

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Российский экономический университет имени Г.В. Плеханова»

Факультет
Институт цифровой экономики и информационных технологий
Кафедра
управления информационными системами и программирования

КУРСОВАЯ РАБОТА
по дисциплине «Вычислительные системы, сети и телекоммуникации»
на тему «Одноранговые (peer-to-peer) сети»

Выполнил
обучающийся группы **БИ 4110**
очной формы обучения
ИЦЭиТ факультета
Хоанг Хай.
Научный руководитель:
Базовая кафедра Цифровой
экономики Института развития
информационного общества,
Старший преподаватель,
Волков Денис Владимирович.

Москва – 2020

Содержание

Введение	3
История возникновения.....	5
Глава 1: Теоретическая часть	7
1.1. Что такое Одноранговая сеть P2P?	7
1.2. Как работает одноранговая сеть?	9
1.2.1. Классификация одноранговых сетей.....	10
1.2.2. Классификация архитектуры компьютерных сетей	13
1.2.3. Маршрутизация в одноранговой сети	16
1.3. Преимущества и недостатки Одноранговых сетей P2P	23
1.3.1. Преимущества.....	23
1.3.2. Недостатки	24
Глава 2: Применение, пользы одноранговых сетей P2P	26
2.1. Применение одноранговых сетей	26
2.1.1. P2P-кредитование	26
2.1.2. P2P-платеж	26
2.1.3. Торговля одноранговыми электронными деньгами	27
2.1.4. Роль одноранговой сети в блокчейне.....	28
2.1.5. Протокол BitTorrent	29
2.2. Пользы одноранговой сети (P2P) в операциях с виртуальными валютами	30
Глава 3: Другие аспекты	31
3.1. Социальные аспекты.....	31
3.1.1. Правовые споры	31
3.1.2. Сетевой нейтралитет	32
3.2. Будущее совместного использования файлов в одноранговых сетях	33
3.2.1. Поставщик: уход в подполье.....	33
3.2.2. Нет места для поддельных файлов	33
3.2.3. Сократить разрыв	34
Заключение.....	35
Список использованных источников	36
Приложения.....	37

Введение

На самом деле Одноранговая сеть peer-to-peer, или P2P (С этого момента я буду использовать термин P2P, когда речь заходит о одноранговых сетях), был очень ранним, и если вы внимательно посмотрите, мы обнаружим, что он очень близок к повседневной жизни. В сфере криптовалют мы часто слышим об этой сетевой технологии.

P2P играет важную роль в развитии интернета. Этот тип сети наиболее часто используется, особенно когда речь идет о сайтах онлайн-медиа, таких как Youtube, Netflix, Spotify и т. д. не сложились. Сегодня клиент-серверные системы несколько более популярны, но это не значит, что P2P исчез. P2P продолжает развиваться, являясь ключевой платформой многих важных технологий и работая параллельно с клиент-серверной системой во многих приложениях в различных областях.

Программное пиратство и файлообмен уже существовали до развития интернета сегодня, в основном через форумы «Message board» и частные FTP-сайты. Но это утомительно, когда поиск файлов занимает даже больше времени, чем их загрузка. Более распространенный способ получить файл - это получить физическую копию непосредственно от друга.

P2P совместного использования файлов изменилось все это. Благодаря этому методу мы имеем прямой доступ к общим данным других пользователей. Конечно, технология обмена файлами P2P не используется в пиратских целях. Но, честно говоря, именно по этой причине и был создан этот метод.

Аспект совместного использования файлов в технологии P2P упоминается много, но это, конечно, не единственный случай использования.

Так что же такое P2P-сеть? Сравнить P2P с клиент-сервером? Каковы преимущества и недостатки P2P-сети? Это те вопросы, которые мы уточним в курсовой работе.

Целью работы – это понять определение одноранговой сети. Понять преимущества и недостатки одноранговой сети. Знать, как классифицировать одноранговые сети. Понять, почему одноранговые сети важны для развития Интернета. Разберитесь в роли и основных приложениях одноранговых сетей. Понять значение одноранговых сетей в развитии технологии блокчейн.

Задачи работы:

1. Разъяснить определение и функционирование одноранговых сетей, тем самым помогая читателям четко понять, как работают одноранговые сети.
2. В работе сравнить с клиент-серверной системой. Предоставить личные мнения и комментарии.
3. Проанализировать преимущества и недостатки одноранговой сети, уточнить приложения и пользы одноранговой сети, особенно в двух областях обмена файлами и торговли криптовалютами.

История возникновения

Интернет изначально задумывался как P2P-система. Со временем, в связи с высоким спросом на использование интернета, модель P2P постепенно трансформировалась и превратилась в модель клиент-сервер. В начале 1960-х годов интернет родился и быстро развивался. Число клиентов, получающих доступ к интернету, резко возросло, в результате чего IP-адресное пространство перестало быть достаточным для удовлетворения потребностей пользователей Сети. Кроме того, развитие интернета влечет за собой требования безопасности. Это препятствия, которые затрудняют построение и высвобождение истинной мощи P2P-моделей. Модель клиент-сервер родилась как решение этих проблем.

Похоже, что модель клиент-сервер оказалась правильным выбором, но сильный рост спроса на использование Интернета заставил разработчиков пересмотреть этот вопрос. Количество пакетов, передаваемых в сети, слишком велико, что приводит к перегрузке полосы пропускания, объем информации и объем памяти ресурсов также являются проблемой, с которой сталкиваются регуляторы и поставщики сетевых услуг. Поэтому стоимость серверной системы очень высока. И проблема этой проблемы вернула сетевых разработчиков к первоначальной модели P2P-сети.

В мае 1999 года, когда в Интернете появилось еще несколько миллионов пользователей, Шон Фаннинг представил музыкальное и файлообменное приложение Napster. Napster положил начало пиринговым P2P сетям, как мы их знаем сегодня, где «участвующие пользователи создают виртуальную сеть, полностью независимую от физической сети, без необходимости подчиняться каким-либо административным властям или ограничениям.»

Это центральная база данных, содержащая информацию обо всех музыкальных файлах, хранящихся у участников. Пользователь может искать песню с этого центрального сервера, но для загрузки он должен фактически подключиться к другому онлайн-пользователю и скопировать файлы с него. В

свою очередь, как только пользователь получит эту песню в библиотеке Napsterr, она станет источником, доступным другим пользователям в интернете.

Пользователь также может добавить свои собственные файлы, Napster затем проиндексирует и добавит их в базу данных, а затем будет готов распространять их по всему миру. Однако развертывание ограничено тем, что вы можете загрузить его только от одного человека. У сервиса есть преимущество в высокой доступности песен, но взамен скорость не слишком велика.

Благодаря этому концепция peer-to-peer стала известна во всем мире.

Napster в конце концов закрылся в 2001 году, после того как аналогичные сети были созданы для предоставления многих других вещей, а не только музыки. Фильмы, программное обеспечение и изображения уже доступны в сетях Morpheus, Kazaa и Gnutella (из которых Limewire, вероятно, является самым известным клиентом Gnutella).

На протяжении многих лет различные одноранговые протоколы обмена файлами и программное обеспечение появлялись и исчезали, но один из открытых протоколов был сохранен и продолжали развивать: BitTorrent.

