CryptoWorkPlace

White Paper

ver. 2.0 06/30/2018

«Protect what is important»

Website: http://cryptoworkplace.io | Web Portal: http://cryptoworkplace.com

Table of contents

INTRODUCTION

Our mission is to design the safest innovative devices & systems to protect personal data and client's finances all around the World.

CryptoWorkPlace - decentralized system based on a personal computer the size of a USB flash drive, providing unprecedented protection against hacker attacks, malicious programs and unauthorized access to data.

There are currently a few options on the market that allow you to protect your cryptocurrency wallet by keeping the keys in a separate device that connects to your PC. That being said, with the current rate of technological development, even if your PC has an up to date anti-virus, one can never be fully confident that it is impenetrable. Hackers can come up with new ways to penetrate your system faster than anti-viruses can come up with the right "medicine" for the attacks. Before long, you can lose access to your cryptocurrency wallet, and thus your money.

The CryptoWorkPlace (CWP) Micro-PC is not a secure key storage, it is a fully independent PC with an operating system and applications; It only needs a monitor, keyboard, and mouse from an external computer. The security of this external computer is irrelevant since it only is used to visualize the information. All of the actual processes take place in the secure internal memory of the CWP Micro-PC.

Since the CWP is a PC and not just a cryptocurrency wallet, it offers the user many useful features. One can get a variety of useful apps such as a multicurrency wallet, access to a few different trading platforms at once, chat channels, and other services which can make life much easier. All of these available services can be conveniently combined on one homepage panel. Thus you are able to move all the vital information you desire to the forefront of the abundance of useful features that are available.

At the core of the CWP ecosystem is a mechanism for automating contract-based functions and distributed registry of statuses.

1. PROBLEM

1.1. STATISTIC OF LOSSES FROM HACKING OF COMPUTERS OR CRYPTOCURRENCY WALLETS

1.2. EXAMPLES OF THE LARGEST ICO HACKS IN 2017

According to a Chainalysis report (https://blog.chainalysis.com/the-rise-of-cybercrime-on-ethereum/) the world is seeing a meteoric rise in cybercrime targeting ICOs.

In June 2017 alone investors loses from such actions reached $100M while in August they were above $220M.

TYPES OF CRIME	DESCRIPTION	LOSS AMOUNT ($M)	NUMBER OF VICTIMS
Phishing	Obtaining of sensitive information (logins, passwords or private keys) by disguising as a trustworthy entity in an electronic communication.	115	16 900
Exploit	Using software, bits of code, or a sequence of commands to attack computer-based system.	103	11 000
Hack	Obtaining unauthorized access to computer system.	7,4	2 100
Ponzi schemes	Fraudulent investment schemes, pyramids	7,4	260
	Total	225,4	30 260

This way investors are at risk from both sides: they can lose the money they invested and the contents of their cryptocurrency wallets. It is obvious that no technical solutions can prevent voluntary participation in a Ponzi scheme, but total losses from that kind of crime are relatively small.

1.3. MELTDOWN AND SPECTRE - HARDWARE VULNERABILITIES OF ALL MODERN PROCESSORS

Vulnerabilities Meltdown and Spectre (https://meltdownattack.com) were independently found by researchers of Google, Cyberus Technology, and Graz University of Technology in the middle of 2017 and were published on January 4, 2018.

The Meltdown attack allows unauthorized access to read privileged memory used by the kernel of operating systems. Intel and ARM processors are vulnerable to the attack, while AMD processors are not.

The Spectre attack allow a program to read random areas of memory, including ones used by other applications, which breaks memory isolation between programs. Intel and AMD processors are vulnerable to the attack, as well as some ARM processors.

Thus there is no computer system safe for these attacks - so there is a probability that users may lose access to their important data, including wallets, in any second.

It is needed to replace hardware, completely update the operating system, and re-compile all software with new compilers replacing vulnerable code to fix these issues. It is clear that it is not enough to use traditional approaches, such as patches, to prevent these attacks - as the vulnerabilities are on the hardware level and they completely destroys assumed notion of sandboxes.

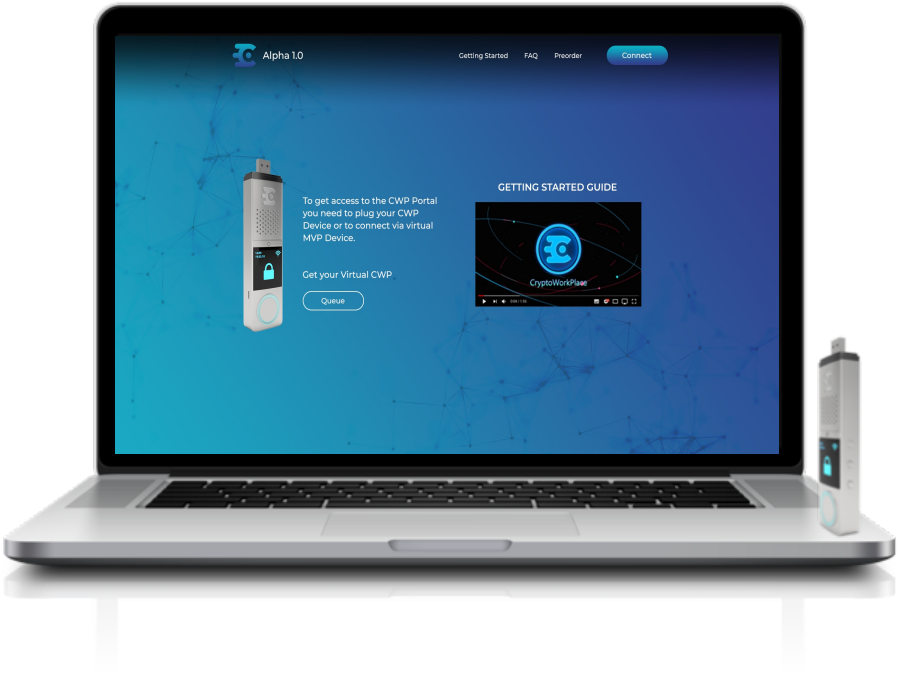
2. CRYPTOWORKPLACE: THE SOLUTION

2.1. THE SOLUTION

The CWP user can protect themselves from these different types of attacks. A common recommendation for maximum security is to use a separate PC running Linux with all applications that have access to the internet removed for your cryptocurrency wallet uses. However, it is not enough anymore with recently discovered Meltdown and Spectre vulnerabilities.

The CWP Micro-PC serves exactly that purpose but with the advanced security infrastructure allowing to access the Internet and use crypto wallets without having to worry about hackers. If that wasn't enough, all these features come in a portable USB drive size and can be taken with you wherever you go and used whenever you need it.

The CWP Micro-PC uses an updated kernel of operating system and applications, recompiled with new compilers, to prevent Meltdown and Spectre attacks. Moreover, all important information is kept not in random-access memory, which may be the subject of said attacks, but in the built-in crypto-storage.



2.2. TECHNICAL SOLUTION

CWP is a decentralized ecosystem based on a blockchain technology that includes a Micro-PC that enables applications to run in a secure, isolated environment, special software, a set of CryptoWorkPlace Web portal services designed to organize protection against threats on the network, and a distributed registry of statuses.

The user gets access to the following functionalities as soon as he registers on the CryptoWorkPlace

Web portal:

- Attaching the device to its inventory record;
- AI behavioral user control
- Switching on two-factor authentication and its type;
- Decentralized APP-Store (wallets, mining, trading programs) and update service;
- Setting up a list of third-party Websites and network services accessible from the device;
- Setting up geographical zones to set up VPN connections from the device;
- Blocking the device in case of loss and remote data erasing.

The CWP Micro-PC uses a modern high-efficiency processor and has its own memory. It is connected to a donor computer through a USB connection, which becomes its power source. The donor computer sees the Micro-PC as a regular network card.

A secure tunnel is created over the network connection (VPN-tunnel) and the user communicates with the Operating System of the *CWP* Micro-PC and applications installed there through this VPN-tunnel. As the Micro-PC is powered on, it checks that the device is not blocked on the CryptoWorkPlace Web portal and opens the authentication window for the associated user. To get access, the user should provide, in addition to the standard credentials (username / password), a second authentication factor that he specified in the CryptoWorkPlace settings. Such second factor may be one-time code received by email, SMS-message or a special mobile application (for example, Google Authenticator). Thus isolated environment and access mechanism eliminates phishing possibility.

The Operating System of **the CWP Micro-PC** is located in write protected memory section and doesn't allow to make any changes neither by user nor by harmful programs. Necessary software may be installed and updated only through the *CWP*. The programs, not signed by *CWP* Web portal key, cannot be started or modified. Thus, the isolated environment and electronic signing of programs eliminate exploits possibility.

The programs are executed in the environment isolated from the computer-donor. User data are encrypted on the device (by user's choice) that creates reliable defense from hackers.

