

Министерство образования Республики Беларусь  
Учреждение образования  
Белорусский государственный университет  
информатики и радиоэлектроники

УДК 004.75

Саскевич  
Алексей Владимирович

Применение смарт-контрактов для создания единого реестра пациентов

**АВТОРЕФЕРАТ**  
на соискание академической степени  
магистра информатики и вычислительной техники

по специальности 1-40 81 04 – Обработка больших объемов информации

Научный руководитель  
Стержанов М.В.  
к. т. н., доцент

Минск 2019

## КРАТКОЕ ВВЕДЕНИЕ

История развития информационных технологий и защиты информации может быть представлена в виде нескольких этапов или эпох, каждая из которых отличается способом хранения информации, ее защиты и шифрования.

Первый этап отличался относительной примитивностью хранения и использования данных в информационных системах. Вычислительные машины были доступны лишь узкому кругу исследователей и научных заведений и использовались разве что для различных вычислений и управления. На таком этапе развития вычислительных систем даже не было необходимости задаваться вопросом о защищенности информации.

Затем, с появлением первых персональных компьютеров, появились и первые способы взлома программного обеспечения. Разработка первого прототипа сети Интернет поставила вопрос того, как компьютеры могут обмениваться данными и как обеспечить сохранность их. Были разработаны простейшие алгоритмы проверки данных на целостность, например, контрольные суммы.

Затем, с развитием сети Интернет и появлением множества веб-сервисов, появилась потребность в защите программного кода от взлома, а данных – от подмены. С обретением широкого распространения электронных устройств и сети Интернет появились сотни способов взлома, инструментов и программных средств для защиты данных и физических устройств.

На текущий момент, появление технологии блокчейн перевело вопрос защиты информации и вычислительных систем в новую плоскость. Блокчейн позволил взглянуть на вопрос отказоустойчивости, распределенных вычислений и хранения информации, шифрования и анализа данных с новой стороны.

Изначально, технология блокчейн неразрывно связана с таким явлением как “биткойн”. Виртуальная валюта, разработанная неизвестным автором, скрывающимся под псевдонимом Сатоши Накамото, обрела свою популярность среди гиков, а затем – среди огромного множества людей, интересующихся технологиями и финансами. Рост популярности биткойна привел к появлению множества альтернативных решений и программных средств, так или иначе основанных на технологии блокчейн.

На текущий момент таких решений более двух тысяч. Многие из них решают задачи, связанные со сферой финансов, однако есть и такие решения,

которые призваны улучшить или изменить такие сферы жизни как политику, образование и здравоохранение.

Активное развитие информационных технологий не всегда означает, что жизнь и развитие общества будет успевать за ними. На сегодняшний день существуют такие направления и сферы жизни общества, которые условно могут считаться отстающими от современных технологий. К ним можно отнести и здравоохранение. Современная организация системы здравоохранения не позволяет собрать воедино всю ту информацию, статистику и опыт, получаемый в процессе обслуживания миллиардов людей. Разрозненные данные о болезнях, методах лечения, исследованиях, испытаниях лекарств и тому подобные “крупницы” информации чаще всего находятся во владении отдельными субъектами медицины, в результате чего качество обслуживания и перспективы решения вопросов медицины (например, поиск лекарств от неизлечимых на текущий момент болезней) отстает от активного роста информационных технологий.

Блокчейн и смарт-контракты как сами по себе уникальные технологии имеют определенный шанс на то, чтобы сместить традиционные методы хранения и обработки информации и занять доминирующее положение.

Данная диссертационная работа посвящена именно этим новым технологиям, способным кардинально изменить не только сферу здравоохранения, но и подход человека к работе с информационными технологиями в целом. Работа рассматривает непосредственную возможность применения технологий блокчейн и смарт-контрактов в рамках работы с информацией пациентов, страховых компаний, фармацевтических корпораций.

# ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

## Цель и задачи исследования

*Целью* диссертационной работы является исследование научного и практического применения технологий блокчейн и смарт-контрактов для хранения больших объемов информации, их последующей обработки и анализа, в частности, в сфере здравоохранения.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Исследовать выбранные технологии на предмет применимости в отношении обработки больших объемов информации.
2. Обосновать необходимость применения технологий блокчейн и смарт-контрактов в сфере здравоохранения.
3. Разработать архитектуру приложения для хранения информации о пациентах учреждений здравоохранения и использования ее для дальнейшего анализа.

*Объектом* исследования являются технологии блокчейн и смарт-контрактов и их применение в хранении и обработке информации, в частности, в сфере здравоохранения.

