УДК 004.75

Адамович В.А.
студент, бакалавр
кафедра информационных и робототехнических систем
научный руководитель: Федоров В.И.
ассистент
кафедра информационных и робототехнических систем
НИУ «БелГУ»
Россия, г. Белгород

BLOCKCHAIN – КАК ТЕХНОЛОГИЯ БУДУЩЕГО

Аннотация:

В статье описана технология блокчейн, и некоторые варианты ее использования.

Ключевые слова:

Blockchain, криптовалюта.

Adamovich W.A.
Student faculty Information and robotic systems
National University of BelSU
Russian Federation, Belgorod
Fedorov V.I.
Assistant faculty Information and robotic systems
National University of BelSU
Russian Federation, Belgorod

BLOCKCHAIN – HOW TECHOLOGY OF FUTURE

Abstract:

In article described technology blockchain and some use case.

Keywords:

Blockchain, digital currency.

В последний год слова блокчейн и биткоин, стала общенародной темой для обсуждения не только специалистов в области IT, но и среди людей из других профессий. Давайте разберемся, в основных принципах работы технологии, рассмотрим её применение и предположим вероятные пути развития блокчейна.

Высокая стоимость валюты на рынке «Forex» и сложность технологии дает почву для рассуждений подогревает определенный интерес. Чтобы разобрать в устройстве этой технологии, вспомним историю появления первой цифровой валюты, основанной на технологии P2P (Peer-to-Peer, «связь человек-человек») [1].

Есть два определения блокчейна:

- Реплицированная распределенная база данных;
- Непрерывная последовательная цепочка блоков, содержащих информацию[2].

Чтобы понять, что все-таки представляет собой блокчейн, рассмотрим наиболее популярные и современные архитектуры компьютерных систем.

Всего существует два типа архитектур:

- Клиент-серверная сеть;
- Одноранговая (пиринговая) сеть.

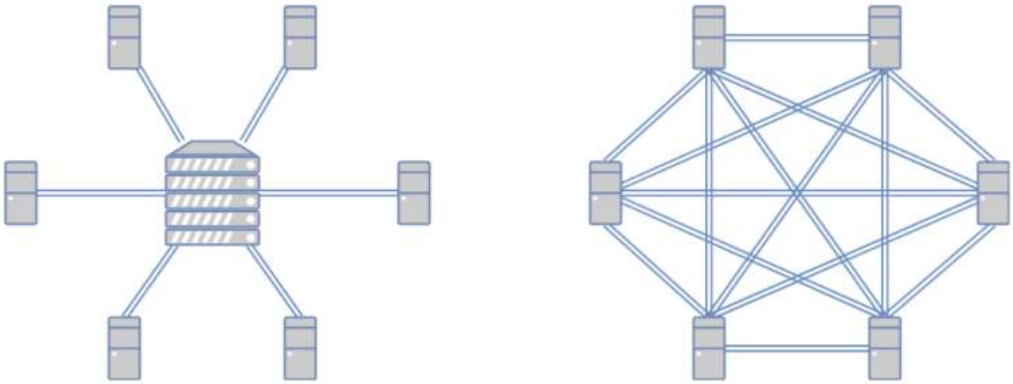

Рис. 1 Типы архитектур компьютерных систем. 1 – Клиент-серверная архитектура. 2 – Одноранговая архитектура

Клиент-серверная архитектура в первую очередь представляет собой централизованное управление всем: приложениями, данными и доступом. Сервер содержит всю системную логику и скрывает внутреннюю информацию от клиентов, что позволяет клиентам использовать гораздо менее производительные устройства, что в свою очередь снижает стоимость, а также повышает скорость обработки данных. И такой подход реализован практически везде, начиная от сайтов, заканчивая корпоративными сетями.

Со вторым типом архитектур все стоит иначе. Там нет определенного главного устройства, что означает равные права у всех участников сети. И каждый такой участник, не только потребляет, но и сам становится поставщиком сервиса.

Еще в далеком 1979 году, в университете Дьюка была изобретена технология распределенного обмена сообщения – USENET, - кстати, эта технология до сих пор используется. Он является частью интернета, осуществляет доступ по протоколу NNTP. После этого появилась технология совместного доступа P2P (Peer-to-Peer). На ее основе были созданы: популярный Napser – файлообменная пиринговая сеть созданная еще в 1999 году, BOINC – платформа для организации распределенных вычислений, а также протокол BitTorrent, который является основополагающим для всех современных торрент-клиентов.

Системы на основе децентрализованных сетей продолжают существовать, но заметно проигрывают клиент-серверным в распространенности и соответствии потребностям потребителей.

Большая часть современных приложений и систем требует возможность оперирования набором данных. Для организации такой работы, есть множество возможных вариантов реализации, один из таких вариантов использует метод одноранговых сетей. Распределенные, или параллельные, базы данных отличаются от реляционных тем, что информация в частичном или полном составе хранится на каждом устройстве сети.

Как одно из преимуществ данной системы можно выделить доступность данных. А именно, нет единой точки отказа, как в случае с базой данных, расположенной на одном сервере. Минусы такой системы является скорость обновления данных и их распространении по сети. Такие системы не рассчитаны на миллионы запросов от пользователей, которые выполняют централизованные системы.

В основе блокчейна лежит распределенная база данных блоков, которая представляет собой связный список (каждый блок содержит частичную информацию о предыдущем и следующем). Что означает, при получении информации из одного блока она будет бесполезна без других. Также каждый участник сети хранит у себя копию всех операций, проведенных за все время. Такая возможность организации сети была бы невозможна без определенных нововведений, обеспечивающих работоспособность и безопасность сети. И это приводит нас к последней основе блокчейна – криптографии.

