Health Insurance Support System

[github.com/maksimov1/HISS](https://github.com/maksimov1/HISS) , hissbb.com

Описание сервиса

HISS – единая база данных для хранения зашифрованных медицинских документов с использованием технологии блокчейн. Логика взаимодействия пациентов, врачей и страховой клиники реализована на смарт-контрактах.

Какие проблемы пользователей он решает

Для пациентов:

* Сложность взаимодействия с несколькими медучреждениями

На данный момент не существует удобного способа перенести свою историю болезни, например, из одной частной клиники в другую.

* Недоверие к системе хранения персональных медицинских данных

Для многих пациентов важно, чтобы записи в их медицинской книжке не прочитали посторонние. В нашем сервисе только пациент может расшифровать записи о себе.

Для врачей:

* Невозможно быстро получить всю историю болезни из других медучреждений

Например, при экстренной госпитализации будет тяжело получить записи из частной клиники, в которой обслуживался пациент. В HISS пациент может быстро расшифровать свои записи и передать врачам скорой помощи.

* Подделка документов

Существующий бумажный документооборот позволяет подделывать справки и направления к врачам. В нашей системе блокчейн – гарант того, что записи никто не подделал и не удалил из медицинской карты.

Страховой:

* Возможность обмануть страховую, подделка справок

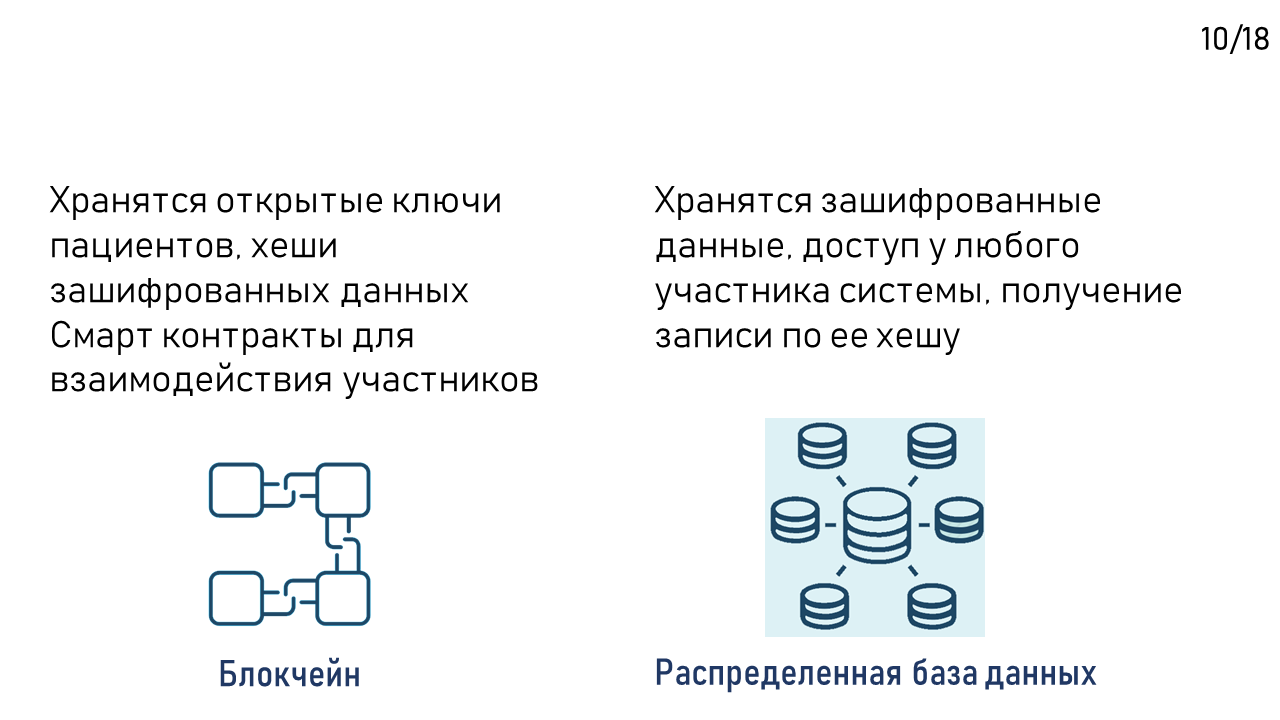
На данный момент можно обмануть страховую при наступлении страхового случая на бумаге, сделать какие-то справки задним числом. В нашем сервисе это невозможно.

* Отсутствие доверия со стороны клиентов

Регулировка взаимоотношений в системе при помощи смарт-контрактов позволит повысить доверие со стороны больниц или пациентов.

