordingly.

5.6.4. Guardian Architecture

Guardian is an embedded JavaScript that will be included into webpages and will work in the browser. The goals are:

- ✓ Detect all external adware scripts on the website and block them according to the blacklist;
- ✓ Detect that users are on that webpage and there is some activity from them;
- ✓ Calculate time spent by user on this website and every 1 minute notify backend that user spent more than 1 minute on this website.

Guardian diagram



5.6.5. Bad Actors

To prevent bad actors from trying to game Online.io and include ads on their websites as well as our platform, the included script and the ad blocking extensions will check for the presence of ads

on the page and prevent visits that include ads from being counted towards the Proof of Online calculation.

One more method of preventing abuse will be to use automated crawlers and check for the presence of ad scripts on the same pages and flag pages that are seen to include ads.

5.6.6. Initialize Guardian Script and Activity Event Listeners

- ✓ Include guardian script into “head” of HTML to be sure that it will be loaded before all other scripts;
- ✓ Initialize guardian params (website token, blacklist, whitelist, intervals and activity counters settings);
- ✓ Attach activity event listeners;
- ✓ Attach Mutation Observer listeners (to detect website code changes).

5.6.7. Initialize and Start Verification Timer

What if the website initially is fine, but produces malicious scripts after some period of time?

Website operator will be able to choose if he wants to use hash checks or not for the website. Interval for this check should be big enough so we will not abuse website performance. We will periodically verify that content on webpage has not changed a lot. We can calculate hash every iteration and if it is the same as previous time - we don’t need to validate elements. Here we are setting interval between webpage verifications and flag to check hash or not.

In addition, we can monitor events within the DOM tree to find out that the website has changed greatly and we need to re-validate for malicious scripts.

5.6.8. Verification Timer Iteration

a. Set 'verified' flag to false (to disable sending stats to backend until we make sure that page is clean).
b. Scan for external scripts, iframes, embedded.
    i. Search document and look for <script>, <embedded>and <iframe> tags.
    ii. Check every found element by specified (for current type) pattern and if pattern matches with suspicious:
        - Create suspicious element object with specified type (script, iframe or embedded), link to the element in DOM and other required paraments.
        - Add suspicious element object to the list of external scripts.
    iii. Proceed each found element in the list:
        - If element is blacklisted:
            - Remove it from page;
            - If possible - remove any instance created by suspicious code in global scope;
            - Notify user (via snackbar or modal).
        - If element is whitelisted
            - If it’s hash is correct - continue with next element;
            - Else:
                - Remove it from the page;
                - If possible - remove any instance created by suspicious code in global scope;
                - Notify user (via snackbar or modal).

- If element is not in black / white lists - decision depends on initial config parameter (can be splitted into multiple rules for different types of suspicious element: script, iframe, embedded).

c. Scan forms:
   i. Search the DOM document for <form>, <input>, <textarea>, <button>, <radio>, <select> or <checkbox> tags;
   ii. Check every element found whether it's value matches any specified (for current type) pattern and whether this pattern matches any suspicious patterns. For example, some browser extension can inject JavaScript or SQL into hidden textarea or text input, or form "action" attribute can be modified to send form data to external resource:
      - Clean the suspicious attribute;
      - Notify the user (via snackbar or modal) about a suspicious pattern.

d. Set the "verified" flag to true to enable sending statistics to backend;

5.6.9. Initialize and Start the Activity Timer. Activity Timer Iteration

a. is equal to true:
   i. If "no" - iteration ends;
   ii. If "yes":
      - Check that activity counters exceed the threshold:
        - If "no" - iteration ends;
        - If "yes" - send statistics to backend.

5.6.10. Gas Usage Considerations

5.6.10.1. What is Gas and How Does it Work?

Gas in Ethereum is the name of a measurement unit that is used to specify the amount of calculations. Each transaction in Ethereum must be executed on some hardware (miner's hardware). This hardware has its price + amortization + maintenance price. Also, it consumes electricity that isn't free. And access to the Internet also isn't free. So, we can assume that transaction execution cannot be free. Plus, we want to prevent bad guys or newbies from running unlimited complex calculations on network hardware for free.

So non-free calculations within Ethereum framework limit network users from running unwanted calculations.

