

УДК 334.021.1

DOI 10.21685/2072-3016-2018-3-15

*А. Г. Финогеев, Л. А. Гамидуллаева, С. М. Васин,
А. А. Финогеев, В. В. Проничев, А. М. Лычагин*

СМАРТ-КОНТРАКТЫ КАК ИНСТРУМЕНТАРИЙ БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ СУБЪЕКТОВ РЕГИОНАЛЬНОЙ ИННОВАЦИОННОЙ СИСТЕМЫ¹

Аннотация.

Актуальность и цели. Рост взаимодействия между участниками инновационной системы представляет собой механизм развития инновационной деятельности на различных этапах инновационного процесса, от возникновения идеи до коммерциализации инновации. При этом основным барьером, препятствующим эффективному взаимодействию субъектов инновационной деятельности, является высокий уровень трансакционных издержек инновационной деятельности. Предметом исследования в статье является процесс взаимодействия участников инновационных систем регионов в России. Целью работы является разработка механизма надежного и безопасного взаимодействия участников региональных инновационных систем на основе смарт-контрактов в блокчейн-системе.

Материалы и методы. Для снижения рисков в процессе реализации инновационных проектов предлагается использовать технологию распределенного реестра (блокчейн), которая позволяет снизить возможность недобросовестных действий сторон, передать функции третьей стороны интеллектуальной системе (смарт-контракту).

Результаты. Предложенная технология позволяет минимизировать риски реализации проектов в сфере инноваций, снизить уровень трансакционных издержек в процессе инновационной деятельности. Результатом внедрения технологии является формирование и поддержка доверительных и прозрачных отношений как между участниками инновационных взаимодействий, так и со всеми заинтересованными субъектами социально-экономической деятельности в регионах. Смарт-контракты создаются на базе выбранной блокчейн-платформы Ethereum и представляют собой инструменты для заключения договоров, создания и внедрения инноваций, передачи прав интеллектуальной собственности, использования прав и лицензий при инновационной деятельности и т.п.

Ключевые слова: смарт-контракт, блокчейн, региональная инновационная система, трансакционные издержки, результаты интеллектуальной деятельности, инновационные взаимодействия, Ethereum.

¹ Исследование выполнено при поддержке проектов РФФИ № 18-010-00204, № 16-07-00031, № 18-07-00975.

© 2018 Финогеев А. Г., Гамидуллаева Л. А., Васин С. М., Финогеев А. А., Проничев В. В., Лычагин А. М. Данная статья доступна по условиям всемирной лицензии Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), которая дает разрешение на неограниченное использование, копирование на любые носители при условии указания авторства, источника и ссылки на лицензию Creative Commons, а также изменений, если таковые имеют место.

A. G. Finogeev, L. A. Gamidullaeva, S. M. Vasin,
A. A. Finogeev, V. V. Pronichev, A. M. Lychagin

SMART CONTRACTS AS A TOOL FOR SAFE INTERACTION OF THE REGIONAL INNOVATION SUBJECTS

Abstract.

Background. The growth of interaction between the participants of the innovation system is a mechanism for the development of innovative activity at various stages of the innovation process, from the emergence of the idea to the commercialization of innovation. At the same time, a high level of transaction costs of innovation activity is the main barrier that prevents effective interaction between subjects of innovation activity. The subject of the study is the organization of effective and safe interaction between participants in Russian regional innovation systems. The aim of the work is to develop a mechanism for ensuring reliable and secure interaction between participants in regional innovation systems based on the created smart contracts in the blockchain system.

Materials and methods. To reduce risks in the implementation of innovative projects, it is proposed to use distributed registry technology (blockchain), which reduces the probability of fraud on the part of dishonest participants, and excludes the need for third-party intervention by transferring its functions to an intellectual system.

Results. The technology offered by the authors allows to minimize the risks of implementing projects in the sphere of innovations, reduce the level of transaction costs on the innovation process. This is of importance for ensuring confidential and transparent relations between participants in innovation projects, as well as with all stakeholders in the regions. To create smart contracts, the Ethereum block-platform was chosen, on the basis of which components were developed for performing transactions in contracting, creating and implementing innovations, transferring intellectual property rights, using rights and licenses for innovation, etc.

Key words: smart contract, blockchain, regional innovation system, transaction costs, results of intellectual activity, innovative interactions, Ethereum.

Введение

Для инновационного развития экономики страны необходимо наличие благоприятной для ученых, предпринимателей и инновационных предприятий среды. Этот общепризнанный тезис сформулирован в стратегических документах почти всех передовых в плане инноваций стран мира. На сегодняшний день необходимость построения благоприятной инновационной среды на различных уровнях управления рассматривается как краеугольный камень всей экономической политики государства, обеспечивающей достижение Россией глобальной конкурентоспособности и национальной безопасности. При этом следует учитывать, что активное информационно-технологическое развитие в мире ставит новые вызовы перед Россией. К ним относятся цифровая трансформация экономики и построение общей экосистемы цифровой экономики с высокой экономической эффективностью. Сегодня Россия находится далеко позади развитых экономик мира, которые на протяжении многих лет занимались проблемой цифровизации. Следует отметить, что некоторые шаги в данном направлении уже сделаны, однако они отрывочны и

не обеспечивают комплексное решение проблемы цифровизации инновационной экосистемы.

В целом особенностью экосистемного подхода к инновационному развитию является акцент на коллаборционных процессах (процессах взаимодействия) участников, обеспечивающих создание и диффузию потоков знаний, трансформацию этих потоков в инновации и их дальнейшее распространение.

Организация безопасного и надежного взаимодействия между участниками региональной экосистемы является механизмом развития инновационной деятельности от идеи до реализации и коммерциализации инновации. Значительный вклад в понимание важности взаимодействия субъектов экономики внесли И. Ансофф и Э. Кемпбелл [1], показав, что синергетические эффекты инновационной экономики являются уникальными скрытыми ресурсами, которые проявляются лишь в случае открытой деятельности предприятий, предполагающей активное сотрудничество, взаимодействие, обмен опытом и осуществление кооперативных проектов. Однако при этом важно принимать во внимание, что эти процессы обуславливают рост нестабильности и неопределенности в имеющихся у предприятий партнерских связях и отношениях, что, в свою очередь, вызывает рост транзакционных издержек. Таким образом, в современных условиях функционирования инновационных экосистем российских регионов основным барьером, препятствующим эффективной коллаборации субъектов экономики, является высокий уровень издержек инновационной деятельности, которые носят преимущественно транзакционный характер. Такие затраты имеют транзакционную природу, которая обусловлена необходимостью взаимовыгодных контактов и коллабораций. Именно транзакционные издержки необходимо считать основным барьером регионального инновационного развития, так как они сдерживают внедрение инноваций собственниками предприятий [2, 3].

