Patientory: Одноранговая сеть хранения электронных медицинских карт v1.0

Крисса Макфарлэйн, Майкл Бир, Джесси Браун, Нельсон Прендергаст

Апрель 2017

Этот документ представлен только в информационных целях и не является предложением или рекомендацией продавать акции или ценные бумаги Patientory или любой связанной компании. Любое такое предложение или рекомендация будут сделаны только посредством конфиденциального информационного письма и в соответствии с условиями всех применимых конфиденциальных мер и других законов.

Антонация

Обмен медицинской информацией на базе блокчейна может открыть истинное значение совместной работы и кибербезопасности. Эта система имеет потенциал устранить проблемы и затраты нынешних сторонних посредников, занимающихся управлением здоровья населения. Звучат обещания улучшить целостность данных, уменьшить операционные издержки, децентрализовать сеть и отказаться от посредничества доверительных фондов. Способный скоординировать уход за больным с помощью блокчейна, Обмен медицинской информацией существенно сокращает ненужные услуги и дублированные тесты, снижая затраты и улучшая эффективность непрерывного цикла ухода за больным, придерживаясь всех правил и стандартов HIPAA. Сосредоточенный на пациенте протокол, поддержанный технологией блокчейн, Patientory изменяет способ, которым заинтересованные стороны в сфере здравоохранения управляют электронными медицинскими данными и взаимодействуют с врачами.

1 Введение

1.1 Что такое блокчейн?

Технология, стоящая за появлением цифровой валюты биткоин, блокчейн родился благодаря неопознанному лицу (или группе лиц) под псевдонимом Сатоши Накамото. С 2009 года блокчейн получил более широкое использование в финансовой отрасли со множеством новых выходящих на

рынок компаний и сервисов, работающих на блокчейне. Технология блокчейна используется для совместного использования реестра финансовых операций через бизнес-сеть без управления одним объектом. Распределенный реестр упрощает создание экономически эффективных коммерческих отношений, где практические все, имеющее ценность, может прослеживаться и торговаться без центральной точки управления. Технология помещает конфиденциальность и управление данными в руки частного лица. Доверие и целостность устанавливаются без привлечения сторонних посредников.

1.2 Существующая инфраструктура здравоохранения

Смена фокуса, основанного на "процедуре", на фокус "целостной заботы о человеке" заставляет поставщиков медуслуг формировать "сети", работающие вместе для достижения общей цели улучшения состояния здоровья людей, находящихся на лечении, после интенсивного лечения при приступах или между курсами подобного лечения. Потребность в сотрудничестве между поставщиками услуг - от специалистов, врачей первой помощи, сиделок и специалистов по оздоровлению (таких как диетологи и медсестры реабилитации) - приводит к увеличению использования цифровых технологий. Хотя эти решения значительно улучшили отслеживание и эффективность предоставления медицинской помощи, они привели к созданию хранилищ медицинской информации, прежде всего в системах электронных медицинских карт (ЭМК).

Медицинские и правительственные организации тратят существенное количество времени и денег для установки и управления традиционными информационными системами и сетями обмена данных; требуются ресурсы, чтобы постоянно находить проблемы, обновлять параметры поля, выполнять резервное копирование и восстановление, извлекать информацию для создания отчетов.

Федеральные законы и программы стимулирования сделали данные медицинского обслуживания более доступными, несмотря на сопротивление больниц относительно реализации системы ЭМК. Однако подавляющее большинство систем больниц все еще не может легко (или безопасно) совместно использовать свои данные. В результате этого врачи тратят больше времени на ввод данных в компьютер, чем на общение с пациентами. Случаи профессионального выгорания врачей участились с 45 до 54 % за 2011 - 2014 года [1].

Несмотря на это, существуют понятие «индивидуализированной» медицинской информации и в клинической сфере, и в сфере поддержания

здоровья, которые не перевелись в «персонализированные» планы медпомощи. Кроме того, даже при том, что существует множество данных, вся экосистема медпомощи неспособна адекватно спроектировать значение или риск, чтобы точнее предсказывать будущие курсы лечения пациента. Следовательно, существующие решения, к которым стремится индустрия технологий здравоохранения, привели к трудному выбору между заботой о пациенте и мошенничеством, связанным с конфиденциальностью и деньгами. Мы видим, что эта проблема увеличивается, поскольку увеличивается количество данных, производимых отраслью. **Безопасная технология, свойства и распределенная природа блокчейна могут помочь уменьшить стоимость и увеличить эффективность этих операций, а также обеспечить жизнеспособную инфраструктуру безопасности.**

1.3 Отношения поставщика медуслуг и пациента

Новая парадигма здравоохранения нуждается в эффективном и оптимальном предоставлении медпомощи пациентам для получения лучших результатов лечения. Необходимо, чтобы Основные поставщики медпомощи были в состоянии активно связываться и сотрудничать с другими специалистами и вспомогательными медицинскими организациями, такими как лаборатории и аптеки. В конечном счете, для успешной работы медкарты пациентов должны своевременно обновляться.

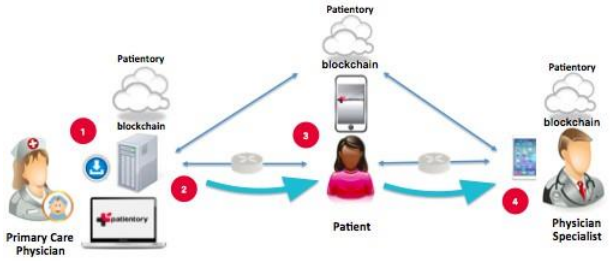

Рисунок 1: Схема Patientory

Программное обеспечение системы ЭМК в настоящее время не поддерживает эффективную связь поставщика медуслуг и пациента. Порталы для пациентов не имеют большой популярности вследствие их изолированного использования. Кроме этого, это программное обеспечение дает ограниченную возможность обмена информацией между системами и обычно требует наличие назначенного лица, которое участвует в такой передаче информации. Это привело к замедлению работы организаций в процессе оказания медпомощи пациенту, а также общему

ухудшению качества услуг. Кроме того, поскольку поставщики медуслуг тратят больше времени на координацию ухода за пациентами, лечение пациентов стало эффективнее, а рабочая нагрузка увеличилась, что приводит к неочевидному влиянию на результаты их работы.

