
t.
toxic

TOXIC WHITEPAPER

Last Updated: May 06, 2020

Table of Contents

1. Introduction

How often the information one told during private communication sessions came back in the form of perfectly suited online advertisement… rhetorical question. How often it is needed to use extraordinary approaches to protect own crypto wallet with a reasonable amount of money on it… lots of people know the answer.

While communication & crypto services more and more move towards fully secured solutions, still there are plenty of cases when protected messengers & email services are broken and the most reliable crypto currency wallets are hacked and money stolen… why does it happen? There are following reasons:

- the usage of standard cryptography (even the newest encryption protocols are based on the same principals) & standard encryption procedures;
- the usage of standard user authentication approaches;

The real cases why it happens could be very different, starting from human factor when people don't keep own devices & applications protected with strong passwords or just use web resources with viruses and malware and ending up with encryption infrastructure that utilize standard approaches, so can possess keys and decrypt information when needed.

Our new cryptography which based on Keyless Cipher Generator (KCG) system with Geometric Vector Encryption Method (GVEM) will be implemented in complex communication & crypto financial solutions to guarantee that no third party can get any communication/interaction details, personal data or personal preferences. To reach maximum protection in line with smart monetization approaches we are developing a set of software solutions (Toxic Ecosystem) based on new encryption and consisting of:

- mobile and desktop messenger (Toxic messenger): secret chats/ group chats, calls/video calls/ conference calls/ corporate messenger solution + purchase of mobile/ landline phone numbers worldwide and external calls;
- VPN service and email service with plug-in to major email services (Toxic bi-mail);
- mobile & desktop crypto currency wallet with fiat-crypto gateways and integrated to crypto exchanges and DEX functionality based on new authentication Keyless methods (Toxic multi-wallet);

1.1 Concept

Secured communication & crypto financial services became an issue… historically and potentially communication secrets, financial information and technology know-how always attract the interest of national security forces, corporate espionage professionals and rivals. As a result, no one can be sure that using existing the most secure tools gives full protection and absence of third party interference or user keys are not decrypted and all the communication history and financial data is sold online.

Referring to the history of communication gives clear vision that people always wanted to reach protection in messaging and calls using "newest" technical solutions in all the times with always the same result. When finally it became obvious to everyone that the highest level of security is just a marketing trick. Whether it was possible to happen due to lack of reliable technology or just because small company was taken over by large corporations, the result was always the same - secured communication has been discriminated.

Keyless Cipher Generator (KCG) system and Geometric Vector Encryption Method (GVEM) are provided to make impossible to decrypt interaction simply because encryption keys don't exist (in a general sense, since dynamic data are changing all the time), so it is impossible to get access to information online as well as communication history, even by security services.

1.2 Advantages

Toxic Ecosystem (including Toxic messenger, Toxic multi wallet, Toxic VPN & bi-mail) is totally different new technical solutions that:

- ➢ will use new encryption technology called Keyless Cipher Generator (KCG) system with Geometric Vector Encryption Method (GVEM) together with utilization of supplemented technical solutions to protect, hide & mix data flows that will guarantee the full confidence in financial operations and communication information protection to users;

- ➢ already has Toxic messenger Alfa version available to the public in App Store and Google Play and is going to be supplemented with integrated VPN service;

- ➢ as a final Ecosystem solution will guarantee full communication & crypto financial freedom;

Also, the Toxic messenger, Toxic wallet & Toxic bi-mail will use a set of features that make impossible to understand users' interactions and communication details from outside, such as blocking of third party tracking system interference, utilization of data mixers, white noise (fake traffic generation), hidden metadata, etc. making impossible to trace anything.

Additionally:

- ✓ Toxic messenger is supplemented with possibility to purchase any mobile/ landline phone numbers worldwide and external calls;

- ✓ Toxic bi-mail service will be supplemented with encryption tool that can be installed into similar services to stay always secured with email service which are common to users;

- ✓ Toxic wallet will use new passwordless authentication approach based on KCG with GVEM that gives no chance to hack such wallet.

2. Vision of the project

2.1 Core pillars of the model

- **Breakthrough technical solution** >> The project core development is a new cryptography technology that will be developed in the scope of the Toxic project (Keyless Cipher Generator (KCG) system and Geometric Vector Encryption Method (GVEM) and have to become breakthrough technology that will hit the market. Given technology will be used in every new Toxic product, such as messenger, email service & VPN and crypto-fiat wallet .Also this technology will become a basis for future Toxic solutions related to special type of crypto currency.