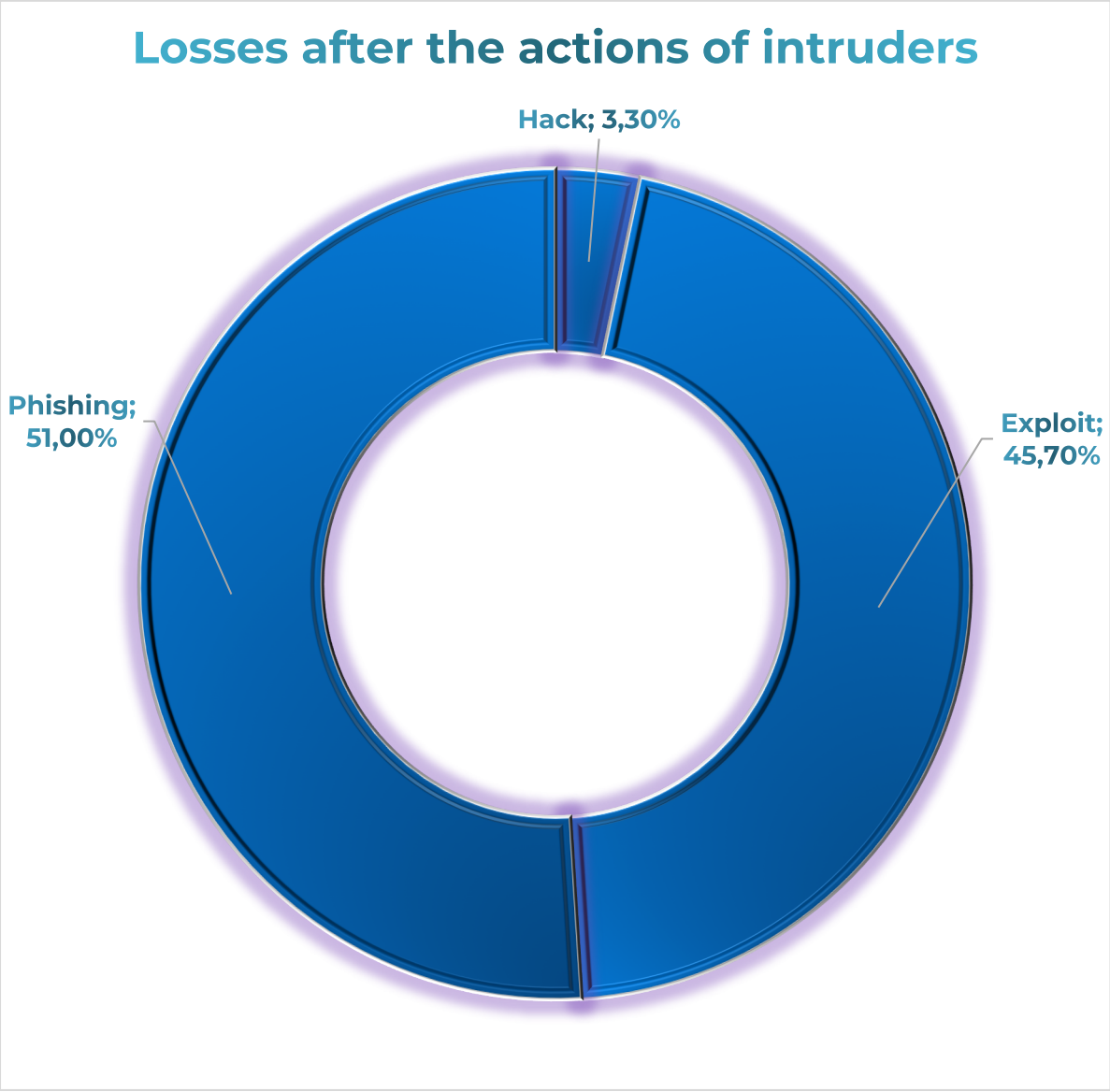
The CWP Micro-PC uses built-in 4G-modem or WiFi-adapter to connect to the Internet, establishing a VPN-connection to the server specified in the settings. There are multiple connection points for encrypted traffic in different countries, so it is not limited by geography. Any traffic around VPN is cut off.

In case of loss or damage of the device *CWP* user can block the device and remove all data saved there, which would be executed as soon as the Micro-PC would be connected to the Internet. A new device may be attached to your account restoring all settings and all programs from the previous device.

The device has built in crypto-storage for transaction signing to secure crypto-wallets private keys.
The pre-install browser allows to open only the sites from the white list of addresses on the CryptoWorkPlace server to prevent phishing attacks.

Thus, returning to Chainalysis data about cyber-crimes, we may see that CWP prevents all existing security problems for crypto-wallets:

- Phishing - by using the pre-configured browser and applications, signed by a special key;
- Exploits - by working in an isolated environment and by signing programs;
- Hacker attacks - by using built-in unbreakable crypto-storage.



2.3. PRODUCT HISTORY SINCE 2008

The Micro-PC CWP was first thought of in 2008. In 2009 the product was patented and work started on the prototypes for corporate clients.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ПОЛЕЗНУЮ МОДЕЛЬ

№ 89256

МИКРОМИНИАТЮРНЫЙ ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР С ЗАЩИТОЙ ИНФОРМАЦИИ

Патентообладатель(ли): *Саруханов Ваган Арменович (RU)*

Автор(ы): *Саруханов Ваган Арменович (RU), Комов Игорь Юрьевич (RU)*

Заявка № 2009131804
Приоритет полезной модели 24 августа 2009 г.
Зарегистрировано в Государственном реестре полезных моделей Российской Федерации 27 ноября 2009 г.
Срок действия патента истекает 24 августа 2019 г.

Руководитель Федеральной службы по интеллектуальной собственности, патентам и товарным знакам

Б.П. Симонов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ПОЛЕЗНУЮ МОДЕЛЬ

№ 98104

РАСПРЕДЕЛЕННАЯ АВТОМАТИЗИРОВАННАЯ СИСТЕМА МОНИТОРИНГА ЗДОРОВЬЯ

Патентообладатель(ли): *Государственное образовательное учреждение высшего профессионального образования "Московский государственный медико-стоматологический университет Федерального агентства по здравоохранению и социальному развитию" (RU)*

Автор(ы): *см. на обороте*

Заявка № 2010102485
Приоритет полезной модели 27 января 2010 г.
Зарегистрировано в Государственном реестре полезных моделей Российской Федерации 10 октября 2010 г.
Срок действия патента истекает 27 января 2020 г.

Руководитель Федеральной службы по интеллектуальной собственности, патентам и товарным знакам

Б.П. Симонов

US PATENT & TRADEMARK OFFICE
PATENT APPLICATION FULL TEXT AND IMAGE DATABASE

Help | Home | Boolean | Manual | Number | PTDLs | Hit List | Bottom | View Shopping Cart | Add to Shopping Cart | Images

(1 of 1)

United States Patent Application	*20160196154*
Kind Code	**A1**
Sarukhanov; Wagan ; et al.	**July 7, 2016**

MICROMINIATURE PERSONAL COMPUTER AND METHOD OF USING THEREOF

Abstract

A microminiature personal computer that is connected to external devices using standard interfaces for information input and output. The microminiature personal computer has an interconnected processor, a memory, a security module, a network module, and connectors. At least part of memory should be non-volatile to keep operating system, drivers to work with external devices, programs and data. The microminiature personal computer does all its processing and all its programs are running inside its memory while external computing device is used only for information input and output through a connector and a windowing system thus ensuring security of both systems and lack of unauthorized interaction between them.

Inventors: **Sarukhanov; Wagan**; *(Moscow, RU)* ; **Komov; Igor**; *(Moscow, RU)* ; **Podelko; Alexander**; *(Stamford, CT)*

Applicant: **Name** **City** **State Country Type**

In 2010 the patent process was started in the USA with the expertise extended in 2016.

From the beginning of the project **in 2008**, there have been six different versions of the Micro-PC with different features and uses. At the time it was called the uPC.

2009

ARM ATMEL AT91RM9200, 256 MB, 512 GB, RTC w/battery
OS: Linux
Application: system admin PC, thin client with pre-installed VPN

2010

ARM ATMEL AT91RM9200, 256 MB, 1 GB, Backup Battery, RTC w/battery
OS: ALT Linux
Application: system admin PC, thin client with pre-installed VPN, access key to remote server or database, portable workspace

2011

ARM ATMEL AT91RM9200, 256 MB, 1 GB, RTC w/battery
OS: ALT Linux
Application: portable workplace with pre-installed VPN and access key to remote server and medical database as a part of the automated health monitoring system

2012

ARM TI AM3359, 512 MB, 1 GB, Wi-Fi, Backup Battery, Graphic LCD
OS: Debian Linux
Application: access key and remote workplace as a part of the health monitoring system, researcher workplace for remote knowledge bases

2015

ARM Allwinner A10, 512 MB, 2 GB, Wi-Fi, microHDMI, Audio
OS: Debian Linux, Android
Application: portable workplace with business and game applications

2016 Photo is omitted due to NDA

ARM TI AM3359, 512 MB, 1 GB, Backup Battery, Graphic LCD
OS: Debian Linux, Android
Application: portable workplace for client-server applications, for example, 1C Enterprise, 1C Accounting, or 1C HR

Note. There are only printed board photos in the table above without devices exterior due to customer requirements and signed **Non-Disclosure Agreements (NDAs**).