Учитывая, что многие врачи не хотят, чтобы пациенты имели доступ к электронным медкартам, пациенты играют пассивную роль в слежении за своим здоровьем. Это, в конечном счете, заставляет их чувствовать недостаток контроля, что расстраивает пациентов и уменьшает их желание следить за своим здоровьем. Хотя недавно увеличилось число приложений Мобильного Здравоохранения, помогающих людям отслеживать состояние наиболее важных органов и медицинских параметров, новинка не приводит к улучшению ухода за больными или соблюдению предписанного лечения и результатам, поскольку она тоже сталкивается с трудностями интегрирования в систему ЭМК.

2 Обзор системы

Существующие проблемы решаются с помощью блокчейн-сети Patientory. Прежние системы ЭМК являются централизованными структурами, объектами хакерского взлома, строгой техники безопасности и обременительных накладных расходов. Реализовывая блокчейн инфраструктуру Patientory, поставщики медуслуг могут видеть устранение пробелов здравоохранения, канал для упрощенной координации ухода за пациентом и общее улучшение результатов мероприятий по охране здоровья. Выше представлено схематическое описание блокчейн инфраструктуры Patientory и ее функциональной совместимости пациентов и поставщиков медуслуг.

3 Внедрение системы

3.1 Предписания HIPAA и руководство по соблюдению требований

Перед любым значимым обсуждением реализаций необходимо обратиться к ограничениям, наложенным предписаниями Закона о преемственности и подотчётности медицинского страхования 1996 года (HIPAA). Его правила особой важности: Правило Конфиденциальности, Правило безопасности и Инструкция по облачным вычислениям. Задача этого текста состоит не в том, чтобы провести полное исследование закона HIPAA. Мы определим предписания, подходящие для обсуждения реализации, и далее обсудим их, согласно соответствующему использованию.

A. Правило конфидециальности

Бизнес-модель Patientory предусматривает, что требования Правила Конфиденциальности должны соблюдаться вследствие электронного хранения и передачи частной медицинской информации. Применимость правила конфиденциальности сводится к тому, что “Правило Конфиденциальности... (применяется) к программам медицинского страхования, центрам обмена медицинской информацией, и любому поставщику медуслуг, который передает медицинскую информацию в электронной форме” [2]. В дополнение к этим агентам те стороны, которые действуют от их имени, такие как поставщики услуг, также ответственны за выполнение правил HIPAA. Эти второстепенные агенты называются Деловыми партнерами (BA), и правовой документ, определяющий для них правила и нормы, называется Договором делового партнера (BAA). Закон HIPAA налагает строгие требования на содержание этих договоров.

В результате первоначального исследования было выявлено, что важнейшими являются те требования, в которых указана информация об авторизацию использования, использовании обезличенной информации и определении частной информации. Частная медицинская информация (PHI или ePHI для электронных данных) определяется как “вся индивидуально идентифицируемая медицинская информация, хранимая или переданная объектом, или его деловым партнером, в любой форме - электронной, бумажной, или устной” [2]. Обезличенная информация о здоровье определяется как “Медицинская информация, которая не идентифицирует частное лицо и относительно которой нет никакого разумного основания полагать, что информация может использоваться для идентификации частного лица” [2]. Обезличенные данные используют следующие ограничения: “Нет никаких ограничений на использование или раскрытие обезличенной медицинской информации. Обезличенная медицинская информация не идентифицирует и не обеспечивает разумное основание для идентификации частного лица” [3]. Обезличенные данные определяются как любая информация, которая может ограничить возможное число частных лиц, с которыми связан набор информации, до менее 0,04% всего населения США.

B. Правило безопасности и инструкция по облачным вычислениям

Вследствие длины содержания, связанного с этой темой, только самые важные элементы выделены для рассмотрения: “Когда объект, определенный законом HIPAA, пользуется услугами Провайдера облачного хранения (CSP), чтобы создать, получить, обслужить или передать ePHI (например, обработать и/или сохранить ePHI), от своего лица, CSP является деловым партнером по закону HIPAA. Далее, когда бизнес-партнер заключает субподрядный договор с CSP для создания, получения, обслуживания или передачи ePHI от своего лица, субподрядчик CSP сам является деловым партнером. Это верно, даже если CSP обрабатывает или хранит только зашифрованную ePHI и не имеет ключа шифрования данных. Отсутствие ключа шифрования не освобождает CSP от статуса

делового партнера и обязательств по Правилам HIPAA. В результате объект, определенный законом HIPAA, (или деловой партнер) и CSP должны заключить соответствующий HIPAA Договор делового партнера (BAA), и CSP и по контракту ответственен за соблюдение условий BAA, и непосредственно ответственен за соответствие применимых требований Правил HIPAA" [3].

Объекты, определенные законом HIPAA, часто используют Провайдеров облачного хранилища (CSP) для хранения медицинской информации, часто говоря, что это более экономически эффективно и сокращает затраты на IT. Однако, поскольку потребители полагаются на поставщиков облачных вычислений, чтобы хранить персональные данные, они оставляют прямое управление этим данными и в результате не знают, у кого есть доступ и где данные географически расположены. Даже если между Деловым партнером и Провайдером облачного хранилища составлен детальный Договор делового партнера, он предоставил бы только условия того, кто берет на себя ответственность конфиденциальности и безопасности данных в случае нарушения. Потребитель потенциально управляет доступом к этим потокам данных, но будет полагаться на Провайдера облачного хранилища для выполнения полномочий.

Несмотря на то, что использование облачного хранилища популярно, существует все еще много рисков для потребителя при использовании этого механизма для его персональных данных. В основанной на облачных вычислениях архитектуре данные дублируются и часто перемещаются, поэтому риск несанкционированного использования данных возрастает. Кроме того, существует множество частных лиц с доступом к данным, таких как администраторы, сетевые инженеры и технические специалисты, которые обслуживают большое количество серверов, в которых хранится информация. Это также увеличивает риск несанкционированного доступа и использования.

Однако даже если данные находятся в безопасности благодаря строгим средствам управления доступом и зашифрованы в исходном пункте, во время перемещения данные все еще представляют собой проблему для развития Показателей результатов, связанных с пациентом (PROM). Понятие PROM должно разработать сфокусированную на пациентах меру, которая касается области или цели, которая представляет интерес для пациента, и то, в чем их вовлеченность и обратная связь важны для ее успешного внедрения. Доступ к большим потокам данных от множества устройств, которые являются частью сети IoT, которая используется теперь в сочетании с основанными на облачных вычислениях услугами, может обеспечить основу для PROM, но трудно понять, смогут ли данные, хранящиеся в облаке, произвести меру, которая будет иметь вкладываемый смысл и уместность для пациента.