Each operation has its own fixed cost in gas:

Operation	Gas Cost	Description
step	1	Default amount of gas to pay for an execution cycle.
stop	0	Free.
suicide	0	Free.
sha3	20	Paid for one SHA3 operation.
sload	20	Paid for a SLOAD operation, getting from the permanent storage.

Operation	Gas Cost	Description
sstore	100	Paid for a normal SSTORE operation (doubled or waived sometimes), putting into the permanent storage.
balance	20	Paid for a BALANCE operation.
create	100	Paid for a CREATE operation, contract creation.
call	20	Paid for a CALL operation, initiating a read-only call.
memory	1	Paid for every additional word when expanding memory.
txdata	5	Paid for every byte of data or code for a transaction.
transaction	500	Paid for every transaction, basic fee.
contract creation	53000	Changed in homestead from 21000.

But gas cost cannot be directly converted to Ethereum. Ethereum market price changes rapidly and isn't related to hardware price / maintenance price / electricity price. That's why the gas price should be set in Ethereum per-transaction and hardware owners (miners) will decide if this price is enough - so the market decides what is correct computation price dynamically.

Another one important moment is that user sets not only gas price but also the limit of gas that can be used to execute transaction. The issue is that one transaction can initiate multiple operations that can recursively initiate another operations and user's wallet can get empty before transaction executed all required operations (that can never happen if it has bad or malicious code). So, user sets the limit of total gas that can be used by a transaction to prevent such situation. The gas paid for executed operations of a non-finished transaction will not be returned to user's wallet (execution of already executed operations cannot be free - because of electricity price and other parts of cost that were described above).

So, in total:

a. Every operation in Ethereum has its cost. Gas is a measurement unit that is used to specify the cost of operations.
b. User sets the price of gas in Ethereum that he can pay. If it's lower than the current market price - then miners will not execute this user's transaction.
c. User sets maximum amount (in Gas) that he can pay for execution of the whole transaction, in other words "budget". If the budget is exceeded - that transaction execution stops, and gas will be paid only for already performed operations.

5.6.10.2. Why Does Online.io care about Gas?

Online.io distributes ICE tokens to webmasters for free. But each transaction to the Ethereum Blockchain costs gas and, finally, money. For each ICE token to be issued, Online.io needs some kind of a transaction to the Ethereum Blockchain. Especially this becomes important when there is

a real bulk of web sites for which the Ice token needs to be withdrawn. Also, gas price is increasing over time while more and more Ethereum-based projects (especially games) appear.

Therefore, to achieve our goal to keep Internet clear from malware, ads and viruses, we work to create a Gas-effective algorithm of ICE token distribution to make sure that the project will work with any amount of websites and users.

There is too much data to be processed while generating ICE tokens. It includes information about all the websites and how much time was spent on each website by each visitor. This data should not be loaded into the Blockchain due to Gas considerations. So, we keep anything like that data in the Node.js cluster which accepts data from the guardian and keeps it before the ICE token is passed to appropriate wallet. This data is not publicly available. Such approach is best described as a “private Blockchain”. Initially we are going to use Node.js and MongoDB to handle this data. Later we are going to migrate to a distributed ledger stack and make this data publicly available (Reference #6).