2.4. USING OF THE PRODUCT IN CRYPTO-WORLD AND ITS MODIFICATION

The existing product – **uPC** – was used to create **the CWP Micro-PC**. uPC was designed to secure personal data and remote connections. Linux kernel modules were re-worked; all modules and applications, not-safe from the intrusion point of view, were removed; update system was modified; and the hardware non-breakable storage *Rutoken S micro* was added.

Rutoken S micro is a micro-module designed for safe two-factor user authentication and secure storage of encryption keys, digital signature keys, digital certificates, and other confidential information.

Rutoken S micro implements the following functions:

Function	Description
Authentication	❖ Two-factor authentication for access to the device, Operating System, servers, and applications (depending on settings)
Keys secure storage	❖ Keys usage for encrypting inside the device without a possibility to expose private keys ❖ The keys, generated on the micro-token, cannot be copied
Securing personal data	❖ Securing of electronic communications: email encryption, digital signature ❖ Securing access to computer and local network domain ❖ Possibility to encrypt data
Usage	❖ Storing business information, user's personal information, passwords, encryption keys, digital certificates, and any other confidential information ❖ Single identification device to access crypto-wallets, digital signature, authentication for access to wallets and applications

Rutoken S micro module support the following international standards:

- ISO 7816-3 — protocol T=0
- ISO 7816-4 — internal device and commands

- ISO 7816-8 — cryptography
- ISO 7816-9 — lifecycle

In addition to modifying hardware, we redesign the online services of the CryptoWorkPlace Web portal, which allows remotely configure one or several **CWP Micro-PCs** for the needs of a user or a group of users. In the beta version, the portal is made using traditional technology, however, at one of the stages of the project's road map, a decentralized blockchain platform will be launched that ensures the storage of states, transactions, authorization and automation of contract execution.

2.5. ONLINE SERVICES SUBSCRIPTION

Subscription is done for each device in user's personal cabinet. After subscribing, the following functionality is available to the user:

- Two-factor authentication
- VPN-tunnel configuration
- Application store
- Application restore to a new device

Two-factor authentication additionally secures the device and the data in the user's personal cabinet from unauthorized access. For that the user, in addition to the username and password, need to enter a code, which he gets by one of the following ways: email, SMS-message, or mobile application. The two-factor authentication is used by both the device and user's personal cabinet.

The VPN-tunnel service allows creating a secure channel between the device and the destination point. The channel is encrypted and secured from interception. Sending information through such channel is secure and anonymous. The user may select the traffic destination point in his personal cabinet.

Applications can be installed on the device only through the application store. It allows to eliminate a possibility to install a harmful program and to secure data on the device. If the device is lost or stolen, the user can block the device in the personal cabinet and restore applications on a new device. When working with third-party blockchain projects, native subscriptions are used.

2.6. PRODUCT OPTIONS

Name	Composition	Uses
CWP	Micro-PC CWP and a subscription to the online service (for a month, quarter or year)	An individual Micro-PC unit with an online subscription to an online service that allows you to recover passwords, block a lost device, or change settings for it.
CWP DUO	Two CWP Micro-PCs with a common key for secure communication + a subscription to the online service (for a month, quarter or year) + blockchain based online service	A set of two CWP Micro-PCs for two partner users. Both the CWP have preset **the same encryption key**, allowing **to make transfers** between crypto wallets and establish a secure direct connection for secure communication with the integrated messenger. It is possible to manage one wallet from two Micro-PCs
CWP CORP	A set of 10 CWP Micro-PCs with an annual subscription to the online service	A corporate set of 10 CWP Micro-PCs with an annual subscription to the online service, which allows you to recover passwords, block a lost device, configure applications
CWP CORP100	A set of 100 CWP Micro-PCs with an annual subscription to the online service	A corporate suite of 100 CWP Micro-PCs with an annual subscription to online services, which allows you to customize, activate and lock applications in addition to restoring passwords and locking lost devices

The project team has the competence to use modern technologies AI and ML, which will accumulate and analyze usage statistics to improve product resistance to malicious attacks. In this connection, the product will be continuously upgraded, the number and quality of CryptoWorkPlace online services will continue to grow, the CWP performance will be increased through the use of advanced BOM (Bill of Materials) and optimization of the modules of operating system kernel.

CWP Lite this is the standard solution for one user, ensuring the protection of the Wallets and Keys, as well as securing access to the Internet from any untrusted environment. CWP has an additional router mode, which allows you to securely connect applications of your smartphone from an untrusted environment with the resources that are of interest to you. In this mode, simply plug CWP to a standard charger with USB. In addition, CWP can be used as a gift with a pre-installed wallet and funds on it.

CWP CORP is a solution for corporate clients or groups of users with a single administrative panel that allows you to configure each of the CWP separately or together based on a common security policy. A security policy may include black and white lists, activating or blocking applications, installing applications and updates from the app store.

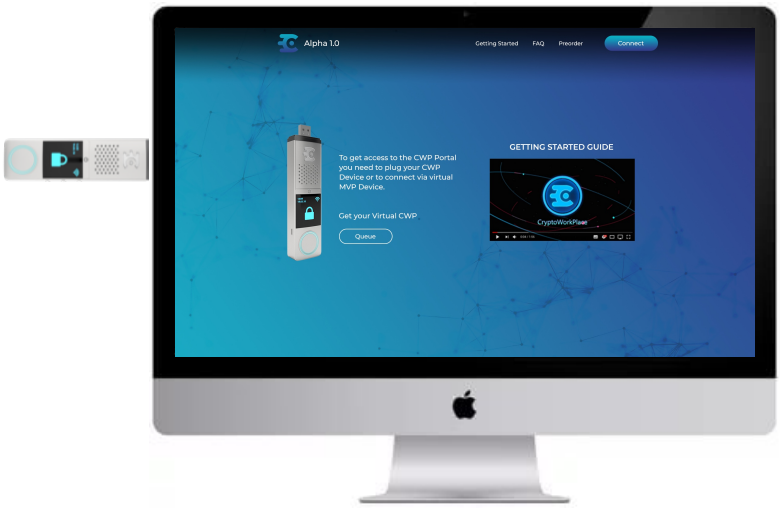
CWP DUO is the most interesting product offered by our project for today. A set of two CWP Micro-PCs that are configured to work together with one shared or two separate wallets. In the mode of working with separate wallets it is possible to transfer funds between them in one click without giving details of the transfer. To accompany (commenting) money transfers, you can use the built-in instant messenger with an encrypted communication channel. With such a set of devices, two people located in different parts of the world in the untrusted environment (unknown network, foreign Wi-Fi), can safely carry out transfers of funds to each other by pressing a button or by a timer or by smart-contract when the device is turned on. It is enough to connect CWP to a standard charger with USB.

To increase the audience using CWP, the project team offers a Micro-PC with client software of third-party blockchain projects that implements a game console for cloud gaming. Possible variants of game consoles Nvidia, GeForceNow, Steam. This version of the application allows gamers to abandon the purchase of expensive personal computers in favor of an inexpensive compact PC that provides streaming service. Gamers will be able to experience the following benefits:

- the ability to play anywhere
- the ability to play on any device (Windows PC, Mac, TV)
- tenfold savings compared to the purchase of gaming equipment