Реализация блокчейн технологии, чтобы гарантировать и улучшить безопасность данных для всей медицинской документации, связанной с

системой, поможет устранить нарушения и окончательно децентрализовать принадлежность медкарты. При отправке в базу данные будут шифроваться при помощи различных алгоритмов и дешифроваться во время извлечения.

В отношении быстро растущего числа утечек данных, с которыми сталкивается медицинская отрасль, блокчейн технология делает соответствие HIPAA выполнимым и для пациентов, и для поставщиков медуслуг.

C. Анализ ограничений системы блокчейн относительно требований HIPAA

Блокчейн Ethereum упрощает работу с разнообразным подмножеством реализаций систем вследствие применения полного по Тьюрингу языка программирования, которая выполняется на Виртуальной машине Ethereum. Эти системы имеют ограничения в том, что виртуальная машина не подвергается никакой прямой внешней проверке со стороны более широкого Интернета, кроме Oracle Services. Кроме того, ограничения хранения блокчейна зависят от стоимости хранения и стоимости доступа к этим данным. Что касается записи, время создания блока в цепи устанавливает минимальное предельное значение для запросов изменения состояния в 15 секунд.

Ограничение блокчейна для размещения частной информации может быть преодолено через запутывание данных, такое как шифрование, но если случится утечка ключа расшифровки, нет никакого способа удалить уязвимые данные из блокчейна. Из-за необходимости соответствия данных HIPAA, это может потенциально привести к постоянной, некорректируемой утечке информации вследствие неизменности самого блокчейна. Несмотря на то, что обезличенные данные могут теоретически храниться на Общедоступном блокчейне Ethereum, опасно предполагать, что обезличивающий механизм фильтрации никогда не перестанет работать, или что информация боковой полосы, связанная с взаимодействиями блокчейна, не может непреднамеренно раскрыть личность. Этот вывод был также сделан MIT Media Lab во время формирования Протоколов MedRec и описан в Брошюре [3] MedRec. Получение этой информации боковой полосы может быть столь же простым как наблюдение временных меток и взаимодействий с известными контрактами хранения данных.

Посредством этого анализа можно связать частное лицо с учреждением, и что еще более важно - время, в течение которого оно присутствовали в системе. Учитывая специализированную природу некоторых систем, этой информации достаточно для появления нарушения соответствия HIPAA вследствие способности пассивного наблюдателя вывести идентификационные данные, расположение, время взаимодействия, и возможно, класс диагноза.

Ожидая, что это расположение является удаленным по своей природе, сокращение значения до менее 0,04% населения США становится

бесполезным. Эти факты составляют неоправданные одиночные отказы, которые должны быть подтверждены. Далее, прямое хранение даже зашифрованных данных о блокчейне создает необходимость внесения ответственности менеджеров базы данных в Договор BAC вследствие их действий как средства хранения данных HIPAA (См. раздел Правила безопасности и Инструкция по облачным вычислениям). Неблагоразумно ожидать, что каждый получать информации, и даже частные лица, размещающие пассивные узлы, будут выполнять требования HIPAA. Вследствие этих проблем мы реализовываем механизм для постоянного хранения уязвимых данных посредством использования частной реализации блокчейна на базе Ethereum.

D. Цели реализации для удобства пользования и безопасности

Основные цели любой системы безопасности могут быть в целом сформулированы как цели конфиденциальности, целостности, доступности, учета и страхования информации / идентификационных данных. Для достижения этих целей необходимо определить понятия злоумышленника и пользователя. Каждая из этих ролей требует определенных подтверждений своих способностей. С точки зрения пользователя система должна быть достаточно прозрачной, не требующей каких-либо специальных знаний. Кроме того, вследствие неспособности обычного пользователя понять сложные ограничения кибербезопасности, процесс должен быть стойким к действиям пользователя.

Если нападение действительно происходит, система создана таким образом, что усилие, которое нужно приложить, чтобы поставить под угрозу ресурс, гораздо больше, чем значение самого ресурса. Реализация определяет то, что достаточно усовершенствованная сторона с надлежащими ресурсами всегда будет способна взломать любую систему, приложив достаточное количество времени и усилия. Проще говоря, совершенной защиты не существует. Теперь, когда все ограничения описаны, мы можем обсудить саму реализацию и достигнуть все ранее упомянутые цели.

3.2 Определение реализации аппаратных средств и сети

Для размещения вышеупомянутых проектных целей выбранная реализация системы требует нескольких независимых систем. Каждая система разделяет полномочия, гарантирует, что только авторизованные объекты могут взаимодействовать утвержденным способом, и предоставляет механизм для увеличения безопасности при сохранении доступности. Эта система была также разработана таким образом, что масштабирование может быть выполнено посредством

добавления иерархических схем вызова. Эти системы полностью описаны ниже.

Общедоступным объектом является Сервер дистанционного вызова процедур (RPC), который действует как интерфейс частной реализации блокчейна Ethereum (разрешенный блокчейн). Это сеть блокчейн узлов, которой разрешено взаимодействовать только с другими блокчейн узлами, ключевым объектом разработки, соответствующим HIPAA хранилищем и Сервером RPC. Ключевой объект разработки - это ресурс, который генерирует закрытые/открытые ключи для использования в блокчейне. Соответствующее HIPAA хранилище содержит фактические данные, которые составляют электронную частную медицинскую информацию (ePHI).

Когда появляется запрос на данные, соответствующая HIPAA система может получить разрешение говорить с отправителем, который затем перенаправляет данные назад на сервер RPC. Также можно сделать так, что хранилище HIPAA говорит непосредственно с сервером RPC. Каждая реализация обладает преимуществами, которые нужно рассмотреть до окончательного выбора. Так или иначе, хранилище HIPAA дешифрует соответствующие части базы данных при обработке запроса. Эта дешифрованная информация затем повторно зашифровывается с помощью открытого ключа запрашивающей стороны для передачи. Этот открытый ключ является также открытым ключом контракта, который действует как интерфейс управления от блокчейна до данных HIPAA.

Далее представлена схема топологии сети:

3.3 Определение реализации программного обеспечения

В дополнение к физической изоляции систем в реализации аппаратных средств и сети, управление доступом к программному обеспечению упрощает целостность данных и проверку авторизации для запрашивающих объектов. Программная система, с точки зрения управления доступом и шифрования данных, описана ниже.