В ходе создания инноваций происходят взаимодействия между участниками инновационной деятельности, которые определяются транзакциями внутри предприятия и отношениями экономического агента с институциональной средой. Среда фактически синтезирует условия для организации взаимодействий участников инновационной деятельности в плане поиска финансовых, информационных, кадровых и других ресурсов, а также определяет поведение экономических агентов при заданных условиях. Она включает ряд институциональных структур, которые выполняют роль инструментов принятия решений в процессе создания и внедрения инноваций. Важную роль в таких условиях играет цифровая безопасность и прозрачность сделок (транзакций), которая обеспечивается современными технологиями (например, блокчейн).

На современном этапе необходимо говорить о новых киберсоциальных технологиях, которые целесообразно использовать для формирования и поддержки региональных инновационных систем. Такие технологии стимулируют взаимодействие участников инновационной деятельности, реализуют интеллектуальный механизм для анализа больших данных об инновационных процессах и участниках, поддержки принятия решений при внедрении инноваций. Таким образом, инновационная система, реализующая киберсоциаль-

ные технологии взаимодействия, является интеллектуальной системой [4]. Традиционным примером ее реализации может быть интернет-портал, с помощью которого участники региональной инновационной системы (хозяйствующие субъекты, высшие учебные заведения, научно-исследовательские институты, государственные структуры, пользователи и общественность) получают доступ к информационным ресурсам.

Киберсоциальная инновационная система должна быть ориентирована на снижение транзакционных издержек, на взаимодействие субъектов инновационной деятельности через вовлечение в инновационный процесс большого числа участников и обеспечение их безопасного взаимодействия. Для решения второй задачи необходим механизм, посредством которого субъекты инновационной деятельности могут создавать новые системы и технологии, обмениваться знаниями в сетевой среде.

1. Блокчейн для взаимодействия субъектов инновационной деятельности

Эффективность функционирования региональной инновационной системы зависит от многих факторов, в том числе и от обеспечения информационной безопасности взаимодействий участников в ходе транзакционных процессов. Внедрение цифровых механизмов в экономику регионов направлено на снижение влияния антропогенных факторов на большинство процессов информационного взаимодействия. Целью является обеспечение безопасности и прозрачности транзакций между взаимодействующими экономическими агентами. Для решения данной задачи считаем целесообразным использовать технологию блокчейн и смарт-контракты.

Общеизвестно, что осуществление коммерческих сделок с помощью сети Интернет и технологий электронной коммерции является непростой задачей. Основной проблемой является установление доверительных отношений между незнакомыми участниками сделки. Для решения проблемы приходится использовать стороннюю организацию, выступающую гарантом добросовестного исполнения условий сделки. Но приходится констатировать, что даже в случае участия третьей стороны проблема безопасности не решается с высокой степенью надежности. В современных условиях для снижения рисков взаимодействия участников активно начинает использоваться технология распределенного реестра (блокчейн), позволяющая минимизировать вероятность недобросовестного поведения участников сделок. Кроме того, данная технология позволяет исключить необходимость участия третьей стороны путем передачи ее функций интеллектуальной информационной системе [5].

Блокчейн представляет собой последовательную цепочку блоков, созданную по определенным правилам, которая также называется связным списком или распределенным реестром [6]. Копии блоков хранятся на сетевых узлах пользователей блокчейна и обрабатываются независимо друг от друга [7, 8]. Первым применением распределенного реестра стали транзакции при операциях с криптовалютой «биткоин». В дальнейшем было показано, что технология блокчейн может использоваться для операций с любыми информационными объектами. Поскольку в каждом из узлов блокчейна хранится

часть информации в виде блоков или их копий, защищенных криптографическими ключами, то это делает систему неуязвимой для информационных атак. Криптографические ключи вычисляются с помощью хэш-функций. В нашем случае распределенный реестр должен хранить информацию об участниках инновационной деятельности, инновациях, правах интеллектуальной собственности, сделках о передаче прав и т.п.

Преимуществами блокчейна являются прозрачность транзакций, а также копирование и хранение блоков на множестве узлов, что позволяет всем участникам процесса получить доступ к информации о действиях партнеров. Таким образом поддерживаются доверительные отношения между участниками инновационной деятельности и другими заинтересованными субъектами экономической деятельности в регионах.

В качестве информации, хранящейся в блокчейне региональной инновационной системы, отметим информацию об инновациях, информацию об экономических агентах, информацию о правообладателях, правоустанавливающие документы, записи о транзакциях между участниками, договорные обязательства, персональные данные, описание результатов интеллектуальной деятельности (РИД), цифровые копии объектов интеллектуальной собственности и т.п. Суть использования технологии заключается в том, что депонировать авторство РИД возможно без участия третьей стороны, без привязки к географическому местоположению, причем подлинность цифровых инновационных объектов подтверждается цифровым сертификатом. Также технология позволяет обеспечить безопасность при хранении актуализированной информации о любых инновационных объектах.

В распределенном реестре отображается весь жизненный цикл инновации и ее влияние на получение новых знаний и РИД [9]. Рассмотрим пример. Часто результаты инновационных исследований описываются в открытых научных публикациях. Сотрудники вузов, публикующие результаты, не всегда включены в реальные экономические процессы. Сторонние лица могут использовать данные результаты чужих исследований в процессе создания инноваций и регистрации прав интеллектуальной собственности без указания ссылок на источники. Если создать блокчейн для хранения и обмена информацией об объектах интеллектуальной собственности и научных публикациях с описанием результатов исследований по аналогичной тематике, то можно выявить автора идеи, отследить процесс передачи и использования знаний в процессе синтеза инноваций. Примером являются разработки компании Ascribe, которая посредством технологии блокчейн помогает художникам подтверждать авторство на предметы искусства при помощи уникальных идентификаторов и цифровых сертификатов, передавать права владения ими [10].

