Предисловие

Сеть Lightning (Lightning Network, аббр. LN, или сеть-молния) – это второслойная одноранговая сеть, которая позволяет совершать платежи Bitcoin «вне цепи», то есть без фиксации их в качестве транзакций в блочной цепи (блокчейне) системы Bitcoin.

Сеть Lightning предоставляет безопасные, дешевые, быстрые и гораздо более приватные платежи Bitcoin, даже для очень малых платежей.

Основываясь на идее платежных каналов, впервые предложенной изобретателем системы Bitcoin Сатоши Накамото, сеть Lightning представляет собой маршрутизируемую сеть платежных каналов, в которой платежи делают «прыжки» вдоль пути платежных каналов от отправителя к получателю.

Первоначальная идея сети Lightning была предложена в 2015 году в новаторской статье Джозефа Пуна (Joseph Poon) и Тадеуша Дриджа (Thaddeus Dryja) «Сеть Lightning в рамках системы Bitcoin: масштабируемые мгновенные платежи вне цепи» (The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments). К 2017 году в интернете была запущена «тестовая» сеть Lightning, по мере того разные группы строили совместимые имплементации и координировали работу, чтобы установить какие-нибудь стандарты совместимости. В 2018 году сеть Lightning заработала, и потекли платежи.

В 2019 году Андреас М. Антонопулос, Олаолува Осунтокун и Рене Пикхардт согласились сотрудничать в написании этой книги. И похоже, мы добились успеха!

Целевая аудитория

Эта книга в основном предназначена для технически подкованных читателей, имеющих представление об основах системы Bitcoin и других открытых блочных цепей.

Условные обозначения в книге

В книге используются следующие типографические условные обозначения:

курсивный шрифт
: обозначает новые термины, URL-адреса, адреса электронной почты, имена файлов и расширения файлов;

`моноширинный шрифт`
: используется для листингов программ, а также внутри абзацев для ссылки на элементы программ, такие как переменные или имена функций, базы данных, типы данных, переменные среды, инструкции и ключевые слова;

`жирный моноширинный шрифт`
: показывает команды либо другой текст, который должен быть набран пользователем;

`моноширинный шрифт курсивом`
: показывает текст, который должен быть заменен значениями, передаваемыми пользователем, либо значениями, определяемыми по контексту.

Данный элемент обозначает подсказку или совет.

Данный элемент обозначает общее замечание.

Данный элемент обозначает предупреждение или предостережение.

Примеры исходного кода

Примеры проиллюстрированы на языках Go, C++, Python и с использованием командной строки Unix-подобной операционной системы. Все фрагменты исходного кода доступны в репозитории на GitHub в подкаталоге *code*. Сделайте ответвление исходного кода книги, попробуйте примеры кода или отправьте исправления через GitHub[1].

Все фрагменты исходного кода могут быть воспроизведены в большинстве операционных систем с минимальной инсталляцией компиляторов, интерпретаторов и библиотек для соответствующих языков.

Там, где это необходимо, мы предоставляем базовые инструкции по инсталляции и пошаговые примеры результата работы этих инструкций.

Некоторые фрагменты исходного кода и результаты его работы были переформатированы для печати. Во всех таких случаях строки были разделены символом обратной косой черты (\), за которым следует символ новой строки. При транскрибировании примеров удалите эти два символа и снова соедините строки, и вы должны увидеть результаты, идентичные тем, которые показаны в примере.

Во всех фрагментах исходного кода, там, где это возможно, используются реально существующие значения и вычисления, так что вы можете переходить

[1] См. https://github.com/lnbook/lnbook.

от примера к примеру и видеть одни и те же результаты в любом программном коде, который вы пишете для вычисления одних и тех же значений. Например, все приватные ключи и соответствующие им публичные ключи и адреса реально существуют.

Использование примеров исходного кода

Если у вас возникли технические вопросы или проблемы с использованием примеров исходного кода, то, пожалуйста, отправьте электронное письмо по адресу bookquestions@oreilly.com.

Ссылки на компании и продукты

Все ссылки на компании и продукты предназначены для образовательных, демонстрационных и справочных целей. Авторы не поддерживают ни одну из упомянутых компаний или продуктов. Мы не тестировали работу или безопасность ни одного из продуктов, проектов или сегментов исходного кода, показанных в этой книге. Используйте их на свой страх и риск!

Адреса и транзакции в этой книге

Адреса, транзакции, ключи, QR-коды и данные блочной цепи Bitcoin, используемые в этой книге, по большей части реальны. Это означает, что вы можете просматривать блочную цепь, просматривать предлагаемые в качестве примеров транзакции, извлекать их с помощью ваших собственных скриптов или программ и т. д.

Однако обратите внимание, что приватные ключи, использованные для создания адресов, напечатанных в этой книге, были «сожжены». Это означает, что если вы отправите деньги на любой из этих адресов, то деньги будут либо потеряны навсегда, либо (что более вероятно) присвоены, поскольку любой, кто читает книгу, может забрать их, используя напечатанные здесь приватные ключи.

НЕ ОТПРАВЛЯЙТЕ ДЕНЬГИ НИ НА ОДИН ИЗ АДРЕСОВ, УКАЗАННЫХ В ЭТОЙ КНИГЕ. Ваши деньги будут взяты другим читателем или потеряны навсегда.

Как с нами связаться

Информация о книге «Освоение сети Lightning», а также открытое издание и переводы доступны по адресу https://lnbook.info.

