Augur: децентрализованный оракул и платформа для рынков предсказаний

Джек Петерсон (Jack Peterson), Йозеф Крюг (Joseph Krug), Мика Золту (Micah Zoltu),
Остин Уильямс (Austin K. Williams) и Стефани Александер (Stephanie Alexander)
Forecast Foundation
(5 марта 2018 года)

Augur – это не требующий доверия децентрализованный оракул и платформа для рынков предсказаний. Исходы рынков предсказаний Augur определяются пользователями, которые ставят выпускаемые платформой и принадлежащие им токены Reputation на актуальный для данного момента времени прогнозируемый результат и получают от рынков выплаты на основании принятого решения об исходе события. Структура стимулов в Augur выстроена таким образом, чтобы добросовестные и точные сообщения об исходе события во всех случаях являлись для держателей токенов Reputation наиболее выгодным вариантом. Для того чтобы оспорить определенный рынком исход события, держатели токенов могут пошагово увеличивать сумму своего залога в токенах Reputation. Если совокупный размер этих залогов достигает определенного порогового значения, то токены Reputation разделяются на несколько версий – по одной для каждого возможного исхода спорного рынка. В таком случае их держатели должны будут обменять свои токены Reputation на одну из этих версий токенов. Те версии Reputation, которые не соответствуют исходу события в реальном мире, утратят свою ценность, так как никто не станет участвовать в рынках предсказаний, если не будет уверен в точности и справедливости решений рынков об исходе событий. Следовательно, держатели токенов будут выбирать единственную версию токенов Reputation, которая, по их мнению, будет иметь ценность в будущем – ту версию, которая соответствует действительности.

Augur – это не требующий доверия децентрализованный оракул и платформа для рынков предсказаний. На рынке предсказаний люди могут спекулировать на исходах будущих событий; те, чей прогноз оправдается, получат денежный выигрыш, а те, чей прогноз окажется неточным, потеряют деньги [1–3]. Цена рынка предсказаний может служить точным и хорошо откалиброванным индикатором того, насколько велика вероятность наступления того или иного события в реальности [4–7].

С помощью Augur люди получат возможность торговать на рынках предсказаний по очень низким ценам. Единственные существенные расходы, которые покрываются за счет комиссий, это компенсации создателям рынка и пользователям, которые сообщают об исходе определяющего рынок события после того, как оно произошло. Результатом является рынок предсказаний, на котором требования к доверию, возможные препятствия и комиссии будут настолько низкими, насколько это возможно без потери функциональности рынка.

Исторически рынки предсказаний были централизованными. Самый простой способ агрегировать сделки на рынке предсказаний – это реестр, поддерживаемый заслуживающей доверия стороной. Аналогичным образом, самый простой способ определения исхода события и распределения выплат трейдерам – это беспристрастный доверенный арбитр, определяющий исходы рынков. Однако централизованные рынки предсказаний несут в себе множество рисков и ограничений: они не допускают глобального участия, они ограничивают типы рынков, которые могут быть созданы и на которых может вестись торговля, а также они требуют от трейдеров доверия к оператору рынка в том, что он не украдет их средства и правильно определит исход рынка.

Augur стремится сделать процесс определения исхода события полностью децентрализованным. Децентрализованные, не требующие доверия сети, такие как Bitcoin[8] и Ethereum[9], устраняют риск перехода личной заинтересованности в коррупцию или воровство. Единственная роль разработчиков Augur заключается в публикации смарт-контрактов в сети Ethereum. Контракты Augur полностью автоматизированы: разработчики не могут потратить внесенные на счет контракта средства, повлиять на результаты рынков, одобрять или отклонять сделки или другие транзакции в сети, не могут отменять сделки постфактум, изменять или отменять ордера пользователей и т. д. Оракул Augur позволяет переносить информацию из реального мира в блокчейн, не полагаясь на доверенных посредников. Augur станет первым в мире децентрализованным оракулом.

I. КАК AUGUR РАБОТАЕТ

Жизненный цикл рынков Augur состоит из четырех этапов: *создание*, *торговля*, *репортинг* (сбор сообщений об исходе события) и *расчет*. Любой пользователь может создать рынок, основанный на любом реальном событии. Торговля начинается сразу после того, как рынок создан. Все пользователи могут торговать на любом рынке платформы. После того как событие, на котором основан рынок, происходит, оракул Augur определяет его исход. После того как исход события определен, трейдеры могут закрыть свои позиции и получить выплаты.

У платформы Augur есть собственный токен, Reputation (REP). REP нужны создателям рынков и репортерам, когда они сообщают об исходах рынков, созданных на платформе Augur. Репортеры сообщают о результате, ставя свои REP на один из возможных для рынка исходов. Тем самым репортер заявляет, что исход, на который он поставил свои деньги, соответствует действительному исходу события, которое послужило основой для рынка. В целях определения исхода рынка, консенсус его репортеров признается "истиной". Если отчет об исходе рынка одного или нескольких репортеров не совпадает с консенсусом, достигнутым другими репортерами, Augur перераспределяет REP, поставленные меньшинством репортеров на неконсенсусный исход, между теми репортерами, которые пришли к консенсусу относительно исхода рынка.

Держателям REP, принимающим участие в процессе репортинга и сообщающим точные сведения об исходах событий, выплачивается часть от собираемых платформой комиссий. Каждый поставленный токен REP дает своему владельцу право на получение соразмерной доли от комиссий Augur, собранных на соответствующем рынке. Чем больше REP есть у репортера, тем большую награду он может получить за свой вклад в обеспечение безопасности платформы, сообщая о правильных исходах рынков.

Хотя токены REP играют центральную роль в операциях на платформе Augur, для торговли на рынках платформы они не используются. Для трейдеров никогда не будет прямой необходимости владеть или пользоваться токенами REP, так как им необязательно принимать участие в процессе репортинга.

Рисунок 1. Упрощенная схема жизненного цикла рынка предсказаний.

A. Создание рынка

Augur позволяет любому пользователю создать рынок на основе любого предстоящего события. *Создатель рынка* устанавливает *время окончания события* и выбирает *назначенного репортера*, который должен будет сообщить об исходе события. Назначенный репортер не принимает решение об исходе рынка единолично. У сообщества всегда есть возможность оспорить и скорректировать отчет назначенного репортера.

Следующим шагом создатель рынка выбирает *источник решения*, который репортеры должны использовать для определения исхода. Источником решения может быть как просто "общеизвестный факт", так и конкретный источник, например, Министерство энергетики США, bbc.com или адрес определенной конечной точки API.[1] Создатели рынков также устанавливают размер комиссии, выплачиваемой создателю рынка трейдерами, которые соглашаются с контрактом рынка (подробнее о комиссиях в разделе I D). Наконец, создатель рынка размещает два залога: *залог на валидность* и *залог на случай бездействия назначенного репортера* (для краткости называемый также *залогом на бездействие*).

Залог на валидность удерживается в ETH и возвращается создателю рынка при любом исходе рынка за исключением тех случаев, когда рынок признается недействительным.[2] Залог на валидность мотивирует участников создавать рынки на основе четко определенных событий, подразумевающих объективный и недвусмысленный исход. Размер залога на валидность определяется динамически, исходя из доли[3] недопустимых исходов на недавних рынках.

Залог на бездействие состоит из двух частей: *gas-залог на бездействие* (пополняется в ETH) и *REP-залог на бездействие* (пополняется в REP). Эти залоги возвращаются создателю рынка, если назначенный репортер этого рынка сообщил об исходе события в течение трех дней после обозначенного времени окончания события. Если назначенный репортер не предоставит свой отчет в течение отведенного для этого 3-дневного периода, то создатель рынка лишается залога на бездействие, который выплачивается *первому публичному репортеру*, сообщившему об исходе рынка (см. раздел I C 6). Это мотивирует создателя рынка выбирать надежного назначенного репортера, который должен помочь быстро определить исход рынка.

Gas-залог на бездействие предназначен для покрытия расходов на "газ" (gas) первого публичного репортера. Это предотвращает сценарий, в котором затраты на газ первого публичного репортера слишком высоки для того, чтобы репортинг был для него прибыльным. Размер gas-залога на бездействие в два раза превышает среднюю стоимость расходуемого при репортинге газа для предыдущего расчетного периода.

В случае, если назначенный репортер не предоставляет отчета об исходе события вовремя, REP-залог на бездействие отдается первому публичному репортеру в форме ставки на заявленный этим репортером исход рынка, так что первый публичный репортер получает REP-залог на бездействие только в том случае, если предоставляет правильный отчет. Как и в случае с залогом на валидность, размер REP-залога на бездействие определяется динамически на основе доли назначенных репортеров, которые не предоставили вовремя отчет об исходе события в предыдущий расчетный период.[4]

Создатель рынка создает рынок и размещает все необходимые залоги посредством одной Ethereum-транзакции. Как только транзакция подтверждается сетью, рынок начинает действовать и открывается для торгов.

B. Торговля

Участники рынка прогнозируют исходы событий, торгуя *акциями* исходов рынков, созданных для этих событий (долями в соответствующих пулах). *Полный комплект акций* включает в себя по одной акции для каждого допустимого исхода события [10]. Полные комплекты создаются включенным в контракт расчетным модулем Augur при необходимости завершить сделки.

Возьмем для примера рынок, имеющий два возможных исхода:А и Б. Алиса желает заплатить 0,7 ETH за акцию А, а Боб готов заплатить 0,3 ETH за акцию Б.[5] Сначала Augur суммирует эти ордера и получает от Алисы и Боба в общей сложности 1 ETH.[6] Затем Augur создает полный комплект акций и выдает Алисе акцию А, а Бобу – акцию Б. Так появляются акции исходов рынков. Выпущенные акции можно свободно покупать и продавать.

---

[1] Например, если для рынка на "Максимальную температуру воздуха (в градусах Фаренгейта) в аэропорту Сан-Франциско 10 апреля 2018 года по сведениям Weather Underground в качестве источника решения определен сайт https://www.wunderground.com/history/airport/KSFO/2018/4/10/DailyHistory.html, то репортеру нужно просто перейти по этому URL-адресу и ввести в отчете максимальную температуру, отображаемую на этой веб-странице.

[2] Недействительный рынок – это рынок, который репортеры признали недействительным, потому что ни один из исходов, указанных создателем рынка, не является корректным или потому что определение рынка сформулировано его создателем неоднозначно либо субъективно; см. раздел III F.

[3] Подробнее об этом в приложении E 1.

[4] Подробнее об этом в приложении E 2.

[5] На начальном этапе для торговли на рынках Augur будут использоваться коины сети Ethereum, эфиры (ETH). В последующих релизах Augur будет реализована поддержка рынков, выраженных в произвольных токенах, выпущенных в сети Ethereum, включая акции других рынков, а также токены с ценой, привязанной к фиатным валютам ("стейблкоины"), если и когда они станут доступны.

[6] 1 ETH приводится здесь только для удобства. Действительная стоимость полного комплекта акций намного меньше; см. docs.augur.net/#number-of-ticks.

Торговые контракты Augur поддерживают журнал ("стакан") ордеров для каждого рынка, созданного на платформе. Любой пользователь в любое время может выставить новый ордер или исполнить существующий. Ордера исполняются автоматическим расчетным модулем, встроенным в смарт-контракты Augur. Заявки на покупку или продажу исполняются немедленно, если в стакане ордеров уже есть соответствующий ордер. Они могут быть исполнены путем покупки или продажи акций другим участникам рынка, что может подразумевать выпуск новых полных комплектов либо закрытие существующих полных комплектов. Расчетный модуль Augur всегда секвестирует минимальное количество акций и/или денежных средств, необходимых для покрытия суммы под риском. Если нет соответствующего ордера или заявка может быть исполнена только частично, то остаток средств будет помещен в стакан заявок как новый ордер.

Ордера никогда не исполняются по цене, худшей, чем та, что указал трейдер, но могут быть выполнены по лучшей цене. Незаполненные и частично заполненные ордера могут быть в любое время удалены из стакана своим создателем. Комиссии оплачиваются трейдерами только после того, как был продан полный комплект акций; расчетные выплаты обсуждаются более подробно в разделе I D.