- **Smart monetization** >> Toxic Ecosystem is free to use by people, no charges are applied. Also, to make the project profitable and protect value of TOX tokens there is a set of paid services, which we believe to bring significant profits, such as

  - purchases by users of mobile & landline phone numbers worldwide, plus purchases of external calls minuts

  - purchases of integrated VPN service to protect all device traffic

  - while we don't charge any money for crypto and fiat money transactions (except third party chargers by service providers, such as exchanges or banks) we will charge small fee for crypto-fiat gateway service;

  - Corporate/Group Toxic messenger solution with extended security, separate hardware and support configurations;

- **TOX tokens minimal market price** >> irrespectively to the tokens sale price on every stage of pre-sale and general sale rounds, as well as TOX token price on exchanges we guaranty to use TOX tokens to buy Toxic paid services in every Toxic product with the fixed rate 1 TOX = 1 USD, if the market price is higher then this rate

(TOX token worth more than 1 USD it is up to a user to pay for Toxic services with TOX tokens or fiat currency. This is done to get more people to buy TOX tokens during pre-sale and general sale round and to make attractive purchases of TOX tokens and keep them to grouw in value;

- **Maximizing TOX tokens value** >> while token minimal value is protected by setting minimal fixed exchange rate, the maximum TOX token price will be influnced by the utilization of the tokens to generate advertisement posts (non-personalized) delivered to each user of all Toxic products with a fixed amount of 10,000 (ten thousands) tokens per one post to all users. Minimum number of advertisements will be possible to not bother users. Also it is a pretty good way to cover costs and guaranty system independence;

- **Toxic company & Toxic development society** >> develop Toxic Ecosystem following the approach that is based on the Teal emerging organizational paradigm and refers to the evolution of organizational structures. It rejects the old type of management and hierarchy and replaces it with independence and common purpose. Such organizations are characterized by self-management and wholeness. It means every member is free to make own inputs to the company's growth and development and gets a deserved share of profits (to be remunerated according to a value brought). It guarantees high quality of our product and stable permanent development.

2.2 Business model

		phase 1: START (pre-ICO)	phase 2: GROWTH (after ICO 15 months)	phase 3: GOAL (after ICO 36 months)
Products		1) Toxic messenger already on Play Market & App Store 2) Security: TLS 1.2, DTLS 3) Anonymity: landline/ mobile number purchase of any country 4) International landline/ mobile calls 5) New encryption system concept, protocols and methods described in techpaper	1) Keyless Cipher Generator (KCG) system 2) Geometric Vector Encryption Method (GVEM) 3) Toxic messenger based on KCG with GVEM 4) Toxic be-mail (new email service & encryption plug-ins to existed email services 5) Toxic multi wallet (desktop & mobile) with authorization based on KCG	*Toxic Ecosystem:* 1) Communication freedom: Toxic messenger & bi-mail (email service) 2) Financial freedom: Toxic multi wallet (desktop & mobile) & fiat currency & crypto currency gateways 3) Token monetization: advertisement channel for non-personalized ads posts to be sold with Toxic tokens (TOX) only 4) New techpapers: - New crypto currency & blockchain technologies - Special hardware for encryption
Financial forecasts	**Toxic ERC20 token (TOX)**	**0.10-0.20 USD** **Token highest nominal price during pre-ICO & ICO**	**1.00 USD** **Token market price estimation after new KCG & GVEM encryption and updated messenger available on the market**	**8.50 USD** **Token price estimation after all Toxic services are launched, with increased number of messenger users**
		nominal value, based on project financial model	fixed exchange rate 1TOX=1USD to purchase Toxic paid services by users	market value estimation is based on number of users & ads' prices as of 0,01% Ecosystem users receive ads posts per 1 TOX Token
	Project funding	1) ICO: Hard cap 1.8 mln USD (Soft cap 1.25 mln USD) // 8 mln tokens (TOX)	1) ICO 2) Operational Revenue: - phone number purchase -international calls worldwide	1) Operational Revenue 2) Accumulated Toxic tokens (TOX): by ads in products (messenger, wallet, VPN, bi-mail)
	Token distribution		1) ICO investors 78,12% 2) pre-ICO investors 9,38% % 3) reserve 6,25% 4) bounty & advisers 6,25%	
	Ownership structure		Founders: 100%	

Technology	*TLS 1.2, DTLS*	*Keyless Cipher Generator (KCG) system* *Geometric Vector Encryption Method (GVEM)* *New authorization protocol based on KCG* *Security plugins for major email service*	New crypto currency & blockchain technology *Encryption devices as supplement to smartphones*
	phase 1: START (pre-ICO)	**phase 2: GROWTH (after ICO 15 months)**	**phase 3: GOAL (after ICO 36 months)**
Company & Society	The team: - founders - encryption experts - former military encryption experts - developers - marketing - administration	Self-management company, which is based on Holacracy as a part of the Teal movement Established development society (part of the ecosystem that shares the company's income)	Ecosystem society: - Self-management company - Development society - Toxic Ecosystem users

3. Demand for new technical solution

While governments more and more put all communication channels and finance flows under total control to fight against terrorism, corruption and other negative essences, protection of individual's and financial transactions information decreased dramatically. People's personal & financial data and user's behavior are not only being traced on the internet for better advertisements targeting , but traced and stored with very sophisticated systems of individual scoring (e.g. Big Data) that are already being implemented wider and wider in different countries and corporations.

Lots of solutions were developed to make finding and sharing information faster, easier, free. But in recent years security and safety issues came into the first place in all communication and financial spheres. There are lots of solutions on the market to provide secure communication & protect crypto wallets that utilizing:

- highly secure messengers,
- private mail services with VPN & firewall access,
- crypto currency and blockchain,

but still there is a leak of information with no difference intentional or unintentional it was and it is hardly possible to find reasons for such problems. But we know the essence of the problem - these are current encryption systems and security protocols that are too weak for powerful new computers, so called quantum computers, being installed even by private companies or for combined computing resources that can be purchased on the internet.