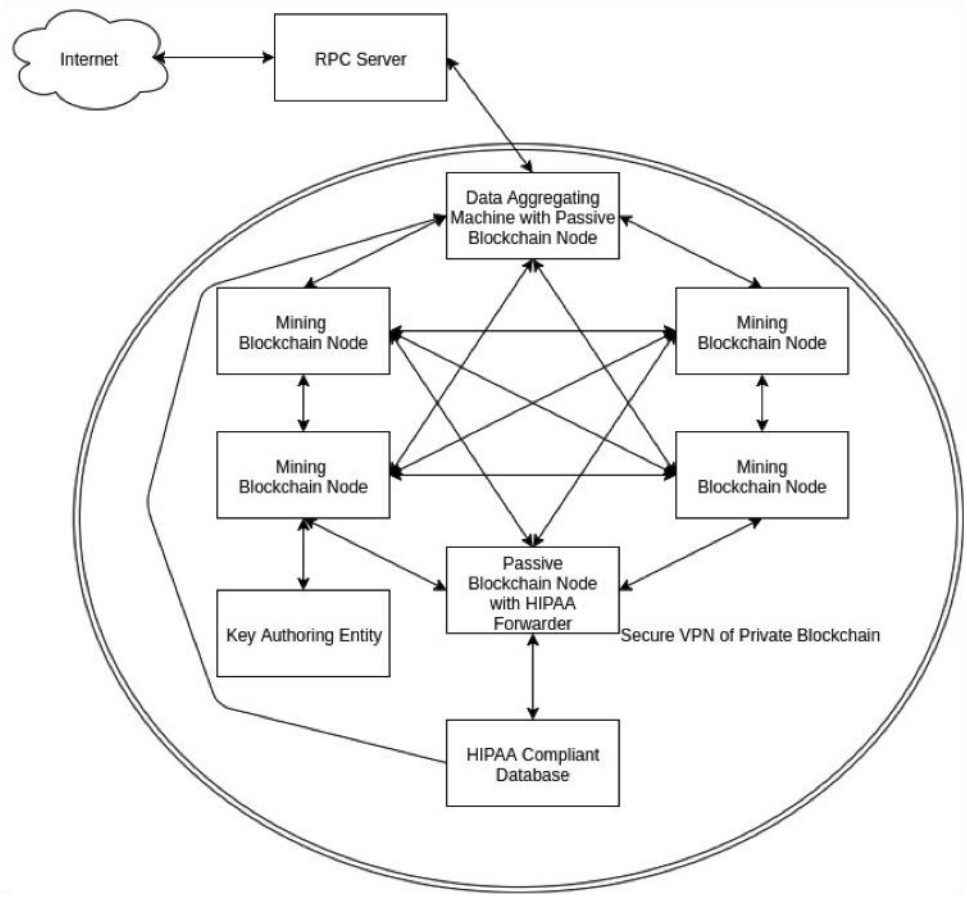

Рисунок 2: Топография сети блокчейн Patientory

База данных, соответствующая HIPAA, примет только входящие соединения от ретранслятора HIPAA. Это гарантирует, что поток трафика изолируется до известных управляемых путей. Ретранслятор HIPAA будет действовать только для передачи запроса хранилищу HIPAA, до того как допустимая операция произойдет на блокчейне, и эта операция приведет к событию запроса. Это событие запроса должно содержать открытый ключ запрашивающей стороны и запрашиваемые поля данных. Наконец, сервер RPC использует Прикладной программный интерфейс (API) с управляемым доступом, таким образом, что только известные пользователи могут взаимодействовать с сервером.

Для понимания иерархии вызовов системы необходимо рассмотреть структуру контракта для упрощения управления доступом. Каждый пользователь в системе получает свой адрес на частном блокчейне. Каждый

частный адрес может говорить только с ОДНИМ контрактом на блочейне. Этот контракт является контрактом класса частного лица. Учреждения, сотрудники учреждения и клиенты являются объектами уровня классов.

Эти объекты уровня классов являются интерфейсами, основанными на разрешении. Контракт учреждения имеет список всех клиентов, которые предоставили полномочия просмотра учреждению, и каждый контракт с клиентом имеет список всех учреждений, которым он дал разрешение. Контракт учреждения имеет функции, которые упрощают любое аннулирование полномочий учреждению со стороны пользователя. **Контракт учреждения не может сам изменять этот список, таким образом, предотвращая несанкционированный доступ к медкартам частных лиц.** Кроме того, Контракт учреждения обладает списком авторизованных сотрудников, который он может полностью обслуживать. Эта схема разрешения должна идеально функционировать таким образом, что автоматическое аннулирование разрешения выполнялось в полуправильных интервалах для предотвращения непреднамеренного сохранения учреждением прав доступа бывших сотрудников.

В этой системе все третьи стороны взаимодействуют посредством предоставления подписанных операций, которые кодируют вызов запроса. Эти операции предоставляются через сервер RPC после пользовательской проверки. Сервер RPC отправляет эти запросы серверу агрегации данных, который затем передает эти запросы получателям, на основе механизма разделения нагрузки. Получатели затем обрабатывают запрос, предоставляя операцию от имени вызывающей стороны соответствующей управляющему контракту стороне. Этот контракт содержит разрешения данных о том, что объекту разрешено получить доступ к ним, внутренние для контракта. Этот контракт является единственным объектом, который примет операцию от внешнего запроса. Таким образом, механизм может полностью управлять операциями вызова на блокчейне.

Для любой данной операции создается неизменная запись вызывающей стороны. Это гарантирует, что все попытки получить доступ к информации записываются. Фактические данные, хранящиеся в контракте пользователя, являются системой указателей хеша, которые, когда это разрешено сервером хранения HIPAA, приводят к возвращению соответствующих данных. Эта информация передается ретранслятору HIPAA за счет выполнения допустимой операции запроса. Механизм, который упрощает эту коммуникацию, является косвенным и проявляет себя через систему передачи сообщений о событиях блокчейна. Вследствие ограничения того, что запрашивающая сторона может запросить базу данных только с помощью допустимой операции, и того, что пользователь

не может непосредственно изменять свою собственную информацию, управление доступом доказывает свою значимость. С точки зрения учреждений механизмы похожи друг на друга, за исключением того, что контракт учреждения хранит список пользователей, у которых он может запросить данные и список пользователей, которые могут взаимодействовать с этим учреждением как сотрудники. Когда операция запроса исходит от контракта сотрудника учреждения, управляющий контракт вызывает контракт учреждения, который вызывает контракт пользователя, чтобы попросить указатели данных, которые решают ePHI. Видя, что учреждение находится в списке утвержденных учреждений для пользователя, контракт возвращает соответствующие указатели хеша. Эти указатели затем публикуются как сообщение о событии, которое снова передается в хранилище HIPAA.

