DOI: 10.51790/2712-9942-2023-4-3-09

СТАТИСТИЧЕСКАЯ УЯЗВИМОСТЬ СРЕДНИХ ЦЕН АВТОМАТИЧЕСКИХ МАРКЕТ-МЕЙКЕРОВ С ПОСТОЯННЫМ ПРОИЗВЕДЕНИЕМ

П. Н. Анохин
Индивидуальный предприниматель, г. Орёл, Российская Федерация
ORCID: https://orcid.org/0009-0009-4393-6531, ✍ pavel@anokhin.name

Аннотация: для корректной работы множества финансовых сервисов на технологии блокчейн требуются независимые поставщики цен, устойчивые к манипуляциям. Одним из наиболее распространенных поставщиков таких цен, который сам полностью работает на блокчейне, является автоматический маркет-мейкер с постоянным произведением, который является механизмом расчета цены обмена на основании количества двух активов под его управлением. Разработчики финансовых приложений должны учитывать все возможные уязвимости, которые могут возникнуть в приложении при использовании таких поставщиков цен. Этим обусловлена актуальность исследований уязвимостей цен автоматических маркет-мейкеров с постоянным произведением. В данной работе изучено влияние комиссии автоматических маркет-мейкеров с постоянным произведением на среднюю цену на основе данных реальных торгов из блокчейна и биржи Binance. В результате исследования показано, что среднее отклонение цен автоматических маркет-мейкеров от среднерыночных обладает высоким коэффициентом автокорреляции, позволяя достаточно точно предсказывать будущее среднее отклонение цен между биржами. По результатам моделирования определены конкретные значения предсказаний для разных временных промежутков. На основе предсказуемости будущих средних отклонений цен описаны возможные критические статистические уязвимости приложений, использующих средние цены автоматических маркет-мейкеров, а также даны рекомендации по предотвращению этих уязвимостей. Материалы исследования представляют практическую ценность для разработчиков приложений на блокчейне и экспертов по безопасности смарт-контрактов, позволяя им предотвратить или устранить потенциальные критические статистические уязвимости в приложениях.

Ключевые слова: статистическая уязвимость, децентрализованные финансы, смарт- контракт, блокчейн безопасность, автоматический маркет-мейкер.

Для цитирования: Анохин П. Н. Статистическая уязвимость средних цен автоматических маркет-мейкеров с постоянным произведением. *Успехи кибернетики*. 2023;4(3):86–94. DOI: 10.51790/2712-9942-2023-4-3-09.

Поступила в редакцию: 06.08.2023. *В окончательном варианте: 17.09.2023.*

STATISTICAL VULNERABILITY OF MEAN PRICES IN AUTOMATED CONSTANT PRODUCT MARKET MAKERS

P. N. Anokhin
Sole proprietor, Orel, Russian Federation
ORCID: https://orcid.org/0009-0009-4393-6531, ✍ pavel@anokhin.name

Abstract: to work correctly, many financial services using the blockchain technology require independent manipulation-resistant price feed providers. One of the most common providers of such prices, which works completely on the blockchain technology itself, is an automated constant product market maker, which is a tool for price calculation based on the amount of two assets under its control. Financial application developers should consider all the possible vulnerabilities which can be introduced by using such price providers. This is the reason for the relevance of research into the vulnerabilities of automated constant product market makers prices. We studied the effects of the automated constant product market maker fees on the mean price based on the real trading data from the blockchain and Binance exchange. The results show that mean price deviation between automated market makers and the market average shows high autocorrelation making it possible to predict a future mean deviation of the prices between the exchanges. The simulation results show the predicted values for different prediction time frames. Based on the predictability of a future mean deviation of the prices, potential critical statistical vulnerabilities in the financial applications using

the mean prices provided by constant product market makers are described, and vulnerability mitigation recommendations are given. The practical value to the blockchain application developers and smart contract security experts is that now they can prevent or mitigate potential critical statistical vulnerabilities in their applications.

Keywords: statistical vulnerability, decentralized finances, smart contract, blockchain security, automated market maker.

Cite this article: Anokhin P. N. Statistical Vulnerability of Mean Prices in Automated Constant Product Market Makers. *Russian Journal of Cybernetics*. 2023;4(3):86–94. DOI: 10.51790/2712-9942-2023-4-3-09.

Original article submitted: 06.08.2023. *Revision submitted: 17.09.2023*.

Введение

Децентрализованные финансы — это термин, который используется для финансовых сервисов на технологии блокчейн, которые не зависят от посредников, таких как брокеры и банки.

Смарт-контракты — это приложения, которые работают на блокчейне, предоставляя функциональность для реализации бизнес-логики различных сервисов. Смарт-контракты могут взаимодействовать друг с другом, в совокупности составляя децентрализованные финансы.