Как работает HISS?

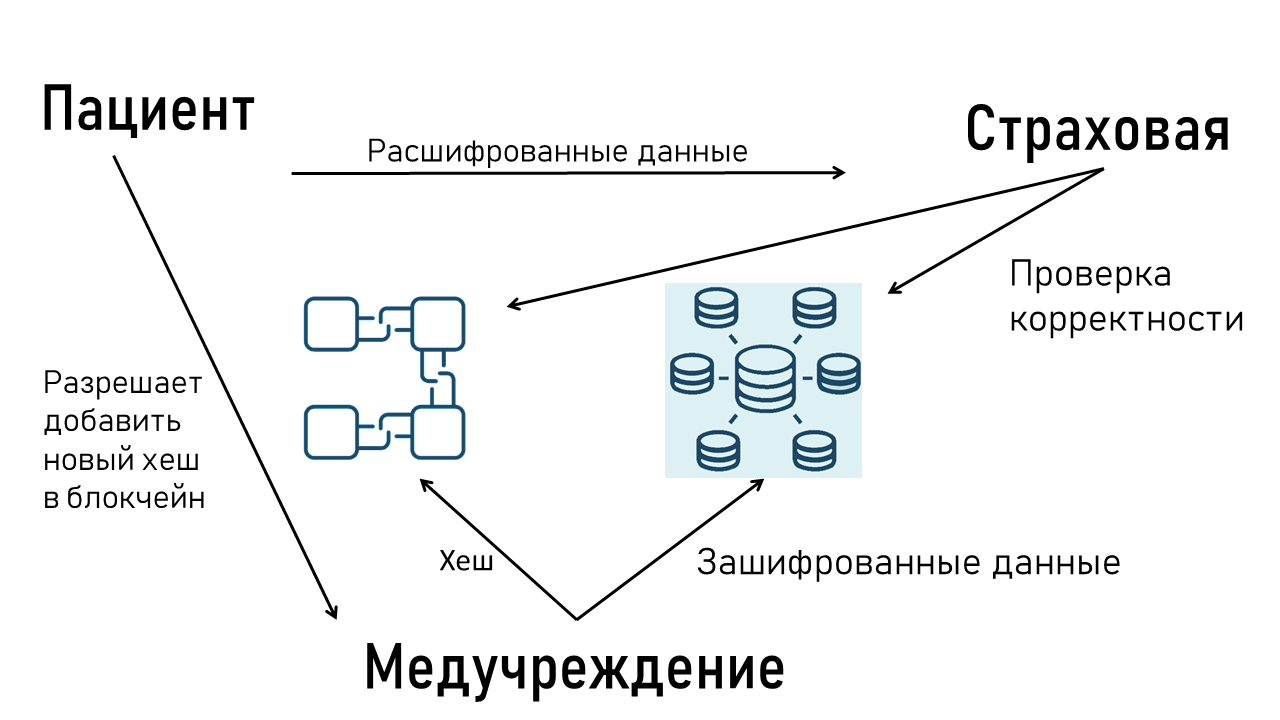
В блокчейне хранятся в открытом виде открытые ключи пациентов, которыми можно зашифровать данные. Закрытые ключи хранятся только у пациентов. Только они могут расшифровать медицинские записи врачей.