С развитием технологий появилась необходимость в анонимности и безопасности в сети, осуществлялось это при помощи разработки новы криптографических методов. Появилось новое общество, называемое шифропанками. Они полагали, чтобы сохранить анонимность в сети необходимо было шифровать данные. Первые их попытки создать новую цифровую валюту были в начале 2000-х.

Первые версии таких валют обладали большим недостатком — несовершенством системы принятия решения среди удаленных абонентов. Это были: созданная Вэй Дайем - b-money, и созданная Ником Сабо – BitGold.

Bitcoin – первая полноценная криптовалюта, появившаяся в 2008 году. Ее автором является Сатоши Накамото, который собрал все наработки единомышленников и выложил научную работу в открытый доступ, в которой описал основным элементом – блокчейн, а также описал принцип работы и математическую модель. Главной целью его работы является создание нового способа передачи средств (транзакций) между клиентами без посредников.

Чтобы было проще понять технологию блокчейн, рассмотрим пример показывающий работу этой технологии.

Представим, что у нас есть некая группа из 10 человек, сидящих в комнате. Все что скажет один будет услышано всеми. Рассмотрим последовательно, действия, совершаемые участниками в системе, где блокчейн будет представлен обычными листами бумаги.

У каждого имеется пустая коробка, в которую он будет складывать листы бумаги с информацией о всех совершенных транзакциях в системе. А также каждый участник записывает, все действия, совершаемые в этой комнате.

Настал момент, когда участнику под номером 7 необходимо отправить 10 рублей, участнику под номером 1. Поэтому он говорит вслух: «Я хочу отправить 10 рублей, участнику номер 1. Поэтому сделайте запись об этом в своем листе».

После этого все участники, проверяют имеется ли у номера 7, достаточная сумма, и если все сходится, то делают заметку о транзакции на листах. Именно после этого транзакция является выполненной.

После истечении некоторого времени и выполнения аналогичных операций другими участниками и заполнении листа бумаги, а в нашем случае это 10 записей, его складывают в коробку и берут новый.

И эта операция показывает, что все участники согласны с валидностью всех операций и невозможность изменения этого листа в будущем. Такая политика, позволяет обеспечить открытость, подразумевающая честность, всех транзакций между людьми, которые не доверяют друг другу.

Последний шаг является обычным решением задачи Византийских генералов. При взаимодействии пользователей сети, некоторые могут быть злоумышленниками, и чтобы избежать инцидентов, необходимо выбрать наиболее выигрышную стратегию. Но также необходимо, чтобы число злоумышленников было меньше некого значения, обычно это треть или половина от всего количества участников. Для решения этой задачи можно рассматривать через призму состязательных моделей.

Под состязательными моделями понимается нахождение среди пользователей зловредной группы, которая бы эксплуатировала уязвимость двойной траты (проведение операции перевода средств на два счета и последующая отмена честной транзакции). Можно выделить несколько категорий моделей:

Вычислительные пороговые модели. Для выбора правильного блока используется вычислительные мощности участников. Основателем этой модели является Сатоши Накамото. Такие системы основаны на принципе Proof-of-Work (Доказательство работы). Примером можно назвать: Bitcoin, Etherum и другие.

Долевая пороговая модель. Совокупность всех идей, где все компьютерные вычисления заменяются неким объектом, выполняющий роль ценности. Например, пользователь для подтверждения валидности блока использует как залог - криптовалюту. Следующее поколение блокчейна использует этот метод под названием Proof-of-Stake (Доказательство доли владения). Ярким представителем такой модели является NEO.

Получение вознаграждения за создание нового блока определяется состязательной моделью блокчейна. Поскольку, блокчейн – это распределенная БД, состоящая из блоков. Поэтому сложность добавления новых блоков зависит от состязательной модели.

Модель Proof-of-Work использует вычислительную мощность компьютеров пользователей сети. Первые участники, чьи устройства первыми создали новый блок, получают вознаграждения в виде криптовалюты (майнинг).

Модель Proof-of-Stake использует активы пользователей, как залог для того, чтобы подтвердить валидности операций в новом блоке. По итогу каждому участнику выдается вознаграждение, пропорционально тому, сколько они вложили своих активов.

Что определяет блокчейн как особенную технологию – это устранение человека из цепочки экономических операций. Что соответственно перекладывает ответственность на математику и ЭВМ, которые надежнее, чем люди.

Блокчейн по своей природе гораздо более удобен для продавцов, чем для покупателей:

Для продавцов блокчейн, гораздо удобнее, нежели чем для покупателей.

- необратимость транзакции и получения обратно денег за некачественный товар или услугу;

- единственная защита от неправомерного доступа к электронному кошельку — приватный ключ. При его потере, невозможно вернуть доступ.

Технология позволяет не только записывать транзакции, но и хранить любую другую информацию. Это позволяет обеспечить безопасность и доступность данных в любое время. Но есть и минус, который может быть и плюсом. Процесс изменения данных занимает большое время, поэтому злоумышленник, при подмене данных, потратит больше времени, и у него больше шансов быть пойманным.

Блокчейн, как мы рассмотрели выше, является технологией для всего. И сейчас многие компании работают с этой технологией, не исключено, что в ближайшее время они исчезнут. Именно эта технология позволяет, организовать работу множества участников, без определенного управляющего центра. И где это будет востребовано, именно там и найдет технология применение.

Использованные источники:

1. Одноранговая сеть. — Википедия. [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Одноранговая_сеть

2. Блокчейн — будущее финансовых технологий? — Хабрахабр. [Электронный ресурс]. Режим доступа: https://habrahabr.ru/company/selectel/blog/347848/