Семинар по информационным технологиям
(Челябинск, ЮУрГУ (НИУ), 18 сентября 2018 г.)

ТЕХНОЛОГИЯ БЛОКЧЕЙН И ЕЕ ПРИМЕНЕНИЕ

старший преподаватель кафедры СП,
Никольская Ксения Юрьевна

ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)

Децентрализация & распределенность

Распределенная система:

Компоненты, находящиеся на компьютерах, соединены общей сетью и находятся в взаимодействии и координации через передачу сообщений.

Децентрализованная система:

При децентрализации отсутствует единственная центральная точка контроля и обработки информации.

Блокчейн (технология)

- Сеть, состоящая из компьютеров, хранящих реестр транзакций
- Есть два ключа (приватный/публичный)
- Транзакция, которую можно проверить
- Каждая транзакция связывается с предыдущей
- Механизм консенсуса(кто вносит запись)

Ключевые особенности технологии

Децентрализация – в цепочке нет сервера. Каждый участник – это и есть сервер. Он поддерживает работу всего блокчейна.

Прозрачность – информация о транзакциях, контрактах и так далее хранится в открытом доступе. При этом эти данные невозможно изменить.

Теоретическая неограниченность – теоретически блокчейн можно дополнять записями до бесконечности. Поэтому его часто сравнивают с суперкомпьютером.

Надежность – для записи новых данных необходим консенсус узлов блокчейна. Это позволяет фильтровать операции и записывать только легитимные транзакции. Осуществить подмену хэша нереально.

