Общее описание программного обеспечения “Блокчейн-платформа IZZZIO версия 1.2.0”

ООО “Изио”

Москва, 2020

Содержание документа:

1. Введение

Данный документ содержит общую информацию о программном комплексе “Блокчейн-платформа IZZZIO версия 1.2.0”.

2. Общие сведения о блокчейн-платформе IZZZIO версия 1.2.0

Технология распределенных реестров – это новый подход к хранению, передаче и обработке любых данных, который помогает значительно оптимизировать бизнес-процессы.

Блокчейн является базой данных, представляющей из себя выстроенную по определенным правилам цепочку блоков (распределенный реестр), где каждый участник системы ведет обновление данных независимо от других участников системы и хранит у себя копию реестра. Цепочка блоков выстраивается на основе алгоритма консенсуса, который математически гарантирует невозможность подделки данных. Все данные, которые поступают в распределенный реестр являются доверенными, а все изменения - прозрачными.

Основные преимущества технологии блокчейн:

- отсутствие единого центра управления и посредников;
- прозрачность;
- неизменность данных;
- неограниченность;
- надежность системы защиты данных.

Блокчейн-платформа IZZZIO версия 1.2.0 (далее – блокчейн-платформа IZZZIO, Платформа IZZZIO, Система, ПО) - это программный комплекс, предназначенный для хранения, передачи и обработки любых данных, а также, для автоматизации бизнес-процессов с помощью применения технологии распределенного реестра.

В основе платформы лежит идея создания блокчейн экосистемы, максимально приближенной к потребностям бизнеса, облегчающая интеграцию и использование технологии блокчейн в бизнес-процессах компаний.

Блокчейн-платформа IZZZIO - это универсальная блокчейн платформа для реализации любых задач.

Исходный код платформы открыт и доступен по лицензии Apache-2.0. Использование частей или всего кода платформы в любом из проектов требует публикации исходного кода этих проектов любым доступным способом.

Преимущества использования блокчейн-платформы IZZZIO:

- Надежная защита и целостность данных.
- Оптимизация бизнес-процессов.
- Интеграция в бизнес-процессы блокчейн-технологий позволяет сократить расходы на реализацию всех процессов, путем автоматизации большинства операций и сокращения расходов на администрирование системы.
- Прозрачность всех данных и действий участников системы.
- Непрерывный доступ из любой точки мира.
- Отказоустойчивость системы.

Основные сущности Системы:

Блокчейн-сеть (далее - сеть, цепочка блоков) – выстроенная по определенным правилам цепочка блоков, копия которой хранится у каждого участника.

Консенсус - алгоритм защищающий сеть от атаки, и обеспечивающий выбор и добавление блоков в цепочку.

Транзакция - запись каких либо данных в распределенный реестр. Каждая транзакция должна быть подписана цифровой подписью. Также возможно использовать механизм Квалифицированной электронной подписи для обеспечения юридической значимости в сети. Транзакции группируются в блоки, которые последовательно добавляются в сеть в виде списка.

Блок - хранилище транзакций, из которых складывается цепочка блоков.

Основные виды цепочек блоков:
Публичная - распределенная база данных, доступная для просмотра любому участнику.
Приватная - распределенная база данных, которая имеет ограничения по чтению и записи информации.

Токен - выражение какого-либо цифрового актива в рамках Системы.

Смарт-контракт - программа, обеспечивающая создание и выполнение договора.

Цифровая подпись - криптографический метод доказательства достоверности данных.

Узел сети (участник сети, адресат, нода) - точка (компьютер или сервер), подключенная к распределенному реестру, в которой данные могут созданы, получены или переданы.

Block Explorer - инструмент для просмотра содержимого блокчейн сети.

Основные характеристики сети блокчейн-платформы IZZZIO:

- **Стоимость транзакций**: транзакции в сети бесплатны, но существует также возможность настройки “платных” транзакций за счет каких-либо ресурсов в рамках системы.

- **Скорость транзакций**: производительность некоторых сетей на базе блокчейн-платформы IZZZIO достигает более 50 000 транзакций в секунду на среднестатистическом компьютере и более 100 000 транзакций в секунду на специальном оборудовании.

- **Размер блока**: 15 Мегабайт и более

На базе исходного кода блокчейн-платформы IZZZIO можно реализовывать как публичные, так и приватные сети.