Полный процесс одного запроса следующий: третья сторона запрашивает данные у сервиса, вызывая сервер RPC с помощью криптографически подписанной операции для предоставления в блокчейн. Сервер RPC проверяет идентификационные данные третьей стороны через подпись запроса входа в систему.

Видя, что подпись соответствует на входе в базу данных разрешенным открытым ключам, сервер RPC принимает запрос и подает запрос к Машине агрегации данных. Машина агрегации данных затем подает запросы к частным блокчейн верификаторам. Верификаторы получают запрос как вызов учетной записи блокчейна против целевого контракта. Верификаторы исполняют этот вызов, и если запрос является допустимым действием, операция вводится в следующий блок. Эта операция также отправляет сообщение о событии в блокчейне. Это сообщение о событии читается ретранслятором HIPAA, который действует для создания зашифрованного запроса против хранилища HIPAA, основанного на хешах сообщения о событии. Это сообщение также содержит открытый ключ запрашивающей стороны. Соответствующая HIPAA система баз данных рассматривает этот запрос и передает зашифрованную копию информации серверу RPC с помощью открытого ключа запрашивающей стороны. Сервер RPC затем возвращает эту информацию запрашивающей стороне, повторно назначая запрашивающий IP открытому ключу в сообщении. Сервер RPC передает это сообщение, не узнав ключевые данные. Эти данные затем сразу уничтожаются сервером RPC, таким образом, гарантируя, что сервер RPC действует как проводник, который не должен соответствовать HIPAA.

Механизм публикации данных аналогичен по своей природе, но данные, который должны быть представлены, зашифрованы открытым ключом хранилища HIPAA. Другие операции идентичны, кроме того, что публикующиеся данные передаются через систему отправки сообщения о событии. Таким образом, вследствие использования неконфликтных хеш-функций и данных случаев с временными метками, данные могут храниться с контрактом, который может вычислять адрес, на котором представленные данные располагаются в хранилище HIPAA.

Наконец, необходимо рассмотреть распределение закрытых ключей по объектам. Оно может быть упрощено для пользователей смартфона через оптические средства. Распределение закрытых ключей аналогично использованию QR-кодов как ссылок на адреса Ethereum. Альтернативные средства также возможны, при использовании приложения на ПК и планшете/смартфоне. Потеря ключа не является катастрофическим событием вследствие возможности административно отменить доступ к управляющему контракту одного ключа и предоставить его другому.

3.4 Функциональная совместимость

Системы ЭМК основываются на изолированной учетной архитектуре проверки, в которой данные пациента хранятся в каждой из отдельных систем. Это привело к индивидуальным, координирующим уход за больным решениям "надстроек" для этих систем для возможности координации ухода за больным через других поставщиков медуслуг и вспомогательные медицинские организации. Однако доступ к информации от основной Организации-поставщика медуслуг к другим организациям предоставляется только через ограниченные возможности, например, Прочитать, Предоставить, Отправить или Уведомить. Кроме того, Пациент/Потребитель имеет очень ограниченную возможность взаимодействия или участия в этом обмене информацией. Более того, любую ошибку, связанную с отсутствием передачи или ошибкой, очень трудно исправить.

Как только блокчейн и его умные контракты сконфигурированы, параметры становятся абсолютными. Пациент становится основным посредником в отправке и получении медицинской информации, без необходимости частых обновлений и диагностики любого программного обеспечения. Поскольку записи блокчейна также неизменны и хранятся у всех участвующих пользователей, необходимость восстановления отсутствует. Кроме того, прозрачная информационная структура блокчейна может отменить много точек интеграции обмена данными и операции отчетности, отнимающие много времени.

3.5 Процессы и масштабируемость

Пользователи управляют всей своей информацией и передачами, что гарантирует высококачественные данные, которые являются полными, непротиворечивыми, своевременными, точными, и широкодоступными, таким образом, делая их долгосрочными и надежными. Благодаря децентрализованной базе данных, блокчейн не имеет центральной точки отказа и способен лучше противостоять вредоносным атакам.

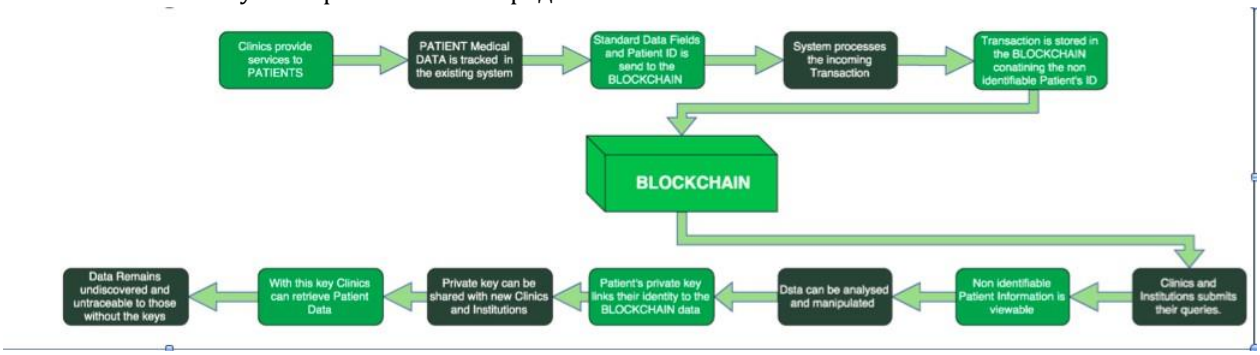

Рисунок 3: Схема выполнения процессов блокчейна

В любой сети медпомощи необходимо гарантировать, что участники, работающие вместе, могут зависеть друг от друга для предоставления необходимых услуг. Для достижения этого должно быть средство, которое гарантирует учет задачи и услуг, которые, как ожидается, будут оказаны своевременно, и также связанную ответственность, если они не будут оказаны своевременно на ожидаемом уровне качества. Следовательно, любая медицинская инфраструктура должна быть способна беспрепятственно контролировать необходимую информацию, чтобы позволить Поставщику Первой помощи оценить его сеть медпомощи. Дальше - больше, поскольку сеть медпомощи растет, и взаимодействие между поставщиками медпомощи сети увеличивается, медицинская инфраструктура должна быть способна эффективно работать с этим масштабом.

