

УДК 519.85  
ББК 32.973.5 + 22.18

## **ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ СОЗДАНИЯ ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ АРЕНДЫ СОБСТВЕННОСТИ С УЧЕТОМ ПОТРАЧЕННЫХ РЕСУРСОВ**

**Печеркин А. А.<sup>1</sup>**

*(Московский Государственный Университет имени М. В. Ломоносова, Москва)*

**Дауркин А. В.<sup>2</sup>**

*В статье рассматривается применение технологии блокчейн и IoT-датчиков для создания системы сдачи собственности в аренду, исключая посредников, и учитывая количество потребляемых при аренде ресурсов. Рассматривается система с агентами – владельцем, арендатором и датчиками, установленными для учета ресурсов. Смарт-контракт на блокчейн-платформе Ethereum используется для управления финансовым взаимодействием между двумя людьми и гарантирует оплату за потраченные ресурсы для обеих сторон. IoT-датчики нужны для фиксации потребляемых ресурсов и автоматического открытия доступа к ним. В работе представлено подробное описание системы и реализован прототип. Описаны возможности применения блокчейна в данной сфере и преимущества смарт-контракта.*

Ключевые слова: блокчейн, смарт-контракт, интернет вещей, распределенная система

---

<sup>1</sup> Печеркин Антон Анатольевич, студент ([aa.pecherkin@yandex.ru](mailto:aa.pecherkin@yandex.ru)).

<sup>2</sup> Дауркин Александр Владимирович, ([adaurkin@rambler.ru](mailto:adaurkin@rambler.ru)).

## **1. Введение**

На середину 2017 года по различным оценкам в мобильных сетях функционировало 400 - 500 миллионов устройств, осуществляющих передачу данных без участия человека и количество подобных устройств неуклонно растет. [19] Появляется все больше датчиков и систем, которые могут автоматически производить замеры и управлять окружающей средой.

Рынок интернет-вещей (Internet of Things – IoT) значительно увеличивается за последние годы, соединяя все больше датчиков в одну единую сеть. Появляются датчики измерения и получения информации об окружающей среде, датчики управления окружающей средой (установка и поддержание заданной температуры, влажности и другие), контролирующие устройства и автоматизированные системы безопасности. Развитие и внедрение датчиков в жизнь людей способствует автоматизации многих видов деятельности и охватывает самые разнообразные области – от частных лиц до компаний. Сами устройства IoT становятся все дешевле для производства, благодаря развитию новых материалов и создания специализированных производящих центров. Это позволяет внедрять датчики в самые разнообразные области – от производственных систем в компаниях, до систем «Умного дома» для частных потребителей.

Значительное внимание уделяется защите, обработке и хранению информации, получаемой от многочисленных датчиков глобальной сети. Один из безопаснейших и открытых способов обработки, хранения и обмена информацией является технология блокчейн.

Блокчейн представляет собой цепочку взаимосвязанных блоков, в каждом из которых хранится ценная информация. Каждый блок создается «майнерами». Блоки связаны между собой единственным образом в цепочку так, что для изменения информации в одном из блоков нужно изменить информацию во всех последующих блоках, что является экономически очень дорого. Благодаря сложности и дороговизне изменения информации в блоках гарантируется надежность и защита данных в блокчейн-цепи.

В промежутке между 2017 и 2023 годом совокупные темпы годового прироста глобального рынка распределенных реестров

и технологии блокчейн составят 57,6%. [6] Как ожидается, к концу обозначенного периода его объем превысит \$5 млрд.

Блокчейн является полезной технологией распределенного взаимодействия участников и может быть применен во многих областях, таких как финансы [8], здоровье [7, 14], коммунальные услуги [9], недвижимость [10, 11], государственное управление [16].

На основе технологии блокчейн был разработан надежный механизм взаимодействия между объектами, называемый смарт-контракты. Смарт-контракт (Smart-contract) — алгоритм, предназначенный для заключения и поддержания самоисполняемых контрактов, выполняемых в блокчейн-среде. Такие контракты записываются в виде кода, существующего в распределенном реестре — блокчейне, который поддерживается и управляется сетью компьютеров. Смарт-контракты позволяют обмениваться активами, не прибегая к услугам посредников, осуществлять P2P обмен (peer to peer).

Смарт-контракты дают возможность выполнять надежные и конфиденциальные транзакции без участия внешних посредников. Кроме того, такие транзакции являются прослеживаемыми, прозрачными и необратимыми. Смарт-контракты не только содержат информацию об обязательствах сторон и санкциях за их нарушение, но и сами автоматически обеспечивают выполнение всех условий договора. Благодаря чему возможно создавать автоматизированные системы, которые управляются согласно прописанным в коде смарт-контракта условиям и надежно защищены посредством технологии блокчейн.

Широкое практическое применение смарт-контракты получили с появлением и развитием проекта Ethereum [15]. В 2013 году был впервые создан наиболее подходящий для смарт-контрактов протокол. Позднее этот протокол претерпел много изменений и усовершенствований, а также начали появляться другие платформы, поддерживающие смарт-контракты (Hyper Ledger, Waves, EOS, и другие).

Таким образом мы видим, что происходит параллельное развитие двух технологий: IoT-устройств и блокчейн, в частности смарт-контрактов, как одного из способов автоматизации взаимодействия с блокчейном. Внедрение смарт-контракта, находящегося в блокчейне, в реальную жизнь и его взаимодействие с IoT-датчиками может быть применимо в разных обла-

стях. Проводятся исследования для решения основной в этой сфере проблемы – “проблемы оракулов” [5]. А также учета, сбора и управления с помощью данных в расширяющейся системе IoT. В [3] описаны основные тренды развития в области блокчейн и IoT.