Прочие характеристики и особенности блокчейн-платформы IZZZIO

- Используемый язык программирования - JavaScript.
- Система состоит из модульных компонентов.
- Тьюринг полные смарт-контракты с возможностью взаимодействия с оффчейн-системами.
- Возможность реализации блокчейн-сетей на базе исходного кода блокчейн-платформы IZZZIO для любых задач, с соответствующими настройками сети.
- Отсутствие необходимости в больших вычислительных ресурсах.
- Поддержка контрактов без привязки к токенам, возможность описания бизнес логики внутри контракта
- Легкая интеграция блокчейн-сети в любую систему благодаря простому API.
- Безопасная среда выполнения умных контрактов с проверкой целостности данных.
- Надежное хранение данных с многократным децентрализованным резервированием.

Цели применения Системы:

- повышение доверия между участниками различных систем;

- обеспечение прозрачности истории действий в различных процессах;
- оптимизация процессов за счет автоматизации действий и минимизации посредников;
- подтверждение достоверности данных и действий участников;
- надежная защита данных в системе и обеспечение безопасного обмена данными между участниками.

Выгоды от внедрения Системы:

- экономия ресурсов при реализации бизнес-процессов;
- сокращение расходов на реализацию бизнес-процессов;
- 100% доверие к данным системы;
- ускорение процессов;
- минимизация рисков.

Сферы применения Системы:

- финансовый сектор
- юридические услуги
- здравоохранение
- государственное управление
- производство
- грузоперевозки
- образование
- энергетика
- страхование
- информационная безопасность
- интернет вещей (IoT)

и другие.

Возможности и варианты реализации систем для бизнеса и государственных учреждения на базе блокчейн-платформы IZZZIO:

- Системы хранения и архивации любых данных в распределенном хранилище.
- Программы лояльности, системы накопления баллов, с произвольными правилами поведения.
- Электронный документооборот с многократным распределенным резервированием документов и операций.
- Системы подтверждения владения, проверки цифровых подписей, отпечатков данных, идентификационных карт, паспортов и других документов.
- Анонимные приватные компьютерные сети, а также надежные и безопасные сети передачи данных.
- Надежные и безопасные сети для интернета вещей (IoT), робототехники, в средах без постоянного подключения между участниками сети, наподобие Mesh-сетей.

- Автоматически выполняемые контракты с возможностью интеграции с оффлайн и онлайн проверками
- Контракты-голосования
- Автоматические договора с указанием условий выполнения и проверкой внешних ресурсов.

и другие.

3. Технические особенности блокчейн-платформы IZZZIO версия 1.2.0

3.1. Функциональные модульные компоненты

Блокчейн-платформа IZZZIO состоит из функциональных модульных компонентов и позволяет конфигурировать сети под любые задачи и требования сценариев использования.

Дистрибутив Системы включает:

1) Основные функциональные модули блокчейн-платформы IZZZIO версия 1.2.0:

- Модули алгоритмов консенсуса LCPoA, DLCPoA, Proof-of-Authority

- Модуль выполнения смарт-контрактов

- Модуль работы с криптографией и методами конвертации публичных ключей в различные форматы
    - хеширование;
    - цифровая подпись данных;
    - проверка цифровой подписи;
    - конвертация hex-ключа в PEM-формат;
    - конвертация PEM-ключа в hex-формат.

2) Подключаемый модуль базовой криптографии SHA256 + ECDSA-SHA2
3) Подключаемый модуль организации шифрованных соединений по протоколу Диффи-Хеллмана

Дополнительные подключаемые модули не входящие в дистрибутив:

1) Подключаемый модуль криптографии на основе bitcore-lib
2) Подключаемый модуль ГОСТ криптографии на основе WebCrypto GOST Library
3) Подключаемый модуль ГОСТ криптографии на основе КриптоПро CSP 4.0
4) Подключаемый модуль ГОСТ криптографии на основе VipNet CSP 4.2

Блокчейн-платформа предоставляет пользователям большое количество настраиваемых возможностей.

3.2. Блокчейн-сеть

Основной механизм хранения информации в блокчейн-платформе IZZZIO - ее хранение в виде направленной цепи блоков данных со следующими свойствами:

- каждый последующий блок криптографически зацеплен с предыдущим блоком;
- цепь распределенного реестра не может иметь ветвлений.

