А.В. КУРБЕСОВ,
к.э.н., Ростовский государственный экономический университет (РИНХ), г. Ростов-на-Дону, Россия,
e-mail: akurbesov@yandex.ru
И.И. МИРОШНИЧЕНКО,
к.э.н., Ростовский государственный экономический университет (РИНХ), г. Ростов-на-Дону, Россия,
e-mail: iimo2@yandex.ru

О ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН ПРИ РЕГИСТРАЦИИ ГРАЖДАН В СИСТЕМЕ МЕДИЦИНСКОГО СТРАХОВАНИЯ

УДК 614.1, 004.02

Курбесов А.В., Мирошниченко И.И. ***О возможности применения технологии блокчейн при регистрации граждан в системе медицинского страхования*** *(Ростовский государственный экономический университет (РИНХ), г. Ростов-на-Дону, Россия)*

Аннотация. В работе предложены требования, которые могут быть предъявлены к информационным системам, задействованным в процессе регистрации граждан в системе медицинского страхования. Обоснована возможность и целесообразность использования технологии блокчейн для успешного осуществления указанных процессов.

Ключевые слова: *медицинская организация, страховая медицинская организация, блокчейн, децентрализованное приложение.*

UDC 614.1, 004.02

Kurbesov A.V., Miroshnichenko I.I. ***On the possibility of using blockchain technology in the registration of citizens in the health insurance system*** *(Rostov State University of Economics (RINH), Rostov-on-Don, Russia)*

Abstract. The paper proposes the requirements that can be presented to the information systems involved in the process of registration of citizens in the health insurance system. The possibility and expediency of using blockchain technology for the successful implementation of these processes are substantiated.

Keywords: *medical organization, medical insurance organization, blockchain, decentralized application.*

Введение

Появление технологии распределенного реестра и децентрализованного хранения информации (блокчейн) ставит вопрос о необходимости обоснования адекватности проблемной области для применения указанной технологии [2, 7, 9]. Стоимость и трудоемкость решений, использующих технологию блокчейн, достаточно велика, и нужна тщательная проработка вопроса необходимости перехода на эту технологию в той или иной отрасли [10–16]. Следует учесть, что в настоящее время почти все сферы деятельности людей в той или иной степени уже автоматизированы, поэтому оценки полезности перехода, его стоимости и соответствия решаемой задаче должны быть рассмотрены в сравнении с уже использующимися решениями [5–6, 8]. В работе мы хотим рассмотреть задачу о применимости технологии блокчейн в процессе информатизации процедуры выдачи полисов в системе обязательного медицинского страхования.

Цель исследования

Рассмотрение возможности и целесообразности использования технологии блокчейн при автоматизации процессов обращения полисов обязательного медицинского страхования.

© А.В. Курбесов, И.И. Мирошниченко, 2019 г.

Методы

Анализ процессов выписки, корректировки и аннулирования основного документа системы обязательного медицинского страхования (ОМС) – полиса застрахованного, а также методы моделирования информационных систем медицинского назначения [3, 4].

Результаты исследования

Выделены особенности архитектуры и сформулированы требования, которые должны предъявляться к информационным системам, задействованным в процессе организации обращения полиса медицинского страхования. Обоснована целесообразность использования технологии блокчейн в системе ОМС РФ. Показана возможность решения возникающих проблем на основе этой технологии.

Обсуждение

Применение технологии блокчейн в системе ОМС РФ потенциально эффективно и обеспечивает децентрализацию основных информационных потоков циркулирующих в указанной системе. При этом архитектура системы позволяет автономную работу информационных систем субъектов страхования и обеспечивает решение основных задач, что, в конечном счете, должно привести к более оперативному поступлению финансовых средств как в страховые, так и медицинские организации. Распространение обновлений программного обеспечения и децентрализованная среда обеспечиваются особенностями технологии блокчейн. В силу своей децентрализованной природы получение обновлений программного обеспечения происходит практически одномоментно (в течение нескольких минут) для всех заинтересованных сторон. Регулятор отвечает при этом только за алгоритмы его корректного функционирования, а не за поддержку и функционирование больших массивов централизованной информации. Кроме того, указанная технология обеспечит оперативное и абсолютно достоверное предоставление данных о пациенте при его обращении за медицинской помощью. Одновременно достигается высокий уровень защиты персональной информации и исключение возможности подделки данных страхового полиса.