Об авторах

Андреас М. Антонопулос – автор бестселлеров, оратор, преподаватель и очень востребованный эксперт по системе Bitcoin и открытых технологий на основе блочных цепей. Он известен тем, что облегчает понимание сложных тем и подчеркивает как положительное, так и отрицательное воздействие, которое эти технологии могут оказывать на наши глобальные общества.

Андреас написал еще два технических бестселлера для программистов с O'Reilly Media, «Освоение системы Bitcoin» (Mastering Bitcoin) и «Освоение системы Ethereum» (Mastering Ethereum). Он также опубликовал серию книг «Интернет денег», в которых основное внимание уделяется социальному, политическому и экономическому значению и последствиям этих технологий. Андреас еженедельно выпускает бесплатный образовательный контент на своем канале YouTube и проводит виртуальные семинары на своем веб-сайте. Узнайте больше по адресу aantonop.com.

Олаолува Осунтокун является соучредителем и техническим директором компании Lightning Labs, а также ведущим разработчиком lnd, одной из главных имплементаций сети Lightning. Он получил степень бакалавра и магистра в области информатики в UCSB и в 2019 году был членом класса Forbes 30 для молодых специалистов до 30 лет. Во время учебы в аспирантуре он сосредоточился на прикладной криптографии, в частности на шифрованном поиске. Более пяти лет он активно участвовал в разработке системы Bitcoin и является автором нескольких предложений по совершенствованию системы Bitcoin (BIP-157 и 158). В наши дни его основное внимание сосредоточено на строительстве, конструировании и разработке частных масштабируемых автономных протоколов блочной цепи, таких как Lightning.

Рене Пикхардт – опытный математик и консультант по науке о данных, который использует свои статистические знания для проведения исследований с NTNU по отысканию путей, конфиденциальности, надежности платежей и соглашениям об уровне обслуживания в сети Lightning. Рене ведет технический и ориентированный на разработчиков канал YouTube[2] о сети Lightning и уже ответил примерно на половину вопросов о работе сети Lightning на бирже Bitcoin, что делает его одним из лучших консультантов для всех новых разработчиков, которые хотят присоединиться к этому пространству. Рене провел множество публичных и частных семинаров о сети Lightning, в том числе обучал студентов резидентуры Chaincode Labs 2019 года вместе с другими ключевыми разработчиками сети Lightning.

[2] См. https://www.youtube.com/renepickhardt.

Часть I

Понимание сети Lightning

Обзор сети Lightning, подходящий для всех, кто заинтересован в понимании базовых концепций и использовании сети Lightning.

Глава 1

Введение

Добро пожаловать в книгу «Освоение сети Lightning»!

Сеть Lightning (часто сокращенно LN от англ. Lightning Network) меняет способ обмена стоимостями в интернете, и это одно из самых захватывающих достижений в истории системы Bitcoin. Сегодня, в 2021 году, сеть Lightning все еще находится в зачаточном состоянии. Сеть Lightning – это протокол для использования системы Bitcoin разумным и неочевидным способом. Это технология, накладываемая вторым слоем поверх системы Bitcoin.

Концепция сети Lightning была предложена в 2015 году, а первая ее имплементация была запущена в 2018 году. Начиная с 2021 года мы только начинаем видеть возможности, которые сеть Lightning предоставляет системе Bitcoin, включая улучшенную конфиденциальность, скорость и масштабирование. Обладая базовыми знаниями о сети Lightning, вы поможете сформировать будущее данной сети, одновременно создавая возможности для себя.

Мы исходим из того, что у вас уже есть некоторые базовые знания о системе Bitcoin, но если нет, то не волнуйтесь – в приложении A мы объясним наиболее важные концепции системы Bitcoin, которые вы должны знать, чтобы понять сеть Lightning. Если вы хотите узнать о системе Bitcoin больше, то можете прочитать книгу Андреаса М. Антонопулоса «Освоение системы Bitcoin», 2-е издание (Andreas M. Antonopoulos, Mastering Bitcoin, 2nd edition, O'Reilly), доступную бесплатно онлайн[3].

Хотя большая часть данной книги написана для программистов, первые несколько глав написаны так, чтобы быть доступными любому, независимо от технического опыта. В этой главе мы начнем с некоторой терминологии, затем перейдем к рассмотрению концепции доверия и ее применения в этих системах и, наконец, обсудим историю и будущее сети Lightning. Давайте начнем.

Базовые понятия сети Lightning

Когда мы займемся разведывательным анализом того, как на самом деле работает сеть Lightning, то столкнемся с некоторой технической терминологией, которая поначалу может немного дезориентировать. Хотя все эти понятия и термины будут подробно объяснены по мере продвижения по книге и определены в глоссарии, ознакомление с несколькими базовыми определениями

[3] См. https://github.com/bitcoinbook/bitcoinbook.

сейчас облегчит понимание концепций в следующих двух главах. Если вы еще не понимаете всех слов в этих определениях, то не беда. Вы будете понимать все больше по мере продвижения по тексту.

Блочная цепь, блокчейн

Распределенный реестр транзакций, создаваемый сетью компьютеров. Bitcoin, например, – это система, которая создает блочную цепь. Сеть Lightning сама по себе не является блочной цепью и не создает блочную цепь. Это сеть, которая опирается на существующую внешнюю блочную цепь для обеспечения своей безопасности.

Цифровая подпись

Цифровая подпись – это математическая схема для верифицирования подлинности цифровых сообщений или документов. Валидная цифровая подпись дает получателю основание полагать, что сообщение было создано известным отправителем, что отправитель не может отрицать отправку сообщения и что сообщение не было изменено при передаче.

Хеш-функция

Криптографическая функция хеширования – это математический алгоритм, который соотносит данные произвольного размера с битовой строкой фиксированного размера (хешем) и предназначен для однопутной функции, то есть функции, которую невозможно инвертировать.