*Предметом* исследования является возможность и перспективность использования объекта исследования для создания реестра пациентов с целью хранения и последующего анализа информации.

*Актуальность* исследования заключается в том, что технологии смарт-контрактов и блокчейн позволяют хранить большие объемы информации практически без ограничений по количеству, без привязки к централизованному хранилищу или владельцу. Кроме того, технология смарт-контрактов позволяет не только хранить данные, но и применять различные алгоритмы, позволяющие работать над ними – изменять, вычислять, контролировать. В сфере здравоохранения способы хранения и обработки информации особенно важны, что делает вопрос хранения, защиты и обработки данных самой разнообразной формы особенно актуальным.

Основной *гипотезой*, положенной в основу диссертационной работы, является перспективность технологий блокчейн и смарт-контрактов, их положительные качества по сравнению с альтернативными традиционными технологиями хранения и обработки информации, возможность синтеза на основе новых и традиционных технологий. Возможности применения данных

технологий и результата их применения способны улучшить качество услуг, получаемых в медицинских учреждениях самого широкого спектра.

### **Личный вклад соискателя**

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя М. В. Стержанова, заключается в формулировке целей и задач исследований.

### **Апробация результатов диссертации**

Основные положения диссертационной работы докладывались на 55-ой научной конференции аспирантов, магистрантов и студентов БГУИР (Минск, Беларусь, 2019).

### **Опубликованность результатов диссертации**

По теме диссертации опубликовано 4 печатные работы, из них 2 статьи в рецензируемом издании, 2 работы в сборниках трудов и материалов научных конференций.

### **Структура и объем диссертации**

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, списка использованных источников, списка публикаций автора и приложений. В первой главе представлен анализ предметной области, выявлены исторические особенности развития объекта исследования, выявлены недостатки и преимущества технологий блокчейн и смарт-контрактов в решении поставленной задачи. Вторая глава посвящена анализу сферы здравоохранения на предмет недостатков, процессов, требующих автоматизации путем внедрения информационных систем. Третья глава содержит этапы проектирования архитектуры системы, отдельных ее модулей и общего результата. В четвертой главе представлены результаты исследования, полученные преимущества и недостатки разработанной системы, ее перспективы, а также сравнение с существующими аналогами в сфере блокчейн-проектов.

Общий объем работы составляет 81 страницу, из которых основного текста – 58 страниц, 13 рисунков на 6 страниц, 6 таблиц на 4 страницы, список использованных источников из 84 наименований на 6 страниц и 4 приложений на 7 страниц.

## ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** представлено краткое описание истории технологии блокчейн и смарт-контрактов, их истоки и причины появления. Также обозначены причины для выполнения данной диссертационной работы.

В **первой главе** проведен анализ технологий по нескольким показателям, таким как быстрдействие, удобство разработки, целенаправленность и другие. В первую очередь стоит описать непосредственно само понятие блокчейн-технологии, основные ее понятия. Среди таких такие понятия как “транзакция”, “блок транзакций”, “цепочка блоков”, “блок”, “сложность” и некоторые другие.

В первую очередь стоит определить, что является транзакцией. В данном случае, транзакция – это подписанная криптографической функцией операция по передаче информации от одного владельца другому, хранящаяся в блоке транзакций и содержащая ссылку на предыдущую транзакцию, тем самым обеспечивая безопасность и защищенность записи.

Блок транзакций – специальная структура данных, хранящая совокупность транзакций, подписанная с использованием определенной криптографической функций. Особенность блока в его открытости – возможно отследить, какие транзакции были сохранены в блок, а какой блок является предшественником данного блока.

Информация в блоках хранится в открытом виде, а ее корректность подтверждается на основе хэш-функции, альтернативы цифровой подписи. Генерация хеш-функции нового блока на основе предыдущих блоков лишает возможности подменить информацию где-то ранее – необходимо будет произвести повторную генерацию всех блоков, лежащих между измененным и последним, а это достаточно ресурсоемкая задача, с которой текущие технические средства не могут справиться за лимитированное время.

Если сравнивать сеть блокчейна и стандартную клиент-серверную сеть, можно заметить разницу, что в сети блокчейн все устройства могут быть связаны со множеством остальных устройств и имеют одинаковый приоритет в работе. В то же время стандартная модель, в которой различают клиентское

устройство и сервер, указывает на то, что устройства, функционирующие в данной сети, имеют разный приоритет и функционирование одних зависит от функционирования других.

Биткоин не является единственной системой, которая использует в своей основе блокчейн. На текущий момент блокчейн получил свое развитие в различных формах и альтернативах.

