



CryptoWorkPlace

Copyright 2017-2018 © CryptoWorkPlace



CryptoWorkPlace

*“Защищать то,
что важно”*

Оригинальным языком этого документа является английский язык. Перевод этого документа на любой другой язык тщательно не проверялся, поэтому нет никакой уверенности в точности, надежности и полноте такого перевода. В случае любых расхождений или конфликтов между любыми такими переводами и английской версией этого документа, английская версия всегда будет иметь наивысший приоритет.

White Paper ver. 1.8

01/23/2018

Copyright 2017-2018 © CryptoWorkPlace

Содержание

Введение	2
1. Проблема	3
1.1. Статистика потерь от взломов компьютеров и кошельков	3
1.2. Примеры крупнейших взломов ICO в 2017 году	3
1.3. Meltdown и Spectre - аппаратные уязвимости всех современных процессоров	4
2. CryptoWorkPlace — это решение проблемы	5
2.1. Решение проблемы	5
2.2. Описание технического решения	6
2.3. История продукта с 2008 года	9
2.4. Применение существующего продукта в криптомире и его модификация	11
2.5. Онлайн-сервисы UniDefense по подписке	13
2.6. Варианты продуктов	14
3. Экономика проекта	16
3.1. Token Pre-Sale	18
3.2. Token Sale	19
3.3. Применение скидок при покупке токенов	20
3.4. Применение скидок при покупке продукта	21
4. План развития	22
4.1. Дорожная карта проекта	22
4.2. Производственные планы проекта	22
5. Команда	23
5.1. Руководители и разработчики	23
5.2. Эдвайзеры	26
5.4. Партнеры	28
6. Важное уведомление	29
6.1. Отказ от ответственности	29
6.2. Отсутствие эмиссии ценных бумаг	30

Введение

CryptoWorkPlace — первая в мире децентрализованная система на базе персонального компьютера размером с флешку, предоставляющая беспрецедентную защиту от хакерских атак, программ злоумышленников и несанкционированного доступа к данным.

На рынке существует несколько замечательных аппаратных решений, позволяющих защитить ваш криптокошелек за счет надежного хранения ключей на внешнем устройстве, которое подключается к вашему персональному компьютеру (ПК). Однако при той степени развития технологий, которую мы наблюдаем сегодня, нельзя с полностью доверять собственному ПК, даже при условии, что у вас установлена актуальная версия антивирусной защиты. Ведь сначала появляются зловредные программы, и только после этого разработчики находят «лекарство» для борьбы с ними. Поэтому угроза утраты доступа к вашему криптокошельку и, соответственно, к вашим деньгам, существует всегда.

Микрокомпьютер *CryptoWorkPlace* (*CWP*) представляет собой не просто хранилище ключей, а автономно функционирующий полноценный специализированный персональный компьютер с собственной операционной системой и набором приложений. Для его работы требуется внешний компьютер (компьютер-донор), на мониторе которого отображается вся информация и с помощью клавиатуры и мыши которого вводятся данные. Уровень защищенности внешнего ПК не имеет никакого значения для безопасности вашего кошелька, так как он только отображает информацию, а все приложения выполняются на защищенном микрокомпьютере *CWP*.

Поскольку *CWP* — это персональный компьютер, то в отличие от существующих аппаратных кошельков, обеспечивающих только хранение ключей, он предоставляет возможность полноценной работы с приложениями, такими как мультивалютные кошельки от широкого спектра поставщиков услуг, доступ к нескольким биржам одновременно, переписку в интересующих вас каналах и другие, связанные с использованием криптовалюты, сервисы.

Все предоставляемые сервисы могут быть легко сведены на единой панели управления для удобства восприятия большого объема информации. Так, можно отобразить содержимое нескольких ваших кошельков, суммарные итоги, предыдущие траты за заданный период и любую статистическую информацию.

В основе экосистемы CryptoWorkPlace лежит механизм автоматизации функций на базе контрактов и распределенный реестр состояний.

1. Проблема

1.1. Статистика потерь от взломов компьютеров и кошельков

На сегодня в криптоМире в день происходит огромное количество событий, связанных с привлечением большого количества средств. Сейчас популярны Pre-ICO на сотни тысяч долларов и ICO на десятки миллионов долларов. Основатели проектов используют крипто кошельки от известных поставщиков услуг, однако при использовании традиционных методов защиты от взлома степень защищенности инвесторов невысока, так как либо сайты проектов необдуманно создаются на сомнительных движках и хостингах, либо кошельки хранятся (или к ним предоставляется доступ) на компьютерах, защита которых давно дискредитирована, но пользователи об этом просто не знают.

2017 год был богат на случаи взлома кошельков проектов, когда хакерам удавалось украсть в самый разгар ICO \$2M, \$6M и даже \$8M.

1.2. Примеры крупнейших взломов ICO в 2017 году

Наиболее известный и трагичный взлом произошел во время проведения ICO проекта CoinDash. В 16:30 17 июля 2017 организаторы сообщили о том, что их сайт был взломан, адрес кошелька был подменен и за первые 5 минут злоумышленники «увели» более \$6 миллионов, а в конечном счете общая сумма потерь превысила \$8 миллионов.

CoinDash.io
@coindashio

Website has been hacked.

Язык твита: английский

16:13 - 17 июл. 2017 г.

994 ретвита 686 отметок «Нравится»

183 994 686

Согласно отчету, опубликованному компанией Chainalysis (см.

<https://blog.chainalysis.com/the-rise-of-cybercrime-on-ethereum/>),

в мире наблюдается взрывной рост киберпреступлений, направленных на ICO-проекты. Так, в июне 2017 года объем потерь инвесторов от действий преступников составлял \$100 миллионов, в августе этот показатель уже превысил \$220 миллионов.

Тип преступления	Описание	Сумма потерь (\$M)	Количество жертв
Фишинг	Получение чувствительной информации (логинов, паролей или приватных ключей) путем подделки сообщений от доверенного источника.	115	16 900
Экспloit	Использование компьютерных программ, фрагментов кода или последовательности команд для проведения атаки на вычислительную систему.	103	11 000
Хак	Получение несанкционированного доступа к компьютерной системе.	7,4	2 100
Схемы Понци	Финансовые махинации, пирамиды	0,004	260
ВСЕГО:		225,4	30 260

Инвесторы, таким образом, оказываются уязвимыми с двух сторон: они могут потерять не только деньги, которые вложили в проект, но и средства из своих криптокошельков.