В рамках децентрализованных финансов возникает множество новых технологий и сервисов, которые существенно отличаются от общепринятых технологий и сервисов в традиционной финансовой системе. Краткое описание децентрализованных финансов и основных технологий можно найти в [1].

Одной из таких технологий является автоматизированный маркет-мейкер (AMM) — механизм, который позволяет автоматически рассчитывать цены покупки и продажи в соответствии с определенной формулой, тем самым предоставляя рынку непрерывные котировки [2]. В настоящее время большинство используемых на практике AMM применяют формулу постоянного произведения (AMMПП), т.е. произведение количества двух активов, находящихся во владении маркет-мейкера, должно быть постоянным после любого обмена [3].

Особенность работы AMMПП состоит в том, что цена обмена, которую он предлагает, не зависит ни от каких внешних данных, только от количества двух активов в его наличии, однако цена AMMПП всегда будет близка к цене внешних рынков благодаря участникам рынка, которые для извлечения прибыли будут менять активы по выгодному курсу, предоставляемому AMMПП до тех пор, пока этот курс не перестанет быть выгодным (станет очень близок курсу внешнего рынка). Из-за этой особенности цен AMMПП его цены часто используются в качестве оракулов цен.

Оракулом в децентрализованных финансах называется любой механизм предоставления смарт-контрактам данных, которые являются внешними по отношению к блокчейну, на котором работают эти смарт-контракты [4]. Например, такими данными может являться содержимое страницы сайта в Интернете, т.к. получить доступ к этому содержимому напрямую смарт-контракт не может, ведь смарт-контракту доступны только данные, находящиеся в блокчейне. В рамках децентрализованных финансов наиболее востребованными внешними данными являются цены различных активов, таких как криптовалюты, акции и т.п.

Оракулы бывают централизованные и децентрализованные. Централизованные оракулы используют некое доверенное лицо (человека или организацию), которое напрямую поставляет данные в смарт-контракт. Децентрализованные оракулы используют механизмы, при которых множество поставщиков данных могут предоставлять данные смарт-контракту, а смарт-контракт на основе данных от множества поставщиков определяет некие «усредненные» данные, которые используются в дальнейших расчетах. При этом каждый поставщик данных не должен быть доверенным и может поставлять неверные данные, однако при условии, что большинство поставщиков поставляет данные, близкие к верным, «усредненные» данные от всех поставщиков будут являться близкими к правильным. Под «усреднением» здесь понимается некоторая функция преобразования, а не просто среднее значение. Например, часто используется медиана (т.е. число, находящееся в середине упорядоченного набора исходных чисел), которая даёт намного лучший результат, чем среднее арифметическое в случаях, когда несколько поставщиков данных предоставляют экстремально неправильные данные (например, 0 или очень большое число).

Оракул цен — это механизм получения внешней цены какого-либо актива смарт-контрактом. Одно из важнейших свойств, которым должен обладать оракул цен, — это его устойчивость к манипуляциям (т.е. ни один пользователь не должен иметь возможность с минимальными издержками краткосрочно существенно увеличить или уменьшить цену оракула). Для этого, как правило, программы, внешние к блокчейну, определяют цены активов на внешних рынках, например из цен покупки-продажи активов на крупных биржах, и посылают эти данные в блокчейн. Большинство таких оракулов цен требуют специальных программ сбора цен внешних рынков и затрат на газ при исполнении транзакции передачи данных в блокчейне.

Газ транзакции — это стоимость исполнения транзакции в блокчейне, которая зависит от загруженности сети, количества операций, которые исполняются при выполнении смарт-контракта в транзакции, а также размера данных, передаваемых в транзакции. Газ транзакций выплачивает пользователь, который добавляет свою транзакцию в блокчейн (исполняет какую-либо функцию смарт-контракта).

АММПП являются уникальным децентрализованным вариантом определения рыночной цены актива, не требуя никаких дополнительных программ или оплаты стоимости выполнения транзакций. Рыночную цену АММПП определяют сами участники рынка, т.к. отклонение цены АММПП от рыночной создаёт возможность извлечения безрисковой прибыли, что стимулирует участников рынка использовать эту возможность получения прибыли, одновременно приближая цену АММПП к рыночной цене.

Эффективность АММПП в определении рыночной цены разных рынков и использовании цены АММПП в качестве оракулов цен исследовалась в работах [5, 6]. При этом для оценки эффективности нахождения рыночной цены чаще всего используется сравнение с ценами крупных централизованных бирж обмена [7, 8].

Многие приложения децентрализованных финансов используют для своих целей оракулы цен, предоставляемых АММПП, такими как Uniswap, который является одним из самых крупных АММПП, благодаря чему долгосрочно манипулировать его цены достаточно сложно. Однако, несмотря на удобство использования таких оракулов цен, они обладают существенными уязвимостями (примеры атак с манипулированием цены оракула можно найти в [9]), что неоднократно доказывалось на практике множеством взломов различных децентрализованных финансовых приложений через манипулирование ценами таких оракулов.