6. Roadmap

2017

The idea first appeared in June

June to December: Initial research Phase

December: Validated the potential of the idea

2018

1st Quarter

January

Studying blockchain in terms of platform integration perspective

Risk analysis, associated with blockchain

Starts the development for the TGE Website & Platform

February

2nd phase of research completed

March

Whitepaper published

Development finished for the test network and base contracts code

Development finished for user API

Development starts for data aggregation and financial dispatcher

Smart contract development starts

UI design finished

Private TGE sales starts

TGE platform beta version

2nd Quarter

April

TGE platform published accepting user registrations

Malware protection development starts

User validation development starts

Online time tracking development finished

May

Chrome and Firefox browser extensions development starts

Web dashboard for OIO token owners development starts

ICE token distribution algorithm implemented

June

TGE starts

Malware protection beta

User validation beta

Private cloud beta, guardian script beta

Wallet development starts

3rd Quarter

July

Chrome and Firefox browser extensions beta

ICE token smart contract published

Web dashboard for OIO token owners release

Private cloud release

Guardian script release

August

Beta version of web dashboard for OIO and ICE token owners release

Chrome and Firefox Browser extensions release

September

Wallet beta release

4th Quarter

October

Web dashboard for OIO and ICE token owners release

December

Mobile applications development starts

2019

1st Quarter

January

Marketplace architecture

API SDK for custom integrations architecture

February

Plug-ins for E-Commerce solutions architecture

March

API SDK for custom integrations release

Wallet additional security features

2nd Quarter

April

Marketplace beta release

June

Plug-ins for E-Commerce solutions beta release

3rd Quarter

July

Marketplace release

4th Quarter

October

Plug-ins for E-Commerce solutions release

7. Online.io Team & Advisors

7.1. Selected team members

ALEXANDRU IULIAN FLOREA

Founder &Chief Executive Officer at MICROLEAVES LTD

LinkedIn

- Iulian is a serial entrepreneur with over 9+ years experience and over 10 start-up exits.
- He started his online venture as a very successful Affiliate Marketer which lead him on the path of Online Entrepreneurship.
- He is the founder and CEO of Microleaves, which under his management has grown to the World Largest Peer-to-Peer Residential Proxy Network with over 30 million IPs and around 20k customers including top Fortune 500 Companies.

ALEXANDRU EFTIMIE

Chief Technology Officer at MICROLEAVES LTD

LinkedIn

- Alex is one of Romania's top Software Developers with vast experience in over 20 programming languages like C++, C#, Java, JavaScript, Python, PHP and so on.
- He is also an expert on high concurrency scalable infrastructure and the go-to man for building or optimizing systems like: crawlers, Blockchain and peer-to-peer networks.
- Since 2012 he is acting as the CTO and Head Development Manager at Microleaves, where he designed and developed a revolutionary proxy system.

MAI RICHARD

China Chief Representative

LinkedIn

- Entrepreneur with proven track experience across East China ranging from machine or deep learning, database speed optimisation, trade data analyses, as well as customer support. Also, he has been involved in SEO and online marketing projects for various large websites.
- Richard will be responsible for managing the affairs of Online.io across China and will serve as main point of contact for those interested in Online.io solution.

SEBASTIAN DRACOPOL

Development Manager | Scrum Master & Project Manager | Blockchain | ICO | Agile Development

LinkedIn

- Over 15 years of experience in software development industry, in companies like Electronic Arts, Forbes, Upwork, Vodafone, Sebastian is our Project Management agile wizard.
- Sebastian also poses a solid knowledge of the crypto world and a lot of experience in human resources.

 ROSTYSLAV BORTMAN JavaScript / Ethereum Developer at Zfort Group LinkedIn	▪ Senior Developer with wide experience in working with smart contract functionality
 ROMAN KORZH Business Development Consultant at Zfort Group LinkedIn	▪ Senior level results-driven leader with exceptional knowledge of establishing long-term cooperation and generating revenue. ▪ Thorough understanding of project management, strategic planning, operation management, business analysis, sales training, customer service and more. The ability to maintain and develop working relationships with existing partner organizations and explore opportunities to bring new potential cooperation.
 ANDREW MIKHAILOV CTO at Zfort Group LinkedIn	▪ Specialization: architect, project manager, scientific research, Blockchain, data science. ▪ Stack: C#, JavaScript, GoLang, multimedia transmission, CRM, signal processing, IoT, R, UNIX.
 LILIYA GIRINOVA Business Analyst at Zfort LinkedIn	▪ Business analyst, project manager; ▪ Interaction and proactive work with clients; ▪ Managing projects using SCRUMBAN methodology; ▪ Describing business logic of tasks, requirements gathering; ▪ Collecting artifacts and writing documentation under the project; ▪ Compiling and prioritizing of product backlog; ▪ Drawing-up and control of project risks

 ANATOLIY GORDIENKO JavaScript Department Lead at Zfort LinkedIn	▪ Technical lead and architect ▪ Full stack developer - Typescript, JavaScript, Python, PHP, SQL, NoSQL, CSS, IAAS/PAAS, serverless.
 VADYM DOLZHENKO Node.js Developer at Zfort LinkedIn	▪ Full stack developer - JavaScript, TypeScript
 ALEXANDRU DOBRIN Art Director at Deklyn LinkedIn	▪ Talented Art Director who enjoys working in a wide variety of design-related areas and photography
 ALEXANDRU DANETE Customer Support Lead at Microleaves LTD. LinkedIn	▪ Wide experience as a customer lead, able to solve delicate problems and always seeking to make clients happy
 BOJANA MILOSEVIC MAZEE LinkedIn	▪ Bojana is a marketing expert with more than 6 years' experience in big tech companies like ManageWP, GoDaddy, etc. She is involved in ICO market since 2017 acting a marketing specialist for several ICO's by providing strategic business consulting, brand management, and marketing strategy dedicated to inspiring the entrepreneurial spirit and bringing business dreams to life.