Ключевым аспектом строительства хорошо масштабируемой и распределенной Системы управления медицинской помощи является одноранговая архитектурная платформа. Такая платформа уже использовалась во многих отраслях, таких как СМИ, спортивные состязания, недвижимость, цепь поставок, которые показывают, что блокчейн может легко быть надстраиваемым связующим звеном программного обеспечения для существующих централизованных платформ [7]. Это

подвигло нас исследовать применимость блокчейн платформы в качестве одноранговой платформы в сфере здравоохранения.

Блокчейн открывает перспективу проверки двух или более объектов, занятых в “операции медпомощи”. Здесь существует два ключевых атрибута по сравнению с моделью централизованной аутентификации. Первый атрибут состоит в том, что заинтересованные стороны могут связаться друг с другом на «уровне операций» «доверительных отношений». Второй атрибут состоит в том, что потенциальная ответственность в таком отношении ограничена только связью «уровня операций». Это очень удобно, поскольку это ограничивает доступ к информации и обязательствам между участвующими сторонами и одновременно позволяет стороне войти в операционное отношение со многими другими поставщиками, на основе их определенных возможностей и типа медпомощи, которая будет оказана пациенту. Такая система значительно лучше, чем стандартные централизованные системы, которые должны ограничивать число поставщиков для широкого ряда потребностей пациентов вследствие усилия, требуемого для управления доступом и обязательствами.

3.6 Обмен медицинской информацией и токены

Чтобы США успешно перешли от модели сдельного способа оплаты к современной ценностно-ориентированной модели, необходимо создать IT инфраструктуру здравоохранения, которая позволяет организациям связать качество, стоимость и эффективность медицинских вмешательств через надежную модель компенсации.

Компенсация будет основываться на том, насколько эффективно работает сеть поставщиков для улучшения качества ухода за больным и результата лечения, одновременно сокращая стоимость медуслуг. Чтобы действительно простимулировать различных участников сети для превентивного создания лучших режимов ухода, вступает в силу основанная на заслугах компенсация совместно используемых сбережений (компенсаций). Для эффективного выделения пропорциональной доли поставщику в сети, который больше всего вкладывал в общие сбережения, четкое отслеживание их вклада измеряется умными контрактами в блокчейн сети.

Другое ключевое влияние новой парадигмы здравоохранения - это модель компенсации, в которой поставщики могут получать дополнительную компенсацию вне оказанной медпомощи. Эта компенсация является результатом сгенерированных сбережений,

основанных на том, насколько эффективно поставщики управляют результатами медицинского обслуживания пациентов (стимулы). Любые сбережения, сгенерированные через эффективное управление уходом за пациентом, могут быть сохранены поставщиками и их сетевыми партнерами как часть совместно используемого сберегательного аспекта новой парадигмы здравоохранения.

Наше предложение предоставляет плательщикам способность передавать токены в качестве стимулов поставщикам, которые достигают этих показателей качества. Способность беспрепятственно отслеживать и управлять умными контрактами, которые с легкостью выплачивают прибыль, обеспечивает необходимую «приманку» для поставщиков и пациентов для активного привлечения в симбиотическое сотрудничество. Наоборот, если один или несколько участников колеблется, по обязательствам, могут также просто быть наложены соответствующие штрафы. Этот подход «кнута и пряника» обеспечит необходимое давление, необходимое для сдвига медицинской отрасли от мышления управления болезнью до мышления здорового образа жизни.

С этого времени, выпущенные Patientory токены (PTY), являются родными токенами платформы Patientory. В обмен на токены PTY пользователи смогут использовать сеть для аренды пространства памяти для медицинской информации и выполнять платежи и операции по умному контракту здравоохранения.

Мы твердо верим, что использование токена является лучшей платежной системой для поддержки этой инфраструктуры в обозримом будущем. Будущее является активной экосистемой многих токенов, для которых здравоохранению будет нужна платежная система замкнутого цикла на месте. Результатом будет эффективное управление циклом медпомощи с положительными отзывами и значительной экономией миллиардов долларов, в настоящее время приписываемых мошенничеству в здравоохранении [4].

Система также стимулирует крупные организации с вполне достаточным серверным хранением торговать токенами с медицинскими организациями меньшего размера, которым будет нужен прямой доступ в медицинскую блокчейн сеть без непосредственной установки узла. Хотя новые политики здравоохранения обеспечивают потенциал, чтобы стимулировать поставщиков для сотрудничества по улучшению методов работы, данная архитектура ЭМК скорее предложит эту возможность,

поскольку, простое предоставление или получение токенов упрощают этот процесс.

Вот почему стоимость токенов связана с объемом операций, выполняемых в сети. Поскольку сеть Patientory последовательно увеличивает число операций, спрос на токены увеличивается, что приводит к увеличению их стоимости.

3.7 Приобретение токенов

PTY можно приобрести через приложение Patientory, рынок криптовалюты и от другого пациента, врача или страховой компании путем передачи. У пользователей платформы будет возможность получить PTY, отправляя Эфир («ETH») в контракт создания PTY на блокчейне во время предпродажи. Интерфейс Patientory интегрирует сторонние торговые решения, такие как Shapeshift и Coinbase, для пользователей, у которых нет ETH.

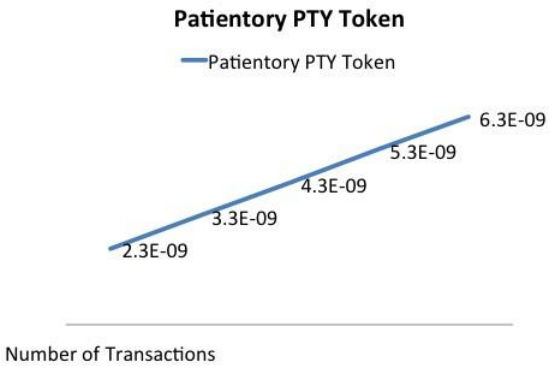

Рисунок 4: стоимость токенов Patientory как функция операций

Начальное распределение токенов Patientory будет иметь форму предпродажи. Каждый будет в состоянии приобрести PTY по заниженной ставке, закладывая ETH в умный контракт продажи токенов. Контракты, вместе с другими криптовалютами, такими как ETC или BTC, могут

создавать PTY через сторонний сервис преобразования, который будет доступен на странице предпродажи.

Команда основания получит 10% PTY согласно годовому периоду владения. Эти токены будут служить долгосрочным стимулированием для команды основания Patientory. Дополнительные 20% будут распределены по фонду Основания Patientory, который будет использоваться для научных исследований блокчейн технологии для использования в сфере здравоохранения.