Для управления правами интеллектуальной собственности в России разрабатывается сеть IPChain на блокчейн-платформе HyperLedger Fabric, поддерживаемой консорциумом таких компаний, как Intel, Oracle, Cisco, Digital Assets и др., под руководством компании IBM. Система позволяет работать с различными каналами информации в реестре с подтверждением транзакций для правообладателей [11]. Особенностью системы является адаптивный алгоритм соглашения между доверенными узлами, который помогает децентрализованно выполнить регистрацию транзакции на заданном

числе равноправных узлов, а затем подтвердить ее в случае достоверности результатов. Система IPChain включает сеть с узлами регистрации и фиксации транзакций, управления сетью и выдачи доверительных сертификатов, распределенную базу данных объектов интеллектуальной собственности, реестр выполненных транзакций.

Несмотря на то что идея смарт-контрактов была предложена еще в 1994 г. [12], ее реализация стала возможной в 2008 г. после появления технологии блокчейн. Смарт-контракт – это алгоритм автоматического заключения и поддержания договорных обязательств между сторонами в интеллектуальной информационной системе [13]. Смарт-контракты могут использоваться в любых сделках, так как они гарантируют перевод финансовых средств или выполнение иных действий, предусмотренных контрактом, только после того, как стороны исполнят свои обязательства. Для поддержки процесса автоматического исполнения обязательств в рамках смарт-контракта требуется специальная среда. Фактически смарт-контракт существует внутри данной среды в виде программного кода, реализующего заданный алгоритм. В таком контракте все взаимоотношения между сторонами имеют четкую математическую формализацию и логику исполнения. Алгоритм контракта отслеживает моменты достижения или нарушения его пунктов и принимает решения в автоматическом режиме для отклонения сделки или подтверждения достоверности исполнения обязательств.

Для функционирования смарт-контрактов необходимо:

- 1) существование распределенной сетевой среды исполнения контракта (тип Ethereum, Codius, Counterparty и т.п.);
- 2) наличие распределенной базы данных для хранения данных об исполняемых транзакциях с доступом для сторон контракта;
- 3) использование технологий цифровой электронной подписи на основе технологии асимметричного шифрования;
- 4) подтверждение достоверности источника данных посредством центров сертификации.

К основным объектам смарт-контракта относятся:

- 1) предмет договора с описанием всех объектов в среде существования контракта;
- 2) участники сделки, принимающие или отказывающиеся от условий контракта с помощью цифровых электронных подписей;
- 3) алгоритм исполнения пунктов договора в виде формализованного математического описания, который можно перевести в программный код и исполнить в среде блокчейн.

2. Анализ блокчейн-платформ

Кроме поддержки операций с криптовалютами, на практике блокчейн-платформы могут использоваться в качестве среды для смарт-контрактов, а также для создания других децентрализованных приложений (DApps), которые не связаны с финансами и позволяют использовать цепочки взаимосвязанных информационных блоков в любых целях [14]. Блокчейн-платформы делятся на глобальные и приватные. Глобальные платформы представляют

собой блокчейн, открытый для пользователей и разработчиков, на базе сети пиринговых (peer-to-peer) узлов с данными о всех транзакциях.

Для сравнительного анализа возьмем четыре блокчейн-платформы, такие как Ethereum, Aeternity, Hyperledger Fabric, Cardano [15], которые уже используются для создания смарт-контрактов и децентрализованных приложений.

Особенностью платформы Aeternity является оригинальное решение проблемы масштабирования блокчейна таким образом, чтобы сложность создаваемых приложений и смарт-контрактов не влияла на производительность сети [16]. Для поддержки финансовых транзакций в системе используется проприетарный платежный протокол Lightning Network [17], который работает с блоками, исполняя транзакции между узлами. Для решения задачи масштабирования он добавляет новый логический уровень для балансировки нагрузки из-за увеличения числа транзакций. Сами транзакции в рамках смарт-контрактов проходят в выделенных каналах без вовлечения в процесс всей сети блокчейн. Сеть блокчейн используется в качестве реестра для учета финансовых последствий успешных транзакций или в качестве арбитра в случае возникновения разногласий.

Платформа Hyperledger Fabric также является открытым блокчейном для универсального применения [18]. Именно эта особенность и определила выбор платформы для разработки системы IpChain. Платформа обладает необходимым функционалом для синтеза децентрализованных приложений и смарт-контрактов. Особенностью является возможность многослойного конфигурирования системы блокчейн. Для решения проблемы масштабирования также реализуются приватные каналы транзакций с повышенной надежностью и пропускной способностью.

Платформа Cardano является системой третьего поколения [19]. Она реализует технологию масштабируемой программируемой передачи стоимости криптовалюты. Основным отличием платформы является наличие разделения вычислительных слоев. В системе есть базовый слой для обращения криптовалюты и слой для синтеза и работы смарт-контрактов. Особенностью является применение алгоритма достижения консенсуса на основе доказательства доли владения (Proof-of-Stake). Здесь вероятность синтеза блока в блокчейне пропорциональна доле, которую составляют принадлежащие участнику единицы криптовалюты, что позволяет владельцам контролировать процесс транзакций в сети.

Платформа Ethereum реализована как единая децентрализованная виртуальная машина в сети Интернет и позволяет выполнять транзакции любого уровня сложности [20]. Смарт-контракты, создаваемые на базе платформы, помогают регистрировать сделки с любыми активами в распределенном реестре, защищая транзакции посредством хэш-сумм в блокчейне. Пользователи реализуют вычисление хэшей в своих компьютерах. Для разработки смарт-контрактов в Ethereum применяется встроенный язык программирования Solidity [21], на котором можно создавать контракты с произвольными условиями владения, форматами транзакций и функциями изменения состояния. Сравнение платформ приведено в табл. 1.