Несмотря на то, что большая часть торгов, как ожидается, будет происходить до момента расчета по рынку, акции могут торговаться в любое время после создания рынка. Все активы Augur, включая акции исходов рынков, токены расчетного периода, доли в апелляционных пулах и даже право собственности на сами рынки могут быть переданы в любое время.

C. Репортинг

После того как событие, на котором основан рынок, произойдет, для того, чтобы финализировать рынок и начать расчет, нужно определить его исход. Исходы определяются оракулом Augur, состоящим из репортеров, которые сообщают о действительном результате произошедшего в реальном мире события и получают за это вознаграждение. Участвовать в репортинге и оспаривать результаты может любой держатель токенов REP. Репортеры, чьи отчеты согласуются с консенсусом, получают финансовое вознаграждение, а те, чьи отчеты не согласуются с консенсусом, подвергаются финансовому взысканию (см. раздел I D 3).

1. Расчетные периоды

Система репортинга Augur работает по циклам следующих один за другим 7-дневных *расчетных периодов*. Все комиссии, собираемые Augur в течение одного расчетного периода, поступают в *пул оплаты репортинга* для этого расчетного периода. В конце расчетного периода средства из пула оплаты репортинга выплачиваются держателям REP, участвовавшим в процессе репортинга. Репортеры получают вознаграждение пропорционально количеству REP, которое они оставляли в залоге во время этого расчетного периода. Участие в процессе репортинга включает: внесение залога при подаче первичного отчета, оспаривание предварительного исхода или покупку *токенов участия*.

2. Токены участия

Во время любого расчетного периода держатели REP могут приобрести любое количество токенов участия по цене 1 атто-REP[7] за каждый. В конце расчетного периода они могут погасить свои токены участия по цене 1 атто-REP за каждый в дополнение к пропорциональной доле в *пуле оплаты репортинга для расчетного периода*. Если никаких действий, требующих участия репортера – например, представления отчета или оспаривания отчета, представленного другим пользователем, – не происходило, то репортер может приобрести токены участия, чтобы обозначить свое присутствие во время этого расчетного периода. Точно так же, как переданные в залог REP, токены участия могут быть погашены их владельцами за *пропорциональную* часть сборов в этом окне сбора.

Как говорилось в разделе II, важно, чтобы держатели REP были готовы принять участие в разрешении рынка в случае форка. Токены участия создают стимулы для держателей REP следить за событиями на платформе, появляясь не реже чем раз в неделю и, следовательно, быть готовыми к участию в решениях в случае такой необходимости. Даже те держатели REP, которые не хотят участвовать в процессе репортинга, поощряются к тому, чтобы заходить на Augur хотя бы раз за 7-дневный расчетный период, чтобы приобрести токены участия и собрать выплаты. Такая регулярная активная проверка будет гарантировать, что эти пользователи понимают, как пользоваться Augur, осведомлены о происходящих форках и, следовательно, готовы к участию в этих форках.

10. Последовательность состояний рынка

После создания рынки Augur могут проходить через семь различных состояний. Список потенциальных состояний, или "фаз", рынков Augur выглядит следующим образом:

- Пре-репортинг
- Репортинг назначенным репортером
- Открытый репортинг
- Ожидание следующего расчетного периода
- Апелляционный раунд
- Форк
- Рынок финализирован

Схема переходов между этими состояниями приведена на рисунке 2.

4. Пре-репортинг

Пре-репортинг или фаза *торговли* (рис. 1) – это период между началом торгов на рынке и наступлением события, на

---

[7] Один *атто-REP* равен 10^{-18} REP.

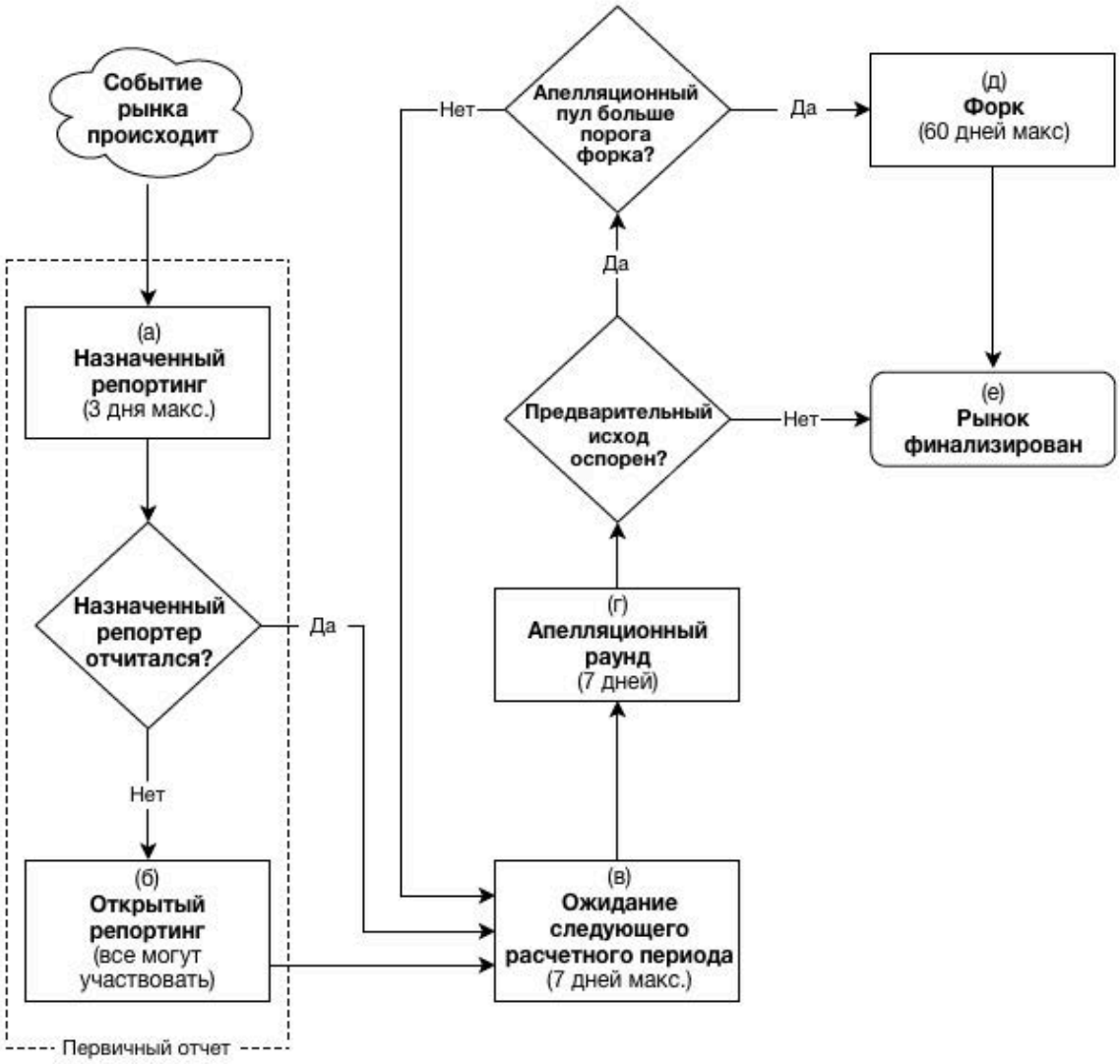

Рисунок 2. Схема процесса репортинга.

котором основан рынок. Как правило, это наиболее активный торговый период для любого рынка Augur. По наступлении времени окончания события рынок переходит в фазу репортинга назначенным репортером (рис. 2а).

5. Назначенный репортинг

При создании рынка пользователи должны выбрать назначенного репортера и разместить залог на бездействие. Максимальная продолжительность фазы репортинга назначенным репортером (рис. 2а) составляет три дня, в течение которых назначенный репортер рынка должен представить отчет об исходе события. Если за это время назначенный репортер не представит отчет, то создатель рынка лишится залога на бездействие и рынок автоматически перейдет в фазу *открытого репортинга* (рис. 2б).

Если назначенный репортер предоставляет отчет вовремя, то залог на бездействие возвращается создателю рынка. Назначенный репортер обязан внести в пул соответствующего исхода залог[8], которого он лишится, если рынок будет финализирован с любым другим исходом, помимо того, о котором отчитался назначенный репортер.[9] Как только назначенный репортер предоставит свой отчет, рынок переходит в фазу *ожидания следующего расчетного периода* (рис. 2в), а представленный в отчете назначенного репортера исход становится предварительным исходом рынка.

6. Открытый репортинг

Если назначенный репортер не предоставил отчет в отведенные для этого три дня, то создатель рынка лишается залога на бездействие и рынок автоматически переходит в фазу

[8] Подробнее о размере ставки назначенного репортера в приложении E 3.

[9] Удержанный залог добавляется в пул оплаты репортинга для установленного расчетного периода рынка и используется для вознаграждения добросовестных репортеров и пользователей, оспаривающих исход рынка; подробности см. в разделе I D 3.

открытого репортинга (Рис. 2б). После того как рынок переходит в фазу открытого репортинга, представить отчет об исходе рынка может любой пользователь. После того как назначенный репортер не представил отчет об исходе рынка, первый репортер, представивший такой отчет, называется *первым публичным репортером* рынка.

Первый публичный репортер рынка получает изъятый у создателя рынка залог на бездействие в форме доли в пуле выбранного репортером исхода рынка, так что он может претендовать на REP-залог на бездействие только в том случае, если окончательный исход рынка будет соответствовать представленному отчету. Gas-залог на бездействие он тоже получает после финализации рынка и только в том случае, если окончательный исход рынка будет соответствовать представленному отчету.

Первому публичному репортеру, сообщая об исходе рынка, *не нужно* ставить собственные токены REP. Таким образом, ожидается, что любой рынок, чей назначенный репортер не представит отчет, получит отчет *любого другого пользователя* вскоре после перехода в фазу открытого репортинга.

После получения *первичного отчета* – от назначенного или первого публичного репортера – представленный в отчете исход становится предварительным исходом рынка, и рынок переходит в фазу ожидания следующего расчетного периода (рис. 2в).

7. Ожидание следующего расчетного периода

Как только рынок получает свой первичный отчет, он переходит в фазу ожидания следующего расчетного периода (рис. 2в). Процесс репортинга для этого рынка приостанавливается до окончания текущего расчетного периода. С началом следующего расчетного периода наступает *апелляционный раунд*.

8. Апелляционный раунд

Апелляционный раунд (рис. 2г) – это 7-дневный период, в течение которого любой держатель токенов REP может оспорить *предварительный исход* рынка.[10] (В начале апелляционного раунда предварительный исход рынка – это тот исход, который станет окончательным исходом рынка в случае, если не будет успешно оспорен держателями REP.) Процесс оспаривания заключается во внесении залога в REP (в этом контексте называемого *апелляционной ставкой*) в пул любого другого исхода рынка, *отличного от* текущего предварительного исхода. Апелляция *успешна*, если общая сумма апелляционных ставок на определенный исход рынка соответствует требованиям к *размеру апелляционного пула*, предъявляемым в этом раунде. Размер апелляционного пула рассчитывается следующим образом.

Пусть A_n – это общая сумма ставок на все доступные для данного рынка исходы к началу апелляционного раунда n; ω – это любой исход рынка, *отличный от* предварительного исхода в начале этого апелляционного раунда; $S(\omega, n)$ – это общая сумма ставки на исход ω в начале апелляционного раунд n. Тогда размер *апелляционного пула*, необходимого для оспаривания текущего предварительного исхода в пользу нового исхода ω в течение раунда n обозначается $B(\omega, n)$ и рассчитывается по формуле:

$$B(\omega, n) = 2A_n - 3S(\omega, n) \quad (1)$$

Размеры залогов определяются таким образом для того, чтобы обеспечить фиксированную рентабельность инвестиций в размере 50% для успешно оспаривающих ложные исходы репортеров (см. раздел II D).

