

ТЕХНОЛОГИЯ «БЛОКЧЕЙН» И ЕЕ ПРИМЕНЕНИЕ В РАЗЛИЧНЫХ СФЕРАХ ДЕЯТЕЛЬНОСТИ

Прокопенко.Д.М., студент, гр. ПИБ-182, IV курс
Научный руководитель: Смыков.А.Б., доцент
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

Блокчейн — это архитектура хранения информации таким образом, что обеспечивает неизменность исторических данных. По определению это децентрализованный и распределенный реестр в сетевой инфраструктуре.

Регистром блоков может быть распределена база данных или односторонний журнал событий. В таком реестре новые блоки могут быть добавлены только к концу структуры блоков.

Подходя к теме с практической стороны, а не теоретического определения, можно сказать, что блокчейн – это цифровая книга, действующая как реестр транзакций. Чаще реестр касается данных в форме финансовых операций. Простейшие примеры – операции, касающиеся криптовалют, акций.

Характерные особенности блокчейна.

Суть основана на том, что каждый последующий блок сохраняет необратимый хэш, хранящий информацию из предыдущего блока. Другими словами, хеш работает как итог предыдущего блока.

Одной из характерных частей информации наряду с хэшем является метка времени, то есть информация о том, когда был создан конкретный блок. Как результат, хэш и метка времени гарантируют, что блоки тесно связаны между собой и что невозможно незаметно вмешиваться в блокчейн.

Обратите внимание на то, что каждый блок сохраняет определенный объем данных (например, в форме определенного количества финансовых операций). Когда один блок заполнен, создается следующий.

Отличительной особенностью является децентрализация. Для правильной работы системы не требуется центральная база данных, один основной сервер, компьютер или любой другой элемент технической инфраструктуры. Сохраненные данные хранятся только в последовательных блоках. Это означает, что транзакции распределяются на уровне одноранговой сети. Это очень важно, поскольку на практике это означает, что операции не контролируются главным брокером (хотя они прозрачны).

Это делает блокчейн очень хорошим информационным носителем, поскольку это общий и полностью прозрачный доступ к не редактированным данным. Данные прозрачны и надежны для всех пользователей, что способствует доверию, безопасности и развитию. Более конкретно, блокчейн обеспечивает конфиденциальность, но этого не следует путать с анонимностью. Адреса общедоступны, а это означает, что хотя никакие личные данные не

известны, что-то вроде «номер счета в блокчейне» общедоступно, и каждый может просмотреть историю транзакций.

Безопасность

Говоря о сети блокчейнов, невозможно игнорировать тему безопасности. Защита реестра транзакций в блокчейной технологии использует усовершенствованные криптографические алгоритмы для защиты от редактирования данных и несанкционированного доступа. Теоретически можно сломать криптографию, но на практике требуется компьютер с огромными вычислительными возможностями. Было подсчитано, что для таких целей потребуется компьютер мощностью - половины всех пользователей Интернета. Что бы ни означало это вычисление, вывод один – нужна огромная вычислительная мощность, и реальной угрозы проникновения в сеть блокчейнов нет. Тем не менее, ходят слухи, что проблем безопасности может вернуться после того, как квантовые компьютеры станут доступны. Однако это не то, что сейчас беспокоит специалистов по безопасности.

С точки зрения безопасности, характеристики технологии блокчейна делают это решение, которое способствует повышению безопасности данных. Практика показывает, что подделывать сделки гораздо сложнее. Во-первых, невозможно изменить транзакцию (как только транзакция будет размещена, она останется такой), а во-вторых, история транзакций прозрачна для всех. Это делает технологию блокчейна безопасным и надежным методом хранения информации.

Характерные преимущества технологии блокчейн

Доверие и безопасность – пользователи могут быть уверены, что получают данные без ошибок. Редактировать данные невозможно. Нет администратора, который может удалять или изменить данные. Конфиденциальная информация не является публичной. Следует отметить, что каждый дополнительный блок придает достоверность предыдущему блоку. Таким образом, любая попытка манипулировать данными просматривается, и невозможно вмешиваться в данные третьими сторонами.

Повышенная эффективность – нет проблемы трудоемкого согласования записей (благодаря тому, что сеть и данные хранятся в одной целостной экосистеме, работающей на основе одноранговой сети).

Полнота информации – чаще всего реестр транзакций отвечает на следующие вопросы: что было куплено/продано, когда, сколько и где (конечно, что именно содержит реестр транзакций, зависит от особенностей данного реестра). Умные контракты – набор правил может храниться в блокчейне (в форме смарт-контракта, который называется смарт-контрактом). В рамках такого набора правил могут быть определены разные типы условий в зависимости от потребностей, например, условия продажи/покупки конкретного актива.