Сравнение блокчейн-платформ

Платформа	Достоинства	Недостатки	Языки программирования
Ethereum	+ Широкое распространение + Гибкость + Низкий порог вхождения	– Оплата транзакций в сети – Нагрузка на сеть	• Solidity • Serpent • Mutan
Aeternity	+ Масштабируемость + Снижение себестоимости	– В стадии разработки	• Erlang • Solidity
Hyperledger Fabric	+ Ориентированность на корпоративный сегмент + Растущая экосистема	– Небольшое сообщество – Высокий порог вхождения	• Go • Java • JavaScript
Cardano	+ Масштабируемость + Интероперабельность	– В стадии разработки	• Haskell

Практически у всех платформ есть свои достоинства и недостатки. Однако для достижения цели исследования в плане создания смарт-контрактов и обеспечения безопасных и надежных взаимодействий между субъектами инновационной региональной системы предлагается использовать платформу Ethereum. Это обусловлено следующими соображениями. Две платформы Cardano и Aeternity пока находятся в стадии тестирования и требуют больше времени на изучение инструментария. Платформа Hyperledger Fabric более сложная и предназначена для создания крупных проектов в больших компаниях. Платформа Ethereum является универсальной и наиболее распространенной системой с низким порогом вхождения. Она наиболее проработана, что позволяет сразу приступить к реализации бизнес-задач. Ethereum является открытой платформой и не требует получения лицензий, а уже созданные приложения находятся в свободном доступе, что важно для бюджетных образовательных организаций. Основным ограничением является требование к отсутствию ошибок при создании смарт-контрактов. Дело в том, что Ethereum постулирует необратимость и неизменность транзакций, поэтому исполнение смарт-контракта с ошибками невозможно изменить или отменить, что может повлечь рост транзакционных издержек вместо их снижения. Разработка алгоритмов смарт-контрактов на данной платформе требует повышенного внимания и высокой квалификации разработчика, многократного тестирования, так как цена ошибки велика.

Рассмотрим данную платформу подробнее. Ethereum включает ряд доступных инструментов для решения конкретных задач: Solidity, Remix, Truffle, Geth, Parity, CPP-Ethereum, протокол Ethereum, браузеры MetaMask и Mist, Web3.js и т.д. Как уже было сказано, смарт-контракты создаются на объектно ориентированном JavaScript-подобном языке Solidity в облачной среде Remix, которая позволяет создавать и запускать код в стандартном браузере. После трансляции контракты выполняются на виртуальной машине Ethereum.

Недостатком системы является то, что для достижения консенсуса используется метод доказательства выполнения работы (Proof-of-Work), где подлинность транзакций подтверждается вычислительной мощностью узлов сети, причем вероятность создания блока зависит от данной мощности. В настоящее время проводится перевод Ethereum на метод Proof-of-Stake.

Фреймворк Truffle поддерживает управление контрактами, их размещение в блокчейне и миграцию. Инструменты Geth, Parity и CPP-Ethereum используются для подключения узлов к блокчейну. Они загружаются в качестве клиентов на узлы сети и реализуют протокол Ethereum. Для взаимодействия с блокчейном применяются браузеры с плагинами типа MetaMask и Mist. Они представляют связующее звено между браузерами и блокчейном, через которое можно выполнять программы и отправлять команды в систему. Также для взаимодействия между браузером и блокчейном необходима библиотека Web3.js, которая позволяет работать с узлами сети Ethereum по протоколу Remote Procedure Call (RPC) и HTTP, как показано на рис. 1.

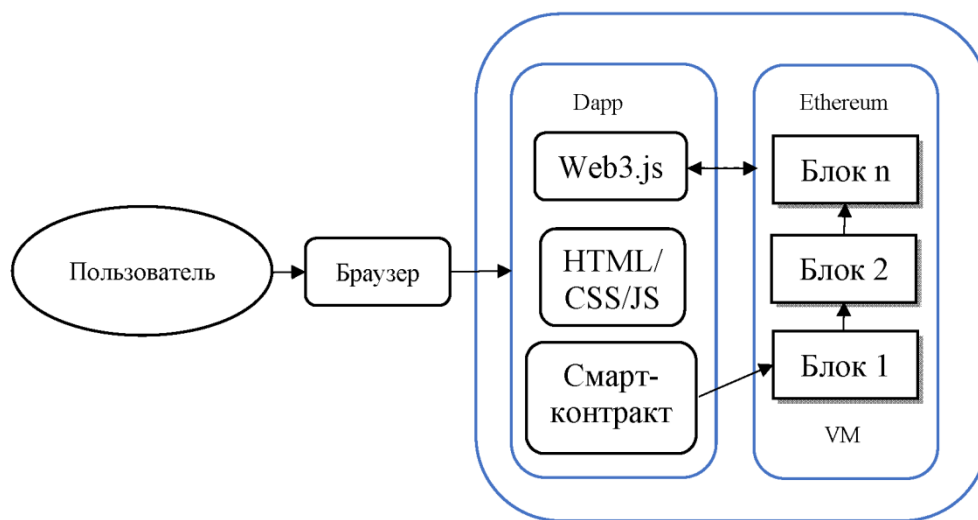


Рис. 1. Схема работы с блокчейном из браузеров

3. Смарт-контракты в блокчейне

Для поддержки взаимодействий субъектов инновационной системы региона необходимо разработать инструменты исполнения транзакций. Они должны обеспечить безопасные процедуры для автоматизированного заключения договоров, передачи прав интеллектуальной собственности, выполнения условий лицензионных договоров, хранения и обмена данными об инновациях и участниках инновационного взаимодействия, мониторинг использования прав и лицензий при инновационной деятельности и т.п. Примерами транзакций являются:

- 1) идентификация пользователей системы;
- 2) сбор данных об инновациях и загрузка в систему;
- 3) сбор средств для реализации инновационных процессов (краудфандинг);
- 4) создание реестра инновационных активов и криптовалюты для взаиморасчетов;

- 5) подтверждение подлинности файлов, документов, блоков;
- 6) проверка и подтверждение прав интеллектуальной собственности;
- 7) проведение анкетирования, электронного голосования и аукционов и т.д.

Для записи информации о транзакциях формируется распределенный реестр, в который записываются такие транзакции, как например:

- 1) регистрация инновационного объекта;
- 2) установка прав доступа к цифровому паспорту инновационного объекта;
- 3) результаты экспертиз инновационных объектов;
- 4) оценка объекта по различным критериям;
- 5) постановка объекта на бухгалтерский учет;
- 6) описание сделки по передаче прав собственности на объект;
- 7) финансовые взаиморасчеты;
- 8) выплата авторского вознаграждения;
- 9) ведение споров по правам интеллектуальной собственности и т.п.