We advocate the widespread adoption of secure personal communications and crypto currency finance to counter the growing cybercrime, mass cases of unauthorized covert surveillance and access to private data. Some of popular personal communication tools have implemented end-to-end encryption, other modern software products have been launched with the security option as a key point in ensuring their massive demand in the market.

In contrast to the well-implemented technical capabilities to ensure confidentiality, there are legal aspects that require assistance from service centers in opening access to personal information, these points are clearly defined by the legislator and are not generally discussed. The content providers assure that the entrusted data is completely safe, and even when it is really well implemented there is no permanent protection. It is explicitly indicated in user agreements and related documents, and is strictly observed. In such cases, you can't even rely on the "canary effect" - we won't be given a sign by "suddenly coming silence" to open access to our private data. And it is the problem of existing security systems.

Information about the possibility of implementing a scenario in which the protection created by the content provider can be hacked is well known to cybercriminals who conclude that it is fundamentally technically possible to successfully implement their attacks. And the number of these attacks steadily increase. Developers and providers of security software are forced to accept more and more challenges from cybercrime, modern tools and approaches which quickly become obsolete, therefore new fundamental solutions are required to leave no chance for an attacking hacker.

It is believed that the problem, for E2E encrypted communication tools, to provide guarantees that the user is really communicating with the intended recipient, basically comes down to confirming the ownership of cryptographic keys in the form of a signed certificate from a trusted authority. However, there are lots of problems associated with managing certificates, distributing, storing and revoking (destroying) keys. Popular E2E encryption and implemented solutions that support users protection free users from key management, just by requesting a trusted server that confirms the authenticity of the public keys of other users. These are very convenient, technological processes, haven't been disputed, but when it takes into account user's position, about trusted certification server, all that is asked is whether user accepts or not a certain user agreement written in difficult wording and always large in volume. In addition, most of these services use a proprietary server part with closed source code, which means that such software is only the private property of its authors or copyright holders and does not meet the criteria for free software. The main weak point in any security system is a "human factor". If the interests of the state or other powerful structures exceed the user's expectations, it becomes possible to use the so-called SSL proxy (the man-in-the-middle attack option), thereby losing confidence that the data exchange remains confidential.

In this regard, we offer an original technology of keyless encryption system, in which the role of the human factor, by chance or under duress, affecting the vulnerability of the system is minimized, and the targeted influence of the user on the control functions and security level increase is maximized.

In general, the keyless encryption technology, in our opinion, has good chances to offer the user a new security system, on a point-to-point basis, without using key information in data encoding-decoding procedures, passwordless client authentication, identifying and quickly responding to any modification of encrypted code, the ability to instantly verify all traffic regardless of the amount of information being checked.

4. Keyless Cipher Generator system & Geometric Vector Encryption Method

We believe the future of secure communication fully belongs to our invented Keyless Cipher Generator system that will be developed and implemented in scope of a given project in the Toxic Ecosystem and will provide the following:

a. new type of encryption with no any keys! will be based on Keyless Cipher Generator system and Geometric Vector Encryption invented & developed by our company. This opens a new era in communication that assure full anonymity/ privacy & no communication trace;

b. no any possibility to decode communication data for third users not participating in messaging or conversation. No communication and media data stored on servers, peer to peer connections is used only;

c. no any integrated behavioral-based and machine-learning integrated functionality that prevent intrusions of third parties, but can lead to scanning of user behavior;

d. no any personal data stored and no user behavior trace for marketing purposes. Any person that uses the messenger is totally anonymous and can be confident in full privacy;

We understand that the Toxic messenger will fully close any possibility to trace, read and listen to people what may cause some problems to state security agencies… and the company will not be able to provide any user data and communication history even in case of request from the legal authorities simply because we don't have any keys and our software can be easily examined. On the other hand, this is the major project goal to give people solutions that can not be hacked & traced.

Modern cryptography is completely based on a complex mathematical apparatus and on the need to generate, distribute, store and update key information, use keys in the encoding process. Good cryptographic systems strive for the *Kerckhoffs's principle*, according to which the security of the cipher is determined only by the security of the key.

In addition, an important parameter is the "distance of uniqueness" of the cipher or the "distance of uniqueness" of the code, which shows how much ciphertext you need to intercept for unambiguous key recovery (decryption). In key systems, the cryptographic code has some hidden correlation with the key, which the system uses for decoding, therefore, to understand the distance of uniqueness, it is necessary to know and take into account the entropy of the key, i.e. measure of its randomness.

The proposed technology of keyless vector-geometric encryption is not based on a modern, complex mathematical apparatus and does not rely on mathematical paradoxes of number theory, which seem to us unsolvable in normal time, but only during astronomically large periods.

The technology is based on an original, internally consistent, rationally organized geometric model of internal space-time with the properties of a full-fledged virtual continuum, which is constantly changing according to hybrid functions, the arguments of which are many dynamically changing parameters.

The space-time continuum is in constant relationship, but not defined for an external observer (no key), correlative with all encrypted and decrypted information and with all events of information transmission-reception processes and with all geometric events of the system occurring according to the time stamps of the internal event timer. This is a completely symmetric encryption system in which the main mode of operation is keyless.

