Сеть Conflux:

Разработка и экономическое проектирование

Андреас Парк [1,2] и Андреас Венерис [1,3,4]

[1] Советник Фонда Conux

[2] Школа менеджмента Ротмана, Университет Торонто

[3] Кафедра электротехники и вычислительной техники, Университет Торонто

[4] Кафедра компьютерных наук, Университет Торонто

andreas.park@rotman.utoronto.ca , veneris@eecg.toronto.edu

Абстрактный

Распределенные реестры или блокчейны, в частности те, которые основаны на протоколах Proof-of-Work (PoW), полагаются как на экономические механизмы, так и на технологии. В этой статье мы описываем, как мы подходим к проектированию экономических механизмов, которые подчеркивают Conflow, блокчейн PoW с высокой пропускной способностью и производительностью, предоставляя подробный анализ его экономической жизнеспособности. Conflow предлагает несколько нововведений по сравнению с хорошо изученными блокчейн-сетями, такими как Биткойн и Эфириум, как с точки зрения дизайна технологии, так и с точки зрения экономики, лежащей в основе технологии. В частности, основное отличие Conflow от существующего положения состоит в том, что обработка блоков происходит параллельно, а не последовательно, и пользователи, которые передают код или информацию в блокчейн, сталкиваются с постоянными затратами и / или выгодами в течение всего времени, в течение которого они занимают цепочку. Космос. Следовательно,

УВЕДОМЛЕНИЕ

НИЧТО В ЭТОЙ БЛОКЕ НЕ ЯВЛЯЕТСЯ ЮРИДИЧЕСКИМИ, ФИНАНСОВЫМИ, ДЕЛОВЫМИ ИЛИ НАЛОГОВЫМИ КОНСУЛЬТАЦИЯМИ, И ВЫ ДОЛЖНЫ КОНСУЛЬТИРОВАТЬСЯ С СОБСТВЕННЫМ ЮРИДИЧЕСКИМ, ФИНАНСОВЫМ, НАЛОГОВЫМ ИЛИ ДРУГИМ ПРОФЕССИОНАЛЬНЫМ КОНСУЛЬТАНТОМ, ПРЕЖДЕ ЧЕМ УЧАСТВОВАТЬ В ЛЮБОЙ ДЕЯТЕЛЬНОСТИ, СВЯЗАННОЙ С НЕЙ. НИ КОМПАНИЯ CONFLUX FOUN- DATION LTD. (CONFLUX), ЛЮБОЙ ИЗ ЧЛЕНОВ КОМАНДЫ ПРОЕКТА, КОТОРЫЕ РАБОТАЛИ НА ПЛАТФОРМЕ CONFLUX ИЛИ ПРОЕКТЕ ЛЮБОЙ СПОСОБ (КОМАНДА CONFLUX), И НИ ЛЮБОЙ ПРЕДСТАВИТЕЛЬ СТОРОННИХ СЕРВИСОВ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ ПРАВИЛЬНЫЕ ИЛИ НЕПОСРЕДСТВЕННЫЕ УЩЕРБЫ ИЛИ УБЫТКИ, КОТОРЫЕ ВЫ МОЖЕТЕ СТАТЬ В СВЯЗИ С ДОСТУПОМ К ЭТОЙ БЕЗОПАСНОСТИ, МАТЕРИАЛАМ, ПРОИЗВЕДЕННЫМ CONFLUX, ИЛИ ДОСТУПОМ НА ЭТОЙ ВЕБ-САЙТ НА [HTTPS: //WWW.CONFLUX- CHAIN.ORG/] ИЛИ ЛЮБЫМИ ДРУГИМИ МАТЕРИАЛАМИ, ОПУБЛИКОВАННЫМИ CONFLUX. Conflux и команда Conflux не делают и не претендуют на то, чтобы делать и настоящим отказываются от любых заявлений, гарантии или обязательства перед любым юридическим или физическим лицом. Все заявления, содержащиеся в этом техническом документе, заявления, сделанные в пресс-релизах или в любом месте, доступном для общественности, и устные заявления, которые могут быть сделаны Conflux и / или командой Conflux, могут представлять собой прогнозные заявления (включая заявления относительно намерений, убеждений или текущие ожидания в отношении рыночных условий, бизнес-стратегии и планов, финансового состояния, конкретных положений и практики управления рисками). Вас предупреждают, что не следует чрезмерно полагаться на эти прогнозные заявления, учитывая, что эти заявления связаны с известными и неизвестными рисками, неопределенностями и другими факторами, которые могут привести к тому, что фактические будущие результаты будут существенно отличаться от тех, которые описаны в таких прогнозных заявлениях. Эти прогнозные заявления применимы только на дату выпуска этого технического документа, а Conflux и команда Conflux прямо отказываются от какой-либо ответственности (явной или подразумеваемой) за публикацию любых изменений этих прогнозных заявлений для отражения событий после такой даты. . Вы понимаете, что Проект, а также создание и распространение Токенов связаны со значительными рисками, включая, помимо прочего, риск того, что (i) технология, связанная с Проектом Conflux, может не работать должным образом; (ii) Проект Conflow может не вызвать интереса или принятия со стороны основных заинтересованных сторон или более широкого сообщества; (iii) отсутствие гарантий того, что цена за Токен, определенная рынком, будет равна или выше.

Введение

Когда НАСА готовилось к полету в космос, они потратили миллионы на разработку шариковой ручки, чтобы астронавты могли писать в невесомости. Столкнувшись с той же проблемой, Советский Союз использовал карандаши. Этот анекдот вкратце представляет собой философию Conflux: его главная цель - взять лучшие части существующих блокчейнов без прав доступа и значительно расширить эти границы.

Что такое Conflux? Вкратце, это сеть блокчейнов Proof-of-Work (PoW), которая позволяет параллельную обработку блоков и транзакций, в конечном итоге формируя окончательную последовательную цепочку. Эта функция контрастирует с другими известными сетями, такими как Биткойн и Эфириум, в которых блоки обрабатываются строго один за другим. [1] Параллельная обработка создает экономические стимулы для майнеров, которые заметно отличаются от последовательных цепочек, и в этой статье мы обсуждаем, как эти различия повышают безопасность и экономическую жизнеспособность против атак с двойным расходом.

Conflux также стремится решить проблему неоплачиваемого занятия пространства смарт-контрактами. В Ethereum при введении нового контракта пользователь просто платит во время включения кода в цепочку, тогда как сообщество в целом несет бремя сохранения контракта в хранилище. Conflux вводит текущие затраты на обслуживание контрактов, что дает пользователям экономический стимул избегать растраты ресурсов.

Чтобы обеспечить внутреннюю ценность, Con ux стремится привлечь пользователей, которые активно используют сеть для предоставления дополнительных услуг. Конфлукс считает крайне важным, чтобы не было препятствий для входа тех, кто вносит значимый вклад. Вот почему Conflux - это сеть, не требующая разрешения, с экономическими механизмами управления, которые стимулируют сообщество.

[1] Ethereum допускает ограниченное количество так называемых «дядя-блоков» для более быстрой обработки, но настройка Ethereum по своей сути не параллельна.

взносы для обеспечения безопасной, стабильной и предсказуемой среды для коммерческой деятельности.

В этом документе обсуждаются несколько аспектов сети Conflux, в которых задействованы экономические механизмы. Эти механизмы влияют на затраты и вознаграждения пользователей и майнеров и, следовательно, на их поведение, поэтому очень важно планировать заранее, чтобы избежать непредвиденных последствий. Этот документ является сопроводительным документом к технической рукописи Conflux. Он дополняет инженерные аспекты, фокусируясь на микро- и макроэкономических механизмах базовой системы.

По своей сути технология блокчейн - это инфраструктурное решение, которое позволяет *(я)* передача экономической стоимости и (*II)* выполнение программного состояния / хранилища без доверенной третьей стороны. Чтобы добиться успеха в этой области, необходимо сбалансировать несколько основных факторов.

Во-первых, передача экономической стоимости и оплата стоимости такого использования полагаются на собственный токен. Этот токен должен быть спроектирован так, чтобы он служил средством обмена, но также и расчетной единицей для данных на основе блокчейна. Также желательно, чтобы токен можно было использовать в качестве средства сбережения, чтобы он мог поддерживать долгосрочные стимулы для различных сторон использовать цепочку. Наконец, как и в случае с сетями PoW, собственный токен играет роль в компенсации майнеров сети, которые играют центральную роль в работе и безопасности сети. К настоящему времени существует ряд статей, в которых подчеркивается, как собственные токены могут стимулировать внедрение и использование сети. [2] и мы опираемся на эту литературу в нашем анализе.

В этом документе мы описываем распределение токенов, а также правила использования и экономическое влияние различных правил. А именно, токены выпускаются при возникновении в качестве процентных платежей по подмножествам токенов, которые удовлетворяют определенным правилам, и в качестве вознаграждения для

[2] См., Например, Бакос и Халабурда (2018), Конг, Ли и Ван (2018), Фиш (2019), Канидио (2018) или Ли и Манн (2018)).

майнеры, которые включают новые блоки. Затем мы предоставляем откалиброванную модель, которая имитирует ожидаемый доход майнеров. Токены взаимодействуют с внешним миром в том смысле, что существует обменный курс для обмена валют (а также с другими криптовалютами), и поэтому мы также тщательно обсуждаем, как выпуск токенов влияет на обменные курсы.

В заключительной части статьи мы предлагаем два формальных анализа, чтобы лучше понять экономику Конфлюса. Во-первых, есть несколько хорошо известных ограничений на защиту от двойной траты для блокчейнов PoW.[3] и мы подчеркиваем, как Conflux Network расширяет набор экономически жизнеспособных состояний по сравнению с известными сетями. Во-вторых, мы предлагаем формальную модель равновесия взаимодействия пользователей и майнеров, чтобы изучить, как изменения в переменных политики влияют на результаты равновесия.

II. Краеугольные камни существующего мира блокчейнов

Прежде чем представить предлагаемую экономическую систему, мы рассмотрим ключевые концепции из основных существующих моделей блокчейнов.

Биткойн это первая рабочая криптовалюта, решившая проблему двойных расходов. По своей сути, блокчейн Биткойн - это пони с одним трюком, который предназначен для передачи своего собственного токена, биткойнов. Концептуально он задуман как медленный, поскольку блоки фиксированного размера производятся серийно с примерно постоянной скоростью, равной одному блоку, который может содержать только около 3, 500 транзакций, за 10 минут. Хотя для хорошей уверенности в том, что передача значения действительно произошла, недостаточно, чтобы транзакция была включена в блок. Причина в том, что блок может быть не частью самой длинной цепочки, а частью вилки. Это может произойти, например, когда два блока создаются примерно в одно и то же время - только один из них в конечном итоге станет частью самого длинного

[3] См. Chiu and Koeppl (2017) и Budish (2018).

цепь. Следовательно, необходимо дождаться нескольких подтверждений блока, прежде чем транзакцию можно будет считать окончательной. Эта установка со временем формирования блока 10 минут и еще большим временем подтверждения явно не подходит для повседневных платежей. У Биткойна есть и другие ограничения: после того, как все биткойны были добыты с помощью вознаграждений за блоки, майнеры получают только определяемую пользователем комиссию за транзакции для защиты сети. Если мы возьмем текущий доход майнеров в качестве ориентира, эти комиссии должны быть довольно большими: при текущем вознаграждении за блок в размере 6,25 BTC за блок и цене BTC около 10 000 долларов США (на момент публикации) *каждый* из 3 500 транзакций, которые помещаются в блок, необходимо заплатить комиссию в размере около 18 долларов. Все эти функции делают Биткойн непригодным для денежных переводов и, вероятно, слишком дорогим, чтобы быть альтернативной платежной сетью для большинства бизнес-транзакций (Auer 2019).

Однако основными участниками сети Биткойн являются майнеры, краткосрочные спекулянты и долгосрочные держатели. Очень немногие участники сети используют Биткойн по прямому назначению, как «одноранговые электронные деньги». В будущем долгосрочные держатели должны будут полагаться на краткосрочных спекулянтов для создания достаточных транзакций, чтобы майнеры были готовы продолжать обеспечивать безопасность сети. Скорее всего, это станет проблемой в будущем. Другими словами, в нынешнем виде сеть Биткойн сегодня не стимулирует пользователей токена к значимой и приносящей ценность экономической деятельности. Кроме того, технологическая инфраструктура Биткойна имеет ограничения и позволяет немногое, кроме передачи Биткойн. Без полных по Тьюрингу сценариев Разработчики децентрализованных приложений (dApp) имеют для них самое большее периферийное использование за счет внедрения «боковых цепочек», таких как Lightning Network и т. д. Управление также является проблемой. Изменения в протоколе Биткойн требуют согласия майнеров. Это может быть сложно, если эти изменения могут

отрицательно сказывается на доходах майнеров - даже если само изменение хорошо служит более широкой экосистеме.

В *Сеть Ethereum* - это значительно улучшенная система по сравнению с Биткойн, в которой реализована полная по Тьюрингу функция смарт-контрактов, которая позволяет разработчикам кодировать dApps, работающие в сети. Язык смарт-контрактов Ethereum позволяет создавать токены, которые можно использовать как неродные платежные монеты или даже как ценные бумаги. Собственный токен Ethereum Ether не имеет жесткого ограничения на предложение токенов и, следовательно, может расти органически по мере расширения использования сети и увеличения спроса на токены. Управление Ethereum следует тому же механизму, что и Биткойн, с некоторыми улучшениями: майнеры не только получают вознаграждение за каждый созданный блок, но и собирают комиссию за транзакцию за выполнение кода. Следовательно, более сложные транзакции или операции вознаграждаются более высокими комиссиями.

Однако, как и в случае с биткойном, Ethereum также страдает от низкой пропускной способности транзакций: в настоящее время сеть может обрабатывать не более 40 транзакций в секунду. Это далеко не уровень потребности в современной коммерческой финансовой инфраструктуре. Например, Payments Canada обрабатывает около 28 миллионов транзакций в средний рабочий день, в то время как экономика Канады занимает только первое место. 10 th по номинальному ВВП (раз 2019). Предполагая, что большая часть действий происходит более 12 часов в день, платежной сети блокчейн для обработки этого уровня транзакций потребуется примерно минимальная пропускная способность 650 транзакций в секунду (транзакций в секунду). Кроме того, также невозможно использовать блокчейн Ethereum в качестве альтернативной инфраструктуры для торговли ценными бумагами: традиционные централизованные биржи ценных бумаг и внебиржевые рынки ценных бумаг по всему миру обрабатывают миллиарды заказов и транзакций в день. На самом деле, хотя в сети Ethereum есть много децентрализованных бирж, на

при нынешних показателях пропускной способности они принципиально не в состоянии удовлетворить значительную часть сегодняшней деятельности финансового рынка.