Централизованная система управления многими датчиками становится все более дорогостоящей для расширяющегося рынка IoT-устройств. В статье [2] предлагается переход к децентрализованной системе для рынка производства и фабрик и подчеркивается, что переход на эту систему значительно снижает издержки. Переход к децентрализованной системе в потребительском секторе и решение проблемы отсутствия доверия к различным IoT-устройствам, которые собирают и отправляют данные, рассмотрено в статье [1].

Каждая совершаемая транзакция в сети блокчейн является платной. Эта оплата является наградой «майнерам» за добавление и поиск блока в блокчейн-цепи. Для более экономичного обмена данными между датчиками и блокчейном в [13] рассматривается пример построения другой системы блокчейна. Авторы предлагают создание гибридного блокчейна, состоящего из под-блокчейнов. Это позволяет быстрее совершать транзакции и экономить на количестве транзакций в сети блокчейн. Однако отмечают, что данный алгоритм снижает безопасность блокчейн-цепи и будет надежен лишь при большом количестве агентов.

Возможность совершения микроплатежей в блокчейне Bitcoin и Ethereum рассмотрена в [17]. Помимо этого, авторы предлагают использовать умные устройства для проведения транзакций между агентами.

В недавней работе [12] авторы описали основные преимущества и недостатки от внедрения блокчейна в IoT-среду. К основным преимуществам относится: надежность, запись информации, защита от взлома и использование смарт-контрактов. К недостаткам отнесены ограниченность ресурсов на расширение сети, открытость данных в блокчейне, «проблема оракулов», возрастающий объем транзакций.

Одна из главных проблем в построении блокчейн-систем является «проблема оракулов», заключающаяся в сложности проверить достоверность информации до ее попадания в блокчейн. Один из способов решения такой проблемы является создание различных уровней доступа к системе блокчейн. В [18]

авторы рассматривают несколько иерархий уровня доступа к системе и, на примере, создают смарт-контракт, управляющий ролями в системе IoT-датчиков. Результаты могут быть использованы в дальнейшем для разработки большой системы и борьбы с «проблемой оракулов».

В статье обратим внимание на область peer-to-peer-шеринга (P2P), иными словами на взаимодействие между двумя и более агентами, при сдаче в аренду вещей. Рассмотрим задачу сдачи квартиры в аренду собственником квартиры с автоматизированным учетом потребляемых ресурсов арендатором, что позволит справедливее и выгоднее оплачивать проживание, как для арендатора, так и для владельца. Данная технология будет основываться на смарт-контракте (в сети Ethereum в нашем случае). Это обеспечит безопасность, открытость и достоверность P2P обмена между агентами.

Во введении рассмотрены статьи и существующие наработки в схожих сферах. В разделе 2 поставлена задача управления взаимодействием между несколькими агентами при сдаче собственности в аренду. В разделе 3 описан алгоритм децентрализованной системы для решения поставленной задачи, описаны основные применяемые технологии, такие как блокчейн, смарт-контракты, сеть Ethereum, датчики IoT. В разделе 4 описан созданный пример реализации мультиагентной системы, приведено описание ее работы, результаты. В заключении будет описана дальнейшая планируемая работа и возможное развитие направления P2P-шеринга с использованием IoT-датчиков и блокчейна.

## ***2. Задача управления взаимодействием между несколькими агентами при сдаче собственности в аренду.***

Главная задача заключается в создании безопасной системы обмена оплатой за арендованное имущество и открытие доступа к этому имуществу. Для осуществления безопасности сделок, защищенности и достоверности информации об арендуемом объекте, действующих агентах и их предыдущей истории, и отзывах, возникает необходимость использование технологии блокчейн. Кроме того, блокчейн позволяет создать децентрализованную систему, то есть систему, полностью исключаящую посредников между арендодателем и арендующим.

Будем учитывать потраченные при аренде ресурсы и предложим механизм отдельной оплаты за них. Это позволит более справедливо оценивать итоговую стоимость аренды и будет выгодно для обеих сторон: для арендующего и арендодателя.

Для осуществления автоматизированного учета потраченных ресурсов будем использовать IoT-датчики, как счетчики ресурсов, с возможностью открытия/блокировки подачи ресурсов и отправки информации о потраченных ресурсах в блокчейн.

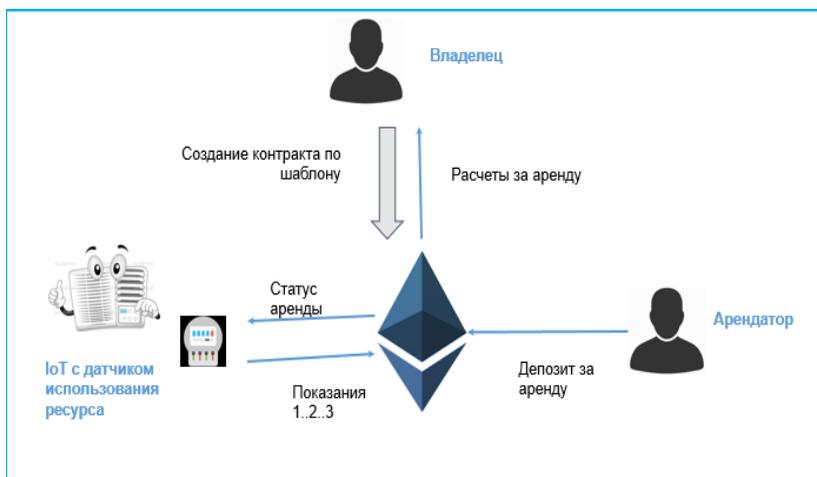
Для управления работой системы, полностью решающей поставленную задачу, будем использовать технологию смарт-контракта, основанного на блокчейне Ethereum. В рамках статьи реализуем полностью работающий смарт-контракт и запустим его в тестовой сети платформы Ethereum, называемой Rinkeby.

