А. А. Баринова, С. В. Запечников
Национальный исследовательский ядерный университет «МИФИ», Каширское шоссе, 31, г. Москва, 115409, Россия,
e-mail: naicqa@yandex.ru, ORCID iD 0000-0002-3784-6224,
e-mail: SVZapechnikov@mephi.ru , ORCID iD 0000-0002-7975-6040

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ СМАРТ-КОНТРАКТОВ

DOI: http://dx.doi.org/10.26583/bit.2017.2.02

Аннотация. В настоящее время наблюдается тенденция качественного и количественного усложнения бизнес-процессов. Электронная форма обмена информацией становится преобладающим средством коммуникаций, а также одним из основных элементов обеспечивающей инфраструктуры для бизнес-процессов. Эти обстоятельства обеспечивают необходимость внедрения электронных смарт-контрактов («умных контрактов») – протоколов, которые описывают набор условий и автоматически следят за их выполнением. Наиболее важным требованием к подобным технологиям является обеспечение конфиденциальности данных. В данной работе были исследованы наиболее известные платформы конфиденциальных электронных контрактов, выявлены методы обеспечения конфиденциальности, критерии их сравнения, проведено сравнение по выделенным критериям и сформулированы выводы о требованиях к платформам электронных контрактов, обеспечивающих конфиденциальность.

Ключевые слова: смарт контракты, блокчейн, конфиденциальность

Для цитирования. **БАРИНОВА, Анастасия А.; ЗАПЕЧНИКОВ, Сергей В.** Методы и средства обеспечения конфиденциальности смарт-контрактов. Безопасность информационных технологий, [S.l.], v. 24, n. 2, p. 16-23, june 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/101>. Дата доступа: 13 dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.2.02..

Anastasia A. Barinova, Sergey V. Zapechnikov
National Research Nuclear University MEPHI, Kashirskoe sh., 31, Moscow, 115409, Russia,
e-mail: naicqa@yandex.ru, ORCID iD 0000-0002-3784-6224,
e-mail: SVZapechnikov@mephi.ru , ORCID iD 0000-0002-7975-6040

On the techniques and tools for privacy-preserving smart contracts

DOI: http://dx.doi.org/10.26583/bit.2017.2.02

Abstract. Currently business processes become more and more complicated. Data used in these processes circulates mainly through the digital communications. Due to these conditions some kind of electronic contracts for business deals become necessary. Smart contracts should describe a set of conditions, implemented through some events in the real world and digital systems. The most important requirement for this technology is privacy ensuring. In this work we have explored existing projects of privacy-preserving smart contracts defined comparison criteria compared projects and made a conclusion about options required for smart contract frameworks.

Keywords: smart contracts, privacy, blockchain

For citation. **BARINOVA, Anastasia A.; ZAPECHNIKOV, Sergey V.** On the Techniques and Tools for Privacy-Preserving Smart Contracts. IT Security (Russia), [S.l.], v. 24, n. 2, p. 16-23, June 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/101>. Date accessed: 13 Dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.2.02.

Введение

Усложнение бизнес-процессов в современном мире влечет за собой необходимость формирования четкого и справедливого аппарата их регулирования, который обеспечит

отсутствие возможности вмешательства третьих лиц в выполнение контракта и снизит риски неоднозначных трактовок условий контракта [1].

Идея внедрения подобной технологии, получившей название смарт-контракт («умный контракт», интеллектуальный контракт), была впервые предложена американским программистом Ником Сабо в 1994 году [2]. Однако для ее практической реализации не существовало необходимых технологических средств.

В связи с активным развитием технологий децентрализованных сетей стало возможным создание платформ для реализации и выполнения смарт-контрактов [3]. Крупные научно-исследовательские центры, университеты и отдельные команды энтузиастов разработали целый ряд платформ смарт-контрактов: Ethereum, Counterparty, Enigma и др. Однако они не решали одну из основных проблем смарт-контрактов: учитывая тот факт, что при заключении и выполнении контрактов стороны зачастую предоставляют множество персональных данных и (или) данных, составляющих коммерческую тайну, одним из важнейших требований к платформам смарт-контрактов является обеспечение конфиденциальности данных. Это требование обуславливает актуальность проблемы обеспечения конфиденциальности смарт-контрактов. В то же время все ранее известные платформы смарт-контрактов основывались на технологии распределенного нередактируемого реестра – блокчейн, который является открытым и доступен всем членам сети. Следовательно, ни о какой конфиденциальности данных говорить в таком случае не приходится.