В качестве инструментов исполнения транзакций и контроля за ними предназначены смарт-контракты. Они выполняют множество функций для организации взаимодействий участников инновационной системы. Рассмотрим пример создания и реализации смарт-контракта на передачу прав собственности на РИД между участниками сделки (рис. 2).

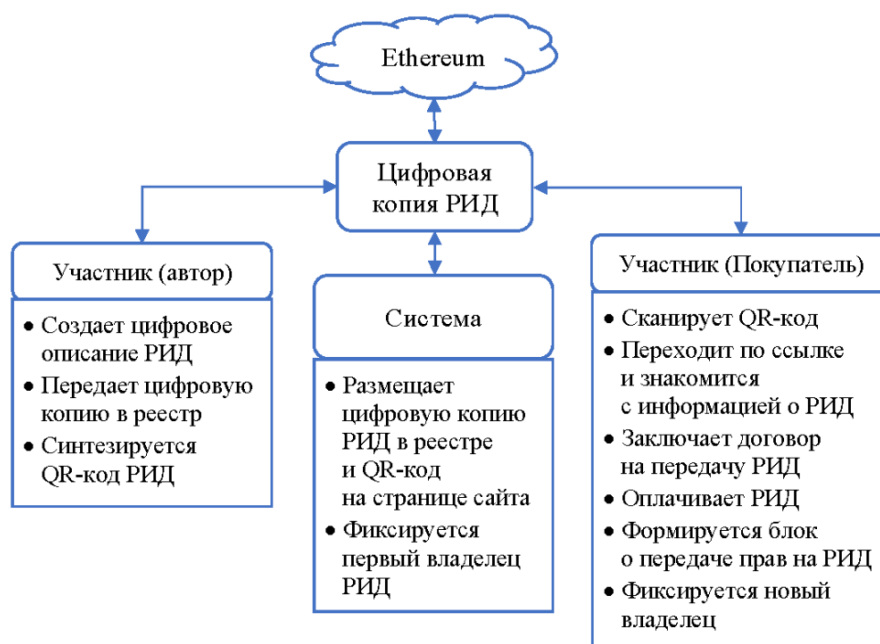


Рис. 2. Схема работы с РИД с помощью смарт-контракта

С помощью веб-приложения создается цифровое описание РИД и заносится в блокчейн. Согласно контракту, передать РИД в собственность другому лицу может только сторона, указанная в переменной «Текущий владелец» контракта. Цифровой копии РИД в блокчейне присваивается уникальный идентификатор в виде хэш-суммы файла, а также формируется QR-код для

отображения на веб-сайте и в мобильном приложении, который фактически реализует ссылку на страницу сайта с информацией о данной инновации.

Потенциальный покупатель может приобрести РИД через браузер или установленное мобильное приложение. При использовании мобильного приложения выполняется сканирование QR-кода, после чего выполняется переход на сайт с подробной информацией РИД, где можно посмотреть следующую информацию: автора РИД, всех последующих владельцев РИД, дату получения и регистрации РИД, информацию о полученном патенте (свидетельстве о регистрации), описание РИД и т.д. При передаче собственности вызывается функция, устанавливающая следующего потенциального владельца. Когда владелец принимает РИД в собственность, вызывается метод, подтверждающий право собственности нового владельца, информация о новом владельце добавляется в смарт-контракт, синтезируется блок с новой хэш-суммой. За проделанную операцию потенциальный покупатель также оплачивает комиссию.

4. Пример синтеза смарт-контракта

Для создания смарт-контрактов на основе блокчейн-платформы Ethereum требуются инструментальные средства: Node.js v6 + LTS, Git, Ganache, VisualStudio Code, Truffle и Web3.js. После установки данных компонент блокчейн-платформы выполняется инициализация фреймворка Truffle и создается конфигурационный файл `package.json` будущего проекта. Для работы веб-приложений развернут сервер OpenLiteSpeed, так как он более производителен, чем популярные серверы Apache и nginx. Разработка смарт-контрактов выполняется в среде IDE Remix, которая запускается в браузере и имеет режим эмуляции блокчейна, в которой можно запускать контракты, выполнять их отладку и тестирование. Для работы с рабочей версией смарт-контракта используется тестовый Ethereum клиент Ganache, а для взаимодействия с браузерами Firefox и Chrome – надстройка Metamask. После установки и конфигурирования инструментальных средств можно приступить к созданию смарт-контрактов. Совокупность смарт-контрактов алгоритмически в точности позволяет описывать бизнес-процессы взаимодействия субъектов инновационной деятельности при решении конкретных задач. В качестве примера приведем процесс контроля транзакций при создании РИД автором и передаче в собственность РИД посреднику (рис. 3).

Из рис. 3 видно, что для обеспечения контроля необходимо создать и отладить три базовых функции смарт-контракта: создание РИД, передачу РИД владельцу, подтверждение права собственности.

Зададим основные переменные для хранения информации в реестре:

- string manufacturer – создатель (автор) РИД;
- string customer – имя владельца;
- string[] customer – массив имен всех владельцев;
- address owner – адрес владельца;
- address[] owners – массив адресной информации владельцев РИД;
- currentOwner – текущий владелец РИД;
- nextOwner – следующий владелец РИД;
- string nameRID – название РИД;
- string model – цифровой паспорт РИД;

- int price – стоимость РИД;
- string createDate – дата создания РИД.