Обработка информации в Системе происходит в сети, представляющей собой совокупность узлов (участников сети), взаимодействующих между собой.

При генерации блока участник помещает в блок данные – транзакцию (блок содержит строго одну транзакцию).

Основная цепочка состоит из JSON блоков со структурой

- Хеш текущего блока
- Хеш предыдущего блока
- Цифровая подпись (опционально)
- Порядковый номер блока
- Время начала генерации блока
- Время окончания генерации блока
- Данные блока

Цепочка блоков сохраняется в виде строк с использованием порядкового номера как ключа в базе LevelDB или в хранилище в ОЗУ.

Доступ участников к сети происходит с использованием сторонних приложений-клиентов, взаимодействующих с внешним API узла сети а также с помощью внешних децентрализованных приложений (DApp).

3.3. Техническая сводка

Способ подтверждения блоков	**Базово:** Своя разработка основанная на гибридном PoW + PoA способе - Limited Confidence Proof of Activity с привязкой подтверждения по времени **Дополнительно:** DLCPoA - Dynamic Limited Confidence Proof of Activity, Proof-of-Authority **Возможен любой другой, подключаемый с помощью системы плагинов**

Программная платформа	Node.js > 12
Хеширование	Фильтрованный SHA256 / ГОСТ Р 34.11-2012 / любой вид, предоставляемый плагином
Цифровые подписи	ECDSA-SHA-256 / ГОСТ Р 34.10-2012 / любой вид, предоставляемый плагином
Криптопровайдер	Встроенный / VipNet CSP 4.2 / предоставляемые плагином
Структура основной цепи блоков	JSON блоки с произвольным содержимым
База данных	LevelDB, Sqlite3, Memory
Смарт-контракты	ECMAScript 6 (JS ES6), тьюринг полные, с расширенным функционалом, WASM, поддержка других языков с помощью плагинов
Сетевой p2p интерфейс	WebSocket, DNS Discovery
API	REST / PHP Class / REPL

3.4. Алгоритмы консенсуса

Платформа IZZZIO поддерживает два основных алгоритма консенсуса: Limited Confidence Proof of Activity (LCPoA) и Dynamic LCPoA (DLCPoA), а также, дополнительные.

LCPoA (Limited Confidence Proof-of-Activity, рус. Доказательство активности с ограниченным доверием) - гибридный алгоритм консенсуса сети блокчейн, состоящий из двух технических элементов:

- Proof-of-Activity (рус. “Доказательство активности”) - принцип, основанный на решении задачи, схожей с задачей принципа Proof-of-Work, но с пониженной сложностью;
- Limited Confidence (рус. "Ограничение доверия") - система автоматического создания “контрольных точек” в сети блокчейн, достигается за счет введения жесткого порога возможности перезаписи блоков.

DLCPoA (Dynamic Limited Confidence Proof-of-Activity, рус. Динамическое доказательство активности с ограниченным доверием) - это алгоритм консенсуса, позволяющий регулировать скорость сети, является модифицированной версией LCPoA с динамической сложностью.

Безопасность самой сети блокчейна и консенсус обеспечивается за счет механизма “зоны ограниченного доверия” с автоматическим созданием контрольных точек, а также с проверкой времени генерации блока и сверкой общего времени сети.
В любой момент времени возможна перепроверка затраченного на генерацию блока времени за счёт константного минимального времени генерации блока.

3.5. WebSocket

WebSocket - это протокол связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером в режиме реального времени. Протокол WebSocket очень распространён, и имеет имплементации во многих языках программирования а также во всех современных браузерах.

Благодаря использованию WebSocket как основного способа взаимодействия с сетью существует возможность писать полностью браузерные клиенты сети блокчейн-платформы IZZZIO.

3.6. Плагины

Плагины - внешние модули, расширяющие функционал узла сети. Плагины инициализируются во время загрузки узла, предоставляя дополнительный функционал во время работы:

1. Внешние криптопровайдеры
2. Расширение функционала смарт контрактов EcmaContracts
3. Дополнительные алгоритмы консенсуса

3.7. DApp

Децентрализованные приложения в IZZZIO позволяют создавать добавочный функционал для узлов. Такие приложения имеют широкий функционал:
1. Взаимодействие с цепочкой блоков, предобработка, реакция на изменения цепочки
2. Взаимодействие со смарт контрактами, в том числе запуск новых
3. Взаимодействие с другими децентрализованными приложениями посредством встроенных протколов StarWave, StarWaveCrypto
4. Интеграция централизованных приложений с децентрализованным.