Технологии распределенного нередактируемого реестра и смарт-контрактов

Для рассмотрения вопросов обеспечения конфиденциальности смарт-контрактов, необходимо выявить основные особенности тех технологий, на которых они основываются, – технологии распределенного нередактируемого реестра, или блокчейна, и классической технологии смарт-контрактов.

Технология распределенного нередактируемого реестра позволяет пользователям взаимодействовать друг с другом в децентрализованной среде без необходимости взаимного доверия и участия третьих лиц [3]. Каждый узел сети обладает специальным реестром («ledger»), который представляет собой полную копию с записями всех транзакций, проводимых участниками сети. Записи в реестр можно вносить лишь с согласия большинства пользователей, а однажды записанная информация не может быть удалена или модифицирована [4]. В реестре данные группируются в блоки, которые, в свою очередь, формируют цепочки блоков – отсюда и название блокчейн (blockchain) – буквально «цепочка блоков». Блоки в распределенном реестре связаны с помощью хэш-кодов, поскольку в заголовке каждого последующего блока хранится хэш-код предыдущего блока. Именно это техническое решение обеспечивает защищенность и устойчивость реестра к несанкционированному редактированию [5].

Смарт-контракт – это часть прикладной программы, которая хранит правила согласования условий контракта, автоматически следит за исполнением контракта и выполняет установленные условия контракта [6].

Основная идея смарт-контракта заключается в том, что договорное управление той или иной сделкой между двумя или более сторонами может осуществляться автоматически (программным способом) через распределенный реестр, и для этого не требуется привлечение какой-либо доверенной третьей стороны (ДТС): арбитра либо третейского судьи [7].

Таким образом решаются проблемы традиционного договорного права — зависимость сторон контракта от ДТС, а также временные и материальные затраты на коммуникации между сторонами контракта и ДТС.

Смарт-контракт реализует получение и отправку любых данных пользователей (“value”) с помощью транзакций, а также изменение своего внутреннего состояния (“state”) посредством событий (рис. 1).

В идеале смарт-контракт должен выполняться в среде, которая позволяет полностью автоматизировать процесс его выполнения, то есть в среде, имеющей беспрепятственный доступ исполняемого кода к объектам договоренностей, фигурирующим в тексте (условиях) смарт-контракта [8]. Следовательно, все условия такого смарт-контракта должны иметь четкое логико-математическое описание.

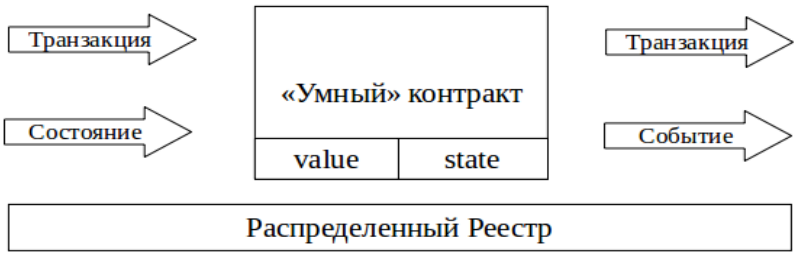

Рис. 1. Общая схема функционирования смарт-контракта
Fig. 1. The General scheme of the functioning of the smart-contract

Платформы конфиденциальных смарт-контрактов

Благодаря многочисленным исследованиям в области обеспечения конфиденциальности при заключении смарт-контрактов многими университетами и научными центрами за последние годы были запущены первые проекты, реализующие эту технологию.

