Модель оценки производительности оракулов в самоисполняющихся смарт-контрактах

В.Д. Булгаков, И.Н. Гвоздевский

Аннотация **- В данной статье представлена модель оценки производительности работы оракулов, используемых в самоисполняющихся смарт-контрактах. Производительность определяется как совокупность параметров, включающих скорость поставки данных, точность передаваемой информации и уровень безопасности работы кластера оракулов, что критически важно для надежного функционирования блокчейн-систем.**

Описанная модель сочетает в себе механизмы взвешенного агрегирования данных, применение асимметричных штрафов за некорректные результаты, а также методы формальной оценки качества работы оракулов в кластере с использованием вероятностных моделей и статистического анализа.

В работе проводится анализ существующих подходов к обеспечению достоверности данных, поступающих от оракулов, включая как консенсусные механизмы, позволяющие агрегировать информацию, предоставляемую множеством независимых источников, так и подходы, основанные на использовании доверенных источников информации, выбранных вручную

Внимание акцентируется на том, что традиционные методы анализа и оценки зачастую не учитывают динамику работы системы и не способны обеспечить необходимую гибкость в условиях изменяющейся среды. В качестве решения предложена методика внутреннего аудита кластеров оракулов, позволяющая количественно и качественно оценить их надежность и эффективность, что особенно актуально для применения в государственных и корпоративных блокчейн-системах.

Ключевые слова **- оракул, блокчейн, смарт-контракт, производительность, модель, оценка.**

I. Введение

Применение технологии смарт-контрактов стало набирать большую популярность по ходу развития DeFi сектора в проектах, построенных на технологии блокчейн. Под самоисполняющимся смарт-контрактом, в контексте блокчейна, понимается определенный программный код, который может быть выполнен только при наступлении необходимых, строго формализованных внутри самого контракта условий.

Так как смарт-контракты являются частью закрытой блокчейн-системы, а таковой она является, прежде всего, из соображений безопасности, то и информация, необходимая, для исполнения контракта, может быть взята только изнутри самой системы. Но существует огромное количество ситуаций, которые требуют получения информации извне. Для решения этой задачи существуют оракулы – сервисы-агенты, которые являются прослойкой между закрытой блокчейн-системой и внешним источником данных (см. рисунок 1). Вопрос производительности таких оракулов является фундаментальным для всей отрасли смарт-контрактов, так как от скорости и точности получаемых данных зависит корректность работы контракта, а соответственно и функционирования всей блокчейн-системы [1].

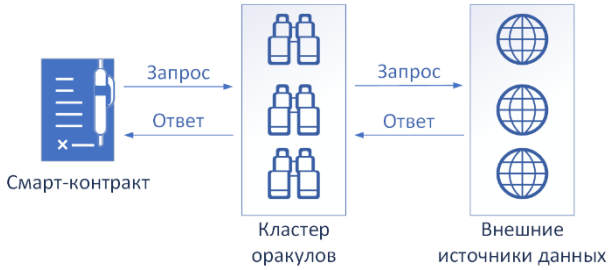

Рисунок 1 – Схема функционирования оракулов

II. Научный взгляд на «проблему оракулов»

В работе Жихарева А.Г., Киданова В.В. и Фефелова О.С. рассмотрен вопрос безопасности обработки информации с использованием смарт-контрактов, в том числе в контексте применения оракулов. Авторы отмечают, что разработанность темы надежности оракулов находится на низком уровне, при условии, что данная технология уже вовсю применяется и в государственном секторе [2].

Согласно открытой статистике Etherscan (блокчейн-обозреватель), на 23 февраля 2025 года в сети Ethereum развернуто 150915 смарт-контрактов против 7601 на 23 февраля 2024 года (20-ти кратный рост), что говорит о взрывном росте популярности технологии [3].

Хотя предполагается, что оракул является доверенным сторонним агентом, существуют системы, в которых вопрос аудита безопасности является ключевым в рамках правового поля. Для

решения задачи внутреннего аудита и формализации полученных в ходе проверки результатов была разработана модель оценки производительности кластеров оракулов, которые используются в самоисполняющихся смарт-контрактах.

«Исследование теоретических вопросов внедрения сетевых договоров (смарт-контрактов) на примере России и зарубежных стран» автора Беликовой К.М. отмечает, что на данный момент в практике используют всего два подхода в вопросе достижения достоверности оракулов: консенсус оракулов и доверенный источник информации, выбранный человеком. Второй способ не удовлетворяет принципам децентрализации, но может быть выбран в сетях, где источник данных является внутренней частью информационного обеспечения предприятия. В случае консенсуса оракулов, на помощь могут прийти не только децентрализованные оракулы, но и децентрализованные сети оракулов, такие как Chainlink. В таком случае вопрос оценки эффективности и безопасности ложиться на сеть, в которой располагаются поставщики данных. Для систем консенсусного плана, где оракулы размещаются неавторизованными участниками сети, требуется аудит, что подтверждает актуальность разработанной модели [4,5,6].