Вторая функциональная проблема Ethereum заключается в том, что пользователи платят за контракт только во время включения кода контракта. Кроме того, единовременное вознаграждение получает только майнер, включивший этот код в цепочку. Тем не менее, каждый новый контракт, представленный в цепочку Ethereum, не только требует, чтобы сеть выполняла код, он также занимает «пространство цепочки» (*т.е.* память в глобальном состоянии цепочки Ethereum), даже если она остается неактивной после отправки. Таким образом, все полные узлы сети должны впоследствии хранить информацию, что приводит к ситуации, когда пользователи могут хранить данные в цепочке с единовременной платой за включение, в то время как хранение таких данных может длиться бесконечно долго без необходимости оплаты обслуживания. . Таким образом, сегодня подавляющая часть пространства дерева состояний Ethereum занята неактивными смарт-контрактами. Эти неиспользуемые данные тратят пространство в дереве состояний блокчейна, замедляют работу системы и создают нежелательные задержки / накладные расходы сети.

Одна из целей проекта Conflux состоит в том, чтобы развить и значительно улучшить возможности существующих систем блокчейнов: гарантированное выполнение программного кода через полную по Тьюрингу виртуальную машину на не требующем разрешения механизме консенсуса с более высокой производительностью без ущерба для безопасности и децентрализации .

III. Обзор сети Conflow

Con ux - это новая сеть PoW с полным по Тьюрингу языком смарт-контрактов, аналогичным Ethereum. [4] Сеть Conflow обеспечивает значительное повышение производительности за счет обработки параллельных блоков в направленном ациклическом графе (DAG).

[4] См. Li, Li, Zhou, Xu, Long, and Yao (2018) и.

структура, которая сокращает время подтверждения и существенно увеличивает пропускную способность транзакций.

Чтобы решить проблему перегрузки пространства, Conflow требует, чтобы пользователи связали собственные токены с хранилищем, чтобы они занимали пространство, что неявно создает препятствия для ненужного занятия пространства. Сдерживающее действие возникает из-за выплаты процентов по существующим токенам в системе. Проценты на связанное хранилище выплачиваются майнерам, а не пользователям, чтобы обеспечить майнерам долгосрочный доход. Чтобы решить проблему атаки на справедливость, Conflux назначает вознаграждение за блок таким образом, чтобы исключить характерную черту майнинга «победитель получает все». Вместо того, чтобы соревноваться за самую длинную цепочку, майнеры в Conflow получают вознаграждение за все блоки, которые они генерируют, хотя и с некоторыми механизмами штрафов, которые поощряют соблюдение протокола консенсуса.

Подобно Ethereum, Confux работает с моделью на основе учетной записи, которая связана с балансом каждой обычной учетной записи, а каждая учетная запись смарт-контракта содержит соответствующие байтовые коды, а также внутреннее состояние. Conflux поддерживает модифицированную версию Solidity (основной язык контрактов в Ethereum) и виртуальную машину Ethereum (EVM) для своих смарт-контрактов, так что смарт-контракты из Ethereum могут легко мигрировать в Conflux.

Транзакция в Conflow относится к сообщению, которое инициирует платежную транзакцию или развертывает / выполняет код смарт-контракта. Каждый блок состоит из списка транзакций, которые проверяет предлагающий майнер. Каждый узел поддерживает пул подтвержденных полученных транзакций, которые еще не были включены в блок. Майнеры соревнуются друг с другом, решая головоломки PoW, чтобы объединить транзакции в блоки. Подобно Биткойну и

Ethereum, Conflow регулирует сложность PoW, чтобы поддерживать стабильную скорость генерации блоков. Каждый узел также поддерживает локальное состояние, созданное из полученных блоков.

Алгоритм консенсуса Conflow работает со специальной структурой направленного ациклического графа (DAG), называемой TreeGraph. В отличие от Ethereum, который принимает транзакции только в одной цепочке в свою бухгалтерскую книгу, алгоритм консенсуса Conflow безопасно включает и обрабатывает транзакции во всех параллельных блоках. Между блоками есть два вида ребер: *родитель* края и *ссылка* края. Каждый блок (кроме генезиса) в TreeGraph имеет ровно одно родительское ребро по отношению к выбранному родительскому блоку. Каждый блок также может иметь несколько ссылочных ребер для ссылки на предыдущие блоки. Все родительские ребра образуют дерево, встроенное в направленный ациклический граф (DAG) всех ребер.

На высоком уровне Conflux использует новый алгоритм Greedy Heaviest Adaptive SubTree (GHAST) (Li and Yang (2020)), который присваивает вес каждому блоку в соответствии с топологиями в TreeGraph. При таком присвоении веса существует детерминированно самая тяжелая цепочка в графе, называемая *поворотная цепь,* что соответствует относительно наиболее стабильной цепи от зарождения до вершины родительского дерева.

Родительские ребра, опорные ребра и сводная цепочка вместе позволяют Con ux разбивать все блоки в DAG на *эпох.* Как показано на рисунке 1, каждый блок в цепочке поворота соответствует одной эпохе. Каждая эпоха содержит все блоки, которые достижимы из соответствующего блока в цепочке поворота через комбинацию родительских ребер и опорных ребер и которые не включены в предыдущие эпохи. Подробности об алгоритме консенсуса можно найти в (Li and Yang (2020)).

Экспериментальные результаты показали, что Conflux способен обрабатывать 4 000 транзакций в секунду для простых платежных транзакций, пропускная способность как минимум на два порядка выше, чем у Ethereum и Bitcoin. Повышение пропускной способности - это

результат структуры TreeGraph и алгоритма консенсуса, так что сеть может работать с гораздо более высокой скоростью генерации блоков, без отбрасывания вилок и с более высоким использованием пространства блоков. Согласно технической спецификации, основная сеть Conflow будет работать с фиксированной скоростью генерации блоков - два блока в секунду. Таким образом, дневная скорость генерации блоков составляет $60 \cdot 60 \cdot 24 \times 2 = 172,800$ блоков в сутки.

IV. Правила токена

В сети Conflow есть уникальный собственный токен, далее именуемый *CFX.*
Каждый CFX содержит 10_{18} *Капать.* Транзакции в Conflow обрабатываются аналогично транзакциям в сети Ethereum, и поэтому CFX играет ту же роль, что и Ether. А именно, пользователи отправляют транскацию с лимитом газа и ценой на газ; последний деноминирован в CFX.

В *Фонд Confux* - это некоммерческая организация, созданная Conflux для внесения корректировок, когда распределение ресурсов отклоняется от равновесия, для создания стимулов для преодоления проблемы холодного старта и для содействия участию / развитию сети на ранней стадии.

A. Жетоны Genesis

Первоначальное количество токенов - 5 000 000 000 (5 миллиардов). Все эти токены заблокированы при запуске основной сети, а затем будут выпускаться постепенно, с ежемесячными интервалами. Эти первоначальные токены будут разделены между следующими сторонами:

1. Основная команда

- *Частные инвесторы:* Нашим частным инвесторам будет выделено до 600 миллионов CFX. В последнем инвестиционном раунде токены CFX продаются по цене 0,1 доллара США за CFX. См. Раздел IV.B. для временной шкалы разблокировки этих жетонов. На момент написания этой статьи инвесторам уже продано более 520 миллионов CFX в этой категории. Непроданные токены в этой категории при запуске Con Conux будут выделены как Foundation Holdings.

- *Фондовые холдинги:* 200 миллионов CFX плюс любые непроданные CFX из предыдущей категории будут выделены для поддержки долгосрочных финансовых потребностей Conflux Foundation. Эти токены будут разблокироваться ежемесячно в течение 2 лет.

- *Команда Genesis:* 1800 миллионов CFX будут переданы команде основателей, включая команду IIIS (из Университета Цинхуа) и акционеров Alt-Chain Technologies (откуда Conflux выделили), сотрудников Conflux Foundation и консультантов. Жетоны команды Genesis будут разблокированы в течение 4 лет.

2. Строительство сообществ и экосистем

- *Фонд сообщества:* 400 миллионов CFX будут использованы для маркетинга и построения сообщества. Эти токены будут разблокированы в течение 4 лет.

- *Экосистемный фонд:* 2000 миллионов CFX из Genesis Issue станут фондом экосистемы для решения проблем холодного запуска и инвестирования в перспективные проекты dApp, которые работают в сети Conflux. Эти токены будут разблокированы в течение 4 лет.

Б. Правила разблокировки токенов инвестора

Выделенные частным инвесторам токены CFX будут разблокироваться ежемесячно в течение двух лет после запуска Confux. Основываясь на рыночной спотовой цене CFX, токены инвесторов могут быть разблокированы заранее, чтобы обеспечить ликвидность на рынке CFX в условиях нестабильности цен. Правила предварительной разблокировки следующие.

1. Если средняя рыночная спотовая цена CFX за последние пять дней превышает 0,6 Долларов США, при

   с одобрения Con Conux Foundation, все частные инвесторы могут получить токены CFX, которые должны быть разблокированы в первую очередь. *два* месяцев после запуска Conflux.

2. Если средняя рыночная спотовая цена CFX за последние пять дней превышает 0,8 Долларов США, при

   с одобрения Con Conux Foundation, все частные инвесторы могут получить токены CFX, которые должны быть разблокированы в первую очередь. *четыре* месяцев после запуска (т. е. на два дополнительных месяца вперед сверх предыдущего правила).

3. Если средняя рыночная спотовая цена CFX за последние пять дней превышает 1.0 Долларов США, при

   с одобрения Con Conux Foundation, все частные инвесторы могут получить токены CFX, которые должны быть разблокированы в первую очередь. *шесть* месяцев после запуска.

4. Если средняя рыночная спотовая цена CFX за последние пять дней превышает 1.2 Долларов США, при

   По утверждению Confux Foundation, все частные инвесторы могут получить токены CFX, которые должны быть разблокированы в первую очередь. *8* месяцев после запуска.

5. Если средняя рыночная спотовая цена CFX за последние пять дней превышает 1.5 Долларов США, при

   По утверждению Confux Foundation, все частные инвесторы могут получить токены CFX, которые должны быть разблокированы в первую очередь. *десять* месяцев после запуска.

C. Формы токенов

Выпущенные токены существуют в двух формах: ликвидные и неликвидные. В жидкой форме они могут быть немедленно переданы / использованы в сети Conflux. Также есть три способа заблокировать токены, что делает их неликвидными. Неликвидные токены не подлежат передаче. Блокировка может принимать три различных формы.

1. Токены можно ставить, чтобы заинтересовать пользователей.

2. Их можно разместить в связанном хранилище для приобретения места в сети (например, для запуска dApps).

3. Их можно заблокировать на заранее определенный период времени, чтобы купить голоса в управлении сетью.

D. Выплаты процентов / сеньоража

Сеть будет распределять проценты по всем неликвидным токенам по фиксированной ставке. Держатели токенов получают этот процент только в том случае, если они ставят свои токены (т. Е. Переводят их в неликвидное состояние). Проценты будут добавлены к авуарам пользователя в то время, когда пользователь снимает ставку с токена и переводит его в жидкое состояние.

Основываясь на тестах производительности из тестовой сети, Conflux создает два блока каждую секунду, так что примерно 63 072 000 блоков в год. Мы используем p_c для базовой процентной ставки системы, выраженной в годовом выражении, а проценты начисляются на

блокировать. Таким образом, пользователь, работающий на $б$ блоки г) $_б$ - 1 получает выплату процентов:

$$1 + \frac{p_c}{63,072,000}$$

за поставленный токен. Например, если годовой процент составляет $p_c = 4\%$, пользователь, который делает ставку на 15 768 000 блоков (около финансового квартала) получат проценты 1% за поставленный токен. В эти расчеты мы округляем выплату процентов в токенах *вниз* до ближайшего (1) капать.

Установив номинальную ставку p_c, (итоговый годовой r) 63 определяется:

$$\text{эффективная годовая ставка} = 1 + \frac{p_c}{63,072,000} - 1.$$

Например, для $p_c = 4\%$ у нас эффективная годовая ставка $\approx 4{,}08\%$. [5]

Экономический механизм прост: предположим, для простоты, что все токены были выпущены, все жетоны поставлены и ни один жетон не перешел из рук в руки. Тогда выплата процентов не создает новой ценности - все, что изменилось, - это увеличение количества токенов («денежная база»), которые представляют сеть. Владельцы токенов в реальном выражении ничего не получают и не теряют. [6] Когда пользователи не ставят свои токены, их интерес переходит в общественный фонд. Следовательно, процентные платежи неявно перемещают стоимость от тех, кто не делает ставки, к тем, кто делает ставку.

E. Ресурсы для хранения

Ключевым компонентом системы мотивации является *таможенное хранение.* Любой, кто хочет развернуть смарт-контракт в сети Conflux, должен отправить несколько токенов для создания связанного хранилища. Выплата процентов по токенам в облигационном хранилище постоянно направляется майнерам, а не тем, кто заблокировал эти токены.

---

[5] Поскольку у нас большое количество платежных интервалов, мы можем приблизить $\lim_{n \to \infty} (1 + x/n)^n - 1 = e^{x} - 1$.

[6] Другая аналогия - дробление акций: когда фирма делит свои акции, скажем, 1: 2, то владельцы получают для каждой «старой» акции две «новые» акции. Однако этот процесс не меняет стоимости фирмы, и поэтому акционеры не становятся ни богаче, ни беднее после дробления акций.

Следовательно, эти процентные платежи создают неявный *поток вознаграждений* от лиц, занимающих пространство в сети, до лиц, обслуживающих сеть.

Требуемый залог для ресурсов хранения измеряется в собственном токене: 0,5 CFX за 1 КБ. Процесс выглядит следующим образом: пользователь (например, разработчик dApp) блокирует несколько токенов. Затем пользователь занимает место в сети (*например,* развертывание dApp или хранение данных из-за выполнения dApps), токены изымаются из заблокированных токенов и помещаются в связанное хранилище. Процентные платежи за токены в таможенном хранилище идут майнерам. Чтобы освободить токены из связанного хранилища, пользователи должны освободить место, которое они занимают.

F. Право голоса

Среднесрочная цель состоит в том, чтобы публичный фонд преобразовался в DAO и чтобы заинтересованные стороны Conflux голосовали за его операции, используя свои права голоса. Пользователи получают право голоса за счет блокировки токенов: чтобы проголосовать, пользователи должны согласиться заблокировать свои токены, а время блокировки определяет количество голосов. Продолжительность блокировки начинается с момента (также называемого блоком) подачи голоса. Право голоса будет предоставлено

$$\text{количество кварталов} \times \text{количество жетонов} \times 0{,}25.$$

Например,

- *Срок погашения менее четверти:* Нет права голоса
- *Срок погашения более четверти:* Один CFX имеет 0,25 голоса
- *Срок погашения более полугода:* Один CFX имеет 0,5 голоса
- *Срок погашения более года:* Один CFX получил 1 голосов

Мы измеряем «время» блоками, исходя из предполагаемого числа в 63 072 000 в год. В то время как токены заблокированы для получения голосов, пользователи сохраняют за собой право делать ставки. Максимальный срок блокировки для голосования - 4 года. Хотя токены заблокированы для получения права голоса, пользователи не могут снимать токены или уменьшать продолжительность блокировки.