Рассмотрим основные идеи двух наиболее интересных проектов — платформы Hawk, созданной на базе Мэрилендского и Корнельского университетов (США), а также платформы Enigma, реализованной исследователями из Массачусетского технологического института (США).

Платформа Hawk. Основная идея, положенная в основу платформы конфиденциальных смарт-контрактов Hawk, заключается в трансляции с помощью собственного компилятора обычной программы смарт-контракта в криптографический протокол взаимодействия пользователей с распределенным реестром [9].

Откомпилированная программа Hawk состоит из двух частей: открытой и закрытой (рис. 2). Закрытая часть непосредственно взаимодействует с данными пользователей, а также проводит вычисления для определения выплат между сторонами контракта. Ее главная функция — обеспечить защищенность данных пользователей, а также денежных потоков. Открытая программная часть не осуществляет взаимодействие с данными пользователей.

Выполнение программы смарт-контракта контролируется специальной стороной, называемой менеджером, который имеет доступ к пользовательским входным данным и обязан не разглашать их [9]. Однако очень важно отметить, что менеджер не соотносится с понятием ДТС — даже в том случае, если менеджер произвольно отклоняется от выполнения протокола либо вступает в сговор с одной из сторон, он не может повлиять на корректность исполнения контракта. В случае прерывания контракта менеджером он будет финансово наказан [10]. Каждая программа на платформе Hawk при работе использует показания специального таймера, который определяет время и очередность наступления событий.

Конфиденциальность контрактов на платформе Hawk обеспечивается за счет следующих особенностей.

1. Обеспечивается конфиденциальность данных каждого отдельно взятого контракта по отношению к внешней среде. Несмотря на то, что стороны контракта обмениваются

данными с реестром, денежные потоки и данные транзакций из закрытой части программы контракта защищены от внешней среды криптографическими методами. В распределенный реестр направляется зашифрованная информация, а доказательство с нулевым разглашением [11] обеспечивает соблюдение корректности выполнения контракта и взаимодействия с данными [10].

2. Обеспечивается конфиденциальность данных внутри одного контракта. Платформа Hawk предполагает, что стороны контракта защищают свои собственные финансовые интересы. В частности, они могут произвольно отклоняться от определенного протокола либо преждевременно прерывать контракт. При этом Hawk обеспечивает не только конфиденциальность и аутентичность данных пользователей, но и финансовую справедливость в случае прерывания сделок. Это достигается с помощью специального механизма возврата денежных средств после достижения определенных временных меток [10].

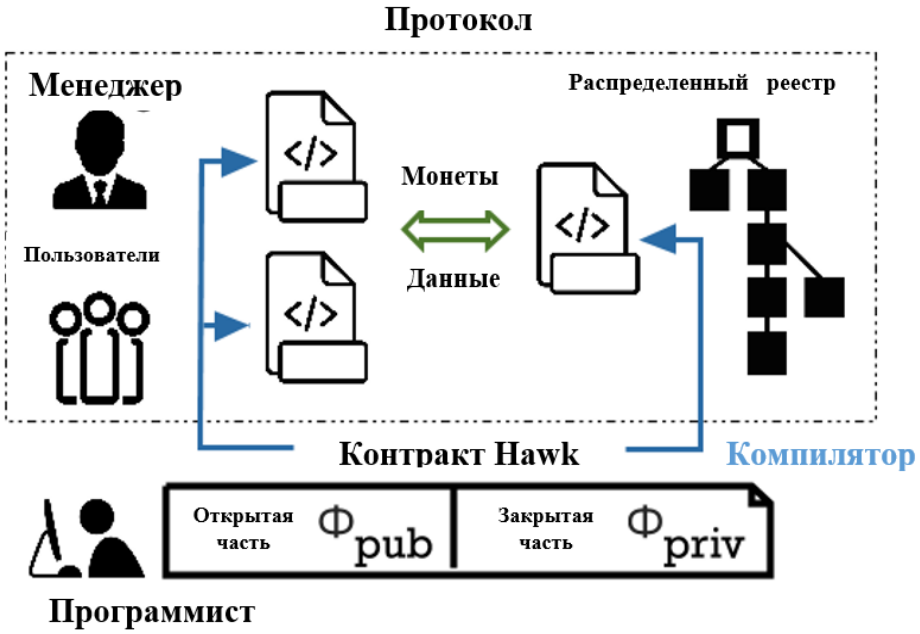

Рис. 2. Схема работы программы Hawk (по материалам [10])
Fig. 2. A scheme of the Hawk program functioning [10]