Использование средних цен таких оракулов за определенный промежуток времени вместо текущих цен решает большинство проблем, однако разработчики, которые их используют, должны учитывать статистические особенности средней цены АММПП при проектировании своих приложений, иначе их приложения могут быть подвержены серьезным уязвимостям и могут привести к существенным финансовым потерям.

Одной из малоисследованных статистических особенностей средней цены АММПП, таких как Uniswap, является влияние на цену комиссии, которую платят пользователи за совершение обмена. Целью данного исследования является изучение влияния комиссии, взимаемой с обменов, на среднюю цену АММПП на основании данных реальных торгов Uniswap на блокчейне Ethereum и определение возможных уязвимостей, связанных с этим влиянием.

Исходные данные

Для исследования влияния цены комиссии на среднюю цену в ходе реальных торгов Uniswap необходимо сравнивать цену Uniswap с некоей эталонной ценой, которая должна точно отражать текущую рыночную цену. В качестве эталонной цены будем использовать цены торгов по обмену криптовалюты Ethereum (ETH) на Tether (USDT) на бирже Binance ([10]). Среднедневной объем торгов в этой паре криптовалют на бирже Binance превышает 300 миллионов долларов, что позволяет сделать вывод о достаточно точном соответствии цены торгов на бирже Binance — рыночной цене обмена ETH/USDT. Данные по котировкам ежедневных торгов на бирже Binance в 1-секундных интервалах доступны в [11].

Данные исследуемых цен Uniswap v2 по обмену ETH/USDT доступны в блокчейне по адресу смарт-контракта *0x0d4a11d5eeaac28ec3f61d100daf4d40471f1852* в сети Ethereum Mainnet. Для получения искомых времени и цен торгов необходимо получить данные всех событий SyncEvent, в которых

содержатся все изменения количества ETH и USDT в смарт-контракте, при этом цена находится простым делением количества USDT на количество ETH.

Для сбора данных Uniswap v2 из блокчейна была написана программа на языке программирования C#. Для связи с блокчейном в программе используется библиотека Nethereum из пакета nuget. Программа собирает данные из блокчейна в заданном временном интервале, записывая данные каждого события в файл csv:

```
номер блока;время создания блока;количество активов ETH;количество активов USDT
```

Для исследования использовались данные торгов с 21.06.2023 по 20.07.2023 включительно. В блокчейне множество транзакций собираются в один блок, который уже добавляется в блокчейн через определенные промежутки времени. В сети Ethereum новый блок формируется каждые 12 секунд. Временной интервал исследования соответствует блокам с 17524329 по 17737810. Листинг основной части программы на языке программирования C# для извлечения данных Uniswap v2 из блокчейна:

```
// адрес Uniswap V2 для пары обменов Ethereum на Tether (ETH / USDT)
string uniswapPairAddress = "0x0d4a11d5eeaac28ec3f61d100daf4d40471f1852";

// номер блока в блокчейне, с которого начинать сбор
ulong fromBlock = 17524329;

// номер блока в блокчейне, до которого собирать данные
ulong toBlock = 17737810;

// программный интерфейс (API) для связи с блокчейн позволяет запросить
// за 1 раз ограниченное количество блоков, поэтому необходимо в цикле
// запрашивать последовательно небольшие интервалы до тех пор, пока не
// будут собраны данные всех блоков
// blocksPerCall – максимальное количество блоков, которое программа
// будет запрашивать за 1 вызов API
ulong blocksPerCall = 1000;

while (fromBlock <= toBlock)
{
  // устанавливаем диапазон блоков, которые будут запрошены за 1 вызов API:
  // блоки от fromBlock до fromBlock + blocksPerCall (но не больше toBlock)
  BlockParameter fromBlockParam = new BlockParameter(fromBlock);
  ulong endBlock = Math.Min(fromBlock + blocksPerCall, toBlock);
  BlockParameter toBlockParam = new BlockParameter(endBlock);

  // первый блок следующего запроса – блок, следующий за последним блоком
  // текущего запроса
  fromBlock = endBlock + 1;

  // запрашиваем все события SyncEvent для исследуемой пары в заданном
  // диапазоне блоков
  var eventHandler = mWeb3.Eth.GetEvent< SyncEventDTO>(uniswapPairAddress);
  var eventFilter = eventHandler.CreateFilterInput(fromBlockParam, toBlockParam);
  var events = eventHandler.GetAllChangesAsync(eventFilter).Result;

  // events содержит массив событий SyncEvent из блокчейна в заданном диапазоне
  // блоков
  ulong lastBlock = 0;
  long lastBlockTimestamp = 0;
  foreach (var ev in events)
  {
    // преобразуем каждое событие из блокчейна в строку, содержащую необходимые
    // данные: номер блока;время создания блока;количество ETH;количество USDT

    // количество криптовалюты ETH хранится умноженным на 10^18, преобразуем
```

```
    // в вещественное значение
    double res0 = MyMath.ToDouble(ev.Event.Reserve0, 18);

    // количество криптовалюты USDT хранится умноженным на 10^6, преобразуем
    // в вещественное значение
    double res1 = MyMath.ToDouble(ev.Event.Reserve1, 6);

    // если номер блока изменился по сравнению с предыдущим, запрашиваем в
    // блокчейне время создания этого блока
    if (ev.Log.BlockNumber.Value > lastBlock)
    {
      lastBlock = (ulong)ev.Log.BlockNumber.Value;
      lastBlockTimestamp = (long)mWeb3.Eth.Blocks.
        GetBlockWithTransactionsHashesByNumber.SendRequestAsync(
        new BlockParameter(lastBlock)).Result.Timestamp.Value;
    }

    // записываем в строку необходимые данные в нужном виде
    string s = string.Format("{0};{1};{2};{3}",
      lastBlock, lastBlockTimestamp, res0, res1);

    // сохраняем строку в файл
    writer.WriteLine(s);
  }
}
```