Глава 1: Теоретическая часть

1.1. Что такое Одноранговая сеть P2P?

Peer-to-peer сеть, или сокращенно P2P, означает одноранговую сеть, компьютерную сеть, работа которой зависит от вычислительной мощности и пропускной способности всех участвующих машин, а не фокусируется на центральном сервере, как обычно.

Компьютерная сеть P2P построена на пропускной способности и производительности отдельных компьютеров в сети, а не на концентрации небольшого числа серверов. P2P-сети используются для подключения узлов к ad_hoc (непреднамеренным) соединениям и полезны для ряда целей, таких как обмен файлами контента, поиск ресурсов и т. д.

Чистая P2P-сеть не имеет понятия клиентов / серверов, но одноранговые узлы выполняют ту же функцию, что и клиент и сервер для других узлов в сети. Эта модель не совпадает с моделью клиент-сервер, частые соединения должны осуществляться через центральный сервер. Типичным примером обмена файлами без P2P является FTP-сервер, клиент и серверные программы не являются одним и тем же, в котором клиент устанавливает запросы загрузки/выгрузки, а сервер отправляет ответы на эти запросы.

Нет четкой границы между моделью P2P и моделью клиент-сервер. Обе модели могут быть интегрированы в одну и ту же сеть для различных целей. Некоторые сети, такие как Napster, OpenNAP и IRC@find, используют архитектуру клиент-сервер для нескольких целей, таких как поиск и использование структуры P2P для других целей. Другие сети, такие как Gnutella или Freenet, используют архитектуру P2P для всех целей, и это совершенно чистый P2P.

Когда P2P-сеть устанавливается через Интернет, центральный сервер может использоваться для индексирования файлов или может быть создана распределительная сеть, в которой общий доступ к файлам предоставляется всем. Оба пользователя в сети размещают определенный файл. Вместо того

чтобы просто принимать файлы, peer-to-peer превращает этот процесс в «улицу с двусторонним движением».

В одноранговых сетях пользователи могут отвечать другим пользователям. На самом деле, этот ответ (теперь известный как «seeding») имеет решающее значение для успеха одноранговых сетей. Если все просто скачивают и ни на что не реагируют (называется «leeching»), то никакой пользы по сравнению с клиент-серверской моделью нет.

В модели сервер-клиент производительность снижается, если пользователей больше, поскольку пропускная способность будет разделена между несколькими пользователями. В одноранговых сетях, чем больше пользователей, тем эффективнее сеть. Чем больше пользователей создадут определенный файл, доступный с их жесткого диска, тем легче будет его получить.

В современных P2P-сетях скорость действительно будет выше, когда все больше пользователей скачают файлы. Вместо того чтобы брать весь файл у одного пользователя, они берут меньшие части у сотен или тысяч других. Даже если у них есть только немного свободной полосы пропускания, объединение нескольких соединений означает, что пользователь получит максимально возможную скорость. Затем будет очередь пользователя - внести свой вклад в распространение файлов.

В предыдущих формах P2P-сетей для организации сети по-прежнему требовался центральный сервер, выступающий в качестве базы данных, содержащей информацию о пользователях и подключенных файлах, доступных в системе. Хотя тяжелая задача передачи файлов была выполнена непосредственно между пользователями, Сети все еще уязвимы. Поражение центрального сервера означает полное отключение связи.

Это больше не существует из-за недавних событий. Сегодня программное обеспечение может напрямую запрашивать сверстников, если

они видят конкретный файл. Нет никакого способа победить эти сети, они действительно не могут быть сломаны.

Новые совместные P2P-системы выходят за рамки эпохи узлов, делающих аналогичные вещи при совместном использовании ресурсов, и ищут разнообразных узлов, которые могут принести уникальные ресурсы и возможности виртуальному сообществу, тем самым расширяя его возможности для участия в более масштабных задачах, чем те, которые могут быть выполнены отдельными узлами, но которые выгодны всем узлам.

1.2.Как работает одноранговая сеть?

Единственное требование для подключения компьютера к одноранговой сети – это подключение к Интернету и программное обеспечение P2P. Популярные P2P – программы включают Kazaa, Limewire, BearShare, Morpheus и Acquisition. Эти программы подключаются к P2P-сетям, таким как «Gnutella», и позволяют компьютерам получать доступ к тысячам других систем в сети.

После подключения к сети программное обеспечение P2P позволяет пользователю искать файлы на компьютерах других людей. Другие пользователи Сети также могут искать файлы на компьютере пользователя, но обычно ограничиваются общей папкой пользователя.

В то время как P2P-сеть делает обмен файлами легким и удобным, она также приводит к пиратству программного обеспечения и незаконной загрузке музыки. Поэтому, чтобы быть в безопасности, программное обеспечение и музыку следует скачивать только с законных веб-сайтов.

Одноранговая сеть состоит из всех узлов, представляющих участвующие хосты, и связей между этими узлами. Связь существует между двумя узлами, когда один узел определяет местоположение другого. Основываясь на топологии между узлами одноранговой сети, мы можем

классифицировать ее на: структурированную, неструктурированную и гибридную P2P.

1.2.1. Классификация одноранговых сетей

1.2.1.1. Неструктурированные одноранговые сети

Узлы в неструктурированных P2P-сетях не организованы в соответствии с какой-либо конкретной структурой. Участники случайным образом общаются друг с другом. Считается, что эти системы обладают сильной способностью отбиваться от действий уходящих пользователей (так как некоторые узлы часто присоединяются и покидают сеть).

Хотя неструктурированные P2P-сети легче строить, они могут потребовать более высокой загрузки памяти и процессора, поскольку поисковые запросы отправляются как можно большему числу одноранговых узлов. Это имеет тенденцию наводнять сеть запросами, особенно если только небольшое количество узлов предоставляет желаемый контент.

1.2.1.2. Структурированные одноранговые сети

Узлы в P2P-сетях имеют организованную архитектуру, которая позволяет узлам эффективно искать файлы, даже если контент не является широко доступным. В большинстве случаев это достигается за счет использования хэш-функций, позволяющих осуществлять поиск в базе данных.

Хотя структурированные сети могут быть более эффективными, они часто демонстрируют более высокий уровень концентрации и часто требуют более высоких затрат на настройку и техническое обслуживание. Кроме того, Сети с менее надежной структурой сталкиваются с высокой частотой выхода пользователей из сети.

1.2.1.3. Структурированные одноранговые сети

Для того, чтобы преодолеть недостатки двух одноранговых сетевых структур, был создан одноранговый гибрид: сочетание традиционной

архитектуры клиент-сервер с некоторыми аспектами горизонтальной архитектуры. ряд. Например, эта сеть может создать центральный сервер для создания соединений между одноранговыми компьютерами в сети. По сравнению с двумя другими архитектурами гибридные модели часто демонстрируют более высокую производительность. Они сочетают в себе основные преимущества каждого метода, принося значительные уровни эффективности и децентрализации.

В этой модели существует центральный сервер, который поддерживает связанные базы данных и таким образом облегчает поиск узлов друг друга. Примером гибридной модели может служить бывший сервис Spotify. Гибридные сети обмениваются децентрализованную, равную структуру узлов, предоставляемых в чистой одноранговой сети с ее эффективностью и скоростью. Децентрализация помогает повысить эффективность процесса запросов и поиска данных.