При развитии данной платформы следует учесть, что для совершения каждой транзакции в сети Ethereum следует платить «майнерам» за их работу определенную сумму, зависящую от количества передаваемой информации, в так называемых токенах «gas». Поэтому следует выстраивать архитектуру взаимодействия агентов с блокчейном с целью минимизировать количество транзакций, при этом без потери качества системы.

### ***3. Алгоритм децентрализованной системы для решения поставленной задачи***

#### ***3.1. СТРУКТУРНАЯ СХЕМА РАБОТЫ ДЕЦЕНТРАЛИЗОВАННОГО АЛГОРИТМА НА ПЛАТФОРМЕ ETHEREUM***

На рис. 1 представлена схема работы технологии. Сначала опишем общий алгоритм работы системы, а затем разберем требования и возможности для каждого объекта в предлагаемой системе.



*Рис. 1. Схема работы технологии*

Основные действующие агенты в системе – владелец квартиры (агент1), арендатор (агент2).

Для начала работы системы, как представлено на Рисунке 1, агент1 создает смарт-контракт для своей квартиры, в котором описывает стоимость аренды квартиры, стоимость потребляемых ресурсов, указывает статус о возможности аренды. После этого смарт-контракт записывается в блокчейн-сеть Ethereum и становится доступным для использования. Любой человек может стать арендатором квартиры (агентом2), для этого ему нужно обратиться к смарт-контракту и если квартира доступна для аренды, то внести депозит за аренду. При получении средств смарт-контракт передает статус начала аренды датчикам в квартире, открывает двери и дает доступ к ресурсам (электричество, вода, отопление). Агент2 пользуется арендованным помещением, а датчики IoT, установленные в доме, передают измерения потребляемых ресурсов в смарт-контракт. Смарт-контракт получает измерения, каждый раз рассчитывает оплату за потраченные ресурсы и переносит оплачиваемые средства из депозита на счет агента1. При окончании депозита смарт-контракт отдает команду датчикам о прекращении подачи ресурсов и остановки аренды. При преждевременной остановке аренды (до исчерпания всего депозита), агент2 может вернуть оставшийся депозит

из смарт-контракта. Агент1 может получить заработанные средства в любой удобный момент. При окончании аренды агентом2, смарт-контракт меняет статус аренды и сможет принимать другого пользователя.

Таким образом получили автоматизированную систему сдачи в аренду объекта. Данная система является мультиагентной и управляется смарт-контрактом. Безопасность и достоверность передаваемых данных обеспечивается блокчейном и использованием микрокомпьютеров (IoT-устройств).

Далее рассмотрим работу смарт-контракта, который управляет системой, а также функции и работу каждого агента в системе.

### *3.2. УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ МЕЖДУ АГЕНТАМИ. СМАРТ-КОНТРАКТ.*

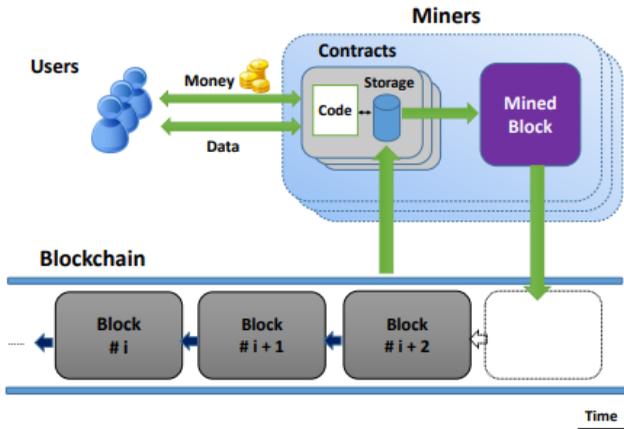
Смарт-контракт в общем случае – это алгоритм, предназначенный для заключения и поддержания самоисполняемых контрактов, выполняемых в блокчейн-среде.

В Ethereum код смарт-контрактов исполняется в определенной среде - виртуальной машине Ethereum (EVM). Каждый узел сети проводит верификацию нового блока, проходя через транзакции, включенные в этот блок, и реализуя иницилируемые этими транзакциями код в EVM [4].

Каждый узел сети выполняет одни и те же вычисления, сохраняет одинаковые значения

Формирование майнерами блоков из транзакций осуществляется за плату: стоимость проведения операции измеряется в единицах газа.

На рис. 3 схематично представлена работа системы Ethereum со смарт-контрактами и блокчейном. Состояние смарт-контракта хранится в публичном блоке блокчейна. Смарт-контракт выполняется сетью майнеров, которые достигают консенсуса по результатам исполнения и соответствующим образом обновляют состояние контракта в следующем блоке блокчейна. Пользователи могут отправлять деньги или данные в контракт; или получать деньги или данные от договора. Все это будет прописано в блокчейне.