Поскольку в данных Binance содержатся цены на начало каждой секунды, а в блокчейне Ethereum время между блоками составляет 12 секунд, то для корректного сравнения цен из каждого блока Ethereum берётся цена Binance на начало той же самой секунды. В блокчейне цена Uniswap меняется не каждый блок (т.к. в некоторых блоках торгов может не быть), поэтому дополнительно к полученным данным блокчейна — при отсутствии торгов в блоке — используется цена предыдущего блока. Таким образом на основе исходных данных получаются данные для 213482 блоков: дата и время, цена Binance и цена Uniswap на момент создания каждого блока.

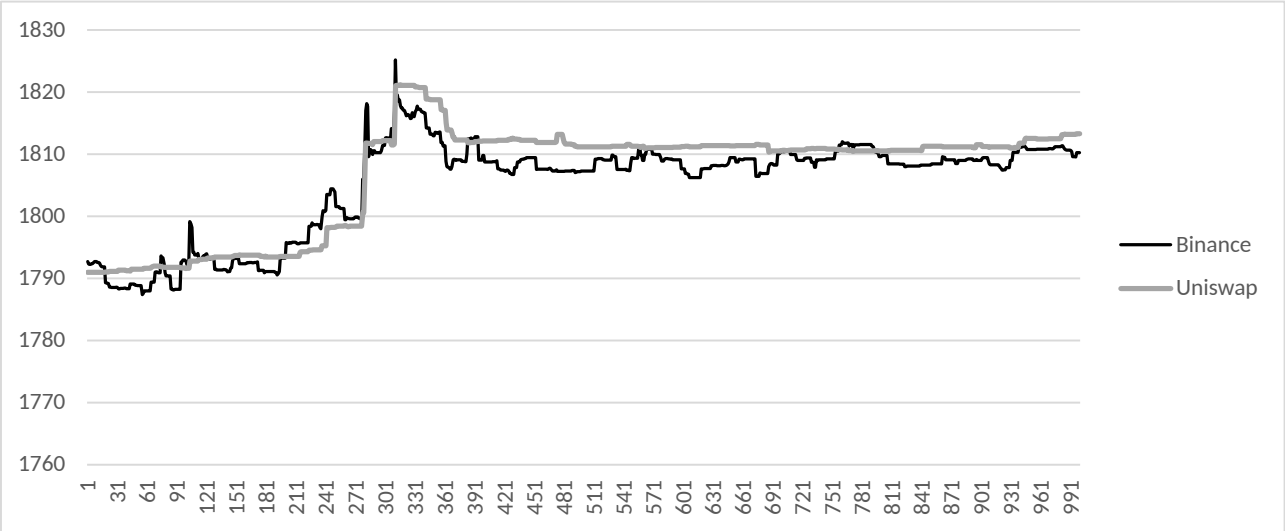

Рис. 1. *Сравнение текущей цены ETH/USDT в биржах Binance и Uniswap в первые 1000 блоков исследуемого временного интервала*

Сравнение цены обмена в Uniswap и Binance

В идеальном мире и при отсутствии комиссий за торговлю, цены на биржах Uniswap и Binance должны быть равны, т.к. иначе существует возможность получить практически безрисковую прибыль — купив ETH за меньшую цену на одной бирже, одновременно продав такое же количество ETH на другой бирже за большую цену.