Узел

Компьютер, который участвует в сети. Узел Lightning – это компьютер, который участвует в сети Lightning. Узел Bitcoin – это компьютер, который участвует в сети Bitcoin. Обычно пользователь LN выполняет узел Lightning и узел Bitcoin.

Внутри цепи и вне цепи

Платеж происходит внутри цепи, если он зарегистрирован как транзакция в сети Bitcoin (или другой базовой) блочной цепи. Платежи, отправляемые по платежным каналам между узлами Lightning и которые не видны в базовой блочной цепи, называются платежами вне цепи. Обычно в сети Lightning единственными транзакциями внутри цепи являются транзакции, используемые для открытия и закрытия платежного канала Lightning. Существует третий тип транзакции, модифицирующий канал, именуемый склеиванием (splicing), который можно использовать для добавления/удаления суммы средств, зафиксированных в канале.

Платеж

Когда стоимость обменивается в сети Lightning, мы называем это «платежом» по сравнению с «транзакцией» в блочной цепи Bitcoin.

Платежный канал

Финансовая взаимосвязь между двумя узлами в сети Lightning, обычно имплементируемая с помощью мультиподписных Bitcoin-транзакций, которые имеют совместный контроль над биткойном между двумя узлами Lightning.

Маршрутизация по сравнению с отправкой

В отличие от системы Bitcoin, где транзакции «отправляются» путем их широковещательной передачи всем, Lightning – это маршрутизированная сеть, в которой платежи «маршрутизируются» по одному или нескольким платежным каналам по пути от отправителя к получателю.

Транзакция

Структура данных, которая регистрирует передачу контроля над некоторыми средствами (например, некоторыми биткойнами). Сеть Lightning опирается на транзакции Bitcoin (или транзакции другой блочной цепи) для осуществления контроля над средствами.

Более подробные определения этих и многих других терминов можно найти в глоссарии. На протяжении всей книги мы будем объяснять смысл этих терминов и то, как на самом деле работают данные технологии.

На протяжении всей этой книги вы будете встречать слово «Bitcoin» с заглавной первой буквой, которое относится к системе Bitcoin и является именем собственным. Вы также будете встречать слово «биткойн» со строчной буквой «б», которое относится к денежной единице. Каждый биткойн далее подразделяется на 100 миллионов единиц, каждая из которых называется «сатоши» (в единственном и множественном числе на русском пишется одинаково).

Теперь, когда вы знакомы с этими базовыми терминами, давайте перейдем к понятию, которое вам уже знакомо: доверие (trust).

Доверие в децентрализованных сетях

Вы часто будете слышать, как люди называют систему Bitcoin и сеть Lightning «бездоверительными» (trustless). На первый взгляд это сбивает с толку. В конце концов, разве доверие – это не хорошо? Банки даже используют его в своих названиях! Разве «бездоверительная» система, система, лишенная доверия, не является чем-то плохим?

Использование слова «бездоверительный» предназначено для того, чтобы передать идею способности работать, не нуждаясь в доверии к другим участникам системы. В такой децентрализованной системе, как Bitcoin, вы всегда можете заключить сделку с тем, кому доверяете. Однако система также гарантирует, что вас не обманут, даже если вы не можете доверять другой стороне транзакции. Доверие – это не обязательное, а приятное свойство системы.

Сравните это с традиционными системами, такими как банковское обслуживание, где вы должны доверять третьей стороне, поскольку она контролирует ваши деньги. Если банк нарушит ваше доверие, то вы можете обратиться в регулирующий орган или суд, но это потребует огромных затрат времени, денег и усилий.

Бездоверительность не означает отсутствие доверия. Она означает, что доверие не является необходимым условием для всех транзакций и что вы можете совершать транзакции даже с людьми, которым вы не доверяете, потому что система предотвращает обман.

Прежде чем мы перейдем к тому, как работает сеть Lightning, важно понять одну базовую концепцию, которая лежит в основе системы Bitcoin, сети Lightning и многих других подобных систем: то, что мы называем протоколом справедливости. Протокол справедливости – это способ достижения справедливых исходов между участниками, которым не нужно доверять друг другу, без необходимости в центральном органе власти, и он является основой децентрализованных систем, таких как Bitcoin.

Справедливость без центральной власти

Когда у людей есть конкурирующие интересы, то как они могут установить достаточное доверие, чтобы участвовать в каком-то совместном или транзакционном поведении? Ответ на этот вопрос лежит в основе нескольких научных и гуманистических дисциплин, таких как экономика, социология, поведенческая психология и математика. Некоторые из этих дисциплин дают нам «мягкие» ответы, которые зависят от таких понятий, как репутация, справедливость, мораль и даже религия. Другие дисциплины дают нам конкретные ответы, которые зависят только от допущения о том, что участники этих взаимодействий будут действовать рационально, руководствуясь своими личными интересами в качестве главной цели.

В общих чертах, существует несколько способов обеспечивать справедливые исходы во взаимодействии между людьми, которые могут иметь конкурирующие интересы:

Требовать доверия

Вы взаимодействуете только с теми людьми, которым уже доверяете, благодаря предыдущим взаимодействиям, репутации или семейным отношениям. Это достаточно хорошо работает в малых масштабах, в особенности в семьях и небольших группах, что является наиболее распространенной основой для кооперативного поведения. К сожалению, это не масштабируется и страдает от трайбалистского предубеждения (внутри группы).