7.2. Advisors

NATHAN CHRISTIAN

BLOCKCHAIN TECHNOLOGY CONSULTANT | END TO END ICO SOLUTIONS | ICO ADVISOR

LinkedIn

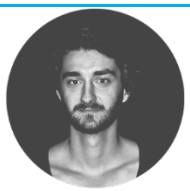
- Ranked as #5 blockchain advisor on icon bench, he is part of a dynamic team building applications on Ethereum and Bitcoin Blockchains, writing Smart Contracts and launching ERC20 tokens. End to end Cryptocurrency development and launch. Initial Coin Offering (ICO) strategy, development, angel & venture capital investment, consulting and advising. Over 35 startups in portfolio. 1.2m Twitter followers.

CRISTIAN RADU

TUCA ZBARCEA &ASOCIATII

LinkedIn

- Cristian Radu is a partner at Ţuca Zbârcea & Asociaţii, and concentrates his practice on mergers and acquisitions, securities transactions and general corporate law. Cristian has significant experience in restructurings and business acquisitions, including cross-border acquisitions, disposition of non-strategic businesses, divestitures, public offerings, squeeze-out and sell-out procedures and mergers. He is involved in all aspects of structuring, negotiation and documentation of these transactions. His work also includes corporate counselling and strategic advice to the boards of directors and other committees of Romanian companies on disclosure issues, corporate governance practices and compliance matters.
- Cristian has experience in a wide variety of industries, including retail, industrial, telecommunications, energy and oil and gas, representing some of the largest companies active in these areas.



ANDREI MIHAI COSTESCU

JECO CAPITAL

LinkedIn

- With over 10 years of progressive experience in finance and banking, Andrei now serves as the CEO of a crypto assets hedge fund and co-founder of a technology company enables people from emerging markets to trade crypto instantly using local fiat.

 ALEXANDRU MANUCU TUCA &ASOCIATII TAX SRL LinkedIn	▪ Alexandru is a Tax Manager mainly covering corporate and international taxation matters. ▪ He previously worked as a senior tax consultant with PwC, he was involved in various consulting and audit projects, diagnostic and fiscal reviews and mergers and acquisition projects across a wide range of industries: automotive, energy and mining, industrial products, IT and communications.
 ALEXANDRU ZOTA ZOTADS LinkedIn	▪ Alexandru is an entrepreneur and investor with several successful exits and 10+ years' experience in the online advertising industry.
 DIANA VADUVA DELOITTE LinkedIn	▪ Diana is a seasoned business professional with more that 8 years of experience in financial services, out of which over 4 years in the Management Consulting practice within Big 4 companies. ▪ She also actively traded natural gas on NYMEX exchange for a couple of years.
 FLORIN MUSATOIU ORACLE LinkedIn	▪ Florin is an engineer with 10+ years' experience in managing IT Systems like CRM and Marketing Cloud Applications. ▪ In 2010 he joined Oracle as a Principal Technical Analyst quickly taking the role of Team Lead and Mentor for a team of 12 engineers, also recognized as one of the most valued employees proven by awards like: "I Am Oracle", "Oracle Pacesetter", "Social Networking", "Team Excellence" and "Oracle Expert" ▪ He is an ITIL Certified Specialist, highly skilled in developing and optimizing IT Service Management processes.

 PAUL BADEA @HUBS LinkedIn	▪ Co-founder @HUBS, a learning catalyst focused on providing a decentralized learning platform while contributing to decreasing youth unemployment rates. ▪ Actively involved in the connected car environment and also in vehicle trading, developing business both for BADSI and Smartogo.
 CRISTIAN CIOBANU OPENHOSTING LinkedIn	▪ He has more than 9 years of experience in IT Engineering and Messaging Encryption, with a passion for building successful projects along the years in Cloud Environments.
 MARCO CALICCHIA MAZEE LinkedIn	▪ Marco is the CEO and Founder of MaZee, the leading ICO Community Management and Marketing Agency. ▪ He is an experienced ICO and Blockchain advisor with a portfolio of over 25 ICOs, including clients like Experty, Remme and Open Platform.