Для написания децентрализованных приложений в IZZZIO используется класс DApp. Класс предоставляет все необходимые методы для работы с функционалом сети, и обеспечивает совместимость приложений с разными версиями узлов блокчейна IZZZIO.

3.8. Смарт-контракты

Блокчейн-платформа IZZZIO поддерживает смарт-контракты написанные на JavaScript ES6, которые выполняются в изолированной виртуальной машине. Контракты могут использовать функционал основного и второстепенных цепочек и токенов.
Основные характеристики смарт-контрактов блокчейн-платформы IZZZIO:

- JavaScript ES6. Поддержка работы со случайными числами (Math.random) и временем (Date)
- События
- Взаимодействие с другими контрактами в сети
- Поддержка объектов больших чисел (BigNumber) для безопасных расчетов данных, в том числе токенов
- Встроенные итерируемые и не итерируемые структуры данных: KeyValue, BlockchainArraySafe, BlockchainArray, TokenRegister, BlockchainMap
- Встроенный функционал рекомендуемых контрактов.

3.9. Протокол обмена данными (Starwave)

StarWave - внутренняя подсистема передачи сообщений в сети состоящий из узлов IZZZIO, не связанная с цепочкой блоков. Протокол StarWave позволяет передавать данные от одного узла другому без организации прямого подключения между узлами.

При этом маршрут доставки сообщения будет сформирован при первой попытке отправки сообщения динамически. При изменении маршрута, система перестраивает подключения автоматически.

Протокол поддерживает передачу широковещательных и персональных сообщений. Сообщения могут быть открытыми, открытыми с криптографической подписью, и шифрованными. Шифрованный канал организован с помощью обмена ключами по протоколу Диффи-Хеллмана (DH) между участниками соединения.

Механизм передачи данных схож с функционалом широковещательных сообщений протокола UDP, и не обеспечивает информацию о статусах доставки сообщений.

Для каждого узла создается внутренний адрес, состоящий из случайной последовательности символов алфавита и цифр. Эти адреса используются для автоматической коммутации сообщений, передаваемых с помощью протокола StarWave.

Каждый узел сети сохраняет информацию об адресах подключенных узлов, что позволяет составлять карту узлов, необходимых для быстрой передачи сообщения (маршруты).

При первой передаче сообщения от одного узла другому, сообщение рассылается всем доступным узлам, при условии, что не существует прямого подключения между узлами. Когда сообщение доходит до адресата, построенный маршрут прохождения

сообщения сохраняется. Все последующие сообщения передаются с указанием маршрута, что позволяет передавать их с минимальными задержками.

В случае нарушения маршрута, и недоступности узлов из списка, маршрут перестраивается заново с последнего доступного узла, что позволяет передавать сообщения даже при постоянном изменении топологии сети.

Сообщения не передаются, если время жизни сообщения превысило заданное отправителем или предельно пороговое из конфигурационного файла.

3.10. Работа в браузерах без расширений и плагинов

Поскольку блокчейн-платформа IZZZIO использует для обмена информацией протокол WebSocket, существует возможность работать с блокчейн-сетью напрямую, доступными инструментами браузера. Для этого разработан специальный скрипт с открытым исходным кодом - Candy.

Candy - инструмент, позволяющий создавать web-приложения, полноценно использующие блокчейн-платформу IZZZIO.

Использование блокчейна для хранения и загрузки любой информации позволяет равномерно распределять нагрузку между нодами, в связи с чем блокчейн-платформа IZZZIO может использоваться как распределитель нагрузки, и защищать от DDoS атак.

3.11. Внешний API узла сети

Программное обеспечение узла блокчейн-платформы IZZZIO предоставляет внешний интерфейс программирования приложений (API). Внешний API может быть использован для подключения сторонних приложений-клиентов к узлу сети, используемых участниками для доступа к сети.