Верховенство закона

Установить правила взаимодействия, которые будут соблюдаться учреждением. Это масштабируется лучше, но не может масштабироваться глобально из-за различий в обычаях и традициях, а также неспособности масштабировать институты правоприменения. Одним из неприятных побочных эффектов этого решения является то, что по мере своего роста институты становятся все более и более мощными, а это может привести к коррупции.

Доверенные третьи стороны

Поставить посредника в каждом взаимодействии, чтобы обеспечивать справедливость. В сочетании с «верховенством закона», обеспечивающим надзор за посредниками, это лучше масштабируется, но страдает от того же дисбаланса власти: посредники становятся очень влиятельными и могут привлечь коррупцию. Концентрация власти приводит к системному риску и системному провалу («слишком большой, чтобы позволить ему обанкротиться»).

Теоретико-игровые протоколы справедливости

Эта последняя категория возникает в результате сочетания интернета и криптографии и является предметом данного раздела. Давайте посмотрим, как она работает и в чем ее преимущества и недостатки.

Доверительные протоколы без посредников

Криптографические системы, такие как Bitcoin и сеть Lightning, – это системы, позволяющие совершать транзакции с людьми (и компьютерами), которым вы не доверяете. Такую работу часто называют «бездоверительной», хотя на самом деле она не является бездоверительной. Вы должны доверять выполняемому программному обеспечению и должны верить, что протокол, имплементированный этой программой, приведет к справедливым исходам.

Большое различие между подобного рода криптографической системой и традиционной финансовой системой заключается в том, что в традиционных финансах у вас есть доверенная третья сторона, например банк, для обеспечения справедливости исходов. Существенная проблема с такими системами заключается в том, что они передают слишком много власти третьей стороне, а также уязвимы перед единой точкой отказа. Если доверенная третья сторона сама нарушает доверие или пытается обмануть, то основание для доверия нарушается.

Изучая криптографические системы, вы заметите определенную закономерность: вместо того чтобы полагаться на доверенную третью сторону, эти системы пытаются предотвратить несправедливые исходы, используя систему положительных и отрицательных стимулов. В криптографических системах вы доверяете протоколу, фактически представляющему собой систему с набором правил, которые при правильной разработке будут правильно применять желаемые положительные и отрицательные стимулы. Преимущество такого подхода двоякое: вы не только избегаете доверия третьей стороне, но и уменьшаете необходимость обеспечения справедливых исходов. До тех пор, пока участники подчиняются согласованному протоколу и остаются в рамках системы, механизм стимулирования в этом протоколе обеспечивает справедливые исходы без контроля за его исполнением.

Использование положительных и отрицательных стимулов для достижения справедливых исходов является одним из аспектов раздела математики, именуемого теорией игр, предметом которого является изучение «моделей стратегического взаимодействия между лицами, принимающими рациональные решения»[4]. Криптографические системы, которые контролируют финансовые взаимодействия между участниками, такие как Bitcoin и сеть Lightning, в значительной степени опираются на теорию игр, чтобы предотвращать обман участников и позволять участникам, которые не доверяют друг другу, добиваться справедливых исходов.

Хотя теория игр и ее использование в криптографических системах на первый взгляд могут показаться запутанными и незнакомыми, скорее всего, вы уже знакомы с этими системами в своей повседневной жизни; вы просто еще

[4] Статья в Википедии (https://en.wikipedia.org/wiki/Game_theory), посвященная теории игр, содержит дополнительную информацию.

не узнаете их. В следующем далее разделе мы задействуем простой пример из детства, который поможет определить базовую закономерность. Как только вы поймете базовую закономерность, вы увидите ее повсюду в пространстве блочной цепи и научитесь распознавать ее быстро и интуитивно.

В этой книге мы называем эту закономерность протоколом справедливости, определяемым как процесс, в котором используется система положительных и/или отрицательных стимулов в целях обеспечения справедливых исходов для участников, которые не доверяют друг другу. Соблюдение протокола справедливости необходимо только для того, чтобы участники не могли избежать положительных или отрицательных стимулов.

Протокол справедливости в действии

Давайте рассмотрим пример протокола справедливости, с которым вы, возможно, уже знакомы.

Представьте себе семейный обед с родителем и двумя детьми. Дети привередливы в еде, и единственное, что они согласятся съесть, – это жареную картошку. Родитель приготовил чашу жареного картофеля («картофель фри» или «чипсы», в зависимости от того, какой английский диалект вы используете). Брат и сестра должны разделить между собой тарелку с чипсами. Родитель должен обеспечить справедливое распределение чипсов между каждым ребенком; в противном случае родителю придется выслушивать постоянные жалобы (возможно, весь день), и всегда есть вероятность того, что несправедливая ситуация перерастет в насилие. Что должен делать родитель?

В этом стратегическом взаимодействии между двумя детьми, которые не доверяют друг другу и имеют конкурирующие интересы, существует несколько разных способов достижения справедливости. Наивный, но часто используемый метод заключается в том, что родители используют свою власть в качестве доверенной третьей стороны: они делят миску с чипсами на две порции. Это похоже на традиционные финансы, где банк, бухгалтер или юрист выступают в качестве доверенной третьей стороны, чтобы предотвратить любой обман между двумя сторонами, которые хотят совершить сделку.

Проблема этого сценария заключается в том, что он возлагает большую власть и ответственность на доверенную третью сторону. В этом примере родитель несет полную ответственность за равное распределение чипсов, а стороны просто ждут, наблюдают и жалуются. Дети обвиняют родителей в том, что они занимают сторону любимчика и несправедливо распределяют чипсы. Они дерутся из-за чипсов, крича, что «этот чипс больше!», втягивая родителя в свою перепалку. Это звучит ужасно, не так ли? Должен ли родитель кричать громче? Убрать все чипсы? Угрожать никогда больше не делать чипсы и отправить детей из-за стола голодными?