From a symmetric state, the system takes itself out to the processes of sending and receiving information, and then returns to a new symmetric state with its pair (pair for information exchange), but only in case the information exchange is identical with an accuracy of one bit.

Events occurring in the system are controlled not by key information, but by a multitude of reconfigurable functions, most of which have the geometric nature of their relations with a multitude of arguments. These include a number of functions whose initial arguments are the entire information flow without exception. The input information (the one that needs to be encrypted) or input of information to be decrypted or information in the form of an intermediate code during all rounds of encryption is rigidly tied to its time stamps. So each specific piece of information has its own unique event management in the system.

In other words, the system proceeds the digital code not by itself, but in a continuum with internal time stamps. The entire internal space of the system, from the point of view of the processes of changing space, is also in a separate continuum with its internal calendar-time. The timestamps of the external calendar-time are used only in individual episodes of work, due to the lack of (or just unnecessary) the function of constant synchronization between 2 or more KCGs. The internal calendar-time, on the contrary, has completely synchronous operation between any number of KCG due to the different, not temporary, nature of its unit of measurement. These two time-calendars do not have common reference points, including metric ones, except for the all measurement units names. The conditional "one second" of the internal calendar-time ends and the "second" occurs only when the internal clock processes of the system are completed, regulated by the appearance and registration of the facts of formation, reception or sending of data packets.

5. Toxic platform & Ecosystem

Toxic platform & Ecosystem unites set of products developing with new type of cryptography. Major goal of Toxic products is to develop and implement environment that guarantees communication and financial freedom.

5.1 Authorization

All Toxic products use the same common authorization model. New Toxic method of authorization which is based on KCG encryption system use totally different smart approaches of user verification. Passwords are often generated with standard model of people thinking, personal biometric data, as well as private keys can be stolen (and definitely will be in extreme cases), but Toxic authorization has very different approach based on dynamic information flows over time, graphical modelling and other smart things.

5.2 Toxic Messenger standard features

Toxic Messenger consist of all the major features that have to ensure free, reliable and highly protected communication of users:

- secure messaging with single and group chats,
- audio and video calls with single and conference calls,
- smart authorization and personal settings,
- hidden chats - chats that are hidden from the main chat room,
- timer for deleting chat history.

Calls (encrypted with KCG system):

- Internal calls:
- One to one calls;
- Conference calls;
- Video calls;
- External calls:

- Landline & mobile operators paid outgoing calls (call to server is secured);
- Number purchase of landline & mobile operators in most of the countries worldwide;
- Incoming calls to purchased number of landline & mobile operators (free to users);

Chats (encrypted with KCG system):

- Regular & Secret chats, where all chats are highly secured, but secret screen is hidden with smart access and password sign protection;
- One to one (P2P) secured chat with communication history stored on devices (also encrypted)
- Switch (slide aside for launch, vertical color line on the left of screen indicated the switching) to One to one (P2P) secret chat with no communication history (history is kept till given chat is closed);
- Group chat (with communication history storage time selected by group admin);
- Desktop synchronized version (communication history is stored on all devices);
- Multimedia data storage in Cloud (Tox cloud) - all multimedia stored in chat can be moved (also encrypted) to Tox cloud to free additional space on devices, supplemented with functionality on Tox cloud to sort/see multimedia data by types (photo, video, weblinks, users, groups, etc…);
- Saved messages;
- Group & News channels;

Find a friend:

- Integrated social network service to meet people by interests;
- Find and chat with people nearby;

5.3 Toxic messenger - mobile & landline number purchase and international calls

Besides the basic functions Toxic messenger will include possibility to buy phone number of about 50 countries worldwide. Toxic gives the opportunity to have several phone numbers with possibility to make calls and receive calls and messages with purchased phone numbers.

5.4 Toxic messenger - channels & user groups

Publishing boards among other known functions will have possibility to publish and disseminate information with media attachments that can never be deleted by anybody (e.g. needed to protect information source rights over time).

New channel & groups by interest can monetize own activities with Toxic token TOX by publishing advertisements in own channels.

5.5 Toxic Wallet

Toxic multi currency wallet features:

- Fully safe usage based on top Keyless Cipher Generator system
- Extremely protected authorization & easy access
- All major crypto currencies and fiat currencies
- Online gateways between fiat currencies and crypto currencies
- Payments (online & offline) with QR code and NFC with mobile phone;
- Online banking and access to major stock and crypto exchanges;

Integrated messenger wallet has an aim to replace classical wallet with mobile phone. Connected to online banking and fiat currencies via credit card services allows to use it instead of classical payment means also, additional gateways to crypto currency world via crypto Exchanges and smart technical solutions allows to use crypto in wallet with the same ease, as classical fiat money.

Mobile wallet is the very near future of mass market financial instruments (mainly payments & transactions) and combining it with reliable communication means gives more freedom to everybody.

