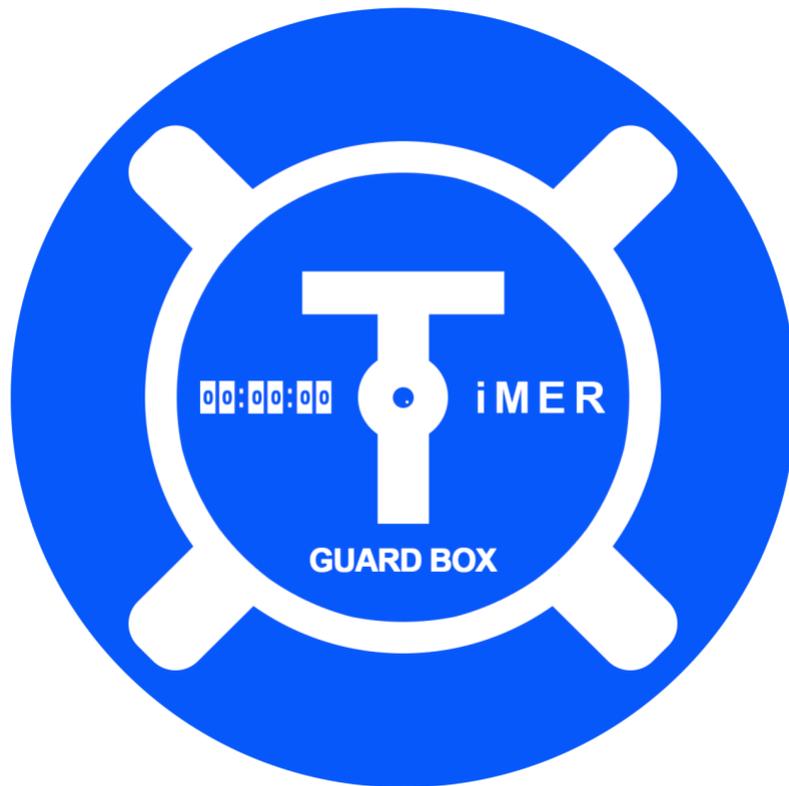


Timer Guard Box

Time is the best Lock & Key

White Paper



2018

Contents

First introduction	3
Conceptual application schema.....	6
Use Cases	8
Technical aspects of the app (will be updated)	11
Tokenization and economy of the project.....	12
Road map.....	14
Team	15

First introduction

From the ancient times, from the moment when human received consciousness, information has gained enormous value. And with it a need of a secret, mystery and confidentiality appeared. For example, information about location of a dead mammoth body was very valuable for the tribe. At the same time it was kept in secret from the competitors. Prosperity and life depended on it. Many years have passed since those times, and information became the most costly thing in the world. Such a rapid growth in the value of information, informational technology has caused no less boost of the problems with storage and protection of the data. Nowadays, there are a lot of scientific works, organizations and institutions, which are working on the problem of security. In the net, reviews of the problems, their actuality and existing solutions could be easily found. But we will not stick at details.

In recent years one of the most revolutionary technologies in the field of securing data storage is blockchain. Now, thousands of engineers are using blockchain to develop innovative solutions to data storage problems.

Back in 1975, Jerry Saltzer and Michael Schroeder in the article "Protecting Information in Computer Systems" proposed to divide the problems related to data security into three categories. This principle is the basis for any security systems. Together, these three categories are called "CIA Triad".

Confidentiality

Confidentiality as a property of information can be unavailable or closed to unauthorized persons, entities or processes.

Integrity

Integrity - the property of preserving the correctness and completeness of assets.

Accessibility

Availability - the ability to be accessible and ready for usage.

Blockchain is the universal solution for the first two categories of problems. This is the best solution to ensure the confidentiality, integrity, completeness of the asset.