Апелляционные пулы не должны быть сформированы из средств только одного пользователя. Платформа Augur позволяет участникам проводить кампании по сбору средств для апелляционных пулов. Любой пользователь, заметивший ложный предварительный исход, может оспорить его, поставив токены REP на исход, отличный от него. Если в пуле какого-либо исхода (отличного от предварительного) собирается апелляционная ставка достаточного размера, чтобы наполнить этот пул, то текущий предварительный исход будет успешно оспорен.

В случае успешной апелляции, рынок переходит либо в следующий апелляционный раунд, либо в *состояние форка* (рис. 2д). Если размер наполненного апелляционного пула превышает 2,5% от всех токенов REP, то рынок переходит в состояние форка. Если размер наполненного апелляционного пула меньше чем 2,5% от всех токенов REP, то вновь выбранный исход становится новым предварительным исходом рынка, и рынок переходит в следующий апелляционный раунд.

Апелляционная ставка в полном объеме удерживается на эскроу-счете в течение всего апелляционного раунда. Если апелляционный пул наполнен не был, то апелляционная ставка возвращается ее владельцам в конце апелляционного раунда. Если ни одна апелляция в течение 7-дневного периода не была успешной, то рынок переходит в *финализированное* состояние (рис. 2е), и его предварительный исход принимается в качестве *окончательного исхода*. Окончательный исход рынка – это предварительный исход, который прошел через апелляционный раунд и не был успешно оспорен или определен через форк. Контракты Augur рассматривают окончательные исходы как *истинные* и распределяют выплаты соответствующим образом.

Все неуспешные апелляционные ставки в конце каждого апелляционного раунда возвращаются владельцам. Все успешные апелляционные ставки применяются к обеспечиваемому ими исходу и остаются в соответствующих пулах до тех пор, пока рынок не будет финализирован (или до выполнения форка на другом рынке Augur). Все апелляционные ставки – успешные или нет – получают часть от *пула оплаты репортинга*[11] для текущего расчетного периода.

9. Форк

Состояние форка (рис. 2е) – это особое состояние рынка, которое может длиться до 60 дней. Форк – это крайнее средство

[10] Продолжительность апелляционных раундов совпадает с продолжительностью расчетных периодов только для удобства; в принципе, их продолжительность может быть разной.

[11] Любые расчетные выплаты и залоги на валидность, собранные во время расчетного периода, добавляются в пул оплаты репортинга для этого расчетного периода. В конце расчетного периода средства из пула оплаты репортинга выплачиваются пользователям пропорционально сумме REP, которую они предоставили в залог в течение этого расчетного периода.

для разрешения рынка; это очень разрушительный процесс, который может использоваться лишь в редких случаях. Форк проводится в случае возникновения рынка с определенным предварительным исходом и с успешно наполненным апелляционным пулом, в котором находится по меньшей мере 2,5% от всех существующих токенов REP. Такой рынок называется *разветвляющимся*.

После инициации форка начинается 60-дневный[12] *период форка*. Оспаривание всех других нефинализированных рынков откладывается до конца периода форка. Период форка намного более продолжителен, чем обычный расчетный период, потому что платформа должна предоставить держателям REP и поставщикам услуг – таких как кошельки или биржи – достаточно времени для подготовки. Окончательный исход, полученный по результатам форка, не может быть оспорен.

Каждый рынок Augur и все токены REP существуют в определенных универсумах. Токены REP могут использоваться для отчета об исходах (и, следовательно, для получения вознаграждения) *только* для рынков, которые существуют в том же универсуме, что и токены REP. В первое время после запуска Augur все рынки и все REP будут существовать внутри одного *генезисного универсума*.

При выполнении форка образуются новые универсумы. В процессе форка создается новый *дочерний универсум* для каждого возможного исхода разветвляющегося рынка (включая недействительный, как уже говорилось в разделе I D 2). Например, "бинарный" рынок имеет 3 возможных исхода: А, Б и недействительный. Следовательно, при форке бинарного рынка будет создано три новых дочерних универсума: универсум А, универсум Б и недействительный универсум. Изначально эти вновь созданные универсумы пусты: они не содержат рынков или токенов REP.

После инициализации форка *родительский универсум* бессрочно *блокируется*. В заблокированном универсуме нельзя создавать новые рынки. Пользователи могут продолжать торговать акциями на рынках в заблокированных универсумах и эти рынки могут получать их отчеты, но награда за репортинг им выплачиваться не будет и рынки в заблокированных универсумах не могут быть финализированы. Для того чтобы рынки или токены REP были полезны, их сначала нужно перенести в дочерний универсум.

Держатели токенов REP в родительском универсуме могут переместить свои токены в дочерний универсум по своему выбору. Этот выбор следует тщательно взвесить, так как это действие не может быть отменено. Токены нельзя переслать из одного дочернего универсума в другой. Такая *миграция в дочерний универсум – это перманентная передача токенов REP в залог под определенный исход рынка.* Токены REP, переносимые в другой дочерний универсум, должны считаться совершенно отдельными токенами, и поставщики услуг – например, кошельки или биржи – должны признавать их таковыми.

После того, как форк инициирован, все токены REP, поставленные на других, неразветвляющихся рынках, *разблокируются*, так что в период форка их можно полностью и беспрепятственно перенести в дочерний универсум.[13]

Тот дочерний универсум, в который к концу периода форка будет перенесено наибольшее количество REP, признается *выигравшим универсумом*, а соответствующий исход становится окончательным исходом разветвляющегося рынка. Нефинализированные рынки в родительском универсуме могут быть перенесены только в выигравший универсум и, если они уже получили первичный отчет, сбрасываются к ожиданию следующего расчетного периода.

Ограничений по времени для переноса токенов из родительского в дочерний универсум не существует. Токены можно переносить и после окончания периода форка, но тогда они уже не будут учитываться в определении выигравшего универсума. С целью поощрения более активного участия в период форка, все держатели токенов, которые переносят свои REP в течение 60 дней от начала форка, будут получать плюс 5% к сумме своего депозита в дочернем универсуме своего выбора.[14] Это вознаграждение выплачивается за счет выпуска новых токенов REP.[15]

Репортеры, которые поставили свои REP на один из исходов разветвляемого рынка, не могут поменять свое решение в период форка. REP, которые были поставлены на исход события в родительском универсуме, могут быть перенесены только в дочерний универсум, соответствующий этому исходу. Например, если репортер в течение апелляционного раунда поучаствовал в наполнении набравшего необходимую сумму апелляционного пула в пользу исхода А, то REP, которые он поставил на исход А, при форке могут быть перенесены только в универсум А.

Дочерние универсумы никак не пересекаются друг с другом. Токены REP, которые существуют в одном универсуме, не могут использоваться для репортинга или получения вознаграждений с рынков другого универсума. Поскольку ожидается, что пользователи не захотят создавать рынки и торговать на них в универсумах, чей оракул признан ненадежным, то REP, существующие в таком универсуме и не соответствующие объективной реальности, вряд ли смогут принести своему владельцу какой-либо доход от комиссий, и, следовательно, не должны иметь какой-либо значимой рыночной стоимости. То есть токены REP, перенесенные в универсум, не соответствующий объективной реальности, не должны иметь рыночной ценности даже в том случае, если в результате форка выиграл объективно ложный универсум. Это имеет важные последствия для безопасности платформы, которые мы обсудим в разделе II.

10. Рынок финализирован

Рынок переходит в финализированное состояние (рис. 2e), если он проходит через 7-дневный апелляционный раунд без того, чтобы его предварительный исход был успешно оспорен, либо после завершения форка. Результат форка не может быть оспорен и в конце периода форка всегда признается окончательным.

---

[12] Периоды форка могут длиться и меньше 60 дней: они заканчиваются либо по истечении 60 дней, либо когда в один из дочерних универсумов переносится более 50% от всех выпущенных токенов REP.

[13] Единственное исключение – это REP, предоставляемые в залог первым репортером при представлении первичного отчета. Эти REP остаются в пуле соответствующего исхода и автоматически переносятся в дочерний универсум, выигравший по результатам форка.

[14] Это происходит даже в том случае, если период форка закончился раньше из-за того, что более 50% всех существующих токенов REP были перенесены в один из дочерних универсумов.

[15] Эффект такой прибавки к общему объему эмиссии REP невелик. Например, если в период форка будет перенесено 20% от всех существующих REP, то этот бонус приведет к увеличению объема предложения REP на 1%. Кроме того, ожидается, что форки будут происходить чрезвычайно редко.

После финализации рынка трейдеры могут получить расчет по своим позициям напрямую от рынка. Когда рынок переходит в финализированное состояние, выбранный для этого рынка исход называется *окончательным*.

D. Расчеты по рынку

Трейдер может закрыть свою позицию одним из двух способов: продав свои акции другому трейдеру в обмен на валюту либо путем расчета по акциям с рынком. Напомним, что каждая акция выпускается как часть полного комплекта, когда на эскроу-контракт Augur передается, в общей сложности 1 ETH.[6] Для того чтобы получить этот 1 ETH с эскроу-счета, трейдеры должны предоставить Augur либо полный комплект акций, либо, если рынок финализирован, акцию выигравшего исхода. Такой обмен называется *расчетом с контрактом рынка*.

Например, рассмотрим нефинализированный рынок с возможными исходами А и Б. Предположим, что у Алисы есть акция исхода А, которую она хочет продать за 0,7 ETH, а у Боба есть акция исхода Б, которую он хочет продать за 0,3 ETH. Сначала Augur согласовывает эти ордера и забирает у участников акции А и Б. Затем Augur выплачивает 0,7 ETH (минус комиссии) Алисе и 0,3 ETH (минус комиссии) Бобу.

В качестве второго примера рассмотрим финализированный рынок, выигравшим исходом которого является А. У Алисы есть акция А и она хочет ее обналичить. Она передает свою акцию Augur и получает взамен 1 ETH (минус комиссии).

1. Расчетные выплаты

Augur взимает комиссии только когда участники рассчитываются с контрактом рынка. При расчете Augur взимает два вида комиссий: комиссия за создание рынка и комиссия за репортинг. Размер обеих комиссий пропорционален уплаченной сумме. Так, в приведенном выше примере расчета участников до финализации рынка, где Алиса получает 0,7 ETH, а Боб – 0,3 ETH, Алиса заплатит 70% от общей суммы комиссий, а Боб – только 30%.

Размер комиссии за создание рынка устанавливается в процессе его создания, и собранные средства выплачиваются создателю при расчете. Размер комиссии за репортинг устанавливается динамически (см. раздел II C) и выплачиваются репортерам, принявшим участие в процессе репортинга.

2. Расчет по недействительным рынкам

В случае если рынок признается недействительным, трейдеры, которые рассчитываются с контрактом рынка, получают равное количество ETH за акции каждого исхода. Если рынок имеет N возможных исходов (не включая недействительный исход) и стоимость полного комплекта акций составляет C, то трейдеры получат при расчете с контрактом рынка C / N ETH за каждую акцию.[16]

3. Перераспределение токенов Reputation

Если рынок финализируется без инициации форка, все REP, поставленные на любой исход, кроме окончательного исхода рынка, перераспределяются среди пользователей, поставивших на окончательный исход рынка, пропорционально сумме поставленных ими REP. Размеры апелляционного пула выбираются таким образом, чтобы любой, кто успешно оспаривает исход в пользу окончательного исхода рынка, получил награду с рентабельностью 50% по отношению к своей апелляционной ставке.[17] Это создает для репортеров сильный стимул оспаривать ложные предварительные исходы.

II. СТИМУЛЫ УЧАСТНИКОВ И БЕЗОПАСНОСТЬ ПЛАТФОРМЫ

Существует сильная взаимосвязь между рыночной капитализацией REP и надежностью протокола выполнения форков Augur. Если рыночная капитализация REP достаточно велика[18], и поведение атакующих экономически рационально, то выигрывающий при форке исход должен соответствовать объективной реальности. Фактически Augur мог бы правильно функционировать и без назначенных репортеров и апелляционных раундов. Ответы оракула Augur были бы верны, даже если бы получались *только* в результате форков.