5.6 Toxic VPN and Email services

Main technological advantage of bi-mail service is data transfer similar to P2P, also with dynamic data information stored on the server till an email is withdrawn by recipient, but dynamic data has a totally different meaning in KCG system technology compared to standard key encryption technologies. Only the dynamic KCG code will be saved on our server until the user receives email, the letters themselves will not be there, the attacker will not be able to pick up the password for the mailbox and crack it, as this is happening with our mailboxes, because the mailboxes themselves will be created on the mailbox user devices. Plugins to regular email services will integrate mentioned workflow to major email services. To protect user from loss of email information when device is lost, there are options to synchronize mailbox on few devices or archive data on distributed servers system where only a small piece of information (also encrypted with KVG & GVEM) is stored on a single server.

Toxic bi-mail (email) service features:

- Fully secured email service with top new encryption based on KCG with GVEM;
- Secured synchronized communication channels;
- Encryption plug-ins for major email services;
- Virtual keyboard for safe set of texts;
- White noise generation;
- Integrated VPN service;
- Access protection from third party software;
- Integrated calendar;

Though messengers already confidently conquered much of the market for personal communication, personal and more business communication is still based on the use of email services from major global brands. So, personal information is still under the control of large corporations and can be sold to different third parties like marketing agencies.

Toxic bi-mail email service (including security plug-ins to major worldwide email services) will allow to hide personal sensitive information and all relevant communication information from unwanted access.

There is no secret that everything person talks or writes is traced and analyzed to give maximum targeted advertisement. And it is obvious that large corporations and governments possess information about people user profile, preferences, friends, emotional pictures. Toxic solutions aim to turn the trend back and close all personal and valuable information from anybody.

6. Roadmap

September Q3, 2018 - R&D and product concept

January Q1, 2019 - Toxic messenger Beta release

May Q2, 2019 - Keyless Cipher Generator (KCG) system with Geometric Vector Encryption Method (GVEM) research & techpaper

October Q4, 2019 - Toxic messenger MVP for iOS and Android with TLS 1.2, DTLS

OctoberQ4, 2019 - Pre-ICO Start: KCG with GVEM & Toxic Ecosystem (messenger, bi-mail service, wallet). ERC-20 Toxic tokens TOX available to early investors with very attractive prices

April Q2, 2020 - General Sale ICO Start : KCG with GVEM & Toxic Ecosystem (messenger, bi-mail service, wallet). ERC-20 Toxic tokens TOX available to all investors

December Q4, 2020 - New encryption technology Keyless Cipher Generator (KCG) system with GVEM available to market

February Q1, 2021 - Toxic messenger Alfa release based on KCG with GVEM available on the market, as part of Toxic Ecosystem

July Q3, 2021 - Toxic multi wallet with fiat-crypto currencies gateways based on KCG authorization available on the market, as part of Toxic Ecosystem

December Q4, 2021 - Toxic VPN and bi-mail (email service based on KCG with GVEM) available on the market, as final product of Toxic Ecosystem

7. Governance, financials & token economy

7.1 Governance

A company developing Toxic project and Toxic Ecosystem is Toxic LLC.

The company is owned and managed by founders according to their own views and follows the requirements and project plan to achieve results indicated in our ICO roadmap, Toxic Whitepaper, Toxic Techpaper and other project documents. All the developments that the company already possess and future solutions in encryption and software development will be fully owned by the Company.

The company management has obligations to reach financial indicators of Toxic token economy such as TOX token market price projections, P&L financials and regular audits.

To attract funds for the Project development the Company issues TOX Tokens according to the rules defined in this document and related ICO agreements with the Token economy defined below in 6.2.

Sales of TOX Tokens goes according to the schedule and rules set out in this document and other related ICO/IEO documents and are performed by the Company and crytpo exchanges contracted by the Company. To make TOX Tokens more attractive for Purchasers and protect the value of Tokens against market fluctuations the Company has decided to provide additional benefits to Token holders in the form of **fixed minimal TOX token exhange rate 1 TOX = 1 USD to be used to purchase paid Toxic services, such as:**

- Corporate messenger;
- Purchase of mobile/landline phone numbers worldwide;
- Purchase of VPN service;
- Few wallet paid services;
- Advertisement posts;

Table: regular audit (outsource):

Audit	**Aggregated 2020 year**	**Aggregated 2021 year**	**Aggregated 2022 year**	**Aggregated 2023 year**	**Total**
Quantity of audits in a period	4	4	1	1	10
Cost per audit, kUSD	12	12	50	50	
Audit company	local licensed	local licensed	big 4	big 4	
Total cost in a period	48	48	50	50	196

Also, we are the company with internal structure corresponding with organizational model that specifically suits the needs of natural growth and self management resulting in higher efficiency. Company's independent employee performance is complemented with inputs from Toxic development society that are self managed according to **Holacracy method** of decentralized management.