Совершенно очевидно, что никакими техническими средствами невозможно обезопасить себя от потерь, вызванных добровольным участием в заведомо мошеннических схемах, однако, суммарный ущерб от этого типа преступлений относительно невелик.

1.3. Meltdown и Spectre - аппаратные уязвимости всех современных процессоров

Уязвимости Meltdown и Spectre (<https://meltdownattack.com>) были независимо обнаружены исследователями корпорации Google, Cyberus Technology и

Грацского технического университета в середине 2017 года и опубликованы 4 января 2018 года.

Атака Meltdown позволяет атакующему приложению получить несанкционированный доступ на чтение привилегированной памяти, используемой ядром операционной системы. Атаке подвержены процессоры Intel и ARM, не подвержены процессоры AMD.

Атака Spectre позволяет атакующему приложению получить доступ на чтение произвольного участка памяти, в том числе используемого другими приложениями, что нарушает изоляцию памяти между программами. Атаке подвержены процессоры Intel, AMD и некоторые ядра архитектуры ARM.

Таким образом на сегодня нет ни одной компьютерной системы, способной противостоять указанным атакам, и следовательно, пользователи с большой вероятностью в любую секунду могут потерять доступ к своим важным данным, в том числе к кошелькам.

Чтобы эффективно бороться с подобными проблемами, нужно заменить аппаратную начинку компьютера, полностью обновить операционную систему и перекомпилировать всё имеющееся на компьютере программное обеспечение при помощи новых компиляторов с заменой уязвимых последовательностей машинного кода. Очевидно, что для защиты от указанных атак недостаточно использовать привычные методы типа патчей, так как уязвимости присутствуют на аппаратном уровне и они полностью разрушают привычные представления об изолированных песочницах.

2. CryptoWorkPlace — это решение проблемы

2.1. Решение проблемы

Пользователь СWP может обезопасить себя от всех распространенных типов атак.

Специалисты рекомендуют для работы с криптокошельками использовать выделенный ПК с операционной системой Linux, не держать на нем приложения, которые могут увеличить вероятность проникновения злоумышленника извне, иногда советуют вообще удалить все приложения, обеспечивающие выход в сеть Интернет. Однако с недавним появлением аппаратных уязвимостей Meltdown и Spectre даже этих мер недостаточно.

Микрокомпьютер СWP как раз и есть тот самый выделенный ПК, но только с более высокой, по сравнению с обычным, уровнем защиты, позволяющим безопасно подключаться к сети Интернет и без ограничений пользоваться несколькими криптошельками. При этом он может всегда находиться с вами и не позволит злоумышленнику получить доступ к вашим данным даже в случае его утери или хищения.

Для борьбы с новыми аппаратными уязвимостями Meltdown и Spectre в микрокомпьютере СWP используется обновленное ядро операционной системы и приложения, перекомпилированные с помощью новых компиляторов. Кроме того, вся важная информация хранится не в оперативной памяти, которая может быть подвергнута указанным атакам, а во встроенном криптохранилище.

2.2. Описание технического решения

CryptoWorkPlace - децентрализованная экосистема на основе блокчейн-технологии, включающей в себя микрокомпьютер, обеспечивающий запуск приложений в безопасной изолированной среде, специальное программное обеспечение, набор сервисов веб-портала UniDefense, призванных организовать защиту от угроз в сети, и распределенный реестр состояний.

После регистрации на веб-портале UniDefense пользователь получает доступ к следующим функциям:

- привязка конкретного устройства к своей учетной записи;
- включение двухфакторной аутентификации и выбор ее типа;
- магазин приложений (кошельки, трейдинговые программы) и службу обновления;
- настройка списка доступных сторонних сайтов и сетевых служб;
- установка географических зон, в которых «приземляются» соединения по VPN (Virtual Private Network), организуемые устройством;
- блокировка устройства в случае потери и дистанционное удаление данных.

Микрокомпьютер СWP использует современный высокопроизводительный процессор и собственные устройства памяти. Он подключается к компьютеру-донору через разъем USB, от которого получает питание. При подключении микрокомпьютер воспринимается как обычная сетевая карта.

Поверх сетевого соединения организуется защищенный туннель (VPN-туннель), через который происходит взаимодействие пользователя с операционной системой микрокомпьютера СWP и установленными на нем программами. После включения микрокомпьютер проверяет отсутствие блокировки

устройства на веб-портале *UniDefense* и открывает окно аутентификации привязанного пользователя. Для доступа пользователь должен предъявить, кроме стандартной пары имени пользователя и пароля, второй фактор аутентификации, указанный им в настройках учетной записи *UniDefense*. Таким вторым фактором может выступать одноразовый код, полученный по электронной почте, в SMS-сообщении или в специальном приложении для смартфона (например, *Google Authenticator*). Таким образом, изолированная среда и механизм доступа сводят на нет возможность использования фишинга.

Операционная система микрокомпьютера *CWP* располагается в защищенным от записи разделе памяти и не допускает внесения в нее изменений как пользователем, так и вредоносными программами. Установка необходимого ПО и его обновление производятся только через веб-портал *CWP*. Не допускается запуск или модификация программ, не подписанных ключом *CWP*. Таким образом, изолированная среда и механизм подписи программ исключают возможность использования эксплойтов.

Выполнение программ производится в изолированной от компьютера-донора среде. Пользовательские данные хранятся на устройстве в зашифрованном виде (выбор пользователя), что позволяет создать надежную защиту от действий хакеров.

Для подключения к интернету микрокомпьютер *CWP* использует собственный встроенный 4G-модем или WiFi-адаптер, которые используются для установления VPN-соединения с сервером, указанным в настройках учетной записи. Любой трафик в обход VPN отбрасывается.

В случае потери или повреждения устройства пользователь *CWP* может, во-первых, отправить команду на блокировку и удаление всех хранящихся на нем данных, которая будет автоматически выполнена при первом подключении микрокомпьютера к сети Интернет. Во-вторых, можно привязать к своей учетной записи новое устройство. Все выполненные для предыдущего экземпляра настройки и установленные программы будут автоматически перенесены на новый экземпляр.