Внешний API имеет архитектуру REST, в качестве транспортного протокола используется HTTP, представление данных – в формате JSON.

Внешний API узла содержит вызовы, имеющие следующую функциональность:

- получение информации об узле распределенного реестра: перечень активных функций узла, конфигурационные параметры, версия программного обеспечения;
- получение информации о других узлах сети;
- получение информации из журнала событий;
- получение информации о блоках распределенного реестра;
- получение информации о смарт-контрактах и результатах их выполнения;
- создание новых транзакций/блоков

4. Требования к программной и аппаратной платформам

ПО узла распределенного реестра блокчейн-платформы IZZZIO функционирует на (П)ЭВМ аппаратной платформы x86 или x86_64, работающей под управлением одной из следующих ОС:

- Windows 7/8/8.1/Server 2008 (x86, x64);
- Windows Server 2008 R2/2012/2012 R2 (x64);
- CentOS 6/7 (x86, x64);
- ТД ОС АИС ФССП России (GosLinux) (x86, x64);
- Red OS (x86, x64);
- Fedora 19/20 (x86, x64);
- Mandriva Enterprise Server 5, Business Server 1 (x86, x64);
- Oracle Linux 6/7 (x86, x64);
- OpenSUSE 13.2, Leap 42 (x86, x64);
- SUSE Linux Enterprise Server 11SP4/12, Desktop 12 (x86, x64);
- Red Hat Enterprise Linux 6/7 (x86, x64);
- Ubuntu 14.04/14.10 (x86, x64);
- Linux Mint 15/16/17 (x86, x64);
- Debian 8 (x86, x64);
- Astra Linux Special Edition (x86-64)
- ALT Linux 7 (x86, x64);
- ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64);
- РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);
- FreeBSD 9, pfSense 2.x (x86, x64);
- Mac OS X (Darwin) от версии 10.6.

Для работы ПО узла распределенного реестра требуется интерпретатор JavaScript Node.js версии 12

Для хранения данных используются библиотеки (и модули Node.js доступа к ним):

- LevelDB - хранилище типа ключ-значение;
- sqlite3 - встраиваемая СУБД реляционной модели.

Минимальные аппаратные требования к аппаратной части (П)ЭВМ для работы ПО узла распределенного реестра:

- Центральный процессор - тактовая частота 1.5 ГГц;
- ОЗУ - 512 Мб.
- Свободное пространство на жестком диске: 1 Гб для размещения программных компонентов, дополнительное пространство для размещения обрабатываемых данных (хранилища блоков цепи, локальных данных смарт-контрактов, журнала событий).

5. Дистрибутив и установка

Общие сведения о дистрибутиве
В программный комплекс IZZZIO входит:

1. Дистрибутив и исходный код узла
2. Модуль базовой криптографии
3. Модуль передачи сообщений StarWave
4. Модуль шифрованной передачи сообщений StarWaveCrypto
5. Модули консенсусов LCPoA, DLCPoA, Proof-of-Authority
6. Классы для работы с API на языке PHP
7. Документация

Подготовка к установке

Установите NodeJS версии 12 и выше. Для установки версии 12 на Debian/Ubuntu можно воспользоваться официальным репозиторием:
$ sudo apt update
$ sudo apt -y install curl dirmngr apt-transport-https lsb-release ca-certificates
$ curl -sL https://deb.nodesource.com/setup_12.x | sudo bash

Установка узла

С помощью NPM
Один из вариантов установки репозитория узла с помощью пакетного менеджера NPM.

$ npm install -g iz3node@1.2.0

Для корректной установки может понадобится установленный набор компиляторов g++/VC++ 2015.3 v14.00(v140)
Установить необходимы комплект библиотек для сборк можно с помощью команды
$ npm install --global --production windows-build-tools

Потом следуя инструкции:

1. Панель управления - Программы и компоненты - Изменить: Microsoft Visual Studio Installer
2. Найдите Visual Studio Build Tools 2017 и нажмите “изменить”
3. В разделе Visual C++ Build Tools установите галочку напротив пункта "...VC++ 2015.3 v14.00(v140)" и нажмите “ок”

С помощью дистрибутива
Скачайте один из дистрибутивов

Распакуйте. Запустите терминал, перейдите в директорию распакованного дистрибутива.

Для запуска используйте команду:

$ ./node main.js