ИСТОРИЯ ТЕХНОЛОГИИ БЛОКЧЕЙНА

Блокчейн – это вопрос, который сегодня очень горячий и считается технологией будущего. Однако следует отметить, что история блокчейна длиннее, чем может показаться. Этот тип технологии впервые упоминается в 1991 году.

В этом случае система использовала криптографически защищенные строчки блоков для хранения отмеченных временем цифровых документов.

Следующими датами на пути развития технологии блокчейн являются 2000 год (концепция распределенной книги, обеспечивающая доступ к финансовым данным), 2004 (разработка системы, позволяющей обмениваться токенами между пользователями), 2005-2006 (концепция виртуальной валюты под названием B Gold и b- деньги).

Все эти даты предшествовали моменту прорыва – 9 ноября 2008 года. В это время криптовалюта с использованием технологии блокчейн была обнаружена. Этой криптовалютой, конечно, был биткойн. В настоящее время существует гораздо больше подобных проектов. Кроме биткойнов, особенной популярностью пользуется Ethereum, базирующийся на так называемом блокчейне 2.0. Прорыв Ethereum состоит в том, что вы можете запускать код (называемый смарт-контрактом) последовательными блоками.

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Как правило, блокчейн ассоциируется или даже отождествляется с криптовалютами, но следует знать, что сфера использования этой технологии намного шире и криптовалюты – это лишь вершина айсберга. В дополнение к широко понятной технологической и финансовой отрасли эту технологию можно найти в государственном управлении или в энергетическом секторе.

Примеры использования блокчейна вне криптовалют приведены ниже.

Авторизация, используемая среди прочего в государственном управлении (цифровые подписи, полномочия, распределенные системы идентификации лиц). Примерами являются: OneName, WorldTable, Uniquld. Примером может служить правительство Эстонии, которое использует блокчейн в таких услугах, как утверждение законов и заботу о многих других административных задачах (используя платформу X-Road).

Система голосования, характеризующаяся прозрачностью поданных голосов без раскрытия персональных данных. Примером является FollowMyVote.

Ведение бухгалтерских книг, используемое широко известной финансовой отраслью.

Управление данными, связанными с государственными услугами, такими как земельные реестры, ипотечные кредиты, налоги, акты (надежные без нотариуса и других учреждений). Примеры ShoCard или BitNation.

Управление данными, касающимися распределения и производства электроэнергии. Торговля электроэнергией (торговля, работающая на линии

потребителя-потребителя), выставление счетов за транспорт энергии, управление данными по счетчикам, выдача сертификатов. Примерами являются Бруклинская микросеть или SolarChange.

Заключение коммерческих сделок на разных рынках, например, фондовый рынок или любые другие активы (без посредников). Примерами валютно-обменных или межбанковских сделок являются Ripple или Coinbase.

Судебный реестр или любой другой реестр государственного управления. Подобный реестр, основанный на технологии блокчейна, может функционировать в корпорациях и различных типах учреждений. Примеры сбора информации включают информацию: о личных данных (PESEL, NIP, имя или любой другой идентификатор), о полученных сертификатах, о принятых обязательствах, о местонахождении, о наличии водительских прав, о медицинской документации и т.д.).

Защита авторских прав в области защиты от получения патента посторонними лицами.

Аренда любых активов без посредников. Примером является аренда автомобилей и токенизация парковочных мест, предложенная Startup Arcade City.

Создать децентрализованные корпорации, не имеющие центральных подразделений управления. Такое видение означает равную организационную структуру, отсутствие посредников и множество возможностей автоматизации задач. На практике децентрализованные компании могут быть использованы при необходимости надзора за ценными бумагами или надзора за уплатой платежей.

Компьютерные и азартные игры. Анонимизация игроков, создание внутриигровой валюты, транзакции между игроками.

Применение таковой технологии, не считая упорядочения административных и складских действий, позволяет сделать бренд надежным в очах клиентов. Потенциальные получатели могут быть уверены, что весь производственный процесс происходил в определенной стране или, например, предлагаемая продукция не тестировалась на животных. Другие примеры этого типа приложений – Everledger и Chainlink.

Системы хранения данных, обеспечивающие повышенную защиту в случае взлома или попытки повлиять на корректность данных. Примерами являются PeerNova или NXT.