Различные алгоритмы консенсуса также привели к появлению разнообразных альтернатив блокчейна, со своими плюсами и минусами. Существует не менее пяти алгоритмов консенсуса, применяемых в современных сетях.

Стоит отметить, что в качестве данных, которые блокчейн способен хранить, могут быть не только данные о том, кто кому и сколько перевел виртуальной валюты, а также любые другие данные, например, передача права собственности на жилье, исторические записи научных наблюдений и многое другое. Блокчейн является распределенной реплицируемой децентрализованной базой данных, и это – самое главное свойство технологии. В тех сферах общества, где необходима защита от подмены информации, подделки ее, где необходима отказоустойчивость и синхронизация, стоит обратить внимание на возможности применения технологии блокчейн в качестве альтернативы традиционным базам данных.

Операции, лежащие в основе транзакций, описываются некоторым программным кодом. В одном случае, этот программный код фиксирован, в другом – имеется возможность создать транзакции со своим программным кодом. Смарт-контракты являются тем самым программным кодом, функционирующим в рамках сети блокчейн.

Более формально, смарт-контракт – компьютерная программа или алгоритм, предназначенный для управления и изменения, контроля владением чего-либо. В техническом понимании, смарт-контракт – набор функций и кода, хранящихся в блокчейне по определенному адресу и которые могут быть выполнены в рамках блокчейна.

Практически каждая имплементация блокчейна имеет в своей основе базовую версию смарт-контрактов. Биткоин, оставаясь по сути практически классическим примером при исследованиях в данном направлении, не является исключением.

Блокчейн-платформа Этериум (Ethereum) стала логическим развитием платформы Биткоин, призванным решить проблемы, лежащие в основе платформы-первопроходца.

Развитие технологии блокчейн закономерно привело к появлению бизнес- и промышленных решений, призванных привести использование блокчейна в различные сферы экономики.

Одним из таких решений является набор инструментов и платформа от компании IBM – Hyperledger Fabric и Hyperledger SDK. Данный набор инструментов позволяет разворачивать частную блокчейн-сеть, основанную на использовании такого подхода как контейнеризация, например, на основе контейнеров Docker.

Преимуществом технологии блокчейн по сравнению с альтернативными реплицируемыми распределенными системами стоит отметить их гибкость, возможность реализации собственных решений (чаще всего традиционные реплицируемые базы данных ограничены стандартными возможностями типа триггеров и событий), а также простоту запуска. Чаще всего нет необходимости выполнять сложную настройку того, как должны работать узлы сети, достаточно всего лишь установить необходимое программное обеспечение на машину и запустить его, поиск других узлов, загрузку смарт-контрактов и реплики программное обеспечение выполнит самостоятельно. Блокчейн применим практически в любой сфере промышленности и жизни человека.

Во **второй главе** описаны недостатки сферы здравоохранения как таковой, а также способы устранения их недостатков. В данной сфере можно выделить следующие направления и области здравоохранения, имеющие недостатки и требующие их устранения:

- Непрозрачность движения персональных данных. Пациент не всегда знает где и как используется его информация.

- Отсутствие структурированности информации. В разных медицинских учреждениях часто свой способ хранения данных, заполнения и обработки медицинских карточек.

- Децентрализованность персональных данных. Порой различные данные об обследованиях, анализах, консультациях или лечениях находятся у разных специалистов, в разных и несвязанных между собой учреждениях здравоохранения и даже на разных устройствах и приборах.

- Отсутствие контроля за состоянием и обеспечением медицинским оборудованием. Отсутствие структурированности и прозрачной доступности данной информации.

- Отсутствие детальной и прозрачной информации об испытаниях медикаментов, их применении и поставке.



– Отсутствие надлежащего контроля за выполнением обязательств персонала, его уровнями доступа и ответственности.

– Отсутствие прозрачного механизма формирования страховых пакетов для разных слоев населения.

– Отсутствие финансового контроля за движением бюджетных средств, средств, выделяемых различными фондами и страховых средств.

Технология блокчейн в своей сути имеет свои преимущества, как например децентрализованность, распределенность, безопасность и другие качества. В то же время в главе были представлены пункты, по которым блокчейн выигрывает у традиционных системах хранения и обработки данных.