3.8 Умные контракты и обработка страхового иска

A. Автоматическое присуждение компенсации

Сложность медицинского выставления счетов и сторонней компенсации для пациентов часто приводит к беспорядку или непониманию между пациентом, поставщиком медуслуг и страховой компанией. Эти сложности приводят к незнанию некоторых потребителей когда, кому, или на какую сумму они должны выставить счет или даже то, был ли платеж их ответственностью или ответственностью страховой компании.

Платформа Patientory спроектирована для усиления и блокчейн технологий Ethereum, и Применимых программных интерфейсов, соответствующих Ресурсам быстрого медицинского взаимодействия (FHIR), чтобы увеличить эффективность, позволить присуждать компенсации почти в реальном времени, предоставить прозрачные соглашения между заинтересованными сторонами и сократить мошенничество.

FHIR создавалась как отраслевой стандарт для форматирования данных, таким образом, сокращая сложность интеграции для медицинских и страховых унаследованных систем. Ключевым аспектом нашего решения, вследствие стоимости добавления данных в блокчейн, является использование только данных, необходимых для исполнения умными контрактами.

Со связанными затратами страхования и выставления счета, которые, как ожидается, достигнут 315 миллиардов долларов США в 2018г., и медицинскими офисами, проводящими 3,8 часа каждую неделю во взаимодействии с плательщиками, наша платформа может существенно сократить эти операционные затраты. Те же самые методы, которые могут использоваться для взаимно-корреляционного анализа диагностической информации, могут использоваться для анализа жалоб по мошеннической деятельности. Этот анализ может также показать действия, такие как поведение поиска наркотика, путем одновременного появления многократных жалоб. Оба этих варианта использования увеличивают предлагаемые преимущества использования этой системы страховыми

компаниями, но всецелое преимущество выходит за рамки этой информации.

Вследствие основанной на правилах системы, которая выполняется системой умных контрактов, все соглашения могут быть закодированы умными контрактами, на которые ссылаются конечные пользователи. Это позволяло бы медицинскому учреждению запрашивать систему для проверки существования покрытия до предоставления услуг. Использование системы для хранения информации о затратах также позволяет использовать автоматическое выставление счетов между учреждениями и частными лицами, как долг на основе токена. Таким образом, учреждение и частное лицо могут быть осведомлены относительно затрат, как только они появились. Это сокращает рабочую нагрузку на бухгалтерские отделы, при этом облегчая адаптацию системы.

Вот почему Patientory является платежной системой замкнутого цикла. Ожидается, что соединение перекрестной цепочкой может даже допускать безопасный обмен значениями через общедоступный блокчейн Ethereum. Этот механизм уже работает для решения конфликтов транзакций Биткоина, несмотря на то, что он требует наличия доверенного объекта, чтобы действовать как Oracle.

B. Выполнимость

Эта архитектура может быть создана с помощью существующих механизмов. Примером может быть соединение соответствующей HIPAA системы хранения данных веб-сервиса Amazon, с развертываемым ErisDB. Это программное обеспечение как услуга включает быстрое развертывание блокчейна с умными контрактами Ethereum со средствами управления с полностью разрешенным доступом, такими как вышеупомянутые средства. Понадобится добавление пассивных узлов, но это минимальные затраты на разработку по сравнению с развитием полной архитектуры.

С трехъярусной архитектурой умных контрактов Patientory только подмножество функций умного контракта реализуется на блокчейне Ethereum. Сложная бизнес-логика уходит с пути выполнения, что позволяет оптимизировать ярус данных для отражения распределенной природы сети.

Компоненты пакета умного контракта, реализованные на блокчейне Ethereum, являются схемой базы данных, проверкой и верификацией операций, которые добавляются в реестр, и логикой оптимизации запросов для чтения реестра. Бизнес-логика сдерживается выше блокчейна Ethereum до отдельного среднего (бизнес-) уровня. Этот логический код имеет доступ ко множеству услуг, включая безопасное выполнение, аттестацию, идентификационные данные, криптографическую поддержку, форматирование данных, надежный обмен сообщениями, триггеры и

способность связать этот код со схемой в определенных умных контрактах на любом числе блокчейнов, разрешая Patientory подключаться к различным медицинским консорциумам. Эти услуги предоставляются в матрице, где отдельные части кода, которые поддерживают умные контракты, могут выполнить, отправить операции в блокчейн узлы, и быть связанными со схемой на ярусе данных.

3.9 Дополнительные уникальные преимущества

Несмотря на то, что медицинское учреждение, такое как больница, не должно иметь доступа ни к каким медкартам, которые не были специально утверждены, при наличии предварительной авторизации пользователей на обмен информацией в чрезвычайных ситуациях, конечный пользователь может получить дополнительную выгоду от участия в сервисе. Учитывая это, потребность медицинского учреждения получить доступ к медкарте человека, который находится без сознания, в чрезвычайной ситуации составляет ситуацию, которая поощряет расширение полномочий, данных пользователю, который ранее авторизовал этот доступ. Если пациент находится без сознания и имеет с собой смартфон, учреждение может доказать привязанность устройства пациента при помощи метода вторичной подписи, который доступен на экране блокировки смартфона. Этот второй ключ не должен совпадать с закрытым ключом основной учетной записи. Таким образом, если учетная запись учреждения отправляет запрос блокчейну, содержащему открытый ключ частного лица, и смартфон этого частного лица отправил подпись чрезвычайной ситуации, блокчейн может передать полномочие предоставить доступ к медицинской карте. **Этот закрытый ключ нужно считать опасным и частное лицо должно заменить его как можно скорее. Таким образом, безопасный обмен информацией между частным лицом и уполномоченным учреждением может быть упрощен в экстренных случаях**.

Если учреждение запрашивает эту информацию без надлежащей авторизации, частное лицо будет уведомлено относительно этих действий. Если частное лицо отклоняет этот запрос в предельном интервале, данные не передаются. Далее, если учреждение делает множество попыток мошеннических запросов, учреждение может быть наказано аннулированием полномочий, денежным штрафом и/или юридическими действиями. Ущерб, нанесенный при потере сотового устройства, минимален вследствие потребности и в сотовом устройстве, и в ключе уровня учреждения. В обозримом будущем все страховые карты будут оборудованы встроенными криптографическими микроконтроллерами, такими как у современных кредитных карт, которые упростят те же действия, независимо от смартфона.