Development society inputs are managed and remunerated on the same basis as regular company's employees. Everybody wanted to join Toxic Development society can do this on our website: www.toxic.chat

7.2 Token economy

	Value	Measure	Description
Soft cap	1,250,000	USD	(accepted currencies - BTC, ETH, BCH, LTC)
Hard cap	1,800,000	USD	(accepted currencies - BTC, ETH, BCH, LTC)
Token economy			
Total supply	8,000,000	tokens	
Token distribution:			
- ICO investors	6,250,000	tokens	78,12% of total tokens
- pre-ICO investors	750,000	tokens	9,38% of total tokens
- bounty & advisers	500,000	tokens	6,25% of total tokens
- reserve	500,000	tokens	6,25% of total tokens
Token name	Toxic	TOX	
Token pre-ICO price per 1 TOX	0,10	USD	
Token ICO/IEO price per 1 TOX	0,20	USD	
Token guaranteed exchange rate in Toxic paid services	**1 = 1**	TOX/USD	Corporate messenger; Purchase of mobile/landline phone numbers worldwide; Purchase of VPN service; Few wallet paid services;
Token utilization (advertisement view per 1 TOX)	0.01	% of all Toxic users	Meaning that one advertisement post to all Toxic users in all products cost 10,000 tokens. More users of Toxic the higher is market price
Premine	100	%	There is legal restriction on the level of the Company's articles to NOT issue any other tokens/coins that can be used to sell Toxic services
KYC & restrictions	-	none	KYC check is not required / There are no restrictions for international investors

More detailed token economy will be provided upon the request.

7.2.1 General information

The major point of Toxic token utilization model giving maximum growth of TOX token value in future is based on legal Company's obligation to sale advertisement posts in any product comprising the Toxic Ecosystem to third parties (provide advertisement channels in all Toxic products) with Toxic tokens (TOX) only. Given obligation is indicated in the Company's statutory documents and in documents related to the TOX Token sales in scope of this ICO. In parallel, there is a way to guarantee token owners the minimal value of TOX token by using it as a payment mean for paid Toxic services, such as corporate messenger subscriptions, purchase of mobile/ landline phone numbers worldwide, VPN services, some of crypto-fiat wallet services.

User groups and media channels (news, gamer clubs, etc…) in Toxic Ecosystem have to sell own advertisement posts via Toxic platform tools also utilizing Toxic tokens (TOX).

All related advertisement transactions will be made on a per-view or per-click basis accompanying with the necessary statistics and guarantees provided to all parties.

To get resources needed to realize our project an ICO/IEO (including pre-ICO) consisting of rounds (Tiers of pre-ICO and ICO) with TOX Toxic token sale will be launched in 2020. Toxic token called TOX is ERC-20 token based on Ethereum blockchain.

7.2.2 Token Pricing, Allocation and Distribution

To reward our early Purchasers who believe in us and entrust us with their money before everyone else recognizes the amazing potential of the new Encryption technology and Toxic Ecosystem products, we are organizing the Token sale in stages.

We are convinced that everyone who joins us now, while the company is barely taxiing to the runway, will see amazing returns on their purchase price when we really take off, including those who join us later in this Campaign.

In fact, our first-Tier token Purchasers will get almost 5 times more for their money than those who join us in the final stages of the Campaign!

The following table shows the Tiers of pre-ICO and ICO and available TOX Tokens for sale:

Stage (Tier) of pre-ICO & ICO	**Amount of USD to be collected**	**TOX Token price in USD**	**Tokens Available for Purchase**
pre-ICO	75,000	0.10	750,000 Active
ICO/IEO	1,250,000	0.20	6,250,000
TOTAL	**1,325,000.00**		**7,000,000**

7.2.3 ICO details

Bounty program benefits:

- Article Writing & Distribution

Reward per unique post with min 500 words. Must be positive and interesting. Reward per post: 1.000 TOXs. High traffic articles which perform well up could be rewarded up to 5.000 TOXs.

- Social Media Tasks

Share on Facebook/Twitter/LinkedIn and get up to 100 TOX tokens i.e. 10 TOX for every share. Share any interesting content from our social channels. Minimum audience size of 200 friends. No fake spam profiles will be rewarded. We reserve the right to accept or deny any bounties or amounts to be rewarded based on the quality of audiences reached.

- Video Review

Positive videos with an interesting explanation and decent audience (min 500 views): 2.000 TOXs + bonus tokens based on views and incoming traffic up to 10.000 TOXs.

7.2.4 Token Utilization model

Step 1, in 15 months after successful ICO/IEO finish:

All paid Toxic services, such as corporate messenger subscriptions, purchase of mobile/ landline phone numbers worldwide and external call minutes, set of VPN services, some of crypto-fiat wallet services can be paid using fiat money and TOX tokens. The exchange rate will be fixed for all the times and is 1 TOX token = 1 USD. This is the minimal price we can guaranty for token holders that purchased TOX during pre-ICO and ICO/IEO rounds.

Step 2, in 36 months after successful ICO/IEO finish

After first Toxic product - Toxic messenger based on new encryption technology KCG & GVEM is fuuly deployed and the number of all Toxic products achieves the number of 1 mln users the company will start to sell advertisement posts to third parties. The permanent ratio how to calculate advertisement cost is following:

