УДК 004.75
ББК 32.971.353
А 64

Тарасов Елизар Саввич
Кандидат технических наук, доцент кафедры компьютерных технологий и информационной безопасности Кубанского государственного технологического университета, Краснодар, e-mail: helisar@mail.ru
Бачманов Дмитрий Андреевич
Студент Кубанского государственного технологического университета, Краснодар, e-mail: bachmanov.dm@gmail.com
Янкевич Алексей Анатольевич
Студент Кубанского государственного технологического университета, Краснодар, e-mail: helisar@mail.ru
Синицын Алексей Андреевич
Аспирант академии маркетинга и социально-информационных технологий, Краснодар, e-mail: cm.haf932@gmail.com

Анализ подходов к мониторингу и управлению инфраструктурой Интернета вещей на основе блокчейн

(Рецензирована)

Аннотация. *Рассмотрены методические аспекты обеспечения безопасности Интернета вещей с использованием блокчейн-технологии с учетом особенностей построения и функционирования данной архитектуры. Рассмотрены этапы разработки и внедрения блокчейн-решений в контур IoT, обеспечивающие эффективность и безопасность жизненного цикла функционирования инфраструктуры, представлено описание типовой архитектуры такого комплекса.*

Ключевые слова: *Интернет вещей, блокчейн, информационная безопасность, управление безопасностью.*

Tarasov Elizar Savvich
Candidate of Technical Sciences, Associate Professor of Department of Computer Technologies and Information Security, Kuban State University of Technology, Krasnodar, e-mail: helisar@mail.ru
Bachmanov Dmitry Andreevich
Student of the Kuban State University of Technology, Krasnodar, e-mail: bachmanov.dm@gmail.com
Yankevich Aleksey Anatolyevich
Student of the Kuban State University of Technology, Krasnodar, e-mail: helisar@mail.ru
Sinitsyn Aleksey Andreevich
Post-graduate student of Academy of Marketing and Socio-Information Technologies, Krasnodar, e-mail: cm.haf932@gmail.com

Analysis of approaches to monitoring and control of infrastructure of the Internet of things based on blockchain

Abstract. *The paper deals with the methodical aspects of ensuring the security of the Internet of things with the use of blockchain technologies taking into account the features of the construction and functioning of this architecture. The stages of development and implementation of blockchain-based solutions in the IoT loop that ensure the efficiency and safety of the life cycle of the infrastructure functioning are considered, and a description of the typical architecture of such a complex is provided.*

Keywords: *Internet of things, blockchain, information security, information security control.*

Современный Интернет эволюционирует от объединения компьютеров и людей к объединению (умных) объектов/вещей. Эта концепция получила название Интернет вещей (Internet of Thing – IoT) и стала неотъемлемой частью и трендом ИТ-инфраструктуры и экономики в целом. Она связана с увеличением количества и типов устройств, подключенных к сети и взаимодействующих не только с пользователями, но и друг с другом (рис. 1).

При нынешних темпах развития, областях применения и степени конфиденциальности обрабатываемой информации все более остро встает вопрос обеспечения безопасности инфраструктуры Интернета вещей. Комбинирование отдельных блоков аппаратного и программного обеспечения IoT и услуг, предоставляемых разными производителями, приводит к появлению проблем безопасности, конфиденциальности, прозрачности и соответствия требованиям.

Рис. 1. Области применения IoT и составляющие компоненты инфраструктуры

Вместе с тем конечным пользователям крайне важны прозрачность и стабильность работы оборудования [1].

Таким образом, весьма актуальным является вопрос разработки и практической реализация методики контроля, управления и обеспечения безопасности архитектуры «Интернета вещей», а именно (рис. 2):

- создание программного комплекса, обеспечивающего безопасное и стабильное функционирование развернутой инфраструктуры Интернета вещей (в умных домах, офисах, на предприятиях и т.д.);
- повышение взаимного доверия элементов развернутой инфраструктуры и ее надежность (отказоустойчивость);
- гарантированный уровень функциональности, стабильности и защиты от НСД/НСВ, от нарушения логики работы компонентов;
- полная прозрачность функционирования и ведения отчетности устройств инфраструктуры.