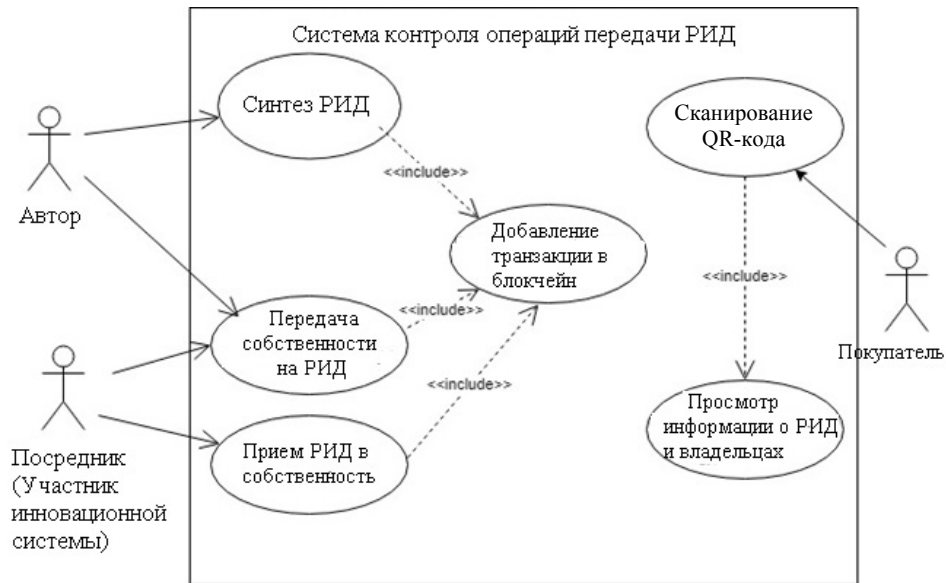


Рис. 3. Процесс синтеза и передачи РИД

Для создания РИД реализуется функция `RIDItem` с переменными, характеризующими РИД, такими как: название, автор, цифровой паспорт, стоимость, дата, адрес следующего владельца.

```
function RIDItem(string nameRID, string manufacturer, string model, int
price, string createDate, address nextOwner) public {
    _currentOwner = msg.sender;
    _customer.push(manufacturer);
    _nameRID = nameRID;
    _model = model;
    _color = color;
    _price = price;
    _createDate = createDate;
    _owners.push(msg.sender);
    _nextOwner = nextOwner;
}
```

После создания РИД и добавления в блокчейн передать права собственности может только текущий владелец (`currentOwner`) следующему владельцу (`nextOwner`) с помощью соответствующей функции.

```
function setNextOwner(address nextOwner) public returns(bool set) {
    if (_currentOwner != msg.sender) {
        return false;
    }
    _nextOwner = nextOwner;
    return true;
}
```

Первым текущим владельцем по умолчанию является автор (string manufacturer).

Последней функцией является подтверждение права собственности `confirmOwnership`, которая в качестве входной переменной берет имя нового владельца `string customer`:

```
function confirmOwnership(string customer) public returns(bool confirmed) {
    if (_nextOwner != msg.sender) {
        return false;
    }
    _owners.push(_nextOwner);
    _currentOwner = _nextOwner;
    _nextOwner = address(0);
    _customer.push(customer);
    return true;
}
```

В процессе подтверждения права в массив собственников `string[] customer` добавляется значение переменной `nextOwner`, а переменной `address owner` присваивается его адрес (если новый владелец неизвестен, то в переменную записывается нулевой адрес). В массив имен владельцев `string[] customer` добавляется имя нового владельца.

Для проверки подлинности передаваемой РИД в смарт-контракт необходимо добавить еще одну функцию получения списка всех предыдущих владельцев РИД.

```
function confirmOwnership(string customer) public returns(bool confirmed) {
    if (_nextOwner != msg.sender) {
        return false;
    }
    _owners.push(_nextOwner);
    _currentOwner = _nextOwner;
    _nextOwner = address(0);
    _customer.push(customer);
    return true;
}
```

Создаваемые контракты на языке Solidity версии 0.4.17 хранятся в виде файлов с расширением `.sol`. В одном файле можно размещать несколько связанных контрактов, каждый из которых имеет свои свойства и реализует алгоритмически связанные процедуры-функции. После создания функций смарт-контракта необходимо его скомпилировать и протестировать. Пример с результатами тестирования созданного смарт-контракта в среде IDE Remix показан на рис. 4.

После успешного тестирования смарт-контракт готов к размещению его в блокчейне и запуску. Для этого выполняется компиляция рабочей версии контракта с помощью инструмента Truffle. В результате получается JSON файл с метаданными и интерфейсом Application Binary Interface (ABI) для взаимодействия с библиотекой `web3.js`. Однако для работы с созданным смарт-контрактом необходим доступ к нему посредством веб-интерфейса, который включает веб-страницы с формами для ввода значений переменных и передачи процедурам-функциям. В приведенном примере это следующие html-страницы: создание РИД, передача РИД, подтверждение права на РИД и проверка подлинности РИД. С помощью библиотеки `web3.js` создаются обработчики событий, которые реализуют соответствующие функции смарт-контракта. Рассмотрим пример функции создания цифрового паспорта РИД.

The screenshot displays the Remix IDE interface during a smart contract deployment. The top panel shows the 'Environment' tab with details for a JavaScript VM, including an account (0xca3...a733c), gas limit (300,000), and value (0 wei). The 'Product' dropdown is set to 'Deploy'. The middle panel shows the 'Load contract from Address' field and a '0 pending transactions' status. The bottom panel is divided into two sections: the left shows the source code of the smart contract, and the right shows the transaction results.

Smart Contract Source Code:

```

22  _createDate = createDate;
23  _owners.push(msg.sender);
24  _nextOwner = nextOwner;
25  }
26  }
27  ~
28  ~
29  ~
30  ~
31  ~
32  ~
33  ~
34  ~
35  ~
36  ~
37  ~
38  ~
39  ~
40  ~
41  ~
42  ~
43  ~
44  ~
45  ~
46  ~
47  ~
48  ~
49  ~
50  ~
51  ~
52  ~
53  ~

```

Transaction Results:

The results section shows a list of transactions. The first transaction is a 'call' from 0xca3507d915458ef540ae606dfe2f44e8f73c to Product._currentOwner, with a gas cost of 2657a. Subsequent transactions show calls to Product._currentOwner, Product._nextOwner, and Product.setNextOwner, all with a gas cost of 59897. The final transaction is a 'call' from 0xca3507d915458ef540ae606dfe2f44e8f73c to Product._currentOwner, with a gas cost of 2657a.

Рис. 4. Результаты тестирования смарт-контракта

```

$("#makeRID").click(function() {
  var RIDContract = web3.eth.contract(abi);
  var RID = RIDContract.new(
    {
      from: web3.eth.accounts[0],
      data: '0x608060405234801561001057600080fd5b50611253806...',
      gas: '4700000'
    }, function (e, contract) {
      console.log(e, contract);
      if (typeof contract.address !== 'undefined') {
        console.log('Contract mined! address: ' + contract.address + ' transactionHash: ' + contract.transactionHash);
        addr=contract.address;
        var code="http://localhost:3000/check.html#" + addr;
        contract.RIDItem($("#nameRID").val(),$("#manufacturer").val(),$("#modelRID").val(),$("#priceRID").val(),String($("#createDate").val()),$("#nextOwner").val(),function(e,contract){
          $("#bigText").qrcode(code);
          console.log(e,contract);
        });
      }
    }
  );
});

```

Аналогично разрабатываются смарт-контракты для организации и взаимодействия участников инновационной системы.