Платформа Enigma. Эта платформа позиционируется разработчиками как распределенная вычислительная платформа с гарантированным обеспечением конфиденциальности [12]. Основные свойства, которые обеспечивает платформа, заключаются в следующем.

1. *Конфиденциальность*. С помощью безопасных распределенных вычислений (sMPC — secure multi-party computation) работа с данными на этой платформе осуществляется вообще без участия ДТС. Данные разделяются между узлами сети, и те выполняют операции лишь со своей частью данных, которая представляет собою лишь бессмысленный фрагмент [12].

2. *Масштабируемость*. В отличие от традиционной формы распределенного реестра, вычисления, необходимые при выполнении контракта, не дублируются в каждом узле сети. Точно так же не дублируются многократно и данные, участвующие в выполнении контракта. Кроме того, это позволяет платформе Enigma выполнять вычисления над зашифрованными данными контракта без доступа к открытому тексту.

Интерпретатор разбивает процесс выполнения конфиденциального контракта, как показано на рис. 3, позволяя уменьшить время выполнения и при этом сохранив конфиденциальность [13].

Собственное хранилище данных Enigma осуществляет взаимодействие с распределенным реестром посредством использования схем разделения секрета и распределенных вычислений (рис. 4). Для этого вне блокчейна используется распределенная хэш-таблица (Distributed Hash Table – DHT) [14], которая доступна через реестр. При этом в реестре хранятся уже не сами данные, а ссылки на них. Личные данные должны быть зашифрованы на клиентской стороне перед началом взаимодействия с хранилищем и выполнением протоколов доступа [13].

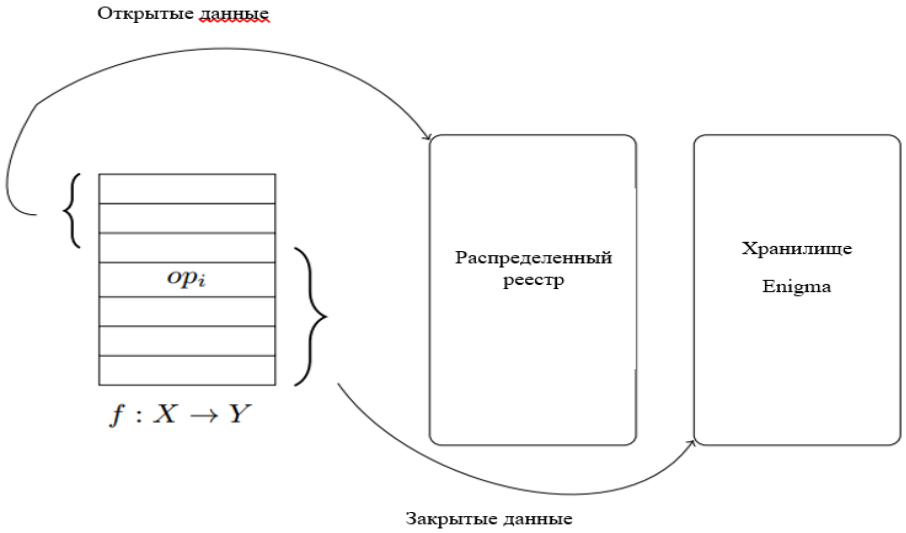

Рис. 3. Схема функционирования платформы распределенного реестра Enigma
Fig. 3. The scheme of functioning of the distributed registry platform Enigma

На сетевом уровне хранилище работает по протоколу Kademlia DHT [15] с использованием широковещательных каналов связи и схем шифрования с открытым ключом.