G. Network Bootstrap

Далее мы обсудим, как с экономической точки зрения оптимизировать сеть Conflow и как управлять Фондом сообщества и Фондом экосистемы в долгосрочной перспективе.

Сообщество Bootstrap: Для поддержки сообщества Conflux Foundation предлагал вознаграждения и гранты в форме токенов FC (Fan's Coin) тем членам сообщества, которые внесли вклад в Conflow до его запуска. Con ux Foundation конвертирует выпущенные токены FC в CFX из Фонда сообщества, как только сеть Con ux будет запущена. Обратите внимание, что масштабы программ баунти и грантов Conflux умеренные. Общее количество выпущенных токенов FC на момент запуска Conflux будет менее 20 миллионов. После запуска мы продолжим программы баунти и грантов с CFX в Фонде сообщества в аналогичном масштабе.

Экосистема Bootstrap: Одна из проблем начальной загрузки экосистемы Conflux - привлечь разработчиков к разработке и развертыванию dApps на Conflux. Отправка массивных эирдропов CFX разработчикам - не идеальное решение, потому что можно обыгрывать систему и продавать эирдропы CFX на вторичном рынке вместо того, чтобы использовать их для разработки. Чтобы решить эту проблему, Conflux имеет уникальный механизм спонсора, в котором можно стать спонсором развернутого смарт-контракта, чтобы покрыть его транзакционные сборы и затраты на хранение. Con ux Foundation будет использовать Ecosystem Fund для спонсирования развернутых смарт-контрактов на Con ux в период начальной загрузки. В отличие от обычных воздушных капель,

Механизм спонсора в Conflux гарантирует, что эти спонсирующие CFX не пойдут в обращение, если они не будут сначала выплачены майнерам в качестве комиссии за транзакцию.

Управление DAO: Фонд Confux планирует постепенно передать управление Фондом сообщества и Фондом экосистемы DAO заинтересованных сторон Confux. Текущая дорожная карта предусматривает завершение перехода в течение двух лет после запуска Conflux.

Инвестиции в фонд экосистемы: В долгосрочной перспективе мы можем использовать Ecosystem Fund для создания инвестиционных фондов для инвестирования в важные проекты dApp, которые являются выгодными для экосистемы Conflow. Confux Foundation пригласит предыдущих частных инвесторов Confux для совместного управления такими инвестиционными фондами. Мы считаем, что создание таких инвестиционных фондов должно происходить под контролем DAO, заинтересованного лица Conflux.

Награды за майнинг

Сопровождающие систему сети Conflux будут получать доход из трех источников: комиссионные за транзакции, вознаграждение за блок и процентный доход, который возникает в результате «аренды» пользователями места в цепочке блоков.

Сборы с пользователей: Пользователи должны будут компенсировать майнерам при отправке транзакций и изменении состояния в цепочке блоков. Плата за транзакцию распределяется пропорционально двоичным базовым коэффициентам блоков, как определено в Li and Yang (2020).

Награды за блок: Как обычная практика в PoW-сетях, добыча блока включает вознаграждение в виде монет, которое увеличивает денежную базу и приводит к инфляции. Мы обозначаем это вознаграждение за блок, обусловленное скоростью инфляции, как p_b. Игнорируя любые рыночные изменения цен, экономически вознаграждение, основанное на монетах, представляет собой передачу богатства от существующих держателей CFX коллективно к победившему майнеру.

Начальное вознаграждение за базовый блок за блок составляет 7 CFX. По результатам голосования сообщества DAO награда за блок снижена до 2 CFX на блок, начиная с высоты эпохи 3 615 000, что соответствует p_b =2,52%.

Есть некоторые технологические тонкости, выходящие за рамки данной статьи, но мы хотим здесь упомянуть. А именно, хотя вознаграждение за блок определяется детерминированно в децентрализованной сети, не существует заранее определенного количества монет, которые получает майнер, который успешно майнит блок. Вместо этого блоки организованы в «эпохи», и вознаграждения за блоки определяются / распределяются для каждой эпохи. Для каждого блока протокол назначает «вес» на основе так называемых характеристик ориентированного акрилового графа, который фактически является мерой важности в параллельно организованной цепочке, а вознаграждение основывается на весе блока. За подробностями мы отсылаем читателя к техническому документу.

Интерес к хранению: Когда токены используются в качестве облигаций для хранения, проценты, выплачиваемые по этим токенам, передаются майнерам. Подобно вознаграждению за блок, общая сумма процентов от связанного хранилища будет распределяться пропорционально фактически полученному базовому вознаграждению за каждый блок.

Хотя подробности вознаграждения за блоки описать нетривиально, основной принцип такой же, как и в любой публичной сети PoW: майнеры предоставляют вычислительную мощность, чем больше мощности они предоставляют, тем больше вероятность, что они выиграют блок, тем больше блоков они выигрывают, тем выше их доход и т. д.

В следующем разделе мы представляем откалиброванную модель привлечения пользователей и инфляции, чтобы дать рекомендации относительно ожидаемого дохода от майнинга.

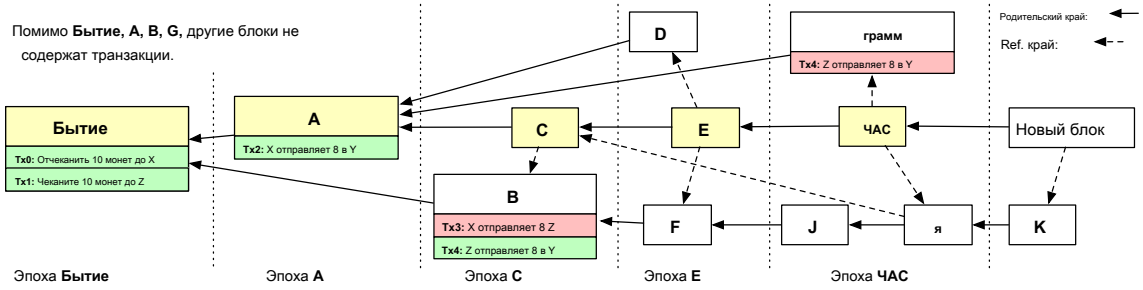


Рисунок 1
Пример структуры TreeGraph в Con ux

Штраф против конуса: Награда за блок майнинга модифицируется

коэффициент штрафа против конуса в Con fl u { Икс. В-й (|Антикон (*б)* |, мы определяем коэффициент штрафа блока *б:*

$$\text{макс}\left(0,\ 1 - \frac{|\text{Антикон}(б)|}{100}\right)$$

куда Антикон (*б)* обозначает набор блоков, которые не находятся в прошлом подграфе *б*

(т. е. достижимо через родительские и / или ссылочные ребра из *б)* и которых нет в будущем подграфе *б (* т.е.

достижимый через родительские и / или ссылочные ребра для *б).* Например,

Антикон (*F) = {A, C, D, G}* на рисунке 1. Поскольку антиконус блока может продолжать расти, Антикон (*б)* сюда входят только блоки, которые находятся в пределах 10 эпох после эпохи, когда *б* находится в. Обратите внимание, что для простоты мы исключаем трудность настройки из рассмотрения формулы и предполагаем, что трудность остается постоянной. См. Полную формулу в Li and Yang (2020).

Для нового блока базовое вознаграждение - это максимальное вознаграждение за блок, которое может получить генератор. Для каждого блока антиконуса нового блока часть вознаграждения за блок будет вычтена до нуля. Интуитивно эта формула вознаграждения за блок побуждает генератор следовать честному поведению, определенному протоколом консенсуса. Это

побуждает генератор ссылаться на как можно больше блоков, чтобы избежать антиконусных блоков из-за блоков, на которые нет ссылок. Это также побуждает генератор распространить новый блок как можно скорее, чтобы избежать блоков, препятствующих конусу из-за сетевой задержки. В отличие от майнинг-игры «победитель получает все» для самой длинной цепочки в Биткойне, все блоки в Conflow получают вознаграждение за блоки, а майнеры, которые сотрудничают друг с другом, минимизируют антиконус. Это делает Conflux защищенным от атак «самодостаточного майнинга», в которых используется принцип принципа «победитель получает все»; см. Эяль и Сирер (2013).

В наших калибровках мы абстрагируемся от антиконуса и устанавливаем его на ноль; неявное предположение состоит в том, что все майнеры правильно ссылаются на все предыдущие блоки и не делают ошибок.

I. Эволюция скорости потока.

Рыночная цена свободно торгуемых токенов CFX из-за неразрешенного характера сети, очевидно, находится вне контроля Conflux. Хотя никто не может предотвратить спекуляции, в конечном итоге можно утверждать, что (как и любой другой актив или товар) цена токена будет определяться спросом на услуги Conflux. Далее мы предлагаем формальную модель, чтобы подчеркнуть взаимосвязь между использованием услуги и ценой.

По сути, цена CFX зависит от двух основных параметров: встроенной инфляции системы и влияния рыночной цены на внешний мир. Это аналог *покрытый процентный паритет,* это экономическая концепция, описывающая изменения обменного курса во времени. Если мы используем $п_0$ для обозначения сегодняшней цены CFX в валюте (т. е. сколько инкорпорации платит за один CFX), $п_1$ для цены токена на год вперед (формально форвардный курс на 1 год), $р_с + р_б$ для реальной процентной ставки в Conflux (вызванной как вознаграждением за блок, так и выплатой процентов за хранение), и $р$ для усредненной реальной процентной ставки финансового кризиса (*например,* над корзиной основных

фи в валютах)

$$\pi_1 = \pi_0 \times \frac{1 + p}{1 + p_c + p_б}.$$

Другими словами, если Conflux платит более высокую процентную ставку, чем то, что доступно на рынках, то ожидается, что цена CFX механически изменится. *снижаться* через некоторое время.

V. Калиброванная модель вознаграждения майнеров

A. Обзор

Одним из важных факторов для функционирования сети PoW является то, что майнеры готовы тратить ресурсы на блоки для майнинга в обмен на некоторую форму компенсации. Безопасность такой сети напрямую связана с вычислительной мощностью, предоставляемой участвующими майнерами. Поскольку вычислительная мощность может быть дорогостоящей, для поддержки участия майнеров требуется достаточная компенсация майнерам, что, следовательно, имеет решающее значение для безопасности цепочки. В этом разделе мы развиваем наш подход к определению ожидаемых доходов, которые майнеры получат от участия в такой системе. Мы калибруем нашу модель на основе наших технических характеристик, а также наблюдений из проекта блокчейн Ethereum, учитывая схожесть доступных функций.

Майнеры получают прямой доход из трех источников: вознаграждения за блоки, сборы с пользователей и проценты, выплачиваемые по токенам, которые пользователи должны депонировать в качестве облигаций, когда они хотят хранить данные в цепочке блоков.

Награды за блоки - это недавно отчеканенные токены, и, следовательно, они увеличивают денежную базу Confux. Игнорируя изменения цены токенов Conflux, увеличение денежной базы снижает ценность каждого токена Conflow, и поэтому вознаграждения за блок являются передачей стоимости от владельцев собственных токенов (которые получают «безопасность» и согласованность реестра

как услугу) майнерам. Таким образом, мы считаем, что лучше всего думать о вознаграждении за блок с точки зрения годовой скорости инфляции, которую они создают. Мы формально обсудим, как взаимодействуют награды за блок и инфляция за блокировку, в следующем подразделе.

Сборы с пользователей зависят от конечного использования блокчейна, и поэтому для определения сборов с пользователей нам необходимо разработать модель привлечения пользователей; мы делаем это в Подразделе C., а затем мы выводим соответствующий доход от комиссионных в Подразделе D. Выплаты процентов также увеличивают денежную базу, и мы разрабатываем модель для этих выплат в Подразделе E. Более того, выплаты процентов майнерам зависят от того, насколько пользователи предпочитают занимать хранилище; мы строим модель для этого в подразделе F., а затем выводим процентные платежи майнерам в подразделе G. Майнерам, вероятно, придется оплачивать свои счета (за электроэнергию и оборудование для работы в режиме реального времени) непосредственно. Следовательно, необходимо построить модель цены CFX, чтобы приспособить эту цену, тема, которая обсуждается в подразделе H.

В подразделе I. мы согласовываем все эти компоненты, чтобы определить общий доход, который получат майнеры. В заключительной части этого упражнения мы представляем результаты моделирования для этого дохода и различных параметров в подразделе J.

Все обозначения, введенные в этом разделе, обобщены в таблице I ниже.

Таблица I

Список символов для раздела V.

Символ	Смысл
грамм	жетоны генезиса, 5B
D	количество секунд в день, 60 × 60 × 24
d	дней с момента получения вознаграждения
B	за блок запуска основной сети
б (г)	вознаграждения за блок в день, определяемые в уравнении (1), годовая скорость инфляции на основе коэффициента
p б	использования вознаграждений за блокировку пользователей ∈ (0, 1); оценивается на основе данных Ethereum с
u (d)	использованием уравнения (2)
ты ETH	расчетная скорость привлечения пользователей с использованием Ethereum в качестве эталона, описанного в уравнении (3)
ты быстрый(*г), ты* медленный(*г)*	коэффициент привлечения пользователей, смоделированный на основе Ethereum, но в одном случае рост происходит быстрее, а в другом - медленнее; определены в уравнениях (4) и (4)
T (г)	транзакции в день *d;* вычисляется как *u (d)* × *D* × 4000 (максимальная теоретическая пропускная способность) средняя комиссия за транзакцию,
ж	уплачиваемая в эквивалентной денежной форме
F (d)	общая сумма транзакционных сборов, выплачиваемых майнерам за день *d,* определенная в уравнении (6) доля токенов,
α	которые средний пользователь блокирует для получения процентных платежей, годовая скорость инфляции,
p c	создаваемая процентными выплатами в сети Conflux, ежедневная процентная ставка для сложных транзакций;
p	выводится из уравнения (7)
γ (d)	доля газа, используемого вычислениями, не являющимися простыми токенами; оценивается с использованием уравнения (8) и определяется в уравнении (9)
β	система требует доли токенов, которые необходимо поместить в бондовое хранилище для получения процентного дохода от
Идентификатор)	связанных токенов для майнеров; определенная в уравнении (10)
п(0)	цена CFX в день при запуске в основной сети Цена с поправкой на инфляцию в день *d,* определенное в уравнении (12) и в сокращенной форме
p (d)	в уравнении (13) количество монет в обращении в день *d;* это генезис плюс жетоны процентов плюс жетоны вознаграждения за блок, описанные
G (d)	в уравнении (11)
м (д)	общий доход майнеров за день *d,* полученный из уравнения (14), общий доход
m̄ (d)	майнера, усредненный за 1 год
грамм	гипотетический дневной темп роста цены CFX, так что через 3 года рыночная стоимость всех токенов Confux будет такой же, как рыночная стоимость всех ETH в начале 2020 года.