However, the most difficult problem is accessibility. That is the vulnerable spot. This category of problems can be represented by two words - **lock and key**. And these two words also have a long history. Evidently there are million of things, processes and mechanisms that perform the function of a lock. Though the lock can not exist without the key. In the opposite case, it loses any sense. Then, you can not help agreeing the fact that if there is a lock, there is someone who can hack it for sure or, to be more

precise, open it unauthorizedly. The uncracked lock can be compared to any other utopia, such as a perpetual motion machine or the elixir of youth. Every invented lock has been hacked or will be hacked in the future. It's hard to argue with that.

But there is one absolute parameter which was not overcome by the modern humanity - **time**. No one can hack time, no one can change it. That is why time is the perfect lock. It can not be hacked (at least in the 21st century). But time is the lock and the key simultaneously. Moreover the time key has the unique quality - it can open other locks as well! All these thoughts led us to the idea of creating of decentralized application which will use Tron`s blockchain. Timer Box for Timer Protection - "**Timer Guard Box**".

Conceptual application schema

Timer Guard Box is a multifunctional platform for storing valuable information. The main principle of operation is closing and opening of information using the time. For simpler perception, you can call it timer. Or draw an analogy with a time capsule. Any object that is placed in the box will be available at the specified time. At the same time, ensuring the exact, guaranteed fulfillment of the condition opening the box will be the blockchain network. Since today, this is undoubtedly a revolutionary solution, such a category of information security problems as the integrity or authenticity of Integrity.

Let's look at the box structure in more details.

The box itself will be a container that will contain various kinds of information and have the following parameters:

- **Content** is the information that we need to save: text, video, audio, photo and other files.
- **Opening date.** Time settings Period of opportunity and conditions for changing the opening date of the box. This is a rather important parameter, the key feature of which is the possibility of shifting the date of opening the box with information only forward in time (hereinafter this position will be described in more detail).
- **Addressee or recipient** of the opened box. The method of notification and delivery of information.

- **Estimated cost** of the box, as an additional option. Set the price for early opening of the box.
- **Description.** Public, publicly available description of the contents of a closed box.

Such a schematic description of **Timer Guard Box** does not provide a complete picture of the capabilities and functions of this platform. Therefore, we suggest you to acquaint yourself with the description of the possible examples of using the application below. That will give a clearer picture of the work of the **Timer Guard Box**

Use Cases

Storing of private keys of a cryptocurrency wallet. Do you use cryptocurrency? Probably you keep your keys in secret. Write down on paper, keep cryptocurrency on a cold wallet. Have you ever had cases when you lost your private key and with it access to your money? Sheet of paper was spoiled. A cold wallet was stolen. The hard drive was destroyed. Perhaps you have seen funny situations in modern films and TV shows when the characters are looking for the lost wallets with cryptocurrency at the dump. Yes, it's really fun, until it happens to you. With the **Timer Guard Box** help, such problems will stop to disturb you. You will have the opportunity to create a box in which you place your access keys, it will be stored in the blockchain. In the **Timer Guard Box**, you will indicate that once a month (*optional*) you will receive a message with a link, using which you confirm that everything is in order and the date of opening the box will be moved further in time. If you miss several confirmations (*optional*), this private key will be sent to you at the specified address at the specified time. There is no other way to open the private key box. Let's imagine that you have lost your key and there is no way to restore it. In this case, you stop confirming incoming requests from **Timer Guard Box** and a month later (*optional*) after the last request, your key will come to your e-mail address. In this example, it works like this. You have created a box in which you placed your private key and indicated when it will be opened. In each subsequent message with a confirmation request, the date of opening is transferred to the future for a specified period. Thus, **Timer Guard Box** as if pings you and in case of not receiving a response from you, the box opening mechanism starts.

Holder. Are you a real holder? Are you going to store coins for several years? Create a box and set the time to access the wallet. **Timer Guard Box** will give you access at the exactly designated time. If this moment has not come, you could still have the opportunity to accumulate coins in this vault without worrying about the security of your private keys anymore.