Сеть, построенная на базе Enigma, может выполнять код без утечки исходных данных к какому-либо узлу сети с помощью схемы линейного разделения секрета [13]. Для безопасных распределенных вычислений необходимо, чтобы каждый узел сети взаимодействовал с другим с коммуникационной сложностью$O(n^2)$ и с постоянным числом раундов. В случае линейных схем разделения секрета [16] эта вычислительная сложность в основном обусловлена операциями умножения, в то время как операции сложения могут выполняться параллельно, без обмена данными [12].

Сравнение платформ конфиденциальных смарт-контрактов

Сравнение двух платформ конфиденциальных смарт-контрактов – Hawk и Enigma – позволяет сделать следующие основные выводы.

1. Используемый платформой Hawk механизм доказательств с нулевым разглашением является более пригодным для использования в качестве средства обеспечения конфиденциальности по сравнению со схемой линейного разделения секрета в сочетании с безопасными распределенными вычислениями на платформе Enigma, так как доказательство с нулевым разглашением является широко апробированным и легко реализуемым криптографическим примитивом.

2. Принципиальная схема создания и выполнения контракта в реализациях Hawk и Enigma совпадает: контракт программируется, создается криптографические и иные протоколы его выполнения и взаимодействия пользователей, после чего он выполняется. Однако на каждом этапе этого процесса различаются используемые методы. В схеме Hawk контракт после создания выполняется в распределенном реестре, в то время как в схеме Enigma контракт выполняется распределенным образом и в двух местах: распределенном

реестре и хранилище Enigma. На стадии выполнения контракта Hawk большую роль играет специальный участник сети — менеджер, который обеспечивает корректное выполнение контракта, проводит основные операции с криптовалютой, отправляет данные пользователей в распределенный реестр и получает данные из него. В платформе Enigma выполнение контракта и гарантия его корректного исполнения обеспечивается за счет распределенных вычислений и специального протокола , который сопровождает такие вычисления.

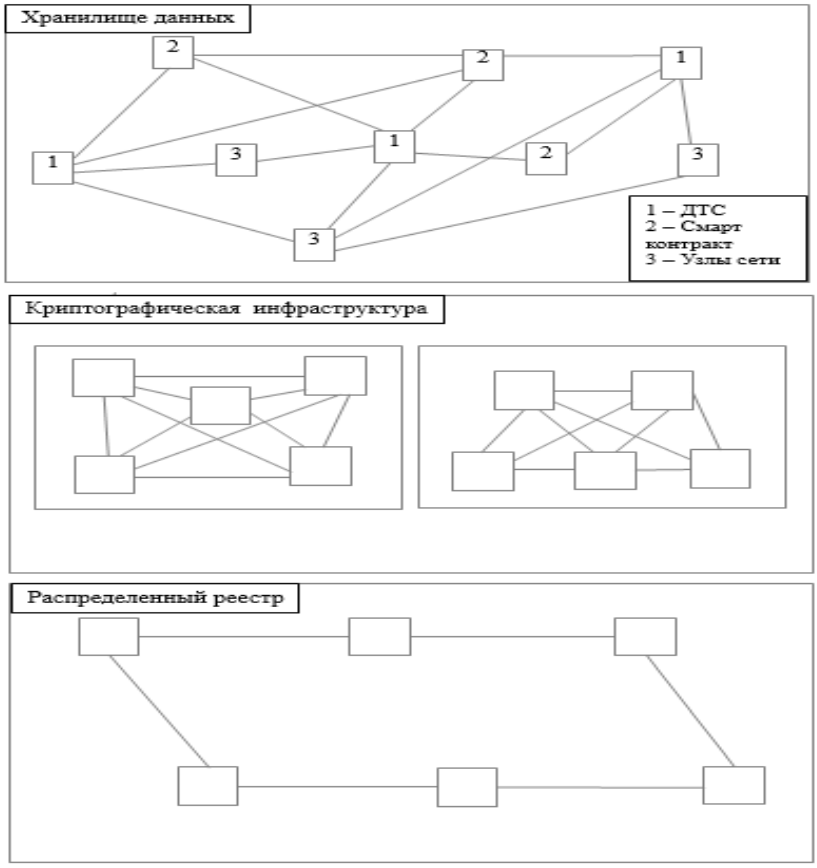

Рис. 4. Архитектура платформы Enigma (по материалам [17])
Fig. 4. The architecture of the platform Enigma [17]

3. В отличие от схемы хранения данных в платформе Hawk, схемы Enigma не предполагает стандартного хранения данных – дублирования данных реестра у каждого участника сети. Данный факт позволяет повысить производительность работы платформы Enigma за счет схемы доступа к данным через распределенный реестр и распределенную хэш-таблицу (DHT).