Заключительным этапом разработки смарт-контракта является тестирование его рабочей версии в реальном блокчейне с помощью инструментов фреймворка Truffle:

- truffle/Assert.sol – проверяет различные утверждения;
- truffle/DeployedAddresses.sol – разворачивает новый экземпляр контракта, который тестируется в блокчейне;
- import "../contracts/Product.sol" – импортирует контракт, который необходимо протестировать;
- truffle compile – компилирует контракт и генерирует интерфейс;
- truffle migrate – выполняет миграцию контракта в сети;
- truffle test – запускает процесс тестирования.

Заключение

В статье рассмотрены инструменты создания смарт-контрактов и их развертывания в блокчейне для обеспечения надежного и безопасного взаимодействия участников региональных инновационных систем. В качестве базовой среды функционирования смарт-контрактов была выбрана платформа Ethereum, для работы с которой установлены и конфигурированы инструментальные средства, разработан веб-интерфейс для запуска функций контрактов. Приведен пример практической реализации четырех функций смарт-контракта по контролю за созданием и передачей РИД. В настоящее время ведутся работы над созданием серии смарт-контрактов, реализующих алго-

ритмы заключения договоров, проверки выполнения условий лицензионных договоров, обнаружения фактов нарушения лицензионных соглашений и авторских прав, оценки инновационного потенциала экономических агентов в регионе и т.д. Автоматизация процесса регионального управления инновациями с помощью смарт-контрактов поможет объединить авторов РИД и заинтересованных субъектов экономической деятельности, обеспечить безопасность и прозрачность их взаимодействия, координировать работу сторон при реализации инновационных проектов, что в конечном итоге приведет к снижению транзакционных издержек участников инновационной системы региона.

Библиографический список

1. **Кемпбелл, Э.** Стратегический синергизм / Э. Кемпбелл, К. Лачс. – СПб. : Питер, 2004. – 416 с.
2. **Гамидуллаева, Л. А.** О построении концепции управления инновационной системой России / Л. А. Гамидуллаева // Экономическое возрождение России. – 2016. – № 4 (50). – С. 74–84.
3. **Васин, С. М.** Development of Russian innovation system management concept / С. М. Васин, Л. А. Гамидуллаева // Инновации. – 2017. – № 5 (223). – С. 34–40.
4. **Финогеев, А. Г.** Моделирование и исследование системно-синергетических процессов в информационных средах : монография / А. Г. Финогеев. – Пенза : Изд-во ПГУ, 2004. – 223 с.
5. **Финогеев, А. Г.** Технология смарт контрактов на основе блокчейн для минимизации транзакционных издержек в региональных инновационных системах / А. Г. Финогеев, С. М. Васин, Л. А. Гамидуллаева, А. А. Финогеев // Вопросы безопасности. – 2018. – № 3. – URL: http://e-notabene.ru/nb/article_26619.html. – DOI 10.25136/2409-7543.0.0.26619.
6. **Swan, M.** Blockchain: Blueprint for a New Economy / M. Swan. – Sebastopol : O'Reilly Media, Inc., 2015. – 152 p.
7. **Franco, P.** The Blockchain / P. Franco // Understanding Bitcoin: Cryptography, Engineering and Economics. – New York : John Wiley & Sons, 2014. – 288 p.
8. **Andreas, M.** Antonopoulos. 7. The Blockchain / M. Andreas // Mastering Bitcoin. – Sebastopol : O'Reilly Media, Inc., 2014.
9. Сергей Матвеев: блокчейн обеспечит ученым справедливое вознаграждение. – URL: <https://4science.ru/articles/Sergei-Matveev-blokchein-obspechit-uchenim-spravedlivoe-voznagrazhdenie> (дата обращения: 10.06.18).
10. Сайт компании Ascribe. – URL: <https://www.ascribe.io/> (дата обращения: 10.06.18).
11. Сеть IPchain. – URL: <http://ipchain.ru> (дата обращения: 10.06.18).
12. **Szabo, N.** Smart Contracts: Formalizing and Securing Relationships on Public Networks / N. Szabo // First Monday. – 1997. – 1 September. – Vol. 2, № 9. – URL: <http://firstmonday.org/ojs/index.php/fm/article/view/548/469> (дата обращения: 10.06.18).
13. **Tar, A.** Smart Contracts, Explained. Partnership Material / A. Tar. – URL: <https://cointelegraph.com/explained/smart-contracts-explained> (дата обращения: 10.06.18).
14. Децентрализованные платформы для смарт-контрактов: вызовы и решения. – URL: <https://forklog.com/detsentralizovannye-platformy-dlya-smart-kontraktov-vyzovy-i-resheniya/> (дата обращения: 10.06.18).
15. Блокчейн платформы. – URL: <http://smart-contracts.ru/platforms.html> (дата обращения: 10.06.18).
16. Платформа Ethereum. – URL: <https://www.ethereum.org/> (дата обращения: 10.06.18).
17. Язык Solidity. – URL: <http://solidity.readthedocs.io/en/v0.4.24/> (дата обращения: 10.06.18).

18. Платформа Aeternity. – URL: <https://aeternity.com/> (дата обращения: 10.06.18).
19. Poon, J. The Bitcoin Lightning Network: scalable off-chain instant payments / J. Poon, Thaddeus Dryja. – 2016. – URL: <http://lightning.network/lightning-network-paper.pdf> (дата обращения: 10.06.2018).
20. Платформа Hyperledger Fabric. – URL: <http://hyperledger-fabric.readthedocs.io/en/release-1.1/> (дата обращения: 10.06.2018).
21. Платформа Cardano. – URL: <https://www.cardano.org/en/home/> (дата обращения: 10.06.2018).