4 Национальные и международные приоритеты здравоохранения

4.1 Персонализированный уход

Для достижения эффективного ухода за больным, важен подход, сфокусированный на личности. Такой подход должен принять во внимание не только клинические аспекты, но и социально-экономические факторы, которые препятствуют способности успешно участвовать в лечении и здоровом образе жизни для получения постоянного хорошего здоровья.

Чтобы получить эффективные результаты лечения, нужно четко определить препятствия для здоровья человека и жизненные ситуации. С растущим числом пациентов, имеющих более двух сопутствующих заболеваний, "изолированный" однотипный подход оказания медпомощи "для всех" не способствует мотивации и достижению эффективных результатов лечения. Следовательно, нужно рассмотреть более гибкую модель ухода за больным, адаптированную для включения многоаспектных потребностей здоровья и хорошего самочувствия пациентов. Требуется всесторонний, динамичный, интерактивный план ухода, за которым пациент может активно следить, управлять им и участвовать в своем лечении.

4.2 Результаты лечения

Показатели результатов, связанных с пациентом (PROM) получили дополнительное значение и важность в течение последних нескольких лет. Это произошло, частично, благодаря повышенному вниманию к опыту лечения пациентов и сфокусированной на пациентах оценке нагрузки и влияния болезни. PROM могут включать признаки и другие аспекты индикаторов качества жизни, связанных со здоровьем, такие как физическая или социальная функция, соблюдение предписанного лечения и удовлетворенность лечением. Они могут также упростить более детальное общение врача и пациента с точки зрения нагрузки заболеваний, обеспечив более подробную и полную оценку лечения для особых случаев, таких как рак или рассеянный склероз.

PROM отличны от традиционных клинических мер по эффективности (например, продление выживаемости при раке, отказ от курения), потому что они непосредственно отражают влияние болезни и ее лечения с точки зрения пациента. Можно исследовать баланс между эффективностью лечения и его нагрузкой на пациента. Контроль показателей результатов

также эффективен при рассмотрении таких областей, как физическое функционирование и общее состояние здоровье, и при выделении эффективности и безопасности лечения по отношению к его общему клиническому преимуществу. Поскольку сами меры разработаны для пациента, они могут также упростить участие пациента в принятии решений относительно своего лечения, а также дать инструкции для решений здравоохранения. По существу, укрепление блокчейн инфраструктуры PROM улучшает возможность стимулировать поставщиков и плательщиков соответственно стандартам ухода за пациентом.

5 Заключение

Блокчейн будет играть все более и более значительную роль в IT здравоохранения и приносить полезную дестабилизацию и новую эффективность каждой заинтересованной стороне в экосистеме. Жизненно важно, чтобы медицинские организации поняли сущность блокчейн технологии, чтобы гарантировать, что они готовы к изменениям, которые влечет за собой технология.

Результатом будет новое поколение мощных, основанных на блокчейне приложений, которые сформируют следующую эру бизнеса в здравоохранении. Для выполнения своего потенциала в здравоохранении блокчейн должен основываться на стандартах для выполнения совместимости и взаимодействия в изолированной среде системы здравоохранения. www.patientory.com
Google Slack Twitter Facebook Reddit BitcoinTalk GitHub Telegram Medium

Упоминания

[1] “A Begoyan. An overview of interoperability standards for electronic health records.” In: (2007.).

[2] Charles N Mead et al. “Data interchange standards in healthcare itcomputable semantic interoperability: Now possible but still dicult. do we really need a better mousetrap?” In: (2006.).

[3] Thiago Vieira Joe Paradiso Andrew Lippman Ariel Ekblaw Asaf Azaria. “MedRec”. In: (2016). url: www.pubpub.org/pub/medrec.[Accessed: 05-Apr-2017].

[4] National Healthcare Ant-Fraud Association. “The Challenge of Health Care Fraud”. In: (). url: https://www.nhcaa.org/resources/healthcare-anti-fraud-resources/the-challenge-of-health-carefraud.aspx.

[5] Vitalik Buterin. “A next-generation smart contract and decentralized application platform. White Paper”. In: (2014.).

[6] Yan-Cheng Chang and Michael Mitzenmacher. “Privacy preserving keyword searches on remote encrypted data.In International Conference on Applied Cryptography and Network Security”. In: ().

[7] Mayo Clinic. “Changes in Burnout and Satisfaction With Work-Life Balance in Physicians and the General US Working Population Between 2011 and 2014”. In: (). url: www.mayoclinicproceedings.org.

[8] Hendrik Tanjaya Tan Darvin Kurniawan David Chandra. “Reidao: Digitising Real Estate Ownership”. In: (). url: http://reidao.io/whitepaper. pdf.

[9] et al. Centers for Disease Control Prevention. “HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services.” In: (2003.).

[10] Roy Thomas Fielding. “Architectural styles and the design of networkbased software architectures.” In: (2000.).

[11] HHS.gov. “H. H. S. O. of the Secretary Summary of the HIPAA Privacy Rule”. In: (2013). url: www.hhs.gov/hipaa/for-professionals/ privacy/laws-regulations/index.html.[Accessed:04-Apr-2017].

[12] HHS.gov. “Methods for De-identification of PHI”. In: (2015). url: https: //www.hhs.gov/hipaa/for-professionals/privacy/specialtopics/de-identification/index.html#protected.[Accessed:04Apr-2017].

[13] Alex Mizrahi Iddo Bentov Charles Lee and Meni Rosenfeld. “Proof of activity: Extending bitcoin’s proof of work via proof of stake.” In: (2014).

[14] Sunny King and Scott Nadal. “PPCoin: Peer-to-peer crypto-currency with proof-of-stake.” In: (2012).

[15] Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. In: (2008).

[16] Stean D Norberhuis. In: ().

[17] Pishing Chiang Philip Chuang Maureen Madden Rainer Winnen-burg Rob McClure Steve Emrick Olivier Bodenreider Duc Nguyen and Ivor DSouza. “The NLM Value Set Authority Center.” In: (2013.).

[18] Amit P Sheth. “Changing focus on interoperability in information systems: from system, syntax, structure to semantics. In Interoperating Geographic Information Systems,” in: (1999.).

[19] Nick Szabo. “Formalizing and securing relationships on public networks.” In: (1997.).

[20] “US GPO. CFRx 164 security and privacy. 2008.” In: (). url: http:

//www.access.gpo.gov/nara/cfr/waisidx08/45cfr16408.html. Accessed:2016-08-06..