Б. Награды за майнерский блок

Майнеры получают вознаграждение за каждый добытый блок, и точная сумма зависит от того, где блок находится в цепочке относительно основной цепи и его антиконуса. Примечательно, что для представленной калибровки вместо представления точной *за блок* вознаграждение, мы вычисляем совокупный *повседневная* блокировать сумму вознаграждения.

Согласно техническим характеристикам, там сеть производит два новых блока в секунду, и, таким образом, $60 \cdot 60 \cdot 24 \times 2 =: D \times 2$ новых блоков в сутки. Предполагая постоянную скорость майнинга, есть $D \cdot 730$ блоков добывается в год. Таким образом, если B обозначает количество вновь отчеканенных токенов, созданных в качестве вознаграждения за блок для майнеров, системе требуется проблема

$B \cdot D \cdot 730$ новые токены ежегодно в качестве награды за блок. Награды за блок увеличивают денежную базу и создают инфляцию. Другими словами, устанавливая уровень вознаграждения за блок, система может напрямую определять скорость инфляции, создаваемую вновь созданными блоками. Эта инфляция - это переход от держателей монет к майнерам, и при установке скорости блока Confux может повлиять на то, сколько богатства он перераспределяет в течение данного года. В частности, цель Confux состоит в том, чтобы установить вознаграждение за блок на основе годового целевого уровня инфляции в размере $p_б \in (0, 1)$. Следовательно, для целевого значения $p_б$, награда за блок должна решить

$$B \cdot D \cdot 2 \cdot 365 \equiv грамм \cdot p_б \Leftrightarrow B = \frac{Gr_б}{730\ D}$$

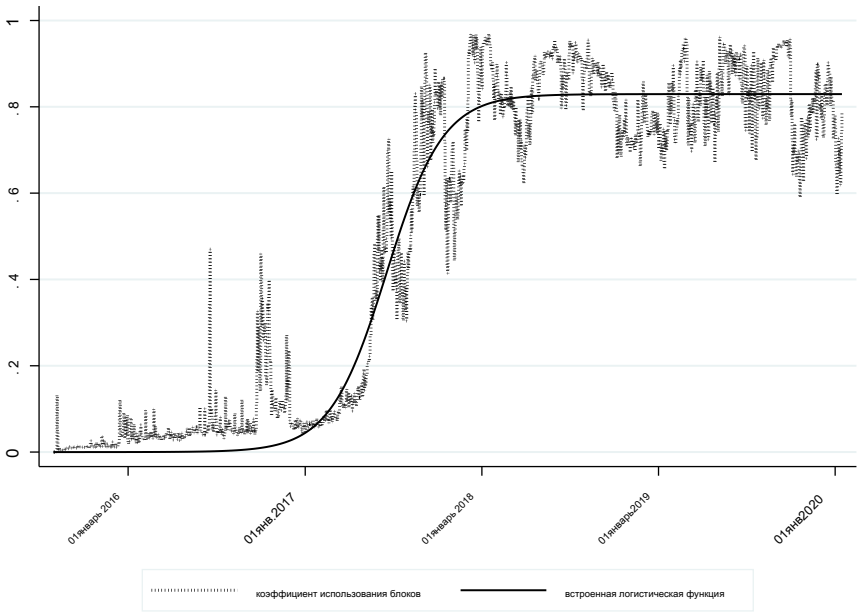
Обратите внимание, что в Conflow блоки создаются непрерывно и могут фактически быть пустыми, если нет действительных транзакций. В целом, в любой день d, общее вознаграждение за блок, обозначенное

$б\ (г)$ поэтому

$$б\ (г) = \frac{Gr_б}{365} \tag{1}$$

фигура 2

Скорость принятия Ethereum и встроенная логистическая функция



C. Привлечение пользователей

Принятие пользователями сети будет определять спрос на транзакции и вычисления, плату, уплачиваемую пользователями, и арендную плату за хранилище, распределяемую среди майнеров. Мы обсудим эти количества в следующих подразделах, так как здесь наша цель - разработать модель принятия пользователями.

Общей чертой новых технологий является то, что их внедрение происходит по S-образной схеме с медленным увеличением использования на раннем этапе, а затем внезапным скачком активности. Примером может служить использование сети Ethereum, показанное на Рисунке 2, где мы наносим на график среднесуточную долю использованного лимита газа; этот график основан на данных

из https://etherscan.io/charts.[7] Поскольку Conflux - новая технология, разумно ожидать, что поглощение Conflux также будет следовать S-образной схеме при условии, что сеть будет успешной. Con fl ux и Ethereum имеют много схожих функций, и поэтому мы будем использовать исторические данные о принятии Ethereum, чтобы оценить, что мы считаем разумной скоростью использования для Con ux.

В качестве первого шага мы охарактеризуем скорость использования Ethereum пользователями в форме параметрического функционала. Есть несколько способов описать S-образную функцию (также известную как сигмовидная кривая), стандартный - это логистическая функция, которая имеет форму:

$$Y = \frac{\xi_0}{1 + e^{-\xi_1 \cdot (Икс - Икс_0)}}, \quad (2)$$

В приведенном выше уравнении Y скорость приема во время X, ξ_0 это максимальное значение для поглощения, ξ_1 - скорость роста, а $Икс_0$ представляет собой временное значение, когда кривая достигает 50% своего максимального значения (формально значение горизонтальной оси в средней точке сигмоида). Наши результаты оценки представлены в Таблице II, на Рисунке 2 также изображена подобранная функция.

Теоретически блоки могут быть заполнены до 100% от установленного лимита газа, однако оценка для ξ_0 указывает на то, что уровень использования блокчейна Ethereum в настоящее время достигает 83%. Этому может быть несколько объяснений: одно из них заключается в том, что майнеры вступают в сговор, чтобы не включать транзакции с низкими комиссиями за транзакции. Другой заключается в том, что уровень использования 83% - это постоянная ежедневная «технологическая» верхняя граница того, что майнеры могут фактически включать с учетом задержки при проверке и отправке транзакции. Наконец, возможно, что как только сеть станет перегруженной, пользователи больше не будут отправлять новые транзакции.

[7] Аналогичную форму имел бы график ежедневных транзакций. Мы отмечаем, что существует верхняя граница транзакций, потому что общее количество газа на блок ограничено.

Таблица II.

Подбор логистической кривой для скорости охвата пользователей Ethereum

Таблица содержит результаты для нелинейной регрессии по методу наименьших квадратов (2) с использованием данных о скорости обращения пользователей Ethereum. *Y,* измеряется как часть лимита газа, используемого на блок в день *ИКС.* Т-статистика указана в скобках. *, **, *** указывают на статистическую значимость коэффициентов на уровнях 10%, 5% и 1%.

	ξ_0	ξ_1	$Икс_0$
Оценивать	0,83 *** (244,800)	0,02 *** (30,809)	690,54 *** (316,067)
Наблюдения 1631		1,631	1,631
R-квадрат	0,978	0,978	0,978

в цепочку из-за большой задержки; это создаст эндогенный верхний предел по запросу (отраженный в размере пула памяти) для обработки транзакций.

Следующий https://bitinfocharts.com/ethereum/, комиссии за транзакции постоянно составляют менее 3% дохода майнера за блок, и похоже, что майнеры, вероятно, не слишком озабочены использованием всего пространства в блоке.

В дальнейшем мы будем использовать оценки из Таблицы II в качестве эталона для моделирования потребления пользователями. $u(d) \in (0, 1)$. Другими словами, мы предполагаем (прогнозируем), что в день d фракция $u(d)$ от общей емкости Conflux. В тестовой сети Conflux имеет пропускную способность 4 000 транзакций в секунду. Как день 86, 400 секунды, в день *d,* будут $u(d) \times 4\,000 \times 86,400$ много сделок. Используя результаты таблицы II, получаем:

$$ты_{\text{ETH}}(г) = \frac{0,83}{1 + e^{-0,017 \cdot (d - 690)}}. \quad (3)$$

Согласно этой модели, потребуется 718 дней, прежде чем Conflow достигнет емкости сети 50%, и 793 дня (*т.е.* примерно два года) для выхода на мощность 70%.

Несомненно, использование Conflux может отличаться от модели, описанной выше, с точки зрения времени, необходимого для достижения определенной скорости принятия. Инвестиции в экосистемы и разработка децентрализованных приложений могут способствовать более быстрому освоению. Платформа смарт-контрактов Con ux совместима с Solidity, одним из основных языков программирования для смарт-контрактов на Ethereum. Эта совместимость подразумевает, что многие нынешние разработчики dApp блокчейнов из сообщества Ethereum сталкиваются с неглубокой кривой принятия. По контракту, когда был запущен Ethereum, было значительно меньшее сообщество разработчиков, опытных в Solidity. Следовательно, разумно ожидать более быстрого освоения Conflux пользователями по сравнению с Ethereum.

При калибровке нашей модели мы проводим анализ с двумя различными поправками к предлагаемой модели. Во-первых, мы сдвигаем кривую внедрения на 180 дней вправо, что означает, что принятие откладывается на квартал. Во втором случае мы сдвигаем кривую внедрения на 180 дней влево, что означает, что внедрение ускоряется на четверть. Формально этот сдвиг представляет собой увеличение / уменьшение параметра $Икс_0$ на 870 и 510 календарных дней соответственно, чтобы:

$$ты_{\text{быстрый}}(г) = \frac{0{,}83}{1 + e^{-0{,}017 \cdot (d - 510)}}, \tag{4}$$

$$ты_{\text{медленный}}(г) = \frac{0{,}83}{1 + e^{-0{,}017 \cdot (d - 870)}}. \tag{5}$$

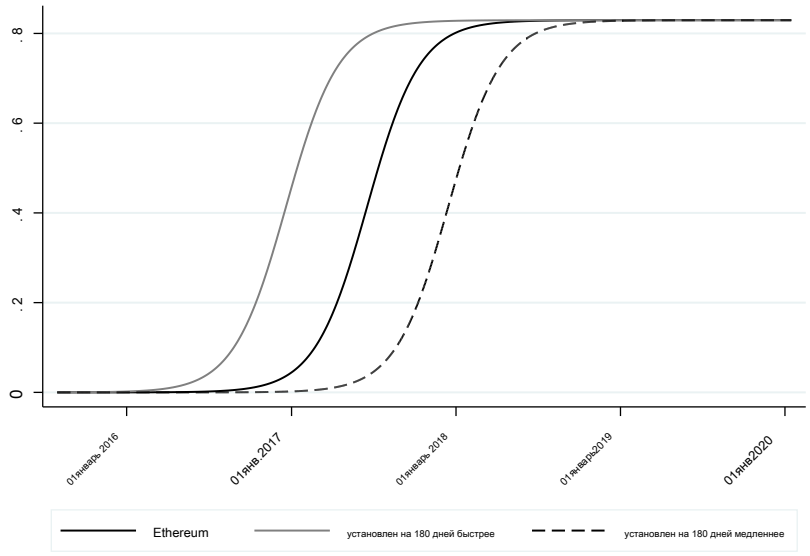
На рисунке 3 показаны три разные модели скорости внедрения, обозначенные как *быстрый* ($ты_{\text{быстрый}}(г)$), *Эфириум* ($ты_{\text{ETH}}(г)$), и *медленный* ($ты_{\text{медленный}}(г)$).

При максимальной мощности Conflux обрабатывает 4000 транзакций в секунду. При долгосрочной скорости внедрения $и(d) = 80\%$, это составляет ожидаемую утилизацию 3200 тонн в секунду. Со скоростью освоения $и(d)$, среднее количество транзакций в день составляет

$$T(д) = и(д) \cdot 4\,000\ D = и(d) \cdot 345{,}6 \times 10^{6}.$$

Рисунок 3

Три калиброванных коэффициента усыновления



Мы отмечаем, что мы используем данные из Ethereum для оценки частичного использования максимальной емкости, и мы ожидаем, что фактическая частота обновления в Conflow превысит ранее заявленное число. Мы оправдываем это мнение следующим образом: Ethereum, вероятно, большую часть времени загружен (см. Рисунок 2, и его пул памяти невыполненных транзакций не пуст). Поскольку Ethereum работает на полную мощность, у разработчиков есть ограниченный стимул для внедрения новых приложений dApp, особенно для сценариев использования в масштабе предприятия. Более высокая пропускная способность Con ux снижает опасения, что транзакции не подтверждаются своевременно, а поскольку Con ux совместим с Solidity, разработчики сталкиваются с трудностями в обучении. Вместе это должно способствовать быстрому внедрению Conflux.

D. Сборы с пользователей

Пользователи платят за вычислительные циклы, иначе говоря, за использованный газ. Обычной практикой является обозначение емкости блокчейна количеством транзакций в секунду, где транзакция относится к простой передаче собственного токена с одного адреса на другой. Такая сделка требует фиксированного количества газа; например, на Ethereum это 21000 газа. Поэтому мы следуем этому соглашению и приравниваем плату за пользование к плате, которую пользователи платят за передачу адреса на адрес.

Мы предполагаем, что пользователи в среднем платят комиссию за транзакцию в размере *f.* Таким образом, средние дневные сборы в зависимости от *день F (d),* рассчитываются следующим образом:

$$F(d) := \underbrace{ж}_{\text{средняя дневная плата}} \times \underbrace{T(d)}_{\text{количество транзакций в день } d} \quad \text{знак равно } F \cdot u(d) \cdot 4\,000 \cdot Д. \tag{6}$$

В приведенной ниже таблице представлены примеры годового дохода от комиссий в сети Conflux, который уровень использования «по мощности» предоставляет майнерам для различных уровней средней комиссии. *f:*

средний	в день	ежегодный
0,001 доллара США	276 480 долл. США	88 300 800 долл. США
0,005 долл. США	1 382 400 долл. США	441 504 000 долл. США
0,010 доллара США	2 764 800 долл. США	883 008 000 долл. США
0,020 доллара США	5 529 600 долларов США	1 766 016 000 долларов США
0,050 доллара США	13 824 000 долларов США	4 415 040 000 долларов США

Для Ethereum, при его текущем вознаграждении за блок и его производительности, общие вознаграждения составляют порядка 2,3 миллиона долларов в день или около 840 миллионов долларов в год, включая как вознаграждения за блоки, так и

сборы с пользователей. В результате сборы с пользователей составляют менее 3% вознаграждений.[8] В Con ux при аналогичной скорости использования блоков пользовательские сборы будут обеспечивать такой же общий доход от сборов, как и *общий* доход (комиссии плюс вознаграждение за блок) в Ethereum, если пользователь готов платить в среднем 0,01 доллара за транзакцию. Даже при умеренном желании пользователей платить комиссию годовой доход может быть значительным. Для сравнения, средняя комиссия за транзакцию в блокчейне Ethereum за январь – февраль 2020 года составляла от 0,08 до 0,15 доллара США.