Существует гораздо более оптимальное решение: детей учат играть в игру под названием «дели и выбирай». За каждым обедом один ребенок делит чашу чипсов на две порции, а *другой* выбирает ту порцию, которую он хочет. Почти сразу же дети начнут понимать динамику этой игры. Если один из них совершает ошибку или пытается обмануть, то другой может его «оштрафовать», выбрав чашу побольше. Играть честно – в интересах обоих детей, но в особенности того, кто делит чашу. В этом сценарии проигрывает только обманщик.

Родителю даже не нужно использовать свою власть или обеспечивать справедливость. Родителю лишь нужно *обеспечивать соблюдение протокола*; до тех пор, пока дети не смогут избежать назначенных им ролей «делющего» и «выбирающего», протокол сам по себе обеспечивает справедливый результат без необходимости какого-либо вмешательства. Родитель не может занимать сторону любимчика или искажать исход.

Хотя печально известные битвы за чипы 1980-х годов четко иллюстрируют эту точку зрения, любое сходство между описанным выше сценарием и реальным детским опытом любого из авторов со своими двоюродными братьями совершенно случаен … или нет?

Примитивы безопасности как строительные блоки

Для того чтобы подобный протокол справедливости работал, должны существовать определенные гарантии, или *примитивы безопасности*, которые можно комбинировать для обеспечения соблюдения. Первый примитив безопасности – это строгая *временная упорядоченность/последовательность*: действие «деление» должно происходить до действия «выбор». Это не сразу очевидно, но если вы не сможете гарантировать, что действие A произойдет до действия B, тогда протокол развалится. Второй элемент безопасности – это *обязательство без возможности отказа*. Каждый ребенок должен определиться со своим выбором роли: либо делющий, либо выбирающий. Кроме того, как только деление завершено, делющий привязан к созданному им делению – он не может отказаться от этого выбора и повторить попытку.

Криптографические системы предлагают ряд примитивов безопасности, которые могут объединяться разными способами для строительства протокола справедливости. В дополнение к упорядоченности и обязательству мы также можем использовать целый ряд других инструментов:

- хеш-функции для генерирования отпечатков данных как форма обязательства или как основа для цифровой подписи;
- цифровые подписи для аутентификации, неразглашения и подтверждения права собственности на секрет;
- шифрование/дешифрование для ограничения доступа к информации только авторизованным участникам.

Это лишь небольшой список целого «зверинца» используемых средств обеспечения безопасности и криптографии. Все время изобретаются более простые примитивы и комбинации.

В нашем примере из реальной жизни мы увидели одну из форм протокола справедливости под названием «дели и выбирай». Это всего лишь один из множества различных протоколов справедливости, которые могут быть построены путем комбинирования строительных блоков примитивов безопасности различными способами. Но базовая закономерность всегда одна и та же: два или более участника взаимодействуют, не доверяя друг другу, выполняя ряд шагов, которые являются частью согласованного протокола. Шаги протокола устанавливают положительные и отрицательные стимулы для обеспечения

того, чтобы, если участники рациональны, обман был контрпродуктивным, а справедливость – автоматическим исходом.

Контроль за соблюдением не является необходимым для получения справедливых исходов – он необходим только для того, чтобы участники не нарушали согласованный протокол.

Теперь, когда вы понимаете эту базовую закономерность, вы начнете видеть его повсюду в системе Bitcoin, сети Lightning и многих других системах. Давайте рассмотрим несколько конкретных примеров далее.

Пример протокола справедливости

Наиболее ярким примером протокола справедливости является консенсусный алгоритм системы Bitcoin под названием *Доказательство работы* (Proof of Work, аббр. PoW). В системе Bitcoin майнеры соревнуются за верификацию транзакций и их агрегирование в блоки. В целях обеспечения того, чтобы майнеры не обманывали без наделения их полномочиями, в Bitcoin используется подсистема положительных и отрицательных стимулов. Майнеры должны использовать электричество и выделять оборудование для выполнения «работы», которая встроена в качестве «доказательства» внутрь каждого блока. Это достигается благодаря свойству хеш-функций, при котором выходное значение случайно распределяется по всему диапазону возможных выходов. Если майнерам удается произвести валидный блок достаточно быстро, то они получают вознаграждение, зарабатывая блочное вознаграждение за этот блок. Принуждение майнеров использовать много электроэнергии до того, как сеть рассмотрит их блок, означает, что у них есть стимул правильно проверять транзакции в блоке. Если они обманывают или совершают какую-либо ошибку, то их блок отклоняется, и электричество, которое они использовали, чтобы «доказать» это, тратится впустую. Никому не нужно заставлять майнеров производить валидные блоки; вознаграждение и наказание стимулируют их к этому. Протоколу лишь нужно обеспечить, чтобы принимались только валидные блоки с доказательством работы.

Закономерность протокола справедливости также можно найти во многих разных аспектах сети Lightning:

- те, кто финансирует каналы, обеспечивают, чтобы у них была подписана транзакция возврата средств, прежде чем публиковать финансовую транзакцию;
- всякий раз, когда канал переводится в новое состояние, старое состояние «отзывается», обеспечивая, что если кто-либо попытается выполнить его широковещательную передачу, то он потеряет весь остаток средств и будет оштрафован;
- те, кто пересылают платежи, знают, что если они подтверждают/фиксируют пересылку средств вперед, то могут либо получить возврат, либо получить оплату от узла, предшествующего им.