Sudden loss of capacity. Have you ever thought about what will happen to your crypto wallets and money if you suddenly lose your capacity as a result of an accident? Do your relatives know what a cryptocurrency is, how to use it, and in general that you have it? If something happens to you will your money be gone? To solve this kind of problem, you can use **Timer Guard Box**. Put the data in the box with your private keys. Create detailed instructions on what to do with this information. Specify contact details of proxies, relatives or loved ones. Specify the way the message will be delivered (*sms, e-mail, phone call*). After that, you will begin to receive a message once a month (*optional*) with a link, clicking on which will confirm that everything is fine with you. If **Timer Guard Box** does not receive a message from you, the mechanism for opening the box with information on the previously specified parameters will start.

Safety guarantee. Perhaps you have the information that you need to deliver to interested parties if something happens to you and you do not get in touch? Put the secret information in the box. Start the timer. At the appointed time, you will receive a notification with a link that confirms that everything is fine

with you and the sending of information will be canceled. But if you do not get in touch, the data from the box will be sent to the addressee.

Time capsule. Do you have a message that you want to send to the future of humanity, friends, and perhaps yourself? Put the message in the box. Specify the date when it will be opened. Specify who should receive your message and **Timer Guard Box** will deliver it.

Data merchant. The box with the price of early opening. Do you have information that is valuable? Box valuable content in the box. Create a description of the contents of the box. Specify the cost of early opening the box. If your information finds a buyer, you will receive payment, and the buyer will receive the contents of the box using **Timer Guard Box** platform.

These are just examples of the possible use of **Timer Guard Box**. But these examples provide an opportunity to more clearly present the principles of operation and the potential for using this application.

Technical aspects of the app (will be updated)

At the time of writing, the paper is under development. As progress progresses, this section will be updated.

The infrastructure and mechanisms of the application will be organized in the environment of **TRON**. Each key event will be confirmed by the blockchain network through the implementation of smart contracts.

Tokenization and economy of the project

Timer Guard Box will be provided with its own **TGB** token.

To create the box, the user will need to spend 5000 TGB.

In this case, at the time of creation, the token will be frozen. The token remains frozen until a data disclosure condition occurs. After the information is opened and all the conditions are met, the token will be available for use again. In the event that the box received the status of permanent information hiding, the token will be burned, access to the token will be impossible.

In addition, as you expand the functions of the application, additional paid options will be created.

The funds earned from the sale of services will be spent on the maintenance of the project, payment for the work of the attendants, development of the application.

Scheduled services and service

Premium payment services		
Box with its own design in the TimerGuardBox space (Personalized-Box)	5000	TGB
Box with info for sale - early opening (Trade-Box)	1 %	fee
Box with the cost of destruction (Secure-Box)	1 %	fee
Store media files in Box integrated with BitTorrent and Atlas project, per MB per month (File-Box)	5000	TGB
Box for quests and other games (Game-Box)	5000	TGB
Personal address delivery from the (Delivery-Box)	250000	TGB
Certificate of confirming the contents of the file in the past (Contract-Box)	500000	TGB
Base services		
Auto-Extended Box (Holder-Box)	5000	TGB

Simple Box with a deadline and 1 recipient (Simple-Box)	5000	TGB
Demand Box by unique id (Demand-Box)	5000	TGB
Box with a message with a choice of receive messenger (Message-Box)	5000	TGB
Every added extra email option	3000	

Also, payment of dividends to holders of tokens is provided. The minimum number of tokens that is needed to obtain a portion of the profits from sales of services and services is 2500000 **TGB**.

The project **Timer Guard Box** one-time released 3 000 000 000 **TGB** tokens, which go on sale from the moment of creation.