2.7. Portal on blockchain & D-APP Store

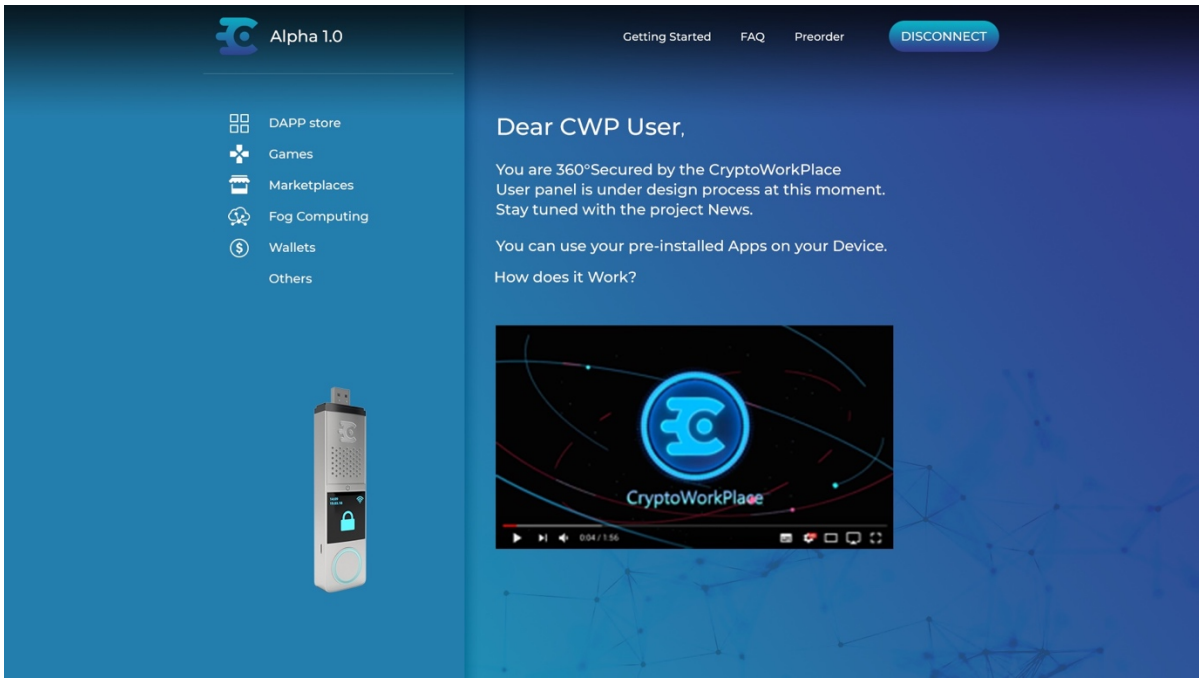
Owners of each version of CWP can take advantage of additional features of the system. After activation in the personal cabinet of the CryptoWorkPlace **PORTAL ON BLOCKHAIN**, additional software is installed on the Micro-PC, after which it becomes **the node** of the CryptoWorkPlace blockchain, along with standard solutions for nodes. The user will be able to save in the blockchain own information, create a backup copy of the programs installed in the Micro-PC or leave encrypted notes, without fearing to permanently lose them in the event of a breakdown or loss of the device, because this information permanently and invariably is placed in distributed storage, whose nodes are all participating devices.



For the version of the **CWP DUO**, knowing its unique identifier, one user can forward an arbitrary message to another, being sure that the transmitted information will not be tampered with and distorted, and the recipient will receive a message when connecting his device to the network, which can serve as an accompaniment to the automatic execution of smart- contract.

A participant in the ecosystem can at any time stop participating in the blockchain, return your device to its original state and stop receiving messages from other users or send your own. However, already placed by that time the data will always be available for download to its Micro-PC.

We are interested to provide users the most powerful & secure 3rd party Dapps. Dapps link developers and users directly, without middlemen hosting software or managing user data.



The CryptoWorkPlace team is open to cooperation with other projects, and is interested in providing compatibility with new and additional software that offers users additional services such as secure messengers, crypto-exchanges, crypto-wallets, cloud computing and more.

CWP D-App Store exclusive partners*:

universa	Successfully ended ICO, Launched
CRYPTOCEAN	Successfully ended PRE-ICO
Arm Pack	Successfully ended ICO, Launch in progress

* Pre-Installed on every CWP B2C Device

2.8. AI: Behavioral user control & CWP crack resistance

The project team has the competence to use modern technologies AI and ML, which will accumulate and analyze usage statistics to improve product resistance to malicious attacks by implementing AI/ML technology to the CWP Web Portal.

The system using only the password for authentication is an example of weak protection with a large number of imperfections from penetration.

In addition to multifactor authentication, the latest technologies allow our system to use data during a user session to analyze its behavior:

- stress test
- continuous keystroke authentication
- continuous biometric authentication from a third-party device
- continuous authentication based on user actions

Checking the stress state

Assessing the psychological state of the user can allow the system to take security measures. shows how the use of a neural network in a classification problem allows you to determine the following user states from the dynamics of keystrokes:

- anger
- irresolution
- nervousness
- confidence
- defecation
- relaxation
- delight
- melancholy
- stress
- fatigue
- happiness
- etc.

According to the results of the work **[1]**, the accuracy of determining the psychological state reaches **80%**

Continuous keystroke authentication

Basic parameters when measuring the dynamics of keystrokes:

- **delay time between clicks**
- **hold-down time**

The use of machine learning allows us to compare the user's behavior with the previous behavior in the system by considering changes in the dynamics of keystrokes.

Continuous biometric authentication from a third-party device

Using sensors (motion sensors, heart rate, and GPS) of a third-party device, CWP systems performs continuous user authentication. Reliable results can be obtained through a smart-clock (smartwatch). As shown in **[2]**, it is possible to achieve a test accuracy of up to **99.2%**, for this, the smart clock is used to measure the time of movement during printing on the keyboard.

Continuous authentication based on user actions

In addition to biometric indicators, the CWP system, for security purposes, can record user actions at certain stages of interaction with the system to further define typical behavior, as well as highlight typical behavioral behaviors, which generally allows users to be divided into clusters and pay attention if the user changes the behavior cluster during the new session.

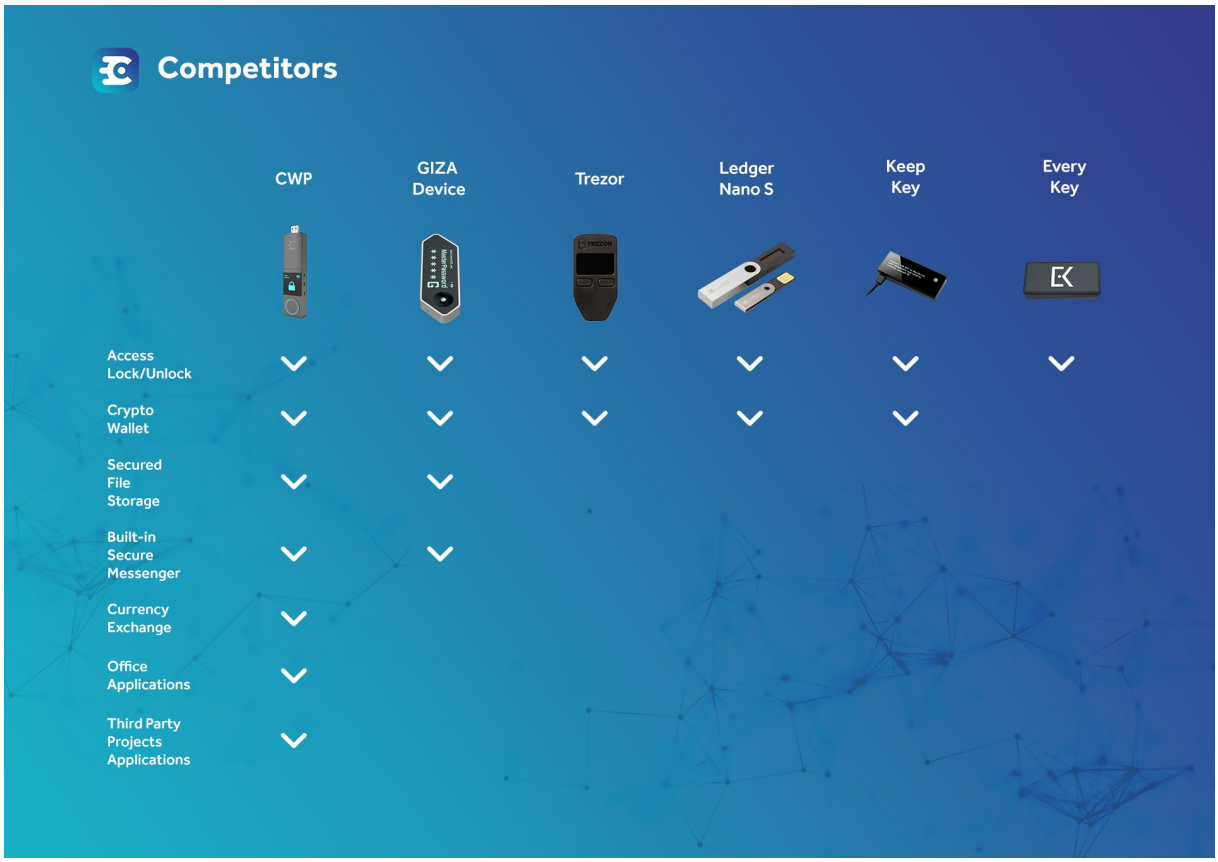
[1] Keystroke Dynamics for User Authentication,
http://biometrics.cse.msu.edu/Publications/SoftBiometrics/ZhongDengJain_KeystrokeDynamicsUserAuthentication_CVPR12biometricworkshop.pdf

[2] WACA: Wearable-Assisted Continuous Authentication
https://arxiv.org/pdf/1802.10417.pdf

2.8. COMPARISON WITH COMPETITIVE SOLUTIONS

There are several successful solutions on the market, each of which solves a number of security problems, and offers additional services. However, with a deep analysis of the functionality of these devices, it should be noted that there are no solutions providing an expanded set of functions necessary for a modern user whose needs are growing daily. Among such devices should be noted Trezor and Ledger Nano S, as the most popular. But the limitations of their functionality require the user to purchase several different devices in order to solve a complex of information security problems in modern conditions. The advanced GIZA device combines several functions in one package: a hardware crypto-wallet, a password manager and a secure file storage.

Nevertheless, all considered devices can be characterized as hardware crypto-wallets with different set of functions. The proposed device CryptoWorkPlace is a full-fledged personal computer in the USB flash form factor with a built-in hardware crypto-purse.