Снова и снова мы видим эту закономерность. Соблюдение справедливых исходов не обеспечивается никакими органами власти. Они возникают как естественное следствие протокола, который поощряет справедливость и штрафует обман, протокола справедливости, в котором задействуются личные интересы, направляя их на справедливые исходы.

Система Bitcoin и сеть Lightning являются имплементациями протоколов справедливости. Тогда зачем нужна сеть Lightning? Разве системы Bitcoin недостаточно?

Мотивация для сети Lightning

Bitcoin – это система, которая регистрирует транзакции в глобально реплицируемом публичном реестре. Каждая транзакция видна, валидируется и хранится каждым участвующим компьютером. Как нетрудно себе представить, это генерирует большой объем данных, и его трудно масштабировать.

По мере роста системы Bitcoin и спроса на транзакции число транзакций в каждом блоке увеличивается, пока в конечном итоге не достигает предельного размера блока. Как только блоки «заполняются», избыточные транзакции остаются ждать в очереди. Многие пользователи будут увеличивать сумму комиссионных, которые они готовы платить, чтобы купить место для своих транзакций в следующем блоке.

Если спрос продолжает опережать емкость сети, то все большее число транзакций пользователей остаются неподтвержденными. Конкуренция за комиссионные также увеличивает стоимость каждой транзакции, делая многие транзакции с меньшей стоимостью (например, микротранзакции) совершенно неэкономичными в периоды особенно высокого спроса.

В целях решения этой проблемы мы могли бы увеличить лимит на размер блока, чтобы создать пространство для большего числа транзакций. Увеличение в «предложении» блочного пространства приведет к более низкому ценовому равновесию для транзакционных комиссий.

Однако увеличение размера блока перекладывает затраты на операторов узлов и требует, чтобы они тратили больше ресурсов на валидирование и хранение блочной цепи. Поскольку блочные цепи являются эпидемическими протоколами обмена сообщениями, каждый узел должен знать и валидировать каждую отдельную транзакцию, которая происходит в сети. Более того, после валидации каждая транзакция и блок должны быть распространены на «соседей» узла, умножая потребность в емкости. Таким образом, чем больше размер блока, тем выше потребность в емкости, обработке и хранении каждого отдельного узла. Увеличение емкости транзакций в таком ключе приводит к нежелательному эффекту централизации системы за счет сокращения числа узлов и операторов узлов. Поскольку операторы узлов не получают компенсации за работу узлов, если работа узлов обходится очень дорого, то только несколько хорошо финансируемых операторов узлов будут продолжать выполнять узлы.

Масштабирование блочных цепей

Как показывают несколько расчетов, побочные эффекты увеличения размера блока или уменьшения времени блока по отношению к централизации сети являются серьезными.

Предположим, что использование системы Bitcoin растет настолько, что сеть должна обрабатывать 40 000 транзакций в секунду, что является приблизительным уровнем транзакционной обработки сети Visa во время пиковой используемости.

Исходя из того, что на транзакцию в среднем приходится 250 байт, это приведет к потоку данных 10 мегабайт в секунду (МБ/с) или 80 мегабит в секунду (Мбит/с) только для того, чтобы иметь возможность получать все транзакции. Сюда не входят накладные расходы на трафик, связанные с пересылкой информации о транзакции другим одноранговым узлам. Хотя 10 МБ/с и не кажутся экстремальными в контексте высокоскоростных оптоволоконных и мобильных скоростей 5G, это фактически исключило бы любого, кто не может удовлетворить данное требование, из работающего узла, в особенности в странах, где высокопроизводительный интернет недоступен или недоступен широко.

У пользователей также есть много других требований к пропускной способности, и нельзя ожидать, что они будут тратить столько лишь на получение транзакций.

Более того, хранение этой информации локально привело бы к 864 гигабайтам в день. Это примерно один терабайт данных, или размер жесткого диска.

Верифицирование 40 000 подписей алгоритма цифровой подписи на основе эллиптической кривой (Elliptic Curve Digital Signature Algorithm, аббр. ECDSA) в секунду также едва выполнимо (см. соответствущу статью на StackExchange[5]), что делает скачивание начального блока (initial block download, аббр. IBD) блочной цепи Bitcoin (синхронизирование и верифицирование всего, начиная с генезисного (первичного) блока) практически невозможным без очень дорогого оборудования.

В то время как 40 000 транзакций в секунду кажутся большими, они достигают паритета с традиционными финансовыми платежными сетями только в пиковые моменты. Инновации в межмашинных платежах, микротранзакциях и других приложениях, скорее всего, повысят спрос на много порядков.

Проще говоря: масштабировать блочную цепь для валидирования транзакций по всему миру децентрализованным способом невозможно.

Но что, если бы каждый узел не был бы обязан знать и проверять каждую отдельную транзакцию? Что, если бы существовал способ удерживать масштабируемые транзакции вне цепи без потери безопасности сети Bitcoin?

В феврале 2015 года Джозеф Пун (Joseph Poon) и Тадеуш Дриджа (Thaddeus Dryja) предложили возможное решение проблемы масштабируемости системы Bitcoin, опубликовав работу под названием «Сеть Lightning в рамках системы Bitcoin: масштабируемые мгновенные платежи вне цепи» (The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments)[6].

В (ныне устаревшем) техническом документе Пун и Дриджа подсчитали, что для того, чтобы система Bitcoin достигла 47 000 транзакций в секунду, обрабатываемых системой Visa на пике, потребуется 8 ГБ блоков. Это сделало бы опе-

---

[5] См. https://bitcoin.stackexchange.com/questions/95339/how-many-bitcoin-transactions-can-be verified-per-second.

