# ПРИМЕНЕНИЕ ТЕХНОЛОГИИ РЕЕСТРА БЛОКОВ ТРАНЗАКЦИЙ ДЛЯ ПОСТРОЕНИЯ РАСПРЕДЕЛЕННЫХ СИСТЕМ

Жилинская Е.Р., Кардаш И.П, Захарьев В.А.
Кафедра систем управления, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: {katyazhilinskaya, ivan.kardash11}@gmail.com, zahariev@bsuir.by

*Данная статья посвящена исследованию технологии реестра блоков транзакций для построения распределенных систем (блокчейн). В ней представлены различные типы систем, подробно рассмотрена архитектура, основные консенсусные алгоритмы, а также возможности внедрения технологии как в коммерческих, так и в некоммерческих целях.*

## Введение

Реестр блоков транзакций (блокчейн) — выстроенная по определённым правилам непрерывная последовательная цепочка блоков, содержащих информацию. Чаще всего копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга. Концепция технологии блокчейн похожа на базу данных, за исключением того, что взаимодействия с ними различаются. Блокчейн — это, по существу, распределенная база данных или публичная книга всех транзакций или цифровых событий, которые были выполнены и распределены между участвующими сторонами в одноранговых сетях.

Блокчейн имеет две основные особенности:

1.Блокчейн является общедоступной. Любой может просмотреть ее в любое время, поскольку она находится в сети, а не в одном учреждении, которому поручено поддерживать и вести запись.

2. Блокчейн также шифруется, она использует шифрование с использованием открытых и закрытых ключей, чтобы гарантировать её безопасность.

Существует семь принципов проектирования для создания программного обеспечения, услуг, бизнес-моделей, рынков и организаций на основе блокчейн: сетевая целостность, распределение нагрузки, ценность как стимул, безопасность, приватность, защищенность прав и вовлеченность.

В основном существует три типа блокчейнов: частная блокчейн, консорциум блокчейн и публичная блокчейн. Частный или консорциум блокчейн связаны с ограниченной средой, такой как компания, группа компаний или одна определенная цепочка создания стоимости, в то время как публичная блокчейн поддерживает тип блокировки без разрешения.

## I. Архитектура блокчейн

Элементы архитектуры могут варьироваться в зависимости от того, какие типы блокчейна используются. Базовыми элементами являются:

Блок. Блокчейн облегчает высокораспределенную регистрацию для записи транзакций, перенос их на определенный узел в сети и организацию их во времени.

Данные постоянно записываются в сеть через файлы, называемые блоками.

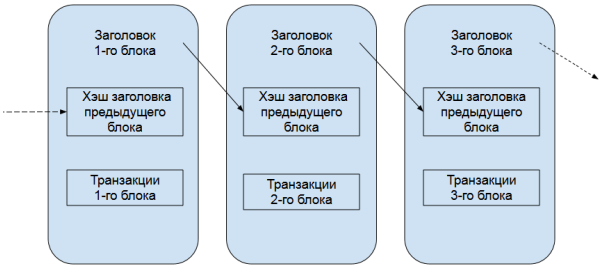


Рис. 1 – Упрощённый пример цепи блоков

Каждый блок состоит из заголовка блока и блока. Заголовок блока состоит из трех наборов метаданных блока.

Цифровая подпись. Для создания транзакции блокчейн требуется цифровая подпись для аутентификации транзакции.

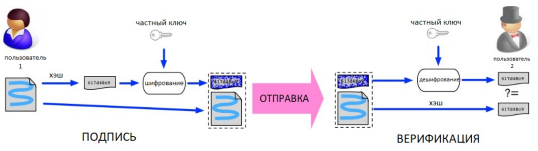


Рис. 2 – Цифровая полпись, используемая в блокчейн

Типичная цифровая подпись включает в себя две фазы: фазу подписи и фаза проверки.

Распределенная сеть. Взаимодействия между пользователем по цепочке блоков в основном используют распределённую сеть, в которой каждый пользователь представляет узел, на котором установлен клин-блок-клин.

Консенсус в сети. Проведение транзакции требует принятия и проверки всеми пользователями в сети, обычно называемой консенсусом. Но каждый узел имеет другой вид состояния всей сети.