3. PROJECT ECONOMICS

As was mentioned earlier, the team had worked on the Micro-PC project under the name uPC for a number of years, addressing problems of IT security for corporate clients. To tailor these security advances to the cryptocurrency community, it will be necessary to produce a batch of a few tens of thousands CWP units.

This is why we are offering all interested persons an opportunity to join in on the financing, which would give them access to get project tokens with discounts from 10% to 40% depending on the time of participation and a product with a 50% discount. For this we will be selling the CWP token in two parts.

The first stage of the Token Pre-Sale will raise funds for marketing and preparation for the main stage of the process. It will also go towards releasing the first batch of the CWP Micro-PC and the beta version of the CryptoWorkPlace Web portal.

The second and main stage of the Token Sale plans to release the experimental batch of the CWP and offers to the crypto community of the first samples of the product in the Light version.

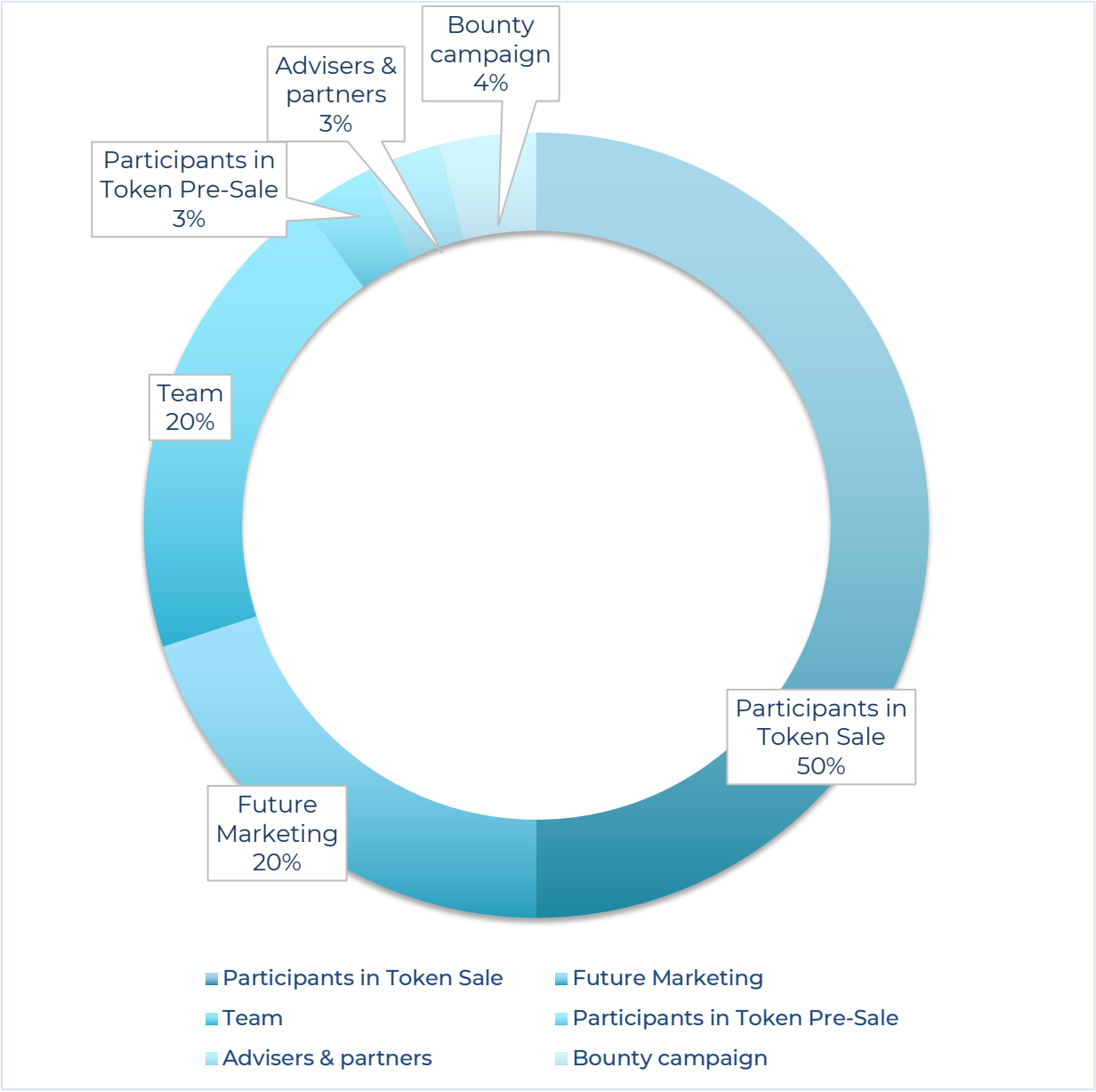
To attract funds at these two stages, a smart-contract will be developed and available on the Ethereum platform. The token is compatible with the ERC20 standard. The release of tokens occurs at the time of sale, and is limited to **500,000,000 CWT**

At the first stage, a CWT-P token will be created especially for the presale. At the moment of start TGE (Token Generation Event) participants can exchange the CWT-P token to the primary token CWT at **1 CWT-P = 1 CWT**

General Parameters

Token	CWT
Circulation	500,000,000
Currency accepted	BTC, ETH, LTC

After the two stages of raising funds, **the tokens** will be distributed as following:

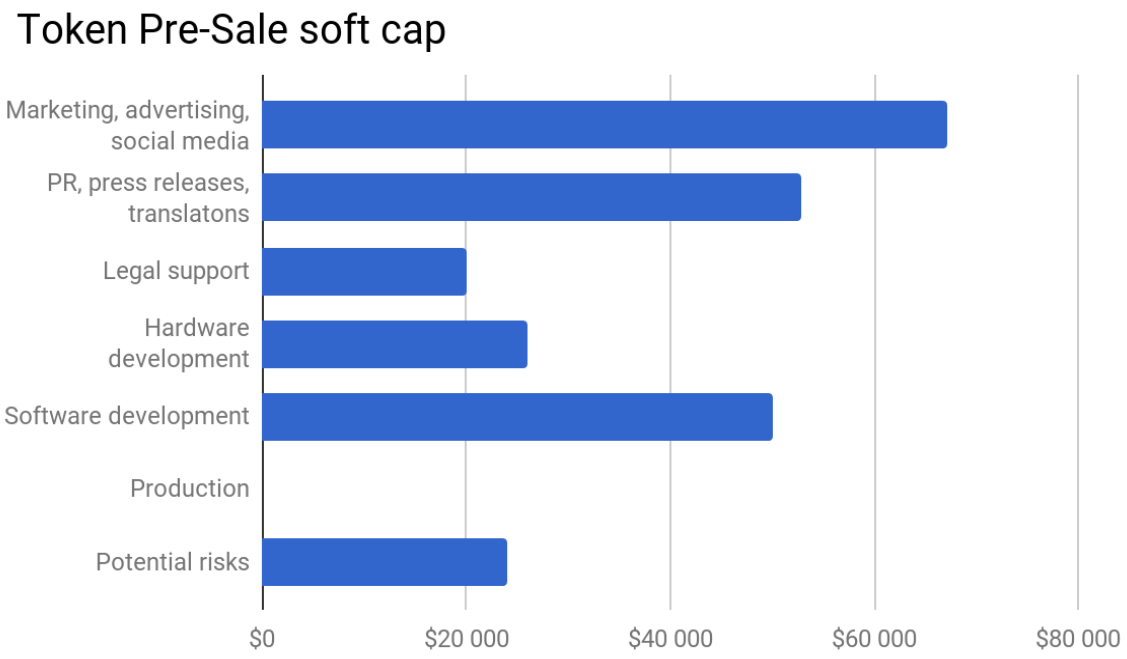


3.1. TOKEN PRESALE

Token:	CWT-P
Soft cap:	180 ETH ($240K)
Hard cap:	1351 ETH ($1.8M)
Tokens available:	15,000,000 (3%)
1 CWT-P =	**$0.12**