(источник: ycharts.com).

Также интересно сравнить эти цифры с комиссиями в традиционных розничных платежных сетях. Например, при транзакциях с кредитными картами различные субъекты, участвующие в транзакции, компании-эмитенты кредитных карт, такие как Visa или Mastercard, а также банки, занимающиеся обработкой платежей, в настоящее время взимают от 1% -3% от стоимости транзакции за розничные транзакции. А именно, любая транзакция на сумму более 2,5 долларов США влечет за собой минимальную комиссию в размере 0,05 доллара США.[9] На другой платежной платформе FinTech компания Square взимает фиксированную комиссию в размере 2,75% за транзакцию; на других платформах, которые взимают из расчета за транзакцию, пользователи обычно сталкиваются с комиссией за транзакцию в размере не менее 0,15 доллара США.

E. Выплата процентов пользователям

Confux планирует выплачивать проценты пользователям, у которых их токены приостановлены. Как мы указали в предыдущем разделе, выпущенные токены существуют в двух формах: ликвидные и неликвидные. В жидкой форме они «бесплатны», их можно сразу переносить и использовать на

[8] Как и большая часть эмпирического анализа в этой статье, эти цифры основаны на состоянии блокчейна Ethereum в начале 2020 года. Однако во второй половине 2020 года плата за использование Ethereum резко выросла в результате перегрузки цепочки. вызвано сильным распространением децентрализованных финансовых приложений. На данный момент мы считаем, что это скопление не является устойчивым состоянием, а, скорее всего, является временным явлением. Таким образом, мы основали наш анализ на более консервативной оценке, которую мы представляем здесь.

[9] Это отличается от операций с дебетовыми картами. В США Поправка Дурбина к Закону Додда-Франка ограничивает комиссию за обмен для дебетовых транзакций до 0,05% + 0,21 доллара; до того, как этот закон вступил в силу к 2011 году, средняя комиссия составляла около 0,44 доллара. Помимо этих сборов, платежные системы обычно взимают надбавку в диапазоне от 0,10 до 0,20 доллара плюс процент от стоимости транзакции.

Конвейерная цепь. Эти ликвидные токены не получают процентов. Это состояние похоже на деньги, хранящиеся на «чековом» или «текущем» счете в банке: в большинстве западных стран сегодня такие средства не приносят процентов, но они доступны для немедленного использования.

Пользователь также может обозначить свои токены как «ставку». В этом случае они заблокированы, недоступны для немедленного использования и, следовательно, неликвидны. На такие поставленные токены начисляются проценты в виде новых токенов. Этот процент за токен начисляется во время размещения токена и будет выплачиваться в то время, когда пользователь разблокирует свой токен и конвертирует его в жидкую форму. Однако процесс размещения / блокировки и снятия / разблокировки требует времени и затрат на газ. Это аналогично деньгам, хранящимся на сберегательном счете: такие средства получают процентные платежи, но обычно не доступны для немедленного использования и / или могут нести комиссию при их выдаче. Технические подробности стейкинга / разстейкинга можно найти в техническом документе сети Conflux.

Мы представляем анализ выплаты процентов в следующем содержании. Для простоты мы предполагаем, что заблокированные токены Genesis выпускаются с постоянной скоростью ежедневно в течение 4-летнего периода (они выпускаются с ежеквартальными интервалами). Позволять $G =$ 5, 000, 000, 000
быть количеством токенов Genesis, заблокированных при запуске основной сети. Чтобы упростить анализ, мы предполагаем, что они высвобождаются с постоянной скоростью $п$ в сутки с момента запуска такое, что $п \cdot 365 \cdot 4 = ГРАММ.$ [10] Другими словами: $п \approx 343\ K$ токены выпускаются каждый день.

Предположим, что пользователи (включая тех, у кого есть выпущенные токены Genesis) будут блокировать / делать ставки в среднем на небольшую долю $α$ своих жетонов. потом $α \cdot d \cdot п$ токены имеют право на получение процентных платежей в день $d,$ а остальные $(1 - α) \cdot дн$ токены ликвидны и доступны для транзакций. В большей части нашего анализа мы предполагаем, что пользователи ставят все свои токены,

[10] Большинство этих жетонов выпускаются с фиксированными контрактными интервалами.

$\alpha = 1$, так что они получают проценты, когда это возможно, и снимают ставки только прямо перед тем, как захотят использовать свои токены.

Con ux выплачивает ежедневную сумму начисленных процентов p за поставленный токен в виде вновь отчеканенных токенов. Эти токены увеличивают денежную базу и, следовательно, приводят к инфляции. Мы также предполагаем, что Con ux установит цель для годовой ставки p_c такое, что больше года, $грамм \cdot p_c$ вновь отчеканенные токены от процентных выплат добавляются к денежной базе. Чтобы упростить изложение, мы также предполагаем, что вновь отчеканенные процентные токены возвращаются майнерам в виде ликвидных токенов.

Поскольку проценты начисляются за создание блока, во время которого токены заблокированы, для годовой эквивалентной ставки p нужно найти значение для p так что общая

процентные платежи в сумме составляют $грамм \cdot p_c$ к $\sum$ Кенс

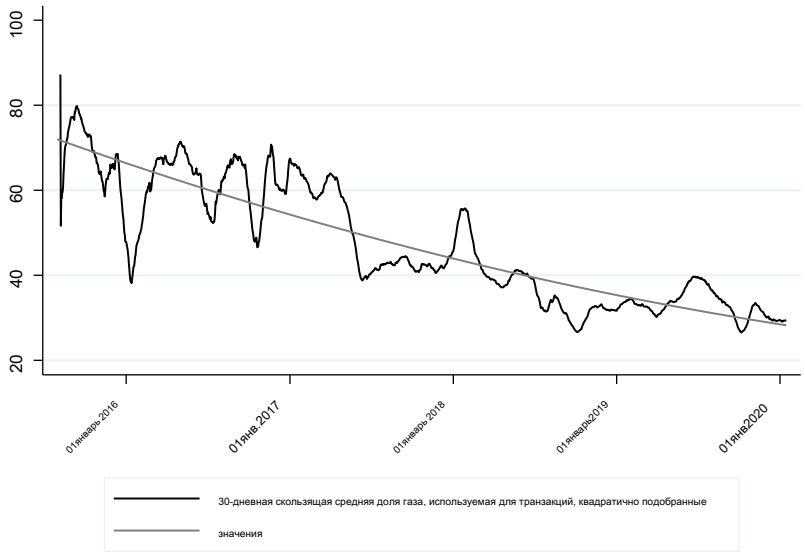
$$\underbrace{p_c}_{\text{общая годовая процентная ставка}} \text{ знак равно } \underbrace{p \cdot \alpha}_{\text{сумма индивидуальных процентных выплат}} \quad \Leftrightarrow \quad R = \frac{8 \cdot p_c}{366\ \alpha} \tag{7}$$

F. Транзакции против вычислений

До сих пор в описании мы рассматриваем транзакции как синоним использования базовой сети. Однако, в частности, полная по Тьюрингу цепочка блоков может делать гораздо больше, чем просто обрабатывать транзакции. Чтобы понять эту проблему, рассмотрите рисунок 4. Сплошная черная линия отображает ежедневные транзакции в цепочке блоков Ethereum. Серая линия отображает процентную долю газа, приходящуюся на транзакции. [11] Как показано на рисунке, со временем на транзакции с обычными токенами приходится уменьшающаяся доля транзакций.

[11] Формально мы выводим эту строку следующим образом. Получаем из etherscan.io/chart ряды данных для ежедневных транзакций и ежедневного использования газа. Для простого перевода транзакции ETH требуется 21000 газа, поэтому мы получаем количество газа, не связанное с транзакцией, путем вычитания количества транзакций, умноженных на
21 тысяча из всего газа.

Рисунок 4
Транзакции против вычислений



Как и в случае с привлечением пользователей, мы используем действия блокчейна Ethereum в качестве эталона для ожидаемого поведения в сети Conflow. В частности, мы запускаем регрессию OLS для квадратичной подгонки для скорости, не связанной с транзакциями:

$$\%\ нетранзакционного\ газа = \alpha + \beta_1 \cdot d + \beta_2 \cdot d_2 + \varepsilon, \tag{8}$$

куда d - количество дней с момента запуска основной сети. Цель здесь - измерить% *нетранзакционный газ* как количество $\in [0, 100]$. Таблица III содержит результаты наших оценок. В дополнение к необработанной ставке, которая очень шумна в начале выборки, мы используем 30-дневную скользящую среднюю долю использованного нетранзакционного газа. Результаты

Таблица III

Аппроксимация квадратичной кривой для скорости использования газа Ethereum, не связанного с транзакциями

Таблица содержит результаты нашей нелинейной регрессии по методу наименьших квадратов (8) с использованием данных для Ethereum - доли ежедневного нетранзакционного использования газа на Ethereum. MA относится к 30-дневной скользящей средней. T-статистика указана в скобках. *, **, * * * указывают на статистическую значимость соответствующих коэффициентов на уровнях 10%, 5% и 1%.

	% нетранзакций	MA (% нетранзакций)
β_1	- 0,04 ***	- 0,04 ***
	(-17,952)	(-26,239)
β_2	0,00 ***	0,00 ***
	(5,598)	(7,710)
α	71,88 ***	72,07 ***
	(94 875)	(141,995)
Наблюдения	1623	1,623
R-квадрат	0,615	0,782

очень похожий. Отметим, что параметр, оцененный для квадратичного члена, $\beta_{2,}$ очень маленький, около 7,05 $\times 10^{-6,}$ из-за размера связанной переменной.

До сих пор в этом подразделе мы обсуждали использование газа для целей, не связанных с транзакциями. Далее нам нужно определить, какой процент получают майнеры за хранение кода смарт-контракта. Мы измеряем доход майнера по транзакциям, потому что пользовательские сборы выплачиваются за транзакцию, а блок имеет фиксированную емкость с точки зрения количества транзакций. Более интуитивным подходом было бы измерить это количество в зависимости от расхода газа. Чтобы анализ оставался последовательным, мы конвертируем часть нетранзакционного газа в гипотетические транзакции, а затем делаем процентные платежи функцией этих гипотетических транзакций. В частности, пусть $\gamma(d)$ обозначают долю использования газа, которая не связана с транзакциями CFX, подобными денежным переводам. Следуя таблице III,

мы получаем:

$$\gamma(d) := 1 - \left(72 - 0{,}04 \cdot d + 7{,}05 \cdot 10^{-6} \cdot d^{2} / 100 = -0{,}0000000007\,(d - 2{,}837)^{2+.}\right) 85. \quad (9)$$

Поэтому, когда есть $T(г)$ транзакции в день d, мы говорим, что $(1 - \gamma(г)) \cdot T(г)$ из них простые переводы монет и $\gamma(d) \cdot T(г)$ включают выполнение смарт-контрактов, требующих хранения данных в цепочке.

G. Выплата процентов майнерам

При использовании цепочки для хранения информации (например, кода смарт-контракта) пользователи должны поместить определенное количество токенов в связанное хранилище. Эти токены приносят проценты, и проценты выплачиваются майнерам (а не тем, кто помещает токены на хранение).

При калибровке модели существует возможный сценарий, когда пользователь покупает хранилище (*т.е.* помещает токены в таможенное хранилище), но никогда не выполняет договор в дальнейшем. Чтобы решить эту проблему, мы предполагаем, что пользователи принимают решение о том, хранить ли токены в связанном хранилище каждый день, и, следовательно, что общие транзакции полностью отражают размер процентных выплат. Другими словами, мы учитываем только «новое» связывание токенов. Таким образом, калибровочная модель, вероятно, *консервативно недооценивает* процентный доход майнерам.

Con ux определяет, сколько токенов пользователи должны поместить в связанное хранилище по отношению к объему пространства, которое занимает контракт. Мы предполагаем, что эта сумма пропорциональна использованию газа по контракту или, как можно утверждать, количеству фактических транзакций, поскольку каждая из них требует газа.

Таким образом, для *Икс* транзакции, пользователям необходимо поставить $\beta \cdot$ *Икс* токены в таможенное хранилище и в день d это $\gamma(d) \cdot T(г)$ транзакции, требующие от пользователей размещения токенов в связанном хранилище.

Итого необходимая сумма составляет $\beta \cdot \gamma(d) \cdot T(r)$. Мы пришли к выводу, что каждый день майнеры, получающие проценты по этим облигационным токенам, как описано в (7), выглядят следующим образом:

$$I(d) := \beta \times \gamma(d) \cdot T(r) \times P. \tag{10}$$

Цена Н. CFX

Грубо говоря, рыночная капитализация сети Conflow - это рыночная цена токенов, умноженная на количество токенов, находящихся в обращении. В дополнение к рыночным изменениям цены токена, CFX изменяется в зависимости от встроенной инфляции, поскольку цена одного токена по отношению к денежным средствам при прочих равных условиях падает при увеличении количества токенов, находящихся в обращении. Это не означает, что сеть становится менее ценной, это просто означает, что теперь доступно больше токенов для использования в сети. Эта инфляция вызвана расширением денежной базы в виде вознаграждений за блоки и выплаты процентов.

Позволять $п(0)$ обозначают начальную цену токена CFX. При запуске основной сети количество токенов в обращении составляет $G = G(0)$. После d дней количество токенов

увеличено за счет вознаграждения за блок и выплаты процентов $\sum$ nts, как показано ниже:

$$G(d) = G(0) + \underbrace{б(d) \cdot d}_{\text{блокировать награды}} + \underbrace{\sum_{j=1}^{d} p \cdot \alpha \cdot j \cdot п}_{\text{выплаты процентов}}, \tag{11}$$

где плательщики процентов $\sum$ ts упростить до

$$\sum_{j=1}^{d} p \cdot \alpha \cdot j \cdot п = \frac{d(d+1)}{365 \cdot 366} \, ГРАММ(0) \cdot p.$$

Предполагая, что внешние силы отсутствуют, рынок вызвал изменения цены токена CFX в течение дня. *d* является:

$$p(d) = p(0) \cdot \frac{ГРАММ(0)}{G(d)}. \quad (12)$$

Используя выводы (1) и (7) (, цена CFX там же) - 1 руда:

$$p(d) = p(0) \cdot 1 + \frac{d}{365_{б}} r + \frac{дд + 1}{365\ 366} p_{c} . \quad (13)$$

Согласно нашей текущей информации, при запуске основной сети CFX будет иметь номинальную стоимость 0,1 доллара США, а совокупная стоимость сети составит 500 миллионов долларов США. По состоянию на начало 2020 года рыночная капитализация сети Ethereum составляла около 16 миллиардов долларов, то есть в 32 раза больше, чем у Conflux. Примечательно, что цена эфира начала торговаться около 1 доллара при запуске, а сейчас она превышает 300 долларов. В более поздней части этой статьи мы разрабатываем модель равновесия использования токенов и затрат на майнинг, которая помогает обосновать зависимость цены токена от *полезность* что сеть (и, следовательно, майнеры) предоставляют пользователям.