Для решения этой проблемы необходим распределенный механизм.

Как правило, существует три основных консенсусных алгоритма, которые могут быть применены:

– Доказательство работы (PoW)

Алгоритм консенсуса является наиболее широко используемым алгоритмом в блочной цепочке. Он был введен биткойном и предполагает, что все коллеги голосуют с их «вычислительной властью», решая случаи и строя соответствующие блоки.

– Доказательство доли (PoS)

Алгоритм направлен на замену существующего способа достижения консенсуса в распределенной системе; вместо решения этот узел, который генерирует блок, должен обеспечить доказательство того, что он имеет доступ к определенному количеству монет до того, как он будет принят сетью.

– Делегированное доказательство доли (DPoS)

Основное различие между PoS и DPoS заключается в том, что PoS является прямым демократическим процессом, в то время как DPoS является представительной демократией - заинтересованные стороны избирают делегатов для создания и проверки блока.

## II. Применение технологии блокчейн

Первый блокчейн, биткойн, был разработан для совершенствования системы финансовых приложений. А в настоящее время широко развивается и для некоммерческмх услуг, таких как системы голосования для правительственных дел. В связи с этим сферы, использующие блокчейн, можно разделить на два сектора: коммерческие и некоммерческие приложения.

1. Коммерческие приложения

Цифровая платежная система. Это в основном основная функция биткойна как цифровой валюты. Рождение биткойна вызвало эволюцию и нарушение традиционных платежных систем, управляемых банками или другими финансовыми организациями. Схема цифровой валюты включает в себя как новую децентрализованную платежную систему, так и новую.

Смарт-договор. В принципе, смарт-контракт - это компьютерное приложение, которое может автоматически выполнять коммерческие транзакции и соглашения. Он также обеспечивает выполнение обязательств всех сторон в контракте без дополнительных расходов посредника.

Страхование. Любой ценный актив или имущество, которое трудно реплицировать или уничтожить, можно зарегистрировать в блокчейне. Она может проверять право собственности и отслеживать историю транзакций. Crowdfunding. В настоящее время увеличение числа стартапов реализует криптографические маркеры и протоколы блокчейн в качестве средства поиска своих предприятий. Идея заключается в том, чтобы использовать платформы обратного преобразования, основанные на технологии blockchain, устраняя необходимость в посреднической третьей стороне.

2. Некоммерческие приложения

Распределенное управление. Наиболее распространенное использование блокчейна в органах управления осуществляется в виде нотариуса. Применение блокчейна к нотариальному удостоверению обеспечивает конфиденциальность документа, а также тех, кто для кого производится сертификация. Еще одной формой службы управления, которая также была принята блокчейн, является система онлайн-голосования или электронного голосования.

Распределенное хранилище. Эта концепция была реализована в индустрии здравоохранения и музыки. Для связанных со здоровьем приложений блокчейн предоставляет структуру для хранения медицинских данных или электронных медицинских записей, чтобы их можно было анализировать, но оставаться конфиденциальными.

С другой стороны, в музыкальной индустрии блокчейн применялся для поддержки всеобъемлющей и точной распределенной базы данных прав собственности на музыку.

Распределенный интернет вещей. Использование интернет вещей также представляет некоторые большие проблемы. Один из них связан с централизованной экосистемой, известной также как парадигма клиент-сервер. Хотя эта модель десятилетиями подключала общие вычислительные устройства и будет продолжать поддерживать малые сети интернет вещей, как мы их видим сегодня, она не сможет реагировать на растущие потребности огромных экосистем интернет вещей будущего.

## III. Список литературы


1. Технология Блокчейн и децентрализованное управление: является ли государство все еще необходимо?/ Атзори, Марселла // –2015.
2. Кросби, Майкл Технология Блокчейн: Beyond bitcoin. Прикладные инновации 2. – 2016, – С. 6–10.
3. Кастро, Мигель, Лисков, Барбара. Практическая византийская отказоустойчивость. –1999. – С. 173–186.
4. Женг, Зыбин. Проблемы и возможности блочной цепи: обзор. –2016.