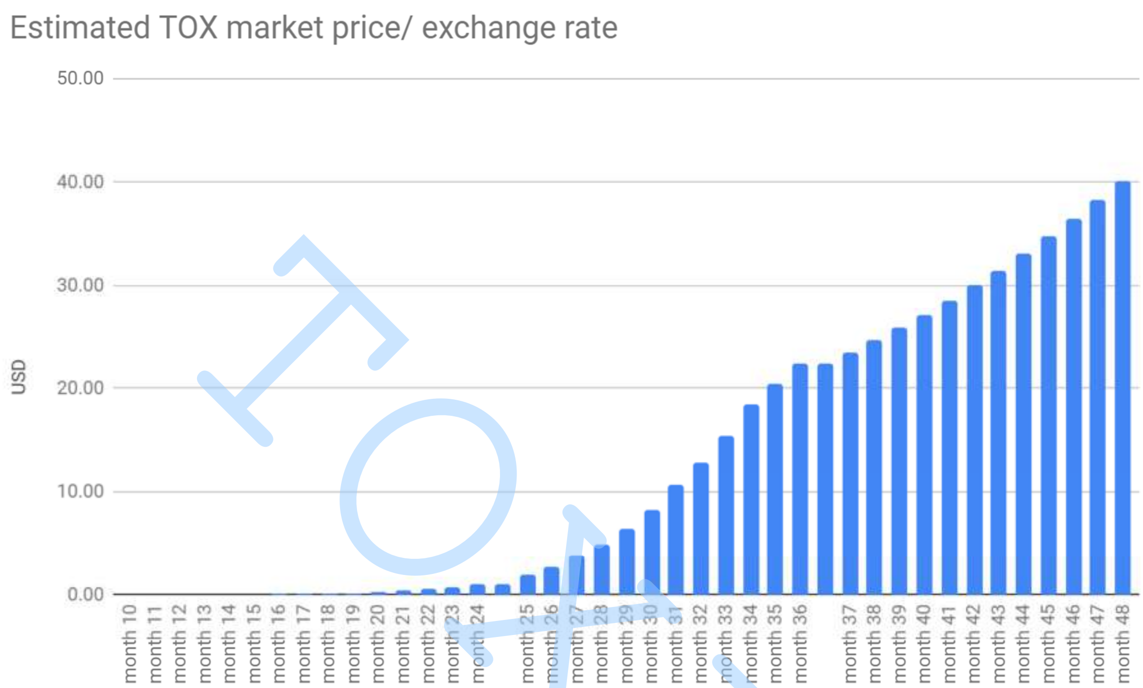
1 TOX = number of one time views by 0,01% of total product users

Following Toxic products - Toxic multi wallet online banking & exchange trading and Toxic bi-mail will bring additional sale channels for the Company to sell advertisement posts with TOX tokens. There is no possibility to clearly indicate market price of TOX token. While nominal TOX price (ICO price) is defined as 0,20 USD there are formula to estimate future market price of TOX tokens:

$$\text{1 TOX market price***} = \frac{\text{Number of applications users}}{1\ 000\ 000}$$

*** based on minimal projected rate for non-personalized advertisements:

1 advertisement post = 0,01 USD

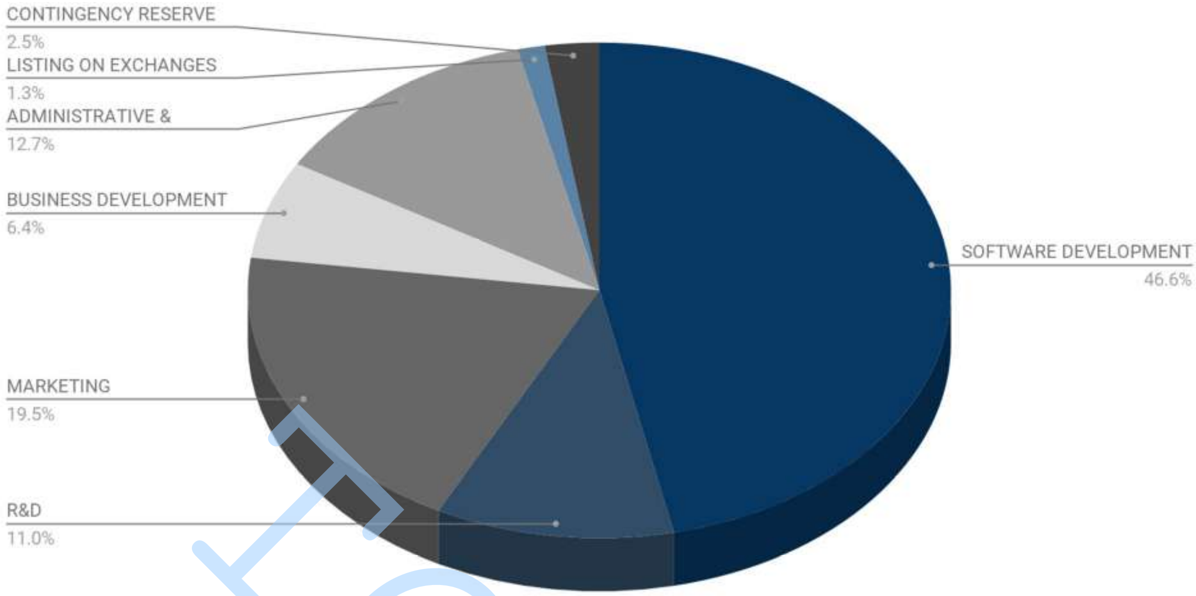


TOX exchange rate volatility	In 2 years	In 3 years	In 4 years	Future projection
%	99.18	93.18	84.63	permanent decrease

7.3 Financial model (P&L):

Financial model will be provided upon the request.