Однако форк – это разрушительный и времязатратный процесс. Форк занимает до 60 дней для разрешения одного рынка и может определять исход только одного рынка за раз. В течение 60 дней, когда исход одного рынка определяется посредством форка, все другие нефинализированные рынки приостанавливаются.[19] Поставщики услуг вынуждены обновлять программное обеспечение, а держатели REP – переносить свои токены в один из новых дочерних универсумов. Поэтому механизм форка должен использоваться только в тех случаях, когда это абсолютно необходимо. Форк – это крайнее средство.

К счастью, поскольку установлено, что форк является надежным средством для установления истины, могут использоваться и другие стимулы для того, чтобы мотивировать участников вести себя добросовестно – без необходимости инициировать форк. *Эта реальная угроза форка и уверенность участников в том, что исход, определенный в результате форка, будет верным, являются ключевыми элементами системы стимулов Augur.*

Далее мы поговорим об условиях, при которых системе форка можно доверить определение истины. Затем мы обсудим систему стимулов и то, как она поощряет быстрое и правильное разрешение всех рынков.

---

[16] Из-за технических ограничений, сделки не могут быть просто отменены, если рынок в итоге признается недействительным. Акции исходов – это лишь токены, которыми пользователи могут торговать непосредственно между собой. Таким образом, ETH и акции не контролируются Augur и не могут быть возвращены исходным владельцам, если рынок будет признан недействительным.

[17] См. теорему 3 в приложении А.

[18] Подробнее об этом в разделе II A.

[19] Трейдеры могут продолжать торговать на этих рынках, но эти рынки не могут быть финализированы раньше, чем закончится период форка.

A. Надежность протокола выполнения форков

Здесь мы поговорим о надежности процесса форка и условиях, при которых ему можно доверять. Для удобства, применительно к форкам, мы будем называть дочерний универсум, соответствующий объективной реальности, "истинным" универсумом, а любой другой дочерний универсум – "ложным" универсумом. Дочерний универсум, в который в период форка было перенесено наибольшее количество REP, мы будем называть выигравшим универсумом, а все другие дочерние универсумы – проигравшими универсумами.

Естественно, мы всегда заинтересованы в том, чтобы истинный универсум стал выигравшим универсумом, а ложные универсумы стали проигравшими универсумами. Мы считаем, что протокол выполнения форков был успешно атакован в тех случаях, когда ложный универсум в итоге стал выигравшим универсумом форка, вследствие чего выплаты по разветвляемому рынку (и, возможно, всем нефинализированным рынкам) будут произведены некорректно.

Наш подход к обеспечению безопасности оракула заключается в такой организации процессов, чтобы максимальная выгода от успешной атаки всегда была меньше минимальной стоимости ее проведения. Ниже мы формализуем этот подход.

1. Максимальная выгода для атакующего

Злоумышленник, успешно атаковавший оракул, заставит все нефинализированные рынки Augur перейти в ложный универсум. Если злоумышленник контролирует большую часть REP в ложном универсуме, то он может принудительно разрешить все нефинализированные рынки нужным ему образом. В самом крайнем случае он может также захватить все средства, депонированные на эскроу-счетах всех нефинализированных рынков.[20]

Определение 1. *Собственный открытый интерес* Augur мы определяем как суммарную стоимость всех средств, находящихся на эскроу-счетах нефинализированных рынков Augur и обозначаем I_a.[21]

Определение 2. *Паразитическим рынком* мы называем любой рынок, который не платит Augur комиссию за репортинг, но разрешается в соответствии с окончательным исходом нативного рынка Augur.

Определение 3. *Паразитический открытый интерес* мы определяем как сумму всех средств, депонированных на эскроу-счета всех паразитических рынков, которые разрешаются в соответствии с нефинализированными нативными рынками Augur, и обозначаем I_p.

В самом крайнем случае злоумышленник сможет захватить также все средства во всех паразитических рынках, которые разрешаются в соответствии с нефинализированными нативными рынками Augur.

Наблюдение 1. Максимальная (общая) выгода от успешной атаки оракула равна $I_a + I_p$.

2. Паразитический открытый интерес неизвестен

Augur может точно и эффективно измерять значение I_a. Однако, как правило, I_p узнать невозможно, поскольку может существовать сколь угодно много паразитических рынков офлайн, каждый с произвольно большим открытым интересом. Поскольку максимально возможная выгода для атакующего включает неизвестное значение I_p, то нельзя быть объективно уверенным в том, что оракул защищен от экономически рациональных злоумышленников.

Однако, если мы беремся утверждать, что значение I_p на практике ограничено, то мы можем определить условия, при которых можно утверждать, что оракул является безопасным.

3. Минимальная стоимость успешной атаки

Рассмотрим теперь стоимость атаки на оракула. Обозначим цену токена REP буквой P. Один атто-REP обозначим как ϵ.[22] Буквой M обозначим общее количество существующих токенов REP (объем эмиссии REP). Буквой S обозначим долю M, которая в период форка будет перенесена в истинный универсум.

Тогда $S\,M$ – это абсолютное количество REP, перенесенных во время форка в истинный универсум, а $P\,M$ – это рыночная капитализация REP.

Пусть P_f обозначает цену REP, перенесенных в ложный универсум по выбору злоумышленника. Обратите внимание, что, если $P \leq P_f$, то оракул не будет защищен от экономически рациональных атакующих, поскольку перенести REP в ложный универсум будет не менее выгодно, чем не переносить их вовсе.

4. Надежность

Допущение 1. Репортеры, не являющиеся атакующими, никогда не станут во время форка переносить REP в ложный универсум.[23]

По определению, для успешной атаки на оракул нужно, чтобы большая часть токенов REP в период форка была перенесена в некий ложный универсум, вместо истинного. Согласно допущению, переносить REP в ложный универсум будет только злоумышленник. Количество REP, перенесенных в истинный универсум в период репортинга, выражается как SM. Следовательно, для того, чтобы атака была успешной, злоумышленник должен перенести по меньшей мере $S\,M + \epsilon$ REP. Для простоты мы отбросим пренебрежимо малое ϵ и скажем, что для успешной атаки необходимо перенести в некий ложный универсум по меньшей мере $S\,M$ REP, общая стоимость которых перед переносом равна $S\,M\,P$.

---

[20] Это потребовало бы от атакующего захватить все акции определенного исхода и затем вынудить рынок финализироваться с этим исходом.

[21] Включая внешние рынки, которые выплачивают Augur комиссии за репортинг.

[22] Один атто-REP равен 10^{-18} REP.

[23] Возможны случаи переноса REP в ложный универсум добросовестными репортерами случайно или по неосторожности. Однако на практике такое поведение неотличимо от сотрудничества с атакующим.

Если злоумышленник переносит *SM* REP в период репортинга во время форка, то он получит в соответствующем дочернем универсуме *SM* REP.[24] Если злоумышленник переносит REP в ложный универсум, то стоимость этих токенов становится *SMPf*. Таким образом, минимальная стоимость атаки равна $(P - Pf)SM$.

Наблюдение 2. Для успешной атаки необходимо в период форка перенести в ложный универсум, не менее *SM* токенов REP, стоимость которых для атакующего составит $(P - Pf)SM$.

Заметим, что,если $S > \frac{1}{2}$, то атака *невозможна*, потому что за пределами истинного универсума нет достаточного количества REP для того, чтобы сделать выигравшим любой из ложных универсумов.

При экономически рациональном поведении атакующего, оракул будет обеспечивать исходы, соответствующие объективной реальности, если максимальная выгода для атакующего меньше минимальной стоимости атаки. Из наблюдений 1 и 2 видно, что это происходит, когда $S > \frac{1}{2}$ или $I_a + I_p < (P - Pf)SM$. Исходя из этого, можно дать формальное - определение надежности.

Определение 4. (Свойство надежности) Протокол выполнения форков считается надежным, если $S > \frac{1}{2}$ или если $I_a + I_p < (P - Pf)SM$.

Можно решить приведенное выше неравенство для *PM*, чтобы увидеть взаимосвязь между надежностью протокола выполнения форков и рыночной капитализации REP.

Теорема 1. *(Теорема безопасности рыночной капитализации) Протокол выполнения форков можно считать надежным, если и только если:*

1. $S > \frac{1}{2}$ или
2. $P_f < P$, при этом рыночная капитализация REP больше,чем $\frac{(I_a+I_p)P}{(P-P_f)S}$.

Доказательство. Предположим, что протокол выполнения форка надежен. Тогда, по определению, $S > \frac{1}{2}$ или $I_a + I_p < (P - P_f)SM$. Допустим, что $I_a + I_p < (P - P_f)SM$. Поскольку $I_a + I_p \geq 0$ и $SM > 0$, мы знаем, что $P_f < P$. Тогда, решив неравенство $I_a + I_p < (P - P_f)SM$ для PM, мы видим, что $\frac{(I_a+I_p)P}{(P-Pf)S} < PM$. Таким образом, первое утверждение можно считать доказанным.

Теперь предположим, что $S > \frac{1}{2}$, или что $P_f < P$ и $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Если $S > \frac{1}{2}$, то протокол выполнения форков безопасен по определению. Если $P_f < P$ и $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$, тогда, неравенство для $I_a + I_p$, мы видим, что $I_a + I_p < (P - P_f)SM$, и протокол выполнения форков надежен. □

B. Наши предположения и следствия из них

Мы полагаем, что трейдеры не захотят торговать на Augur в универсуме, в котором репортеры солгали. Мы также полагаем, что создатели рынков не будут платить за создание рынков Augur в универсумах, в которых нет трейдеров. В универсуме без рынков и без трейдинга, во владении токенами REP нет никакой выгоды. Следовательно, мы полагаем, что рыночная стоимость REP, перенесенных в ложный универсум, будет пренебрежимо мала, и мы моделируем это, допустив значение $P_f = 0$.

Разумно предположить, что по меньшей мере 20% существующих REP в период репортинга во время форка будет перенесено в универсум ис-тинного исхода, и мы моделируем это, допустив значение $S \geq \frac{1}{5}$. Мы также готовы допустить паразитический открытый интерес в размере 50% от собственного открытого интереса Augur, и поэтому мы допускаем, что $I_a \geq 2I_p$.

При этих допущениях, теорема 1 говорит нам, что протокол выполнения форков надежен, если рыночная капитализация REP как минимум в 7,5 раз превышает собственный откры-тый интерес Augur.[25]

C. Коррекция рыночной капитализации

Augur получает информацию о цене REP так же, как получает любую другую информацию о реальном мире: через рынок Augur. Это дает Augur возможность рассчитывать текущую рыночную капитализацию REP. Augur также получает информацию о текущем собственном открытом интересе и, следовательно, может определять, какое значение рыночной капитализации необходимо иметь, чтобы оно соответствовало требованиям безопасности Augur.

По умолчанию, размер комиссии за репортинг для каждого универсума составляет 1%. Если текущая рыночная капитализация ниже целевого показателя, то размер комиссии за репортинг автоматически увеличивается (но никогда не превышает 33,3%), способствуя повышению цены REP и снижению прироста собственного открытого интереса. Если текущая рыночная капитализация превышает целевой показатель, то размер комиссии за репортинг автоматически снижается (но никогда не бывает ниже 0,01%), так что трейдеры не платят системе больше, чем это необходимо для обеспечения ее безопасности.

Размер комиссии за репортинг рассчитывается следующим образом. Пусть *r* – это размер комиссии за репортинг предыдущего расчетного периода, *t* – целевое значение рыночной капитализа-ции, а *c* – текущая рыночная капитализация. Тогда размер комиссии за репортинг для текущего расчетного периода должен быть не более, чем $\left\{\min\left\{\frac{t}{c}r, \frac{333}{1000}\right\}, \frac{1}{10,000}\right\}$.

D. Использование угрозы форка

Как мы уже упоминали выше, форки – это разрушительный и медленный способ финализации рынков. Вместо того чтобы разрешать каждый рынок посредством форков, Augur использует для эффективного разрешения рынков угрозу форка.