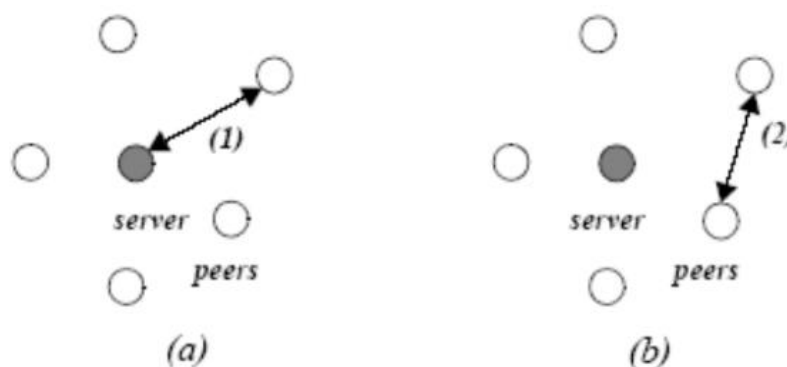


Рис. 1 - гибридная модель P2P

На рис. 1 приведен пример гибридной модели P2P. Чтобы подключиться к сети P2P, одноранговые узлы сначала иницируют контакт с сервером (1), чтобы сохранить позицию или идентификационные характеристики однорангового узла, а затем одноранговые узлы связываются друг с другом напрямую (2). Некоторые типичные примеры гибридных моделей P2P включают: Napster, Groover, Aimster, Magi, Softwax и iMesh ...

Существует несколько сетевых систем, которые объединяют как чистые P2P, так и гибридные модели P2P для разработки персональных проектов, таких как Skype, KaZaa. Решение заключается в том, что помимо использования центрального сервера для проверки учетных данных однорангового узла, можно также использовать общедоступные одноранговые узлы IP в качестве Супеузла. Эти супеузлы могут хранить некоторую информацию или нет, другие узлы будут искать информацию в Супеузле. В зависимости от цели разработки проекта, может быть использована одна из двух моделей P2P или их комбинация, как некоторые из упомянутых выше проектов.

Таблица 1

Сравнение неструктурированных и структурированных P2P

	Неструктурированные P2P	Структурированные P2P
Связи между узлами сети	Организованная, следуя определенному алгоритму (DHT-распределенная хэш-функция)	Случайным образом, нет никаких правил.
Построение узлов сети	Построение каждого узла сети будет отвечать за общий фрагмент данных	Строить по ссылке, доступной в сети. Затем добавить его новые ссылки.
Метод искать данные	Поисковый запрос применяет общий протокол для определения того, какой сетевой узел отвечает за данные, подлежащие поиску	Поисковый запрос передается по всей сети, отправляя как можно больше узлов сети.
Преимущества	Искать файлы эффективно и быстро, даже если они не широко доступны в сети.	Легко строить сетевые узлы; Сильная способность противостоять деятельности пользователей покидает сеть.

Недостатки	Высокий уровень концентрации; Высокие затраты на установку и техническое обслуживание.	Нужно больше памяти и процессора; Вероятность найти необычные, менее распространенные данные в интернете довольно мала.
-------------------	---	--

1.2.2. Классификация архитектуры компьютерных сетей

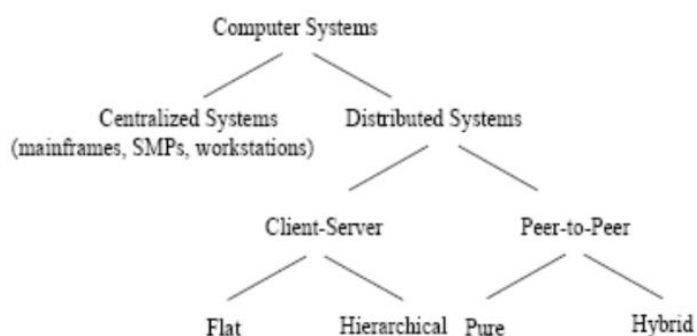


Рис. 2

Все компьютерные системы можно разделить на два типа: распределенные и централизованные. Распределенные системы можно разделить на две модели: клиент-серверную и P2P. в клиент-серверной модели все клиентские компьютеры взаимодействуют с одним сервером или могут быть децентрализованы для развития масштабируемости. В иерархической модели сервер уровня будет выступать в качестве клиента более высокого уровня.

В централизованных P2P-сетях существует Центральный индекс, поддерживаемый в одном фиксированном местоположении, содержащий информацию о местоположении объектов и адресах узлов в сети. Участники находят местоположение нужных ресурсов в сети, запрашивая центральный сервер индексирования. Эта P2P-структура не соответствует масштабам расширения и центральный индексный сервер может быть атакован или поврежден, прерван, что приведет к нарушению работы всей сети.

В отличие от централизованной архитектуры, P2P может использовать распределенную структуру каталогов, в которой существует несколько централизованных индексных центров. Эти системы могут быть полностью децентрализованы, как Gnutella, в которой узлы работают совершенно одинаково, то есть содержат ресурсы и структуры для запросов в сети. Или системы могут также иметь согласованную архитектуру, в которой некоторые узлы в сети играют роль поддержания индексных баз данных, называемых узлами уведомлений или «суперузлами» для обслуживания запросов. Поиск и запрос ресурсов других общих узлов.

Все эти сетевые архитектуры используются в блокчейне, в зависимости от дизайна функции блокчейна. Например, большинство публичных блокчейнов децентрализованы и не имеют кнопок уведомлений. Однако некоторые блокчейн-системы все еще имеют централизованные узлы для регулирования данных, такие как IoTА и т. д.

Исходя из этих сетевых структур и децентрализации в блокчейн, Блокчейн можно разделить на три категории: государственные блокчейн (публичный блокчейн), отдельный блокчейн (частный блокчейн) и совместной работы с blockchain (блокчейн-консорциум):

- **Публичный блокчейн:** тип блокчейна, к которому может присоединиться любой желающий и который имеет право читать и записывать данные. Как правило, для этого типа блокчейна используются такие криптовалюты, как Биткоин, Эфириум и т. д. Узлы могут присоединяться к сети или выходить из нее, и каждый узел в сети полностью независим, нет центрального узла управления или таблиц. адрес маршрутизации. Аутентификация транзакций в публичных блокчейнах происходит через основанные на доказательствах механизмы консенсуса (такие как доказательство работы или доказательство доли участия) и требует участия многих узлов в сети. Эта блокчейн-система

считается вполне безопасной, потому что затраты, необходимые для совершения атаки на систему, довольно высоки и намного выше, чем выгоды, полученные при успешной атаке.

- **Частный блокчейн:** это блокчейн-сети, статус которых определяется одним или ограниченным числом участников. Эти члены проходят проверку подлинности и часто знают и полностью доверяют друг другу. Эти участники имеют возможность записывать данные и определять операционный статус блокчейна. Кроме того, другие пользователи могут только читать данные, а не писать. Частные блокчейны строятся из надежных групп членов, поэтому они часто используют механизмы консенсуса, основанные на византийской устойчивости к ошибкам с относительно быстрым временем проверки транзакций (поскольку для аутентификации требуется лишь небольшое количество устройств). Ripple - это форма частного блокчейна, которая требует, чтобы только 80% узлов работали стабильно для проведения транзакций.
- **Разрешения:** также известный как Консорциум, форма частного блокчейна, но добавляющий определенные функции, сочетая «веру» при участии в публичном блокчейне и «абсолютную веру» при участии в частном блокчейне. Затем участники будут проверены и им будет предоставлен доступ к сети группой других участников. Например: банки или финансовые учреждения совместного предприятия будут использовать свой собственный блокчейн.