8. Use of Funds



EXPENDITURE	in kUSD	%
RESEARCH & SOFTWARE DEVELOPMENT	1,108,495	83.66%
MARKETING & BUSINESS DEVELOPMENT	147,737	11.15%
ADMINISTRATIVE & OPERATIONS	68,767	5.19%
Total	**1,325,000**	**100.00%**

9. Toxic Development Society

We invite developers and Toxic product users to join further development of our products by means of collecting users feedback, features development, technical solutions development. From our side we can guarantee that every useful input will be properly remunerated.

Communication and management among team members, developing society and Toxic users will be done using multi level of management circles (Holacracy principles) connecting people by interests. Please, join us via our website.

Holacracy is a part of the Teal movement focused on self-management. Positions, called “Roles”, are defined around the work, not people. Each person fills several roles according to one’s skills and talents. They may come from different circles (groups of roles) and are defined by name, purpose (an inspiring reason to act), accountabilities and few other elements. Roles can be created, removed or updated during the Governance Meetings. This regular and structured process helps the organization to adapt and resolve “tensions”, which are problems or improvements.

10. Team

10.1 Founders

Yaroslav Pryymak

CEO & Co-Founder

Senior strategic adviser with 15+ years of progressive experience in finance, law, IT in business development and optimization within startups and global multi-billion organizations. Streamlines business operations that drive growth and increase company's profitability via improving product vision and business models resulting in smart monetization strategies. High qualifications in IT start-ups, corporate governance & business optimization, developing financial controls and business processes audits leading to productivity improvements.

Strong experience and high results achieved are based on breakthrough solutions for optimization of governmental and business structures & development/ launch of top market products. Supplemented with strategic market/product visions & smart implementation plans, comprehensive business models that always led me to introducing best solutions on the market.

Marina Lishchenko

COO & Co-Founder

Experienced strategist, manager and startup enthusiast with a passion for building and growing businesses. 8+ year track-record of launching new ventures, and delivering operational impact, both as a co-founder and management expert. across a wide range of industries including enterprise software, digital marketing and government. Major experience lies in strategizing and leading cross-functional teams to bring about fundamental change and improvement in strategy, process, and profitability.

Result-oriented professional with attention to details and thoughtful approach. Ability to operate in complex multicultural environments with the tough deadlines.

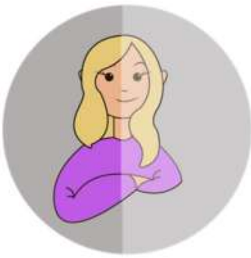
Andrew Mykhaylyshyn

CTO & Co-Founder

Extensive international and domestic experience in executive leadership (CTO) and development roles. Technology leader with a background in fintech, commerce, and telecommunications. Experience building various ios, android applications from the scratch. Experience with cryptography, PKI, and data security area. Passionate to achieve scalability, high-availability, fault-tolerance and performance increase. Turning vision into a tangible technical roadmap.

Experience in development on several programming languages for ios, android linux, windows, osx. Oriented on high quality.

10.2 Other Notable Team Members



Julia
Business Development
Passionate about Internet Technology, Innovation & Blockchain. I work with cross-functional teams to develop global businesses.
Business Development Specialist with more than 10 years of experience in conducting business and networking around the Globe. With a keen understanding of public and private chains, Julia is one of the most passionate, and insightful influencers in the space for her views.
Julia's background is in international business development and investment management.

Sergey
Senior Full Stack Developer
Senior Full Stack Developer with extensive experience in building high quality products.
Sergey has more than 4 years of experience in web and server-side

development. Worked with corporate websites, mobile applications for iOS and Android, different e-commerce platforms. The main principles of work are: quality and punctuality.

Den

Senior iOS Developer

6 years of iOS development experience, 10 years overall IT background. Deep knowledge of Swift, Objective-C and C/C++. Mathematical and cryptographic background. Projects in portfolio: telecom, social networks, e-commerce, healthcare, games.

Experienced in team leading and mentoring, conducting full development lifecycle.

Maxim

Senior Android Developer

Highly experienced specialist with more than 7 years of Android development and C++ language background. Actively involved with the latest technology and updates Java/Kotlin and Android application development field.

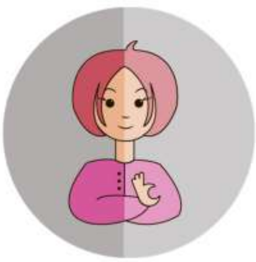
Passionate about writing well-designed, testable and efficient code.

Alex

Web Developer

Web Developer with a passion to build world-class web products from the ground-up. Overall 5 years of Web development experience including 3 years of Web applications development experience.

Alex likes to enhance skills and learn about new technologies.



Alice

Designer

Over 4 years of experience which covers the entire design process of creating web and mobile projects, including user interface design and user experience design, brand and visual communication design. Experienced with responsive & adaptive design. Adores to create digital products to make people's lives easier and more colorful. Alice strives to build a product experience that will be manageable, user-friendly, and scalable.

Team of encryption experts and mathematicians:
3 encryption experts, 1 mathematician expert