III. Оценка вероятности корректного ответа

Если система получает числовые данные только от одного оракула, его ответ принято считать априори корректным, так как отсутствуют альтернативные источники для проведения сравнительного анализа. То есть, формально, при наличии единственного источника данных его корректность будет равняться 100%.

В случае, если в системе присутствует два или более оракула, каждый из которых поставляет измеряемое значение (r_i), а вместе они называются кластером оракулов, для определения агрегированного значения целесообразно использовать взвешенное среднее (r_w):

$$r_w = \sum_{i=1}^{n} w_i r_i, \text{ где } w_i \text{ – вес оракула } O_i;$$

Для оценки качества каждого ответа введем функцию ошибки, характеризующую степень отклонения от агрегированного значения. Определим ошибку для оракула O_i как:

$$\varepsilon_i = |r_i - r_w|;$$

Чтобы привести значение отклонения в показатель корректности, введем функцию сходства q_i в виде экспоненциальной функции:

$$q_i = \exp\left(-\frac{\varepsilon_i^2}{2\upsilon^2}\right), \text{ где } \upsilon > 0 \text{ - масштаб допустимых отклонений;}$$

Если у нас есть N наблюдений, то υ определяется по формуле:

$$\upsilon = \sqrt{\frac{1}{N-1}\sum_{i-1}^{N}(\varepsilon_i - \bar{\varepsilon})^2}\text{, где } \bar{\varepsilon} \text{ — среднее значение ошибок;}$$

Функция q_i принимает значения от 0 до 1, где $q_i \approx 1$ означает, что значение r_i практически совпадает со взвешенным средним (r_w), а $q_i \to 0$ означает, что поставленные оракулом данные значительно разнятся с ним.

Для системы с n оракулами рассмотрим вероятность того, что агрегированный ответ окажется корректным, если оракулы предоставляют непрерывные данные. Пусть качество каждого ответа описывается значением q_i, полученным по формуле выше. При этом итоговое значение определяется как взвешенное среднее, а корректность агрегированного ответа P_{agg} можно интерпретировать через совокупное доверие, накопленное за счет весов оракулов, давших близкие к истинному результату значения.

Если разделить множество оракулов на группы по «значению», например, если r_i близки друг к другу, то можно определить корректность агрегированного ответа как условие:

$$\sum_{i\in S} w_i \geq \frac{1}{2}, \text{ где S-подмножество оракулов, давших ответ в пределах допустимой разницы;}$$

Общая вероятность корректности агрегированного ответа определяется суммой произведений индивидуальных качеств q_i по всем подмножествам S, удовлетворяющим условию взвешенного большинства:

$$P_{agg} = \sum_{\substack{S\subseteq\{1,\dots,n\} \\ \sum_{i\in S} w_i \geq \frac{1}{2}}} \left(\prod_{i\in S} q_i \prod_{i\in S^c}(1-q_j)\right);$$

IV. Механизм взвешенного агрегирования

В работе Кацко И.А., Швырёвой О.И. и Киёк М.А. рассмотрен эксперимент с доказательством гипотез относительно надежности фирм по показателям наличия прибыли и своевременного расчета с бюджетом с использованием механизма Байеса. Если заменить финансовые показатели на показатели производительности оракулов, а именно на апостериорную характеристику корректности ответов, то можно получить значение показателя «доверия» системой оракулу [7].

Для каждого оракула O_i вводится оценка вероятности корректного ответа p_i, которая определяется с помощью байесовского подхода. Изначально, при отсутствии эмпирических данных, устанавливается априорное распределение для каждого оракула. Чаще всего в качестве априорного распределения выбирается бета-распределение, поскольку оно удобно для моделирования вероятностей:

$$p_i \sim Beta\left(\alpha_i^{(0)}, \beta_i^{(0)}\right);$$

$\alpha_i^{(0)}$ и $\beta_i^{(0)}$ устанавливаются равными единице при инициализации параметров.

После каждой итерации, когда от оракулов получены данные, проводится оценка качества их ответов. При этом для непрерывных данных, используется функция качества $q_i \in [0,1]$, основанная

на экспоненциальной функции отклонения от агрегированного значения q_i.