*Рис. 3. Схематичное представление работы децентрализованной системы со смарт-контрактами*

В текущей задаче смарт-контракт создается агентом1 и выполняет роль главного управляющего устройства, которое связывает всех агентов:

- Выдает (при запросе) информацию из блокчейна об объекте для агента1 и агента2 по запросу (стоимость, история, транзакции)
- Возвращает (при запросе любым агентом) статус аренды (свободен/занят) в текущий момент по запросу
- Принимает на счет депозит от агента2
- Управляет статусом аренды, основываясь на текущем остатке депозита и расчетов за потраченные ресурсы
- Принимает от датчиков новые измерения
- Осуществляет расчет, основываясь на измерениях потраченных ресурсов и цене каждого
- На основании расчета вычитает средства за потраченные ресурсы из депозита агента2 и добавляет на счет агента1
- Если депозит становится равным нулю, то прекращает аренду, меняя статус на «свободен», таким образом датчики ограничивают доступ к ресурсам и к объекту

- При запросе агента<sup>2</sup> останавливает аренду и делает доступным забрать остатки депозита текущему агенту<sup>2</sup>
- Есть возможность забрать заработанные средства агентом<sup>1</sup> объекта
- Может выдавать экстренные сообщения агенту<sup>1</sup> и блокировать доступ для IoT-устройств (при попытке взлома и в экстренных случаях)

### 3.3. УПРАВЛЯЕМЫЕ УСТРОЙСТВА

IoT-устройства в данном случае - это приборы для измерения потраченных ресурсов и отправки их, с помощью интернет-соединения, в блокчейн, а именно, в смарт-контракт, к которому они привязаны. Также они имеют функционал открытия доступа к ресурсам и закрытия, при считывании и получении информации из смарт-контракта.

В работающей системе, после внесения депозита на счет смарт-контракта, открывается доступ к ресурсам и арендованному объекту. Это осуществляется с помощью специальных устройств IoT, когда смарт-контракт передает сигнал начала аренды. Далее датчики считывают информацию об используемых ресурсах и отправляют эту информацию в смарт-контракт с заданной периодичностью, при помощи транзакции на счет смарт-контракта. В смарт-контракте осуществляются расчеты и проверка доступного депозита.

Датчики обращаются с определенной частотой к смарт-контракту (например, раз в сутки для объекта недвижимости, частота может быть произвольной для других объектов) для проверки доступности аренды в текущий момент времени агентом<sup>2</sup>. Если аренда закончена, то датчики перекрывают доступ к ресурсам и объекту.

Для устройств IoT важно обеспечить защиту и невозможность вмешательства извне с целью сбить работу. Это осуществляется несколькими способами. Во-первых, каждые измерения записываются в смарт-контракте (блокчейне). Это обеспечивает их достоверность на текущий момент и в случае, если следующие показания будут меньше предыдущих, то можно остановить работу системы и обратиться к агенту<sup>1</sup>. Во-вторых, нужно обеспечивать защищенность самих оракулов (IoT-устройств). Это можно обеспечить путем создания пломб, которые при взломе могут также передавать информацию в смарт-контракт. Также

могут быть и другие доступные методы решения «проблемы оракулов».

В качестве IoT-устройств будем использовать микрокомпьютер Raspberry Pi (см. Рис.2), обладающий необходимой функциональностью:

- Возможность считывания ресурсов
- Обработка получаемой информации
- Подключение к блокчейну, посредством интернет-соединения
- Создание собственной ноды в блокчейн-сети
- Открытие\закрытие доступа к ресурсам

Микрокомпьютер обладает высокой скоростью передачи данных и имеет возможность работать автономно, связываясь с сетью лишь необходимое количество раз. Однако при внедрении необходимо задуматься о защите и невозможности внешнего вмешательства в микрокомпьютер.



*Рис. 2. Микрокомпьютер Raspberry PI*

### **3.2. ФУНКЦИОНЛЬНОСТЬ ДЛЯ АГЕНТА1**

Собственник (агент1), сдаваемого в аренду объекта, создает смарт-контракт для своего объекта. После этого имеет возможность проверять статус аренды, прерывать аренду, выводить заработанные средства из смарт-контракта.

При помощи смарт-контракта и открытых записей в блокчейне в любой момент может посмотреть данные об агенте2, текущий баланс, а также историю всех предыдущих арендаторов в смарт-контракте, историю выплат.

При необходимости есть возможность добавить дополнительные функции и условия в смарт-контракте, например, оставка аренды, дополнительная верификация и проверка новых пользователей, система рейтингов для агента1 и агента2 (как это осуществлено у Airbnb, но с гарантией достоверности при записи в блокчейн).

### *3.3. ФУНКЦИОНАЛЬНОСТЬ ДЛЯ АГЕНТА2*

Человек, который хочет арендовать выбранный объект (агент2) изначально выбирает подходящий для аренды объект из предложенных. Для этого может просмотреть информацию об объектах, записанную в блокчейне. Есть возможность просмотреть информацию о собственнике (агенте1) и отзывы предшествующих арендаторов (агентов2), что тоже записано в блокчейне, и поэтому гарантируется достоверность данных.

Далее пользователь отправляет запрос на аренду в смарт-контракт. Если данный объект доступен для аренды, то возвращается положительный ответ. Далее пользователь кладет депозит на баланс смарт-контракта. После прохождения транзакции агент2 получает арендованный объект и пользуется им. В любой момент он может проверить текущий остаток на счету, историю списанных средств, обратившись к смарт-контракту. Также есть возможность пополнить баланс, перечислив средства на счет смарт-контракта.

В любой момент агент2 может по собственному желанию прекратить аренду и забрать оставшийся депозит из смарт-контракта. Истраченные средства будут удержаны смарт-контрактом и, в дальнейшем, их сможет забрать агент1.