---

[24] На практике, атакующий получил бы в дочернем универсуме 1,05 *SM* REP с учетом 5% бонуса за перенос в течение 60 дней с начала форка. Здесь мы игнорируем этот 5% бонус для удобства. Расчеты с учетом 5% бонуса можно найти в приложении C.

[25] Несколько альтернативных предположений и следствия из них см. в приложении B.

Напомним, что любая ставка, успешно оспорившая исход рынка в пользу его окончательного исхода, принесет сделавшему ее пользователю 50% дохода по отношению к размеру его апелляционной ставки.[26] В случае форка все REP, поставленные на любой из ложных исходов рынка, должны потерять всю свою экономическую ценность, тогда как каждый токен REP, поставленный на истинный исход рынка, приносит доход 50% в дочернем универсуме, соответствующем истинному исходу рынка (независимо от результата форка). Следовательно, в случае форка держатели REP, которые оспаривают ложные исходы в пользу истинных, всегда будут получать прибыль, тогда как REP, поставленные на ложные исходы, будут терять всю свою экономическую ценность.

Мы считаем, что этого обстоятельства достаточно, чтобы гарантировать, что все ложные предварительные исходы будут успешно оспорены.

III. ПОТЕНЦИАЛЬНЫЕ ПРОБЛЕМЫ И РИСКИ

A. Паразитические рынки

Напомним, что паразитическим мы называем любой рынок, который не платит Augur комиссии за репортинг, но разрешается в соответствии с окончательным исходом нативного рынка Augur. Поскольку у паразитических рынков нет репортеров, которым нужно платить, они могут предложить те же сервисы, что и рынки Augur, но с более низкими комиссиями. Это может иметь серьезные последствия для надежности протокола форков Augur.

В частности, если паразитические рынки перетягивают на себя долю от объема торгов, то репортеры Augur получат меньшее вознаграждение за репортинг. Это будет оказывать давление на рыночную капитализацию REP в сторону ее снижения. При слишком сильном снижении рыночной капитализации REP надежность протокола выполнения форков оказывается под угрозой (Теорема 1). В результате паразитические рынки потенциально могут угрожать жизнеспособности Augur, и должны активно подавляться.

Наша лучшая защита от появления паразитических рынков заключается в том, чтобы сделать торговля на платформе Augur как можно более дешевой (не ставя при этом под угрозу безопасность оракула), чтобы минимизировать выгоду от создания паразитических рынков.

B. Волатильность открытого интереса

Неожиданное значительное увеличение открытого интереса – например, во время популярных спортивных событий – приводит к быстрому росту рыночной капитализации, требуемой для сохранения надежности протокола выполнения форка (Теорема 1). Когда требуемое значение для рыночной капитализации превышает фактическую рыночную капитализацию, появляется риск того, что экономически рациональные атакующие попытаются спровоцировать форк и разрешить рынки некорректно. Хотя Augur в таких случаях провоцирует рост рыночной капитализации (см. раздел II C), это действие является реакционным и корректируется только один раз за 7-дневный расчетный период.

Однако стоит отметить, что спекулянты, обратившие внимание на внезапное увеличение открытого интереса, могут скупать REP в ожидании реакционного повышения рыночной капитализации, тем самым дополнительно способствуя ее росту, возможно, даже до тех значений, которые обеспечивают надежность протокола выполнения форка. Таким образом, времени, в течение которого оракул остается уязвимым, может просто оказаться недостаточно для того, чтобы атакующий успел этой уязвимостью воспользоваться.

C. Непоследовательные или вредоносные источники решений

Во время создания рынка пользователи выбирают источник решения, который репортеры должны использовать для определения исхода рассматриваемого события. Если создатель рынка выбирает непоследовательный или вредоносный источник решения, то добросовестные репортеры могут потерять деньги.

Предположим, что рассматриваемый рынок имеет исходы А и Б, и создатель рынка, Серена, выбрала в качестве источника решения собственный сайт, attacker.com. По наступлении времени окончания события Серена, которая является также и назначенным репортером рынка, отчитывается о наступлении исхода А, а на сайте attacker.com пишет о наступлении исхода Б. Добросовестные репортеры, проверившие сайт attacker.com, увидят, что первичный отчет неверен и во время первого апелляционного раунда должны будут успешно оспорить предварительный исход в пользу исхода Б. Тогда Серена снова обновит attacker.com, чтобы тот отображал в качестве верного исход А, и рынок перейдет во второй апелляционный раунд. Опять же, репортеры, которые проверят сайт attacker.com, будут видеть, что предварительный исход (исход Б) неверен, и могут успешно его оспорить. Серена может повторять эти действия до тех пор, пока рынок не будет разрешен тем или иным образом. Независимо от окончательного исхода рынка, часть добросовестных репортеров потеряет деньги.

Существует несколько вариантов этой атаки. Простого игнорирования рынков с сомнительными источниками решений недостаточно, так как в случае, если такой рынок спровоцирует форк, то все держатели REP должны будут выбрать дочерний универсум, в который они перенесут свои токены. Репортеры должны сохранять бдительность и вовремя выявлять рынки с сомнительными источниками решений. Информация о таких рынках должна быть общедоступной, чтобы репортеры могли скоординировать свои действия и обеспечить, финализацию этих рынков как недействительных.

D. Автореферентные запросы оракула

Рынки, на которых ведутся торги на будущее поведение оракула Augur, могут иметь нежелательные последствия для поведения самого оракула [11]. Например, рассмотрим рынок с торгами по вопросу "Будет ли любой назначенный репортер не предоставлять отчет в течение трехдневного периода репортинга до 31 декабря 2018 года?" Ставки на исход "Нет" этого рынка будут создавать для назначенных репортеров соблазн намеренно не сообщать об исходах вовремя. Если назначенный репортер может скупить достаточное количество акций "Да" по достаточно низкой цене, чтобы компенсировать

[26] В REP, существующих в универсуме, который соответствует окончательному исходу рынка; см. теорему 3 в приложении А.

потерю залога на бездействие, то он может намеренно не сообщать об исходе.

Если рыночная капитализация REP достаточно велика (теорема 1), то эти автореферентные запросы оракула не будут угрожать надежности протокола выполнения форка. Тем не менее, они могут негативно повлиять на производительность Augur, вызывая задержки в финализации рынков. Несмотря на то, что рынки по-прежнему будут финализироваться правильно, такое поведение является разрушительным и нежелательным.

E. Неуверенность относительно участия в форке

Мы не можем знать заранее, какое количество REP будет перенесено в истинный универсум в период форка, поэтому мы не можем заранее знать, будет ли рыночная капитализация достаточно высока для обеспечения надежности оракула (Теорема 1). Наша уверенность в надежности протокола выполнения форка может быть не сильнее, чем убежденность в наших допущениях относительно нижней границы добросовестного участия в период форка. Мы предполагаем, что по меньшей мере 20% всех REP в период форка будут перенесены в истинный дочерний универсум, но мы не можем этого гарантировать.

Форки Augur отличаются от форков блокчейнов в одном важном аспекте: в результате форка блокчейна держатель коина на родительской цепочке получает коины на обеих версиях блокчейна. Игнорируя атаки повторения, форки блокчейна представляют опасность для пользователей. После форка Augur держатель токена REP в родительском универсуме может перенести этот коин только в один из дочерних универсумов. Если пользователь переносит свой токен в любой универсум, отличный от универсума консенсуса, то этот токен может утратить всю свою ценность. Таким образом, перенос REP в период форка до того, как станет известно, в отношении какого из дочерних универсумов был достигнут консенсус, подвергает пользователя риску. Этот риск может лишить пользователя стимула участвовать в принятии решений по рынкам в период форка.

Для того чтобы компенсировать этот риск и поощрить участие в периоды форка, все держатели токенов, которые перенесут свои токены в течение 60 дней с начала периода форка, будут получать дополнительные 5% REP в универсуме, который они выбрали для переноса (см. раздел I C 9). Однако мы не можем знать заранее, хватит ли этого 5% бонуса на то, чтобы компенсировать риск и стимулировать участие в разрешении рынков в период форка.

F. Неоднозначные или субъективные рынки

Для рынков Augur подходят только события с объективно узнаваемыми исходами. Если репортеры считают, что рынок не подходит для разрешения на платформе – например, по причине его неоднозначности, субъективности или результат неизвестен к дате окончания события – они должны отчитаться о рынке как о недействительном. Если рынок разрешается как недействительный, трейдерам выплачиваются равные доли для всех возможных вариантов исхода; для скалярных рынков выплаты трейдерам производятся исходя из среднего значения между минимальной и максимальной ценами.

Можно представить себе рынки, на которых некоторые репортеры уверены, что правильным исходом является А, а другие считают правильным исход Б. Например, в 2006 году TradeSports разрешила своим пользователям спекулировать на том, нарушит ли Северная Корея границы своего воздушного пространства при запуске баллистических ракет до конца июля 2006 года. 5 июля 2006 года Северная Корея успешно запустила баллистическую ракету, которая упала за пределами территории Северной Кореи, и это событие широко освещалось мировыми СМИ и подтверждено многими источниками правительства США. Однако Министерство обороны США не выступило с подтверждением этого факта, как того требовал контракт TradeSports. TradeSports заключила, что условия контракта выполнены не были, и произвела выплаты соответствующим образом.[27]

Это тот случай, когда исход события – факт нарушения границ при запуске баллистической ракеты – явным образом соответствовал "духу" рынка, но не его "букве" – отчету Министерства обороны США. TradeSports, будучи централизованной компанией, смогла единолично разрешить этот рынок и объявить о его исходе. Если подобная ситуация сложится на рынке Augur, то держатели REP, вероятно, будут иметь разные мнения относительно того, как следует разрешить этот рынок, и ставить свои токены соответствующим образом. В худшем случае это может привести к форку, в результате которого ненулевую рыночную стоимость сохранят токены в более чем одном дочернем универсуме.

БЛАГОДАРНОСТИ

Мы благодарим Абрахама Отмана (Abraham Othman), Алекса Чепмена (Alex Chapman), Серену Рэндольф (Serena Randolph), Тома Хэйли (Tom Haile), Джорджа Хотца (George Hotz), Скотта Бигелоу (Scott Bigelow) и Пероне Деспень (Peronet Despeignes) за их ценные замечания и предложения.

[1] J. Wolfers and E. Zitzewitz. Prediction markets. *Journal of Economic Perspectives*, 18(2):107–126, 2004.
[2] James Surowiecki. *The Wisdom of Crowds*. Anchor, 2005.
[3] R. Hanson, R. Oprea, and D. Porter. Information aggregation and manipulation in an experimental market. *Journal of Economic Behavior & Organization*, 60(4):449–459, 2006.
[4] D.M. Pennock, S. Lawrence, C.L. Giles, and F.A. Nielsen. The real power of artificial markets. *Science*, 291:987–988, 2001.
[5] C. Manski. Interpreting the predictions of prediction markets. *NBER Working Paper No. 10359*, 2004.
[6] J. Wolfers and E. Zitzewitz. Interpreting prediction market prices as probabilities. *NBER Working Paper No. 10359*, 2005.

[27] Подробнее см. https://en.wikipedia.org/wiki/Intrade#Disputes.

[7] S. Goel, D.M. Reeves, D.J. Watts, and D.M. Pennock. Prediction without markets. In *Proceedings of the 11th ACM Conference on Electronic Commerce*, EC '10, pages 357–366. ACM, 2010.

[8] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf*, 2008.

[9] V. Buterin. A next generation smart contract and decentralized application platform. *https://github.com/ethereum/wiki/wiki/White-Paper*, 2013.

[10] J. Clark, J. Bonneau, E.W. Felten, J.A. Kroll, A. Miller, and A. Narayanan. On decentralizing prediction markets and order books. In *WEIS '14: Proceedings of the 10^{th} Workshop on the Economics of Information Security*, June 2014.

[11] A. Othman and T. Sandholm. Decision rules and decision markets. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: Volume 1 - Volume 1*, AAMAS '10, pages 625–632. International Foundation for Autonomous Agents and Multiagent Systems, 2010.

