­Колледж Автономной некоммерческой образовательной организации высшего образования

"Научно-технологический университет "Сириус"

**Доклад по введению в специальность**

***«Блокчейн. Применение и устройство»***

Работу подготовил:

студент 1 курса группы 1.9.7.3

Терешин Артём

Проверил:

преподаватель введения в специальность

Тенигин А.А.

г.Сочи, 2022

Введение

В настоящее время, блокчейн технологии являются крайне нишевыми и непопулярными. Огромное количество проектов находятся в зачаточной стадии и пока не находят большой популярности среди конечного пользователя. Тем не менее, блокчейн все активнее проникает в различные сферы жизни. Целые страны, вроде Сальвадора или Белорусии признают криптовалюты официальным платежным средством. Крупные компании используют HFT для подтверждения подлинности товаров или упрощения логистики.

На мой взгляд, развитие блокчейн технологий – логичный шаг для перехода в эру web 3 и разработчику необходимо понимать принцип работы данного типа сетей.

Устройство блокчейн сетей

По сути своей, блокчейн – это база данных, которая хранится одновременно на множестве устройств, подключенных к одной сети, и обновляется по мере проведения транзакций. Каждый элемент блокчейн реестра занимает определенную позицию и не может быть изменен или удален, так как все блоки связаны между собой с помощью хэша.

Кроме того, у каждого блокчейна (за исключением сети Bitcoin) есть некоторый набор правил, которые нельзя нарушить. Эти правила зафиксированы в смарт-контрактах и исполняются автоматически при соблюдении условий договора.

Каждое действие в сети должно быть подтверждено с помощью алгоритма консенсуса. Именно он обеспечивает практически нерушимую безопасность блокчейнов.

У современных блокчейн сетей огромное количество сотавляющих, но не одна сеть не сможет существовать без:

* Сети узлов (нод)
* Алгоритма консенсуса
* Адресов пользователей
* Блоков транзакций

Кроме того, важными элементами сетей являются:

* Смарт-контракты
* NFT
* Децентрализованные приложения

Узлы сети (Ноды)

Основным принципом блокчейна является децентрализация. Обеспечивают ее простые пользователи, которые установили на свой компьютер или сервер специальный клиент, называемый нодой.

Нода сети блокчейн – точка, которая, в зависимости от своего типа, может проверять, принимать или отклонять транзакции, шифровать и сохранять информацию в блоке, связываться с другими нодами.

Существует 5 основных типов нод:

* Полные ноды
* Легкие ноды
* Суперноды
* Сверхбыстрые ноды
* Ноды майнинга

**Полные ноды** хранят в себе полную и подробную историю транзакций в блокчейн сети, начиная с самой первой. Это большой объем информации (Например история всех транзакций Bitcoin составляет около 250 Гб), работа с которым требует значительных вычислительных мощностей. Кроме того, чтобы стать полной нодой необходимо иметь подключение к интернету 24/7.

Именно этот тип нод занимается подтверждением транзакций. Поскольку блокчейн не хранит балансы кошельков, во время перевода, ноды должны просканировать всю историю транзакций, узнать сколько токенов поступало на указанный адрес и сколько было с него выведено и утвердить итоговый баланс кошелька. Если сумма токенов на счету пользователя меньше, чем сумма, которую он хочет перевести, транзакция будет отменена.

В некоторых блокчейн сетях, держатели полных нод получают за это вознаграждение.

**Легкие ноды** намного менее требовательны к вычислительным мощностям держателя. Они хранят не всю историю блокчейна, вместе с огромным количеством технической информации внутри блока, а только заголовки блоков.

Заголовок блока весит 80 байт и содержит в себе номер версии блокчейн сети, хеш заголовка предыдущего блока, общий хеш всей сети (корень Меркла), метку времени транзакции и несколько сугубо технических полей.

Легкие ноды могут быть запущены даже на мобильных устройствах, так как они не требуют постоянного доступа в интернет, весят не больше 100 Мб и для работы с ними хватит мобильного процессора. По сути своей, мобильные клиенты кошельков (Вроде Trust wallet или MetaMask) являются легкими нодами, которые подключаются к полным нодам для проведения транзакций.

**Суперноды** – мозг блокчейна. Он связывает между собой полные ноды и позволяет им всем иметь актуальную версию реестра сети. Именно эти узлы следят за соблюдением правил блокчейна, проводят голосования об изменениях этих самых правил и выполняют протокольные мероприятия.

Суперноды всегда активны и потребляют намного больше энергии, нежили полные ноды. Запуск главных узлов требует больших вложений в покупку техники и обеспечении ее корректной работы, а также в финансовое обеспечение криптовалютой.

В связи с большой трудностью содержания супернод и их важности для сети, их держатели регулярно получают вознаграждение.

**Сверхбыстрые ноды** характерны для сетей второго уровня (своего рода надстроек над глобальными сетями, вроде polygon или bitcoin lightning). Они позволяют производить транзакции заметно быстрее и иногда дешевле чем в сети первого уровня. Служат эти ноды непосредственно для проведения транзакций между такими-же элементами сети второго уровня.

**Ноды майнинга** напрямую учувствуют в алгоритме консенсуса и занимаются добавлением новых блоков в сеть. За добавление одного блока майнер получает вознаграждение (В сети биткойн это 6,25 BTC). В связи с такой большой наградой, между майнерами огромная конкуренция. Крупные корпорации устанавливают множество мощный нод майнинга и из-за этого простому пользователю практически невозможно создать собственный блок и получить вознаграждение.