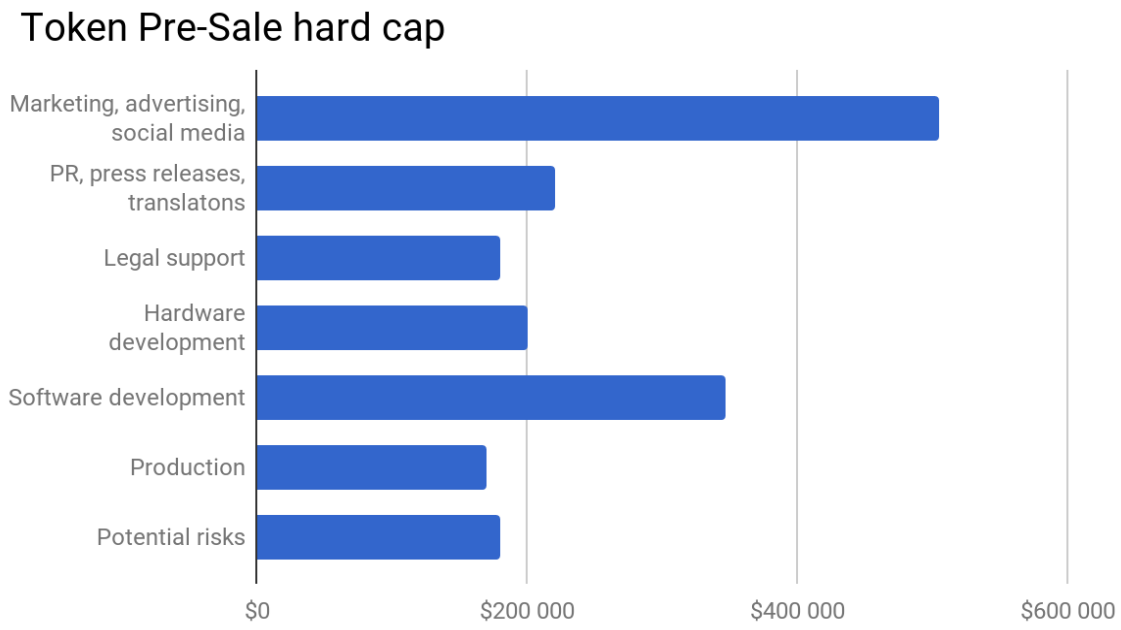
The distribution of funds from the presale has two potential scenarios:

Scenario 1. In the case of attracting the minimum amount required (soft cap), the launch of manufacturing of an experimental batch of Micro-PCs is not possible, since all the funds raised will be spent on preparing the launch of the main stage.



Scenario 2. If an amount between the soft cap and the hard cap is reached, there will be a first release batch with 100 CWP units. The amount of batches will depend on the amount over the soft cap according to the below table.

Attracted Amount by the Token Presale Participants	2M CWT $240 000	3M CWT $360 000	4M CWT $480 000	5M CWT $600 000	10M CWT $1 200 000	15M CWT $1 800 000
The number of batches of the pilot series of 100pcs	0	0	1	2	4	7

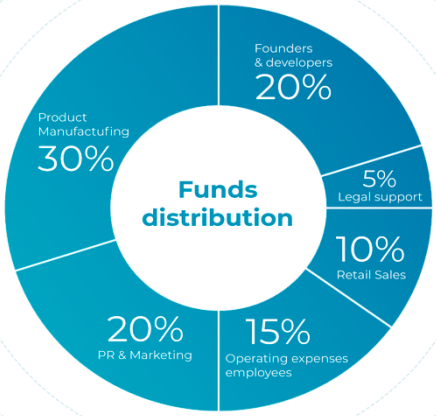


More detailed information about the TGE and the potential benefits of owning CWT given in this White paper.

Mandatory terms and conditions of sale will be outlined in the terms and Conditions published on the website. Deposits for the Private Pre-Sale is available from Q2 2018. The first phase of the TGE is scheduled for Q3-H1 2018.

3.2. TOKEN SALE

Dates:	**Q3 2018**
Token:	CWT
Soft cap:	$2.4M
Hard cap:	$47.4M
Tokens Available:	250,000,000 (50%)



The second stage will raise no more than **$47,400,000** from the TGE (Token Generation Event) participants. The distribution of the funds raised during the Token Sale will be as following:

30% of the funds raised during the TGE we plan to spend on the launch of production on an industrial scale. 70% of this amount will be spent for the purchase of components, manufacture of printed circuit boards and their assembly. 20% will go to pay for the work of third-party developers from Europe, USA and Asia. 10% - for manufacturing production tooling, test equipment, warehousing services and logistics.

20% of the funds raised during the TGE we allocate for marketing in three regions Europe, the United States and Asia during the first year of the product's release to the world market. 80% of this amount will be spent on the product promotion in the United States, Japan, China and Singapore.

20% of funds raised will be spent on the salaries of our team. 30% of this amount will be spent on research in the first year-to-market, which include accumulation of statistics and the use of AI and machine learning to improve the level of product protection from malicious actions.

3.3. APPLYING DISCOUNTS WHEN BUYING TOKENS

Users who have purchased the CWT tokens, receive discounts whose size will decrease with increasing amounts attracted as follows:

Attracted Amount by the Token Sale Participants	Token Pre-Sale 180 - 1351 ETH	Token Sale 1,8K - 3,6K ETH	Token Sale 3,6K - 13,1K ETH	Token Sale 13,1K - 32K ETH
Discount	40%	20%	10%	0%
1 CWT	$0,12	$0,16	$0,18	$0,20

3.4. APPLYING DISCOUNTS WHEN PURCHASING A PRODUCT

Owners of CWT tokens can purchase a product with a **50% discount** on the price in a fiat currency. During the purchase of the product, the tokens spent on the purchase will be burned to avoid of a double income. Automatic burning of used tokens will lead to an increase in their value, if the project can maintain the popularity of the product.

Product	Price		
	USD	Discount 50%	CWT=$0.2
CWP LITE	**$199**	$100	500 CWT
CWP PRO	**$399**	$200	1000 CWT
CWP DUO	**$1 280**	$640	3 200 CWT
CWP CORP	**$2 199**	$1 100	5 500 CWT
CWP CORP100	**$20 899**	$10 450	52 250 CWT

4. DEVELOPMENT PLAN

4.1. PROJECT ROADMAP

December-January 2017	Q2 2018	Q3 2018	Q3-Q4 2018	Q4 2018
~~Preparing~~	Token Pre-Sale	Token Sale	Testing	Production
~~Development of sample devices, website and web portal~~	~~Preparing for the TGE~~ ~~Release of a prototype~~	~~Launching of the Web Portal Alpha 1.0~~ Release of a pilot batch of devices **CWP Hackathon**	Testing of the product in independent laboratories	Preparing for series production of devices and launching technical support
~~Creating a CWT-P token and launching its smart contract~~	~~Connection to the partner program of blockchain projects~~	Creating a CWT token and launching TGE's smart contract	Opening of the USA, Japan and Czech Republic offices	Launching of the CryptoWorkPlace Web portal and blockchain

Q1 2019	2019	2020	2021	2022
Serial production of products CWP CWP DUO	Serial production of products CWP CORP CWP CORP100	Increase in production CWP CWP DUO up to 1,000 units per quarter	Increase in production CWP CORP CWP CORP100 up to 20 units per quarter	Increase in production CWP CWP DUO up to 10,000 units per quarter

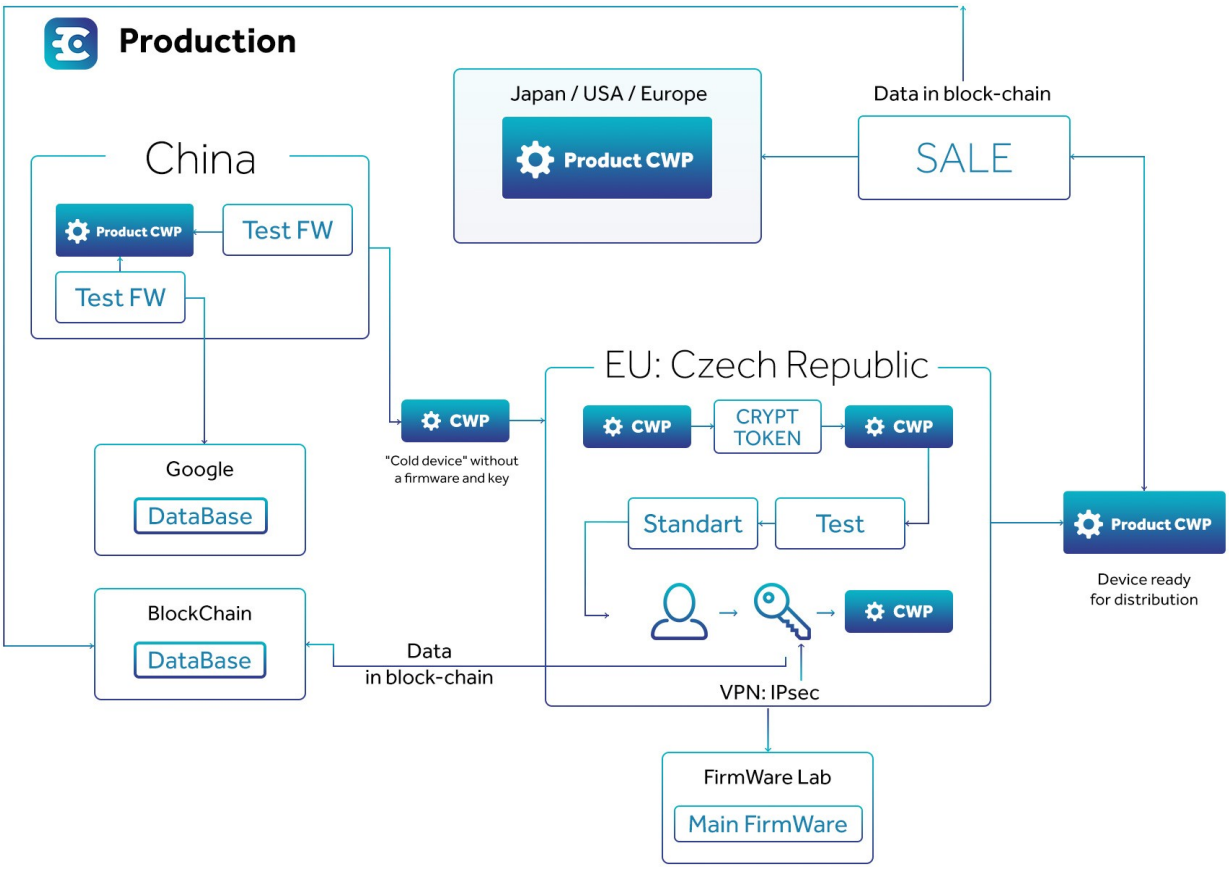
4.2. PRODUCTION PLAN

The anticipated company structure includes offices in a few countries:

- Europe Office — Prague (Czech Republic) (**Registered)**
- Asia Office — Tokyo (Japan)
- North America Office — New York (USA)
- Production Office — Guangdong (China)

The production of circuit boards, ordering of electronic components, the assembly, and the loading of test firmware will be done at the factory of ICAPE Group in Guangdong.