В качестве дополнительной меры защиты приватных ключей криптокошельков, работающих в *CWP*, устройство оснащается встроенным криптохранилищем, непосредственно в котором происходит подпись транзакции.

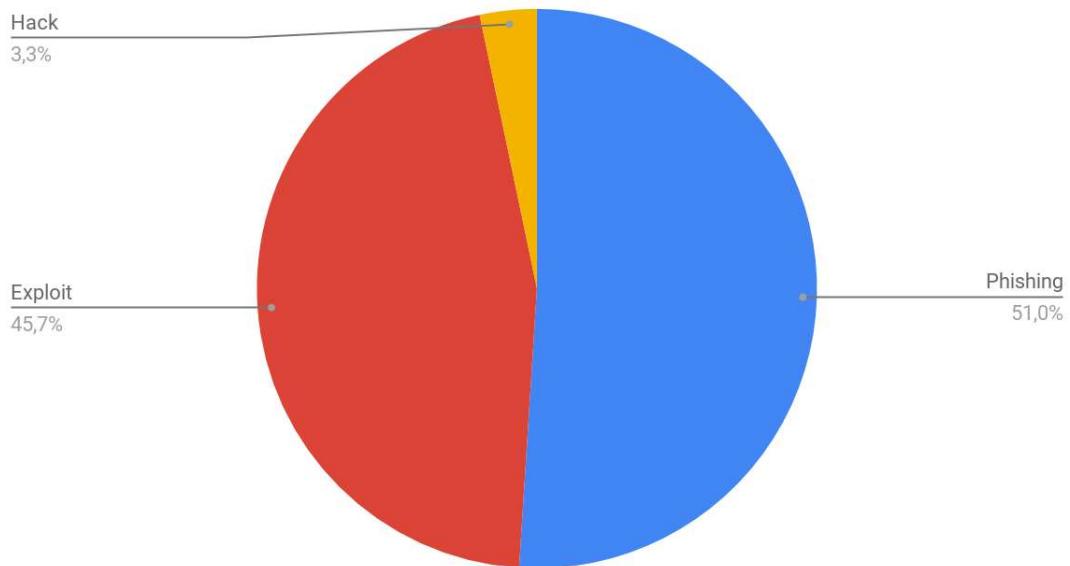
Для защиты от фишинговых атак предустановленный браузер разрешает открывать сайты только из заранее заданного на сервере *UniDefense* белого списка адресов.

Таким образом, вернувшись к данным Chainalysis о способах мошеннических действий, можно отметить, что *CWP* решает все известные проблемы,

связанные с обеспечением безопасности данных при работе с криптокошельками:

- от фишинга - использованием специально сконфигурированного браузера и наличием только подписанных специальным ключом приложений;
- от эксплойта - наличием изолированной среды и механизма подписи программ;
- от хакерской атаки – применением встроенного невскрываемого криптохранилища.

Losses after the actions of intruders



2.3. История продукта с 2008 года

Идея микрокомпьютера СИР впервые появилась в 2008 году. В 2009 году был получен патент на полезную модель и началось производство изделий для нужд корпоративных заказчиков. В то время микрокомпьютер имел иное название — *uPC* (micro PC).



В 2010 году начался процесс патентования микрокомпьютера в США, в 2016 пролонгирование экспертизы.

С начала проекта в 2008 году было разработано шесть версий микрокомпьютера под разные сферы деятельности и применения. В то время микрокомпьютер имел иное название — *uPC* (micro PC).

2009



ARM ATMEL AT91RM9200, 256 MB, 512 GB,
RTC w/battery

OS: Linux

Применение: ПК системного администратора,
тонкий клиент с предустановленным VPN

2010



ARM ATMEL AT91RM9200, 256 MB, 1 GB,
Backup Battery, RTC w/battery

OS: ALT Linux

Применение: ПК системного администратора,
тонкий клиент с предустановленным VPN,
ключ доступа к удаленному серверу или базе
данных, портативное рабочее место

2011



ARM ATMEL AT91RM9200, 256 MB, 1 GB, RTC
w/battery

OS: ALT Linux

Применение: портативное рабочее место с
предустановленным VPN и ключом доступа к
удаленному серверу и медицинской базе
данных в рамках автоматизированной
системы мониторинга здоровья

2012



ARM TI AM3359, 512 MB, 1 GB, Wi-Fi, Backup
Battery, Graphic LCD

OS: Debian Linux

Применение: ключ доступа и удаленное
рабочее место в рамках системы мониторинга
здравья, рабочее место научного сотрудника
для доступа к удаленным базам знаний

2015



ARM Allwinner A10, 512 MB, 2 GB, Wi-Fi, microHDMI, Audio
OS: Debian Linux, Android
Применение: портативное рабочее место с деловыми и игровыми приложениями

2016

Фото отсутствует по требованию клиента

ARM TI AM3359, 512 MB, 1 GB, Backup Battery, Graphic LCD
OS: Debian Linux, Android
Применение: портативное рабочее место, ориентированное на клиент-сервер приложения, например, 1С Предприятие, 1С Бухгалтерия или 1С Кадры

Примечание. В таблице приведены фотографии только печатных плат без внешнего вида изделий. Это сделано по требованиям заказчиков, в связи с необходимостью соблюдения подписанных с ними соглашений о конфиденциальности NDA (Non-Disclosure Agreement).

2.4. Применение существующего продукта в криптомире и его модификация

Для создания микрокомпьютера CWP мы воспользовались существующим продуктом uPC, который изначально был разработан для защиты персональных данных и удаленных соединений. Мы полностью переработали состав модулей ядра Linux, исключили модули и приложения, которые небезопасны с точки зрения проникновения в устройство извне, модифицировали систему обновления и дополнили изделие аппаратным невскрываемым хранилищем *Rutoken S micro*.

Rutoken S micro — это микро-модуль, предназначенный для безопасной двухфакторной аутентификации пользователей, защищенного хранения ключей шифрования и ключей электронной подписи, а также цифровых сертификатов и иной конфиденциальной информации.

Rutoken S micro реализует следующие функции:

Функция	Описание
Аутентификация	Двухфакторная аутентификация при доступе к устройству, к операционной системе, к серверам и приложениям (в зависимости от настроек)
Безопасное хранение ключевой информации	<ul style="list-style-type: none">→ Использование ключевой информации для выполнения криптографических операций на самом устройстве без возможности выдачи наружу закрытой ключевой информации→ Сгенерированные на микро-токене ключи не могут быть скопированы
Защита персональных данных	<ul style="list-style-type: none">→ Защита электронной переписки: шифрование почты, электронная подпись почтовых отправлений→ Защита доступа к компьютеру и в домен локальной сети→ Возможность шифрования данных на дисках
Использование	<ul style="list-style-type: none">→ Хранения служебной информации, персональной информации пользователей, паролей, ключей шифрования, цифровых сертификатов и любой другой конфиденциальной информации→ Единое идентификационное устройство для доступа к криптокошелькам, обеспечивающее разграничение доступа, цифровую подпись, аутентификацию при доступе к кошелькам и приложениям

Модуль *Rutoken S micro* обеспечивает поддержку следующих международных стандартов:

- ISO 7816-3 — протокол T=0
- ISO 7816-4 — внутреннее устройство и команды
- ISO 7816-8 — криптография
- ISO 7816-9 — жизненный цикл

Помимо необходимой модификации аппаратной части, мы переработали портал онлайн-сервисов UniDefense, который позволяет дистанционно настраивать один или несколько микрокомпьютеров СИР, находящихся в распоряжении пользователя или группы пользователей. В бета-версии портал выполнен по традиционной технологии, однако на одном из этапов дорожной карты проекта будет запущена собственная децентрализованная

блокчейн-платформа, обеспечивающая хранение состояний, транзакций, авторизацию и автоматизацию выполнения контрактов.

2.5. Онлайн-сервисы UniDefense по подписке

Подписка оформляется на одно устройство в личном кабинете пользователя.

После оформления подписки пользователю доступны следующие возможности:

- Двухфакторная аутентификация
- Настройка VPN-туннелей
- Магазин приложений
- Восстановление приложений на новое устройство

Двухфакторная аутентификация позволяет дополнительно защитить устройство и данные в личном кабинете пользователя от несанкционированного доступа. Для этого пользователю при входе, помимо имени пользователя и пароля, предлагается ввести код, который он получает одним из следующих способов: по электронной почте, в SMS-сообщении или в приложении для смартфона. Двухфакторная аутентификация применяется как на устройстве, так и в личном кабинете пользователя.

Сервис VPN-туннелей позволяет создать защищенный канал между устройством и точкой назначения. Этот канал зашифрован и защищен от перехвата. Передача информации по такому каналу безопасна и анонимна. В личном кабинете пользователь может выбрать точку назначения трафика.

Установка приложений на устройство возможна только через магазин приложений. Это позволяет исключить возможность применения вредоносных программ и обеспечить защиту данных на устройстве. В случае утери или кражи устройства пользователь может заблокировать его в личном кабинете и восстановить набор приложений на новом устройстве.

При работе с приложениями сторонних блокчейн-проектов используются нативные подписки. Например, при работе с игровой консолью Playkey используется подписка этого проекта, а оплата подписки осуществляется через криптокошелек блокчейн платформы CryptoWorkPlace.

2.6. Варианты продуктов

Команда проекта предполагает выпуск нескольких вариантов продукта.

Продукт	Состав	Назначение
CWP	Микрокомпьютер CWP + подписка на онлайн сервис (месяц, квартал, год)	Индивидуальный комплект портативного выделенного персонального компьютера с выборочной подпиской на онлайн сервис, позволяющего восстанавливать пароли, заблокировать потерянное устройство, настраивать работу приложений
CWP DUO	Два микрокомпьютера CWP, имеющих общий ключ для защищенной связи + подписка на онлайн сервис (месяц, квартал, год) + онлайн-сервис на блокчейн платформе	Комплект из двух микрокомпьютеров CWP для себя и для партнера. Оба CWP имеют предустановленный одинаковый ключ шифрования, позволяющий производить переводы между криптокошельками и устанавливать защищенное прямое соединение для закрытой связи с помощью встроенного мессенджера. Возможно управление одним кошельком с двух микрокомпьютеров
CWP CORP	Комплект из 10 микрокомпьютеров CWP с годовой подпиской на онлайн сервис	Корпоративный комплект из 10 микрокомпьютеров CWP с годовой подпиской на онлайн сервис, позволяющий восстанавливать пароли, заблокировать потерянное устройство, настраивать работу приложений
CWP CORP100	Комплект из 100 микрокомпьютеров CWP с годовой подпиской на онлайн сервис	Корпоративный комплект из 100 микрокомпьютеров CWP с годовой подпиской на онлайн сервис, позволяющий помимо восстановления паролей и блокировки потерянных устройств, производить индивидуальную их настройку, активирование и блокировку приложений
CWP GAME	Микрокомпьютер CWP + клиентское ПО для облачных игр + онлайн-сервис на блокчейн платформе	Индивидуальный комплект портативного выделенного персонального компьютера в качестве игровой консоли для облачных игр

Команда проекта обладает компетенциями для использования современных технологий AI и ML, что позволит накопить и проанализировать статистику использования для повышения устойчивости продукта к атакам злоумышленников. В связи с этим продукт будет постоянно модернизироваться, количество и качество онлайн сервисов UniDefense будет расти, производительность микрокомпьютера CWP будет наращиваться за счет применения современных компонентов и оптимизации модулей ядра операционной системы.

CWP - это стандартное решение для одного пользователя, обеспечивающее одновременно защиту его криптокошельков и ключей, а также безопасный выход в Интернет из любого недоверительного окружения. CWP имеет дополнительный режим роутера, обеспечивающий безопасное соединение приложениям вашего смартфона из недоверительного окружения с интересующими вас удаленными ресурсами. В этом режиме достаточно подключить CWP к стандартному зарядному устройству с USB. Кроме того, этот девайс можно использовать в качестве подарка с предустановленным кошельком и средствами на нем.

CWP CORP - это решение для корпоративных клиентов или групп пользователей с единой административной панелью, позволяющей настраивать каждый из CWP по отдельности или все вместе на основе единой политики безопасности. Политика безопасности может включать черные и белые списки, активирование или блокирование приложений, установку приложений и обновлений из магазина приложений.

CWP DUO - это самый интересный продукт из предлагаемых проектом на сегодня. Комплект из двух микрокомпьютеров CWP, настроенных на совместную работу с одним общим или двумя раздельными кошельками. В режиме работы с раздельными кошельками возможен перевод средств между ними в один клик без указания реквизитов перевода. Для сопровождения (комментирования) переводов можно использовать встроенный мессенджер с шифрованным каналом связи. С таким комплектом два человека, находящихся в разных частях света в недоверительном окружении (чужая сеть), могут безопасно осуществлять переводы средств друг другу нажатием одной кнопки или по таймеру или по смарт-контракту при включенном устройстве. При этом достаточно подключить CWP к стандартному зарядному устройству с USB.

CWP GAME Для увеличения аудитории, использующей CWP, команда проекта предлагает микрокомпьютер с клиентским программным обеспечением сторонних блокчейн-проектов, реализующим игровую консоль для облачных

игр. Возможны варианты игровых консолей Nvidia, GeForceNow, Steam и Playkey. Такой вариант применения позволяет геймерам отказаться от покупки дорогостоящего персонального компьютера в пользу недорогого компактного ПК, обеспечивающего стриминговый сервис. На примере известного проекта Playkey геймеры смогут ощутить следующие выгоды:

- возможность играть где угодно
- возможность играть на любом устройстве (Windows-ПК, Mac, телевизор)
- десятикратная экономия по сравнению с покупкой игрового оборудования

Владельцы каждого варианта CWP могут воспользоваться дополнительными возможностями системы. После активации в личном кабинете портала UniDefense, на микрокомпьютер устанавливается дополнительное ПО, после чего он становится нодой блокчейна CryptoWorkPlace, наряду со стандартными решениями для нод. Пользователь сможет сохранять в блокчейне собственную информацию, создавать резервную копию установленных в микрокомпьютере программ или оставлять зашифрованные заметки, не опасаясь безвозвратно потерять их при поломке или потере устройства, ведь эта информация навсегда и неизменно помещается в распределенное хранилище, узлами которого выступают все устройства-участники.

Для версии продукта CWP DUO, зная его уникальный идентификатор, один пользователь сможет переслать другому произвольное сообщение, будучи уверенным, что переданная информация не будет подделана и искажена, а адресат получит сообщение при подключении своего устройства к сети, что может служить сопровождением автоматического выполнения смарт-контракта.

Участник экосистемы может в любой момент прекратить свое участие в блокчейне, вернуть свое устройство к изначальному состоянию и перестать получать сообщения других пользователей или отправлять собственные. Тем не менее, уже помещенные к тому моменту данные всегда будут доступны к скачиванию на его микрокомпьютер.

Для версии продукта CWP GAME включение режима работы с блокчейн платформой позволит автоматизировать оплату онлайн подписок сторонних сервисов с автоматической конвертацией токенов разных блокчейн-проектов.

3. Экономика проекта

Как было сказано ранее, команда проекта работала над продуктом под названием *iPC* в течение нескольких лет, решая проблемы информационной безопасности корпоративных заказчиков. Чтобы предложить крипто сообществу конкурентное решение, нам потребуется выпустить микрокомпьютеры *CWP* в

промышленной серии из нескольких десятков тысяч единиц. Поэтому мы предлагаем всем заинтересованным лицам участие в финансировании, что позволит получить токены проекта со скидками от 10% до 40% и продукт со скидкой 50%. Для этого мы будем проводить открытую продажу токенов в два этапа.

Первый этап Token Pre-Sale позволит привлечь средства для маркетинга и подготовки к основному этапу. Кроме того, мы планируем на часть привлеченных средств выпустить опытную партию микрокомпьютеров CWP и запустить бета-версию веб-портала UniDefense.

Второй (основной) этап Token Sale предполагает выпуск опытной партии и предоставление крипто сообществу первых образцов продукта в версии Light.

Чтобы привлечь средства на первом и втором этапах будет разработан и публично доступен смарт-контракт на платформе Ethereum. Токен совместим со стандартом ERC20. Выпуск токенов происходит в момент продажи, и ограничен количеством в 500 000 000 CWT.

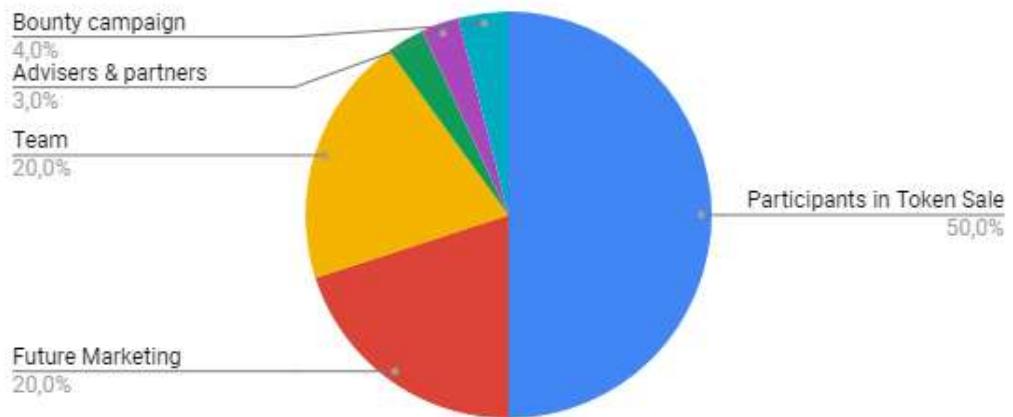
На первом этапе будет создан токен CWT-P специально для пресейла. В момент старта TGE (Token Generation Event) участники смогут обменять токен CWT-P на основной токен CWT по курсу 1 CWT-P = 1 CWT.

Общие параметры:

Токен	CWT
Объем эмиссии	500 000 000
Принимаемые валюты	BTC, ETH, LTC

Распределение токенов после всех этапов привлечения средств:

Participants in Token Sale	50%
Future Marketing	20%
Team	20%
Participants in Token Pre-Sale	3%
Advisers & partners	3%
Bounty campaign	4%



3.1. Token Pre-Sale

Период проведения: January 1, 2018 - January 31, 2018

Токен CWT-P

Soft cap: 180 ETH (\$240K)

Hard cap: 1351 ETH (\$1.8M)

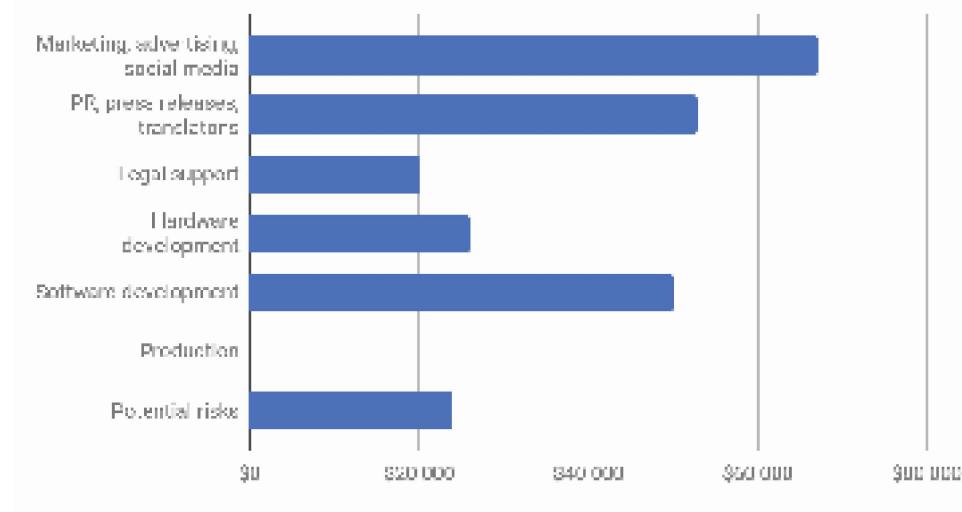
Токенов к продаже: 15,000,000 (3%)

1 CWT-P = \$0.12

Распределение привлеченных средств в двух вариантах развития процедуры pre-sale:

Вариант 1. В случае привлечения минимально необходимой суммы (soft cap), запуск производства опытной партии микрокомпьютеров не представляется возможным, так как все привлеченные средства будут потрачены на подготовку запуска основного этапа.

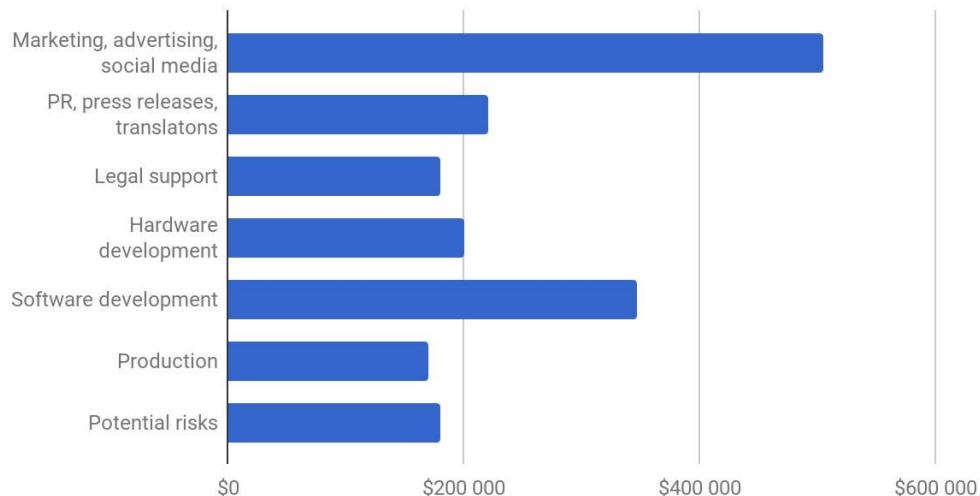
Token Pre Sale soft cap



Вариант 2. В случае успешного привлечения средств больше минимальной суммы (soft cap) и до максимума (hard cap), будет запущено производство опытной партии микрокомпьютеров. Количество микрокомпьютеров СWP в опытной партии равно 100 единицам, а количество партий может варьироваться в зависимости от привлеченной суммы следующим образом:

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

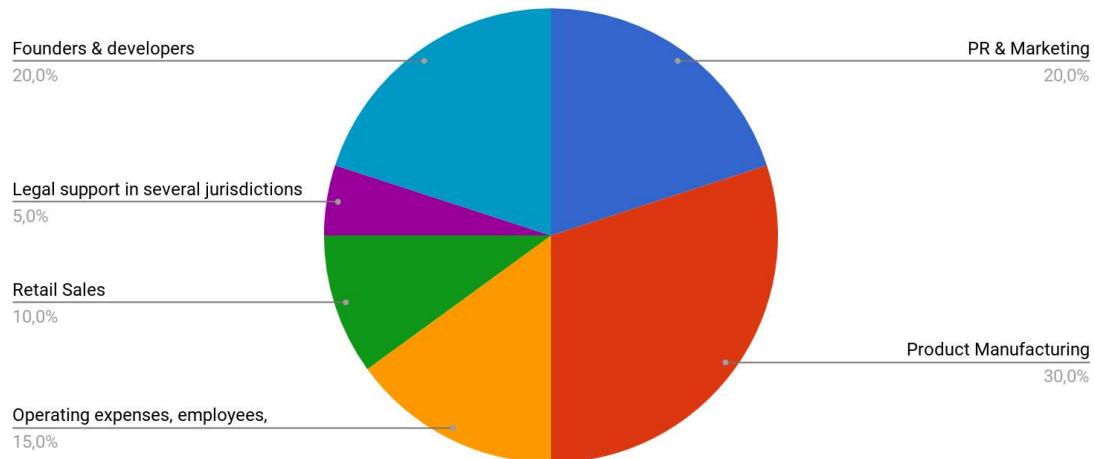
Token Pre-Sale hard cap



3.2. Token Sale

Период проведения:	<i>March 1, 2018 - March 31, 2018</i>
Токен	<i>CWT</i>
Soft cap:	<i>1802 ETH (\$2.4M)</i>
Hard cap:	<i>35,586 ETH (\$47.4M)</i>
Токенов к продаже:	<i>250,000,000 (50%)</i>

На втором этапе будет привлечено не более \$47,400,000 средств участников TGE. Распределение средств, привлеченных на этапе Token Sale будет выглядеть следующим образом:



30% привлеченных в ходе TGE средств мы планируем потратить на запуск производства в промышленных масштабах. 70% от этой суммы будет потрачено на закупку компонентов, изготовление печатных плат и их монтаж. 20% пойдет на оплату работы сторонних разработчиков, привлекаемых в Европе, США и Азии. 10% - на изготовление производственной оснастки, тестового оборудования, складской сервис и межоперационную логистику.

20% привлеченных в ходе TGE средств мы отводим на маркетинг в трех регионах Европа, США и Азия в течение первого года выхода продукта на мировой рынок. 80% от этой суммы будет потрачено на продвижение продукта в США, Японии, Китае и Сингапуре.

20% привлеченных средств будет потрачено на оплату труда нашей команды. 30% из этой суммы планируется потратить на исследовательские работы в течение первого года выхода продукта на рынок, которые включают накопление статистики и применение искусственного интеллекта и машинного обучения для повышения уровня защиты продукта от действий злоумышленников.

3.3. Применение скидок при покупке токенов

Пользователи, приобретающие токены CWT, получают скидки, размеры которых будут уменьшаться с ростом привлеченной суммы следующим образом:

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

3.4. Применение скидок при покупке продукта

Владельцы токенов CWT могут приобрести продукт со скидкой 50% относительно цены в фиатной валюте. Во время приобретения продукта токены, потраченные на покупку, будут сжигаться, чтобы исключить получение двойного дохода. Автоматическое сжигание использованных токенов будет приводить к увеличению их стоимости при сохранении популярности продукта в крипто сообществе.

Product Options	Price		
	USD	Discount 50%	CWT=\$0.2
CWP + Monthly Subscription	\$300	\$150	750
CWP + Quarterly Subscription	\$485	\$243	1 213
CWP + One year subscription	\$1 280	\$640	3 200
CWP DUO	\$1 480	\$740	3 700
CWP CORP	\$13 300	\$6 650	33 250
CWP CORP100	\$120 000	\$60 000	300 000

4. План развития

4.1. Дорожная карта проекта

Декабрь-Январь 2017	Март 2018	Апрель 2018	Q2-Q3 2018	Q4 2018
Token Pre-Sale	Token Sale	Тестирование	Производство	Продажа
Выпуск опытной партии устройств	Запуск бета-версии портала	Тестирование продукта в независимой лаборатории	Начало серийного производства устройств и запуск технической поддержки	Начало продаж в Европе, США и странах Тихоокеанского региона
Создание токена CWT-P и запуск его смарт-контракта	Создание токена CWT и запуск смарт-контракта TGE	Открытие офисов в США, Чехии и Японии	Запуск портала UniDefense и своего блокчейн	Запуск службы поддержки

4.2. Производственные планы проекта

Структура компании предполагает создание нескольких офисов в разных странах:

- Офис Европейского отделения — Прага (Чехия)
- Офис Азиатского отделения — Токио (Япония)
- Офис Северо-американского отделения — Нью-Йорк (США)
- Производственное подразделение — Гуандун (Китай)

Производство печатных плат, заказ электронных компонентов, монтаж компонентов и загрузка тестовых прошивок будут выполняться на заводе ICAP GROUP, Гуандун.

Установка на платы микро-модулей *Rutoken S micro* будет производиться Европейским подразделением, здесь же будет выполняться загрузка рабочей прошивки изделия. Для обеспечения этих работ будет обеспечена защита от несанкционированного доступа на производственные площади, где осуществляется хранение и установка дополнительных компонентов и программных модулей.

5. Команда

5.1. Руководители и разработчики



[Linkedin](#)

CEO Yoji Kishi

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

Shin-Nippon Research (Hong Kong) Co., Ltd.

Vice-President

International Society of Stem Cells Development , Director
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 Алексей Гладков

Президент Kintaro Power Cells Japan

Региональный директор MapMess Inc.

Директор-основатель научно-исследовательской
компании AV-Cells Singapore

30 летний опыт ведения собственного бизнеса

20 лет ведения бизнеса в Сингапуре и Японии





[Linkedin](#)

Microsoft
CERTIFIED
Professional

Microsoft
CERTIFIED
*Technology
Specialist*

СТО Максим Маслич

Microsoft Certified Professional

Microsoft Certified Technology Specialist Exam 511

Blockchain and smart contracts developer

Эксперт в управлении процессом разработки ПО, построении распределенных, высоконагруженных и защищенных систем

Разработка систем мониторинга транспорта (грузовой, легковой, спецтехника, пассажирские перевозки, весовой контроль, контроль производственных линий, автоматизация таксопарка) для компаний Алроса, ГАЗПРОМ, Лукойл, Русал, РЖД, Сатори, Автолайн, городское такси.

Разработка систем документооборота, проведения тендеров и торгов для X5 Retail Group, Лента, Metro C&C



Артур Енокян

Инженер-программист 1 категории

Full-Stack JavaScript Senior Developer

Certified Middle End Android Developer

Certified Middle End iOS Developer

Эксперт в разработке Highload приложений

Разработка трейдинг-платформ для alpari.ru

Разработка специального программного обеспечения для крупнейших ритейлеров

Специалист по криптографии

Разработка систем электронного документооборота





Антон Полянский

Руководитель производства аппаратных средств
Инженер-разработчик аппаратных средств
Инженер-программист встраиваемых систем
Специалист по вычислительным системам микро исполнения
Разработка схемотехнических решений, трассировка печатных плат и разработка встраиваемого программного обеспечения для тепловизионных приборов
Разработка схемотехнических решений, трассировка печатных плат для устройств нижнего уровня системы распознавания музыкальных произведений Quinta
Разработка схемотехнических решений и трассировка печатных плат для устройств системы Умного дома
Разработка микроминиатюрных биометрических датчиков и процессорной системы управления биоэлектрическим протезом верхних конечностей
Разработка встраиваемых систем передачи данных на основе технологий Wi-Fi, GSM и Bluetooth



Денис Кузнецов

Lead Mathematician, Senior Architect Developer
Программист встраиваемых систем
Специалист нейронных систем и глубокого обучения
Разработка агента для ведения нецелевого диалога в банковской системе
Разработка Telegram-ботов с поддержкой искусственного интеллекта
Разработка встраиваемого программного обеспечения для устройств системы распознавания музыкальных произведений Quinta
Соавтор патентов для алгоритмов распознавания музыкальных произведений

[Linkedin](#)



Антон Маслов

Senior System Analyst, PHP-Developer

Оптимизация и автоматизация логистических
бизнес-процессов DAICHI

Системная аналитика многомодульных
высоконагруженных систем с различными
интеграциями для METRO C&C, Lenta

Разработка системы планирования поставок по ТОС
(Theory of Constraints) для производства IKEA,
интегрированной с 1С

Управление разработкой и позиционированием
продукта

[Linkedin](#)

5.2. Эдвайзеры



Александр Поделько

К.т.н., эксперт по разработке и тестированию ПО
Член совета директоров группы компьютерных
измерений.

Oracle, Consulting Member of Technical Staff
Hyperion, Distinguished Performance Engineer
Aetna, Sr. Architect II

[Facebook](#)

[Linkedin](#)

[Personal site](#)

Александр осуществляет координацию продаж и
производства продукта для американского рынка,
управление филиалом проекта в США,
взаимодействие с крупными американскими
компаниями-партнерами, обеспечивающими научную
и техническую поддержку проекта.

Александр имеет 30 летний опыт в тестировании
программного обеспечения, что позволяет ему
организовать взаимодействие проекта с крупнейшими
игроками рынка тестирования ПО, такими как
QAMentor.



Руслан Пичугин

Основатель SandCoin, соучредитель «Ревитал»

Основатель Yocto Games

Сотрудничество с Chillingo, Electronic Arts, Microsoft Studios

Руслан руководитель нескольких проектов, один из которых недавно успешно завершил ICO.

Руслан является популярным блокчейн экспертом, юристом и экономистом, это позволяет ему курировать важные организационные, маркетинговые и экономические вопросы, с которыми сталкиваются основатели проекта.



Алексей Лыков

CTO Playkey

Alexey is a technical specialist with 20 years of experience. He has extensive experience working with high-loaded systems. He develops platform solutions of any complexity.

Alexey is working on the development of the blockchain system in Playkey for 1.5 years. Manages the infrastructure of more than 1,000 video cards. Developed a unique solution for the mining of cryptocurrency on gaming platforms.

Alexey's competencies help the project in the technical issues of TGE.



Ваган Саруханов

CEO Flexlab Ltd.

CTO uPCLabs Inc.

Блокчейн-исследователь и эксперт

30-летний опыт в контрактном производстве

электроники и ПО

Более 20 проектов в различных отраслях

Ментор проектов

Wagan's competencies help the project in the business development and technical issues of product development and manufacturing.

[Facebook](#)
[Linkedin](#)

5.4. Партнеры

ICAPE GROUP	<p>Группа компаний ICAPE с головным офисом в Париже и производством в Китае. Группа ICAPE является одной из ведущих европейских компаний по производству и поставкам печатных плат (PCB) и заказных технических деталей, произведенных в Китае.</p> <p>http://www.icafe-group.com</p> 
Cells Power Japan Japan's state-of-the-art cell technology	<p>На заводах компании будет организовано производство микрокомпьютеров CWP, выходной контроль и загрузка тестовой прошивки.</p> <p>Японская компания Kintaro Cells Power новатор в области клеточной медицины, входит в международную группу компаний, специализирующихся на предоставлении услуг в области здравоохранения и туристической медицины с акцентом на обслуживании ВИП-сегмента.</p> <p>https://cellspower.com</p> 



Партнер -
тестирование
продукта

Американская компания, лидер в области
тестирования программного обеспечения и
оборудования
<http://www.qamentor.com/>



6. Важное уведомление

Если вы еще не стали участником представляемого TGE (Token Generation Event) и не уверены, будете ли участвовать в нём, рекомендуем получить профессиональную консультацию в юридической, финансовой и налоговой сферах у соответствующих специалистов.

Токены CWT-P и CWT не являются цennыми бумаги в любой юрисдикции. Настоящий документ не является для читателя настоящего документа или участника представляемого TGE предложением о покупке ценных бумаг или тендером на инвестиции в ценные бумаги в любой юрисдикции.

6.1. Отказ от ответственности

Проект CryptoWorkPlace, его основатели и команда не несут ответственности за какой-либо специальный, опосредованный или какой-либо косвенный ущерб, а также любые другие потери, такие как потеря дохода, прибыли или потеря использования или данных, вызванных использованием настоящего документа.

Получая доступ к любой информации, представленной в этом документе или любой его части (в зависимости от обстоятельств), вы представляете и гарантируете проекту CryptoWorkPlace следующие:

- вы соглашаетесь и осознаете, что токены CWT-P и CWT не являются собой ценные бумаги в любой юрисдикции;
- вы соглашаетесь и признаете, что в настоящем документе не содержится рекомендаций по покупке токенов CWT-P и CWT. Это не является

инвестиционным решением или контрактом, что означает, что этот документ не может считаться инвестиционным или каким-либо другим договором, и факт его предоставления не может быть основанием для инвестирования или заключения инвестиционного соглашения;

- вы соглашаетесь и признаете, что любая информация, представленная в этом документе, не была проверена или одобрена регулирующими органами. Публикация и распространение этого документа для вас не означает, что соблюдены действующие законы, нормативные требования, правила или положения;
- вы соглашаетесь и признаете, что в случае, если вы хотите приобрести любые токены CWT-R и CWT, они не должны восприниматься или классифицироваться как:
 - ◆ любой вид валюты, кроме как криптовалюты;
 - ◆ долговые ценные бумаги, акции, выпущенные любым лицом или организацией;
 - ◆ права, опционы или деривативы в отношении таких долговых обязательств или акций;
 - ◆ права по договору на разницу или по любому другому контракту цель которого получить прибыль или избежать потерь;
 - ◆ единицы в схеме коллективных инвестиций;
 - ◆ единицы в промышленном или деловом трасте;
 - ◆ производные финансовые инструменты в бизнесе;
 - ◆ любая другая ценная бумага или класс ценных бумаг;
- все вышеупомянутые представления и гарантии являются достоверными, полными, точными и не вводящими в заблуждение со времени вашего доступа и/или владения этим документом и его частями (в зависимости от обстоятельств).

6.2. Отсутствие эмиссии ценных бумаг

Настоящий документ не содержит каких-либо эмиссий и не предназначен для создания таких эмиссий, а также эмиссии ценных бумаг и не требует внесения инвестиций в ценные бумаги в любой юрисдикции. Любое лицо не обязано заключать какой-либо договор или юридическое обязательство на основании настоящего документа. Никакие криптовалюты или другие формы оплаты не должны приниматься на основании этого документа.