4. В отличие от платформы Enigma, контракты на платформе Hawk могут программироваться и сопровождаться людьми, не имеющими знаний в сфере криптографии и программирования.

5. Финансовая справедливость достигается в обеих схемах. Платформа Hawk использует для этого специальные временные метки и таймеры, которые определяют события в системе и контролируют наступление новых. Платформа Enigma реализует эти характеристики за счет распределенных вычислений.

Заключение

В результате данной работы:

- проведен обзор на наиболее известные платформы смарт-контрактов, обеспечивающих конфиденциальность, Hawk и Enigma;
- исследованы возможности обеспечения конфиденциальности смарт-контрактов в проектах Enigma и Hawk и их детальный анализ;
- выявлены основные методы реализации распределенного реестра, смарт-контракта;
- проведено сравнение платформ по выделенным критериям;

На основании сравнения сформулированы выводы, позволяющие выделить критерии, необходимые для проектирования и разработки платформы смарт-контрактов.

СПИСОК ЛИТЕРАТУРЫ:

1. «Умные» контракты и современное договорное право. [Электронный ресурс]. — Режим доступа к ресурсу: https://zakon.ru/blog/2016/8/12/umnye_kontrakty_i_sovremennoe_dogovornoe_pravo. (Дата обращения: 12.12.16)
2. Smart Contracts: The Blockchain Technology That Will Replace Lawyers. [Электронный ресурс]. — Режим доступа к ресурсу: http://blockgeeks.com/guides/smart-contracts/ (Дата обращения: 09.11.2016)
3. Blockchain [Электронный ресурс]. — Режим доступа к ресурсу: http://www.investopedia.com/terms/b/blockchain.asp (Дата обращения: 27.10.2016)
4. The world is now open for business. [Электронный ресурс]. — Режим доступа к ресурсу: https://www.blockchain.com (Дата обращения: 17.01.17)
5. Перевернуть мир. Разработка уникального решения на основе технологии блокчейн. [Электронный ресурс]. — Режим доступа к ресурсу: https://yadi.sk/i/6Axqh0-ipjdHw (Дата обращения: 09.12.2016)
6. Smart Contracts Explained [Электронный ресурс]. — Режим доступа к ресурсу: http://www.blockchaintechnologies.com/blockchain-smart-contracts (Дата обращения: 13.12.2016)
7. Умные контракты (Четвертая революция стоимости). [Электронный ресурс]. — Режим доступа к ресурсу: http://old.computerra.ru/1998/266/194332/ (Дата обращения: 21.01.17)
8. Умные контракты помогут государствам принять криптовалюты. [Электронный ресурс]. — Режим доступа к ресурсу: http://ensrationis.com/умные-контракты-помогут-государства/ (Дата обращения: 23.10.16)
9. Ahmed Kosba. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts/ Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, Charalampos Papamanthou; University of Maryland. — 2016. — С. 1-31
10. Guy Zyskind. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts/ Guy Zyskind, Oz Nathan, Alex Pentland; MIT Living Lab. — 2015. — С. 1-10
11. Венбо, Мао Современная криптография: теория и практика, 2005. — 677 с.
12. Enigma: Decentralized Computation Platform with Guaranteed Privacy [Электронный ресурс]: — Режим доступа к ресурсу: http://enigma.media.mit.edu/enigma_full.pdfpdf (Дата обращения: 10.10.2016)
13. Blockchain Enigma. Paradox. Opportunity [Электронный ресурс]. — Режим доступа к ресурсу: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf (Дата обращения 17.12.16)
14. Distributed Hash Tables [Электронный ресурс]. — Режим доступа к ресурсу: https://www.cs.cmu.edu/~dga/15-744/S07/lectures/16-dht.pdf (Дата обращения: 12.01.17)
15. Децентрализованные сети: Kademlia DHT protocol [Электронный ресурс]. — Режим доступа к ресурсу: https://habrahabr.ru/post/107342/ (Дата обращения: 14.12.2016)
16. Shamir’s Secret Sharing Scheme [Электронный ресурс]. — Режим доступа к ресурсу: http://point-at-infinity.org/ssss/ (Дата обращения: 20.11.2016)
17. Blockchain and Health IT [Электронный ресурс]. — Режим доступа к ресурсу: https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf (Дата обращения: 23.01.17)