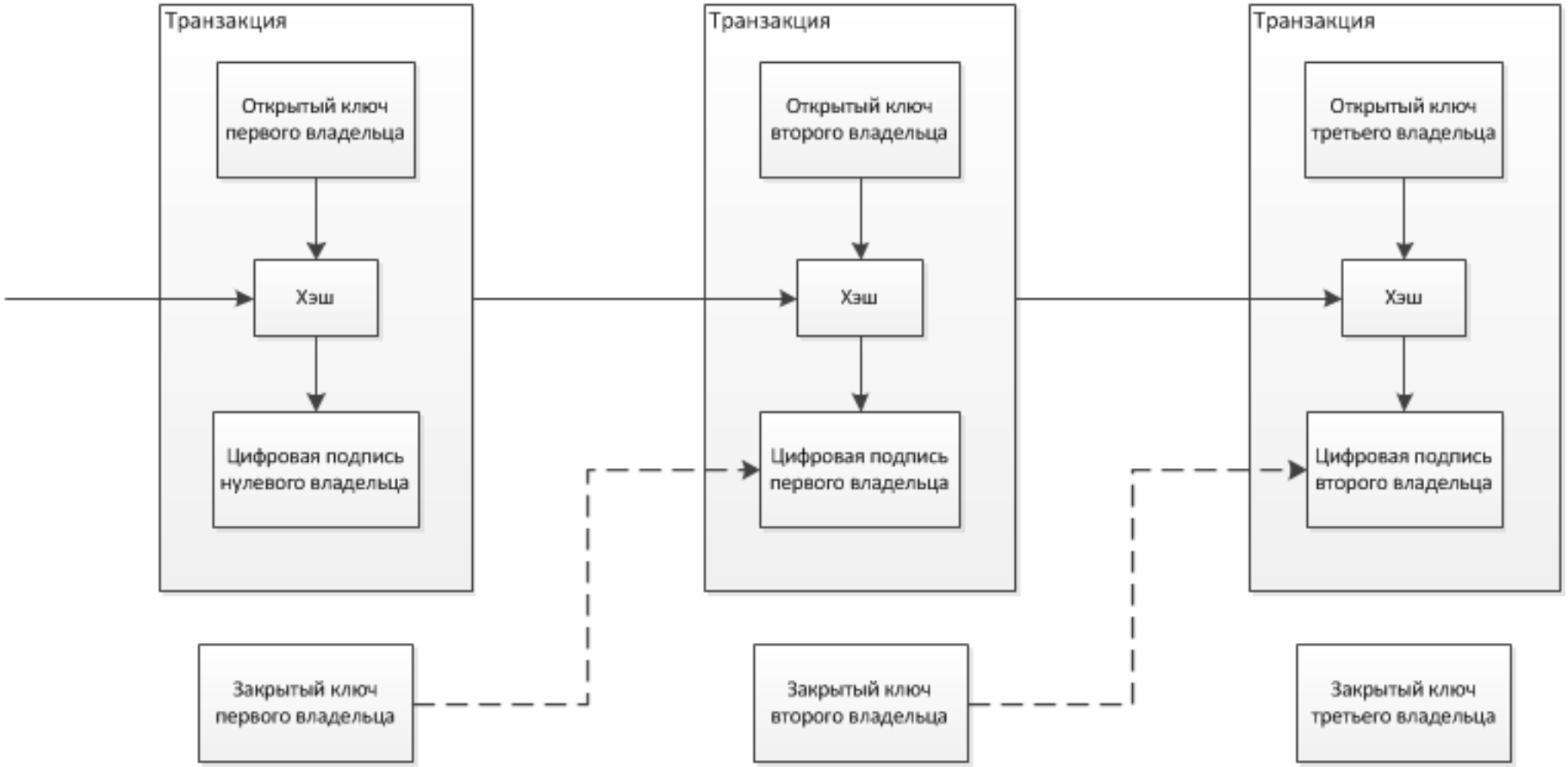
Типы блокчейна

1. Публичный – цепочка блоков, которая доступна другим пользователям.

2. Частный (сервисный) – цепочка блоков доступна всем пользователям, но их количество ограничено.

3. Приватный – цепочка, где доступ к чтению и записи ограничен.

Общий вид блоков данных в технологии распределенного реестра



Правила работы системы

1. Новые транзакции рассылаются всем узлам.

2. Каждый узел объединяет пришедшие транзакции в блок.

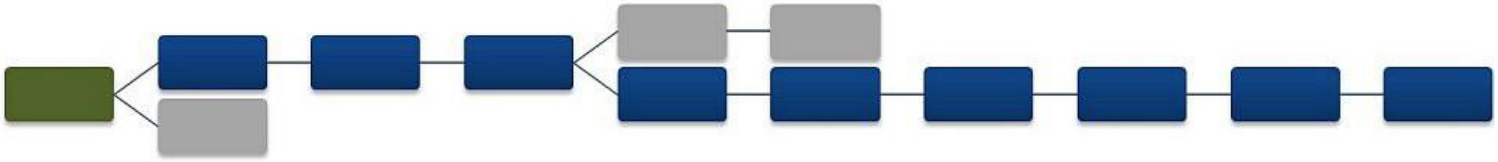
3. Каждый узел пытается подобрать хеш блока, удовлетворяющий текущей сложности.

4. Как только такой хеш найден, этот блок отправляется в сеть.

5. Узлы принимают блок, только если все транзакции в нем корректны и не используют уже потраченные средства.

6. Свое согласие с новыми данными узлы выражают, начиная работу над следующим блоком и используя хеш предыдущего в качестве новых исходных данных.

Блоки



Надёжность работы цепочки блокчейн обеспечивают специальные алгоритмы

1. Proof-of-Work (PoW).
2. Proof-of-Stake (PoS).
3. Delegated Proof-of-Stake (DPoS).
4. Leased Proof-of-Stake (LPoS).
5. Proof-of-Capacity (PoC).
6. Proof-of-Importance (PoI).
7. Proof-of-Activity (PoA).
8. Proof-of-Authority (PoAuthority).
9. Proof-of-Burn (PoB).

Proof-of-Work (PoW)

Основные недостатки:
- бессмысленные энергетические затраты;

- большое количество узлов производят вычисления, но в реальности только один (первый) проводит успешную работу и получает вознаграждение.

Proof-of-Stake (PoS)

Основными преимуществами:
- существенное снижение потребления электроэнергии (относительно PoW метода);
- для создания атаки Double-spending, необходимо сконцентрировать больше 50% от общего количества всей валюты, что будет стоить огромного состояния. В том случае, если же атакующий все же сможет сконцентрировать такое количество средств, он своими действиями нарушит баланс и сам больше пострадает от своей же атаки.

Основные недостатки:
- мотивация, в концентрации средств, что может приводить к централизации сети.

Delegated Proof-of-Stake (DPoS)

Основные преимущества:
- держатели балансов имеют возможность делегировать свои голоса (при этом не передавая сам баланс);
- держатели балансов имеют возможность получить дополнительный доход от их владения;
- минимизация издержек на поддержку блокчейн сети. В отличие от классического PoS, снижается количество "ненужной работы" при выборе следующего голосующего.

Leased Proof-of-Stake (LPoS)

Данный алгоритм консенсуса позволяет получить доход от майнинговой деятельности, не ведя самого майнинга.

Proof-of-Capacity (PoC)

Основное преимущество:

- вычислительные ресурсы необходимые майнеру для работы ограничены временем, которое необходимо для чтения файлов из дисковой подсистемы. Именно этот фактор позволяет производить майнинг с достаточно высокой энергоэффективностью.

Proof-of-Importance (PoI)

Основное преимущество:

- учитывает как количество средств, так и активность пользователя в блокчейн сети. Такой подход вовлекает пользователей не просто держать средства у себя на счету, но и активно использовать их.