Таким образом, структурированная или неструктурированная одноранговая сеть имеет свои преимущества и недостатки; но общим моментом в обеих архитектурах является то, что она помогает обмениваться информацией между узлами сети без необходимости в каком-либо сервере или

посреднике. В результате эта сеть стала системообразующей архитектурой в транзакциях криптовалютного рынка в частности и блокчейна в целом.

1.2.3. Маршрутизация в одноранговой сети

Архитектура сети P2P разработана на основе одноранговых узлов. Эти кнопки имеют возможность одновременно выступать как «клиенты», так и «серверы». Это создает больше трудностей в традиционных моделях. В традиционных моделях сервер обычно имеет фиксированный адрес, поэтому любой клиент может легко запросить сервер через его IP-адрес или через посреднический DNS-сервер. Но этого не существует в одноранговой сетевой архитектуре. Узлы, участвующие в этой P2P-сети, могут присоединиться к системе или покинуть ее в любое время, поэтому P2P-сети очень динамичны и нестабильны. В одноранговой сети существует два важных вопроса: как узлы могут находить друг друга и как распределять и синхронизировать данные по всей сети.

Для этого в P2P-сетях используются два механизма: поиск и адресация. Узлы и ресурсы в сети помечаются определенными адресами, и информация об этом адресе хранится на разных узлах сети. Когда узлы хотят общаться и общаться по сети, они будут искать данные для этих адресов и отправлять и получать информацию. Механизмы поиска и адресации определяют операционную структуру сети, а также эффективность использования ресурсов в сети.

Большинство методов поиска основаны на пересылке пакетов. Узлы, когда возникает необходимость в связи, генерируют пакеты для запроса к другим узлам, этот запрос будет перенаправляться (или маршрутизироваться) до тех пор, пока он не достигнет узла с нужными данными (или указателем на нужные данные). Для пересылки сообщений каждый узел должен содержать информацию о нескольких других «соседях». Информация этих соседей формирует таблицу маршрутизации узла.

Когда запускается новый узел, он должен искать другие узлы в сети для подключения. Чтобы начать этот процесс, новый узел должен обнаружить по крайней мере один узел, доступный в сети, и подключиться к нему.

Теперь возникает вопрос: очевидно, что в P2P-сети у нас не будет сетевой структуры, и каждый компьютер в сети имеет уникальный адрес, поэтому нам будет очень трудно сканировать всю сеть, чтобы найти соседние узлы, и поэтому трудно найти другие узлы онлайн. Итак, как же мы действительно решаем эту проблему в P2P-сети?

Существует множество различных способов подключения узлов к сети, в зависимости от различных протоколов. Но в основном мы можем упомянуть следующие методы:

1.2.3.1. Использовать известный внешний адрес

Узлы, участвующие в сети, могут обращаться к форумам, общедоступным веб-сервисам для получения информации о некоторых IP-адресах внешних сетей. Этот адрес можно использовать для ручного добавления в таблицу маршрутизации.

Для каждого из этих адресов клиент пытается подключиться, отправить HTTP-запросы, прочитать соответствующий ответ и проанализировать IP-адрес с этого адреса. Если этот процесс будет успешным, IP-адрес будет возвращен, он будет транслироваться на другие узлы, к которым он подключен.

1.2.3.2. Подключение к запросу адреса к нему (обратный вызов адреса)

Когда узел получает соединение с ним от узла в сети. Два узла инициируют соединение, и узел, который получает это соединение, передаст свой адрес узлу запроса, чтобы сделать локальное соединение, если это необходимо.

После повторной отправки Вашего адреса этот узел будет отправлять запросы узлу обратного вызова, чтобы получить список других адресов в сети, которые другой узел должен добавить в свою таблицу маршрутизации.

1.2.3.3. IRC-адрес

В дополнение к обучению и обмену собственным адресом, узлы также ищут адреса других узлов через IRC-канал. Это один из способов, используемых в старых версиях биткойна.

После того, как узел кодирует свой собственный адрес в строку, используемую в качестве псевдонима. Он будет случайным образом присоединяться к IRC-каналу (в Биткойне этот канал имеет имя между # bitcoin 00 и # bitcoin99). Затем он выдаст команду WHO, прочитает строки по мере их появления и расшифрует IP-адреса других узлов в канале. Это повторяется вечно, пока кнопка не будет выключена.

1.2.3.4. Адрес кнопок по умолчанию

Когда новый узел присоединяется к сети, он ничего не знает о других членах. Итак, как в этом случае его можно найти и подключить к другим узлам?

В принципе, специальных узлов в блокчейн-сетях не будет, роль узлов будет равна роли друг друга. Однако есть еще некоторые стабильные узлы, которые работают в течение длительного времени, или узлы, которые поддерживаются для определенных целей по замыслу. Эти узлы называются начальными узлами. Начальные узлы поддерживаются и перечислены в списке, который включен в само прикладное программное обеспечение блокчейна или в ряд предоставленных фиксированных баз данных. И другие узлы, которые являются новыми для сети, могут запрашивать и получать список адресов, используемых для их маршрутизации в этих начальных узлах. Хотя это соединение не требуется, полный узел может указать адрес своих соседних узлов, как указано выше, но подключение к начальным узлам может

помочь просто. Процесс инициализации соединений и таблиц маршрутизации на узлах позволяет узлам сети быстро находить друг друга.

Существуют также начальные узлы, обслуживаемые на нескольких DNS-серверах в сети. Для подключения к этим начальным узлам и поиска других компьютеров в сети клиент выдает DNS-запросы к списку выбранных имен серверов службы DNS. Например, с биткоином этот список адресов в настоящее время включает в себя:

seed.bitcoin.sipa.be

dnsseed.bluematt.me

dnsseed.bitcoin.dashjr.org

seed.bitcoinstats.com

seed.bitcoin.jonasschnelli.ch

seed.btc.petertodd.org

Ответы DNS могут содержать несколько требуемых IP-адресов. И эти адреса могут быть добавлены в список маршрутизации узла.

Как только узлы связи будут найдены, клиент подключится к ним через установление TCP-соединений. При установлении соединения узлы начинают инициировать протокол прямого рукопожатия, передавая сообщения для установления соединения и поиска необходимой информации. В Биткойне используется порт по умолчанию – 8333 или какой-то другой альтернативный порт.