БЛОКЧЕЙН И КРИПТОВАЛЮТЫ

Применение очень широкое, но нельзя отрицать, что именно криптовалюты заставили блокчейн выйти из тени, и сегодня этот вопрос интересует людей, мало связанных с криптографией. Большая группа людей даже отождествляет технологии блокчейна с криптовалютами.

Однако следует иметь в виду, что биткоин, криптовалюты и блокчейн – это разные понятия. Биткоин – это криптовалюта, в которой транзакции совершаются децентрализованно и хранятся в одноранговой системе (между пользователями) с помощью блокчейна.

Транзакции блокчейна необратимы, поскольку все транзакции записываются в блокчейн, без возможности изменения информации о транзакциях (необратимость книги транзакций).

Транзакция BTC (как упрощенное объяснение того, как работает технология блокчейна)

Шаг 1) Пользователь собирается перевести криптовалюту с одного адреса на другой.

Шаг 2) Транзакция инициируется, например, с помощью специальной программы (горячий кошелек) или на устройстве, служащем горячим кошельком.

Шаг 3) Транзакция отображается в блокчейне, например, как другой блок, содержащий всю необходимую информацию, в частности адреса получателя, отправителя и сумму переданной криптовалюты. Блок также содержит хэш, который действует как электронная подпись, и указывает, какой блок был предыдущим. Это имеет большое значение для безопасности всей операции и предотвращения возможных манипуляций.

Шаг 4) Если все записи совпадают, криптовалюта успешно передается с одного адреса на другой.

Следует отметить, что такая транзакция просматривается для других пользователей сети (без раскрытия персональных данных).

Майнинг криптовалют – идея, основанная на характеристиках производительности технологии блокчейн.

Добыча криптовалют – это очень увлекательный вопрос. Для многих людей это звучит неясно. Однако, когда мы узнаем основную информацию о том, как работает технология блокчейна, сам майнинг криптовалют становится очень ярким. Когда пользователь совершает транзакцию с использованием криптовалюты, другие компьютеры (другие пользователи) проверяют транзакцию и таким образом позволяют транзакцию. Значительно упростив его, можно сказать, что для этого требуется вычислительная мощность (для проверки произведенных транзакций выполняются усовершенствованные математические операции). Пользователи, которые предоставляют чуть больше вычислительной мощности в качестве вознаграждения, получают часть криптовалюты, которая широко известна как майнинг криптовалюты.

БУДУЩИЕ БИТКОИНА И ДРУГИХ КРИПТОВАЛЮТ

Возникает вопрос, можно ли еще использовать криптовалюту после того, как выкопан последний BTC? Во-первых, до этого еще далеко, поскольку последние биткойны не будут добываться до 2140 года. Однако, по подсчетам, тогда майнеры криптовалюты все еще потребуются для поддержания ликвидности сети. Однако им придется смириться с тем, что они не получают вознаграждение за добычу новых блоков.

Приведет ли это к проблеме с ликвидностью?

На первый взгляд, кажется, что это может быть так, однако, по многим научным теориям, будущее BTC может быть совершенно противоположным. К 2140 году сеть людей, использующих криптовалюты, может быть столь велика, что BTC и другие валюты, хотя дальнейшее извлечение дальнейших блоков невозможно, могут служить очень ликвидным платежным средством. В любом случае это некоторые прогнозы и обсуждения.

Между тем, никто не может предсказать будущее BTC и других криптовалют. Что будет происходить с биткойнами через 100 лет, это то, что, однако, может не всех заинтересовать.

Взгляд на ближайшее будущее криптовалют – это то, что нельзя игнорировать. Криптовалюты приравниваются к альтернативе текущей денежной системе. Интерес к криптовалютам постоянно растет.

Кроме отдельных инвесторов, рассматривающих их как способ хранить стоимость денег со временем, есть фонды, коммерческие учреждения и государственные организации. Интерес к криптовалютам не скрывают крупнейшие корпорации, такие как PayPal, Microsoft или банковские учреждения (Citibank).

Список литературы:

1. Сайт «Wikipedia» [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/>, свободный (дата обращения: 13.04.2022).
2. Сайт Habr [Электронный ресурс]. – Режим доступа: <https://habr.com/>, свободный (дата обращения: 13.04.2022).
3. Сайт It.ua [Электронный ресурс]. – Режим доступа: <https://www.it.ua/>, свободный (дата обращения: 13.04.2022).
4. Сайт Forbes [Электронный ресурс]. – Режим доступа: <https://forbes.ru/>, свободный (дата обращения: 13.04.2022).