Современное функционирование информационных систем ОМС

В настоящее время наполнение базы данных полисов системы ОМС возложено на страховые медицинские организации (СМО). Эти организации в рамках своих полномочий осуществляют страхование граждан в полном соответствии с законодательством РФ [1] и волеизъявлением гражданина. Страховые медицинские компании (СМК) осуществляют ввод необходимой информации в собственные информационные системы и ее передачу в базу данных территориального фонда ОМС. Информационная система территориального фонда осуществляет проверку соответствующей информации, формирование необходимой отчетности и передачу этой информации в единую базу данных Федерального Фонда ОМС, в которой проводится итоговая консолидация и контроль [1, 3–6]. Одновременно с передачей информации происходит выпуск достаточно дорогого бумажного документа (полиса ОМС), печать которого осуществляется Гознаком на бланках, оснащенных специальными средствами защиты. В течение времени его изготовления пациент использует в качестве полиса временное свидетельство, подтверждающее оформление полиса ОМС.

При этом персональная информация гражданина хранится во всех этих информационных системах и требует соответствующих расходов на ее защиту. Возникает проблема доступа к указанной информации большого количества сотрудников этих организаций, так как наличие доступа не является обязательным для осуществления этими сотрудниками своих должностных обязанностей. Технология децентрализованного хранения предполагает иной взгляд на эту архитектуру и позволяет оперативно решать необходимые задачи на более высоком качественном уровне [5–6, 8–9].

Принадлежность персональных данных в системе ОМС

В настоящее время фактическим владельцем данных о гражданине выступает та или иная СМО. Именно она осуществляет ввод персональной информации и последующее распространение данных по системе. Однако если посмотреть в основу этого процесса, то становится очевидным, что основным владельцем указанной информации должен выступать сам гражданин. Технология блокчейн может (и должна) предоставить возможность заполнения необходимой информации ему непосредственно с собственного домашнего компьютера и одновременно позволит обеспечить существенную децентрализацию данных, включив в этот процесс компьютеры значительной части граждан РФ (выразивших такое желание). Для обеспечения проверки

данных, введенных гражданином, должна быть обеспечена такая архитектура системы, которая позволит хранить скан-копии первичных документов, а в дальнейшем (по мере развития информационной системы) автоматизированную выборку необходимой информации непосредственно с этих копий.

Для граждан, которые в силу тех или иных причин не смогут самостоятельно заполнить требуемые данные, СМК должны будут предоставить агентские услуги по вводу необходимых данных в систему, сохраняя право владения и корректировки информации за гражданином.

После ввода всей информации осуществляется ее шифрование. Целесообразно получить группу (ограниченное множество) ключей шифрования, которые должны относиться к одному из двух типов. Гражданин получает право разослать «ключ чтения» (первый тип) всем субъектам, заинтересованным в чтении (но не корректировке) необходимой информации, а «ключ записи» (второй тип) использовать для внесения необходимых изменений. Примерами таких изменений может быть смена фамилии (при вступлении в брак), изменение паспортных данных (при его замене) и т.д.

Группировка ключей в системе ОМС

Собственником и источником распространения всех ключей является непосредственно сам гражданин. Передавая свой ключ стороннему человеку или организации, гражданин выражает свое желание предоставить доступ к той или иной информации. Сам факт наличия легального ключа у того или иного субъекта будет свидетельствовать о желании гражданина передать сторонней организации (личности) ту или иную информацию (или полномочия) При этом целесообразно их разделение на следующие подгруппы: ключи для СМК (дающие право наиболее полного чтения информации о застрахованном); ключи для МО (позволяющие читать только реквизиты его страхового полиса и страховую принадлежность), обеспечивающие идентификацию и выставление счетов (за медицинские услуги) на оплату; ключи для федерального фонда ОМС (дающие доступ к подмножеству информации необходимой для решения задач соответствующего уровня).

«Ключи записи» могут быть классифицированы следующим образом: ключ дающий право на корректировку любой информации, содержащейся в полисе ОМС (данный тип ключа должен принадлежать самому застрахованному или (по его желанию) его ближайшим родственникам); ключ для страховой медицинской организации (или иного уполномоченного органа), который осуществит сверку информации с реальными документами и при отсутствии расхождений проставит отметку о достоверности переданной информации. Для уменьшения нагрузки на СМК, для осуществления аналогичных функций, допустимо передать копию закрытого ключа в медицинскую организацию, к которой прикреплен конкретный застрахованный.

Еще один ключ записи должен быть передан в органы ЗАГС или специализированные МО, для изменения информации в случае смерти гражданина.

«Ключи чтения» (обеспечивающие просмотр интересующей информации) должны быть распределены и использованы следующим образом: с точки зрения большинства граждан, сведения, содержащиеся в их страховом полисе, не содержат секретной информации и могут находиться в открытом доступе. Остальные застрахованные предоставляют открытый ключ той МО, в которой гражданину оказывается медицинская помощь. Ключ должен быть аннулирован через нормативно установленный срок после окончания лечения.