[6] *Джозеф Пун и Тадеуш Дриджа.* Сеть Lightning в рамках системы Bitcoin: масштабируемые мгновенные платежи вне цепи. ЧЕРНОВАЯ версия 0.5.9.2. 14 января 2016 года (Joseph Poon and Thaddeus Dryja. “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments”. DRAFT Version 0.5.9.2. January 14, 2016). https://lightning.network/lightning-network-paper.pdf.

рирование узлом совершенно неприемлемым для кого бы то ни было, кроме крупных предприятий и операций промышленного уровня. Результатом стала бы сеть, в которой только несколько пользователей могли бы фактически валидировать состояние реестра. Система Bitcoin опирается на то, что пользователи сами валидируют реестр, не доверяя третьим лицам в явной форме, чтобы оставаться децентрализованной. Взимание комиссии с пользователей за оперирование узлами вынудило бы среднестатистического пользователя доверять третьим сторонам, чтобы узнавать состояние реестра, что в конечном итоге нарушило бы доверительную модель в системе Bitcoin.

Сеть Lightning предлагает новую сеть, второй слой, где пользователи могут осуществлять платежи друг другу в одноранговом режиме без необходимости публикации транзакции в блочной цепи системы Bitcoin для каждого платежа. Пользователи могут платить друг другу в сети Lightning столько раз, сколько захотят, без создания дополнительных транзакций Bitcoin или взимания комиссии внутри цепи. Они используют блочную цепь системы Bitcoin только для первоначальной загрузки биткойна в сеть Lightning и для расчетов, то есть для удаления биткойна из сети Lightning. Как следствие гораздо больше платежей Bitcoin может происходить вне цепи, при этом только транзакции начальной загрузки и окончательного расчета должны валидироваться и храниться узлами Bitcoin. Помимо снижения нагрузки на узлы, платежи в сети Lightning дешевле для пользователей, потому что им не нужно платить комиссию за блочную цепь, и более приватны для пользователей, потому что они не публикуются для всех участников сети и, кроме того, не хранятся постоянно.

Хотя сеть Lightning изначально была задумана для системы Bitcoin, она может быть имплементирована в любой блочной цепи, которая отвечает некоторым базовым техническим требованиям. Другие блочные цепи, такие как Litecoin, уже поддерживают сеть Lightning. Кроме того, несколько других блочных цепей разрабатывают аналогичные второслойные решения, чтобы помочь им масштабироваться.

Определяющие признаки сети Lightning

Сеть Lightning – это сеть, которая работает как протокол второго слоя поверх системы Bitcoin и других блочных цепей. Сеть Lightning обеспечивает быстрые, безопасные, приватные, бездоверительные и не требующие разрешения платежи. Вот несколько признаков сети Lightning:

- пользователи сети Lightning могут маршрутизировать платежи друг другу по низкой цене и в реальном времени;
- пользователям, которые обмениваются стоимостями через сеть Lightning, не нужно ждать подтверждения блока для платежей;
- как только платеж в сети Lightning завершен, обычно в течение нескольких секунд он является окончательным и не может быть отменен. Как и транзакция в системе Bitcoin, платеж в сети Lightning может быть возвращен только получателем;
- в отличие от внутрицепных транзакций Bitcoin, которые передаются широковещательно и проверяются всеми узлами сети, платежи, маршрути-

зируемые в сети Lightning, передаются между парами узлов и не видны всем, что обеспечивает гораздо большую конфиденциальность;
- в отличие от транзакций в сети Bitcoin, платежи, маршрутизируемые в сети Lightning, не нуждаются в постоянном хранении. Таким образом, Lightning потребляет меньше ресурсов и, следовательно, дешевле. Это свойство также имеет преимущества для конфиденциальности;
- сеть Lightning использует луковичную маршрутизацию, аналогичную протоколу, используемому сетью Tor (от англ. The Onion Router, луковичный маршрутизатор), работающей на основе технологии обеспечения конфиденциальности, в результате чего даже участвующие в маршрутизации платежа узлы напрямую знают только о своем предшественнике и преемнике в маршруте платежа;
- при использовании поверх системы Bitcoin сеть Lightning использует настоящий биткойн, который всегда находится во владении (хранении) и полностью контролируется пользователем. Lightning – это не отдельный токен или монета, это действительно биткойн.

Примеры использования сети Lightning, пользователи и их истории

В целях более глубокого понимания того, как на самом деле работает сеть Lightning и почему люди ее используют, мы проследим за рядом пользователей и их историями.

В наших примерах некоторые люди уже систему Bitcoin использовали, а другие в ней абсолютные новички. Каждый человек и его приведенная ниже история иллюстрируют один или несколько конкретных вариантов применения. Мы будем возвращаться к ним на протяжении всей этой книги:

Потребитель

Алиса – пользователь системы Bitcoin, который хочет совершать быстрые, безопасные, дешевые и приватные платежи за небольшие розничные покупки. Она покупает кофе за биткойны, используя сеть Lightning.

Торговец

Боб владеет кафе «Кофейня Боба». Внутрицепные платежи Bitcoin не масштабируются для малых сумм, таких как чашка кофе, поэтому он использует сеть Lightning для приема платежей Bitcoin почти мгновенно и за низкие комиссионные.

Бизнес по предоставлению программно-информационных услуг

Чан – китайский предприниматель, который продает информационные услуги, связанные с сетью Lightning, а также системой Bitcoin и другими криптовалютами. Чан продает эти информационные услуги через интернет, осуществляя микроплатежи через сеть Lightning. Кроме того, Чан имплементировал службу поставщика ликвидности, которая арендует емкость входящего канала в сети Lightning, взимая небольшие комиссионные в биткойне за каждый период аренды.