8. Legal aspects

8.1. GDPR Compliance

The Data Protection Directive 95/46/ec is set to be replaced by the new General Data Protection Regulation (GDPR), which is meant to be effective May 25th, 2018.

The GDPR aims at standardizing the various different privacy legalizations across the EU into a single set of rules that will enhance the users' data protection across all member states. The new digital privacy regulation is applicable to any organization, anywhere in the world that handles EU citizens' personal data must comply with it.

On one hand, GDPR may sound intimidating since it strengthens the rules regarding how organisations process personal data of their customers, thus enabling stricter regulations for how to use data collected and well as enhancing data protection and privacy by periodically conducting privacy impact assessments and better communicating data breaches.

However, GDPR may be seen as an opportunity to assess and improve the way companies deliver services to their clients. According to a Consumer Privacy study conducted by Truste/NCSA in 2016, 92% of online customers state that data security and privacy are a concern. Moreover, a report

performed by Charted Institute of Marketing emphasises that 57% of clients do not trust companies to use their data responsibly.

Our platform is compliant to the guidelines set forth by the GDPR by implementing privacy processes and procedures aiming fostering the transparency of client's data collection, data storage and processing as well as data removal.

More information is available at: https://gdpr-info.eu/.

8.2. Risks

By buying coins, you accept significant risk. Before purchasing coins, carefully consider the exemplary and non-exhaustive list of risks set forth below and, to the extent necessary, consult a lawyer, an accountant or a tax professional.

Risk of Weaknesses in the Coin Transport Software. The Blockchain-based assets concept is experimental in nature, therefore yet unproven. There is a risk that, as an open source project, any contributor to the software could introduce security weaknesses or errors into the software, causing the loss of coins.

Regulatory Risks. We will operate through the decentralized coins not through a legal entity. However, there are regulatory risks. Blockchain technology represents the new form of economic interactions between individuals and companies where some methods are still to be tested, verified, and certified. It is likely that specific regulations in some jurisdictions might be set to contradict the mentioned methods. Such regulations may or may not be friendly for us, and some might even forbid any relationships using coins.

Loss of Value. The recognized value of coins is unpredictable. Our ecosystem or its representatives or people associated with it will not be responsible for value loss and will not have to buy back any coins from anyone.

Disclaimer of Warranties. The user expressly agrees that the user is buying coins at the user's sole risk, and that coins are created on an "as is" basis without warranties of any kind, either expressed or implied, including, but not limited to, warranties of title or implied warranties, merchantability or fitness for a particular purpose. Without limiting the foregoing, none of third parties or individuals associated with the coins creation warrant that the process for purchasing coins will be uninterrupted or error-free.

Limitations waiver of liability. You acknowledge and agree that, to the fullest extent permitted by any applicable law, you will not hold third parties or individuals associated with the coins creation liable for any and all damages or injury whatsoever caused by or related to use of, or inability to use, coins or the mass software under any cause or action whatsoever of any kind in any jurisdiction, including, without limitation, actions for breach of warranty, breach of contract or tort (including negligence) and that none of the third parties or individuals associated with the coins creation shall be liable for any indirect, incidental, special, exemplary or consequential damages, including for loss of profits, goodwill or data, in any way whatsoever arising out of the use of, or inability to use, or creation of, or inability to create, coins. You further specifically acknowledge that the third parties or individuals associated with the mass-tokens creation are not liable, and you agree not to seek to hold any of the third parties or individuals associated with the

coins creation liable, for the conduct of third parties, including other creators of coins, and that the risk of creating and using coins rests entirely with you.

References

- https://en.wikipedia.org/wiki/Internet_privacy — an article on Internet privacy;
- https://en.wikipedia.org/wiki/Proof-of-work_system — Wikipedia term for the proof-of-work system;
- https://en.wikipedia.org/wiki/Proof-of-stake — Wikipedia term for the proof-of-stake system;
- https://themerkle.com/what-is-proof-of-elapsed-time/ — a description of the proof-of-elapset-time concept;
- http://www.ethdocs.org/en/latest/index.html — main Ethereum documentation;
- https://sawtooth.hyperledger.org/docs/core/releases/latest/introduction.html — a distributed ledger platform.
- https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf
- https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf