МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)

Кафедра защиты информации

ЗАЩИЩЕННЫЙ ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС УПРАВЛЕНИЯ КРИПТОВАЛЮТНЫМИ АКТИВАМИ НА БАЗЕ ПЛАТФОРМЫ МКТ

**ОТЧЕТ ОБ ОБСЛЕДОВАНИИ**

Выполнил: Шарапов Роман Андреевич,

студент ФРТК 419 группы

Научный руководитель:

Конявский В.А.

Москва – 2019

# Содержание

[Содержание](#_Toc13911)

[1 Общие положения](#_Toc18159)

[2 Описание объекта исследования](#_Toc16206)

[2.1 Классификация криптовалютных активов](#_Toc13873)

[2.1.1 Криптовалюты](#_Toc22067)

[2.1.2 Токены](#_Toc14875)

[2.2 Классификация средств работы с криптовалютными активами](#_Toc3277)

[2.2.1 Криптовалютные кошельки](#_Toc31467)

[2.2.2 Криптовалютные обменники](#_Toc6567)

[2.2.3 Криптовалютные биржи](#_Toc28446)

[2.2.4 Боты-трейдеры](#_Toc21220)

[2.2.5 Майнинг пулы](#_Toc20356)

[2.2.6 Перечень потенциально опасных и безопасных сервисов](#_Toc9344)

[3 Программно-аппаратная реализация объекта](#_Toc15587)

[3.1 Общие сведения о программной реализации объекта](#_Toc1506)

[3.2 Реализация доверенной среды](#_Toc11232)

[3.3 Генерация ключевых пар](#_Toc20645)

[3.4 Хранение ключевых пар при длительном подключении к интернету](#_Toc4358)

[3.5 Требования к системе](#_Toc11011)

[4 Инструментарий для разработки](#_Toc22046)

[5 Заключение](#_Toc2634)

[Приложение 1. Техническое задание](#_Toc11065)

[Перечень принятых сокращений](#_Toc13889)

[Термины и определения](#_Toc6427)

[Список используемых источников](#_Toc15463)

# Общие положения

Обследование проводится в рамках предпроектных работ по теме «Защищенный программно-аппаратный комплекс управления криптовалютными активами на базе платформы MKT».

**Заказчиком** работ является кафедра защиты информации, которая относится к факультету радиотехники и кибернетики московского физико-технического института.

**Исполнителем** работ является студент кафедры защиты информации 419 группы ФРТК МФТИ Шарапов Роман Андреевич.

**Объектом обследования** является реализация механизмов управления криптовалютными активами.

**Целью обследования** является формирование требований для реализации ПАК, обеспечивающего управление криптовалютными активами.

В ходе обследования получены сведения о принципах работы сервисов управления криптовалютными активами с закрытыми ключами пользователей, о защитных мерах, необходимых для обеспечения безопасного управления криптовалютными активами на базе платформы МКТ.

Полученные в ходе обследования данные являются основой для реализации ПО.

Результаты проведенной работы отражены в настоящем отчете, который имеет следующую структуру:

- Описание объекта – Раздел 2;

- Программно-аппаратная реализация объекта – Раздел 3;

- Инструментарий для разработки – Раздел 4;

- Заключение – Раздел 5;

- Проект технического задания – Приложение 1.

# Описание объекта исследования

Прежде чем приступить к описанию механизмов управления криптовалютными активами, необходимо понять, что входит в перечень этих активов.

## Классификация криптовалютных активов

Перечислим и классифицируем все виды криптовалютных активов.

### Криптовалюты

Первый вид активов, **криптовалюты** — разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах и ведутся в блокчейн сетях.

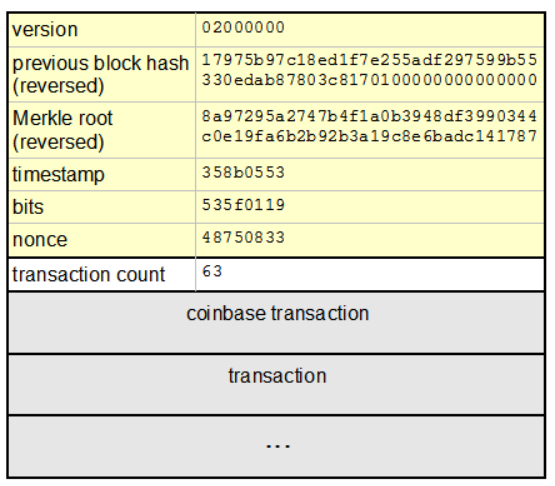
Блокчейн — это база данных, в виде связного списка, которая хранится одновременно на множестве компьютеров. Совокупность этих компьютеров, объединенных через интернет, называется блокчейн сетью.

Майнинг — деятельность по поддержанию распределенной платформы и созданию новых блоков с возможностью получить вознаграждение в форме эмитированной валюты и комиссионных сборов. Клиент, выполняющий майнинг называется майнером.

Майнинг служит для производства денежной массы [1]. Каждый раз, когда майнер создает новый блок, ему за это полагается награда - определенное число монет, которые он может потом потратить, тем самым запуская в сеть новые средства. Таким образом майнинг является основным источником всех криптовалютных активов.

В большинстве криптовалют действует система UTXO (Unspent Transaction Output), аналогичная биткойну: каждая транзакция должна быть потрачена полностью. То есть если у Алисы на аккаунте есть 5 BTC, и она хочет перевести Бобу 1 BTC, то она должна сделать транзакцию с двумя выходами: один для боба (1 BTC) и второй для «сдачи» для Алисы на ее собственный адрес (4 BTC).

В структуре любого блока первой всегда идет так называемая coinbase транзакция — именно она отправляет вознаграждение на адрес майнера. В отличии от обычных транзакций, coinbase transaction не тратит в качестве входов выходы из UTXO pool. Вместо этого у нее указан только один вход, называемый coinbase, который "создает" монеты из ничего. Выход у такой транзакции тоже только один. Он отправляет на адрес майнера награду за блок плюс сумму комиссий со всех транзакций в блоке.



(Рис. 1) Логическая структура Bitcoin блока

В блокчейн имплементирована программа с внутренним хранилищем в которой хранится реестр монет - массив ассоциаций аккаунтов (открытый ключ из ключевой пары) с суммами. Полный доступ к данному реестру имеет только эта программа, она же предоставляет всем желающим возможности просматривать суммы на аккаунтах и переводить суммы между ними, предварительно выполнив проверку на наличие у обратившегося доступа к тому аккаунту, с которого он пытается передать деньги, а также на не превышение суммы на балансе этого аккаунта. Проверка доступа основывается на проверке подписи транзакции, осуществленной с помощью закрытого ключа из классической пары шифрования с открытым ключом. Если проверка прошла, то запрос на транзакцию будет отослан в сеть, после чего запрос будет принят или отвергнут на основании алгоритма консенсуса, принятого в данном блокчейне.

Подытожим. Для того чтобы клиент мог воспользоваться криптовалютой, как денежным средством, необходимо, чтобы:

* только у клиента был доступ к его закрытому ключу;
* в реестре содержалась запись о том, что необходимое количество валюты проассоциировано с аккаунтом клиента;

### Токены

Смарт-контракт — это компьютерный алгоритм, хранимый и исполняемый в блокчейн сети. Он предназначен для формирования, контроля и предоставления информации о владении чем-либо, а также для автоматизации процесса исполнения договоров без привлечения третьей доверенной стороны.  В теле смарт-контракта описаны его условия и исходы исполнения [2].

Рассмотрим пример работы смарт-контракты в Ethereum: смарт-контракты представляют собой объекты, хранящие состояние и методы, при помощи которых это состояние обновляется. Транзакции, соответственно, представляют собой вызовы методов контрактов. Контракты могут взаимодействовать между собой, вызывая методы других контрактов, но любое действие в конечном счете инициируется транзакцией в пределах блокчейна.

Второй вид криптовалютных активов, **токен** — это смарт-контракт определенного формата, оперирование которым осуществляется вторым, родительским смарт-контрактом. Основная часть наиболее популярных на сегодняшний день токенов формируется в сети Ethereum в соответствии со стандартом ERC-20. В этом стандарте описаны условия (необходимые методы, функции и поля), при которых смарт-контракт считается токеном [3]. Перечислим их:

1. Функции и методы
   1. function totalSupply (): Возвращает суммарное количество выпущенных монет. Эту функцию может вызвать любой.
   2. function balanceOf (owner): Возвращает количество монет принадлежащих владельцу. Может вызвать любой. Кошельки для отображения количества токенов у клиента вызывают именно эту функцию.
   3. function transfer (address\_to, value): Передает определенное количество токенов на указанный адрес. Токены снимаются с баланса пользователя, который вызвал эту функцию. Метод должен создавать событие Transfer (описан будет далее) в случае успешного перемещения монет.
   4. function transferFrom (address\_from, address\_to, value): определенное количество токенов c одного адреса на другой. Пользователь должен иметь разрешение на перемещение токенов между адресами. Фактически эта функция позволяет доверенному лицу распоряжаться определенным объемом токенов на счету. Метод должен создавать событие Transfer (описан будет далее) в случае успешного перемещения монет.
   5. function approve (spender, value): Разрешает пользователю снимать со счета пользователя, вызвавшего функцию, средства не более чем указанное значение. На основе этого разрешения должна работать функция transferFrom. Метод должен создавать событие Approval (описан будет далее).
   6. function allowance (owner, spender): Возвращает сколько монет со своего счета разрешил снимать владелец другому пользователю.
2. События
   1. event Transfer (from, to, value): Событие, которое должно возникать при любом перемещении монет. То есть его нужно создавать внутри функций transfer и  transferFrom в случае успешного перемещения монет.
   2. event Approval (owner, spender, value): Событие должно возникать при получении разрешения на снятие монет. Фактически должно создаваться внутри функции  approve.
3. Поля
   1. constant name: Хранит полное название токена. К примеру «Testing».
   2. constant symbol: Хранит «символ», то есть короткое название токена. К примеру «TST». С этим символом токен будет отображаться на биржах и в кошельках пользователей.
   3. constant decimals: Количество знаков после запятой. 18 — это наиболее распространенное значение.

Процесс привлечения финансирования через продажу токенов получил название ICO (Initial Coin Offering). Полный процесс ICO выглядит следующим образом:

* Команда разработчиков имеет какую-то бизнес идею, к примеру, создание какого-либо приложения. При этом у них нет стартового капитала для начала разработки.
* Они объявляют ICO. Теперь каждый желающий может вложить некоторую сумму криптовалюты (к примеру Ethereum) в проект, а взамен получить токены, пропорционально вложенным средствам.
* Когда ICO завершится, и компания приступит к разработке проекта, покупатель может продать токены или продолжать удерживать их, ожидая рост цены токена на бирже

Количество токенов, которое эмитируется на ICO — это число, которое устанавливают сами разработчики внутри родительского смарт-контракта. Балансы токенов — это значения в ассоциативном массиве, где ключами являются адреса Ethereum и адрес смарт-контракта.

Рассмотрим процесс работы с токенами и смарт контрактами.

* Разработчик из своего клиента Ethereum отправляет транзакцию, в которой находится код смарт-контракта. Контракт, как обычный участник сети, размещается по определенному адресу, по которому в дальнейшем и будут обращаться пользователи. Кроме того, он имеет свой собственный баланс криптовалюты и умеет принимать и отправлять ее.
* Покупка токенов выглядит следующим образом:
  + - покупатель переводит криптовалюту на адрес смарт-контракта;
    - смарт-контракт перенаправляет их владельцу контракта;
    - функция внутри смарт-контракта, принимающая криптовалюту, умножает полученную сумму на установленный курс обмена токена и присваивает приславшему адресу соответствующее количество токенов, записывая в блокчейн соответствующую информацию;
    - эти изменения в памяти программы запишет в следующий блок майнер, который исполнит контракт и пришедшую в него транзакцию от пользователя.
* Перевод токенов от одного владельца другому выглядит следующим образом:
  + - пользователь вызывает метод transfer у смарт-контракта, помещённого по заданному адресу;
    - контракт отнимает часть токенов у адреса отправителя и добавляет на адрес получателя;
    - эти изменения в памяти программы запишет в следующий блок майнер, который исполнит контракт и пришедшую в него транзакцию от пользователя.

Токены бывают трех видов [4].

Первый вид — это **токены-акции**, свидетельствующие о внесении криптовалютных средств в капитал эмитента токенов и дающие обладателю токена право на получение части прибыли в виде дивидендов. То есть для эмитента они нужны для привлечения финансирования, а для покупателя - для получения прибыли в будущем.

Второй вид токенов — **аппкойны**, или токены приложений (токены жетоны). Эти токены предназначены в первую очередь для использования внутри приложения или сервиса, который выставили на ICO.

Третий вид токенов — **кредитные токены**, которые используются с целью краткосрочного заимствования денежных средств эмитентом с дальнейшей выплатой процентной ставки от суммы займа. Эти токены являются аналогом облигаций.

Подытожим информацию по двум подразделам. Криптовалютные активы делятся на криптовалюты и токены. Токены бывают трех видов: токены акции, кредитные токены и токены жетоны (аппкойны).

## Классификация средств работы с криптовалютными активами

Перейдем к механизмам управления криптовалютными активами.

**Управление криптовалютными активами** — деятельность клиента по манипуляции криптовалютами и токенами, направленная на сохранение и приумножение активов, а также совершение сделок и транзакций.

Существует несколько видов сервисов и средств работы с криптовалютными активами, которые и предоставляют механизмы управления этими активами. Перечень таких механизмов различается в зависимости от каждого конкретного сервиса.

Средства и механизмы, предоставляемые этими средствами, могут быть реализованы корректно и некорректно с точки зрения безопасности клиента. Необходимо перечислить и систематизировать все средства работы с криптовалютными активами, а также поделить их на две категории: безопасные средства и потенциально опасные средства.

Защищенный ПАК управления криптовалютными активами должен обеспечивать корректную работу пользователя с выделенными безопасными средствами.

При описании процесса работы сервисов в первую очередь будем обращать внимание на то, как в системе ведется работа с закрытыми ключами пользователя, так как именно они представляют наибольшую ценность для потенциальных злоумышленников.

### Криптовалютные кошельки

Для взаимодействия пользователя с блокчейном используют семейство программ, называемых **криптовалютными кошельками**. Их основная функция заключается в получении из управляющей программы блокчейна информации о сумме на аккаунте пользователя и отправлении в эту программу информации о передаче монет, с сигнатурой для идентификации пользователя как владельца. Криптовалютный кошелек должен уметь просканировать реестр блокчейна, прочитать там баланс пользователя, затем изменить его и баланс получателя транзакции.

Кошельки различаются по количеству поддерживаемых монет. Они бывают одновалютные, то есть поддерживающие операции только с одной криптовалютой, и мультивалютные, то есть поддерживающие операции с несколькими криптовалютами, а также с токенами стандарта ERC-20.

Рассмотрим классификацию криптовалютных кошельков:

* Горячие — это кошельки, имеющие постоянное соединение с интернетом.
  + - Онлайн кошельки — горячий кошелёк, запускаемый через интернет браузер на сайте. В этом варианте закрытые ключи генерируются и хранятся на сервере.
    - «Тонкие» локальные кошельки — кошельки, устанавливаемые на компьютере пользователя, при этом блокчейн на устройство не скачивается (в том числе и при первой синхронизации). Когда возникает необходимость прочитать данные из блокчейна или произвести транзакцию, то идет обращение к серверам или к соседним узлам сети.
    - «Толстые» локальные кошельки — кошельки, устанавливаемые на компьютере пользователя, которые общаются только со своим, заранее скаченным и постоянно обновляемым блокчейном.
* Холодные — это кошельки, не имеющие постоянное соединение с интернетом и блокчейном [5]. При этом, с них не совершаются транзакции.
  + - Аппаратные кошельки — кошельки на аппаратных отчуждаемых носителях (обычно флеш накопителях или смарт картах), ведущие взаимодействие с блокчейном через локальный кошелек или же через сайт. Такие кошельки, хранят закрытый ключ внутри себя и получить к нему доступ через сеть будет нельзя (на выходе прибора выдается только уже сформированная транзакция).

Все типы горячих кошельков являются небезопасными, потому что канал связи или сервера могут быть скомпрометированы. Холодные кошельки в пассивном режиме (без соединения с интернетом и без совершения транзакций) являются безопасными, при условии, что компьютер является доверенным, и мы можем гарантировать, что у злоумышленников нет к нему доступа. Однако при переходе кошелька в активный режим (совершение транзакции через интернет) на определённый промежуток времени риск компрометации значительно возрастает, при этом, чем выше хранимая сумма - тем выше риск. После совершения транзакции и отключения интернета риск компрометации ключа снижается, но остается, так как злоумышленники, применяя аналитические методы и вредоносное программное обеспечение, все равно могут получить доступ к закрытым ключам.

Существует модификация модели холодного хранения, которая применяется для уменьшения риска компрометации в момент совершения транзакции:

* Система состоит из двух компьютеров, один из них всегда отключен от интернета, второй - подключен к сети
* На первом компьютере с помощью кошелька создаем пару ключей, импортируем открытый ключ на второй компьютер. После чего на этот адрес можно перевести необходимую сумму для хранения.
* Когда возникает необходимость в переводе, то на втором компьютере создается неподписанная транзакция (Указывается адреса отправителя и получателя, а также объём средств), которая затем копируется на съемный носитель и импортируется на нем на первый компьютер, неподключенный к интернету.
* На первом компьютере транзакция подписывается после чего точно также на съемном носителе импортируется на первый компьютер и отсылается в сеть.

Такая схема называется офлайн подписью транзакций.

Подытожим. Безопасным можно считать только «холодный» вариант хранения ключей. Для совершения транзакций целесообразно применять описанную выше схему с офлайн подписью.

Все сервисы, о которых мы будем говорить ниже, используют криптовалютные кошельки на серверной стороне для совершения клиентских операций в блокчейне.

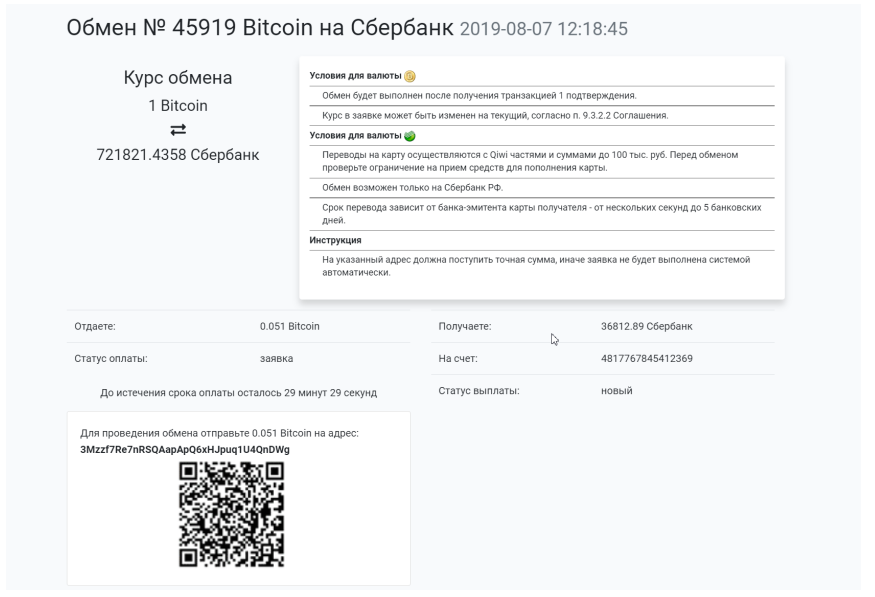
### Криптовалютные обменники

Для покупки/продажи криптовалюты, а также ее обмена на другие валюты используются **криптовалютные обменники**. В ходе обследования были изучены 20 наиболее популярных криптовалютных обменников [6].

1. Netex24
2. Kassa
3. WW-pay
4. Xchange
5. 365Cash
6. 24paybank
7. NixExchange
8. F-Change
9. Baksman
10. FastChange
11. Payget
12. 60cek
13. El-Change
14. Top-Exchange
15. Bitoс
16. Ychanger
17. Prostocash
18. Platov
19. Ramon Cash
20. BTCBIT

Принцип их работы следующий:

* Пользователь выбирает валютную пару, то есть что на что он хочет поменять. Таким образом размещается заявка на обмен.
* Указывается сумма для обмена. В соседнем поле будет рассчитан получаемый объем.
* В случае покупки криптовалюты за реальные деньги пользователь вводит номер электронного кошелька/банковской карты, с которой будут списываться средства, и вводит адрес криптовалютного кошелька, на который будет поступать купленная криптовалюта. После чего ему будет предложено совершить платеж на банковскую карту получателя.
* В случае продажи криптовалюты за реальные деньги пользователь вводит номер кошелька/банковской карты, на которую будет получены средства. И вводит адрес кошелька, с которого будет проводиться транзакция. После чего ему будет предложено совершить платеж на адрес кошелька получателя.



(Рис. 2) Пример работы криптовалютного обменника WW-pay (платежная информация и QR код с адресом получателя)

* Важной деталью является то, что операции и транзакции проводятся не на самом сайте, а в сторонних сервисах. К примеру, сделка по продаже Bitcoin инициируется через обменник на одном компьютере, а подпись транзакции закрытым ключом осуществляется через криптовалютный кошелек на другом компьютере.
* В зависимости от политики сервиса, платеж пройдет только по нескольким подтверждениям транзакции в блокчейне. Обычно требуется от 1 до 4 подтверждений.
* Зачастую, при совершении сделки требуется указать контакты для связи: электронная почта, телефон. Это необходимо на случай внештатной ситуации: изменение курсов, задержки обработки, сбоев на сервере.

Как уже было сказано выше, закрытые ключи пользователя не контактируют с данными сервисами, и подпись транзакций осуществляется отдельным кошельком или сервисом. Главные риски для клиента при работе с обменниками заключаются в следующем:

1. Нет никаких гарантий, что в случае совершения транзакции по нужному адресу кошелька сервис выполнит свою часть сделки обмена.
2. Адрес кошелька получателя передается клиенту вместе с WEB страницей по протоколу htpps. Если сервера или интернет соединение скомпрометированы, то злоумышленники могут подменить адрес кошелька получателя, и после завершения транзакции валюта будет переведена злоумышленникам.

Подытожим. Криптовалютный обменник предназначен для обмена криптовалютных пар, для покупки/продажи криптовалют за фиатные деньги. Закрытые ключи пользователя не контактируют с данным типом сервисов, поэтому данный тип сервисов можно считать надежным с точки зрения сохранности закрытых ключей клиента. Однако остаются риски того, что получатель может не выполнить свою часть обмена, а также, что адрес получателя могут подменить.

### Криптовалютные биржи

Следующий тип криптовалютных сервисов — **криптовалютные биржи**. Криптобиржа является торговой платформой, позволяющей пользователям производить покупку и продажу, хранение и обмен криптовалют. Принцип функционирования таких площадок аналогичен валютным, товарным и фондовым биржам: цены определяются рынком, по принципу «предложение/спрос» для каждого токена. Криптобиржи бывают **централизованные** и **децентрализованные**.

#### Централизованные биржи

Начнем с централизованных. Централизация в данном случае означает, что пользователи доверяют свои средства третьей стороне, доверенному посреднику, при работе с любыми криптовалютными активами.

В некоторых странах централизованные криптобиржи регулируются государством, хотя и менее строго, нежели фиатные биржи. В связи с этим, централизованные биржи выставляют на торги лишь проверенные криптовалюты. Поэтому на таких биржах меньше вероятность наткнуться на мошенников.

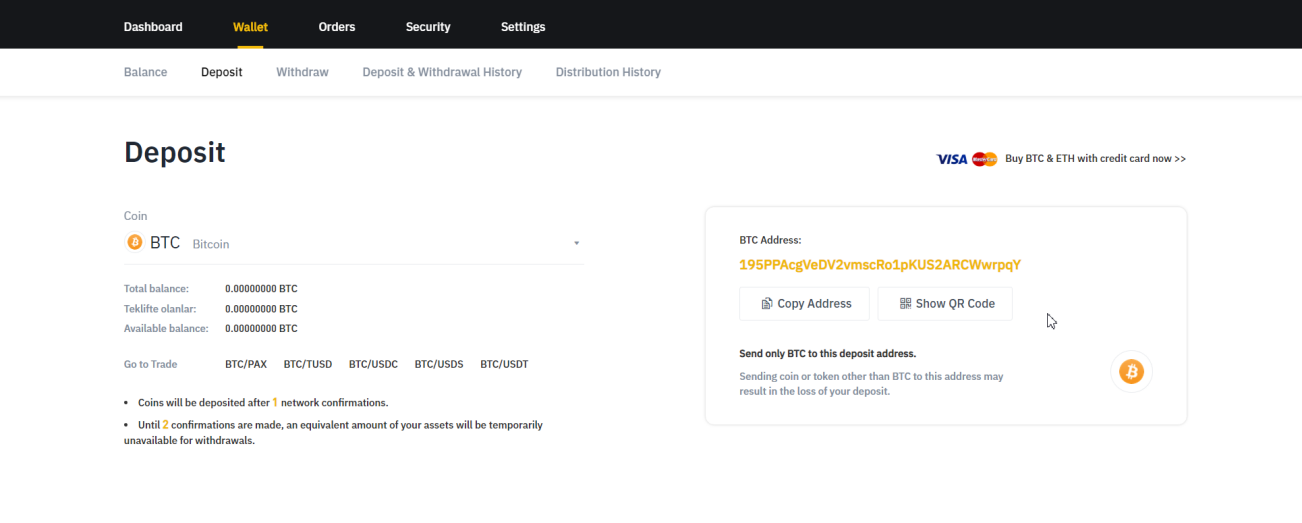
В ходе обследования были изучены 15 наиболее популярных криптовалютных централизованных бирж с наибольшим объемом торгов [7]:

1. Binance
2. EXMO
3. BTC-Alpha
4. Huobi
5. Kucoin
6. OKEx
7. LiveCoin
8. YoBit
9. Coinbase
10. HitBTC
11. Poloniex
12. Kraken
13. Bitfinex
14. Bittrex
15. CEX

Рассмотрим, как пользователь взаимодействует с централизованными криптобиржами.

Пользователь проходит регистрацию на сервисе, указывает телефон и почту. Если он хочет получить доступ ко всему функционалу биржи, то ему необходимо пройти полную процедуру KYC (know your customer) и указать свои паспортные и некоторые банковские данные. Авторизация на большинстве сервисов двухфакторная: ввод логина/пароля и смс кода. После авторизации пользователю открывается доступ к финансовым операциям.

Для начала работы необходимо пополнить баланс аккаунта. Это можно сделать, переведя фиатные деньги на банковский счет биржи и получив взамен криптовалюту на баланс аккаунта, а также с помощью стороннего криптовалютного кошелька, осуществив транзакцию по адресу кошелька, привязанного к аккаунту на бирже.



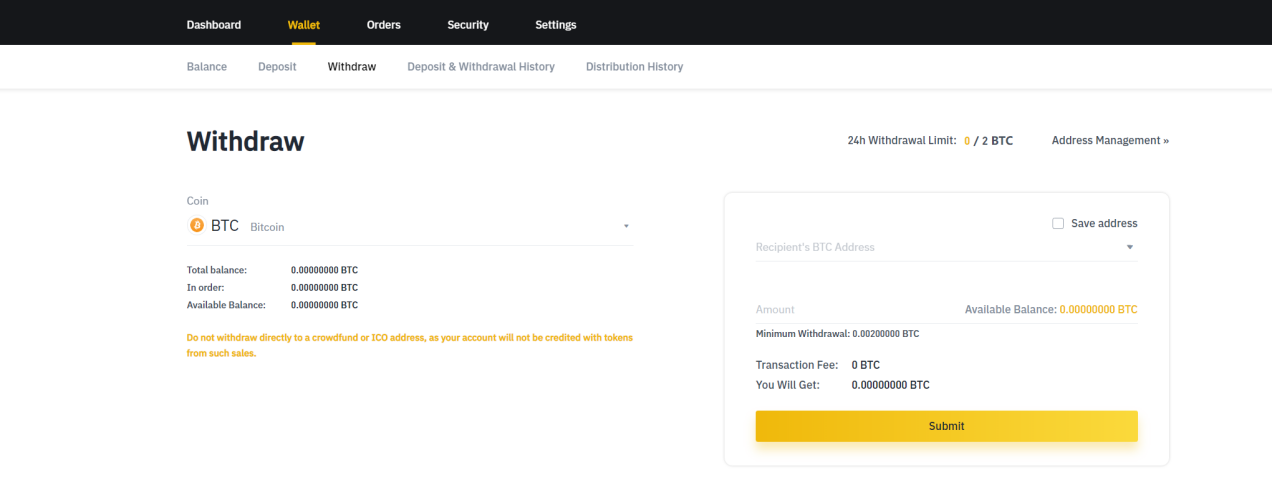
(Рис. 3) Пример работы централизованной криптовалютной биржи Binance (страница с адресом кошелька, привязанного к аккаунту клиента)

Адрес для перевода каждый раз разный, но все эти адреса принадлежат пользователю, так как генерация ключей для пользователей осуществляется биржей по протоколу иерархической генерации ключей BIP32 [8].

Суть этого протокола заключается в том, что все используемые ключевые пары порождаются из одного общего для всех ключей секрета. Особенность состоит в том, что есть возможность из одного секрета породить сколько угодно пар ключей для электронной подписи. Можно использовать новые адреса для каждого входящего платежа и сдачи, при этом все порожденные из основного секрета личные ключи, друг с другом никак не связаны, то есть нельзя проследить связь между порожденными адресами (определить, что все они принадлежат одному пользователю), а имея порожденный личный ключ, нельзя восстановить изначальный общий секрет. Все закрытые ключи хранятся в базе данных сервиса в зашифрованном виде.

Как и в случае классических бирж, пользователи доверяют свои капиталы криптобирже, и она хранит их, а точнее она хранит закрытые ключи клиентов. В этом заключается главный нюанс - у пользователя нет доступа к закрытому ключу из ключевой пары криптовалютного кошелька. Пользователь может видеть свой открытый ключ, но непосредственно подпись транзакций осуществляется на стороне сервиса.

На биржах существует возможность вывода криптовалютных средств на произвольный адрес криптовалютного кошелька, который вводится в соответствующее поле на сайте. Нужный адрес получателя передается сервису по протоколу https. Если сервера или интернет соединение скомпрометированы, то злоумышленники могут подменить адрес кошелька получателя, и после заверешения транзакции валюта будет переведена злоумышленникам.



(Рис. 4) Пример работы централизованной криптовалютной биржи Binance (страница вывода Bitcoin на произвольный адрес)

Несмотря на все меры безопасности, использование таких сервисов все равно является источником повышенного риска для пользователей.

Во-первых, авторизация по логину/паролю является надежной (логин и пароль можно подсмотреть, можно считать кейлогером, можно похитить с помощью фишинга и так далее). Доступ к закрытому ключу из ключевой пары осуществляется с помощью логина и пароля. Система является безопасной ровно настолько, насколько безопасен ее самый уязвимый элемент. Таким образом получается, что из-за уязвимости обычных паролей - уязвима вся система, и злоумышленник при краже паролей, получает доступ к закрытому ключу.

Во-вторых, генерация и хранение закрытых ключей не на стороне пользователя, а на стороне сервера - это грубое нарушение основ идеологии ассимитричной криптографии, нивелирующее все ее основные достоинства. Существует вероятность того, что сторона, осуществляющая хранение закрытых ключей, захочет осуществить несанкционированный доступ к этим ключам или дать этот доступ третьим лицам. Это дополнительный экономический риск.

В-третьих, из-за уязвимостей протокола https существует вероятность: 1) подмены адреса кошелька клиента при пополнении баланса аккаунта; 2) подмены адреса получателя при выводе криптовалюты с биржи.

В результате пользователь вынужден полагаться на то, что хакеры не украдут у него логин и пароль, не взломают базы данных с ключами; на то, что владельцы сервиса не захотят воспользоваться ключевой парой в своих корыстных целях. Возникает дополнительный риск потери своих денежных средств.

#### Децентрализованные биржи

Перейдем к децентрализованным криптовалютным биржам (DEX, decentralized exchange). Это биржи, которые работают на основе распределенного реестра, при этом не хранят закрытые ключи и персональные данные пользователей на своих серверах и выступают только платформой для поиска совпадений по заявкам на покупку или продажу активов пользователей.

DEX биржи стали развиваться относительно недавно, поэтому на рынке их не так много. В ходе обследования были изучены 10 наиболее популярных децентрализованных бирж [9]:

1. IDEX
2. Radar Relay
3. Kyber Network
4. Switcheo Network
5. Waves DEX
6. DEEX
7. Bisq Network
8. Airswap
9. Crypto Bridge
10. EtherDelta

Торговля на таких платформах происходит напрямую между участниками (peer-to-peer) без каких-либо финансовых посредников. Хоть биржи и используют свои собственные серверы для хранения данных о торгах и заявок на покупку/продажу активов пользователей, однако закрытые ключи при этом хранятся у самих пользователей. Таким образом DEX биржа устраняет необходимость в доверенном посреднике, и обеспечивают полную анонимность пользователя.

Большая часть DEX бирж имеют открытый исходный код, с которым можно ознакомиться на Git. Часть бирж для работы с собой предоставляет сайт или приложение, часть - только приложение (к примеру Bisq Network). Вариант с приложением, устанавливаемым на компьютер пользователя, является предпочтительным, так как в этом случае мы можем максимально контролировать процесс взаимодействия пользователя и сервиса.

Серверная часть DEX состоит из смарт-контракта, алгоритма для трейдинга и арбитра обработки транзакций. Смарт-контракт осуществляет хранение всех активов и выполнение всех транзакций. Если злоумышленники получат доступ к серверам, то они не смогу вывести средства из смарт-контрактов, если они не будут знать закрытых ключей пользователей. Поэтому хакерские атаки или закрытие самой биржи не приведут к потери средств клиентов.

Также у DEX биржи нет единой точки входа, через которую можно было бы получить доступ ко всем данным, что усложняет работу для взломщиков и делает саму атаку бессмысленной. Некоторые децентрализованные биржи, работающие с фиатными валютами, обязывают своих пользователей проходить процедуру KYC и поэтому хранят их персональные данные (но не закрытые ключи) на сервере.

Децентрализованные биржи работают по семейству протоколов «0x». В нем описывается принципы децентрализованного обмена валютой/токенами внутри смарт-контракта, а не внутри самого блокчейна [10]. Согласно этому протоколу, чтобы совершить сделку и записать ее в смарт контракт, оба участника обмена должны подписать транзакцию своими закрытыми ключами, при чем подпись осуществляется вне биржи, то есть на стороне пользователя (в браузере или в установленном приложении).

Каждая транзакция представляет собой пакет данных, содержащий параметры заказа и соответствующую подпись. Параметры транзакции конкатенируются и хэшируются до 32 байт с помощью функции Keccak SHA3. Инициатор заказа подписывает хэш заказа своим закрытым ключом для получения подписи ECDSA. Смарт-контракт может аутентифицировать подпись инициатора транзакции с помощью функции ecrecover, которая принимает на вход хэш транзакции и подпись хэша в качестве аргументов и возвращает открытый ключ кошелька, который произвел подпись. Если открытый ключ, возвращенный ecrecover, равен адресу заявленного отправителя, подпись является подлинной.

Процесс работы с DEX биржей выглядит следующим образом. При регистрации на сервисе, пользователю необходимо добавить адрес своего кошелька в смарт-контракт биржи. Для этого ему необходимо подписать транзакцию с помощью своего закрытого ключа. Подпись осуществляется либо приложением, либо скриптами внутри браузера. Есть несколько способов предъявить закрытый ключ:

1. Ввести информацию файла хранилища ключей
2. Ввести закрытый ключ, или seed фразу
3. Использовать для подписи браузерный плагин, обеспечивающий работу горячего кошелька (к примеру Metamask)
4. Использовать аппаратный холодный кошелек (к примеру Trezor)

Ключи по алгоритму «0х» не отправляются сервису, а отправляется только подписанная транзакция. Если, мы можем гарантировать целостность и корректную работу браузера, то 1 и 2 варианты - безопасны. Горячие кошельки не безопасны, поэтому третий вариант также небезопасен. При использовании аппаратных кошельков, закрытые ключи не покидают отчуждаемое устройство, и подпись осуществляется также на этом устройстве. Поэтому вариант 4 - также безопасен.

После чего необходимо пополнить баланс аккаунта на бирже. Клиент переводит криптовалюту/токены со своего кошелька на свой адрес внутри смарт-контракта. Для того чтобы пополнить баланс, вывести оттуда средства или совершить перевод на другой адрес, необходимо совершить подпись транзакции закрытым ключом пользователя. Эту транзакцию в неподписанном виде можно найти на бирже, или найти с помощью сервисов чтения блокчейна, и импортировать на компьютер пользователя, чтобы уже в доверенной среде осуществить подпись.

Подытожим. Криптовалютные биржи используются для купли-продажи, хранения и обмена криптовалют. Криптовалютные биржи бывают двух видов: централизованные и децентрализованные. Их сходства и различия рассмотрим в таблице 3.

Таблица 3.

Сравнение централизованных и децентрализованных криптовалютных бирж.

|  | **Централизованные биржи** | **Децентрализованные** |
| --- | --- | --- |
| **Где хранятся ключи?** | Закрытые ключи генерируются и хранятся на сервере. | Закрытые ключи генерируются и хранятся у пользователя. |
| **Где подписываются транзакции?** | Транзакции подписываются на стороне сервера. | Транзакции подписываются на стороне клиента. |
| **Можно ли отслеживать транзакции?** | Все данные транзакций скрыты от пользователей и доступны только серверу. | Все транзакции публичные, и их можно отслеживать через сервисы сканирования блокчейна. |
| **Есть ли доступ к исходному коду биржи?** | Закрытый исходный код у всех бирж. | Открытый исходный код у большей части бирж. |
| **Анонимность** | При регистрации за частую необходимо указывать свои персональные данные. | Полная анонимность. На большей части сервисов регистрация осуществляется только с помощью ключевой пары. |
| **Взлом или блокировка активов пользователя** | Аккаунт пользователя может быть заблокировать или взломан. В этом случае средства будут безвовзратно утеряны. | Аккаунт невозможно заблокировать или взломать на серверной стороне. |
| **Гарантии выполнения сделок.** | Надежность сделок гарантируется только самой биржей. Возможны ситуации, в которых один из контрагентов не выполнит свою часть сделки. | Все сделки фиксируются в смарт-контрактах. Поэтому обе стороны гарантировано выполнят свою часть сделки. |

### Боты-трейдеры

Следующий вид сервисов предназначен для пользователей, которые не хотят или не могут торговать сами. **Боты-трейдеры** - программы,созданные для автоматической торговли криптовалютой. Бот может представлять собой приложение, установленное на компьютере клиента, или алгоритм, запущенный на сайте, то есть облачно. Облачные боты бывают реализованы внутри самой биржи, или же на отдельном сервисе. Боты бывают и для централизованных, и для децентрализованных бирж.

В ходе обследования были изучены 11 наиболее популярных ботов трейдеров [11]:

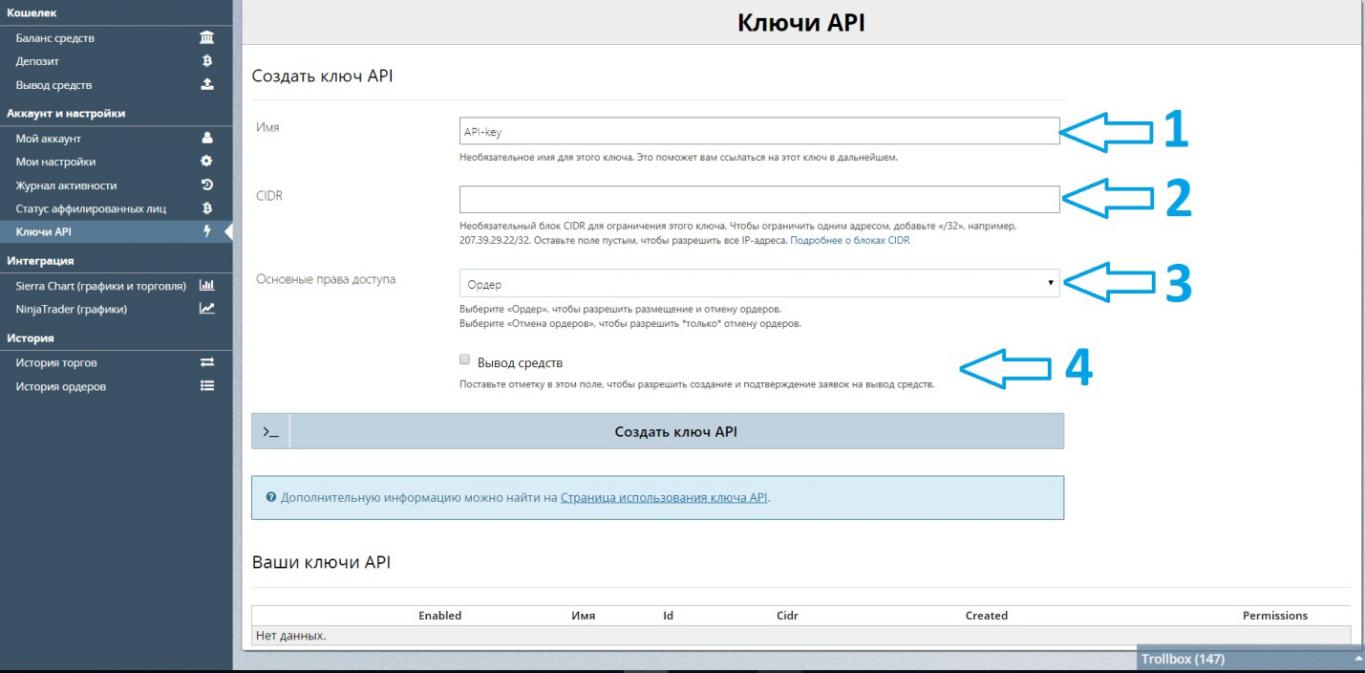
1. Centobot
2. Gekko (приложение для ПК)
3. Cap.Club
4. Zenbot (приложение для ПК)
5. RevenueBot
6. Crypto Trader
7. BTC Robot
8. Gunbot (приложение для ПК)
9. Leonardo
10. HaasOnline
11. PHP Trader (приложение для ПК)

Боты работают по алгоритмам, торговым стратегиям, которые, в свою очередь, создаются на основе технического анализа закономерностей. Для анализа требуются исторические данные об изменениях курса за продолжительный период. После определения закономерностей ведётся проверка стратегии на тех же исторических данных, подсчитывается потенциальные убытки и прибыли. Если результаты устраивают, на их основе создаются правила торговой стратегии робота для биржи криптовалют. Некоторые боты дополнительно используют индикаторы, которые позволяют анализировать текущую ситуацию на рынке, другие выполняются только при возникновении определённых рыночных условий.

Есть два наиболее распространённых вида ботов:

* Биржевой: он действует на определенной торговой площадке. Заработок основывается на разнице цен при купле продаже.
* Арбитражный: он действует на двух и более торговых площадках. Заработок основывается на разнице курсов между ними.