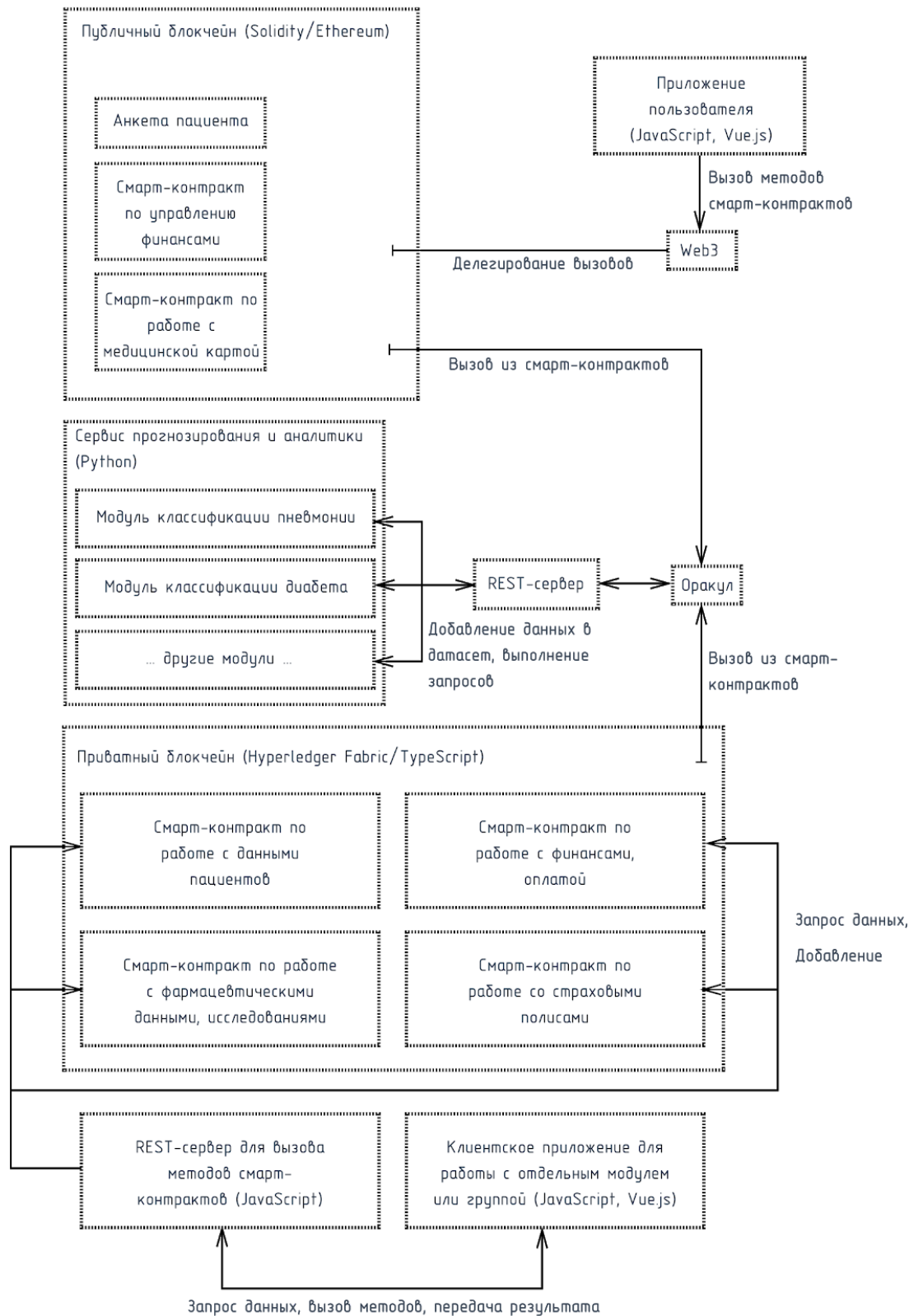
Существующие открытые и экспериментальные проекты также являются примером успешного применения технологии блокчейн и смарт-контрактов.

Все это означает, что в решении поставленной задачи выбранный объект исследования может быть применен и вполне результативно.

В **третьей главе** проводится исследовательская работа по проектированию архитектуры приложения, ее разработке, а также отдельных его частей – клиентской части для пациентов, серверной для врачей и прочих работников сферы, сервиса аналитики с машинным обучением.

С учетом описанной в главе архитектуры получается достаточно гибкая расширяемая система. Гибкость обеспечивается за счет возможности добавлять новую функциональность, новые роли, новые модели. Расширяемость обеспечивается модульной системой – разработчик может добавлять свои новые модули в сервис анализа данных, возможности приватной блокчейн-сети могут быть расширены за счет новых смарт-контрактов, которые могут быть необходимы в работе какой-то узкоспециализированной отрасли медицины и здравоохранения, система ролей, которая предлагается практически “из коробки”, позволяет гибко управлять возможностями и привилегиями как пациентов, так и врачей.

