

Интерактивные доказательства мошенничества: секретный соус Arbitrum

Теперь, когда Arbitrum One открыт в основной сети, мы собираемся опубликовать несколько статей о внутреннем устройстве Arbitrum. Этот пост представляет собой отрывок из Inside Arbitrum, нашего подробного описания того, как работает Arbitrum.

Среди оптимистичных объединений наиболее важным дизайнерским решением является способ разрешения споров. Предположим, Алиса утверждает, что цепочка даст определенный результат, а Боб не согласен. Как протокол будет решать, какую версию принять?

По сути, есть два варианта: интерактивное доказательство или повторное выполнение транзакций. Arbitrum использует интерактивное доказательство, которое, по нашему мнению, является более эффективным и гибким. Большая часть конструкции Arbitrum вытекает из этого факта.

Мы работаем над интерактивными доказательствами мошенничества (и Arbitrum) с 2014 года. Основной механизм был описан в нашей научной статье 2018 года, хотя с тех пор мы значительно его усовершенствовали.

Интерактивное доказательство

Идея интерактивного доказательства заключается в том, что Алиса и Боб будут использовать двусторонний протокол, регулируемый контрактом L1, для разрешения своего спора с минимальной работой, требуемой для любого контракта L1.

Подход Арбитра основан на рассмотрении спора. Если заявка Алисы охватывает N шагов исполнения, она публикует две заявки размером $N/2$, которые в совокупности дают ее первоначальное утверждение из $N/2$ шагов, а затем Боб выбирает для оспаривания одно из утверждений Алисы, состоящих из $N/2$ шагов. Теперь размер спора сократился вдвое. Этот процесс продолжается, сокращая спор пополам на каждом этапе, пока они не разойдутся во мнениях по поводу одного этапа исполнения. Отметим, что арбитра L1 пока не приходилось думать о казни «по существу». Только после того, как спор сведен к одному шагу, рефери L1 должен разрешить спор, проверив, что на самом деле делает инструкция и правильно ли утверждение Алисы по этому поводу.

Ключевой принцип интерактивного доказательства заключается в том, что если Алиса и Боб находятся в споре, Алиса и Боб должны выполнить как можно больше работы вне сети, необходимой для разрешения их спора, а не помещать эту работу в контракт L1.

Повторное выполнение транзакций

Альтернативой интерактивному доказательству было бы наличие сводного блока, содержащего заявленный хеш состояния машины после каждой отдельной транзакции. Затем, в случае возникновения спора, рефери L1 будет эмулировать выполнение всей транзакции, чтобы увидеть, соответствует ли результат утверждению Алисы.

Почему интерактивное доказательство лучше

Мы твердо убеждены, что интерактивное доказательство является лучшим подходом по следующим причинам.

Более эффективно в оптимистическом случае: поскольку интерактивное доказательство может разрешать споры, превышающие одну транзакцию, оно может позволить сводному блоку содержать только одно утверждение о конечном состоянии цепочки после всего выполнения, охватываемого блоком. Напротив,

повторное выполнение требует публикации заявления о состоянии для каждой транзакции в сводном блоке. Учитывая сотни или тысячи транзакций на объединенный блок, это существенная разница в объеме L1, а объем L1 является основным компонентом стоимости.

Более эффективно в пессимистическом случае: в случае возникновения спора интерактивное доказательство требует, чтобы договор судьи L1 был только для проверки того, что действия Алисы и Боба «имеют правильную форму», например, что Алиса разделила свою N-шаговую претензию на две претензии. вполнину меньше. (Рецензенту не нужно оценивать правильность утверждений Алисы — это делает Боб, вне цепочки.) Необходимо повторно выполнить только одну инструкцию. Напротив, повторное выполнение требует, чтобы судья L1 имитировал выполнение всей транзакции.

Гораздо более высокий лимит газа на одну транзакцию: интерактивное доказательство может выйти за рамки жесткого лимита газа на транзакцию Ethereum; На Arbitrum возможна транзакция, требующая столько газа, что она даже не поместится в блок Ethereum. По понятным причинам лимит газа не бесконечен, но он может быть намного больше, чем на Ethereum. Что касается Ethereum, то единственным недостатком трудоемкой транзакции Arbitrum является то, что она может потребовать интерактивного доказательства мошенничества с немного большим количеством шагов (и только в том случае, если она действительно является мошеннической). Напротив, повторное выполнение должно налагать более низкий лимит газа, чем Ethereum, поскольку должна быть возможность эмулировать выполнение транзакции (что дороже, чем ее непосредственное выполнение) в рамках одной транзакции Ethereum.

Нет ограничений на размер контракта: интерактивное доказательство не требует создания контракта Ethereum для каждого контракта L2, поэтому не требуется, чтобы контракты

соответствовали ограничению размера контракта Ethereum. Что касается спорных контрактов Arbitrum, то развертывание контракта на L2 — это всего лишь еще один этап вычислений, такой же, как и любой другой. Напротив, подходы с повторным выполнением должны налагать меньший предел размера контракта, чем Ethereum, поскольку они должны иметь возможность инструментировать контракт, чтобы эмулировать его выполнение, а полученный инструментированный код должен вписываться в один контракт Ethereum.

Большая гибкость реализации: интерактивное доказательство обеспечивает большую гибкость реализации, например, возможность добавлять инструкции, которых нет в EVM. Все, что необходимо, — это возможность проверить одноэтапное доказательство на Ethereum. Напротив, подходы к повторному выполнению привязаны к ограничениям EVM.

Интерактивное доказательство определяет дизайн Arbitrum

Большая часть конструкции Arbitrum обусловлена возможностями, открывающимися при интерактивном доказывании. Если вы читаете о какой-то функции Arbitrum и задаетесь вопросом, почему она существует, можно задать два хороших вопроса: «Как это поддерживает интерактивное доказательство?» и «Какие преимущества интерактивного доказательства?» Ответы на большинство вопросов «почему» в отношении Arbitrum относятся к интерактивному прувингу.

Хотите узнать больше? Посмотрите Inside Arbitrum.