На практике же наличие комиссий не позволяет ценам сравняться. Комиссия на бирже Uniswap составляет 0.3 % от суммы обмена. Таким образом, если, например, цена 1 ETH на бирже Binance составляет 1003 USDT, а на бирже Uniswap — 1000 USDT, то реальная стоимость покупки 1 ETH будет 1000 USDT + комиссия в 3 USDT, итого 1003 USDT, т.е. безрисковая прибыль отсутствует, хотя цены отличаются на 0.3 %. Кроме того, за операцию обмена в блокчейне также придется заплатить стоимость газа транзакции, которая не зависит от суммы обмена, но может составлять существенный процент при маленьких суммах обмена, что также влияет на разницу цен Binance и Uniswap: чем меньше объем ликвидности, тем больше стоимость транзакции влияет на прибыльность операции. Таким образом, можно ожидать, что цены Binance и Uniswap будут достаточно близкими, но могут отличаться на размер комиссии (0.3 %) или немного больше (в зависимости от цены газа транзакции). На рисунке 1 приведены графики цен ETH/USDT на бирже Binance и Uniswap в первые 1000 блоков исследуемого временного интервала.

Как видно из рисунка 1, цена ETH/USDT в Binance подвержена большей волатильности, чем цена ETH/USDT в Uniswap, что подтверждается расчетами статистических показателей изменения цен (таблица). Кроме того, заметны продолжительные периоды, когда цена Uniswap стабильно выше (или ниже) цены Binance, что можно объяснить комиссией и стоимостью транзакций в сети Ethereum, что делает обмен в Uniswap невыгодным по сравнению с обменом в Binance даже при долгом расхождении цен. Это еще нагляднее видно на графиках среднеарифметических цен за 5-минутные интервалы времени на рисунке 2.

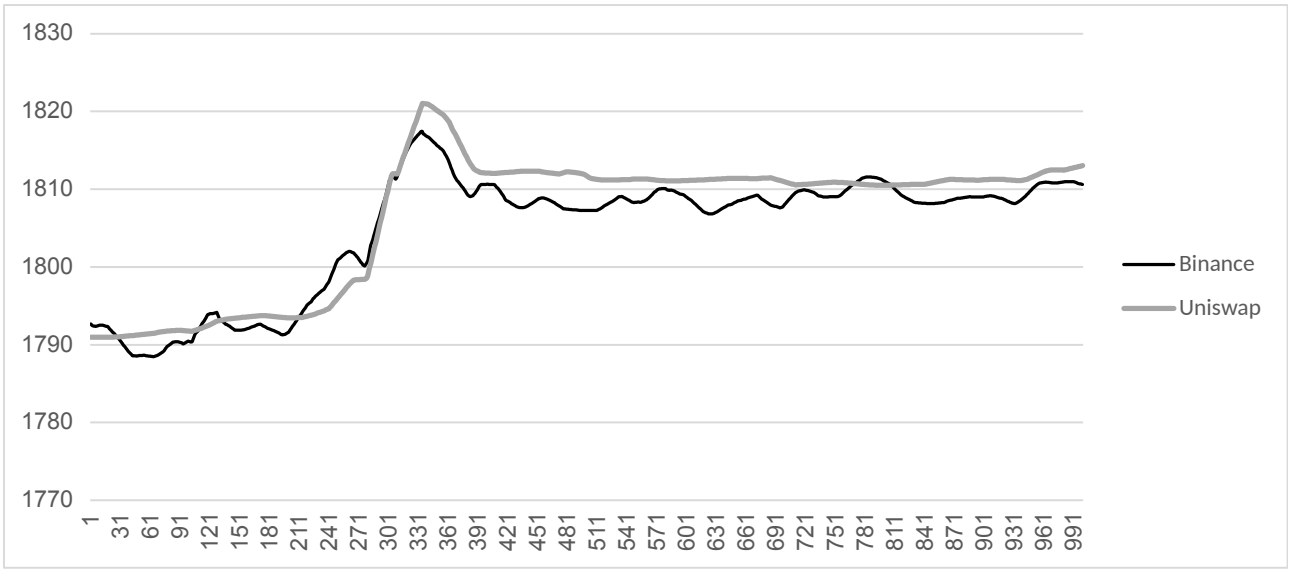

Рис. 2. *Сравнение средней цены ETH/USDT за 5-минутные интервалы в биржах Binance и Uniswap в первые 1000 блоков исследуемого временного интервала*

На рисунке 3 показаны графики отклонения текущих и средних (за 5 минут) цен Binance от цен Uniswap в процентах.

Как видно из рисунка 3, отклонение цен Binance и Uniswap находится в границах 0.3%-й комиссии, однако внутри этих границ отклонение продолжительное время может сохранять один и тот же знак, что указывает на зависимость будущих значений этого ряда от предыдущих. В статистике для определения степени связи уровней ряда за один или несколько периодов используется коэффициент автокорреляции. Высокое значение этого коэффициента (близкое к 1) показывает высокую зависимость, а низкое значение (близкое к 0) — низкую зависимость.