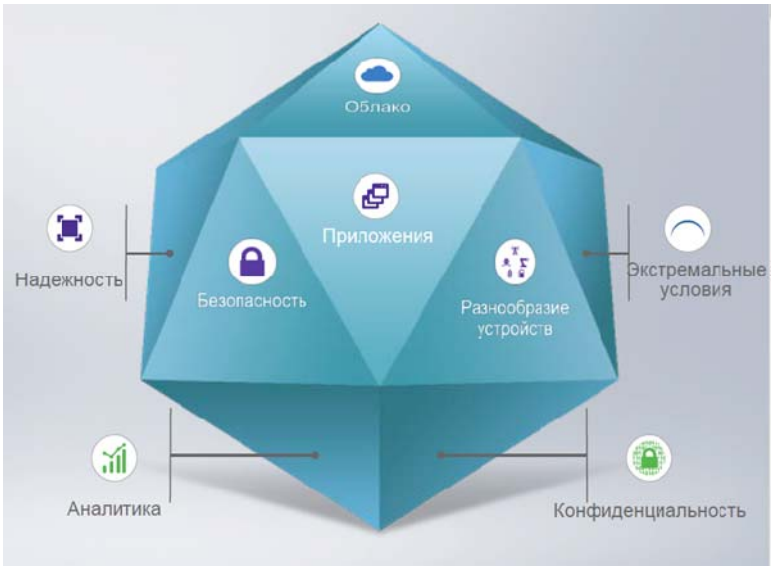

Рис. 2. Основные задачи мониторинга, контроля и управления IoT-инфраструктурой

В целом средства управления IoT можно выделить в три подгруппы. Прежде всего, это управление отдельными устройствами: обнаружение устройств, аутентификация, дистанционная активация и деактивация устройств, конфигурация, диагностика, обновление прошивки и/или ПО, управление рабочим статусом устройства. На более высоком инфраструктурном уровне происходит управление топологией локальной сети и управление конфигурацией сети [2]. На уровне всей экосистемы происходит управление трафиком и перегрузками: обнаружение условий перегруженности сети и реализация резервирования ресурсов для срочных и/или жизненно важных потоков трафика.

Отметим, что в таких системах недостаточно просто разработать «отдельные» протоколы и алгоритмы соблюдения и контроля безопасности, мониторинга и управления инфраструктурой. Необходима поддержка полноценных контуров по мониторингу событий и по управлению рисками в режиме реального времени [3].

При выборе архитектуры такой платформы был проведен аналитический обзор областей применения технологии блокчейн помимо финтеха в областях государственного управления, документооборота, банковской деятельности. Особое внимание мы уделили вопросам применения блокчейна в области проектного управления и сопровождения ИТ-экосистем.

Согласно проведенным опросам, основные преимущества от возможности внедрения блокчейн – сокращение издержек, времени, рисков и коррупционной составляющей.

На рисунке 3 показана схема работы сети блокчейн.

Рис. 3. Схема работы сети блокчейн

Итак, была поставлена задача определить возможность реализации наших задач в блокчейн-экосистеме. Под экосистемой будем понимать набор технологий, включающий как реализации самого блокчейна, так и надстройки к ним: протоколы взаимодействия и файлового обмена, библиотеки, распределенные хранилища и пр. [3].

При этом нами предполагалось использование решений, вышедших в стабильной версии или близких к этому. В процессе исследования предполагалось определить условия успешной интеграции выбранных технологий в единой платформе, а также выявить явные и скрытые проблемы такой интеграции.

Из анализа исходных условий вытекает необходимость использования следующих указанных функциональных компонентов: блокчейн, файловое хранилище, сертифицированное

средство защиты и т.д. [4]. Учитывая, что основной обмен и анализ документов сейчас выполняются вне смарт-контрактов, непосредственно в смарт-контракты передаются только данные, которые те в состоянии обработать. Остальная информация (обосновывающие и распорядительные документы) прикрепляется в виде обычных (для ручной обработки) или формализованных (для автоматической обработки) документов, подписанных усиленной ЭЦП для обеспечения юридической значимости.