При установлении одного или нескольких соединений новый узел отправляет соседям сообщение, содержащее его собственный IP-адрес. Эти соседние узлы, в свою очередь, передадут это сообщение своим другим соседям. Это делает адрес вновь созданного узла рекламируемым по всей сети и лучше подключается. Кроме того, вновь подключенные узлы могут отправлять запросы на запрос узлов соседей и просить их вернуть список IP-

адресов других узлов в сети. Таким образом, один узел может найти другие узлы для подключения и объявить о своем существовании в сети, чтобы другие узлы могли найти его. Это можно описать следующим образом:

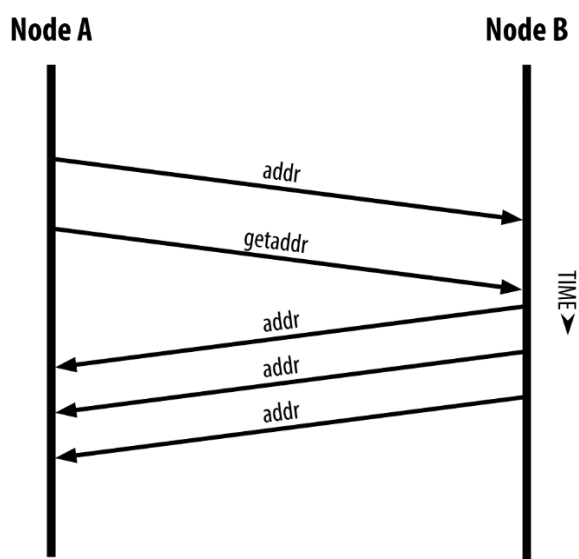


Рис. 3 - Адрес кнопок по умолчанию

Узлы в одноранговой сети могут присоединяться или удаляться случайным образом, поэтому соединения и таблицы маршрутизации не всегда надежны. Таким образом, существуют узлы, которые должны постоянно обнаруживать новые узлы и поддерживать другие узлы для установления соединений, когда они присоединяются к сети. Чтобы повысить эффективность этого процесса, у нас есть концепция, называемая «bootstrap». Эта концепция помогает уменьшить пропускную способность и сетевые ресурсы, используемые при установлении соединения. После начальной загрузки узел будет помнить свои последние успешные одноранговые соединения, так что при перезапуске он сможет быстро восстановить соединения с предыдущей одноранговой сетью. Если ни один из этих старых узлов не отвечает на его запрос на соединение, он будет использовать начальные узлы для перезапуска процесса построения соединения.

Поиск других ресурсов в сети P2P аналогичен, единственное различие заключается в запросах и ответных сообщениях между узлами и заданиями, которые должны выполняться узлами. Например, если мы хотим найти файл,

совместно используемый в сети P2P, узел может запросить его хэш-значение через DHT-хэши, хранящиеся на узлах в соответствии с приведенным выше поиском, когда вместо возвращаемых адресов можно вернуть конкретную информацию об узлах, содержащих эти данные.

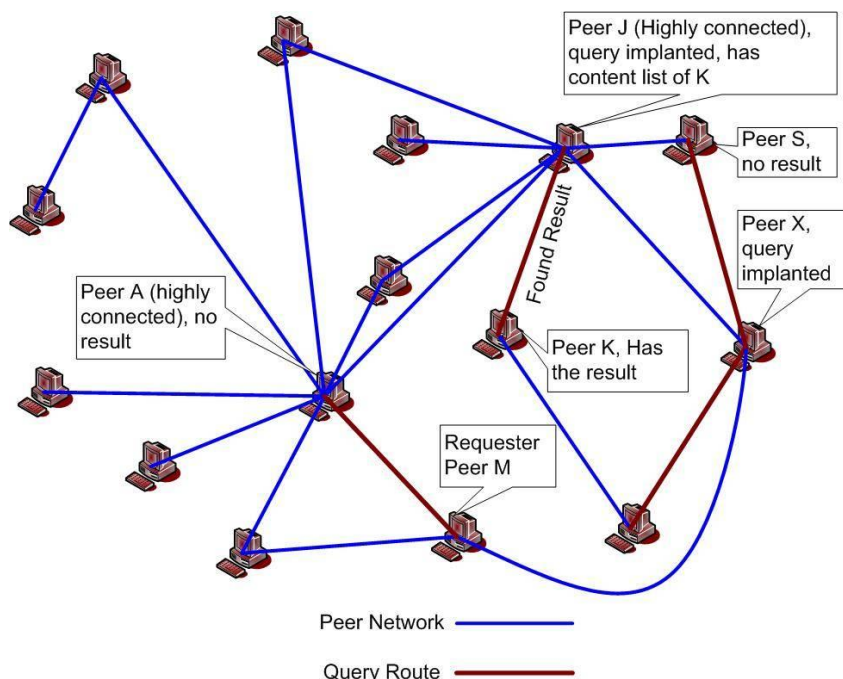


Рис. 4 - Процесс поиска ресурсов на P2P

Вышеупомянутый протокол используется в сети P2P Gnutella и большинстве других протоколов P2P, таких как биткойн или многие другие модели блокчейна. Это называется методом поиска по ширине (BFS) на карте наложенной сети с ограничением глубины D. В этом методе узел запроса будет отправлять запрос запроса всем своим соседям. Каждый сосед обрабатывает запрос и возвращает результат, если данные найдены. Этот сосед затем пересылает запрос запроса всем своим соседям, кроме узла запроса. Этот процесс продолжается до тех пор, пока не будет достигнут предел глубины D. Однако это не единственный метод, используемый для того, чтобы узлы могли находить друг друга и строить свои таблицы маршрутизации. Как видно, приведенный выше метод генерирует большое количество избыточных, дублирующихся и не масштабируемых сообщений. Поэтому существует множество других методов, используемых в других типах протоколов P2P для

его улучшения. Например, глубокий-петля методов итерации, к-Уокер случайных переходов, модифицированный случайный поиск в ширину, к-ходунки случайных шагов, интеллектуальных поисков и т. д. Однако в целом во всех методах таким образом механизм всегда тот же, что и выше, то есть запрос пересылается в подмножество соседних узлов и продолжает пересылаться другим ближайшим соседям, за исключением некоторой обрезки, чтобы избежать повторных переходов.

Эффективность маршрутизации обычно измеряется количеством переходов на запрос. В некоторых системах он также оценивается по количеству сообщений, передаваемых на запрос. Различные методы поиска создают компромисс между этими желательными характеристиками. Сложность протоколов, обусловленная дополнительными ограничениями и требованиями, зависит от типа сети. Желательные характеристики алгоритма поиска в P2P-системах включают высокое качество результатов запросов, минимизацию количества узлов для запроса, высокую эффективность маршрутизации, балансировку нагрузки, устойчивость к ошибкам узлов и возможность поддержки сложных запросов. Качество результатов запроса зависит от приложения. В общем случае она измеряется количеством результатов и релевантностью, такими как ограничения на надежность, анонимность, оптимизация задержек, оптимизация потоков с высокой пропускной способностью нескольких сообщений...

После нахождения необходимых кнопок и ресурсов приложения в сети будут выполнять запросы, соответствующие операционным требованиям сети, такие как загрузка общих файлов, распространение результатов. создание блока (после подтверждения работы или какого-либо другого типа подтверждения работы) ... Эти действия происходят точно так же, как протоколы в среде TCP / IP. На блокчейне узлы будут запрашивать и проводить коммуникацию для синхронизации данных в сети.

1.3.Преимущества и недостатки Одноранговых сетей P2P

1.3.1. Преимущества

В модели сервер-клиент производительность снижается, если пользователей больше, поскольку пропускная способность будет разделена между несколькими пользователями. В P2P-сетях, чем больше пользователей, тем эффективнее сеть. Чем больше пользователей создадут определенный файл, доступный с их жесткого диска, тем легче будет его получить. Вместо того чтобы извлекать весь файл из одного пользователя, вы извлекаете более мелкие разделы из сотен или тысяч других. Даже если у них есть только немного свободной полосы пропускания. Затем будет очередь пользователя - внести свой вклад в распространение файлов.