В таблице указаны коэффициенты автокорреляции отклонения цены Binance от цены Uniswap разного порядка. Как видно из таблицы, отклонение между ценами обладает достаточно высокой степенью автокорреляции даже на 30-минутном интервале (хотя с увеличением временного интервала автокорреляция уменьшается). Другими словами, текущее отклонение цен является очень сильным предсказателем будущего отклонения цен.

Высокая автокорреляция отклонения цен позволяет использовать простой алгоритм предсказа-

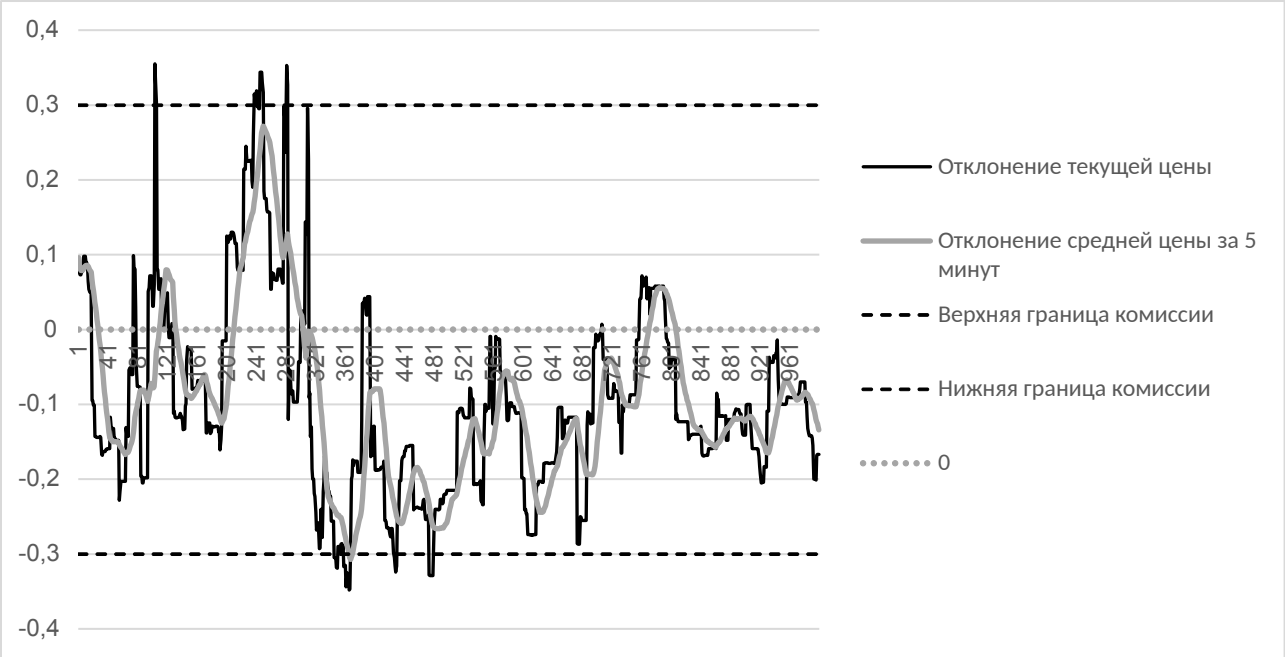

Рис. 3. *Отклонение цены ETH/USDT на бирже Binance от цены на бирже Uniswap в первые 1000 блоков исследуемого временного интервала*

Таблица

Статистические параметры изменения цены в исследуемом временном интервале

Параметр	Binance	Uniswap	Отклонение Binance от Uniswap
Волатильность (годовая)	42 %	29 %	267 %
Стандартное отклонение	0,026 %	0,018 %	0,16 %
Автокорреляция(12 секунд)	0,023	0,021	0,987
Автокорреляция(1 минута)	-0,003	0,017	0,939
Автокорреляция(5 минут)	0,01	0,013	0,764
Автокорреляция(30 минут)	0,003	0,004	0,29

ния будущих отклонений (и средних отклонений) цен:

- если текущее отклонение больше 0, то чем оно больше, тем больше ожидаемое отклонение в будущем;
- если текущее отклонение меньше 0, то чем оно меньше, тем меньше ожидаемое отклонение в будущем.

Чтобы точнее определить ожидаемое отклонение в зависимости от текущего отклонения, было проведено математическое моделирование, которое определяло среднее отклонение через интервал времени T в зависимости от текущего отклонения. Для этого текущее отклонение разбивалось на 60 интервалов (от -0.3 % до 0.3 % с шагом в 0.01 %) и для отклонения, попадающего в каждый из интервалов, считалось среднее отклонение через время T.