[12] J. Peterson and J. Krug. Augur: a decentralized, open-source platform for prediction markets. *arXiv:1501.01042v1 [cs.CR]*, 11 2014.

Приложение A: Время финализации и перераспределение

Начнем с нескольких условных обозначений, определений и наблюдений.

Определение 5. Для рынка M, Ω_M – это пространство исходов (или совокупность исходов) рынка M.

Определение 6. Для $n \geq 1$ и $\omega \in \Omega_M$, $S(\omega, n)$ выражает общую сумму ставок на исход ω в начале апелляционного раунда n. Эта сумма включает все ставки в пользу ω во всех успешных апелляционных пулах, сделанные за все предыдущие апелляционные раунды.

Определение 7. Для $n \geq 1$ и $\omega \in \Omega_M$, $S(\overline{\omega}, n)$ сумму ставок на все исходы в Ω_M, *за исключением* ω в начале апелляционного раунда n:

$$S(\overline{\omega}, n) = \sum_{\substack{\gamma \in \Omega_M \\ \gamma \neq \omega}} S(\gamma, n)$$

Определение 8. Для $n \geq 0$, A_n обозначает общую сумму ставок на все исходы рынка M в начале апелляционного раунда n:

$$A_n = \sum_{\omega \in \Omega_M} S(\omega, n)$$

Наблюдение 3. Отсюда следует, что $A_n - S(\omega, n) = S(\bar{\omega}, n)$.

Определение 9. Для $n \geq 1$, $\hat{\omega}_n$ обозначает предварительный исход в начале апелляционного раунда n. Например, $\hat{\omega}_1$ исход, о котором отчитался первый репортер.

Определение 10. Для $n \geq 1$ и $\omega \neq \hat{\omega}_n$, $B(\omega, n)$ означает сумму ставок, необходимую для успешного наполнения апелляционного пула в пользу исхода ω в течение апелляционного раунда n.

Напомним, что сумма ставок, требуемая для успешного наполнения апелляционного пула в пользу исхода ω в течение апелляционного раунда n, где $\omega \neq \hat{\omega}_n$ рассчитывается уравнением 1: $B(\omega, n) = 2A_n - 3S(\omega, n)$.

Наблюдение 4. Если апелляционный пул в пользу исхода ω успешно наполнен в течение апелляционного раунда n, то $S(\omega, n+1) = B(\omega, n) + S(\omega, n)$. То есть успешная апелляционная ставка является единственной новой ставкой, применяемой к исходу ω в конце апелляционного раунда n.

Наблюдение 5. Для всех $\omega \neq \hat{\omega}_n$, $S(\omega, n-1) = S(\omega, n)$. То есть если апелляционный пул в пользу исхода ω наполнен не полностью, то дополнительная ставка к исходу ω в начале следующего апелляционного раунда не добавляется. Это связано с тем, что все неуспешные апелляционные ставки в конце апелляционного раунда возвращаются пользователям.

Наблюдение 6. Для всех $n \geq 2$, $A_n = A_{n-1} + B(\hat{\omega}_n, n-1)$. То есть общая сумма ставок на все исходы в начале апелляционного раунда – это просто общая сумма ставок с начала предыдущего апелляционного раунда плюс успешная апелляционная ставка из предыдущего апелляционного раунда. Все остальные ставки в конце предыдущего апелляционного раунда были возвращены пользователям.

Лемма 2. $S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$, при $n \geq 2$.

Доказательство. Предположим, что рынок переходит в апелляционный раунд n, где $n \geq 2$. В течение апелляционного раунда $n-1$ исход $\hat{\omega}_{n-1}$ должен был быть успешно оспорен в пользу исхода $\hat{\omega}_n$. Согласно уравнению 1, размер соответствующего апелляционного пула составляет $B(\hat{\omega}_n, n-1) = 2A_{n-1} - 3S(\hat{\omega}_n, n-1)$. Используя наблюдение 3, это можно записать следующим образом:

$$B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = 2S(\overline{\hat{\omega}_n}, n-1) \qquad \text{(A1)}$$

Мы знаем, что апелляционный пул успешно наполнен в течение раунда $n-1$. Используя наблюдение 4, мы видим, что $B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = S(\hat{\omega}_n, n)$. Наблюдение 5 говорит нам, что общая сумма ставок на $\hat{\omega}_n$ при переходе из раунда $n-1$ в раунд n осталась неизменной: $2S(\hat{\omega}_n, n-1) = 2S(\hat{\omega}_n, n)$. Следовательно, уравнение A1 можно сократить до $S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$. □

Теорема 3. *Любой держатель REP, успешно оспоривший исход рынка в пользу его окончательного исхода получит доход в размере 50% от его апелляционной ставки (в REP, существующих в универсуме, соответствующем окончательному исходу рынка), если только разрешение рынка не будет прервано другим рынком, спровоцировавшим форк.*

Доказательство. В процессе форка все пользователи, сделавшие ставки в успешно наполненные апелляционные пулы в пользу окончательного исхода разветвляемого рынка, получают доход в размере 50% от своей апелляционной ставки (в коинах, созданных при форке), когда их апелляционная ставка переносится в соответствующий дочерний универсум. Таким образом, в случае если разрешаемый рынок вызвал форк, теорема верна автоматически.

Теперь рассмотрим случай, в котором действующий рынок разрешается без выполнения форка и процесс репортинга по нему не прерывается форком, спровоцированным другим рынком.

Обозначим окончательный исход рынка как ω_{Final} и предположим, что рынок разрешился в конце апелляционного раунда n, где $n \geq 2$. Это означает, что предварительный исход для раунда n является также ω_{Final}, и этот исход не оспаривается успешно в течение раунда n. То есть $\hat{\omega}_n = \omega_{\text{Final}}$. Тогда, исходя из леммы 2, мы знаем, что $S(\omega_{\text{Final}}, n) = 2S(\overline{\omega_{\text{Final}}}, n)$.

Поскольку рынок разрешается в конце раунда n и больше никаких ставок ни на какой исход не добавляется, то приведенное выше уравнение показывает полную сумму ставок на окончательный исход рынка, ω_{Final}, и сумму всех ставок на все остальные исходы рынка, $\overline{\omega_{\text{Final}}}$. Обратите внимание, что на окончательный исход рынка ровно в два раза больше ставок, чем на все прочие исходы вместе взятые.

Augur перераспределяет всю сумму ставок на неокончательные исходы рынка в пользу тех, кто ставил на исход ω_{Final}, пропорционально сумме, которые они поставили. Таким образом, пользователи, успешно наполнившие апелляционный пул в пользу исхода ω_{Final}, получают доход в размере 50% от поставленных ими REP. □

Рассмотрим теперь максимальное количество апелляционных раундов, которое может потребоваться для разрешения рынка. Уравнение 1 минимизируется, когда ω является не-предварительным исходом, имеющим к началу апелляционного раунда наибольший апелляционный пул.

Лемма 2 подразумевает, что не-предварительный исход с наибольшей суммой ставок является предварительным исходом предыдущего апелляционного раунда. Следовательно, наименьший возможный размер апелляционного пула, успешно наполненного в течение апелляционного раунда n, при $n \geq 2$, составляет $B(\hat{\omega}_{n-1}, n)$.

Другими словами, размер апелляционного пула растет *медленнее всего*, когда одни и те же два исхода постоянно оспариваются в пользу друг друга. Из этого следует, что количество апелляционных раундов, требуемых для того, чтобы рынок инициировал форк, *максимизируется*, когда одни и те же два исхода раз за разом оспариваются в пользу друг друга. Следовательно, мы можем определить максимальное количество апелляционных раундов, через которое может пройти любой рынок, прежде чем будет инициирован форк, найдя максимальное количество апелляционных раундов, которые могут произойти, когда одни и те же два рыночных исхода раз за разом оспариваются в пользу друг друга. Сейчас мы рассмотрим этот случай.

Предположим, что каждый успешный апелляционный пул наполняется ставками в пользу предварительного результата предыдущего апелляционного раунда. Тогда два предварительных исхода, которые итеративно оспариваются в пользу друг друга – это $\hat{\omega}_1$ и $\hat{\omega}_2$.

Наблюдение 7. В случае если два предварительных исхода раз за разом оспариваются в пользу друг друга, $\hat{\omega}_n = \hat{\omega}_{n-2}$ для всех $n \geq 3$.

Определение 11. Пусть d – это сумма ставок на исход $\hat{\omega}_1$, сделанных в период первичного отчета. Учитывая, что предварительный исход для каждого раунда в данном случае известен, мы можем упростить наше обозначение для размеров апелляционных пулов. Введем сокращение B_n для обозначения размера пула, требуемого для раунда n. Тогда $B_1 = 2d$ и $B_n = B(\hat{\omega}_{n-1}, n)$ для всех $n \geq 2$. Это упростит чтение и понимание.

Наблюдение 8. В случае если два предварительных исхода раз за разом оспариваются в пользу друг друга, $S(\hat{\omega}_{n-1}, n) = S(\hat{\omega}_{n-1}, n - 2) + B_{n-2}$ для $n \geq 3$. (То есть все остальные успешные апелляционные пулы добавляются к одному исходу.)

Лемма 4. *Если одни и те же два предварительных исхода раз за разом оспариваются в пользу друг друга, то всех n, где $n \geq 3$:*

1. $S(\hat{\omega}_{n-1}, n) = \frac{2}{3} B_{n-1}$
2. $A_n = 2B_{n-1}$ *and*
3. $B_n = 3d2^{n-2}$

Доказательство. (По индукции по n)

Предположим, что одни и те же два предварительных исхода раз за разом оспариваются в пользу друг друга.

(Базовый вариант) По определению и согласно уравнению 1, мы делаем следующие наблюдения:

- $S(\hat{\omega}_1, 1) = d$, $S(\hat{\omega}_2, 1) = 0$, $A_1 = d$, и $B_1 = 2d$
- $S(\hat{\omega}_1, 2) = d$, $S(\hat{\omega}_2, 2) = 2d$, $A_2 = 3d$, и $B_2 = 3d$
- $S(\hat{\omega}_1, 3) = 4d$, $S(\hat{\omega}_2, 3) = 2d$, $A_3 = 6d$, и $B_3 = 6d$

$S(\hat{\omega}_{3-1}, 3) = S(\hat{\omega}_2, 3) = 2d = \frac{2}{3}(3d) = \frac{2}{3}B_2 = \frac{2}{3}B_{3-1}$. Тогда часть 1 леммы справедлива для $n = 3$.

$A_3 = 6d = 2(3d) = 2B_2 = 2B_{3-1}$. Тогда часть 2 леммы справедлива для $n = 3$.

$B_3 = 6d = 3d2^{3-2}$. Тогда часть 3 леммы справедлива для $n = 3$.

Таким образом, лемма в полном объеме справедлива для базового варианта с $n = 3$.

(Индукция) Предположим, что лемма справедлива для всех n в диапазоне $3 \leq n \leq k$. Мы хотим показать, что лемма справедлива для $n = k + 1$. То есть мы хотим показать, что:

(a) $S(\hat{\omega}_k, k+1) = \frac{2}{3} B_k$

(b) $A_{k+1} = 2B_k$ и

(c) $B_{k+1} = 3d2^{k-1}$

Сначала мы докажем часть (a). Согласно наблюдению 8:

$$S(\hat{\omega}_k, k+1) = S(\hat{\omega}_k, k-1) + B_{k-1}$$

Исходя из наблюдения 7, мы можем переписать это так:

$$S(\hat{\omega}_{k-2}, k+1) = S(\hat{\omega}_{k-2}, k-1) + B_{k-1}$$

По гипотезе индукции, мы можем записать $S(\hat{\omega}_{k-2}, k-1)$ как $\frac{2}{3} B_{k-2}$ справа и получим:

$$S(\hat{\omega}_{k-2}, k+1) = \tfrac{2}{3} B_{k-2} + B_{k-1}$$

По гипотезе индукции, мы можем записать B_{k-2} как $3d2^{k-4}$ и B_{k-1} как $3d2^{k-3}$:

$$S(\hat{\omega}_{k-2}, k+1) = d2^{k-1}$$

Применив наблюдение 7 к левой части уравнения, получаем:

$$S(\hat{\omega}_k, k+1) = d2^{k-1}$$

Наконец, что, согласно уравнению выше и гипотезе индукции, $S(\hat{\omega}_k, k+1) = d2^{k-1} = \frac{2}{3}(3d2^{k-2}) = \frac{2}{3}B_k$. Это доказывает часть (a).