Отдельно следует подчеркнуть возможность создания уполномоченного органа, куда при желании застрахованного, может быть передан экземпляр открытого ключа, который будет использован, если по медицинским показаниям (или иным причинам) застрахованный не сможет предоставить эту информацию лично или через доверенное лицо.

Каждый из сгенерированных ключей должен обладать индивидуальными признаками, что в последующем должно обеспечить точную идентификацию как лиц запрашивающих информацию для ее корректировки, так и использующих ее только для чтения.

Алгоритм обращения страхового полиса в системе блокчейн

Каждый человек, решив застраховаться в информационной системе, основанной на технологии блокчейн, получает ряд преимуществ, которых он лишен в традиционных информационных системах. Генерация полиса в этом случае фактически идентична генерации токена в системе. Сгенерировав токен, человек может направить его в любую страховую организацию, работающую в системе ОМС, и тем самым фактически осуществить свое страхование. При этом собственность на данный токен должна быть передана выбранной страховой организации, а право распоряжения им – остается закрепленным

за гражданином. Такой подход позволит любому застрахованному легко менять своего страхователя неограниченное число раз по своему желанию, любые ограничения в этом вопросе должны исчезнуть.

Использование децентрализованного приложения означает хранение всего массива необходимой информации на каждом компьютере, подключенном к системе, однако системы шифрования, применяемые в системе блокчейн, позволят осуществить только санкционированный доступ к персональным данным и делают их тиражирование по всем узлам сети абсолютно безопасным. Все МО, работающие в системе ОМС, на сегодняшний день обладают вычислительной техникой, позволяющей проводить эксплуатацию систем подобного типа. Поэтому в процессе наращивания пиринговой одноранговой сети данные о застрахованных будут растиражированы по всем ее узлам. Для небольших врачебных амбулаторий и фельдшерско-акушерских пунктов допускается использование клиентов, которые, получая информацию от других узлов, не предоставляют своих ресурсов для поддержки совместно эксплуатируемой сети, но такой режим должен быть скорее исключением.

Особенности архитектуры блокчейн для системы ОМС

При решении задачи поддержки обращения полисов необходимо выбрать архитектуру между блокчейном консорциумом и публичным блокчейном. Здесь под блокчейном консорциумом мы будем понимать информационную систему, в состав которой входят только уполномоченные вычислительные мощности. Иначе права подключения компьютера в систему выбираются уполномоченным органом. Более предпочтительным в рассматриваемом случае является публичный блокчейн, дающий возможность застрахованному корректировать информацию полиса с использованием любого компьютера, подключенного в сеть. Кроме того, большое количество компьютеров, подключенных к сети, обеспечивают практически 100%-ную достоверность и неизменность циркулирующей в ней информации, что позволит полностью исключить возможность того или иного искажения информации. Однако начальный этап развертывания системы подобного типа должен предполагать использование блокчейна консорциумов. Ввод в эксплуатацию подобной системы позволит существенно снизить вычислительную и производственную нагрузку на службы автоматизации Федерального фонда ОМС и его территориальных отделений, так как отпадает необходимость аккумулирования данных на больших выделенных серверах. Вся необходимая информация будет распределена и продублирована в узлах сети. На регуляторы ложится нагрузка формулировать и уточнять требования к алгоритмам функционирования программного обеспечения и тестирование адекватности их выполнения. Все алгоритмы должны быть заранее опубликованы и публичны, что приведет к возможности их адекватной оценки и своевременного выполнения профессиональным сообществом. Доступ к основным функциям системы должен предусматривать как диалоговый режим обращения, так и с использованием функций специализированного интерфейса API, что актуально, так как система должна предусматривать возможность подключения значительного количества информационных систем и их последующего устойчивого функционирования. Таким образом, архитектура системы позволит обеспечить использование большого количества равноправных компьютеров и, как следствие, вычислительных мощностей. Существенно снизятся расходы на эксплуатацию и поддержание информационной системы у традиционных субъектов системы ОМС, она будет во многом перераспределена в пользу вычислительной техники, принадлежащей застрахованным и медицинским организациям. При этом следует отметить, что использование этих дополнительных ресурсов в общем случае не приведет к дополнительным затратам, т.к. может быть использована техника уже имеющаяся у граждан и медицинских организаций, что просто увеличит время ее полезной эксплуатации.