References

1. Kempbell E., Lachs K. *Strategicheskiiy sinergizm* [Strategic synergy]. Saint-Petersburg: Piter, 2004, 416 p.
2. Gamidullaeva L. A. *Ekonomicheskoe vrozozhdenie Rossii* [Economic revival of Russia]. 2016, no. 4 (50), pp. 74–84.
3. Vasin S. M., Gamidullaeva L. A. *Innovatsii* [Innovations]. 2017, no. 5 (223), pp. 34–40.
4. Finogeev A. G. *Modelirovanie i issledovanie sistemno-sinergeticheskikh protsessov v informatsionnykh sredakh: monografiya* [Modeling and research of system-sinergetic processes in informational spheres: monograph]. Penza: Izd-vo PGU, 2004, 223 p.
5. Finogeev A. G., Vasin S. M., Gamidullaeva L. A., Finogeev A. A. *Voprosy bezopasnosti* [Security issues]. 2018, no. 3. Available at: http://e-notabene.ru/nb/article_26619.html. DOI 10.25136/2409-7543.0.0.26619.
6. Swan M. *Blockchain: Blueprint for a New Economy*. Sebastopol: O'Reilly Media, Inc., 2015, 152 p.
7. Franco P. *Understanding Bitcoin: Cryptography, Engineering and Economics*. New York: John Wiley & Sons, 2014, 288 p.
8. Andreas M. *Mastering Bitcoin*. Sebastopol: O'Reilly Media, Inc., 2014.
9. Sergey Matveev: *blokcheyn obespechit uchenym spravedlivoie voznagrashdenie* [Sergey Matveev: blockchain will insure scientists fair remuneration]. Available at: <https://4science.ru/articles/Sergei-Matveev-blokchein-obespechit-uchenim-spravedlivoie-voznagrashdenie> (accessed Jun. 10, 18).
10. *Sayt kompanii Ascribe* [Ascribe company site]. Available at: <https://www.ascribe.io/> (accessed Jun. 10, 18).
11. *Set' IPchain*. Available at: <http://ipchain.ru> (accessed Jun. 10, 18).
12. Szabo N. *First Monday*. 1997, 1 Sept., vol. 2, no. 9. Available at: <http://firstmonday.org/ojs/index.php/fm/article/view/548/469> (accessed Jun. 10, 18).
13. Tar A. *Smart Contracts, Explained. Partnership Material*. Available at: <https://coin-telegraph.com/explained/smart-contracts-explained> (accessed Jun. 10, 18).
14. *Detsentralizovannyye platformy dlya smart-kontraktov: vyzovy i resheniya* [Decentralized platforms for smart-contracts: challenges and solutions]. Available at: <https://forklog.com/detsentralizovannyye-platformy-dlya-smart-kontraktov-vyzovy-i-resheniya/> (accessed Jun. 10, 18).
15. *Blokcheyn platformy*. Available at: <http://smart-contracts.ru/platforms.html> (accessed Jun. 10, 18).
16. *Platforma Ethereum*. Available at: <https://www.ethereum.org/> (accessed Jun. 10, 18).
17. *Yazyk Solidity* [Solidity language]. Available at: <http://solidity.readthedocs.io/en/v0.4.24/> (accessed Jun. 10, 18).
18. *Platforma Aeternity* [Aeternity platform]. Available at: <https://aeternity.com/> (accessed Jun. 10, 18).
19. Poon J., Thaddeus Dryja *The Bitcoin Lightning Network: scalable off-chain instant payments*. 2016. Available at: <http://lightning.network/lightning-network-paper.pdf> (accessed Jun. 10, 18).
20. *Platforma Hyperledger Fabric*. Available at: <http://hyperledger-fabric.readthedocs.io/en/release-1.1/> (accessed Jun. 10, 18).

21. *Platforma Cardano* [Cardano platform]. Available at: <https://www.cardano.org/en/home/> (accessed Jun. 10, 18).

Финогеев Алексей Германович

доктор технических наук, профессор,
кафедра систем автоматизированного
проектирования, Пензенский
государственный университет
(Россия, г. Пенза, ул. Красная, 40)

E-mail: bam@pnzgu.ru

Finogeev Aleksey Germanovich

Doctor of engineering sciences, professor,
sub-department of CAD, Penza State
University (40 Krasnaya street, Penza,
Russia)

Гамидуллаева Лейла Айваровна

кандидат экономических наук, доцент,
кафедра менеджмента и экономической
безопасности, Пензенский
государственный университет
(Россия, г. Пенза, ул. Красная, 40)

E-mail: gamidullaeva@gmail.com

Gamidullaeva Leyla Ayvarovna

Candidate of economic sciences, associate
professor, sub-department of management
and economic security, Penza State
University (40 Krasnaya street, Penza,
Russia)

Васин Сергей Михайлович

доктор экономических наук, профессор,
кафедра экономической теории
и международных отношений,
Пензенский государственный
университет (Россия, г. Пенза,
ул. Красная, 40)

E-mail: pspu-met@mail.ru

Vasin Sergey Mikhaylovich

Doctor of economic sciences, professor,
sub-department of economics and
international relations, Penza State
University (40 Krasnaya street, Penza,
Russia)

Финогеев Антон Алексеевич

кандидат технических наук, доцент,
кафедра систем автоматизированного
проектирования, Пензенский
государственный университет
(Россия, г. Пенза, ул. Красная, 40)

E-mail: fanton3@ya.ru

Finogeev Anton Alekseevich

Candidate of engineering sciences,
associate professor, sub-department
of CAD, Penza State University
(40 Krasnaya street, Penza, Russia)

Проницев Владислав Викторович

магистрант, Пензенский государственный
университет (Россия, г. Пенза,
ул. Красная, 40)

E-mail: vvp-5553233@mail.ru

Pronichev Vladislav Viktorovich

Master's degree student, Penza State
University (40 Krasnaya street, Penza,
Russia)

Лычагин Кирилл Анатольевич

аспирант, Пензенский государственный
университет (Россия, г. Пенза,
ул. Красная, 40)

E-mail: klychagin@ec-leasing.ru

Lychagin Kirill Anatol'evich

Postgraduate student, Penza State
University (40 Krasnaya street, Penza,
Russia)

УДК 334.021.1

Смарт-контракты как инструментальный безопасного взаимодействия субъектов региональной инновационной системы / А. Г. Финогеев, Л. А. Гамидуллаева, С. М. Васин, А. А. Финогеев, В. В. Проничев, А. М. Лычагин // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2018. – № 3 (47). – С. 139–157. – DOI 10.21685/2072-3016-2018-3-15.