REFERENCES:

[1]. "Smart" contracts and modern contractual right [Electronic resource]. — Resource access mode: https://zakon.ru/blog/2016/8/12/umnye_kontrakty_i_sovremennoe_dogovornoe_pravo (Date of reference: 12.12.16) (in Russian).
[2]. Smart contract [Electronic resource]. — Resource access mode: http://blockgeeks.com/guides/smart-contracts/ (Date of reference: 09.11.2016)
[3]. Blockchain [Electronic resource]. — Resource access mode: http://www.investopedia.com/terms/b/blockchain.asp (Date of reference: 27.10.2016)
[4]. The world is now open for business [Electronic resource]. — Resource access mode: https://www.blockchain.com (Date of reference: 17.01.17)

[5]. To change the world. Development of unique solutions based on blockchain technology [Electronic resource]. — Resource access mode: https://yadi.sk/i/6Axqh0-ipjdHw (Date of reference: 09.12.2016) (in Russian).
[6]. Smart Contracts Explained [Electronic resource]. — Resource access mode: http://www.blockchaintechnologies.com/blockchain-smart-contracts (Date of reference: 13.12.2016)
[7]. Smart contracts (Fourth revolution value). [Electronic resource]. — Resource access mode: http://old.computerra.ru/1998/266/194332/ (Date of reference: 21.01.17) (in Russian).
[8]. Smart contracts will enable States to accept the cryptocurrency. [Electronic resource]. — Resource access mode: http://ensrationis.com/умные-контракты-помогут-государства/ (Date of reference: 23.10.16) (in Russian).
[9]. Ahmed Kosba. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts/ Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, Charalampos Papamanthou; University of Maryland. — 2016. — P. 1-31
[10]. Guy Zyskind. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts/ Guy Zyskind, Oz Nathan, Alex Pentland; MIT Living Lab. — 2015. — C. 1-10
[11]. Mao V. Modern Cryptography: Theory and Practice. 2005. 677 p.
[12]. Enigma: Decentralized Computation Platform with Guaranteed Privacy [Electronic resource]: — Resource access mode: http://enigma.media.mit.edu/enigma_full.pdfpdf (Date of reference: 10.10.2016).
[13]. Blockchain Enigma. Paradox. Opportunity [Electronic resource]. — Resource access mode: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf (Date of reference: 17.12.16).
[14]. Distributed Hash Tables [Electronic resource]. — Resource access mode: https://www.cs.cmu.edu/~dga/15-744/S07/lectures/16-dht. (Date of reference: 12.01.17).
[15]. Decentralized network. Kademlia dht protocol [Electronic resource]. — Resource access mode: https://habrahabr.ru/post/107342/ (Date of reference: 14.12.2016) (in Russian).
[16]. Shamir's Secret Sharing Scheme [Electronic resource]. — Resource access mode: http://point-at-infinity.org/ssss (Date of reference: 20.11.2016).
[17]. Blockchain and Health IT [Electronic resource]. — Resource access mode: https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf (Date of reference: 23.01.17).

Поступила в редакцию – 26 января 2017 г. Окончательный вариант – 20 мая 2017 г.
Received – January 26, 2017. The final version – May 20, 2017.