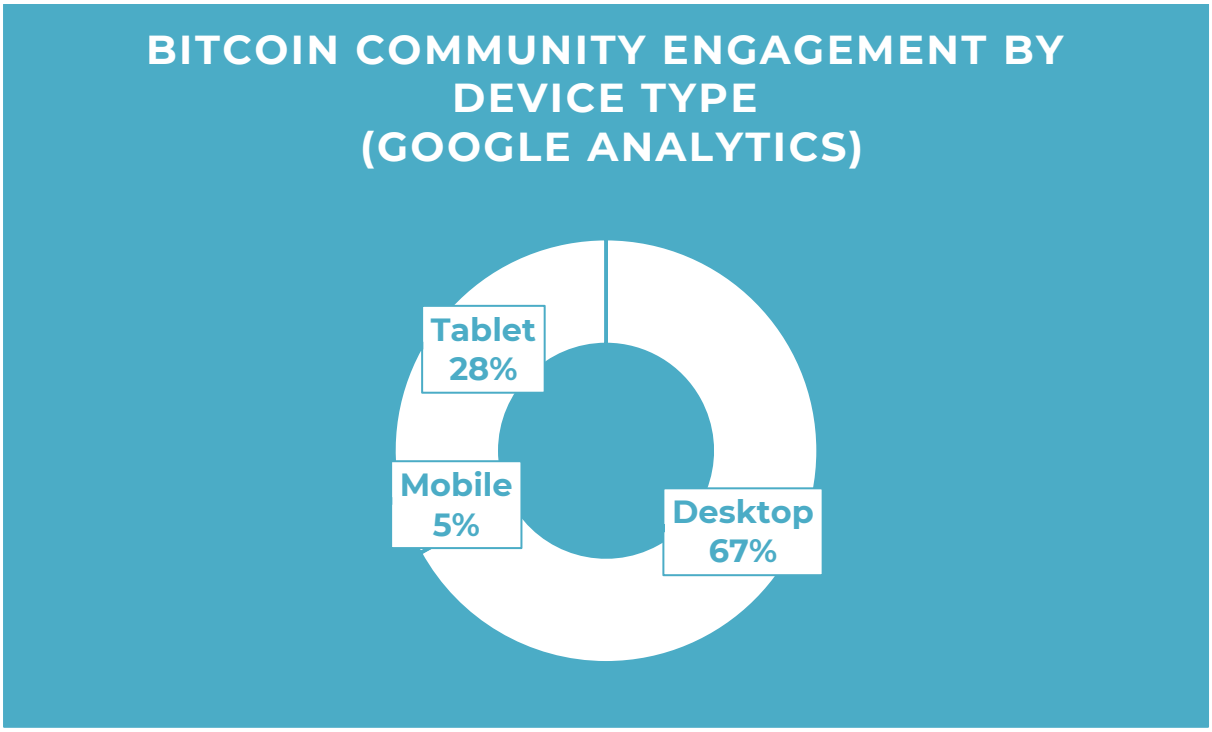
Installation of micro-modules Rutoken S micro on the microcontroller boards will be performed by the European division, here the product firmware will be loaded. To ensure these works, there will be protection against unauthorized access to production areas where additional components and software modules are stored and installed.



4.3. BUSINESS PLAN

The CryptoWorkPlace financial model is based on the forecast of growth of the capitalization of crypto currencies, in particular according to the analysis of McKinsey & Co by 2023 the capitalization will reach about **3 trillion dollars**. Along with the increase in capitalization, the number of companies accepting payments in cryptocurrencies is increasing, which directly affects the expansion of the cryptocurrency wallets market and, as a result, increases the number of our customers. Analysts predict this rapid growth will lead to the emergence of more than **500 million wallets** by 2023.

Also, do not forget about the huge losses as a result of malicious acts, which we are seeing now. At the same time, it is necessary to take into account the statistics of the use of various devices during operations with cryptocurrencies. According to Coin Dance resource **(https://coin.dance/)** and **Google Analytics**, more than half of Bitcoin community users use desktop computers that are most susceptible to hacking and intruder attacks than tablet computers and other mobile devices.



Considering the increase in the number of wallets, the increase in losses from their break-ins, the successful promotion of competitive products and the shortcomings of their technical solutions, our analysis showed that the CryptoWorkPlace project will take more than **0,5%** of the **entire market** of crypto wallets.

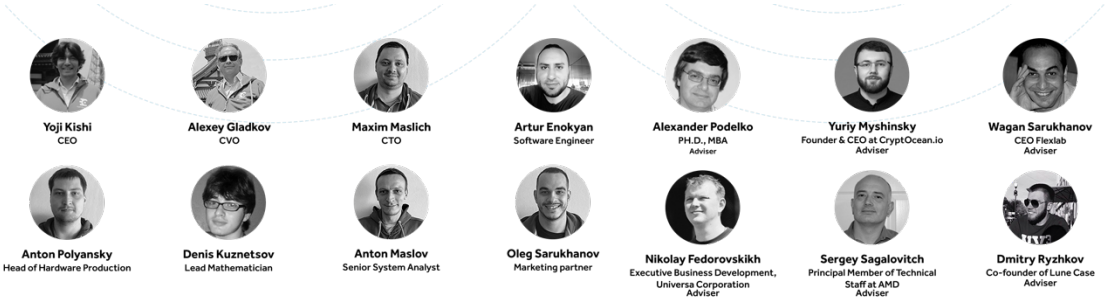
Such a market share will give the project more than **500 000 potential users**

Based on the above market analysis, a business plan was constructed **(Goal: 65 349 devices)**, the results of which are presented in the table below:

	For the 1st year	For 3 years	For 5 years
Revenues from sales	$7 268 673	$30 348 476	$35 905 386
Current expenses	$2 944 759	$9 884 397	$11 567 168
Net profit	$1 241 685	$4 486 014	$5 370 156
EBITDA	$446 552	$1 290 093	$1 596 444

5. TEAM

5.1. THE FOUNDERS AND DEVELOPERS, ADVISERS



CEO Yoji Kishi

Rare type of High-edge Japanese technology specialist with wide international marketing experience.

- International Society of Stem Cells Development, Director
- Shin-Nippon Research (Hong Kong) Co., Ltd. Vice-President
- 5hz Medical Supplies (Xiamen, China) Co., Ltd. Vice-president
- Kintaro Cells Power Co., Member of Board of Director
- Ryukyukan International Kobudo Karate Federation, Honor Member

Linkedin

CVO Alexei Gladkov

Kintaro Power Cells Japan President

- MapMess Inc. Regional Director
- Founding director of the research company AV-Cells Singapore
- 30 years of experience in running own business
- 20 years of doing business in Singapore and Japan

Linkedin

CTO Maxim Maslich

- Microsoft Certified Professional
- Microsoft Certified Technology Specialist Exam 511
- **Blockchain and smart contracts developer**
- An expert in the management of the software development process, the construction of distributed, highly loaded and secure systems
- Development of transport monitoring systems (cargo, passenger cars, special equipment, passenger transportation, weight control, production line control, taxi park automation) for Alrosa, GAZPROM, Lukoil, Rusal, RZD, Satori, Autoline, city taxi.