Игрок

Дина – геймер-подросток из России. Она играет во много разных компьютерных игр, но ее любимые – это те, в которых есть «внутриигровая экономика», основанная на реальных деньгах. Играя в игры, она также зарабатывает деньги, приобретая и продавая виртуальные внутриигровые предметы. Сеть Lightning позволяет ей совершать небольшие сделки по внутриигровым предметам, а также зарабатывать небольшие суммы за выполнение квестов.

Вывод

В этой главе мы поговорили о фундаментальной концепции, которая лежит в основе как системы Bitcoin, так и сети Lightning: протоколе справедливости.

Мы рассмотрели историю сети Lightning и мотивы, лежащие в основе технических решений для масштабирования на втором слое для системы Bitcoin и других сетей, основанных на блочной цепи (блокчейне).

Мы изучили базовую терминологию, включая узел, платежный канал, транзакции внутри цепи и платежи вне цепи.

Наконец, мы познакомились с Алисой, Бобом, Чаном и Диной, за которыми будем следить на протяжении всей остальной части книги. В следующей главе мы встретимся с Алисой и рассмотрим ее мыслительный процесс, когда она выбирает кошелек Lightning и готовится совершить свой первый платеж Lightning, чтобы купить чашку кофе в кофейне Боба.

Глава 2

Приступаем к работе

В этой главе мы начнем с того, с чего начинает большинство людей, впервые сталкиваясь с сетью Lightning, – с выбора программного обеспечения для участия в экономике LN. Мы рассмотрим варианты выбора двух пользователей, которые представляют распространенный вариант использования сети Lightning, и будем учиться на примере. Алиса, посетительница кофейни, будет использовать кошелек Lightning на своем мобильном устройстве, чтобы купить кофе в кофейне Боба. Боб, торговец, будет использовать узел Lightning и кошелек для работы системы кассовых расчетов в своей кофейне, чтобы иметь возможность принимать платежи через сеть Lightning.

Первый кошелек Lightning Алисы

Алиса – давний пользователь системы Bitcoin. Впервые мы встретились с Алисой в главе 1 книги «Освоение системы Bitcoin»[7], когда она купила чашку кофе в кофейне Боба, используя транзакцию Bitcoin. Если вы еще незнакомы с тем, как работают транзакции Bitcoin, или нуждаетесь в освежении своих знаний, то, пожалуйста, ознакомьтесь с книгой «Освоение системы Bitcoin» или кратким описанием в приложении А.

Алиса узнала, что кофейня Боба недавно начала принимать платежи LN! Алисе не терпится узнать о сети Lightning и поэкспериментировать с ней; она хочет стать одним из первых клиентов LN Боба. Для этого Алиса сначала должна выбрать кошелек Lightning, который соответствует ее потребностям.

Алиса не хочет доверять хранение своего биткойна третьим лицам. Она узнала о криптовалюте уже достаточно, чтобы знать, как пользоваться кошельком. Ей также нужен мобильный кошелек, чтобы она могла использовать его для небольших платежей на ходу, поэтому она выбирает кошелек Eclair, популярный неопекаемый (некустодиальный)[8] мобильный кошелек Lightning. Давайте узнаем больше о том, как и почему она сделала этот выбор.

---

[7] *Андреас М. Антонопулос.* Освоение системы Bitcoin. 2-е изд., глава 1 (Andreas M. Antonopoulos, Mastering Bitcoin, 2nd Edition, Chapter 1, O'Reilly, https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch01.asciidoc).

[8] Неопекаемым, или некастодиальным (noncustodial), можно считать криптовалютный кошелек, сохраняющий за пользователем возможность полностью контролировать ключи и свои средства. К данной категории можно отнести аппаратные, мобильные, бумажные, настольные и веб-кошельки. – *Прим. перев.*

Узлы Lightning

Доступ к сети Lightning осуществляется посредством программных приложений, которые могут обмениваться данными по протоколу LN. Узел сети Lightning (узел LN или просто узел) – это программное приложение, обладающее тремя важными характеристиками. Во-первых, узлы Lightning являются кошельками, поэтому они отправляют и получают платежи через сеть Lightning, а также в сети Bitcoin. Во-вторых, узлы должны взаимодействовать на одноранговой основе с другими узлами Lightning, создавая сеть. Наконец, узлам Lightning также необходим доступ к блочной цепи Bitcoin (или другим блочным цепям для других криптовалют) с целью защиты средств, используемых для платежей.

Пользователи имеют наивысшую степень контроля, управляя своим собственным узлом Bitcoin и узлом Lightning. Однако узлы Lightning также могут использовать облегченный клиент Bitcoin, обычно именуемый упрощенной верификацией платежей (simplified payment verification, аббр. SPV), в целях взаимодействия с блочной цепью Bitcoin.

Проводники Lightning

Проводники LN – это полезные инструменты для показа статистики узлов, каналов и емкости сети.

Ниже приведен неисчерпывающий список:

- проводник 1ML[9] по сети Lightning;
- проводник ACINQ[10] по сети Lightning с причудливой визуализацией;
- проводник Amboss Space[11] по сети Lightning с метриками сообщества и интуитивно понятными визуализациями;
- проводник Fiatjaf[12] по сети Lightning с многочисленными диаграммами;
- проводник hashXP[13] по сети Lightning.

[9] См. https://1ml.com/.

[10] См. https://explorer.acinq.co/.

[11] См. https://amboss.space/.

[12] См. https://ln.bigsun.xyz/.

[13] См. https://hashxp.org/lightning/node.