I. Общий доход горнодобывающих компаний

Подводя итог, общий доход майнера, [12] обозначается *м (г),* состоит из (*а)* вознаграждение за блок из уравнения (1), (*б)* процентный доход от облигационных токенов, как показано уравнением (10), и (*в)* сборы с пользователей, выраженные уравнением (6):

$$m(d) = p(d) \cdot б(г) + p(г) \cdot I(d) + F(d)$$

$$\text{знак равно } \frac{p(d) \cdot Gr_{б} + p(d) \cdot \beta \times \gamma(d) \cdot T(г) \times R + f \cdot T(г).}{365} \quad (14)$$

[12] Мы предполагаем, что вознаграждение за блок и процентный доход конвертируются в эквивалентную денежную единицу с использованием цены CFX, вычисленной по уравнению (13).

В следующем подразделе мы проводим моделирование, чтобы проиллюстрировать возможные уровни доходов с разумными параметрами модели.

J. Калибровка доходов майнеров

Перед тем, как представить результаты калибровки доходов майнеров Conflow, мы пролили свет на то, что майнеры Ethereum в настоящее время зарабатывают за свою работу. В день создается около 6500 блоков, при этом выплачивается около 13 500 ETH, так что общее среднее ежедневное вознаграждение за блок составляет всего лишь 3 миллиона долларов США (на основе цен ETH на начало 2020 года). [13] Для Ethereum комиссионные за транзакции, оплачиваемые пользователем, играют незначительную роль в доходе майнеров, тогда как для Conflux ожидается, что комиссионные сборы будут играть более значительную роль из-за его высокой пропускной способности. Однако, пока сеть набирает обороты, транзакций будет немного. Поэтому для нашей калибровки мы усредняем доход майнеров на относительно длительных горизонтах. Ниже мы вычисляем среднегодовые значения с интервалом в 91 день:

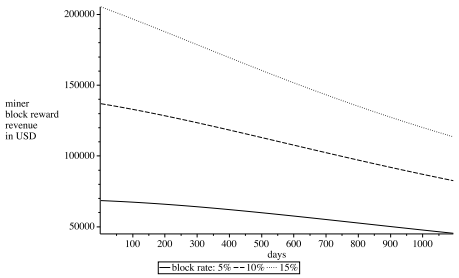
$$\bar{m}(d) = \frac{1}{365} \sum_{d \text{ знак равно } я \cdot 91 + d}^{(я+4) \cdot 91 + d} м(д'), \quad я = 0, \ldots, 7.$$

Мы используем четыре значения средней комиссии за транзакцию, $ж \in \{.005, .01, .02, .08\}$, где наибольшее число 0,08 доллара США соответствует минимальной медианной комиссии, уплаченной на Ethereum в начале 2020 года, как мы обсуждали ранее. Для коэффициента использования мы рассматриваем три базовых показателя. $ты_{\text{быстрый}}(г)$, $ты_{\text{ETH}}(г)$, и $ты_{\text{медленный}}(г)$ из Подраздела C. Для необходимого количества таможенного хранилища мы используем $\beta = 1\%$ Это означает, что если пользователь занимает пространство в цепочке блоков для будущих вычислений, которое эквивалентно тому, что занимает 1 транзакция с кодом операции виртуальной машины, то этот пользователь должен поместить 1/100 токена CFX в связанное хранилище.

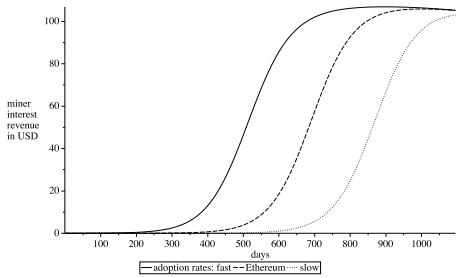
[13] Источник: bitinfocharts.com/ethereum/.

Ниже мы не делаем никаких предположений о повышении цен на рынке, за исключением случаев, когда это явно указано.

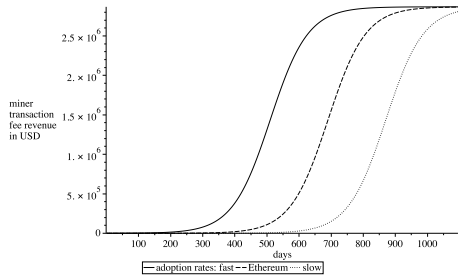
В качестве первого шага мы отдельно наносим на график три составляющих дохода майнера: вознаграждение за блок, процентный доход и комиссию пользователей. На Рисунке 5 показаны эти ежедневные доходы. Эти цифры используют годовые процентные выплаты в размере $p_c = 4\%$, и средняя комиссия в размере 0,01 доллара США.



Панель A: Награды за блок



Панель B: процентный доход



Панель A: Доход от комиссии за транзакцию

Рисунок 5.

Доходы майнеров с течением времени в зависимости от скорости внедрения

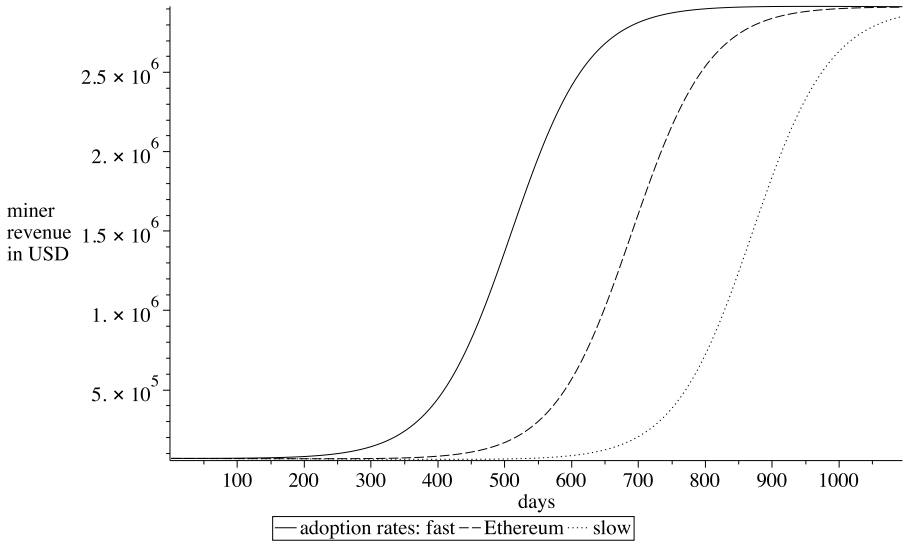


Рисунок 6

Доходы майнеров с течением времени в зависимости от скорости внедрения

На рисунке 5 $ -значение вознаграждения за блок (панель A) снижается, потому что цена снижается из-за инфляции; обратите внимание, что мы предполагаем, что количество токенов, выдаваемых в качестве вознаграждения за блок, постоянно в пределах интервала. Для оставшихся двух панелей мы устанавливаем годовой темп инфляции блока равным ρ_b=5%. Процентный доход (панель B) растет с использованием блокчейна, но он невелик по величине. Наконец, доход от платы за пользование (панель C) отображает доход от комиссии. Значения, записанные на вертикальной оси, показывают, что ожидается, что эти комиссии будут на порядок больше, чем процентный доход или доход от вознаграждения за блок, за исключением случаев сразу после запуска основной сети.

Объединив эти три цифры, на рисунке 6 показан ожидаемый дневной доход майнеров. *м (д)* через три года после запуска основной сети для трех различных сценариев скорости доступа пользователей. На этом рисунке используется годовая скорость инфляции блока в размере ρ_b=5%, ежегодные процентные выплаты в размере ρ_c=4%, и средняя комиссия в размере 0,01 доллара США.

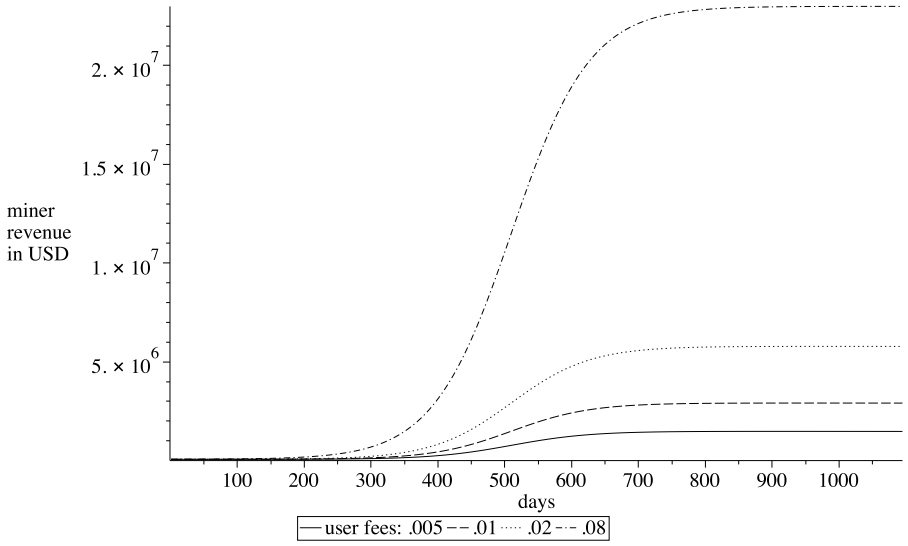


Рисунок 7

Доходы майнеров с течением времени как функция от средних комиссий

На рисунке 7 показан временной ряд ожидаемых доходов майнеров в день с четырьмя различными средними комиссиями за транзакции. Когда Conflux загружен, даже при умеренной комиссии в 0,02 доллара доход майнера составит около 2,5 миллиона долларов. На этой диаграмме используется уровень инфляции блока в 5%, процентные платежи в размере 4% и скорость внедрения Ethereum.

В качестве аргумента мы также рассматриваем ситуацию, когда рыночные силы приводят к росту цен на токены CFX таким образом, что через три года Confux будет иметь такую же рыночную оценку, что и Ethereum сегодня, то есть рыночная капитализация примерно в 15 миллиардов долларов. Далее предположим, что изменение цены следует за линейным ростом с некоторой скоростью. *грамм* так что цена во время *d* является

$\pi_{ETH}(r) = p(0) \cdot (1+грамм)^{d}$. Оценка *грамм* Это гарантирует, что рыночная оценка Conflux через три года после запуска такая же, как у Ethereum в начале 2020 года. *грамм* ≈ 0,0031.

Теперь мы вычисляем общий доход майнера, используя «спекулятивную» цену. $\pi_{ETH}(r)$, т.е. в (14)

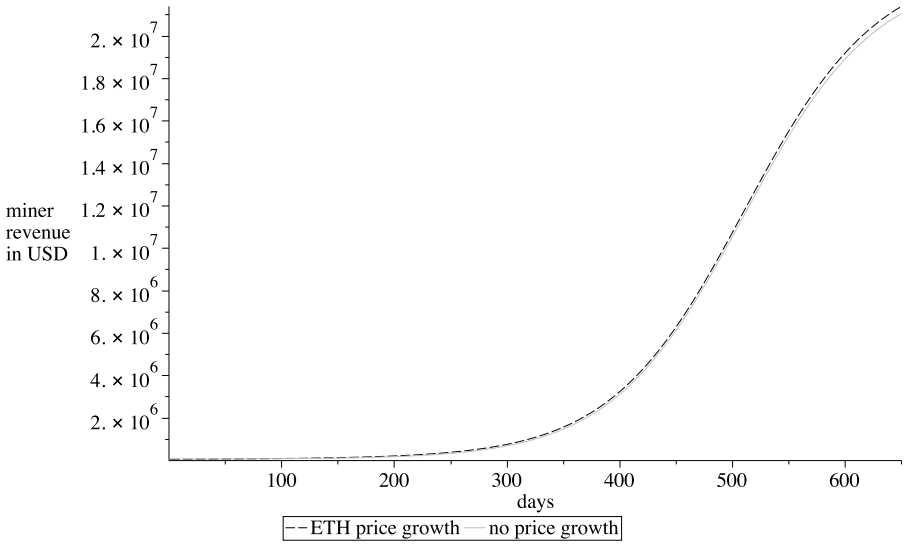


Рисунок 8

Доходы майнеров, если цены вырастут до уровня ETH

мы заменяем *p (d)* с $п_{ETH}(г)$ так что получаем:

$$м_{ETH}(г) = p_{ETH}(г) \cdot б(г) + p_{ETH}(г) \cdot I(d) + F(d) \quad (15)$$

На рисунке 8 показан временной ряд ожидаемых доходов майнеров в день для этого альтернативного ценового пути. $п_{ETH,}$ где мы строим только первые 650 дней. На этом рисунке мы используем уровень инфляции блока в 5%, процентные платежи в размере 4%, уровень внедрения Ethereum и готовность платить комиссию по текущим ставкам Ethereum (0,08 доллара США). Мы также включаем случай выручки, когда нет роста цен (он соответствует наиболее «оптимистичному» случаю на Рисунке 7) в качестве ориентира. В *ключ* Вывод из этого рисунка состоит в том, что, когда мы предполагаем, что цены значительно вырастут, доход майнеров в среднесрочной перспективе не пострадает просто потому, что комиссионные за транзакции продолжают доминировать.

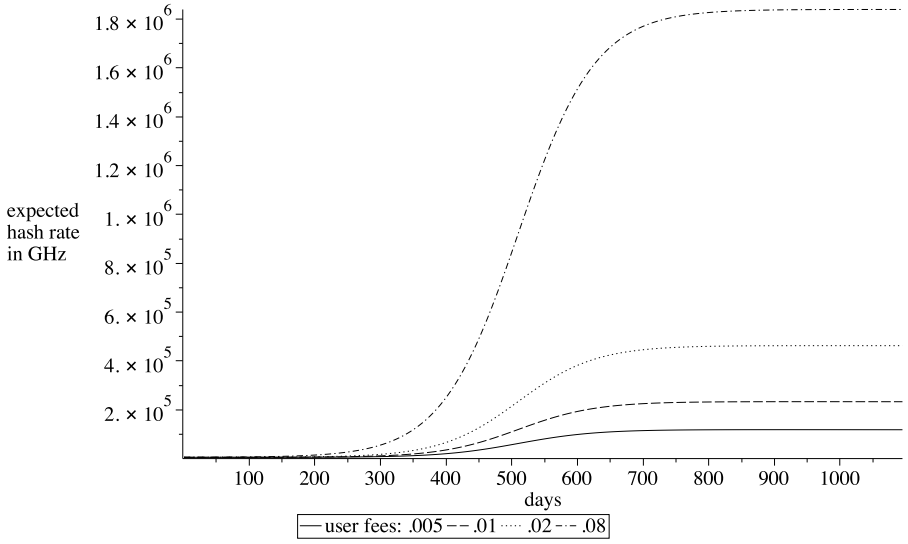


Рисунок 9

Мощность хеширования с течением времени в зависимости от средней комиссии

Поскольку майнеры конкурируют за создание блоков и несут значительные затраты на вычислительную мощность, ожидаемые доходы напрямую связаны с готовностью майнеров предоставить хэш-мощность. По текущим ценам майнеры получают в среднем $ 12,5 за гигагерц хэш-мощности. [14] Рисунок 9 передает рисунок 7, связывая мощность хэширования, которую майнеры были бы готовы предоставить с учетом прогнозируемого вознаграждения за майнинг.