Proof-of-Activity (PoA)

Принцип работы алгоритма:

- каждый майнер блокчейн сети пробует сгенерировать заголовок пустого блока, который включает в себя хеш предыдущего блока, публичный адрес майнера, индекс текущего блока в блокчейне и nonce.
- после генерации заголовка пустого блока отвечающего текущим требованиям сложности, узел рассылает этот заголовок в блокчейн сеть.
- все узлы сети рассматривают заголовок такого блока, как данные полученные от псевдослучайных владельцев. Используя хеш разосланного заголовка блока и хеш предыдущего блока + N пресетов с использованием алгоритма follow-the-satoshi выбираются стейкхолдеры.
- каждый стейкхолдер, находящийся в онлайне, проверяет полученный, пустой заголовок блока на его корректность. Во время проверки, каждый получивший заголовок, проверяет: является ли он одним из первых N-1 стейкхолдеров "счастливчиков" этого блока и в этом случае подписывает заголовок пустого блока своим секретным ключом и отправляет его в блокчейн сеть.
- Когда N-й стейкхолдер видит, что он должен стать подписантом этого блока, он, в дополнение к заголовку пустого блока, добавляет блок с включенными транзакциями (количество включаемых транзакций он выбирает сам), все подписи N-1 от других стейкхолдеров и подписывает блок.
- Стейкхолдер N рассылает новый, подготовленный блок. Узлы получают этот блок, убеждаются в его законности и добавляют этот блок в блокчейн.
- Премия за транзакции, которую получил N-стейкхолдер, распределяется между майнером и N стейкхолдерами "счастливчиками".

Proof-of-Authority (PoAuthority)

Основное преимущество:
- отсутствие майнинга и как следствие, существенное снижение затрат на его обслуживание.

Основной недостаток:
- как понятно из самого описания — ключевыми лицами, являются валидаторы, что приводит к централизации. Вероятно в некоторых случаях, в приватных сетях и при помощи полностью (на сколько это возможно) доверенных эккаунтов это имеет смысл.

Proof-of-Burn (PoB)

Основные преимущества:

- шансы на майнинг увеличиваются при увеличении количества сожженных монет;

- этот метод подходит для трансфера из «старых» в «новые» криптовалюты.

Какие вопросы необходимо решать при внедрении системы?

Архитектурная (де)централизация

Что из себя представляет система с точки зрения физического количества компьютеров? Какое количество компьютеров может выйти из строя, чтобы система при этом продолжала свою работу?

Политическая (де)централизация

Какое количество отдельных независимых организаций или индивидуумов контролируют эти компьютеры?

Логическая (де)централизация

Как выглядят интерфейс и структуры данных при дроблении системы?

Как выглядит консенсус? Кто может писать/читать в реестре?

Какие уровни конфиденциальности?

Голосование

• Электронное

• Тайное

• Но с возможностью отследить свой голос

Примеры:

- голосование в Эстонии (KLI-бесключевая подпись, Cybernetica)

-D-Demos (распределенное, e2e проверяемое интернет голосование)

Система электронного декларирования на блокчейне

- Отсутствие единого публичного реестра
- Представление данных
- Возможности для изменений/удаления информации
- Лист политически значимых лиц

Здравоохранение: коррупционные риски

Бумажная система ведения медицинского учета:

1. Пространство манипуляции информацией

2. Непрозрачность процедуры выдачи рецептов

3. Фальсификация медицинских справок

4. Несовершенство механизма проверки медучреждений со стороны ОМС и ДМС

Развитие электронной медицины в РФ

ЕГИСЗ:

Декабрь 2014 г. «Концепция информатизации регионов до 2018».

Начало 2016 г. Минздрав: ряд поправок в ФЗ. Темой заинтересовались: Совет Федерации, ФРИИ, Институт развития интернета. Создание в АП РФ Научного совета.

Май 2016 г.: общественные слушанья в ГД РФ.

31 августа 2016 Министр здравоохранения РФ Вероника Скворцова сообщила, что ИТ станет одним из главных направлений развития здравоохранения в стране.

Апрель 2017 г.: законопроект с поправками 2016 г. внесен в ГД РФ.

Сфера внедрения

- Медицинские учреждения
- Страховые компании
- Клиническая медицина

Преимущества технологии блокчейн

1. Данные, которые вносятся в блокчейн невозможно подменить
2. Предотвращение манипуляции данных об истории болезней
3. Транспарентность механизма выдачи
4. Прямой и полный доступ к информации медучреждений со стороны ОМС и ДМС

Форма внедрения

• Блокчейн-платформа содержащая в себе информацию о каждом пациенте.