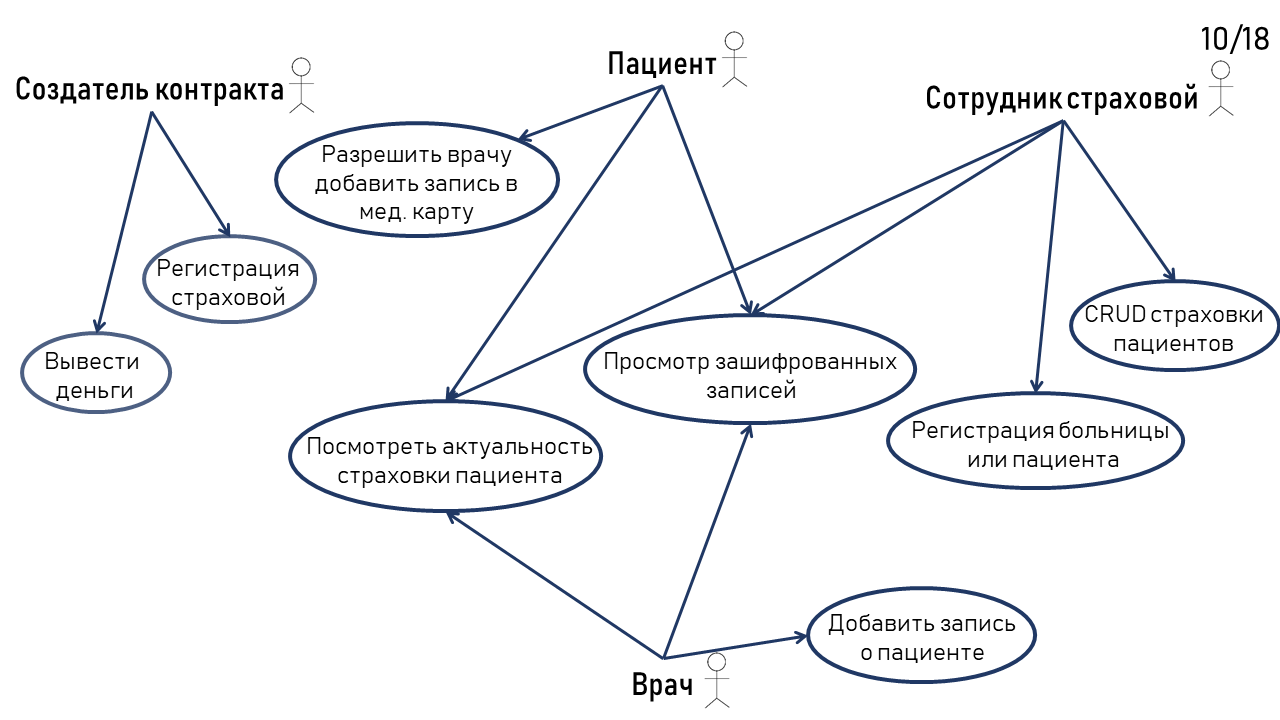
Врач, если он получил разрешение от пациента по смарт-контракту, он может добавить хеш зашифрованной записи в блокчейн. Врач шифрует запись, хеш зашифрованной записи добавляется в блокчейн, а сама зашифрованная запись добавляется в распределенную базу данных.

Пациент, если он хочет расшифровать запись, сверяет хеш зашифрованной записи и хеш в блокчейне, если они совпадают, то значит запись в базе данных никто не подменил, можно ее расшифровать.

Если пациент хочет расшифровать запись и передать ее другому врачу или страховой, то реципиент может верифицировать полученные расшифрованные данные. Если он их обратно зашифрует открытым ключом пациента (который находится в блокчейне и для всех открыт), и возьмет хеш-функцию от полученного документа, то хеш должен совпасть со значением в блокчейне.



UML диаграмма участников



Экономические рассчеты:

Оборот:

По данным опроса ВЦИОМ за 2015г. услугами платной медицины пользуется 8% россиян. Допустим, 10% из них будут пользоваться нашим сервисом за 200 ₽/год.

144.3 \* 10^6 \* 0.08 \* 0.1 \* 200 = 230 880 000 ₽/год.

Ориентировочные расходы на поддержание сервиса:

Облачное хранилище selectel.ru, в среднем 150 МБ и траффик 3гб – 45₽ на пользователя.

((150 \* 10 ^(-3) \* 1) + (3 \*1.2 )) \* 12 \* 144.3 \* 10^6 \* 0.08 \* 0.1 = 51 948 000 ₽/год

Прибыль: 230 880 000 - 51 948 000 = 178 932 000 ₽/год

Реализация

На данный момент реализован прототип hissbb.com. Работает шифрование и дешифрование записей, смарт контракт находится в тестовой сети Rinkeby. Для работы на сайте необходимо открыть в браузере chrome с расширением Metamask. Шифрование на данный момент – RSA.

Используемые технологии:

* Metamask – управление кошельками из браузера
* Web3 – управление работой с контрактом из браузера
* @web3/buzz – управление работой со swarm из браузера
* JSEncrypt – Шифрование в браузере и генерация ключей
* OpenZeppelin – управление ролями в контракте (RBAC)
* Truffle/Ganache – разработка и тестирование контрактов
* Swarm – собственный сервер swarm.hissbb.com для стабилизации работы системы
* IPFS – децентрализованной развертывание системы
* DigitalOcean + Cloudflare – централизованное развертывание системы

Новизна

Такого сервиса, основанного на блокчейне и сложном алгоритме шифрования и верификации данных ни у кого нет.

Осуществимость

На данный момент реализован прототип, демонстрирующий основной функционал сервиса, описанный выше. Реализовать такой сервис полностью не составит проблем.

Полезность

Для страховой HISS уменьшает вероятность подделки страхового случая, приносит дополнительный доход. Для пациента предоставляет гарантированное зашифрованное хранение данных. Для больниц реализует более удобный и надежный документооборот.