Алгоритм консенсуса

Для контроля за соблюдением правил блокчейна, подтверждения или отклонения транзакций существуют алгоритмы консенсуса. Именно они защищают блокчейн-экономику от двойных трат, т.е ситуаций, при которой одни средства были потрачены дважды. От его выбора зависит скорость транзакций, децентрализация сети, вознаграждение для держателейнод и, на удивление, влияние сети на экологическую ситуацию в мире. Алгоритмов консенсуса очень много. Большинство из них крайне специфичны и используются лишь одним блокчейном, например Proof-of-Authority, Proof-of-Importance, Proof-of-Space. Но существует два наиболее распространенных алгоритма подтверждения транзакций, за счет которых существует множество популярных и удобных сетей. Это Proof-of-work и Proof-of-stake.

Proof-of-work

Proof-of-work или алгоритм доказательства работы – древнейший из существующих алгоритмов консенсуса. Именно его использование привело к появлению такой профессии как крипто-майнер.

Для подтверждения транзакций в Proof-of-work сетях держатели нод майнинга, или майнеры, должны решать сложную и, на самом деле, довольно бесполезную задачу по нахождению хеша с нулями в начале. Нода, которая первой нашла данное значение получает вознаграждение. Важно заметить, что сложность задачи изменяется, в зависимости от нагрузки на сеть. Следовательно, при низкой загрузке сети, майнеры должны найти хеш с, например, 5 нулями в начале, а при высокой загрузке с 12 нулями. Вторая задача намного сложнее.

Но в настоящее время многие блокчейн сети отказываются от Proof-of-work в связи с большим количеством недостатков. Во-первых, такие сети крайне энергозатратны. Поскольку между майнерами ведется жесткая конкуренция, крупные держатели нод устанавливают более мощное оборудование, позволяющее перебирать больше хешей и, следовательно, чаще получать награду от сети. Более мощное оборудование потребляет больше электроэнергии. Уже сейчас сеть Bitcoin потребляет больше электричества чем Греция или Швейцария. Экоактивисты недовольны таким положением дел и всячески агитируют переходить на Proof-of-stake.

Кроме того, сети с Proof-of-work подвержены централизации, так как, в погоне за добычей, майнеры объединяются в майнинг-пулы, что подвергает угрозе основной принцип блокчейна – децентрализацию.

Proof-of-stake

Данный алгоритм консенсуса был представлен в 2011 году, как альтернатива Proof-of-work. Он предназначен для решения его проблем с масштабированием и скоростью.

Вместо майнеров, в proof-of-stake существуют валидаторы. Они разворачивают собственную ноду и замораживают на ее балансе некоторую сумму криптовалюты, эта сумма называется стейк. Чем больше монет заморожено в узле сети, тем больше вероятность того, что он создаст следующий блок. В базовой конфигурации proof-of-stake, нода владеющая 1% монет создает 1% всех блоков сети.

Proof-of-stake можно сравнить с банковским вкладом, так как за каждый созданный блок полагается вознаграждение. Единственная проблема заключается в том, что чтобы стать валидатором необходимо обладать относительно большим количеством цифровой валюты, например в сети Ethereum 2.0 это минимум 36 ETH. Для решения этой проблемы криптоэнтузиасты вкладывают свои активы в уже существующие ноды-валидаторы и получают вознаграждение пропорциональное их вкладу.

Блокчейны с алгоритмом консенсуса proof-of-stake значительно быстрее конкурентов. Так сеть Tron проводит 2000 операций в секунду, тогда как bitcoin всего 7. В PoS сетях намного меньше комиссии и, что крайне важно для мирового экокомьюнити, потребляют заметно меньше электроэнергии.

Адреса

Для проведения транзакций необходима система адресации. Важным принципом блокчейн сетей является анонимность и при создании адреса нужно сохранить в секрете информацию о владельце кошелька. Для этого используются алгоритмы ассиметричной криптографии, т.е способы шифрования с открытым и закрытым ключом.

Первоначально для создания адреса генерируется 256-битный закрытый ключ, а затем, с помощью математического алгоритма, создается публичный ключ идентичной длины. Далее открытый ключ сжимается до 160 бит двумя алгоритмами хеширования (в сети bitcoin это SHA-256 и MD5). После этого к преобразованному открытому ключу добавляется контрольная сумма. Именно ее наличие защищает пользователей от переводов средств на несуществующие адреса.

* В блокчейн сети транзакции не могут быть отменены и, в случае ошибки при указании адреса, средства будут отправлены на кошелек, от которого ни у кого из пользователей нет отмычки в виде закрытого ключа.

Блоки

Элементарной единицей блокчейн сети является блок. Само название блокчейна переводится с английского, как цепочка блоков. Конечно, существуют отдельные транзакции, но сеть обрабатывает их только в совокупности с другими операциями, то есть в блоке. Рассмотрим его структуру:

Каждый блок состоит из двух частей – тело (payload) и заголовок (header).

В payload содержится информация о всех транзакциях включённых в блок. Их количество варьируется в зависимости от сети, но объем информации, занимаемой блоком, всегда фиксирован.

Header служит для ускоренной навигации по истории транзакций и для поддержания стабильности сети. В минимальной комплектации заголовок блока содержит номер версии блокчейна, хеш заголовка предыдущего блока, общий хеш всей сети (корень Меркла), метку времени транзакции и несколько сугубо технических полей, предназначенных для майнеров.