Затем мы докажем часть (b). По наблюдению 6:

$$A_{k+1} = A_k + B_k$$

Согласно гипотезе индукции, $A_k = 2B_{k-1}$:

$$A_{k+1} = 2B_{k-1} + B_k$$

По гипотезе индукции, $B_{k-1} = 3d2^{k-3}$, поэтому правую часть уравнения можно сократить до

$$A_{k+1} = 3d2^{k-2} + B_k$$

По гипотезе индукции, $B_k = 3d2^{k-2}$, что позволяет записать эту правую часть как

$$A_{k+1} = 2B_k,$$

и часть (b) доказана.
Наконец, докажем часть (c). Согласно уравнению 1:

$$B_{k+1} = 2A_{k+1} - 3S(\hat{\omega}_k, k+1)$$

По наблюдению 8, $S(\hat{\omega}_k, k+1)$ можно записать как $S(\hat{\omega}_k, k-1) + B_{k-1}$:

$$B_{k+1} = 2A_{k+1} - 3\left(S(\hat{\omega}_k, k-1) + B_{k-1}\right)$$

Согласно наблюдению 7, $\hat{\omega}_k = \hat{\omega}_{k-2}$:

$$B_{k+1} = 2A_{k+1} - 3\left(S(\hat{\omega}_{k-2}, k-1) + B_{k-1}\right)$$

Согласно наблюдению 6, $A_{k+1} = A_k + B_k$:

$$B_{k+1} = 2\left(A_k + B_k\right) - 3\left(S(\hat{\omega}_{k-2}, k-1) + B_{k-1}\right)$$

Исходя из гипотезы индукции, $A_k = 2B_{k-1}$ и $S(\hat{\omega}_{k-2}, k-1) = \frac{2}{3}B_{k-2}$:

$$B_{k+1} = 2\left(2B_{k-1} + B_k\right) - 3\left(\tfrac{2}{3}B_{k-2} + B_{k-1}\right)$$

Согласно гипотезе индукции, $B_k = 3d2^{k-2}$, $B_{k-1} = 3d2^{k-3}$ и $B_{k-2} = 3d2^{k-4}$. В результате, с учетом этих замен и упрощений:

$$B_{k+1} = 3d2^{k-1}$$

Это доказывает часть (c) и завершает доказательство леммы. □

Теорема 5. Не будучи прерванным другим рынком, спровоцировавшим форк, каждый рынок может пройти через не более 20 апелляционных раундов, прежде чем будет финализирован или приведет к форку.

Доказательство. Предположим, что рассматриваемый рынок не прерывается форком, вызванным другим рынком. Тогда, как показано выше, мы знаем, что количество апелляционных раундов, необходимых для того, чтобы рынок инициировал форк, максимизируется, когда одни и те же два исхода раз за разом оспариваются в пользу друг друга. В части 3 леммы 4 говорится, что в этой ситуации, размер апелляционного пула, необходимого оспаривания предварительного исхода в течение раунда n определяется по формуле $3d2^{n-2}$, где d – это сумма ставок, размещенных во время первичного отчета.

Мы знаем, что форки инициируются после успешного наполнения апелляционного пула, размер которого составляет не менее 2,5% от всех выпущенных REP, и мы знаем, что в обращении находятся 11 миллионов REP. Таким образом, форк инициируется, когда размер апелляционного пула достигает 275 000 REP. Мы также знаем, что $d \geq$ 0,35 REP, потому что минимальная сумма ставки на первичный отчет составляет 0,35 REP[28].

Решение $3(0{,}35)2^{n-2} > 275\,000$ для $n \in \mathbb{Z}$ дает $n \geq 20$. Таким образом, можно гарантировать, что рынок разрешится либо инициирует форк в течение не более чем 20 апелляционных раундов. □

[28] См. приложения E 2 и E 3

Приложение B: Альтернативные предположения и следствия из них

Напомним, что:

- S – это доля всех REP, которые в период форка переносятся в истинный универсум
- P – это цена REP в истинном универсуме
- P_f – это цена REP, перенесенных в ложный универсум по выбору атакующего
- I_a – это собственный открытый интерес Augur
- I_p – это паразитический открытый интерес

Augur делает определенные предположения относительно S, P_f и I_p с целью достижения целевой рыночной капитализации. В частности, Augur предполагает, что по меньшей мере 20% всех REP в период форка будут перенесены в истинный универсум, REP, перенесенные в ложный универсум, будут обладать пренебрежимо малой стоимостью, а размер паразитического открытого интереса не будет превышать половины от собственного открытого интереса Augur. Иначе говоря: $S \geq 0{,}2$, $P_f = 0$ и $I_a \geq 2I_p$. С учетом этих допущений, теорема 1 говорит нам, что протокол выполнения форков надежен, если рыночная капитализация REP превышает собственный открытый интерес Augur в 7,5 или более раз.

Вы можете сделать собственные допущения относительно S, P_f и I_p и самостоятельно прийти к заключению о том, насколько большой должна быть рыночная капитализация, чтобы гарантировать надежность оракула. Для вашего удобства, ниже приведены несколько альтернативных сценариев.

Сценарий 1. Более 50% существующих REP в период форка переносятся в истинный универсум. В этом случае P_f и I_p не важны вовсе. Поскольку $S > \frac{1}{2}$, протокол выполнения форка обладает надежностью независимо от размера рыночной капитализации. На рынке просто не останется достаточного количества REP для проведения успешной атаки.

Сценарий 2. 48% существующих REP переносятся в истинный универсум, паразитических рынков нет и REP, перенесенные в ложный универсум, не имеют ценности. В этом случае $S = 0{,}48$, $I_p = 0$ и $P_f = 0$. С учетом этих допущений, для того чтобы протокол выполнения форка сохранял надежность, рыночная капитализация REP должна превышать собственный открытый интерес Augur более чем в два раза.

Сценарий **3.** 20% существующих REP в период форка переносятся в истинный универсум, паразитический открытый интерес равен собственному открытому интересу Augur и цена REP, перенесенных в ложный универсум, составляет 5% от цены REP, перенесенных в истинный универсум. В этом случае $S = 0{,}2$, $I_p = I_a$ и $P_f = 0{,}05P$. С учетом этих допущений, для того чтобы протокол выполнения форка сохранял надежность, рыночная капитализация REP должна превышать собственный открытый интерес Augur более чем в 10,5 раз.

Сценарий 4. Только 5% существующих REP в период форка переносятся в истинный универсум, паразитический открытый интерес в два раза превышает собственный открытый интерес Augur и цена REP, перенесенных в ложный универсум,

составляет 5% от цены REP, перенесенных в истинный универсум. В этом случае $S = 0{,}05$, $I_p = 2I_a$ и $P_f = 0{,}05P$. С учетом этих допущений, для того чтобы протокол выполнения форка сохранял надежность, рыночная капитализация REP должна превышать размер собственного открытого интереса Augur более чем в 63 раза.

Приложение C: Влияние бонуса за ранний перенос REP на надежность протокола выполнения форка

Для удобства, при обсуждении надежности протокола выполнения форка мы игнорировали 5% бонус за ранний перенос REP и малые сроки. Здесь мы рассмотрим теорему 1 с учетом этих двух моментов.

Как и прежде, количество REP, отправленных в период форка в истинный универсум, обозначим SM. Тогда, для того, чтобы атака была успешной, злоумышленник должен до общей миграции перенести в некий ложный универсум по меньшей мере $SM + \epsilon$ REP, стоимость которых составляет $(SM + \epsilon)P$.

Если атакующий переносит в ложный универсум $SM+\epsilon$ REP в период репортинга во время форка, то он получит в дочернем универсуме своего выбора $1{,}05(SM + \epsilon)$ REP. По определению P_f, ценность этих коинов выражается как $1{,}05(SM + \epsilon)P_f$. Таким образом, минимальная стоимость атаки составляет $(SM + \epsilon)P - 1{,}05(SM + \epsilon)P_f$, что может быть выражено как $(SM + \epsilon)(P - 1{,}05P_f)$.

Как и прежде, максимальная (общая) выгода от спешной атаки равна $I_a + I_p$. Тогда мы можем сказать, что протокол выполнения форка остается надежным при $S > \frac{1}{2}$ или:

$$I_a + I_p < (SM + \epsilon)(P - 1.05P_f) \tag{C1}$$

Решив это неравенство для рыночной капитализации, PM, можно увидеть, что протокол выполнения форка обладает надежностью, если и только если:

1. $S > \frac{1}{2}$ или
2. $1{,}05P_f < P$ и рыночная капитализация REP больше чем $\frac{P(I_a+I_p-\epsilon(P-1.05P_f))}{S(P-1.05P_f)}$

Как можно убедиться, влияние бонуса за ранний перенос REP на требования к рыночной капитализации очень невелико.

Приложение D: Влияние бонуса за ранний перенос REP на минимальную стоимость форка

С целью поощрения более активного участия в период форка, все держатели токенов, которые переносят свои REP в течение 60 дней от начала форка, будут получать плюс 5% к сумме своего депозита в дочернем универсуме, который они выбрали. Это вознаграждение выплачивается за счет инфляции валюты.

Этот бонус может стать вредоносным стимулом, если стоимость инициации форка слишком мала. В частности, если атакующий может получить больше выгоды от 5% бонуса в REP, чем он потеряет при инициации форка, то можно ожидать, что форки будут происходить настолько часто, насколько это возможно. Такая атака – мы назвали ее *эксплуатацией инфляции* – не приведет к неверным ответам оракула, однако это приведет к частым и разрушительным форкам.

Для того чтобы избежать такого поведения, Augur нужно следить за тем, чтобы стоимость инициации форка была выше максимальной выгоды, которую можно получить от 5% инфляционного бонуса. Здесь мы получаем нижнюю границу стоимости инициации форка, достаточную, чтобы предотвратить этот вредоносный стимул.

Пусть P_0 обозначает цену REP перед форком, а P_1 обозначает цену REP после форка. Пусть M_0 обозначает объем предложения токенов перед форком, а M_1 обозначает объем предложения токенов после форка. Пусть S обозначает долю M_0, переносимую в период форка в истинный универсум. Пусть b обозначает сумму REP, которые должны утратить экономическую ценность ("сгореть"), чтобы инициировать форк (то есть REP, поставленных на ложный исход). Предположим, что $b > 1$.

Для этого раздела мы сделаем консервативное допущение о том, что все REP, переносимые в период форка, контролируются злоумышленником. Мы также предполагаем (поскольку это минимизирует стоимость такой атаки), что всб REP, переносимые в период форка, переносятся в истинный универсум.

При этих обозначениях, SM_0 будет суммой REP, перенесенных в период форка, а $(1 - S)M_0$ – суммой REP, *не* перенесенных в период форка.

$$M_0 = SM_0 + (1 - S)M_0 \tag{D1}$$

Если в общей сложности в период форка переносится SM_0 REP, то создается посредством инфляции $0{,}05SM_0$ REP:

$$M_1 = 1{,}05SM_0 + (1 - S)M_0 \tag{D2}$$

Сосредоточивая внимание только на эффектах инфляции и для простоты, мы предполагаем, что рыночная капитализация после форка будет такой же, что и перед форком[29]:

$$P_0M_0 = P_1M_1 \tag{D3}$$

В результате замены D1 и D2 на D3 и упрощения получаем:

$$P_1 = \frac{20P_0}{20 + S} \tag{D4}$$

(Общая) выгода для атакующего от инициации форка и использования бонуса за ранний перенос токенов – это стоимость перенесенных REP после переноса минус стоимость этих же REP до переноса:

$$1{,}05SM_0P_1 - SM_0P_0 \tag{D5}$$

Заменив D4 на D5, мы получаем альтернативное выражение для (общей) выгоды атакующего:

$$1{,}05SM_0\frac{20P_0}{20 + S} - SM_0P_0 \tag{D6}$$

[29] Мы считаем такое предположение консервативным. На практике, мы ожидаем, что рыночная капитализация после форка снизится.