Одноранговые сети более безопасны, чем традиционные архитектуры клиент-сервер. Распределение блочных цепочек на большом количестве узлов делает их практически устойчивыми к атакам, которые были использованы для атаки нескольких систем. Точно так же, поскольку большинство узлов должны прийти к консенсусу, прежде чем новые данные будут добавлены в блокчейн, злоумышленник почти не может изменить эти данные. Это особенно верно для крупных сетей, таких как сеть Биткойн.

Помимо безопасности, использование архитектуры P2P в криптовалютных блокчейнах также помогает им противостоять цензуре со стороны центральных властей. В отличие от стандартных банковских счетов, правительство не может заморозить или изъять цифровые кошельки. Кроме того, архитектура P2P также помогает блокчейнам противостоять цензуре платформ контента и частных платформ обработки платежей. Некоторые создатели контента и интернет-торговцы используют криптовалютные платежи как способ избежать блокировки третьими лицами.

- Все компьютеры, участвующие в сети, могут предоставлять информацию, включая пропускную способность, данные и

вычислительную мощность. Чем больше задействовано машин, тем больше информации предоставляется пользователям.

- Благодаря распределенному характеру другие сети все еще хорошо работают, когда один компьютер в сети имеет проблему.
- Компьютеры в системе действуют как серверы и клиенты
- Программное обеспечение является простым в использовании и хорошо интегрированным
- Программное обеспечение имеет различные инструменты и функции поддержки пользователей
- Программное обеспечение поддерживает сетевые протоколы, такие как SOAP или XML-RPC.

1.3.2. Недостатки

- Запросы на обслуживание могут быть настроены, поэтому результаты будут отличаться
- Исходящие запросы не получают ответа, потому что нет никакой гарантии, что машина сможет удовлетворить этот запрос.
- Ресурсы исчезнут, потому что узел, предоставляющий ресурс, будет отключен в любое время.

Несмотря на свои многочисленные преимущества, использование P2P-сетей на блокчейне также имеет определенные ограничения.

Поскольку распределенные бухгалтерские книги должны обновляться на каждом узле, а не на центральном сервере, добавление транзакций в блокчейн требует сложных алгоритмов. Это, одновременно повышая безопасность, значительно снижает производительность и является одним из главных препятствий для масштабируемости и широкого распространения сетевых приложений. Однако криптографы и разработчики блокчейна изучают альтернативы, которые могут быть использованы в качестве масштабируемых решений. Известные примеры включают Lightning Network, Ethereum Plasma и протоколы Mumblewimble.

Еще одно возможное ограничение связано с атаками, которые могут возникнуть во время событий хардфорка. Поскольку большинство блокчейнов децентрализованы и имеют открытый исходный код, группы узлов могут свободно копировать, изменять код и отсоединяться от основной цепочки для формирования новой параллельной сети. Жесткие вилки-это нормально, и сами по себе они не представляют угрозы. Однако, если определенные меры безопасности не будут применены должным образом, обе цепочки могут легко стать объектами атак.

Более того, распределенный характер P2P-сетей делает их относительно трудными для контроля и регулирования, причем не только в сегменте блокчейна. Некоторые P2P-приложения и компании занимались незаконной деятельностью и нарушением авторских прав.

Глава 2: Применение, пользы одноранговых сетей P2P

2.1. Применение одноранговых сетей

Помимо обмена файлами через одноранговую сеть, P2P-системы используются во многих различных областях - особенно в области криптовалют.

2.1.1. P2P-кредитование

P2P-кредитование, также известное как одноранговое кредитование. Это бизнес-модель между физическими лицами, предприятиями и инвесторами через подключение к Интернету для совершения кредитных операций.

Характеристики:

- На основе P2P платформы инвесторы могут выбирать заемщиков
- Генерировать высокую прибыль
- Заемщикам и кредиторам не нужны предварительные отношения
- Процесс кредитования происходит онлайн, всего за несколько простых и чрезвычайно быстрых шагов
- Требуется проверка информации о клиенте, банковском счете, занятии и доходах
- Подходит для небольших кредитов, краткосрочных кредитов
- Онлайн-модель кредитования привлекает большое количество заемщиков, инвесторы могут легко следить за своей прибылью от кредитов.
- Обеспечение соблюдения законов и отчетности

2.1.2. P2P-платеж

P2P-платеж – одноранговая оплата. Это чрезвычайно быстрая форма онлайн-оплаты, когда она способна осуществлять прямой перевод между двумя физическими лицами. Пользователи могут открыть учетную запись поставщика, чтобы подключить услугу к банковскому счету. Затем они будут

вносить деньги на счет для совершения транзакций, совершать платежи с другими лицами, которые также имеют счета у этого поставщика.

Одним из приложений, использующих это применение P2P, является «Metal Pay». Система «Metal Pay» работает на основе блокчейна - следовательно, они работают на платформе P2P. Это приложение позволяет пользователям оплачивать или переводить деньги с помощью MTL - виртуальной валютной единицы, разработанной в 2017 году. Тем более, что за каждый платеж пользователь будет получать вознаграждение в размере MTL до 5% от суммы транзакции. Цель этой системы - широко распространить знание монеты MTL среди всех желающих.

2.1.3. Торговля одноранговыми электронными деньгами

Одноранговая сеть имеет множество приложений, как правило, P2P криптовалютные транзакции (децентрализованные транзакции). Это транзакции, управляемые исключительно программным обеспечением, позволяющим участникам рынка торговать непосредственно друг с другом без необходимости привлечения третьей стороны (например, банков/финансовых учреждений).

Компании будут создавать платформы для торговли криптовалютами P2P, чтобы помочь пользователям упростить транзакции, и взимать плату за каждый раз, когда они совершают транзакцию.

Благодаря криптовалюте P2P были сняты ограничения на биткоин-транзакции. В торговле криптовалютами спрос на обмен виртуальных валют на наличные деньги растет, что приводит к поддержке обмена виртуальных валют с онлайн-бирж, таких как BTC China, Kraken и Bitstamp.

Однако эти сделки контролируются третьими лицами. Эти компании спонсируют сделки, арбитражируют, когда возникают споры, и взимают небольшую плату.

Благодаря программно управляемой одноранговой P2P-торговле рынок может устранить существование третьих сторон и по-прежнему иметь возможность эффективно взаимодействовать друг с другом, даже быстрее и проще много.

2.1.4. Роль одноранговой сети в блокчейне

На ранних стадиях развития Биткойна Сатоши Накамото определил его как «одноранговую электронную денежную систему». Биткойн изначально создавался как форма цифровых денег. Он может быть передан от одного пользователя к другому через одноранговую сеть, которая управляет распределенной бухгалтерской книгой, называемой блокчейн.

В этом контексте речь идет о P2P архитектуре, блокчейн-ориентированной технологии, которая позволяет пользователям торговать Биткоином и другими криптовалютами по всему миру без посредников или каких-либо серверов. центр. Кроме того, любой желающий может стать узлом в сети Биткойн, если он хочет участвовать в процессе проверки и валидации блоков.