При этом на логику смарт-контракта были возложены следующие задачи: обеспечение следования матрице статусов, контроль даты и обработка наступления опорных событий. С каждым из пользователей платформы связывалась следующая регистрационная информация:

- уникальный идентификатор в системе;
- Ethereum-адрес, с которого пользователь направляет транзакции;
- адрес смарт-контракта, используемого для ведения реестра;
- идентификатор сертификата усиленной ЭЦП и ее открытый ключ.

При выборе функциональных компонентов платформы мы ориентировались на открытые решения (Ethereum, Swarm, Storj). Это связано со следующими их преимуществами:

- наличие развернутой и «самоподдерживающейся» инфраструктуры;
- открытость для пользователей и возможность контроля операций через альтернативные источники, а не только через предлагаемый банком интерфейс;
- высокий уровень доверия со стороны пользователей благодаря наличию конкурентных протоколов консенсуса и качественной «нетолерантной» сети независимых узлов.

Таким образом, выбор был сделан в пользу следующих реализаций (рис. 4):

- Блокчейн и смарт-контракты – Ethereum и Solidity;
- Децентрализованные файловые хранилища – Swarm и Storj.io;
- Сертифицированные СКЗИ – КриптоПРО и КриптоАРМ;
- Бродкаст-Оракулы – собственной разработки;
- Провайдеры внешних запросов – собственной разработки;
- Анализатор документов – пока не рассматриваем, поскольку принцип работы аналогичен провайдеру внешних запросов.

Рис. 4. Архитектура и взаимодействие компонентов блокчейн-платформы

Предлагаемый комплекс реализует блокчейн-архитектуру, обеспечивающую повышение стабильности, защищенности и надежности функционирования имеющейся на объекте

инфраструктуры Интернета вещей, обеспечивая эффективную среду исполнения технологических процессов предприятия/офиса и элементов бизнес-логики, построенных на технологии Интернета вещей.

Примечания:

1. Частикова В.А., Березов М.Ю. Определение оптимальных параметров функционирования искусственной иммунной системы для решения задачи обнаружения полиморфных вирусов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2017. № 128. С. 430–440.
2. Частикова В.А., Власов К.А., Картамышев Д.А. Обнаружение DDoS-атак на основе нейронных сетей с применением метода роя частиц в качестве алгоритма обучения // Фундаментальные исследования. 2014. № 8-4. С. 829–832.
3. Чебанов А.С., Власенко А.В., Тарасов Е.С. Разработка подходов к оптимизации сложных организационно-технических систем на основе адаптивных моделей // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2015. № 112. С. 850–861.
4. Хализев В.Н., Федоров С.Ю. Математическая модель синтеза интегрированной системы безопасности // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2012. № 81. С. 341–350.

References:

1. Chastikova V.A., Berezov M.Yu. Determination of the optimal parameters of the artificial immune system functioning to solve the detection problem of polymorphic viruses // Polythematic Online Electronic Scientific Journal of the Kuban State Agrarian University. 2017. No. 128. P. 430–440.
2. Chastikova V.A., Vlasov K.A., Kartamyshev D.A. DDoS attacks detection on the basis of neural networks using the particle swarm optimization as a learning algorithm // Fundamental Research. 2014. No. 8-4. P. 829–832.
3. Chebanov A.S., Vlasenko A.V., Tarasov E.S. Development of approaches to optimization of complex organizational and technical systems on the basis of adaptive models // Polythematic Online Electronic Scientific Journal of the Kuban State Agrarian University. 2015. No. 112. P. 850–861.
4. Khalizev V.N., Fyodorov S.Yu. Mathematical model of synthesis of an integrated security system // Polythematic Online Electronic Scientific Journal of the Kuban State Agrarian University. 2012. No. 81. P. 341–350.