С учетом ассиметричных штрафов, обновление параметров для оракула O_i на итерации t производится следующим образом:

- Если ответ оракула близок к агрегированному:
$$\alpha_i^{(t+1)} = \alpha_i^{(t)} + q_i;$$
- Если ответ сильно разнится с агрегированным:
$$\beta_i^{(t+1)} = \beta_i^{(t)} + \gamma * (1 - q_i), \text{ где } \gamma > 1 -$$
коэффициент ассиметричного штрафа, усиливающий влияние ошибок;

Таким образом, апостериорное распределение для p_i имеет вид:

$$p_i \sim Beta\left(\alpha_i^{(t+1)}, \beta_i^{(t+1)}\right);$$

А точечная оценка вероятности корректного ответа оракула определяется как:

$$\hat{p}_i^{(t+1)} = \frac{\alpha_i^{(t+1)}}{\alpha_i^{(t+1)} + \beta_i^{(t+1)}};$$

Этот механизм позволяет динамически обновлять показатель оценки качества любого оракула, учитывая его прошлые ответы, а также учитывая ассиметричный принцип поощрения и наказания.

V. Механизм инициализации и распределения весов

До проведения первых итераций, веса оракулов могут быть равномерно распределены:

$$w_i^{(0)} = \frac{1}{n}, \qquad i = 1,2,\dots,n;$$

После каждой итерации, когда апостериорные оценки $\hat{p}_i^{(t+1)}$ обновлены, производится перераспределение весов. Для этого:

$$w_i^{(t+1)} = \frac{\hat{p}_i^{(t+1)}}{\sum_{j=1}^{n} \hat{p}_i^{(t+1)}};$$

что гарантирует, что сумма весов всех оракулов останется равной единице.

Обновленные веса $w_i^{(t+1)}$ используются при формирования агрегированного ответа системы. Например, для числовых данных итоговое значение рассчитывается как среднее взвешенное:

$$r^{(t+1)} = \sum_{i=1}^{n} w_i^{(t+1)} * r_i^{(t+1)};$$

В случае, если данные представляют категориальные или более сложные структуры, веса используются для определения «взвешенного большинства».

VI. Обобщенная схема распределения весов кластера оракулов

Учитывая описанные механизмы, можно выделить следующие этапы по распределению весов внутри кластера оракулов на каждой итерации t:

1. Каждый оракул поставляет в систему значение $r_i^{(t)}$.
2. Вычисляется агрегированное значение $\bar{r}^{(t)}$ с помощью принципа взвешенного большинства.
3. Для каждого оракула в системе вычисляется ошибка $\varepsilon_i^{(t)} = \left|r_i^{(t)} - \bar{r}^{(t)}\right|$ и коэффициент качества:
$$q_i^{(t)} = \exp\left(-\frac{(\varepsilon_i^{(t)})^2}{2v^2}\right);$$
4. На основе $q_i^{(t)}$ с помощью механизма Байеса обновляются параметры:
$$\alpha_i^{(t+1)} = \alpha_i^{(t)} + q_i^{(t)},$$
$$\beta_i^{(t+1)} = \beta_i^{(t)} + \gamma * (1 - q_i^{(t)});$$
Затем вычисляется апостериорная оценка:
$$\hat{p}_i^{(t+1)} = \frac{\alpha_i^{(t+1)}}{\alpha_i^{(t+1)} + \beta_i^{(t+1)}};$$
5. Обновленные веса рассчитываются по формуле:
$$w_i^{(t+1)} = \frac{\hat{p}_i^{(t+1)}}{\sum_{j=1}^{n} \hat{p}_i^{(t+1)}};$$

VII. Система поощрений и штрафов

Системы с низким уровнем толерантности к ошибкам должны иметь возможность значительно понижать доверие к оракулам, систематически поставляющим некорректные данные. Для этого модель предусматривает механизм ассиметричных штрафов, что позволяет значительно понижать вес оракула, поставленные данные которым значительно разнятся с агрегированным значением кластера.

Для функционирования механизма введем переменную $\gamma > 1$, которая отражает степень штрафа и определяется на этапе инициализации модели.