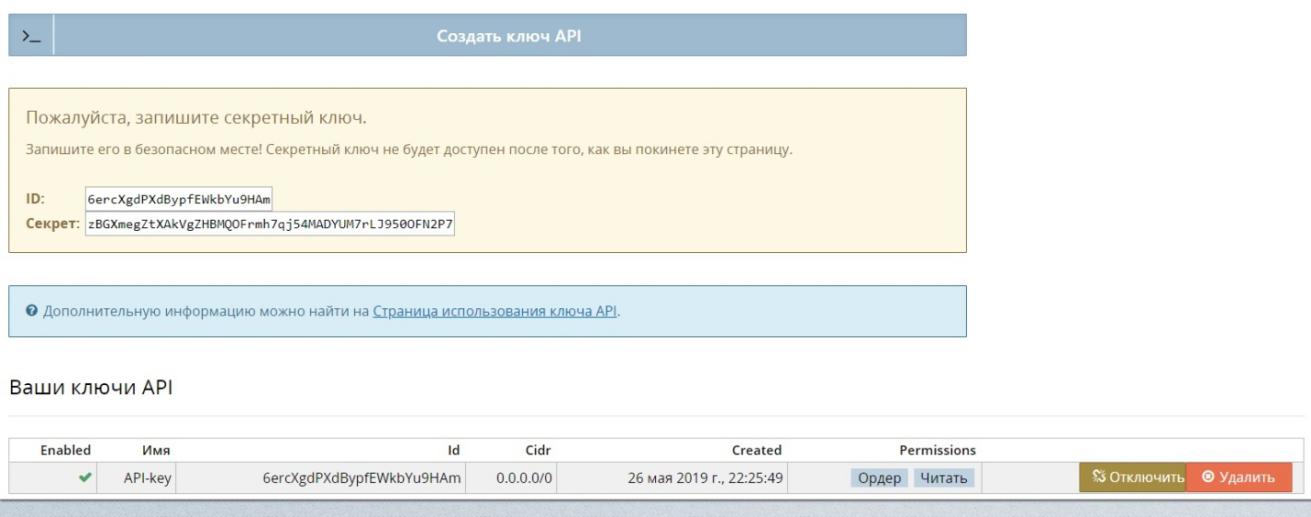
Для выполнения торговых операций на биржах боты трейдеры используют торговые API (application programming interface), открытый набор функций, предлагаемых биржей для использования в сторонних приложениях [12]. Для того, чтобы передать свою криптовалюту в дистанционное управление при помощи API, необходимо создать API-ключ на любой бирже, которая это поддерживает.

  
 (Рис. 9) Пример работы централизованной криптовалютной биржи Bitmax (страница создания API ключей)

Рассмотрим процесс создания API ключей:

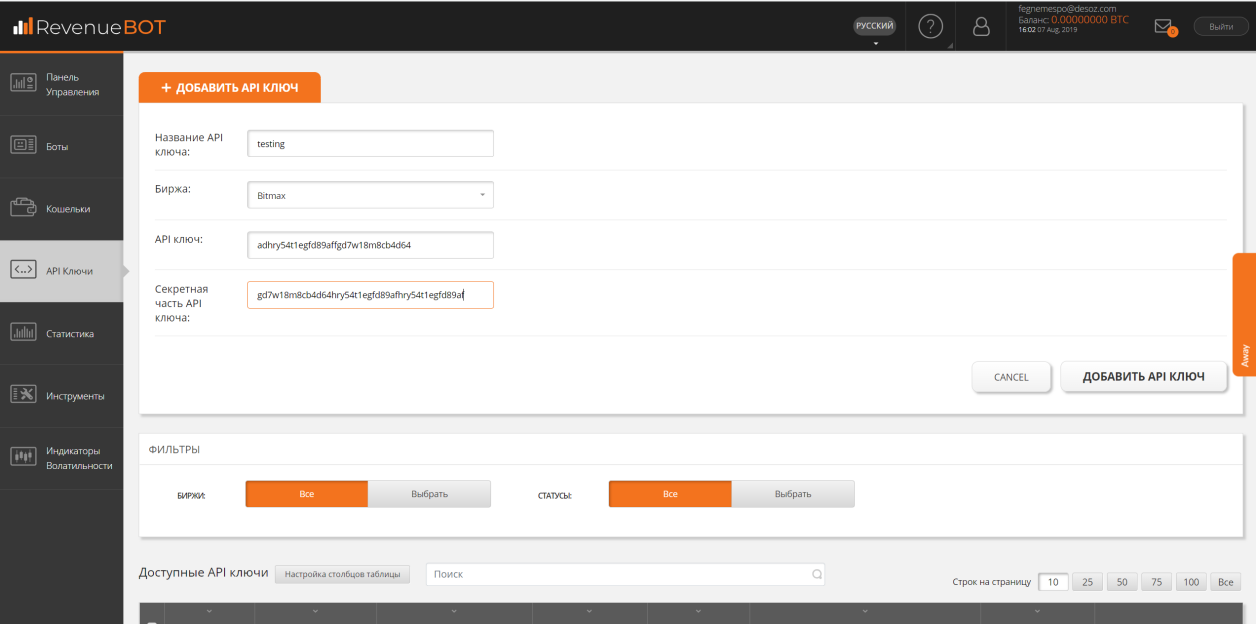
1. Поле «Имя»: имя для ключа. Оно необходимо для удобства, чтобы не запутаться в ключах, если их много.
2. Поле «CIDR»: поле на случай, если клиент решил ограничить доступ по ключу только для определенных IP-адресов. При пустом поле разрешены все IP-адреса.
3. «Основные права доступа»: в этом поле устанавливаются права на перечень сделок, которые может совершать бот.
4. «Вывод средств»: это поле определяет права трейдера, работающего через API, на вывод криптовалюты с клиентского счета.

Ключевая пара создается на стороне сервиса. У пользователя в любой момент есть возможность отключить ее работу, к примеру в случае, если бот, осуществляющий торговлю, начнет вести себя некорректно или подозрительно.



(Рис. 10) Пример работы централизованной криптовалютной биржи Bitmax (страница управления API ключами)

Полученную ключевую пару необходимо ввести в сервис бот трейдинга.



(Рис. 11) Пример работы сервиса бот-трейдинга RevenueBOT (страница ввода API ключей)

Если использовать бота, в виде проверенного ПО, установленного в доверенной среде, то мы можем быть уверены, что бот будет делать именно то, что в нем заложено. Во всех остальных случаях - отдавать криптовалюту на доверенное управлению боту, означает подвергать себя дополнительному риску. Потому что нет никакой гарантии, что бот, расположенный в облаке, вдруг не начнет действовать в интересах сервиса или хакеров. Механизмом отключения API ключей можно просто не успеть воспользоваться. Кроме того, этот механизм так же располагается в облаке, поэтому нет гарантии, что злоумышленники не смогут поменять права API ключей, или выключить/выключить их.

Подытожим. Боты трейдеры - это класс сервисов, предназначенных для автоматической торговли криптовалютными активами на биржах. Некоторые биржи имеют встроенных ботов. Для осуществления дистанционной автоматической торговли на остальных биржах, необходимо предоставить стороннему бот сервису API ключи, которые генерируются биржей. Если биржа устанавливается на ПК пользователя, то ключи генерируются на стороне клиента.

### Майнинг пулы

Что такое майниг уже было рассказано выше. Майнить можно в одиночку, для этого лишь необходимо установить приложение и в настройках указать адрес кошелька, на который будет поступать награда. Однако на момент написания данной работы процесс майнинга является крайне энергозатратным и требовательным к железу, которое быстро изнашивается. Из-за этого майнить самому - экономически не выгодно.

Поэтому майнеры объединяются в майниг пулы. **Майнинг пул** – это сервер, который делит большую задачу по вычислению подписи блока  на маленькие задачи и раздает их подключенным устройствам.

В ходе обследования были изучены 10 наиболее популярных ботов трейдеров [13]:

1. MinerGate
2. Kryptex
3. NiceHash
4. F2pool
5. AntPool
6. ZPool
7. 2Miners
8. Batpool
9. BitClub Network
10. Coinmine

Вклад в общую работу каждого майнера, участвующего в пуле, оценивается с помощью «шар» (от английского «share»). «Шара» – небольшая часть работы по поиску решения хеш-функции для подписания блока, которая выдается пулом майнеру. Собирая шары от майнеров, сервер пула проверяет их валидность. Как только какая-то «шара» удовлетворяет текущим значениям сложности, сервер пула объявляет о подписании блока. После этого пул получает награду за блок и распределяет между майнерами пропорционально количеству переданных «шар» независимо от того, была ли среди них подписавшая блок [14] .

С технической точки зрения для клиента процесс майнинга в пуле выглядит следующим образом: пользователь устанавливает майнер (к примеру Ethminer), и в настройках указывает информацию, необходимую для подключения к пулу. Там же он указывает адрес своего кошелька, на который будет переводиться награда.

При работе с майнинг пулами закрытые ключи пользователя не используются, однако:

* для майнинга внутри майнинг пула необходимо постоянное соединение с интернетом, что значительно повышает риск компрометации системы;
* для получения значимой прибыли, система должна обладать значительными вычислительными мощностями. Чем больше вычислительная мощность, тем универсальнее система, тем сложнее ее защищать. В случае несанкционированного доступа к системе, злоумышленник может использовать вычислительные мощности для перебора паролей или каких-либо других криптографических атак.

Поэтому, в данной работе будем считать работу с данным видом сервисов не безопасным для клиента.

Существует еще одна модель майнинга - **облачный майнинг**. Если в предыдущей модели вычисления велись на стороне клиентов, а сервер лишь выполнял роль координатора, то в облачной модели все вычисления на себя берет сервер, а клиент лишь платит за аренду вычислительных мощностей.

В ходе работы были изучены 8 наиболее популярных сервисов облачного майнинга:

1. IQ Mining
2. BitDeer
3. Hashing24
4. Hashflare
5. Genesis Mining
6. AlienCloud
7. Nuvoo Mining
8. CCG Mining

Главный минус такой схемы - у пользователя нет доступа к ключевой паре, которая генерируется и хранится на стороне сервиса. Соответственно данный вариант сервисов является рискованным по тем же самым причинам, что и в случае централизованных бирж.

Подытожим. Майнинг, и аналогичные ему процессы, является источником всей существующей криптовалюты. Майнить можно:

* самому, что безопасно, но экономически не выгодно;
* с помощью майнинг пула, в этом случае закрытые ключи никак не задействованы;
* с помощью облачного майнинга, в этом случае у пользователя нет доступа к закрытым ключам.

### Перечень потенциально опасных и безопасных сервисов

Подытожим информацию по всем подразделам.

Таблица 2

Сервисы для работы с криптовалютными активами.

| **Тип сервиса** | | | **Описание** | **Безопасность ключей** |
| --- | --- | --- | --- | --- |
| Кошельки | | Горячие | Кошельки, для работы которых необходим интернет. | Ключи могут храниться на сервере или на стороне клиента. При хранении на компьютере клиента, постоянное соединение с интернетом повышает риски компрометации ключей. |
| Холодные | Кошельки, работающие без доступа в интернет. | Если ключи хранятся в доверенной среде без включенного интернета, то им ничего не угрожает. |
| Обменник | | | Сайт, который используют для обмена валюты, покупки и продажи валюты за фиатные деньги. | Закрытый ключ криптовалютного кошелька не используется на сервисе, и транзакция осуществляется сторонними средствами. |
| Биржа | Централизованная | | Выступает в роли третьей доверенной стороны. Используется для купли-продажи, хранения и обмена криптовалют. Хранит все данные пользователей на своих серверах. | Закрытые ключи генерируются и хранятся на стороне сервиса. Пользователь имеет доступ только к открытому ключу. |
| Децентрализованная | | Выступает в роли площадки для агрегации запросов на сделки. Используется для купли-продажи, хранения и обмена криптовалют. Не сохраняет каких либо данных пользователей. | Сервис позволяет использовать собственно сгенерированные ключевые пары. |
| Бот трейдер | Сторонний | | Предназначен для автоматической торговли криптовалютными активами на биржах. Все торговые процессы инициируются на стороне сервиса. | Для осуществления дистанционной автоматической торговли на биржах, необходимо предоставить бот сервису API ключи от аккаунта клиента на бирже. Эти ключи и сам бот располагаются в облаке. |
| Установленный на стороне клиента | | Предназначен для автоматической торговли криптовалютными активами на биржах. Все торговые процессы инициируются на стороне клиента. | Для осуществления дистанционной автоматической торговли на биржах, необходимо предоставить бот сервису API ключи от аккаунта клиента на бирже. Бот установлен на компьютере пользователя |
| Майнинг сервис | Самостоятельный | | Решение задачи алгоритма консенсуса с помощью приложения для получения награды . | Для получения награды в сеть передается лишь открытый ключ. |
| С помощью пула | | Решение определенной доли от задачи алгоритма консенсуса. Доля назначается сервисом. | Для получения награды в сеть передается лишь открытый ключ. |
| Облачный | | Майнинг осуществляется сторонним сервисом. | Генерация и хранение ключей происходит на стороне сервиса. У пользователя нет доступа к ним. |

Разделим вышеописанные сервисы на потенциально опасные и безопасные.

Подробно уязвимости и недостатки потенциально опасных для клиента сервисов были расписаны в предыдущих разделах. С такими сервисами нежелательно вести работу. Перечислим их:

* «горячие» кошельки;
* централизованные биржи;
* бот трейдеры, запущенные не на стороне клиента;
* сервисы облачного майнига;
* майнинг пулы.

Если ключевая пара генерируется или хранится третьей стороной, то существует риск того что эта сторона может сохранить себе копию ключей и в будущем без ведома клиента несанкционированно совершить какую-либо транзакцию. Подпись транзакции третьей стороной, подразумевает передачу закрытого ключа этой стороне, что также подразумевает риск несанкционированного копирования ключа.

Поэтому безопасный сервис, должен удовлетворять как минимум следующим требованиям:

* Для работы с сервисом клиент использует самостоятельно сгенерированную ключевую пару.
* Закрытый ключ хранится только на стороне клиента.
* Подпись транзакций осуществляется также на стороне клиента.

На основе этого, перечислим безопасные для работы сервисы управления криптовалютными активами:

* «холодные» кошельки;
* обменники;
* децентрализованные биржи;
* бот трейдеры, запущенные на стороне клиента.

# Программно-аппаратная реализация объекта

## Общие сведения о реализации объекта

Как уже было сказано выше, клиент при работе с сервисами должен использовать самостоятельно сгенерированную ключевую пару, и хранить ее. Поэтому ПАК должен обеспечивать генерацию и хранение ключевых пар. Для генерации целесообразно применять протоколы BIP32, BIP39, BIP43, BIP44, которые обеспечивают иерархически детерминированную генерацию ключей для мультивалютного кошелька. Целесообразность этого была доказана в [15]. Как именно обеспечить хранение ключей будет рассмотрено ниже.

Для взаимодействия с блокчейном (чтение, скачивание, отправление подписанных транзакций) и подписи транзакции необходим средство выполняющее функциональность криптовалютного кошелька. В качестве такого средства целесообразно использовать кошелек Electrum [15].

При работе с сервисами управления криптовалютными активами мы не можем гарантировать безопасность интернет соединения, корректность работы серверов и целостность ПО, установленного на них. Поэтому все данные, передаваемые через сеть, и все операции, совершаемые на стороне сервера, сопряжены с риском для клиента.

Часть сервисов предоставляет возможность установки приложений на компьютер пользователя (к примеру боты трейдеры или приложения для взаимодействия с DEX биржами). Если выбирать, как взаимодействовать с сервисом: через браузер или через официальное приложение, устанавливаемое на компьютер пользователя, то для минимизации риска целесообразно выбрать второй вариант. В этом случае ПО, обеспечивающее функциональность сервиса, работает на стороне клиента, благодаря чему появляется возможность контролировать целостность этого ПО и корректность его работы.

Если у сервиса есть только сайт, и нет приложения, то им можно пользоваться при условии, что он удовлетворяет требованиям безопасного сервиса, обозначенным выше.

## Реализация доверенной среды

Доверенная вычислительная среда – это фрагмент среды электронного взаимодействия, для которого установлена и поддерживается в течение заданного интервала времени целостность объектов и целостность взаимосвязей между ними [16].

В недоверенной среде возможно осуществление множества различных атак: перехват управления, перехват информации на портах ввода и вывода, работа под гипервизором злоумышленников, копирование ключей из оперативной памяти и так далее.

Также в недоверенной среде возможна атака, в которой злоумышленник осуществляет подмену транзакции при передаче ее на подпись в токен с неизвлекаемыми ключами (для хранения криптовалютных ключей используются токены Trezor и Ledger Nano S). Из-за этого пользователь видит на экране монитора одну информацию, а на подпись отправляется другая, предоставленная злоумышленником.

Поэтому ПАК управления криптовалютными активами должен обеспечивать доверенную среду. Только в этом случае, закрытые ключи будут защищены от утраты, а подписываться будут только санкционированные пользователем транзакции.

В качестве средства, обеспечивающего функционирование доверенной среды будем использовать MKT-card long, микрокомпьютер с динамически изменяемой архитектурой, запатентованной под названием «Новая Гарвардская»[17]. МКТ – это устройство, обладающее специальной подсистемой управления доступом к памяти: память устройства, в которой расположена ОС, находится в режиме Read Only (только для чтения), что исключает возможность несанкционированных модификаций критичного программного обеспечения и обеспечивает неизменность доверенной среды функционирования. Кроме того МКТ обладает блоками сеансовой памяти, что дает возможность исполнения программ, для корректной работы которых необходима возможность записи.

Перечисленные выше ключевые особенности МКТ позволяют решить несколько вопросов при работе с криптовалютными активами:

1. Офлайн подпись транзакций: если в качестве офлайн компьютера использовать МКТ в Read Only режиме, то можно гарантировать, что даже при попадании вредоносного ПО в систему, оно не сможет исполниться, и таким образом транзакция не будет скомпрометирована.
2. Использование U2F токенов для подписи транзакций: используя защищенную ОС МКТ в качестве доверенной среды, мы можем быть уверены, что на входе и выходе устройства будет именно та транзакция, которая нам нужна

## Генерация ключевых пар

Протокол BIP32 (Hierarchical Deterministic Wallets) отвечает за генерацию мастер ключа, и генерацию иерархически детерминированных ключей из этого мастер ключа.

В официальном репозитории биткойна существует несколько реализаций этого протокола на различных языках программирования [18]. Эти реализации используются в большинстве из существующих криптовалютных кошельков и сервисов. Рассмотрим, какие функции отвечают за генерацию закрытых мастер ключей в наиболее часто используемых реализациях:

* Python
  + - Реализация в PyCoin:  
       private\_key = os.urandom(32).encode('hex')
    - Реализация в BIP32Utils:   
      private\_key = ''.join(['%x' % random.randrange(16) for x in range(0, 64)])
* Java
  + - Реализация bitsofproof:  
      SecretKey key = new SecretKeySpec (chainCode, "HmacSHA512");
* C++
  + - pkey = EC\_KEY\_new\_by\_curve\_name(NID\_secp256k1)  
      Эта функция взята из стандартной библиотеки openssl
* JavaScript
  + - Реализация Bitpay  
      var priv\_key = new ECKey(conv(privateKeyHex, {in: 'hex', out: 'buffer'}), false);

Все эти функции объединяет то, что закрытый мастер ключ генерируется из стандартных библиотек, которые обращаются к генератору псевдослучайных чисел (ГПСЧ). Таким образом,можно повлиять на генерацию мастер ключа (а значит и на генерацию всех дочерних ключей) с помощью атаки на ГПСЧ[19].

Перечислим потенциальные программная атаки на ГПСЧ:

* Прямая криптографическая атака основанная на анализе выходных данных алгоритма.
* Атаки, основанные на входных данных, могут быть разделены на атаки с известными входными данными, атаки с воспроизводимыми входными данными.
* Атаки, основанные на вскрытии внутреннего состояния при которых злоумышленник знает начальное или исходное состояние генератора.
* Закладки в программное обеспечение, при которых создатель алгоритма знает любое из хэшированных псевдослучайных чисел и последующие в цепочке. Такой алгоритм сложно определить со стороны, так как числа выглядят равномерно распределенными по всему диапазону.

Этих атак можно избежать, если вместо псевдослучайных чисел использовать случайные числа, которые можно генерировать с помощью аппаратного датчика, выступающего в роли физического генератора случайных чисел. Таким образом, чтобы минимизировать риски компрометации ключей, в ПАК для генерации случайных чисел вместо ГПСЧ необходимо использовать физический источник случайных чисел. В существующих реализациях MKT-card long нет имплементированного аппаратного датчика случайных чисел. Такой датчик необходимо имплементировать в ПАК. Как именно это можно сделать будет рассмотрено ниже.

## Хранение ключевых пар при длительном подключении к интернету

Если мы хотим сократить риски, контакт с сетью нужно минимизировать. Однако в случае, если пользователь хочет торговать на бирже (самостоятельно или с помощью бота), то возникает необходимость длительного подключения к интернету. Из-за этого возрастает риск компрометации ключей. При биржевой торговле часто роль играют лишние минуты и даже секунды при совершении сделок, поэтому использовать для высокочастотной торговли схему с офлайн подписью транзакций не целесообразно.

Есть несколько способов разрешения этого противоречия:

1. Использовать один и тот же ПАК и для холодного хранения больших сумм криптовалюты и для высокочастотной торговли на биржах неразумно. Поэтому целесообразно использовать два устройства: первое использовать для холодного хранения большей части активов, а второй для хранения небольшого количества криптовалюты для оперативных расходов и торговли на биржах.
2. Для минимизации риска компрометации закрытых ключей целесообразно вынести функционал генерации и хранения ключей (а также функционал подписи) в отдельный аппаратный модуль. Ключи в этом модуле должны быть неизвлекаемыми, и все операции (шифрование, хеширование, подпись данных) выполняются также внутри модуля. К примеру, в качестве такого модуля в аппаратном кошельке Ledger Nano S используется микроконтроллер ST31H320, соответствующий банковским стандартам безопасности согласно общим критериям уровня EAL6+[20].

Подытожим. Высокочастотная биржевая торговля подразумевает продолжительно включенный интернет - это повышенный риск. Если пользователь не готов его принять, то ему следует выбрать вариант исключительно холодного хранения, в котором транзакции (и обычные, и для DEX бирж) совершаются редко и с другого компьютера (офлайн подпись транзакций).

Если клиент готов принять такой риск, то ему следует держать на устройстве (которое по сути выступает в роли «горячего» кошелька) только ключи от кошельков, с малым количество валюты для оперативных расходов. Если вынести функционал генерации, хранения и криптографических операций в отдельное аппаратное криптоядро, то это снизит риски компрометации ключей пользователя.

В [15] было показано, что для обеспечения безопасного холодного хранения на платформе МКТ использование аппаратного криптоядра не является обязательным. Однако проектируемый ПАК должен быть универсальным, то есть подходить сразу двум вышеописанным типам клиентов, поэтому аппаратное криптоядро должно входить в состав ПАК в обоих случаях.

Имплементацию ядра в ПАК можно сделать двумя способами: либо модифицировать архитектуру МКТ, интегрировав в нее криптоядро, либо использовать отчуждаемое криптоядро. Считаю второй вариант целесообразным по нескольким причинам:

1. Отчуждаемое устройство с криптоядром, обеспечивающим генерацию и хранение криптовалютных ключей, а также осуществляющее подпись транзакций, по определению является холодным аппаратным кошельком. Хранение ключей в холодном кошельке, отдельно от устройства, подключенного к сети, позволит дополнительно снизить риски компрометации ключей.
2. В случае, если злоумышленник получит доступ к МКТ,не получив доступ к отчуждаемому устройству, он не получит доступ ни к ключам, ни к возможности подписывать транзакции.
3. Модификация архитектуры микрокопьютера подразумевает разработку новой архитектуры, написание ПО для имплементируемого модуля, написание ПО для взаимодействия модуля с остальной системой. Проектирование, тестирование, отладка, учет программных, логических и аппаратных нюансов при разработке - это гораздо более трудозатратный, времязатратный и дорогой процесс.

Поэтому использование отчуждаемого устройства с имплементированным криптоядром, в совокупности с МКТ, выступающим в качестве доверенной вычислительной среды, позволит дополнительно снизить риски компрометации ключей.

## Выбор отчуждаемого устройства

На рынке существуют несколько аппаратных холодных кошельков. Наиболее популярные и проверенные из них - Trezor и Ledger Nano S. У каждого из кошельков есть свое десктопное приложение, устанавливаемое на ПК. С помощью такого приложения пользователь может управлять своими активами: создавать ключи, подписывать импортируемые транзакции, просматривать свои запасы криптовалют и так далее. Для подписи неимпортируемых транзакций в браузере, в браузер необходимо установить официальный плагин от разработчиков, который осуществляет взаимодействие браузера и отчуждаемого кошелька.

Оба кошелька являются хорошим, но дорогим решением (Trezor стоит 110 долларов, а Ledger - 70 долларов). Данные устройства являются зарубежными разработками, и на российском рынке отечественных аналогов пока нет. Если такой аналог разработать, и при этом он будет более дешевым, сохраняя надежность и функциональность, то разработчик сможет занять пустующую рыночную нишу. Увеличение заработка входит в интересы заказчика данной работы, поэтому считаю вариант разработки собственного аппаратного криптовалютного кошелька целесообразным.

Для экономии сил и ресурсов целесообразно не разрабатывать аппаратную платформу для отчуждаемого устройства с нуля, а взять существующее решение и перепрошить его. В качестве такой платформы предлагается использовать ПСКЗИ ШИПКА [21] по следующим причинам:

* Устройство снабжено программно-аппаратным криптоядром в виде микропроцессора.
* Устройство снабжено аппаратным датчиком случайных чисел (ДСЧ);
* В устройстве аппаратно реализовано 10 наиболее часто используемых зарубежных криптографических алгоритмов [22]. При написании криптографических алгоритмов для работы с криптовалютами это поможет сэкономить время на разработку и отладку.
* Устройство стоит в разы дешевле, чем зарубежные аналоги.
* Заказчик работы является разработчиком и владельцем прав на данное устройство. Поэтому разработка и дальнейшая продажа конечного продукта не будет сопряжено с дополнительными юридически - правовыми или экономическими взаимодействиями с другими контрагентами.

Для ПСКЗИ ШИПКА необходимо разработать ПО, обеспечивающее иерархически детерминированную генерацию ключей на стороне отчуждаемого устройства. Также необходимо разработать десктопное приложение для взаимодействия с устройством, и браузерный плагин для подписи транзакций.

## Требования к системе

Подытожим предыдущие разделы и перейдем к составлению функциональных, аппаратных и программных требований к проектируемому комплексу.

ПАК управления криптовалютными активами должен удовлетворять следующим требованиям:

**Функциональные**

Система должна обеспечивать возможность выполнения следующих функций:

* генерация иерархически детерминированных мультивалютных ключевых пар согласно протоколам BIP32 и BIP44;
* восстановление ключей по seed фразе согласно протоколу BIP39;
* защищенное хранение закрытых ключей;
* подпись транзакций;
* взаимодействие с блокчейном (чтение, скачивание, отправление подписанных транзакций);
* обеспечение доступа в интернет, работы интернет браузера для взаимодействия с сервисами;
* обеспечение доверенной среды исполнения, защищенной от вредоносных программ и гарантирующей конфиденциальность, доступность и целостность данных;
* предоставление пользователю возможности работать с заранее установленными приложениями для управления криптовалютными активами (криптовалютные кошельки, клиенты DEX бирж, боты-трейдеры). Перечень установленного ПО должен определяться на этапе настройки устройства.

**Программные**

* Операционная система - Linux, так как данное семейство ОС предоставляет возможность более гибкой настройки системы на всех уровнях;
* Криптовалютные кошельки - Electrum для Bitcoin и Mist для Etherium по умолчанию, остальные мультивалютные кошельки или кошельки для альткойнов устанавливаются при необходимости на этапе настройки устройства;
* Клиенты для DEX бирж - устанавливаются при необходимости на этапе настройки устройства;
* Боты трейдеры - устанавливаются при необходимости на этапе настройки устройства;
* Интернет браузер - Firefox, Chrome, как два наиболее распространенных и популярных браузера;
* Набор ПО необходимый для работы с документами - Libre office, популярный open source офисный пакет;
* Инструментарий для аудита - auditd, auditctl, autrace ausearch,  aureport. Классический пакет для аудита в системах семейства Linux;
* Прошивка отчуждаемого устройства должна быть реализована для аппаратной платформы ПСКЗИ ШИПКА;
  + - Прошивка должна обеспечивать функционал генерации, хранения, восстановления ключей.
    - Прошивка должна обеспечивать функционал подписи транзакций.
* ПО для взаимодействия с отчуждаемым устройством, состоящее из двух компонентов:
  + - Клиентское приложение должно обеспечивать законченный оконный пользовательский интерфейс для проведения криптоопераций:
      * Создание ключевых пар;
      * Восстановление ключей по мнемонической фразе;
      * Просмотр используемых открытых ключей и балансов на них;
      * Подпись транзакций;
    - Плагин для браузера, который позволяет подписывать транзакции, в случае, если с сервисом можно взаимодействовать только через браузер;

**Аппаратные**

* В качестве вычислительного устройства должен выступать MKT-card long.
* Генерация и хранение ключей, а также криптографические операции должны выполняться в отдельном аппаратном отчуждаемом устройстве ПСКЗИ ШИПКА.
  + - Закрытые ключи должны создаваться в этом ядре с применением аппаратного датчика, выступающего в роли физического источника случайных чисел.
    - Реализация на аппаратном уровне криптографических алгоритмов, необходимых для работы с криптовалютами (ECDSA, SHA, KECCAK и так далее)
    - Энергонезависимый блок памяти для хранения ключевой информации.

Разработанные в ходе обследования требования являются основой для реализации ПО, состоящего из двух компонентов: прошивки для отчуждаемого устройства и ПО для взаимодействия с отчуждаемым устройством.

# Инструментарий для разработки

Для разработки прошивки отчуждаемого устройства и внутрисхемной отладки кода предлагается использовать среду разработки Keil uVision, в связи предоставления следующего функционала:

* Средства автоматической компиляции, ассемблирования и компоновки проекта, которые предназначены для создания исполняемого (загрузочного) модуля программы. При этом между файлами автоматически генерируются новые ассемблерные и компиляторные связи, которые в дальнейшем позволяют обрабатывать только те файлы, в которых произошли изменения или файлы, находящиеся в зависимости от изменённых.
* Отладчик-симулятор, отлаживающий работу скомпилированной программы на виртуальной модели микропроцессора, моделирующей работу ядра контроллера и его периферийного оборудования: портов ввода-вывода, таймеров, контроллеров прерываний.

Для реализации прошивки отчуждаемого устройства предлагается использовать язык программирования Си стандарта ISO/IEC 9899, как язык, позволяющий наиболее эффективно управлять памятью и временем работы программы.

Для разработки клиентского приложения для взаимодействия с отчуждаемым устройством предлагается использовать среду разработки QT Creator в связи предоставления следующего функционала, не реализованного в полном объеме в других средах разработки:

* Поддержка встроенного дебаггера для отладки кода;
* Интеграция графического конструктора оконного интерфейса.

Для разработки плагина для браузера предлагается использовать XULRunner, платформу для разработки плагинов, и NPAPI, набор API, позволяющий создавать плагины для Firefox, Chrome, Safari,

Производителем для работы с MKT-card long рекомендуется 64-битная ОС Ubuntu 14.04. Поэтому ПО для взаимодействия с отчуждаемым устройством должно функционировать в 64-битной операционной системе Ubuntu 14.04. Для реализации этого предлагается производить разработку, отладку и сборку также в этой операционной системе для предотвращения кросс-платформенных конфликтов.

В качестве программной реализации хэш-функции и алгоритмов формирования и проверки ЭП предлагается использовать библиотеку OpenSSL [23], которая представлена в виде проекта с открытым исходным кодом, поэтому есть возможность исследовать реализацию криптографических механизмов.

Таким образом для разработки предлагается использовать следующий инструментарий:

* ОС - Ubuntu 14.04.
* Для разработки прошивки отчуждаемого устройства:
  + - Среда разработки Keil uVision для разработки прошивки микроконтроллера и внутрисхемной отладки кода.
    - Язык программирования Си стандарта ISO/IEC 9899.
* Для разработки клиентского приложения для взаимодействия с отчуждаемым устройством:
  + - Язык программирования QT версии 5.13.
    - Среда разработки QT - QT Creator.
* Для разработки плагина использовать платформу XULRunner.
* Библиотека OpenSSL в качестве реализации криптографических механизмов.

# Заключение

В ходе данного обследования были изучены существующие виды сервисов управления криптовалютными активами, среди них были выделены те, с которыми оптимально вести работу с точки зрения безопасности. Также был составлен перечень защитных мер, необходимых для безопасного управления криптовалютными активами на базе платформы МКТ.

Результатом обследования являются:

* Перечень инструментов для разработки ПО;
* Проект технического задания на разработку ПО (Приложение №1).

# Приложение 1. Техническое задание

1. **Наименование**

Темой работы является «Разработка защищенного программно-аппаратного комплекса управления экономическими активами на базе платформы МКТ».

1. **Основание для разработки**

Основанием для разработки является задание на дипломный проект, подписанное консультантами и руководителем дипломного проекта и утвержденное заведующим кафедрой защиты информации МФТИ.

1. **Исполнитель**

Студент 419 группы ФРТК МФТИ Шарапов Р. А.

1. **Цель работы**

Разработать программно аппаратный комплекс управления криптовалютными активами на базе MKT-card long.

1. **Назначение комплекса**

Система предназначена для защищенного хранения криптовалютных ключей и выполнения криптографических операций во время высокочастостной биржевой торговли.

1. **Требования к комплексу**
   1. Требования к аппаратному составу:

* Микрокопьютер MKT-card long в качестве платформы, обеспечивающей доверенную среду;
* ПСКЗИ ШИПКА в качестве отчуждаемого носителя ключей;
  1. Требования к составу программных компонентов:
* Прошивка отчуждаемого носителя ключей для устройства, аппаратной платформой которого является ПСКЗИ ШИПКА;
* ПО для клиентского приложения для взаимодействия с отчуждаемым устройством;
  1. Требования к функциональным характеристикам:

Система должна обеспечивать возможность выполнения следующих функций.

* + 1. Генерация иерархически детерминированных мультивалютных ключевых пар согласно протоколам BIP32 и BIP44.
    2. Восстановление ключи по seed фразе согласно протоколу BIP39.
    3. Осуществление процедуры подписи, хэширования, шифрования и расшифрования.
    4. Обеспечение графического интерфейса для пользователя
  1. Требования к надежности.
     1. Ключи должны быть неизвлекаемы из устройтсва.
     2. Ключи должны генерироваться с применением физического датчика случайных чисел.
  2. Требования к интеграции и совместимости.
     1. Система должна работать в 64-битной операционной системе Linux Ubuntu 14.04.
     2. ПО для работы аппаратного модуля должно быть написано на языке программирования Си стандарта ISO/IEC 9899.
     3. Графический интерфейс и ПО для клиентского приложения для взаимодействия с отчуждаемым устройством должны быть написаны на языке программирования QT версии 5.13.
     4. Плагин должен быть написан с применением NPAPI.

**Требования к программной документации**

Состав документации определяется по ГОСТ 34.201-89 и включает в себя:

1. Ведомость проекта;
2. Пояснительная записка к техническому проекту;
3. Программа и методика испытаний (ПМИ);
4. Описание программного обеспечения;
5. Техническое задание (ТЗ);
6. Схема структурная комплекса технических средств;
7. Схема функциональной структуры;
8. Ведомость эксплуатационных документов;
9. Руководство пользователя;
10. Инструкция по эксплуатации КТС;
11. Технологическая инструкция

**Этапы разработки**

Разработка макета и ПО представляет собой совокупность работ, упорядоченных во времени, взаимосвязанных и объединенных в один этап.

| № | Название этапа | Срок | Отчетность |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| 1. | **Конструкторская часть** |  | **Макет, ПО и комплект документации** |
| 1.1. | Проектирование: разработка структуры ПО и проектирование компонентов. | До 1.10.19 | Описание автоматизируемых функций;  Общее описание системы. |
| 1.2. | Реализация: кодирование, тестирование и отладка программных компонентов и системы в целом. | До 1.12.19 | ПО (исходные коды в git репозитории, инструкцию по сборке проекта), включающее:   * ПО для отчуждаемого устройства * ПО для взаимодействия с отчуждаемым устройством |
| 1.3. | Документирование. | До 1.12.19 | Комплект сопровождающей (программной и эксплуатационной) документации. |
| 1.3.1. | Создание комплекта документации. | До 1.12.19 | 1.Ведомость проекта;  2.Пояснительная записка к эскизному проекту;  3.Программа и методика испытаний (ПМИ);  4.Описание программного обеспечения;  5.Техническое задание (ТЗ);  6.Схема структурная комплекса технических средств;  7.Схема функциональной структуры;  8.Ведомость эксплуатационных документов;  9.Руководство пользователя;  10.Инструкция по эксплуатации КТС;  11.Технологическая инструкция |
| 1.3.2. | Согласование ПМИ главным инженером базовой организации А.В. Кузнецовым | До 1.12.19 | Согласованная ПМИ. |
| 1.4. | Подготовка к испытаниям и испытание макета ПО: создание стенда. | До 1.12.19 | Испытательный стенд на технических средствах кафедры. |
| 2. | **Исследовательская часть.** |  | **Пояснительная записка.** |
| 2.1. | Оценка предполагаемого качества функционирования. | 1.12.19 | Модель и результаты моделирования. |
| 2.2. | Тестирование. | 1.12.19 | Раздел в пояснительной записке. |
| 2.3. | При необходимости – устранение недостатков, выявленных в ходе тестирования. | 1.12.19 | Раздел в пояснительной записке. |
| 2.4. | Оформление результатов проектирования в расчетно-пояснительную записку. | 1.12.19 | Пояснительная записка. |

**Порядок приема работы**

Прием результатов работы осуществляется путем проведения испытаний макета ПО на специально созданном испытательном стенде на технических средствах кафедры комиссией, созданной и утвержденной заместителем заведующего кафедрой.

Испытательный стенд создается Исполнителем.

На испытания Исполнитель предоставляет:

* Согласованное ТЗ;
* Согласованную ПМИ;
* Комплект документов согласно ТЗ.

**Требования к документированию**

Виды, комплектность и обозначения документов должны соответствовать требованиям ГОСТ 34.201-89. Оформление текстовых документов должно осуществляться в соответствии с требованиями ГОСТ 2.105-95 (с Изменением №1 от июня 2006 г.), ГОСТ 2.106-96 (с Изменением №1 от июня 2006 г.).

Документы должны быть представлены Исполнителем Заказчику в печатном виде в 2-х экземплярах и в электронном в виде в формате MS Word/MS Excel/MS Visio на машинном носителе в 1-ом экземпляре.

# Перечень принятых сокращений

|  |  |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| ВрПО | Вредоносное программное обеспечение |
| НСД | Несанкционированный доступ |
| ОС | Операционная система |
| ПАК | Программно-аппаратный комплекс |
| ПК | Персональный компьютер |
| ПО | Программное обеспечение |
| ПСКЗИ | Персональное средство криптографической защиты информации |
| СКЗИ | Средство криптографической защиты информации |
| ЭП | Электронная подпись |

# Термины и определения

**Блокчейн** — это последовательный набор блоков, каждый следующий блок в котором включает в качестве хэшируемой информации значение хэш-функции от предыдущего блока.

**Доверенная среда** – система, использующая аппаратные и программные средства для обеспечения одновременной обработки информации разной категории секретности группой пользователей без нарушения прав доступа.

**Криптовалюта** – вид цифрового финансового актива, создаваемый и учитываемый в распределенном реестре цифровых транзакций участниками этого реестра в соответствии с правилами ведения реестра цифровых транзакций.

**Криптографическая система с открытым ключом** – система асимметричного шифрования или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ.

**Несанкционированный доступ к информации (НСД)** – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

**Смарт-контракт** – договор в электронной форме, исполнение прав и обязательств по которому осуществляется путем совершения в автоматическом порядке цифровых транзакций в распределенном реестре цифровых транзакций в строго определенной им последовательности и при наступлении определенных им обстоятельств. Защита прав  участников (сторон) смарт-контракта осуществляется в  порядке, аналогичном порядку осуществления защиты прав сторон договора, заключенного в электронной форме.

**Токен** – вид цифрового финансового актива, который выпускается юридическим лицом или индивидуальным предпринимателем (далее – эмитент) с целью привлечения финансирования и учитывается в реестре цифровых записей.

**Узел сети** – устройство, соединённое с другими устройствами как часть компьютерной сети.

**Цифровая транзакция** – действие или последовательность действий, направленных на создание, выпуск, обращение цифровых финансовых активов.

**Цифровая запись** – информация о цифровых финансовых активах, зафиксированная в реестре цифровых транзакций.

# Список используемых источников

1. Bitcoin in a nutshell — Mining [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://habr.com/ru/post/320178/>
2. A Next-Generation Smart Contract and Decentralized Application Platform [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://github.com/Ethereum/wiki/wiki/White-Paper>
3. ERC-20 Token Standard [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://eips.ethereum.org/EIPS/eip-20>
4. Токен [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://ru.wikipedia.org/wiki/Токен_(криптовалюта)>
5. Cold storage [Электронный ресурс] /. — Электрон. текстовые дан. — Режим доступа: <https://en.bitcoinwiki.org/wiki/Cold_storage>, свободный
6. Обзор криптовалютных онлайн-обменников [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://miningbitcoinguide.com/trading/market/obmenniki-kriptovalyut#___2019>
7. ТОП-15 лучших криптобирж на 2019 год [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://mining-cryptocurrency.ru/rejting-luchshie-birzhi-kriptovalyut-2017/#-15__2019>
8. bip-0032 [Электронный ресурс] /. — Электрон. текстовые дан. — Режим доступа: <https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki>, свободный
9. Топ децентрализованных криптовалютных бирж (DEX) [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://happycoin.club/top-8-detsentralizovannyih-kriptovalyutnyih-birzh-dex/>
10. «0x» protocol: Detailed review on the project [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://medium.com/paradigm-fund/0x-protocol-detailed-review-on-the-project-5913f363805e>
11. ТОП-10 лучших ботов для автоматической торговли криптовалютами в 2019 году [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://mining-cryptocurrency.ru/bot-dlya-torgovli-kriptovalyutoj-na-birzhe/#i-6>
12. Доверительное управление на биржах криптовалют через API [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://bitexpert.io/news/du-via-api/>
13. ТОП-10: лучшие пулы для майнинга [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://bisnesideya.ru/coins/top-10-luchshie-puly-dlya-majninga.html>
14. Что такое майнинг пул и как он работает [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://investor100.ru/chto-takoe-majning-pul-i-kak-on-rabotaet/>
15. Разработка холодного мультивалютного кошелька на платформе МКТ: НИР / Шарапов Р.А. - Москва: Московский физико-технический институт, 2018. - 64 с.
16. В.А. Конявский, Основы понимания феномена электронного обмена информацией / В.А. Гадасин. - Минск: 2004.
17. Компьютер с «вирусным иммунитетом» [Электронный ресурс] /. — Режим доступа: <http://www.okbsapr.ru/konyavskiy_2015_2.html>, свободный
18. bip-0032 [Электронный ресурс] /. — Электрон. текстовые дан. — Режим доступа: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki, свободный
19. Встраиваем бэкдор в Bitcoin (ECDSA) [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://habr.com/ru/post/248419/>
20. Hardware Wallet Vulnerabilities [Электронный ресурс] /. — Электрон. журн. — Режим доступа: <https://blog.gridplus.io/hardware-wallet-vulnerabilities-f20688361b88>
21. Конявская, С.В. ПСКЗИ ШИПКА: решение разных типов задач [Электронный ресурс] / С.В. Конявская. — Электрон. журн. — Режим доступа: http://www.okbsapr.ru/konyavskaya\_2007\_9.html
22. Конявская, С.В. ПСКЗИ ШИПКА: просто интеллектуальное устройство [Электронный ресурс] / С.В. Конявская. — Электрон. журн. — Режим доступа: http://www.okbsapr.ru/ksv\_shipka.html
23. OpenSSL [Электронный ресурс]. <https://www.openssl.org> (дата обрщения: 18.05.2019);