Наконец, мы покажем, как инфляция, связанная с вознаграждением за блок и выплатой процентов, влияет на доход от майнинга. На рисунке 10 показан средний доход от майнинга как функция вознаграждения за блок, измеренная через инфляцию блока. Мы строим кривые для первого года (все средне-серые линии), затем для второго-пятого кварталов (черные) и с третьего по шестой квартал (светло-серые). Мы используем процентные платежи в размере 1%, 5% и 10% и среднюю комиссию в размере 0,01 доллара США. Принятие основано на уровнях принятия Ethereum (*ты* ETH). Цифра указывает

[14] Для получения этого числа мы используем данные из etherscan.io от общей суточной мощности хэширования сети и средней доходности блока.

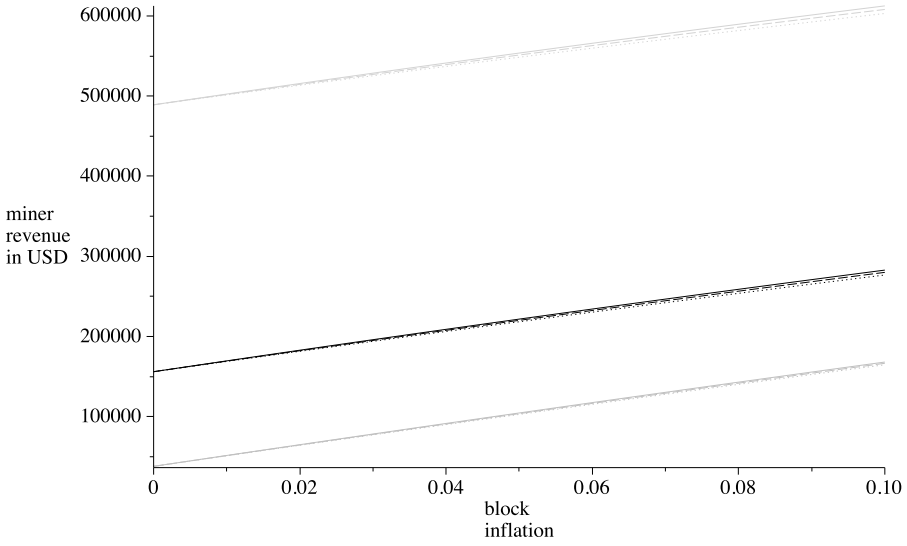


Рисунок 10.
Средний доход и инфляция блока

эти вознаграждения за блок оказывают значительное влияние на доход майнеров, в то время как процентная ставка имеет ограниченное влияние.

Рисунок 11 подтверждает эти последние выводы. На этом рисунке показана зависимость среднего дохода от добычи полезных ископаемых от процентной ставки. Мы снова строим кривые для первого года (все средне-серые линии), затем для второго-пятого кварталов (черные) и, наконец, с третьего по шестой квартал (светло-серые). Для этого мы используем ставки инфляции 1%, 5% и 10% и среднюю комиссию 0,01 доллара США. Принятие снова основано на уровнях принятия Ethereum (*ты* ETH). Линии по существу плоские, как показано на предыдущих рисунках, просто потому, что доход майнера от процентной ставки настолько мал. Мы пришли к выводу, что на раннем этапе вознаграждения за блоки играют наиболее важную роль в доходе майнеров вначале, тогда как при достижении определенного уровня внедрения комиссии с пользователей будут наиболее важным источником дохода. Однако мы подчеркиваем, что это не означает, что интерес не имеет значения для решений пользователей.

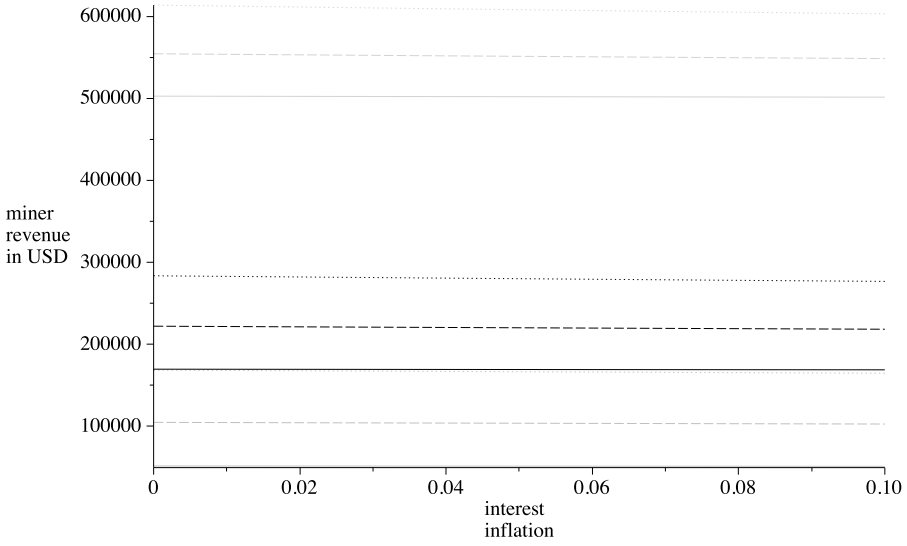


Рисунок 11.

Средний доход и процентные ставки

Вместо этого будет много пользователей, каждый из которых должен будет заплатить небольшую, но, возможно, значительную неявную плату за хранение данных в сети.

VI. Экономические ограничения против атак

В этом разделе мы исследуем пределы сети Conflow при двух различных атаках: атаке с самодостаточным майнингом и атаке с двойным расходом.

A. Атаки на добычу полезных ископаемых

Если участник Биткойна владеет более 23,21% вычислительной мощности сети, он может получить больше прибыли от майнинга, стратегически удерживая добытый блок на определенный период времени, прежде чем транслировать его в сеть (Сапирштейн, Сомполинский и Зохар, 2015). Это потому, что Биткойн дает вознаграждение только за блоки в самом длинном

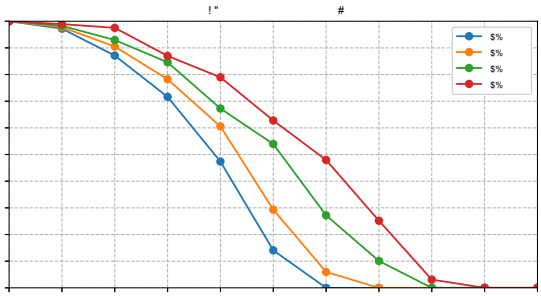


Рисунок 12.

Штраф злоумышленников при различных соотношениях мощности генерации блоков у злоумышленников.

(A)

цепь. Когда она удерживает недавно добытый блок, у нее есть исключительная привилегия на майнинг под своим новым блоком, который на данный момент является самой длинной цепочкой. Конечно, удержание блока влечет за собой риск того, что кто-то другой может одновременно добыть новый блок, чтобы стать новой самой длинной цепочкой, но исследование показывает, что если участник имеет более 23,21% вычислительной мощности сети, выгода от удержания перевешивает риск; см. Сапирштейн, Сомполинский, Зохар (2015). Поскольку майнинг биткойнов - это игра, в которой победитель получает все, честные майнеры ожидают получить меньшее вознаграждение по сравнению с их вычислительной мощностью, когда эгоистичный участник запускает такие атаки справедливости.

Conflux более устойчив к атакам самодостаточного майнинга, потому что удержание блока приводит к меньшему вознаграждению. В отличие от Биткойна, все блоки получают вознаграждение в потоке, а вознаграждение за блок дисконтируется из-за его размера антиконуса. Удержание блока предотвратит обращение к нему в будущих новых блоках. Следовательно, он увеличивает размер антиконуса блока и, следовательно, уменьшает вознаграждение за блок. Учитывая рациональность всех участников сети, честный майнинг совместим со стимулами.

На рисунке 12 представлены наши экспериментальные результаты, чтобы проиллюстрировать устойчивость Conflux к атакам самодостаточного майнинга. Мы запускаем симуляцию сети Conflux с 10000 узлами. Один из них - злоумышленник, который задерживает сгенерированный ею блок на определенный период времени. В моделировании обычные узлы имеют сетевую задержку (в среднем 4,1 секунды). Однако злоумышленник имеет возможность мгновенно получить и отправить свой блок всем остальным узлам. Мы запускаем моделирование для 2000 блоков и измеряем соотношение вознаграждения, которое получает злоумышленник, по сравнению с обычной честной стратегией для последних 1000 блоков при разной мощности генерации блока и периоде удержания блока. Наши результаты показывают, что злоумышленник постоянно получает меньшее вознаграждение, чем при обычной честной стратегии (т. Е. Коэффициент вознаграждения меньше 1). Чем дольше она удерживает блоки, тем меньше награды она получит. Большая вычислительная мощность поможет злоумышленнику получить больше вознаграждения, но даже с 40% вычислительной мощности всей сети злоумышленник все равно получит больше вознаграждения, если он просто будет честно участвовать в сети.

Б. Атаки с двойным расходом

В нескольких работах в экономической литературе подчеркивается, что сети PoW сталкиваются с фундаментальными ограничениями с точки зрения экономических стимулов, которые могут поддерживать постоянную безопасность сети (Auer 2019). Сеть Conflux ничем не отличается, но в дальнейшем мы утверждаем, что ограничения Conflux «слабее» по сравнению с существующими сетями. В этом разделе мы накладываем ограничение, заключающееся в том, что злоумышленник не может реверсировать криптографические функции, поэтому честные майнеры ведут себя правильно даже в присутствии злоумышленника. Мы фокусируемся на атаках с двойным расходом и самодостаточном майнинге через удержание блоков.

Сначала мы повторим аргументы из Budish (2018), которые применимы к последовательным блокчейнам. Мы предполагаем, что добыча каждого блока требует затрат c (включая физическое оборудование и электричество) и что есть N идентичные майнеры, которые соревнуются. Для сценария с незначительной комиссией пользователей самый значительный доход - это вознаграждение за блок. B за блок. Ограничение участия майнеров требует, чтобы ожидаемая прибыль превышала ожидаемые затраты, то есть:

$$\text{вероятность выигрыша блока} \times B \geq \text{Стоимость} \Leftrightarrow B / N \geq c.$$

Это условие выполняется для всех идентичных майнеров, и в равновесии оно должно утверждать, что совокупные затраты на майнинг согласуются с совокупной выгодой:

$$c \times N = B. \tag{16}$$

Теперь предположим, что злоумышленник хочет дважды потратить ценную транзакцию. $V.$ Атака происходит в том смысле, что злоумышленник выстраивает альтернативную цепочку быстрее, чем все оставшиеся майнеры. Предположим, что для получения 50% власть, злоумышленник должен заплатить $c \times N,$ и чтобы получить большинство, они должны платить сверх этого. Если злоумышленник тратит $A \times c \times N$ на оборудовании, с A> 1, они получают преимущество $A / (A +$ 1)> 50%; больший $A,$ тем больше преимущество (и, следовательно, тем быстрее они закончат атаку). За успешную атаку они получают ценность $V,$ это сумма, которую они могут потратить вдвое. Предположим, что при условии преимущества оборудования $A,$ занимает τ блоки (в ожидании) для завершения атаки, что создает более длинную цепочку, чем цепочка, которую совместно генерируют честные майнеры. Тогда стоимость атаки составит:

$$\tau \times A \times c \times H.$$

Однако в случае успеха атакующий получает не только значение атаки. V но и награды за τ блоки. Следовательно, чтобы атаки были *непривлекательный,* он должен утверждать, что:

$$\tau \times A \times c \times N > V + t \times Б. \quad (17)$$

Используя уравнение (16), получаем следующее:

$$\tau \times B\,(A - 1) > B. \quad (18)$$

Следовательно, для ожидаемого времени атаки τ, существует ценность V такое, что для всех $V > V$, $\tau \times B\,(A - 1) = V < V$, и сделка стоимости V не может быть обеспечен. Неравенство (18) является жестким ограничением экономики (и безопасности) последовательной цепочки, такой как Биткойн.

Поток подчиняется другой нижней оценке для V. Во-первых, чтобы быть успешным в атаке, альтернативные цепи атакующего должна стать стержнем цепи. Поскольку любая эпоха может содержать несколько блоков, злоумышленнику необходимо не только создавать блоки быстрее, но и создавать «тяжелую» цепочку, для чего потребуется относительно больше времени (и, следовательно, больше ресурсов). Чтобы упростить рассуждение, мы абстрагируемся от этой проблемы и, как и раньше, предполагаем, что честная цепочка содержит один блок на эпоху.

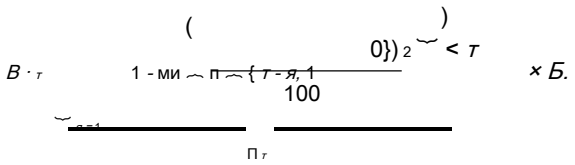
Затем при создании альтернативной цепочки злоумышленник не получает полное вознаграждение, потому что вознаграждение за блок назначается на основе относительного положения в антиконусе блока в следующем 10 эпох. Как и раньше, предположим, что атака успешна после τ периодов, и в системе есть один злоумышленник. Тогда первый блок атакующего в альтернативной цепочке имеет антиконус размером $\min\{\tau - 1, 10\}$, второй из $мин\{\tau - 2, 10\}$,

и так далее. Таким образом, вознаграждение за блок a так как начало атаки

B × (1 - (min { *τ* - *a,* 10} / 100) 2) предполагая фиксированное вознаграждение за блок *Б.* На самый долгий

цепь (теперь поворотный чай ∑ (п) длины *τ* с начала атаки злоумышленник будет

поэтому зарабатывайте:



Используя тот же аргумент, что и выше, и, следовательно, экономическое ограничение для Con fl ux становится следующим:

$$B\,(tA - \Pi_{t}) > V \tag{19}$$

Другими словами, существует значение *V* ·такое, что для всех *V* ∈ *(V, V*]*,* имеет место следующее:

$$B\,(tA - \Pi_{t}) V > B\,(tA - \tau)$$

Значение этой связи состоит в том, что набор значений транзакции *V* которые могут быть защищены в сети Conflow, строго больше, чем в «традиционных» последовательных блокчейнах, таких как Биткойн.