## **4. Пример. Децентрализованная система для P2P аренды собственности на блокчейне Ethereum.**

### *4.1. РЕАЛИЗАЦИЯ АЛГОРИТМА ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ НА ПЛАТФОРМЕ ETHEREUM*

В примере реализован смарт-контракт на платформе Ethereum, запущенный в тестовой сети платформы - Rinkeby, который выполняет основные функции, описанные ранее. Смарт-контракт написан на языке Solidity в среде разработки Remix (см. рис. 4).

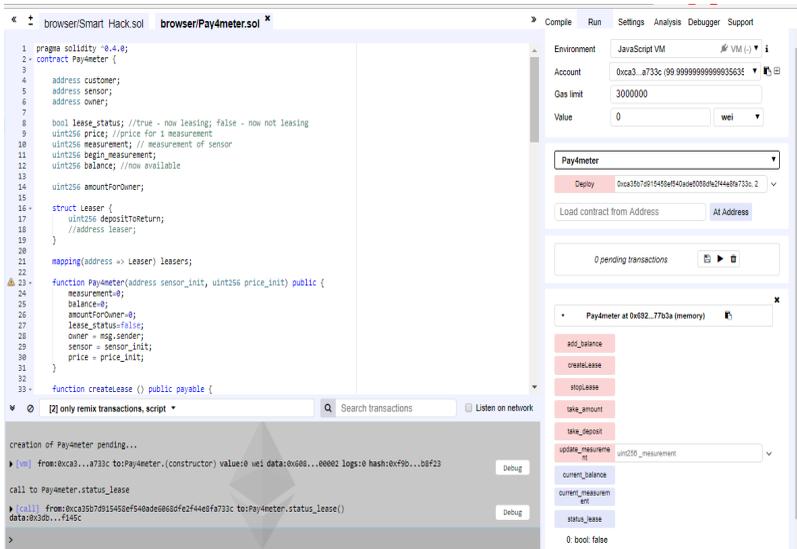
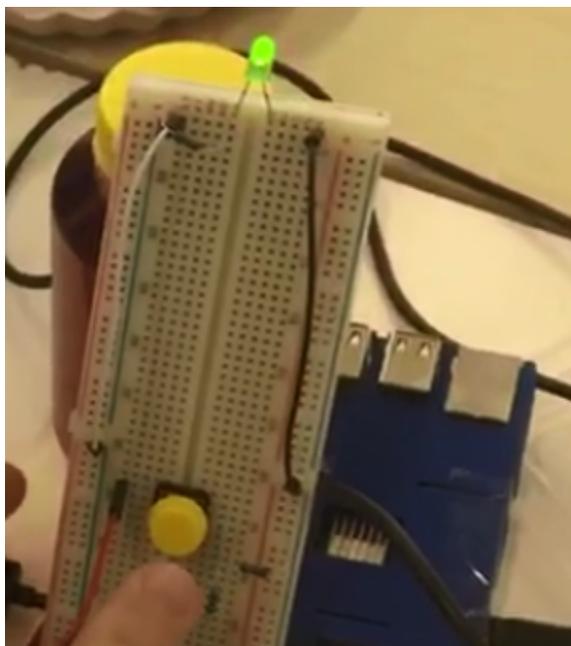


Рис. 4. Смарт-контракт на Solidity в среде Remix

Был реализован прототип датчика на микрокомпьютере Raspberry PI (см. рис. 5). На Raspberry PI создана нода, которая способна обращаться в блокчейн Ethereum к смарт-контракту, узнавать текущий статус из смарт-контракта, управлять подачей электричества. Также сделан прототип счетчика для демонстрации, который отсчитывает потраченные ресурсы при нажатии на кнопку и создает транзакции с информацией в сеть Rinkeby в смарт-контракт.



*Рис. 5. Прототип IoT-датчика на основе RaspberryPI*

Для демонстрации взято два агента – два тестовых кошелька. Один кошелек – агент1, который создает контракт и в дальнейшем может получать заработанные за аренду средства. Второй кошелек – агент2. Он вносит депозит, что свидетельствует о начале аренды, также может забрать оставшиеся средства и остановить аренду.

Далее поэтапно опишем пример реализованной системы по описанному алгоритму для децентрализованной системы и подробно разберем что происходит на каждом этапе и какова функциональность каждого из агентов.

#### *4.2. 1 ЭТАП: СОЗДАНИЕ СМАРТ-КОНТРАКТА*

Агент1 создает смарт-контракт, задает персональные значения – стоимость аренды объекта, стоимость единицы ресурса, адрес подключенного датчика для счета ресурсов, описание объекта и доступность для аренды. После этого агент1 отправляет смарт-контракт на платформу Ethereum (в нашем случае тесто-

вая сеть Rinkeby). С кошелька агента1 снимается оплата сетью Ethereum за размещение смарт-контракта в сети (около 0,04 ETH). После этого агент1 получает роль “owner” в смарт-контракте и может использовать функции доступные данной роли (забирать заработанные средства). Смарт-контракт, размещенный на платформе, становится доступным для взаимодействия для любого человека, кто к нему обратится, в качестве агента2.

The image shows a web interface for deploying a smart contract. It features several input fields and buttons:

- Environment:** A dropdown menu set to "JavaScript VM".
- Account:** A dropdown menu showing the address "0xca3...a733c" and a balance of "(99.99999999999935635)".
- Gas limit:** A text input field containing "3000000".
- Value:** A text input field and a dropdown menu set to "wei".
- Contract Selection:** A dropdown menu showing "Pay4meter".
- Deploy:** A red button with the text "Deploy" and a contract address "0xca35b7d915458ef540ade6088dfe2f44e8fa733c, 2".
- Buttons:** "Load contract from Address" and "At Address".