Результат моделирования представлен на рисунке 4.

Как видно из рисунка 4, текущее отклонение очень точно предсказывает будущее среднее отклонение. При этом чем меньше период предсказания, тем ближе будущее среднее отклонение к текущему отклонению. Через 1 минуту среднее будущее отклонение примерно равно текущему отклонению, через 10 минут будущее среднее отклонение равно примерно половине текущего отклонения, а через 30 минут — примерно одной третьей от текущего отклонения.

Статистическая уязвимость средних цен АММПП

Проведенное исследование сравнения реальных цен обменов в АММПП Uniswap v2 с ценами обменов на бирже Binance показало, что отклонение средних цен Uniswap от Binance не превышает

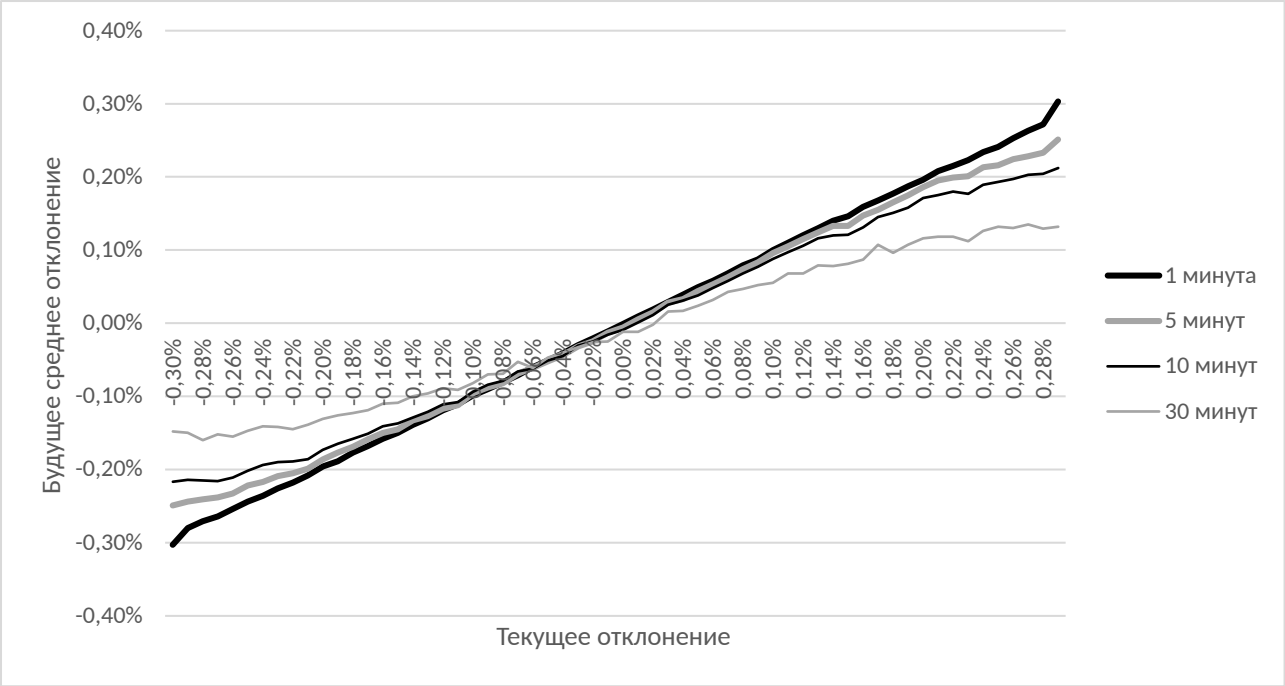

Рис. 4. *Зависимость будущего среднего отклонения цен ETH/USDT от текущего отклонения за разный период предсказания*

(или может несущественно превышать) комиссию Uniswap v2 (0.3 %). Поэтому приложения, которые не требуют точности оракула цены, лучше, чем комиссия (0.3 %), могут использовать оракулы средних цен АММПП.

В то же время если приложение требует большей точности оракула средних цен, то такие приложения могут быть потенциально уязвимы из-за высокой предсказуемости отклонения цен АММПП от рыночной цены.

Например, приложение, которое позволяет совершать обмен или торговлю производными инструментами по средней цене Uniswap за следующие 5 минут, но с пониженной комиссией (например, 0,1 %), будет иметь критическую статистическую уязвимость. Умный пользователь может предсказать, что при текущей разнице Uniswap с Binance 0.3 % или больше — средняя цена обмена за следующие 5 минут будет в среднем на 0,25% выше, чем в Binance. Этот пользователь продаёт 1 ETH в приложении и одновременно начинает покупать по 0,04 ETH каждые 12 секунд на бирже Binance. В результате через 5 минут пользователь купит 1 ETH на бирже Binance по средней цене за 5 минут, и одновременно продаст 1 ETH в уязвимом приложении по цене на 0,25% выше, чем в Binance. После уплаты 0,1% комиссии приложению, пользователь получит прибыль в 0,15% за 5 минут обмена. Проведя множество аналогичных операций, пользователь получит большую прибыль за короткое время за счет средств уязвимого приложения, т.е. из-за статистической уязвимости приложение понесет за короткое время финансовые потери в размере, близком ко всем вложенным в приложение средствам.

