ТРАНЗАКЦИИ БЛОКЧЕЙН СИСТЕМ: СОДЕРЖАНИЕ И ЖИЗНЕННЫЙ ЦИКЛ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кордаш В. Г., Бирич С.С.

Скобцов В.Ю. – к.т.н.,доцент

Работа посвящена вопросам исследования транзакций распределенных систем с целью осознания необходимости всех процессов, поддерживающих состояние и подлинность распределенных систем.

Распределенная система — это совокупность независимых устройств, связанных между собой определенным программным комплексом, позволяющим пользователю рассматривать их как единую систему [1]. Блокчейн – один из способов организации такой системы, декларирующий механизм сохранения и обмена информацией. Существуют два типа подобных систем: открытые и закрытые.

Каждая блокчейн система согласует действия своих компонентов и узлов используя определенные протоколы. В зависимости от концептуальных особенностей узлы могут образовывать иерархические зависимости, или быть равными. Несмотря на то, что изначально открытые блокчейны использовали только равные типы узлов, на данный момент данная опция доступна каждой категории.

Иерархическая структура необходима для распределения нагрузки, а также для разделения функций и полномочий узлов, что может в определенных условиях положительно сказаться на характеристиках системы, таких как надежность, отказоустойчивость и скорость обработки вносимой информации.

Простейшим завершенным элементом данных является транзакция. Традиционной схемой ассамблирования транзакций является блок. Однако в нем могут содержаться совершенно независисые транзакции. Следовательно операции с блоками не являются атомарными. Транзакция может содержать множество полей. Необходимым содержанием является адрес. В зависимости от свойств и назначения системы данный адрес может ссылаться на самые различные понятия: кошелек, контракт, чейнкод, текст и другие. Помимо адреса правильная транзакция содержит ещё какую-либо полезную нагрузку. Данная полезная нагрузка и определяет набор дальнейших действий. Но без привязки к какому-либо адресу она не имеет смысла, ровно как и адрес в отрыве от контекста невозможно использовать. Таким образом, блокчейн следует рассматривать как набор структурированных транзакций.

Для того, чтобы понять роль транзакций будут продемонстрированы жизненные циклы

транзакции открытой системы и закрытой (Hyperledger). Однако следует помнить, что в зависимости от реализации внутренних механизмов жизненные циклы других подобных систем будут отличаться, а также чем более проста система, тем больше пунктов данного процесса в ней может быть вырожденно до простейших операций.

Ниже видны несколько жизненных циклов транзакций публичного Блокчейна. Общая последовательность шагов:

а) Кто-то запрашивает транзакцию с помощью кошелька.

б) Транзакция отправляется (широковещательно) всем участвующим компьютерам в определенной сети цепочки блоков.

в) Каждый компьютер в сети проверяет (валидирует) транзакцию на соответствие некоторым правилам валидации, которые установлены создателями определенной сети цепочки блоков.

г) Проверенные транзакции хранятся в блоке и блокируются (хэшем).

д) Этот блок становится частью цепочки блоков, когда другие компьютеры в сети проверяют правильность хэша блока.

е) Теперь транзакция является частью блокчейна и никак не может быть изменена [2].

Далее находится процесс сохранения транзакции в сети Hyperledger:

а) Пользователь инициирует предложение транзакции, а также подписывает ее.

б) Подтверждающие пиры, верифицируют подпись и исполняют транзакцию. В зависимости от результатов исполнения они формируют ответы на предложения и изменения в состояние.

в) Ответы на предложения подлежат проверке там проверяется их идентичность.

г) Пользователь собирает транзакцию из подтверждений.и отправляет управляющему порядком транзакций узлу.

д) Транзакция проходит валидацию и фиксируется.

е) Обновляется содержание журнала и состояние. Журнал хранит запись о транзакции вне зависимости, была она одобрена или нет [3].

Рассмотрев подробно жизненные циклы открытой и закрытой системы, можно увидеть значительную диверсификацию узлов в закрытой сети. Каждый узел отвечает за свой узкий объем работы по поддержанию гомеостаза системы. Это позволяет упростить вычисления и увеличить поток транзакций, так как они в процессе занесения в журнал будут проходить параллельные этапы. Также такая многоуровневость позволяет уменьшить риск возникновения ошибок, как случайных, так и привнесенных намеренно. На каждом этапе происходит проверка подлинности предыдущего и на состояние системы влияет только верная транзакция. Также важным моментом является тот факт, что каждая из попыток обновления системы посредством внесения транзакций фиксируется, что позволяет производить неподделываемую аналитику, так как все изменения зафиксированы без возможности удаления.

Жизненный цикл публичного блокчейна не обладает столькими механизмами защиты, в них нет необходимости. Так как масштабы узлов велики, данная система не смогла бы поддерживать столь большой набор сообщений, необходимый для учета транзакции.

Список использованных источников:

1. Э. Таненбаум, М. Ван Стеен. Распределенные системы. Принципы и парадигмы // СПб.: Питер, 2003. 877 с.

2. Pulling the Blockchain apart.. The transaction life-cycle [Электронный ресурс]. — Режим доступа : https://medium.com/ignation/pulling-the-blockchain-apart-the-transaction-life-cycle-7a1465d75fa3 Дата доступа : 01.03.2020.

3. Hyperledger: transaction flow [Электронный ресурс]. — Режим доступа : https://www.ibm.com/blockchain/hyperledger — Дата доступа : 01.03.2020.