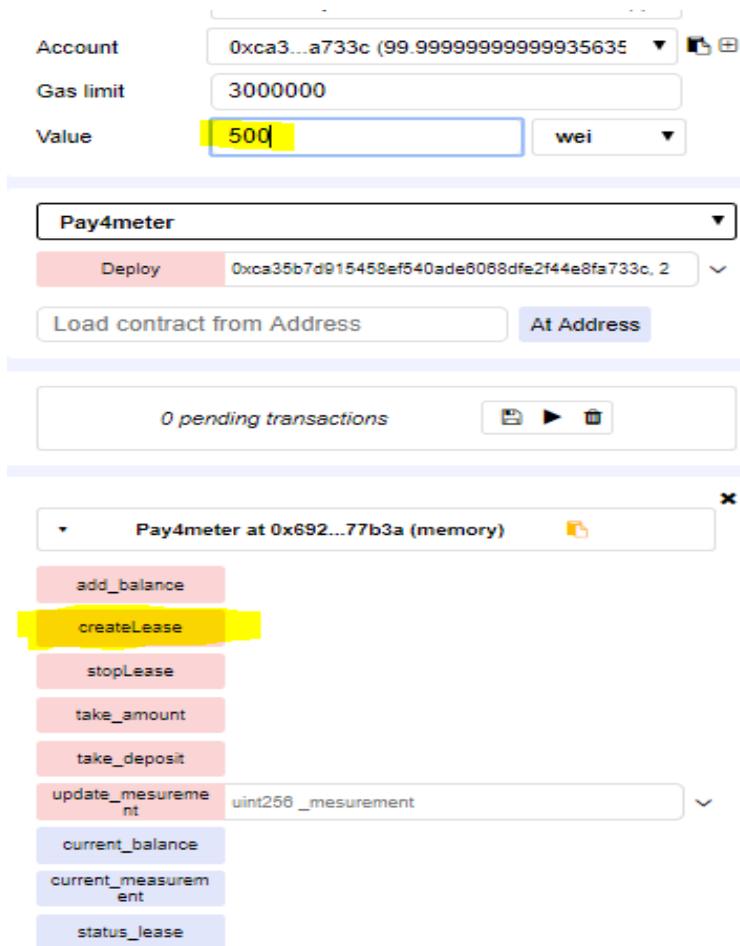
Рис. 6. Создание смарт-контракта

#### 4.3. 2 ЭТАП: НАЧАЛО АРЕНДЫ ОБЪЕКТА

Любой человек может начать аренду объекта, то есть стать агентом2 в системе. Для этого необходимо обратиться к смарт-контракту, узнать статус аренды в данный момент. Если объект свободен, то агент2 должен внести на счет смарт-контракта депозит, который должен быть не менее единицы аренды, заданной агентом1.

Начало аренды вызывается функцией createLease в смарт-контракте и нужно указать вносимый депозит (в wei). (см. рис. 7)

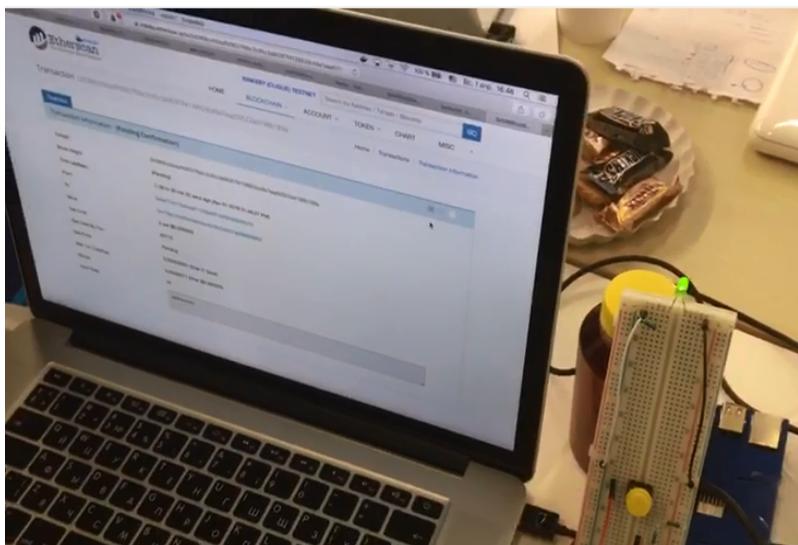
После прохождения транзакции с вызовом метода в тестовую сеть Rinkeby, переменная статуса аренды «lease\_status» меняет значение на «true», что говорит о том, что в данный момент идет аренда.



*Рис. 7. Начало аренды*

#### **4.4. 3 ЭТАП: ВЗАИМОДЕЙСТВИЕ С ИОТ-УСТРОЙСТВАМИ**

После начала аренды датчики считывают со смарт-контракта статус начала аренды (функция `status_lease`) и если возвращаемое значение «true», то включается подача ресурсов в помещении. В качестве прототипа продемонстрировано включение лампочки с помощью Raspberry (в качестве работы IoT-датчика) (см. рис. 8).



*Рис. 8. Начало подачи ресурсов при аренде*

В примере реализован функционал измерений передаваемых ресурсов. Для этого, при нажатии на кнопку осуществляется трата единицы ресурса и осуществляется транзакция в тестовую сеть Rinkeby вызова метода «update\_measurement» в смарт-контракте. Демонстрация передачи транзакции на смарт-контракт показано на Рисунке 8.