Заключение

В данном исследовании на основании данных реальных торгов бирж Binance и Uniswap v2 по обмену криптовалют ETH и USDT выявлены статистические особенности изменения цены обмена автоматических маркет-мейкеров постоянного произведения, связанные со взимаемой комиссией. В частности, установлена высокая степень автокорреляции отклонения цен Uniswap от Binance, что позволяет достаточно точно предсказывать будущее отклонение цен, не превышающее размер комиссии. В результате математического моделирования показаны конкретные значения предсказаний в зависимости от временного интервала предсказывания. Эта статистическая особенность может привести к критической статистической уязвимости в приложении, использующем оракул цены Uniswap.

На основании проведенного исследования можно определить рекомендации по устранению найденной статистической уязвимости для разработчиков и аудиторов по безопасности. Данные рекомендации применимы только для тех приложений, которые требуют точности цены оракула, лучше,

чем комиссия АММПП. В этом случае можно предложить 3 способа устранения статистической уязвимости в зависимости от потребностей и возможностей приложения:

1. Увеличить комиссию приложения до уровня, который компенсирует потенциальные потери и сделает статистическую атаку убыточной. Нужно учитывать особенности приложения при определении минимальной комиссии. Так, для приложения, позволяющего совершать обмен по средней цене оракула цены за 5 минут, минимальная комиссия для устранения уязвимости будет составлять 0,25 %. В то же время, для приложения, позволяющего торговать по утроенной средней цене оракула за 5 минут, минимальная комиссия будет в 3 раза больше — 0,75 %.

2. Увеличить интервал времени расчета средней цены. Например, увеличив среднее время для расчета цены обмена с 5 минут до 30 минут, можно снизить минимальную цену комиссии до 0,15 % вместо 0,25 %.

3. Выбрать другой оракул цен. В частности, вместо Uniswap v2 можно выбрать рынок обмена Uniswap v3 с базовой комиссией 0,05 %. Таким образом, минимальная комиссия приложения для такого рынка может составлять также 0,05 %.

Несмотря на то, что исследование проводилось на основе данных Uniswap v2, все полученные результаты применимы и к другим АММПП, в то числе к Uniswap v3, т.к. базовые предпосылки существования статистической уязвимости не зависят от конкретной реализации АММПП. В то же время другие автоматические маркет-мейкеры (такие, как Uniswap v3) могут иметь и другие факторы, влияющие на среднюю цену, поэтому дальнейшие исследования в этом направлении могут включать изучение статистических уязвимостей цен других АММ.

ЛИТЕРАТУРА

1. Schar F. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis*. 2021;103(2):153–174. DOI: 10.20955/r.103.153-74.
2. Mohan V. Automated Market Makers and Decentralized Exchanges: a Defi Primer. *Financial Innovation*. 2022;8(20). DOI: 10.2139/ssrn.3722714.
3. Angeris G., Chitra T. Improved Price Oracles. *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. 2020. DOI: 10.1145/3419614.3423251.
4. Peterson J., Krug J., Zoltu M., Williams A.K., Alexander S. Augur: a Decentralized Oracle and Prediction Market Platform. 2020. *arXiv:1501.01042 [cs.CR]*.
5. Angeris G., Evans A., Chitra T. When Does the Tail Wag the Dog? Curvature and market Making. 2020. *arXiv:2012.08040 [q-fin.TR]*.
6. Pourpouneh M., Nielsen K., Ross O. Automated Market Makers. *IFRO Working Paper*. 2020. Режим доступа: https://ideas.repec.org/p/foi/wpaper/2020_08.html.
7. Barbon A., Ranaldo A. On the Quality of Cryptocurrency Markets: Centralized Versus Decentralized Exchanges. 2021. *arXiv:2112.07386 [q-fin.TR]*.
8. Lehar A., Parlour A., Christine A. Decentralized Exchanges. 2021. DOI: 10.2139/ssrn.3905316.
9. Wu S. et al. DeFiRanger: Detecting Price Manipulation Attacks on DeFi Applications. 2021. *ArXiv:2104.15068 [Cs]*.
10. Binance Exchange. Режим доступа: https://www.binance.com.
11. Binance Market Data. Daily Spot ETH/USDT, 1-second interval. Режим доступа: https://data.binance.vision/?prefix=data/spot/daily/klines/ETHUSDT/1s/.