Таким образом, нет никакого банка для обработки или записи транзакций в сети Биткойн. Вместо этого блокчейн действует как цифровая бухгалтерская книга, которая публично записывает всю деятельность. По сути, каждый узел хранит копию блокчейна и сравнивает ее с другими узлами, чтобы обеспечить точные данные. Сеть быстро отрицает любые вредоносные или неправильные действия.

В контексте криптовалютного блокчейна узлы могут выполнять различные роли. Например, полные узлы - это узлы, которые помогают поддерживать безопасность сети путем проверки транзакций в соответствии с правилами системного консенсуса.

Каждый полный узел поддерживает полную, актуальную копию блокчейна - что позволяет им участвовать в совместной работе по проверке

реального состояния распределенной бухгалтерской книги. Однако стоит отметить, что не все полностью проверенные узлы являются майнерами.

Одноранговая архитектура является ключевым элементом технологии блокчейн - фундамента криптовалют. Существует множество способов разработки и использования одноранговой архитектуры. Распределяя бухгалтерские книги транзакций по большой сети узлов, архитектура P2P обеспечивает безопасность, децентрализацию и антицензурные возможности.

2.1.5. Протокол BitTorrent

Разработанный в 2001 году, BitTorrent - это протокол с открытым исходным кодом, в котором пользователи создают метафайл (называемый торрент-файлом), содержащий информацию о загрузке, фактически не предоставляя данные о загрузке. Трекер необходим для хранения этих метафайлов, а также человека, который в настоящее время хранит их. Однако в качестве открытого протокола любой может запрограммировать клиентское программное обеспечение или трекер.

Таким образом, даже если он нуждается в Центральном трекере для поддержания базы данных доступных файлов, многие другие трекеры могут существовать одновременно. Любой торрент-файл с описанием может быть зарегистрирован несколькими трекерами. Это делает сеть BitTorrent чрезвычайно мощной и практически невозможной для полного уничтожения.

С момента его первого запуска были сделаны и другие улучшения, позволяющие пользователям загружать файлы без трекера. DHT (distributed hash table) означает индексирование доступных файлов, которые могут быть распределены всеми пользователями.

Магнит линк (Magnet link) совсем не такой. В принципе, магнитная ссылка работает аналогично обычному торрент-файлу, с достаточным количеством информации, чтобы компьютер мог загрузить файл данных из «сверстника» (который может быть понят как источник загрузки или люди,

которые его загрузили). Однако магнитная ссылка не существует в виде фиксированного файла, как торрент, а только текст, содержащий всю информацию.

2.2. Пользы одноранговой сети (P2P) в операциях с виртуальными валютами

- ***Сопротивляться централизованные торговые права:***

Также известный как анти-транзакционный контроль. P2P-транзакции не будут контролироваться каким-либо органом или организацией, интересы участников сделки сохраняются. Даже если одна часть системы перестала работать, остальные остались незатронутыми.

- ***Низкая стоимость***

Нет необходимости платить третьим лицам за торговлю, потому что система P2P контролируется программным обеспечением.

- ***Высокая безопасность конфиденциальности***

Правительство не имеет права вводить правила аутентификации личной информации для P2P-транзакций, поэтому конфиденциальность участников транзакций остается конфиденциальной.

- ***Высокая безопасность***

P2P-сеть не удерживает монеты в каждой транзакции, но помогает сторонам торговать непосредственно друг с другом, поэтому не будем беспокоиться о потере денег во время транзакции.

Однако P2P-транзакции все еще имеют некоторые недостатки, такие как длительное время транзакции и низкая ликвидность.

Глава 3: Другие аспекты

3.1. Социальные аспекты

3.1.1. Правовые споры

Закон об интеллектуальной собственности и незаконный обмен информацией

Хотя одноранговые сети могут использоваться в законных целях, правообладатели нацелились на P2P за участие в совместном использовании защищенных авторским правом материалов. Одноранговая сеть предполагает передачу данных от одного пользователя другому без использования промежуточного сервера. Компании, разрабатывающие P2P-приложения, были вовлечены в многочисленные судебные дела, прежде всего в США, главным образом по вопросам, связанным с законом об авторском праве.¹ Два крупных дела-Grokster vs RIAA и MGM Studios, Inc. v. Grokster, Ltd.²

Возникли разногласия по поводу незаконного использования одноранговых сетей в целях обеспечения общественной и национальной безопасности. Когда файл загружается через одноранговую сеть, невозможно узнать, кто создал файл или какие пользователи подключены к сети в данный момент времени. Надежность источников-это потенциальная угроза безопасности, которую можно увидеть в одноранговых системах.³

Исследование, заказанное Европейским Союзом, показало, что незаконная загрузка может привести к увеличению общих продаж видеоигр, поскольку новые игры взимают плату за дополнительные функции или уровни. Авторы статьи пришли к выводу, что пиратство оказывает негативное финансовое воздействие на кино, музыку и литературу. Исследование опиралось на самоотчетные данные о покупках игр и использовании

¹ Glorioso, Andrea; et al. (2010). "The Social Impact of P2P Systems". In Shen; et al. (eds.). Handbook of Peer-to-Peer Networking. Springer. p. 48. ISBN 978-0-387-09750-3.

² John Borland (April 25, 2003). "Judge: File-Swapping Tools are Legal". news.cnet.com. Archived from the original on 2012-03-10.

³ The Government of the Hong Kong Special Administrative Region, (2008). Peer-to-peer network. Retrieved from website: <http://www.infosec.gov.hk/english/technical/files/peer.pdf>

нелегальных сайтов загрузки. Были предприняты усилия для устранения последствий ложных и неверно припоминаемых реакций.⁴

3.1.2. Сетевой нейтралитет

Одноранговые приложения представляют собой одну из основных проблем в споре о сетевой нейтральности. Интернет-провайдеры (ISP), как известно, ограничивают P2P-файлообменный трафик из-за его высокой пропускной способности. По сравнению с веб-браузингом, электронной почтой или многими другими видами использования интернета, где данные передаются только с короткими интервалами и относительно небольшими количествами, P2P-файлообмен часто состоит из относительно большого использования полосы пропускания из-за продолжающейся передачи файлов и пакетов координации Роя/сети.

В октябре 2007 года Comcast, один из крупнейших провайдеров широкополосного интернета в США, начал блокировать P2P-приложения, такие как BitTorrent. Их обоснование состояло в том, что P2P в основном используется для обмена незаконным контентом, а их инфраструктура не предназначена для непрерывного трафика с высокой пропускной способностью. Критики указывают на то, что P2P-сети имеют законное использование, и что это еще один способ, которым крупные провайдеры пытаются контролировать использование и контент в Интернете, а также направлять людей к клиент-серверной архитектуре приложений. Модель клиент-сервер обеспечивает финансовые барьеры для входа для небольших издателей и частных лиц и может быть менее эффективной для совместного использования больших файлов. В качестве реакции на это ограничение пропускной способности несколько P2P-приложений начали реализовывать обфускацию протоколов, например шифрование протокола BitTorrent. Методы достижения «запутывания протоколов» включают

⁴ Orland, Kyle (September 26, 2017). "EU study finds piracy doesn't hurt game sales, may actually help". Ars Technica. Retrieved 2018-03-29.