Face value 20TGB = 1 TERC/TRX

Primary distribution of tokens:

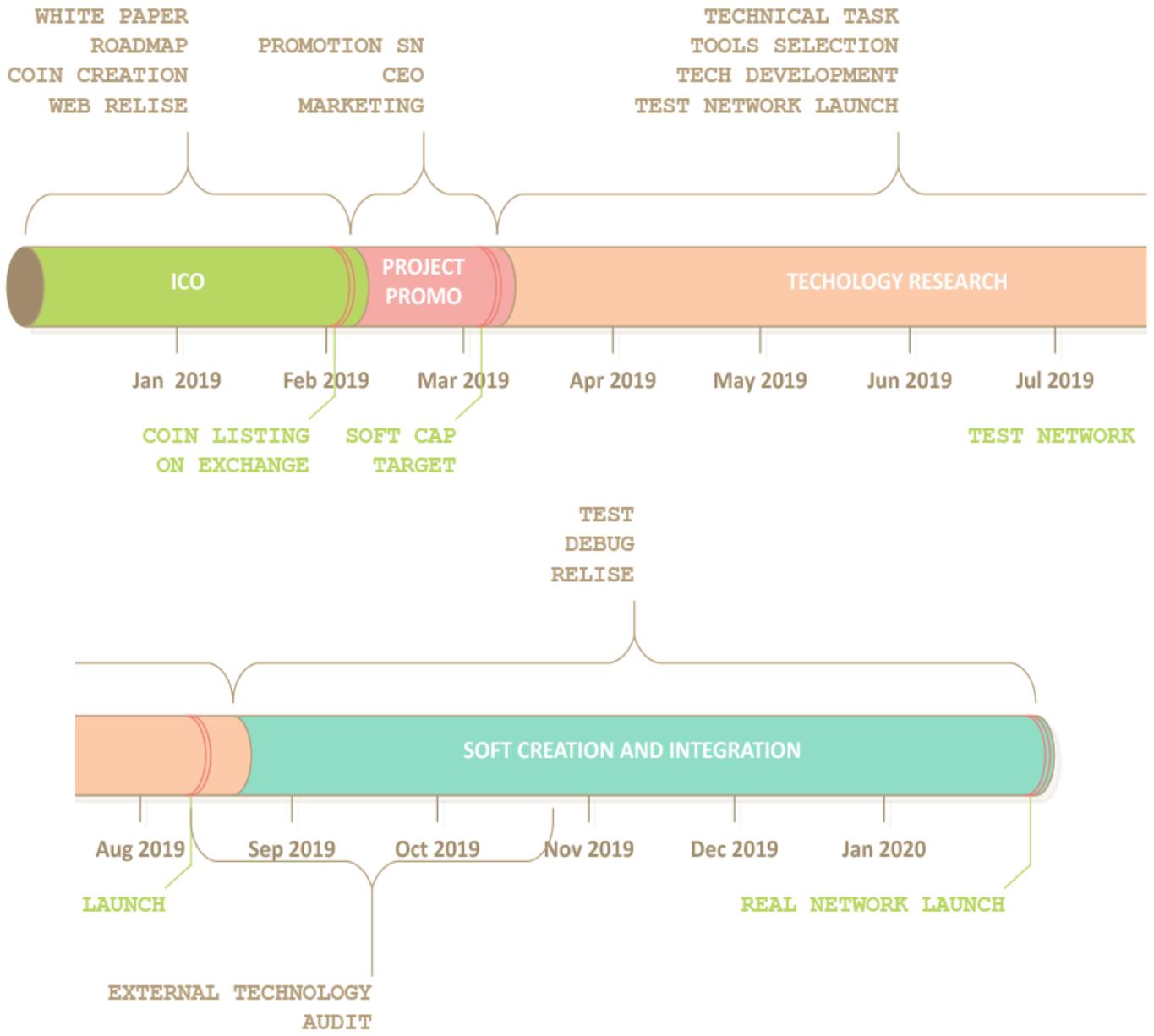
13.3% TGB - reserved for paying team members

20% TGB - reserved for private sale to institutional investors.

3.3% TGB - will be spent as the primary distribution to potential users as an airdrop.

63.3% **TGB** - go to the exchanges

Road map



Team



Aleksey Yemelianov
CEO. Co-Founder



Victor Lushinkov
Chief Technical Officer



Olga Novikova
Chief Marketing Officer



Egor Tkachov
Public Relations Manager