VII. Модель затрат на хранение в потоке

В этом разделе мы разработаем простую модель, чтобы понять правила стоимости хранения в Conflux. Мы начнем с наблюдения, что у пользователей есть выбор между использованием сервиса в Conflux или альтернативной технологией. Последний не обязательно должен быть альтернативной цепочкой блоков, но может быть, например, финансовой услугой или вычислительной услугой в традиционной экономике. Пользователи в этой модели для всех практических целей - это разработчики, использующие Conflux в качестве инфраструктуры. В нашей теоретической модели мы абстрагируемся от многих сложностей, таких как колебания цен и других внешних факторов.

вне контроля сети, и сосредоточьтесь на двух группах составляющих: майнерах и пользователях. В явной форме модель не рассматривает хранение CFX в спекулятивных целях.

Мы пишем модель в статической форме с неявным предположением о стабильном исходе. Например, мы предполагаем, что есть существующие пользователи, которые платят за хранилище, так что майнеры получают вознаграждение за хранилище.

А. Горняки

Эта часть нашей модели вдохновлена Хэ, Тан и Ван (2019). [15] Майнеры покупают или арендуют оборудование для майнинга, и они несут затраты на блок для майнинга и хранения данных, таких как электричество и оборудование; обозначим эти затраты c как в предыдущем разделе. Майнеры не являются стратегическими (т. Е. Они берут цены) и идентичны.

Майнеры получают доход из трех источников: вознаграждение за блок B новых токенов, комиссионных сборов и процентов за пользовательское хранилище, *Я.* Мы измеряем эти предметы в токенах Conflow и используем $п$ для обменного курса денег на токен (т. е. цены токена в долларах США); как следствие, $п \cdot B$ доход майнера от получения вознаграждения за блок

Б. В нашем анализе здесь мы абстрагируемся от комиссий за транзакции, чтобы упростить изложение.

Когда пользователи потребляют количество *Икс* полезности блокчейна (например, исполнение контрактов, игровые транзакции, все измеряется в единицах токенов), им необходимо указать дробную часть q (определяется системой) токенов, т. е. $\beta \times Икс$, в таможенное хранилище. Эти токены (как и все другие токены в системе) получают проценты. $\beta \times Икс \times p_c$, куда p_c - скорость инфляции, устанавливаемая системой. Как мы указали выше, эта выплата процентов распределяется среди майнеров.

[15] Они используют стандартную экономическую модель для анализа жизнеспособности цепочки биткойнов в отсутствие вознаграждения за блок, что аналогично нашему анализу.

Мы предполагаем, что майнеры идентичны по мощности хэширования, которую они предоставляют. Следовательно, у них равные шансы на добычу блока. Есть свободный вход в майнинг, а значит, и совокупный хешрейт *ЧАС* сродни общему количеству майнеров. Если майнеры используют мощность хэширования *час,* они выигрывают блок случайно *ч / ч.* Поскольку майнеры идентичны, мы устанавливаем $h = 1$ для упрощения обозначений. В конкурентной добыче полезных ископаемых баланс затрат выгоден и, следовательно,

$$c = \frac{1}{ЧАС} \times p\,(B + I) \Leftrightarrow H = \frac{p\,(B + I)}{c}. \tag{20}$$

Б. Пользователи блокчейна

Пользователи выделяют в общей сложности *ш* к конкретной услуге, которую предоставляет блокчейн или его альтернатива. Таким образом, анализ представляет собой частичное равновесие, потому что мы начинаем, когда пользователь уже принял решение выделить определенную часть своего бюджета на эту услугу. Пользователь выбирает количество обычных и специальных товаров (также называемых блокчейном), чтобы максимизировать свою полезность. Обозначим потребление нормальных товаров *с* и запрошенный сервис блокчейна *Икс* измеряется в CFX. Наше неявное предположение состоит в том, что все потребление происходит (или, скорее, оно оценивается пользователем) в валюте, и поэтому пользователь потребляет *п × Икс* блокчейна хороши в этом сражении.

Принимая решение использовать товар на блокчейне, пользователю необходимо получить токены для прямой оплаты и дополнительно *β × Икс* жетоны для размещения на таможенном складе.

По истечении одного периода пользователи потребляют остаточную сумму, которая находилась на таможенном складе, в виде альтернативного товара. [16] Поскольку цепочка Confux создает новые токены в промежуточный период, покупательная способность этих токенов (*т.е.* стоимость измеренных жетонов

[16] Вдохновением здесь послужила модель перекрывающихся поколений, в которой пользователь может потреблять один вид товаров только в молодом возрасте.

inf at) отклоняется, и сохраненные токены стоят только $п \times \beta \times Икс/(1 + p_{в)}$, измеряется в сегодняшних ценах. Здесь, $п/(1+ p_{в)}$ это действительно завтрашняя цена CFX. Более того, будущее потребление дисконтируется по ставке $\delta < 1$. [17]

Майнеры получают проценты от связанного хранилища, где мы неявно предполагаем стационарное равновесие в том смысле, что во время формирования блока прошлый (репрезентативный) пользователь поместил в хранилище эквивалентное количество токенов, что и текущий пользователь. Блоки производятся по ставке $б$ за общий горизонт хранения, обычно 1 год, если мы используем годовые ставки для δ и $p_{с.}$ Следовательно,

$$I = \beta x \times p_{с} \times б.$$

Майнеры обеспечивают безопасность цепочки, и мы предполагаем, что безопасность цепочки увеличивается с увеличением скорости хеширования. *ЧАС.* Безопасность становится актуальной для потребления второго периода в том смысле, что это потребление происходит с вероятностью. Pr (безопасный | $H) = \mu (H), \mu \in [0, 1)$,

$\mu' > 0$, $\mu'' < 0$.

Мы предполагаем следующую аддитивную форму функции полезности пользователя:

$$U (с, х) = и_{с (} в) + и_{б (} Икс \times р) + \delta \text{ E } [ты_{с (} \beta \times Икс \times п/(1 + p_{в))} | ЧАС], \quad (21)$$

с $ты' > 0$, $ты'' < 0$ и E [$ты_{с]} = f (H) и_{с.}$ Бюджет потребления пользователя $с,$ токены для использования $Икс,$ и жетоны для таможенного хранения βx должен удовлетворять:

$$с + хр + \beta хр \leq ш. \quad (22)$$

[17] В конкурентном равновесии реальная процентная ставка $р$ на денежном рынке фиксирует дисконтирование времени, а затем $\beta = 1 / (1 + p)$.

Взятые вместе, пользователь максимизирует свою полезность, выбирая хорошее потребление блокчейна как

$$\max_{Икс} U(x) = и_{с}(ш - хр(1+\beta)) + и_{б}(Икс \times р) + \delta f(Н)\, и_{с}(\beta \times Икс \times п/(1+р_{в})). \quad (23)$$

Решение этой проблемы максимизации равно:

$$0 = -п(1+\beta)\, и'_{с} + пу'_{б} + \delta f(Н)\, и'_{с}\, \beta \times п/(1+р) \Leftrightarrow 1+\beta \left(1 - \frac{\delta f(Н)}{1+р_{с}}\right) \text{ знак равно } \frac{ты'_{б}}{ты'_{с}}$$

C. Клиринг на равновесном рынке

Общее количество находящихся в обращении монет составляет $M > 0$. Чтобы упростить анализ, без потери общности здесь мы предполагаем одного репрезентативного потребителя, который ведет себя как покупатель. В состоянии равновесия рынок должен быть очищен таким образом, чтобы:

$$Икс^{*}(1+\beta) = M$$

Таким образом, пользователи должны выбрать количество токенов, $Икс^{*}$, что максимизирует их полезность, и майнеры должны выбирать хешрейт безубыточности $ЧАС^{*}$.

D. Иллюстрация равновесия и сравнительная статика

В качестве простого примера функции полезности потребления логарифмическая функция $ты_{с}(в) = \ln(в)$ и для $ты_{б}(в) = \theta \cdot \ln(в)$. Затем возникают условия равновесия

$$п^{*} = \frac{w\,\delta\theta + f(Н)}{M\,\delta\theta + f(Н) + 1}, \quad (24)$$

и равновесная величина

$$Икс^{*} = \frac{ш}{п^{*}} \frac{1}{1 + \beta} \frac{\delta\theta + f(H)}{\delta\theta + f(H) + 1}, \tag{25}$$

а для хешрейта

$$H = \frac{п^{*}(B + \beta r_{c} Икс^{*})}{C}, \tag{26}$$

при нормализации $б$ к 1.

Количество $ш$ можно интерпретировать как общий размер экономики, которую блокчейн пытается заменить, и $ж/п$ - это размер экономики, измеренный в токенах. Формулировка линейной логической полезности гарантирует, что скорость хеширования и скорость инфляции не влияют напрямую на выбор пользователя. Неявно, скорость инфляции и необходимое связанное хранилище β и

p_{c} имеют схожие эффекты, поскольку оба повышают стоимость для пользователя, и интуитивно понятно, что одного достаточно в качестве переменной политики.

Из приведенных выше условий равновесия мы можем получить путем дифференцирования переменных равновесия некоторые эффекты первого порядка.

1. Скорость хеширования и спрос положительно связаны и положительно усиливают. (например, увеличивается потребность в скорости хэширования, а скорость хеширования увеличивается в спросе).

2. Увеличение денежной базы снижает цену.

3. Повышение рыночной процентной ставки (снижение $б$) снижает спрос.

4. Увеличение скорости инфляции потока приводит к увеличению скорости хеширования и, следовательно, к увеличению цены токена (мы отмечаем, что майнеры не учитывают стоимость хранения токенов - неявное предположение состоит в том, что они немедленно конвертируют токены в токены. оплатить свои расходы).

5. Увеличение денежных средств, выделяемых на деятельность, подобную блокчейну, или увеличение пользовательских предпочтений в отношении товаров блокчейн (увеличение $ш$ или же θ) увеличивает цену и хешрейт.

6. Ужесточение требования о неволе. β напрямую снижает спрос, но увеличивает скорость хеширования. Общая сумма не определена и зависит от относительного размера совокупного предельного дохода от хранения, $M \cdot p_{c,}$ и награда за блок $Б.$

VIII. Вывод

Блокчейны с подтверждением работоспособности должны быть тщательно спроектированы, чтобы создавать надлежащие стимулы для пользователей, участвующих и осознанно использующих свои ресурсы: майнеры должны быть готовы защищать сеть, а пользователи / разработчики должны быть заинтересованы в использовании сервисов блокчейн. В этой статье описывается, как создание сети Conlux Network, высокопроизводительного блокчейна с доказательством выполнения работы, приводит к разумным экономическим стимулам, которые поддерживают социально желательное поведение. В этой статье мы параметризуем уровень дохода и, следовательно, безопасность сети, которую Conflow может генерировать, и описываем, как это зависит от поведения пользователя и «переменных политики», таких как блокировка и инфляция интереса. Мы также обсуждаем, как лежащая в основе экономическая инженерная разработка расширяет сеть Conflow за пределы унаследованных блокчейнов PoW.

Мы подчеркиваем, что мы описываем наше понимание экономических эффектов, которые порождает проектирование сети. Однако мы не знаем, как в конечном итоге будут вести себя пользователи.

Есть некоторые вопросы, выходящие за рамки этого текста. Например, еще предстоит определить, как будут работать сообщество, экосистема и государственные фонды. Можно представить, что все они сольются. Хотя в системе есть положения

Голосование типа DAO, соответствующие фонды еще не созданы. В конечном итоге протокол требует дальнейшего развития, и потребуется обслуживание сетевых компонентов. Можно вообразить и желательно, чтобы Conflux создал регулярный источник дохода для поддержки долгосрочной жизнеспособности разработки протоколов. Одним из примеров является отвлечение минимальной части платежей за газ из транзакций в фонд, аналогично налогу на добавленную стоимость.

РЕКОМЕНДАЦИИ

Ауэр, Рафаэль, 2019, Помимо экономики конца света «доказательства выполнения работы» в криптовалюте. Заявления, Документ для обсуждения, Рабочие документы BIS № 765.

Бакос, Яннис и Ханна Халабурда, 2018, Роль криптографических токенов и ICO в содействии внедрению платформы, Рабочий документ Нью-Йоркского университета https://ssrn.com/abstract=3207777.

Будиш, Эрик Б., 2018, Экономические пределы биткойна и блокчейна, Chicago Booth Научный доклад № 18-07 Чикагского университета https://ssrn.com/abstract=3197300.

Канидио, Андреа, 2018, Финансовые стимулы для разработки с открытым исходным кодом: пример блокчейн, Рабочий документ IMT Lucca, INSEAD.

Чиу, Джонатан и Торстен В. Кеппл, 2017 г., Экономика криптовалюты. tocurrencies - биткойны и не только, Рабочий документ Queens University https://ssrn.com/abstract=3048124.

Конг, Линь Уильям, Е Ли и Нэн Ван, 2018 г., Токеномика: динамическое принятие и оценка, Рабочий доклад № 2018-49 Институт экономических исследований им. Беккера Фридмана https://ssrn.com/abstract=3222802.

Эяль, Иттай и Эмин Ган Сирер, 2013 г., Большинства недостаточно: майнинг биткойнов уязвимый, .

Фиш, Кристиан, 2019, Первоначальные предложения монет (ICO) для финансирования новых предприятий, *Журнал Деловое венчурное дело* 34, 1–22.

He, Ping, Dunzhe Tang и Jingwen Wang, 2019, блокчейн Proof-of-Work (pow) сеть и ее жизнеспособность в качестве платежной системы, Рабочий документ Университета Цинхуа https://ssrn.com/abstract=3441605.

Ли, Чэньсин, Пэйлунь Ли, Дун Чжоу, Вэй Сюй, Фань Лонг и Эндрю Яо, 2018, Масштабирование консенсуса Накамото до тысяч транзакций в секунду,.

Ли, Чэньсин и Гуан Ян, 2020, Спецификация протокола Conflux,.

Ли, Цзясун и Уильям Манн, 2018, Первоначальное предложение монет и создание платформы, Рабочий документ Университета Джорджа Мейсона https://ssrn.com/abstract=3088726.

Сапирштейн, Айелет, Йонатан Сомполинский и Авив Зохар, 2015, Оптимальная самодобыча стратегии в биткойнах,.

Times, статистика, 2019, прогнозируемый рейтинг ввп, данные получены из http: // statisticstimes.com/economy/projected-world-gdp-ranking.php.