В разработке системы используется широкий спектр технологий и подходов, что, конечно, накладывает ограничения на скорость разработки – в идеальном случае требуется несколько узкоспециализированных разработчиков, каждый из которых разбирается в какой-то конкретной области, будь то блокчейн, машинное обучение, веб-программирование. В рамках же работы система состоит из нескольких частей, представленных на рисунке 1:



**Рисунок 1 – Полная архитектура приложения**

В четвертой главе производится заключительный анализ и исследование проведенной работы, оценка результатов и сравнение с аналогами.

Разработанное решение имеет как свои преимущества, так и свои недостатки. Часть недостатков вытекает из молодости технологии блокчейн как таковой. По факту, блокчейн пока не нашел широкого применения в промышленности, а разработанные и разрабатываемые решения – попытки сформировать идею использования технологии среди энтузиастов. Несмотря на это, предпринимаются попытки создать или применить уже существующие решения компаниями-гигантами информационных технологий, такими как IBM и Amazon. Однако, до того момента, как технология стандартизируется, будут решены насущные проблемы с быстродействием, пройдет еще несколько лет. В течение этого времени будут совершаться новые попытки, часть из которых может оказаться успешной.

С другой стороны, рассматривая полученный результат, можно смело утверждать, что свои непосредственные задачи технология выполняет, кроме того, уже существуют инструменты, позволяющие связать традиционные технологии и технологии, которые находятся в зачаточном состоянии. Огромное количество блокчейн-проектов – тому показатель.

## **ЗАКЛЮЧЕНИЕ**

### **Основные научные результаты диссертации**

1. Исследованы и обобщены текущие инструменты и возможности технологии блокчейн. В частности, рассмотрены возможности по части реализации смарт-контрактов, их возможностей и перспектив. Наилучшими из рассмотренных оказались Ethereum с языком программирования Solidity и гибкая блокчейн-платформа для бизнес-решений Hyperledger.

2. Исследованы перспективы и причины для применения технологий блокчейн в сфере здравоохранения, недостатки и проблемы сферы, требующие поиска решений.

3. Разработана и обоснована архитектура программного продукта, призванного решить обнаруженные проблемы сферы здравоохранения и нацеленного на достижение положительного результата в управлении финансами, диагностике, логистике и смежных областях.

4. Исследованы и обобщены текущие недостатки технологии блокчейн, их особенности и последствия для проектов, пытающихся использовать блокчейн в качестве основной и опорной технологии.

## **Рекомендации по практическому использованию результатов**

1. Полученные результаты формируют достаточную теоретическую базу для разработки программного обеспечения на основе технологии блокчейн. Кроме того, они могут быть использованы для дальнейшего исследования и развития представленной системы.

2. Разработанная архитектура приложения и подходы могут применяться не только в сфере здравоохранения, но и в любой другой, способной к автоматизации. На основе разработанной архитектуры возможно создание системы любой сложности и масштаба.

3. Результаты работы могут использоваться при подготовке специалистов в области программного обеспечения, компьютерных сетей и технологий блокчейн.

## **СПИСОК ОПУБЛИКОВАННЫХ РАБОТ**

1-А. Саскевич, А. В. ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ БЛОКЧЕЙН И СМАРТ–КОНТРАКТОВ В СФЕРЕ ЗДРАВООХРАНЕНИЯ / Саскевич А.В. // Научный потенциал молодежи – будущему Беларуси: материалы XII международной молодежной научно–практической конференции, УО "Полесский государственный университет", г. Пинск, 6 апреля 2018 г. Ч.1 / Министерство образования Республики Беларусь [и др.]; редкол.: К.К. Шебеко [и др.]. – Пинск: ПолесГУ, 2018. – С. 264-265

2-А. Саскевич, А. В. БЛОКЧЕЙН-ПЛАТФОРМА HYPERLEDGER В СФЕРЕ ЗДРАВООХРАНЕНИЯ / А. В. Саскевич // Компьютерные системы и сети : материалы 55-й научной конференции аспирантов, магистрантов и студентов. (Минск, 22 – 26 апреля 2019 года). – Минск : БГУИР, 2019. – С. 133 - 134.

3-А. Саскевич, А. В. Актуальные направления блокчейн-проектов в сфере здравоохранения / А. В. Саскевич, В. М. Родько // Молодой ученый. — 2019. — №20. — С. 40-43.

4-А. Саскевич, А.В. ЦИФРОВИЗАЦИЯ И ИНФОРМАТИЗАЦИЯ В СФЕРЕ ЗДРАВООХРАНЕНИЯ / А.В. Саскевич, В. М. Родько // Международный научный журнал «Научные вести». – 2019. – №5 (10). – С. 182-187.