Напомним, что b – это сумма REP, которые должны утратить экономическую ценность ("сгореть"), чтобы инициировать форк. Тогда стоимость инициации форка – это bP_0. Таким образом, платить цену инициации форка для того, чтобы получить бонус за ранний перенос REP, имеет смысл только если выполняется следующее неравенство:

$$0 < 1{,}05SM_0\frac{20P_0}{20+S} - SM_0P_0 - bP_0 \qquad \text{(D7)}$$

Зафиксировав, что $P_0 > 0$ и $S \neq -20$, мы решаем неравенство для b и видим, что такая атака выгодна, когда:

$$b < \frac{21M_0S}{S+20} - M_0S \qquad \text{(D8)}$$

Для того чтобы предотвратить образование вредоносного стимула, Augur должен обеспечить выполнение следующего неравенства:

$$b \geq \frac{21M_0S}{S+20} - M_0S \qquad \text{(D9)}$$

Отмечая, что S ограничено интервалом $[0, 1]$, мы видим, что значение правой части неравенства D9 максимизируется, когда

$$S = 2\sqrt{105} - 20 \approx 0.4939.$$

То есть такая атака наиболее выгодна для злоумышленника, когда в течение периода форка переносится около 49,39% всех существующих REP. Сохраняя консервативный подход, мы используем для S именно это значение.[30]

Подставив значение $S = 0{,}4939$ в D9, мы получаем $b \geq 0{,}012197M_0$. Следовательно, если стоимость инициации форка составляет по меньшей мере 1,2197% всех существующих REP, то атака эксплуатации инфляции становится невыгодной.

Напомним, что форк инициируется только после успешного наполнения апелляционного пула на сумму не менее 2,5% от всех существующих REP. Предположим, что такой апелляционный пул был наполнен в пользу исхода ω, и форк был инициирован. Исход ω может быть либо истинным, либо ложным.

Если исход ω является ложным, то по меньшеймере 2,5% всех существующих REP было поставлено на ложный исход и, следовательно утратили экономическую ценность. Таким образом, если исход ω является ложным, то эксплуатация инфляции невыгодна.

Если исход ω является истинным, то, согласно лемме 2, по меньшей мере 1,25% всех существующих REP поставлено на ложные исходы (в общей сложности) и, следовательно, утратят экономическую ценность. Таким образом, в случае, когда исход ω является истинным, эксплуатация инфляции также невыгодна.

Причина этого заключается в том, что инициация форка требует успешного наполнения апелляционного пула на сумму не менее 2,5% от всех существующих REP.

Приложение E: Определение размера залогов

Размер залога на валидность, REP-залога на бездействие назначенного репортера и ставка назначенного репортера определяются динамически на основе поведения участников в течение предыдущего расчетного периода. Здесь мы опишем, как определяются эти значения.

Определим функцию $f : [0, 1] \to [\frac{1}{2}, 2]$ как:[31]

$$f(x) = \begin{cases} \frac{100}{99}x + \frac{98}{99} & \text{for} \quad x > \frac{1}{100} \\ 50x + \frac{1}{2} & \text{for} \quad x \leq \frac{1}{100} \end{cases} \qquad \text{(E1)}$$

Функция f используется для определения множителя, используемого в этих корректировках, как описано в подразделах ниже. Вкратце, если нежелательная активность составляет ровно 1% от всей активности во время предыдущего расчетного периода, то размер залога остается прежним. Если нежелательное поведение случалось реже, то размер залога будет уменьшен наполовину. Если оно случалось чаще, то размер залога увеличивается в 2 раза.

1. Залог на валидность

Для самого первого расчетного периода после запуска залог на валидность будет установлен в размере 0,01 ETH. Затем, если более 1% финализированных в течение предыдущего расчетного периода рынков были недействительными, залог на валидность будет увеличен. Если недействительными были менее 1% рынков, финализированных в течение предыдущего расчетного периода, размер залога на валидность будет уменьшен (но никогда не будет меньше 0,01 ETH).

Обозначим символом ν долю недействительных рынков среди финализированных в течение предыдущего расчетного периода, а b_v – суммарный залог на валидность для предыдущего расчетного периода. Тогда залог на валидность для текущего расчетного периода составит максимум

$$\left\{\tfrac{1}{100}, b_v f(\nu)\right\}.$$

2. REP-залог на бездействие

Для самого первого расчетного периода после запуска REP-залог на бездействие будет установлен в размере 0,35 REP. Как и залог на валидность, REP-залог на бездействие корректируется в сторону повышения или понижения, отталкиваясь от базового показателя в размере 1% случаев бездействия назначенных репортеров в течение предыдущего расчетного периода и с минимальным значением 0,35 REP.

Обозначим символом ρ долю рынков, назначенные репортеры которых не предоставили свои отчеты своевременно в течение предыдущего расчетного периода, а b_r – суммарный REP-залог на бездействие для предыдущего расчетного периода. Сумма REP-залога на бездействие для текущего расчетного периода составит максимум $\{0{,}35, b_r f(\rho)\}$.

3. Ставка назначенного репортера

Для самого первого расчетного периода после запуска ставка назначенного репортера будет установлена в размере 0,35 REP. После этого ставка назначенного репортера динамически корректируется в зависимости от того, сколько отчетов

[30] В действительности, атакующий не может помешать другим участникам перенести свои REP в течение периода форка, а потому не может гарантировать, что S не превысит идеального для атакующего значения около 0,4939. Но поскольку мы рассматриваем защиту при наихудшем сценарии, мы используем значение S = 0,4939.

[31] Эта формула может измениться после получения эмпирических данных с живых рынков.

назначенных репортеров в течение предыдущего отчетного периода были некорректными (не смогли конкурировать с окончательными исходами рынков).

Обозначим символом δ долю некорректных отчетов назначенных репортеров, представленных в течение предыдущего расчетного периода, а b_d – суммарную ставку назначенных репортеров в течение предыдущего расчетного периода. Тогда размер ставки назначенного репортера для текущего расчетного периода составит максимум $\{0{,}35, b_d f(\delta)\}$.

Приложение F: Изменения дизайна

К текущему дизайну Augur мы пришли после трех лет исследований и итераций. Структура, возникшая в результате этого процесса, существенно отличается от видения, изложенного в нашей старой whitepaper (меморандуме) [12]. В этой части мы расскажем о трех значительных изменениях и об основаниях для них.

1. Комиссии за репортинг

В старой структуре, создатель рынка устанавливал торговую комиссию, сборы по которой делились между ним и репортерами в пропорции $50/50$. В нынешней структуре комиссии за создание рынка и за репортинг не зависят друг от друга и размер комиссий за репортинг динамически изменяется самим Augur, чтобы обеспечить безопасность системы.

Комиссии, выплачиваемые репортерам, влияют на цену REP, что оказывает прямое влияние на безопасность протокола выполнения форков (теорема 1). Если размер комиссий за репортинг слишком мал, то надежность оракула ставится под угрозу. Если размер комиссий за репортинг слишком велик, то возрастает угроза создания паразитических рынков. Следовательно, для обеспечения безопасности Augur размер комиссий за репортинг важно динамически корректировать, а не оставлять его на усмотрение создателям рынков.

Новый подход к определению размера комиссий за репортинг обеспечивает также то, что репортеры – и, как следствие, надежность протокола выполнения форков – не будут страдать от конкуренции между создателями рынков, стремящихся создать рынки с наименьшим размером комиссий. Качество рынков и качество репортинга должны оцениваться и вознаграждаться раздельно. Конкуренция за счет снижения комиссий до минимума уместна среди создателей рынков, но она не должна затрагивать выплаты за репортинг.

2. Торговые комиссии

В старой структуре комиссии удерживались при совершении каждой сделки. По новым правилам комиссии взимаются с трейдеров только при прямом расчете с контрактом рынка. Отчасти это изменение связано с тем, что Augur не может контролировать офлайн-торговлю. Акции исходов рынков – это просто токены, которые могут свободно торговаться между пользователями. Поскольку взимание комиссий за каждую сделку является неосуществимым, Augur, вместо этого, удерживает их только когда трейдеры рассчитываются непосредственно с контрактами рынков Augur. Дополнительная польза такого подхода заключается в том, что это снижает средний размер комиссий, выплачиваемых трейдерами, и повышает конкурентоспособность Augur.

3. Универсумы

В старой структуре существовала только одна “версия” REP, и общий объем их эмиссии был фиксирован. В текущей структуре REP могут разделяться на множество различных версий (универсумов), каждая из которых в итоге может получить больше или меньше REP, чем есть в оригинальной версии. Если форк является спорным, то объем предложения REP в каждом дочернем универсуме может быть только частью от общего предложения REP в родительском универсуме. Если форк спорным не является, то выплата бонуса за ранний перенос токенов в дочерний универсум может привести к тому, что в дочернем универсуме образуется больше REP, чем в родительском.

Новые версии REP, возникающие при форке, представляют собой совершенно разные токены, каждый со своей ценой и объемом предложения, и поставщики услуг должны воспринимать их соответственно. Непосредственно после запуска Augur будет существовать только один (генезисный) универсум и единственная версия REP, как сейчас. Однако после форка единственная версия REP разделится на несколько версий: например, в результате форка рынка, имеющего исходы `A` и `B`, возникнут новые токены REP-`A`, REP-`B` и REP-`Invalid` (для недействительного исхода). Теперь кошельки и биржи с поддержкой REP будут иметь четыре разные версии REP, которые они (в теории) могут поддерживать – REP-`genesis` (оригинальная версия REP, которая теперь будет заблокирована), REP-`A`, REP-`B` и REP-`Invalid`.[32]

Общий объем предложения REP в каждом дочернем универсуме зависит от того, сколько токенов и было перенесено в него пользователями и в какой момент. Перенос токенов в период форка, до момента достижения окончательного консенсуса в отношении одного из дочерних универсумов, подразумевает небольшой (но ненулевой) риск для пользователя (см. раздел III E), что может лишить пользователей стимула участвовать в спорных форках до момента разрешения этих рынков. Для того чтобы поощрить пользователей участвовать в разрешении спорных рынков в период форка, этот риск нужно компенсировать.

Пользователи, не перенесшие свои токены в дочерний универсум в период форка, могут лишиться некоторой части своих сбережений в REP. В действительности, прежняя структура работала по принципу “выбирай или потеряешь”, когда "молчуны" наказывались так же, как репортеры, представившие ложный отчет. Однако наказание не принявших участия в форке пользователей создает значительные проблемы в использовании. Это проблематично для кошельков и бирж, которые хранят токены своих клиентов. В случае форка биржи должны будут в период форка перенести REP своих клиентов в один из дочерних универсумов или они потеряют часть своих сбережений в REP.[33]

---

[32] На практике поставщики услуг могут счесть самым простым для себя (и наименее болезненным для их пользователей) решением побудить пользователей участвовать в форке, а затем просто поддержать выигравший по результатам форка универсум.

[33] Мы также обнаружили, что код смарт-контракта, необходимого для реализации связанных с форком вознаграждений только посредством перераспределения токенов, на практике оказался необычайно сложен. Чрезмерно сложный код контракта уже несет в себе угрозу безопасности, поэтому мы старались упростить практическую реализацию насколько это возможно.

Вместо наказания неучаствующих пользователей, участники форка, перенесшие свои токены в период форка, получают 5% бонус к своим REP в выбранном дочернем универсуме. Если в проигравший универсум переносится 4,762% (или больше) от всех существующих REP – из которых от 1,25% до 2,5% уже было заявлено в качестве апелляционной ставки – то все дочерние универсумы будут иметь меньший объем предложения REP, чем родительский универсум.