После этого в смарт-контракте обновляются текущие показатели измеряемых ресурсов и вычисляется оплата за последний период использования ресурсов. Эта оплата вычитается из депозита агента2 и прибавляется на счет агента1.

После того как весь депозит будет истрачен (путем нажатия на кнопку несколько раз) смарт контракт прерывает аренду (путем вызова функции stopLeaseEnforce()), изменяя переменную «lease\_status» на значение «false». После этого IoT-устройство (RaspberryPI) считывает со смарт-контракта статус аренды (функция status\_lease) и перекрывает подачу ресурсов (выключается лампочка, имитирующая подачу ресурсов в прототипе).

#### 4.5. 4 ЭТАП: ОСТАНОВКА АРЕНДЫ

Текущая аренда может быть остановлена агентом1 или агентом2, с помощью вызова функции «stopLease()» в смарт-контракте.

При этом оставшийся депозит агент2 сможет забрать в любой момент после вызова этой функции.

Агент1 аналогично может забрать заработанные на текущий момент средства со смарт-контракта на свой кошелек в любой момент. (см. рис. 9).



*Рис. 9. Текущий баланс и статус аренды*

Видео-демонстрацию описанного со всеми этапами работы прототипа можно посмотреть ниже. Здесь подробно показана работа всей системы и реализованы все описанные выше этапы.

<https://youtu.be/SJ0OXu95Fhc>

## 5. Заключение

В статье была рассмотрена задача применения технологии блокчейн для создания децентрализованной системы аренды собственности с учетом потраченных ресурсов. Это было осуществлено с помощью применения смарт-контракта и IoT-устройств, которые выступают в роли оракулов и позволяют получать информацию из реального мира и отправлять в блокчейн.

В задаче приведено описание и выполнен пример системы сдачи в аренду объекта, которая включает смарт-контракт и IoT-

устройство, взаимодействующее с окружающей средой и отправляющее данные в блокчейн.

Основное преимущество предложенной системы – это то, что система децентрализована. Технология peer-to-peer позволяет разным людям легко взаимодействовать друг с другом. При использовании блокчейна взаимодействие становится безопасным для обеих сторон, при этом исключаются посредники, а значит лишние траты для обеих сторон. Благодаря технологии IoT-устройств можно получать измерения из реального мира, а, подключив их к интернету, и передавать данные в блокчейн, что позволяет автоматизировать систему общения с реальным миром.

Использование смарт-контракта на платформе Ethereum позволяет выполнить все необходимые функции, чтобы обеспечить безопасность и надежность взаимодействия между агентами в описанной системе. Однако при дальнейшем развитии и масштабировании системы придется столкнуться с несколькими основными сложностями.

Загруженность сети Ethereum (слишком много транзакций в сети при недостаточном количестве «майнеров») сильно замедляет проведение транзакций. Эту проблему можно решить рассмотрев для использования другой блокчейн, либо в будущем при расширении сети (смены архитектуры) проблемы будет уменьшена.

Используя транзакции для передачи данных от IoT-устройств к смарт-контракту возможно придется тратить большую комиссию за проведение транзакций (так как транзакций много). Можно уменьшить число транзакций, путем объединения показателей со всех приборов и отправляя одной транзакцией. Также можно устанавливать небольшую частоту обновления, отвечающую основным требованиям.

Использование в качестве IoT-устройств Raspberry PI можно реализовать весь необходимый функционал. Можно получать нужную информацию, передавать в блокчейн, сделать защиту с передачей экстренной информации при взломе. Однако также есть ряд существенных недостатков.

Во-первых, стоимость таких датчиков, их настройка и обслуживание может быть очень затратным. Стоимость можно сократить, используя более простые датчики и систему взаимодействия.

Во-вторых, «проблема оракулов» становится актуальна для данной задачи. По-прежнему нельзя доверять информации до ее записи в блокчейн. Блокчейн может гарантировать лишь надежность помещенной в нее информации, однако сложно гарантировать достоверность получения информации. Для решения данной проблемы было предложено вносить записи по мере поступления показаний и каждый раз сверять с предыдущими, для выявления подделок.

В-третьих, нужно определить систему доступа для каждого агента при масштабировании системы. Продумать уровень доступа и возможности каждого агента в масштабной системе, учитывая много IoT-устройств с разными показаниями, а также много агентов.

В итоге можно отметить, что технологии блокчейн и IoT сильно развиваются и решается все больше прикладных задач. В статье было рассмотрено применение этих технологий для создания децентрализованной системы аренды собственности с учетом потраченных ресурсов. Важно отметить, что в качестве агента1 и агента2 в рассмотренной задаче, могут быть люди, взаимодействующие в разных областях при сдаче различной собственности в аренду (автомобили, велосипеды, квартиры, дома, техника и другое) с учетом расходуемых ресурсов.

В дальнейшем, с развитием технологий и исследованиями, возможно будет построить полностью автоматизированные платформы в разных сферах для взаимодействия между агентами, избегая посредников.