Преимущества, предоставляемые технологией блокчейн

Используя предложенный подход, мы в среднесрочной перспективе можем обеспечить достижение следующих результатов [3, 4, 6, 9, 11]:

- существенную экономию затрат федерального фонда ОМС и его территориальных отделений за счет снижения затрат на эксплуатацию и сопровождение централизованных баз данных, которые в результате будут равномерно распределены по системе;
- снижение временных задержек получения заинтересованными сторонами необходимой информации за счет фактического расположения требуемой информации на всех заинтересованных вычислительных мощностях;
- обеспечение устойчивости всей информационной структуры за счет тиражирования данных

по узлам сети, что сохраняет работоспособность системы даже при выходе из строя большого числа компьютеров;

• прозрачность алгоритмов контроля и верификации данных о застрахованных, а также обеспечение контроля за ними информационного сообщества, что порождается самой природой системы блокчейн, предусматривающей верифицированный консенсус;

• поэтапный отказ от бумажного полиса ОМС и, как следствие, экономию бюджетных средств на печать документов строгой отчетности, которая предусматривается существующей нормативной базой;

• более высокий уровень защиты персональных данных, что характерно для методов шифрования, использующихся в блокчейн – системах;

• снижение риска ошибок, увеличение прозрачности циркуляции данных, снижение незащищенности системы вследствие ее децентрализации, уменьшение количества случаев мошенничества (приписок) со стороны медицинских и страховых организаций, сокращение необоснованного и нерегламентированного вмешательства со стороны субъектов системы.

Обсуждение результатов

Предложенный подход даст возможность создать открытую архитектуру информационной системы, позволяющую объединить неограниченное число МО, СМО, отделений ТФОМС и отдельных коммерческих разработчиков. Многие выводы были получены как результат использования материалов, полученных от ООО «Электронная медицина» (г. Ростов-на-Дону) [5, 6].

Полученные результаты могут быть использованы для построения систем электронного документооборота в области выписки электронных полисов ОМС и направлений на госпитализацию.

Выводы

1) Проведен анализ предполагаемых изменений нормативной базы, и обоснована актуальность применения технологии блокчейн в системе ОМС.

2) Показана возможность существенного снижения расходов системы ОМС.

3) Описан механизм санкционирования доступа к персональным данным в системе.

4) Предложен ряд возможных оригинальных архитектурных решений для информационных комплексов системы ОМС на основе технологии блокчейн.

5) Проанализированы преимущества перехода к технологии блокчейн в системе ОМС.

Финансирование. Исследование не имело спонсорской поддержки

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

ЛИТЕРАТУРА

1. Федеральный закон от 29.07.2017 г. № 242ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья». [Электронный ресурс] – URL: http://www.consultant.ru/document/cons_doc_ LAW_221184 (Дата обращения: 18.12.2018).
2. *Винья П., Кейнси М.* Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок: Пер. с англ. – М.: Манн, Иванов и Фербер, 2017. – 432 с.
3. *Воронова Л.В., Гольчевский Ю.В.* Статистическое моделирование в процессах управленческого учета на примере медицинского подразделения вуза // Врач и информационные технологии. – 2014. – № 3. – С. 46–57.
4. *Гулиев Я.И., Белышев Д.В., Михеев А.Е.* Моделирование бизнес-процессов медицинской организации: классификация процессов // Врач и информационные технологии. – 2015. – № 4. – С. 6–13.
5. *Егоренкова Т.Ю., Курбесова Е.С., Курбесов А.В.* Электронный больничный лист // Главный врач юга России: Специализированный медицинский журнал. – 2017. – № 3. – С. 33.
6. *Курбесов А.В., Калугян К.Х.* Актуальность применения технологии блокчейн в вопросах лекарственного обеспечения граждан. // Врач и информационные технологии. – 2018. – № 2 – С. 23–28.
7. *Поппер Н.* Цифровое золото: невероятная история биткоина: Пер. с англ. – М.: ООО «И.Д. Вильямс», 2016. – 368 с.
8. *Равал С.* Децентрализованные приложения. Технология Blokchain в действии. – СПб.: Питер, 2017. – 240 с.
9. *Свон М.* Блокчейн: схема новой экономики: Пер. с англ. – М.: Издательство «Олимп-бизнес», 2017. – 240 с.
10. *Siraj Raval.* Decentralized Applications: Harnessing Bitcoin's Blockchain Technology, 2016. – 150 p.
11. *Champagne Ph.* The Book Of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto, 2014. – 396 p.
12. *Castronova E.* Wildcat Currency: How the Virtual Money Revolution Is Transforming the Economy Hardcover, 2014. – 288 p.
13. *Graf Konrad S.* Are Bitcoins Ownable?: Property Rights, IP Wrongs, and Legal – Theory Implications, 2015. – 92 p.
14. *Martin W.* Black Market Cryptocurrencies: The rise of Bitcoin alternatives that offer true anonymity, 2014. – 156 p.
15. *Brito J., Castillo A.* Bitcoin: A Primer for Policymakers, 2016. – 118 p.
16. *Clark J.* Bitcoin, blockchain, cryptocurrency, cryptology» (A detailed and technical study of Bitcoin, blockchain, cryptocurrency, and cryptology), 2016. – 499 p.