• Страховые медучереждения смогут просматривать информацию о пациенте на основе «умных» контрактов, где можно прописать условия получения доступа к персональным данным.

Примеры внедрения в сфере здравоохранения

Эстонии и Германии действует блокчейн-платформа, в которой существует электронная медкарта, выдача электронных рецептов. Подлог данных со стороны любой организации и самого гражданина невозможен.

В ОАЭ совместно с эстонскими разработчиками ведется внедрение эстонского типа блокчейн-платформы в здравоохранении.

В Великобритании разрабатывается собственная блокчейн-система в медсфере. Уже идет тестирование данной платформы.

В США создание блокчейн-системы пока на стадии обсуждения.

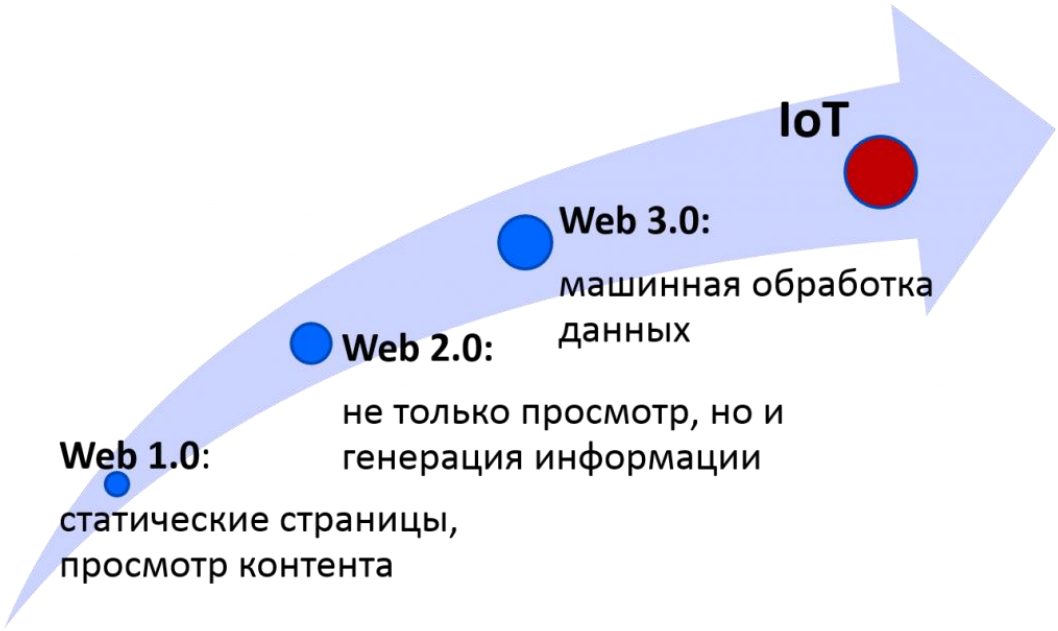
Проблемы применения в РФ

• На данный момент граждане не понимают, как работает блокчейн, из-за этого нет доверия к введению единой медицинской карты.

• Для общей базы нужна постоянно проверяемая защита, которая выстоит перед хакерскими атаками, иначе личные данные будут взломаны злоумышленниками и «утекут» в сеть.

• Стоит вопрос и о необходимости ресурсных затрат на обучение медперсонала для работы с электронными платформами, а также оснащение необходимым электронным оборудованием.

Технология блокчейн и «интернет-вещей»



Зачем объединять блокчейн и «интернет-вещей»?

1. Решение проблемы надзора.
2. Обеспечение секретности и прозрачности.
3. Возможность создавать соглашения.
4. Общее улучшение безопасности IoT-среды.

Примеры эффективного взаимодействия блокчейна и «интернет-вещей»

1. Компания Filament использует блокчейн и «интернет-вещей» для умного управления крупными промышленными системами. Разработанные компанией решения способны повысить эффективность в самых различных отраслях, будь то горнодобывающая промышленность или сельское хозяйство.

2. Сервис Chimera предлагает инновационную систему ухода за престарелыми и нуждающимися в опеке людьми. В ней используются физические устройства (в виде браслетов и медальонов) и приложения для удаленного сбора и анализа показателей жизнедеятельности, а также определения ситуаций, когда носитель этих устройств нуждается в помощи.

3. Российская компания Acronis недавно представила на рынок новые решения на базе блокчейна — Acronis Notary и Acronis ASign. Функция Acronis Notary предназначена для электронного подписания документов и обеспечения целостности данных. Функция Acronis ASign предназначена для цифровой подписи документов с использованием блокчейна. По мнению представителей компании, использование блокчейна исключает необходимость участия третьей стороны, удостоверяющей подлинность документов.

Спасибо за внимание!

Вопросы?