## **Литература**

Данная статья реализована при частичной поддержке гранта РФФИ № 16-08-01285

1. J. ANGWIN. (2015). *Own a Vizio Smart TV? It's Watching You*. Available: <https://www.propublica.org/article/own-a-vizio-smart-tv-itstwatching-you>
2. P. BRODY AND V. PURESWARAN, *Device democracy: Saving the future of the Internet of Things*, IBM Institute for Business Value, Tech. Rep., Sep. 2014. Available: <http://www935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/>

3. K. CHRISTIDIS, M. DEVETSIKIOTIS. (2016). *Blockchains and Smart Contracts for the Internet of Things*. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467408>
4. DELMOLINO K. ET AL. *Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab* // International Conference on Financial Cryptography and Data Security. – Springer Berlin Heidelberg, 2016.
5. EARL T. BARR, MARK HARMAN, PHIL MCMINN, MUZAMMIL SHAHBAZ, AND SHIN YOO. *The oracle problem in software testing: a survey*. Available: <https://ieeexplore.ieee.org/iel7/32/7106034/06963470.pdf>
6. HIMAL SRIVASTAVA *Blockchain Distributed Ledger Market by Type (Private Blockchain & Public Blockchain) and End User (Government, BFSI, Automotive, Retail & e-commerce, Media & Entertainment, and Others). Global Opportunity Analysis and Industry Forecast, 2017-2023*. Available: <https://www.alliedmarketresearch.com/blockchain-distributed-ledger-market>
7. I. KAR. (2016). *Estonian Citizens Will Soon Have the World's Most Hack-Proof Health-Care Records*. Available: <http://qz.com/628889/this-eastern-european-country-is-moving-its-health-recordsto-the-blockchain/>
8. J. KELLY AND A. WILLIAMS. (2016). *Forty Big Banks Test Blockchain-Based Bond Trading System*. Available: <http://www.nytimes.com/reuters/2016/03/02/business/02reuters-bankingblockchain-bonds.html>
9. S. LACEY. (2016). *The Energy Blockchain: How Bitcoin Could be a Catalyst for the Distributed Grid*. Available: <http://www.greentechmedia.com/articles/read/the-energy-blockchain-could-bitcoin-be-a-catalyst-forthe-distributed-grid>
10. A. MIZRAHI. (2015). *A Blockchain-Based Property Ownership Recording System*. Available: <http://chromaway.com/papers/A-blockchainbased-property-registry.pdf>
11. D. OPARAH. (2016). *3 Ways That the Blockchain Will Change the Real Estate Market*. Available: <http://techcrunch.com/2016/02/06/3-ways-that-blockchain-will-change-the-real-estate-market/>
12. G. RAMACHANDRAN, B. KRISHNAMACHARI. (2018). *Blockchain for the IoT: Opportunities and Challenges*. Available: <https://arxiv.org/pdf/1805.02818.pdf>

13. GOKHAN SAGIRLAR, BARBARA CARMINATI, ELENA FERRARI, JOHN D. SHEEHAN, EMANUELE RAGNOLI. (2018) *Hybrid-IoT: hybrid blockchain architecture for Internet of Things - PoW Sub-blockchains*. University of Insubria, Italy. IBM research - Ireland
14. W. SUBERG. (2015). *Factom's Latest Partnership Takes on US Healthcare*. Available: <http://cointelegraph.com/news/factoms-latestpartnership-takes-on-us-healthcare>
15. VITALIK BUTERIN. (2013) *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. Available: <https://github.com/ethereum/wiki/>
16. M. WALPORT, *Distributed ledger technology: beyond block chain*, U.K. Government Office Sci., London, U.K., Tech. Rep., Jan. 2016. Available: <https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review>
17. S. YASSAMI, N. DREGO, I. SERGEEV, T. JULIAN, D. HARDING, AND B. S. SRINIVASAN. (2016). *True Micropayments With Bitcoin*. Available: <https://medium.com/@21/true-micropayments-with-bitcoine64fec23ffd8>
18. YUANYU ZHANG, MEMBER, IEEE, SHOJI KASAHARA, MEMBER, IEEE, YULONG SHEN, MEMBER, IEEE, XIAOHONG JIANG, SENIOR MEMBER, IEEE, AND JIANXIONG WAN. (2018) *Smart contract-based access control for the Internet of Things*
19. ADVANCED COMMUNICATIONS & MEDIA “Обзор рынка IoT в России”. Available: [http://www.acm-consulting.com/data-downloads/doc\\_download/191-iot-report-in-russian.html](http://www.acm-consulting.com/data-downloads/doc_download/191-iot-report-in-russian.html)

## **APPLICATION OF BLOKCHAIN TECHNOLOGY FOR DEVELOPING A DECENTRALIZED PROPERTY LEASE SYSTEM**

**Anton Pecherkin**, Lomonosov Moscow State University, Moscow, student (aa.pecherkin@yandex.ru)

**Alexander Daurkin**, (*adaurkin@rambler.ru*)

*Abstract: This article discusses the use of blockchain technology and IoT-sensors to create a rental system, excluding intermediaries, and taking into account the amount of resources used for leasing. The system is considered with agents - the owner, the tenant and the sensors, established for the account of resources. A smart contract on the Ethereum blockchain platform is used to manage the financial interaction between two people and guarantees payment for the spent resources for both parties. IoT-sensors are needed to fix consumed resources and automatically open access to them. The work presents a detailed description of the system and implemented a prototype. The main problems of the implementation of this system are considered, such as the "oracle problem", connection to the network and interaction with the blockchain. The possibilities of using blockchain in this area and the advantages of a smart contract are described. Also proposed are methods to improve the proposed system and how to use it. There are presented ways to improve the smart contract, use other block systems, improve the system of sensors, and protect the system from hacking.*

Keywords: blockchain, smart contract, internet of things, distributed system

*Статья представлена к публикации  
членом редакционной коллегии ...заполняется редактором...*

*Поступила в редакцию ...заполняется редактором...  
Опубликована ...заполняется редактором...*