удаление легко идентифицируемых свойств протоколов, таких как детерминированные последовательности байтов и размеры пакетов, путем придания данным вида случайности. Решением ISP для высокой пропускной способности является P2P-кэширование, где ISP хранит часть файлов, наиболее доступных клиентам P2P, чтобы сохранить доступ к интернету.

3.2. Будущее совместного использования файлов в одноранговых сетях

Судебные иски, связанные с авторским правом, не препятствуют развитию этой файлообменной платформы, но и делают ее более развитой, продолжая вносить изменения в систему для адаптации ситуации. Несмотря на юридические действия, особенно иск ассоциации звукозаписывающей индустрии Америки (RIAA) о закрытии Napster, форма обмена файлами не показала никаких признаков упадка - по крайней мере, в настоящее время.

3.2.1. Поставщик: уход в подполье

Вскоре после того, как RIAA начала уделять внимание файлообменным сервисам, «поставщики» быстро изменили способ их работы, наиболее распространенным из которых было «скрыть» информации о клиентах. Сами жесткие судебные иски против Napster или KaZaA побуждали файлообменные сервисы уходить в подполье и все труднее поддаваться контролю.

3.2.2. Нет места для поддельных файлов

В стремлении сохранить поддержку большинства пользователей и избежать из «заботы» со стороны звукозаписывающих компаний, проигрывателей записей, качество одноранговых приложений и сетей будет все больше улучшаться. В частности, механизм публичного скрининга поможет удалить поддельные, никчемные файлы или рекламное ПО (spyware), шпионские программы (spyware) с «рынка транзакций».

Инструменты оценки также будут интегрированы прямо на предоставляемых веб-сайтах. Пользователи имеют возможность объективно оценить размещенную информацию. После цикла сетевой администратор

находится под давлением «клиентов», чтобы устранить файлы низкого качества, постоянно находящиеся в нижней части таблицы.

Общий доступ к файлам также постоянно совершенствуется с помощью новых технологий для обмена файлами между одноранговыми сетями. Одна из самых обсуждаемых технологий-циклическая проверка избыточности (CRC). CRC проверяет, что пакеты отправляются как на стороне отправителя, так и на стороне получателя в одноранговых сетях. Помимо CRC, многие люди используют метод «gemailer» - отправляют информацию о своих запросах через посредников (прокси), поэтому их местонахождение легко скрыть. В будущем общие файлы также могут быть разделены на более мелкие пакеты, которые не могут быть идентифицированы (не отслеживаются), а затем автоматически «собраны» по прибытии.

3.2.3. Сократить разрыв

Ассоциация электронного фронта (EFF) выступает за легализацию обмена файлами через одноранговые сети. Среда, в которой художники получают вознаграждение от самой сети, предлагает, казалось бы, бесплатный сервис. Идея EFF заключается в том, чтобы «минимизировать потенциал обвинений, гарантируя, что пользователям разрешено хранить файлы в общих папках, устраняя все легко запутанные имена файлов». - с певицей или песней, принадлежащей RIAA.

Заключение

Нет никаких сомнений в том, что P2P-сети навсегда изменили интернет. С пиком в 2006 году, по оценкам, на P2P-сети приходится более 70% трафика во всем интернете. С тех пор использование этих сетей резко сократилось, главным образом из-за легкодоступных потоковых сервисов видео, таких как Netflix и YouTube, в сочетании с потоковыми музыкальными сервисами, такими как Spotify. P2P-сети заполнили важный пробел в истории Интернета, когда традиционные медиа-сервисы изо всех сил старались идти в ногу с потребностями пользователей.

Сегодня, с быстрым развитием информационных технологий, P2P не только развивается на компьютерах, но и сильно развивается на смартфонах и многих других типах интеллектуальных электронных устройств.

Архитектура P2P также является ключевым элементом многих технологий, особенно технологии блокчейн - основы криптовалют - технологии будущего, или протокола BitTorrent - платформы обмена файлами и широко используется многими пользователями в мире.

Список использованных источников

1. Peer-to-peer / Википедия - Электрон. дан. - Режим доступа: <https://en.wikipedia.org/wiki/Peer-to-peer> (Дата обращения: 14.06.2020)
2. Одноранговая сеть / Википедия - Электрон. дан. - Режим доступа: https://ru.wikipedia.org/wiki/%D0%9E%D0%B4%D0%BD%D0%BE%D1%80%D0%B0%D0%BD%D0%B3%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C (Дата обращения: 28.11.2019)
3. Одноранговая компьютерная сеть / Автор24 - © 2020 - Электрон. дан. – Режим доступа: https://spravochnick.ru/informacionnye_tehnologii/organizaciya_kompyuternyh_setey/odnorangovaya_kompyuternaya_set/
4. Пиринговые сети. Что такое Peer-to-peer? / ArtisMedia - Электрон. дан. - Режим доступа: <http://artismedia.by/blog/что-такое-peer-to-peer/> (Дата обращения: 11.09.2018)
5. P2P — Следующий этап развития информационных систем / Shiftstas - © 2006 – 2020 «ТМ» - Электрон. дан. - Режим доступа: <https://habr.com/ru/post/239225/> (Дата обращения: 06.10.2014)
6. Peer-to-Peer Networks Explained - Электрон. дан. - Режим доступа: <https://academy.binance.com/blockchain/peer-to-peer-networks-explained> (Дата обращения: 01.07.2020)
7. What Is a Peer-to-Peer Network? - © 2020 Indeed - Электрон. дан. - Режим доступа: <https://www.indeed.com/career-advice/career-development/what-is-a-peer-to-peer-network> (Дата обращения: 07.10.2019)
8. Peer-to-Peer (P2P) Service / JIM CHAPPELOW - Электрон. дан. - Режим доступа: <https://www.investopedia.com/terms/p/peertopeer-p2p-service.asp> (Дата обращения: 11.10.2019)
9. Peer-to-peer networks / Guillermo Escobero - © 2018 Teldat Group - Электрон. дан. - Режим доступа: <https://www.teldat.com/blog/en/peer-to-peer-network-blockchain-bitcoin/> (Дата обращения: 13.11.2019)

Приложения

Таблица 2

Сравнить систему Одноранговую сеть с клиент-серверной.

	Клиент-серверный	P2P
Характер	Централизованный сервер	Распределенный-децентрализованный
Основное	Существует определенный сервер и определенные клиенты, подключенные к серверу.	Клиенты и серверы не различимы; каждый узел действует как клиент и сервер.
Услуга	Клиент запрашивает услугу, и сервер отвечает на нее.	Каждый узел может запрашивать услуги и может также предоставлять услуги.
Сосредоточить	Делиться информацией.	Соединение между узлами сети
Данные	Данные хранятся на централизованном сервере.	Каждый узел имеет свои собственные данные.
Сервер	Когда несколько клиентов запрашивают услуги одновременно, сервер может быть перегружен.	Поскольку услуги, предоставляемые несколькими серверами, распределены в одноранговой системе, один сервер не перегружен.
Стоимость	Клиент-сервер дорог в реализации. (Требуется большая пропускная способность)	Недорог
Стабильность	Клиент-сервер является более стабильным и масштабируемым.	P2P страдает, если число коллег увеличивается в системе.