Linkedin

Microsoft CERTIFIED Technology Specialist

CMO Oleg Sarukhanov

- Co-Founder & COO
  at Glory Event Agency LLC.
- Marketing & Events specialist since 2006
- **Aggregate implementation of marketing projects for $ 5,000,000**
- Promoted marketing campaigns as an Agent for international brands such as BIC, Facebook, General Electric

Linkedin

Arthur Enokyan
Software Engineer 1st category

Linkedin

- Full-Stack JavaScript Senior Developer
- Certified Middle End Android Developer
- Certified Middle End iOS Developer
- **Expert in developing Highload applications**
- Development of special software for major retailers
- Cryptography, electronic document management

Anton Polyansky
Head of Hardware Production

Linkedin

- **Hardware Engineer**
- **Embedded Software Engineer**
- **Microcomputer Systems Expert**
- Development of circuit solutions, trace of printed circuit boards and development of embedded software for thermal imaging devices
- Development of circuit design solutions, trace of printed circuit boards for low-level devices of the Quinta music recognition system
- Development of circuit solutions and trace of printed circuit boards for Smart House devices
- Development of microminiature biometric sensors and processor control system for bioelectrical upper limb prosthesis
- Development of embedded data transmission systems based on Wi-Fi, GSM and Bluetooth technologies

Linkedin

Denis Kuznetsov
Lead Mathematician,
Senior Architect Developer

- Embedded Systems Programmer
- **Expert in Machine Learning and AI**
- Development of an agent for the conduct of non-targeted dialogue in the banking system
- Development Telegram-bots with AI support
- Embedded Software Development for Quinta Music Recognition System Devices
- Co-author of a patent for music recognition algorithms

Linkedin

Anton Maslov
Senior System Analyst,
PHP-Developer

- Optimization and automation of DAICHI logistics business processes
- System analytics of multimodule high-loaded systems with various integrations for METRO C & C, Lenta
- The development of a supply planning system for TOC (Theory of Constraints) for the production of IKEA, integrated with 1C
- **Product development and positioning management**

[Facebook]
[Linkedin]
[Personal site]

Alexander Podelko

Adviser

Ph.D., MBA
An expert in software development and testing

- Member of the Board of Directors of the Computer Measurement Group
- **Oracle, Consulting Member of Technical Staff**
- Hyperion, Distinguished Performance Engineer
- Aetna, Sr. Architect II
- Alexander coordinates the sales and production of the product for the US market, the management of the project's branch in the United States, the interaction with major US partner companies that provide scientific and technical support for the project.
- **Alexander has 30 years of experience in software testing, which allows him to organize the interaction of the project with the largest players in the software testing market, such as QAMentor**

Nikolay Fedorovskikh

Adviser

Executive business development at Universa Corporation

- **Over 11 years experience in TVMedia, VAS & Data field.**
- Strong focus on Telecom/Media with expertise in DVB/IPTV/Online Video (OTT), VAS, CDN.
- Creating for overall architecture and engineering of complex TV & Pilot Blockchain projects.
- Proven track in identifying customer needs and implementing technical strategies, to secure long-term revenue growth on TV/Media markets (IPTV, VOD, OTT, CDN).

Wagan Sarukhanov

Adviser

CEO Flexlab Ltd.
CTO uPCLabs Inc.

- Blockchain researcher and expert
- **30 years of experience in contract manufacturing of electronics and software**
- More than 20 projects in various industries
- Mentor
- **Wagan's competencies help the project in the business development and technical issues of product development and manufacturing**

Serguei Sagalovitch

Adviser

Principal Member of Technical Staff at AMD

Facebook
Linkedin

- An expert in software development including design and implementation of device drivers and embedded systems, as well as graphics and compute solutions with the strict robust and security requirements. Serguei has experience working with customers on product delivery.
- Serguei has experience working with small and big companies including Nortel and AMD in positions of Team Lead as well as Principal Member of Technical Staff.
- Serguei has experience working with scientific organizations including University of Vienna.
- Serguei has been co-authors of several patent applications.
- Serguei has more than 25 years of experience.

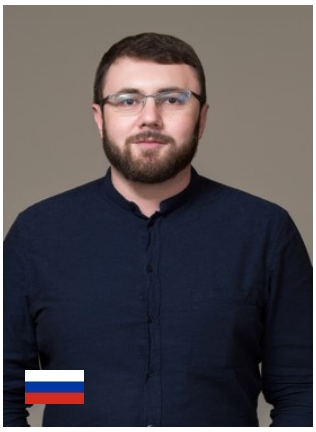
Facebook
Linkedin

Dmitriy Ryzhkov

Adviser

Co-founder LuneCase

- The businessman, the crypto-currency investor
- Co-founder of a successful international brand LuneCase
- **ICO adviser, a pool of more than 15,000,000 $**



Facebook
Linkedin

Yuriy Myshinsky

Adviser

Founder & CEO at CryptOcean

- **Experience of successful founding of companies and management in the field of information technologies**
- The implementation of infrastructure projects for large state and international companies
- Crypto enthusiast
- Investor in fintech, startups and ICO

If you want to join the Team CWP, please contact us via e-mail: team@cryptoworkplace.io

5.4. PARTNERS

http://www.icape-group.com

ICAPE Group, headquartered in Paris, and production in China.

Partner-Manufacturer

ICAPE Group is one of the leading European companies producing and supplying printed circuit boards (PCBs) and custom-made technical parts manufactured in China.

The factories of the company will organize the production of Micro-PC CWP, output control and download of the firmware.

https://cellspower.com

Kintaro Cells Power

Partner-Client

The Japanese company Kintaro Cells Power is an innovator in the field of cellular medicine, it is part of an international group of companies specializing in providing health and medical tourism services with an emphasis on serving the VIP segment.

Kintaro Cells Power is a potential corporate customer who will use CWP in their research to protect patient personal data and ensure secure remote connections of company employees to corporate databases.

QAMentor

http://www.qamentor.com/

Partner- Product testing

American company, a leader in software and hardware testing

Universa Corporation

http://www.universa.io

Partner-Client,
Blockchain developer

- **Blockchain Protocol**
- ICO/DAO platform
- UTN/BTC Wallet
- Secure Messenger

CryptOcean

http://www.cryptocean.io

Partner-Client,
Decentralized Crypto-exchange

Estonian company, aiming to be a leader on cryptomarket

ArmPack

http://www.armpack.io

Decentralized protection against counterfeiting

CWP Devices will be protected by Armpack

6. IMPORTANT NOTICE

If you have yet to become a participant in our Token Generation Event (TGE) and are not sure if you want to participate, we recommend that you seek a professional consultation in legal, financial, and tax related spheres with the respective specialists.

CWT-P and CWT coins do not constitute securities in any jurisdiction. This document does not constitute an offer to the reader nor to a participant in the upcoming TGE to buy securities or an investment in securities in any jurisdiction.

6.1. DISCLAIMER OF LIABILITY

To the maximum extent possible by the applicable laws, rules and regulations, CryptoWorkPlace is not responsible for any special, vicarious or any kind of consequential damages as well as any other losses, like loss of income, profits, or loss of use or data, caused by reliance on CryptoWorkPlace Whitepaper or any part of it by you.

By receiving and / or accessing any information provided in this Whitepaper or any part thereof (depending on the circumstances), you represent and guarantee to CryptoWorkPlace following:

- you agree and fully understand that the CWT-P and CWT tokens are not meant to constitute securities in any jurisdiction;
- you agree and acknowledge that the CryptoWorkPlace Whitepaper does not contain any recommendations or advice to purchase CWT tokens. It does not constitute any investment decision or contract which means that this document cannot be considered an investment or any other contract, and the fact of its provision cannot be the basis for investing or concluding an investment agreement;
- you agree and acknowledge that any information provided in this Whitepaper has not been checked or approved by regulatory bodies and authorities. Publishing and distributing this Whitepaper to you does not mean that the applicable laws, regulatory requirements and rules or regulations have been complied with;

- you agree and acknowledge that in case you wish to purchase any CWT-P and CWT tokens, they should not be perceived or classified as:

    - any kind of currency other than cryptocurrency;
    - debt securities, stocks or shares issued by any person or organization;
    - rights, options or derivatives in relation to such debt obligations, shares or stocks;
    - rights under a contract for differences or for any other contract the purpose or feigned purpose of which is to gain profit or avoid loss;
    - units in a scheme of collective investment;
    - units in business trust;
    - derivative units in business; or
    - any other security or class of securities;

- all of the abovementioned representations and warranties are true, complete, accurate and non-misleading from the time of your access and / or possession of this Whitepaper and part thereof (as the case may be).

6.2. NO OFFER OF SECURITIES OR REGISTRATION

This Whitepaper doesn't contain any offer of any sort and kind and is not intended to constitute such offer, as well as offer of securities, and is not prompting for making investments in securities in any jurisdiction. Any person isn't bound to enter into any contract or binding obligatory legal commitment on the basis of the CryptoWorkPlace Whitepaper.

No cryptocurrencies or other forms of payment is to be accepted on the basis of this Whitepaper.

THANK YOU SO MUCH FOR YOUR TIME

FEEL FREE TO CONTACT US:
TEAM@ CRYPTOWORKPLACE.IO

+ 420 728 931 549 (EU: CZ)
+1 (484) 707 7877 (US)

Telegram News channel
https://t.me/CWP_News

Telegram Chat [ENG]
https://t.me/CWP_Official

Official Twitter channel
https://twitter.com/cryptoworkplace

Official Facebook page
https://www.facebook.com/cryptoworkplace