Введение

Блокчейн (blockchain) — распределенная (децентрализованная) база данных, которая позволяет осуществлять прямые транзакции между двумя сторонами без необходимости в доверенном посреднике. Эта технология получила широкую известность благодаря криптовалютам, но её применение выходит далеко за рамки финансовых операций. Среди областей использования блокчейна можно выделить следующие.

Криптовалюты. Это одно из самых известных применений блокчейна. Криптовалюты, такие как Bitcoin и Ethereum, используют блокчейн для записи транзакций и обеспечения безопасности сети. Блокчейн позволяет проводить децентрализованные платежи без участия посредников, таких как банки.

Смарт-контракты. Это программа, записанная в блокчейне, которая автоматически выполняет условия договора при наступлении определенных событий. Например, смарт-контракт может автоматически выплатить вознаграждение исполнителю после выполнения работы. Это устраняет необходимость в посредниках и снижает риски мошенничества.

Управление цепочками поставок. Блокчейн помогает отслеживать движение товаров от производителя до конечного потребителя. Каждый этап цепочки поставок фиксируется в блокчейне, что делает процесс прозрачным и надежным. Это особенно полезно в отраслях, где важна прослеживаемость продукции, например в пищевой промышленности или фармацевтике.

Цифровая идентификация. Блокчейн может использоваться для создания надежных цифровых идентификаторов. Такие системы позволяют пользователям контролировать личные данные и предоставлять доступ к ним только тем организациям, которым они доверяют. Это улучшает безопасность и конфиденциальность личных данных.

Голосование. Блокчейн может обеспечить честность и прозрачность выборов. Голоса избирателей фиксируются в блокчейне, что исключает возможность их изменения или удаления. Это также упрощает проверку результатов голосования и повышает доверие к процессу.

Недвижимость. В сфере недвижимости блокчейн может упростить процессы купли-продажи и аренды имущества. Все сделки могут быть зафиксированы в блокчейне, что обеспечивает достоверность информации о правах собственности.

Здравоохранение. Медицинские записи пациентов могут храниться в блокчейне, обеспечивая безопасный и удобный доступ врачам и пациентам. Это облегчает обмен данными между медицинскими учреждениями и защищает конфиденциальную информацию.

Логистика и транспортировка. Блокчейн может улучшить управление логистическими операциями, отслеживая перемещение грузов и документируя все этапы транспортировки. Это уменьшает вероятность ошибок и ускоряет обработку документов.

Финансовые услуги. Помимо криптовалют, блокчейны находят применение в традиционных финансах. Они могут ускорить проведение международных платежей, снизить затраты на обслуживание клиентов и повысить безопасность транзакций.

Авторское право и защита интеллектуальной собственности. С помощью блокчейна можно регистрировать авторские права на произведения искусства, музыку, тексты и другие виды контента. Это предотвращает плагиат и обеспечивает защиту прав авторов.

Эти примеры показывают, насколько универсальной является технология блокчейна. Она имеет потенциал для трансформации многих отраслей экономики и общества, делая процессы более эффективными, безопасными и прозрачными.

Данное пособие посвящено разработке смарт-контрактов. Смарт-контракт представляет собой набор инструкций, написанных на специальном языке программирования (например, Solidity для платформы Ethereum). Этот код определяет правила взаимодействия участников контракта. Контракт содержит определенные условия, выполнение которых запускает автоматическое исполнение действий. Эти условия могут включать в себя передачу денег, предоставление доступа к данным, выполнение задачи и другое. У каждого смарт-контракта есть уникаль-

ный адрес в блокчейне, который позволяет другим участникам взаимодействовать с контрактом.

Процесс разработки смарт-контракта состоит в следующем. Сначала разработчик пишет код смарт-контракта и публикует его на блокчейне. После публикации контракт становится доступным всем участникам сети. Пользователи могут отправлять запросы к контракту через транзакции. Например, если контракт предназначен для выплаты вознаграждения, пользователь отправляет запрос на выплату вместе с необходимыми данными. Когда контракт получает запрос, он проверяет, выполнены ли все необходимые условия. Если да, контракт автоматически исполняет заложенные в него инструкции. Например, переводит деньги на указанный счет, предоставляет доступ к данным или выполняет другую задачу. Все действия, выполненные смарт-контрактом, записываются в блокчейне. Это обеспечивает прозрачность и невозможность изменить результаты исполнения контракта.

Преимуществами смарт-контрактов являются автоматизация операций, отсутствие посредников, открытость и доступность для проверки — все действия записываются в блокчейне; безопасность — благодаря криптографической защите и неизменности данных, смарт-контракты защищены от несанкционированного вмешательства.

Недостатками смарт-контрактов являются риски, связанные с возможными ошибками в программном коде, так как исправление кода невозможно после публикации контракта, высокая стоимость разработки, а также зависимость от инфраструктуры — работа смарт-контрактов зависит от надежности и производительности блокчейна, на котором они размещены.

Тем не менее использование смарт-контрактов продолжает расширяться, открывая новые возможности для бизнеса и общества.

Разработка и тестирование смарт-контрактов и приложений, использующих блокчейн, происходит в тестовых блокчейн-сетях. Под «тестовыми» будем понимать среды для разработки и отладки, которые не предполагается использовать в реальных условиях. Они могут быть развернуты как локально на компьютере разработчика, так и на сервере. Если среда развернута на локальном компьютере, тогда понятия тестовой и локальной среды совпадают.

Одним из самых известных и распространенных примеров применения технологии блокчейн является блокчейн-сеть Ethereum, для которой разработаны локальные и тестовые среды.

Ganache (или аналог Hardhat) — это локальная блокчейн-среда, которую используют разработчики для создания локальной сети Ethereum.

Sepolia — это публичная тестовая сеть Ethereum для целей разработки и тестирования. Это реальная тестовая сеть, к которой может подключиться любой разработчик, и она позволяет тестировать смарт-контракты в условиях, максимально приближенных к основной сети (Mainnet).

Таким образом, сети Ganache или Hardhat разработчик разворачивает самостоятельно, и только он имеет к ним доступ, а Sepolia — это публичная сеть, к которой каждый имеет доступ, она уже развернута, постоянно работает и поддерживается сообществом.

Учебное пособие посвящено практическому освоению блокчейн-разработки на платформе Ethereum с использованием тестовых сетей Sepolia, Ganache и Hardhat.

В главах 1-10 изложен процесс создания смарт-контрактов на языке Solidity. Описаны методы взаимодействия со смарт-контрактами с использованием библиотек Web3.py (для Python) и Web3.js (для JavaScript), а также создание приложений для локальных и тестовых сетей. Приведены примеры создания смарт-контрактов, таких как опционные контракты.

В главах 11 и 12 рассмотрена работа с децентрализованным хранилищем Swarm и с BigchainDB — распределённой базой данных с технологией блокчейн.

В главах 13 и 14 рассмотрена реализация блокчейна на Python, а также взаимодействие с блокчейном, разработанное на Flask.

Исходный код всех примеров, а также образы виртуальных машин находятся в открытом доступе.

В приложении А приведены задания для самостоятельной разработки смарт-контрактов с решениями, которые читатели могут развивать в рамках своих проектов.

Авторы выражают благодарность: Трошину Павлу Игоревичу, ведущему программисту журнала «Известия вузов. Математика», а также студентам групп Университетского колледжа БРИКС: ОИСП-291, ОИСП-292, ДИСП-391, ДИСП-291, ОИСП-411, ОИСП-391, ОИСП-211, ДИСП-211.