Рассмотрим пример системы, в которой коэффициент штрафа $\gamma = 2$:

Два оракула O_1 и O_2 имеют начальные параметры:

$$\alpha_1^{(0)} = \alpha_2^{(0)} = 1, \qquad \beta_1^{(0)} = \beta_2^{(0)} = 1;$$

Пусть на итерации t оракул O_1 дает ответ, близкий к агрегированному ($q_1^{(t)} = 0.95$), а O_2 - $q_2^{(t)} = 0.7$. Тогда обновление происходит следующим образом:

- Для O_1:
$$\alpha_1^{(t+1)} = 1 + 0.95 = 1.95,$$
$$\beta_1^{(t+1)} = 1 + 2 * (1 - 0.95) = 1 + 0.1 = 1.1;$$
- Для O_2:
$$\alpha_1^{(t+1)} = 1 + 0.7 = 1.7,$$
$$\beta_1^{(t+1)} = 1 + 2 * (1 - 0.7) = 1 + 0.6 = 1.6;$$

Тогда точечные оценки доверия будут:

$$\hat{p}_1^{(t+1)} = \frac{1.95}{1.95 + 1.1} \approx 0.64,$$
$$\hat{p}_2^{(t+1)} = \frac{1.7}{1.7 + 1.6} \approx 0.52;$$

После нормализации веса оракулов перераспределяются следующим образом:

$$w_1^{(t+1)} = \frac{0.64}{0.64 + 0.52} = 0.5517,$$

$$w_2^{(t+1)} = \frac{0.52}{0.64 + 0.52} = 0.4483;$$

VIII. Оценка скорости поставки данных

Скорость поставки данных в смарт-контракт также оказывает значительное влияние на производительность системы, поэтому введение метрик мониторинга периода задержки (латентности) для каждого оракула и кластера в целом позволит ввести механизм отслеживания «отстающих» оракулов [8].

Для комплексной оценки скорости, основанной на времени задержки и исторической эффективности (параметров точности и доверия) отдельного оракула или всего кластера используется следующая формула:

- Для отдельного оракула:

$$S_i = \frac{q_i * \hat{p}_i * S_{target}}{\Delta t_i}, \text{ где } S_{target} - \text{эталонное значение латентности, заданное вручную и вычисленное эмпирически;}$$

- Для кластера:

$$S_{cluster} = \sum_{i=1}^{n} w_i S_i;$$

IX. Обобщенная оценка качества

Для того, чтобы получить общую формальную оценку производительности кластера оракулов, введем характеристику, учитывающую все вышеописанные показатели корректности:

1. Агрегированную корректность $P_{agg}^{(t)}$;
2. Среднее взвешенное текущей корректности $\bar{q}^{(t)}$, где:

$$\bar{q}^{(t)} = \sum_{i=1}^{n} w_i^{(t)} q_i^{(t)};$$

3. Согласованность текущих оценок:

$$D^{(t)}(q) = \sum_{i=1}^{n} w_i^{(t)} (q_i^{(t)} - \bar{q}^{(t)})^2;$$

4. Индекс скорости поставки данных кластером $S_{cluster}$;

$$Q_{total}^{(t)} = P_{agg}^{(t)} * \bar{q}^{(t)} * \exp\left(-\theta D^{(t)}(q)\right) * (S_{cluster})^{\mu};$$

Здесь:

- $\exp\left(-\theta D^{(t)}(q)\right)$ – корректирующий множитель, снижающий значение $Q_{total}^{(t)}$ при высокой дисперсии ответов оракулов. Параметр $\theta \geq 0$ регулирует чувствительность к расхождению оценок;
- $S_{cluster}$ – агрегированный индекс скорости поставки данных;
- $\mu \geq 0$ – параметр, задающий относительный вклад скорости в показатель обобщенной оценки.

X. Использование алгоритма RSA

В системах, где данные, получаемые от оракулов, служат основой для принятия автоматизированных решений, необходимо обеспечить аутентичность данных, их целостность и защиту от повторного использования. «Атака посередине» позволит злоумышленнику повлиять на данные, поступающие в смарт-контракт, чтобы извлечь выгоду. Нарушение целостности поставленных данных, также как и повторное их использование окажет отрицательное влияние на работу системы и оценку производительности оракула.

Для решения вышеописанных проблем, модель использует алгоритм цифровой подписи RSA. В случае, если данные, отправленные оракулом и принятые смарт-контрактом подверглись изменению умышленно или в ходе технического сбоя, цифровая подпись окажется неверна, и система сможет распознать угрозу [9].

Алгоритм верификации данных будет выглядеть следующим образом:

1. Вычисление оракулом публичного n, e и приватного d ключей:
   a. Вычисление n:
   $$n = p * q, \text{ где } p \text{ и } q - \text{большие простые числа}$$
   b. Вычисление e:
   $$\varphi(n) = (p-1)(q-1);$$
   $$1 < e < \varphi(n) \text{ и } gcd(e, \varphi(n)) = 1;$$
   c. Вычисление d:
   $$d \equiv \frac{1(mod \varphi(n))}{e};$$
2. Передача смарт-контракту публичного ключа (n, e);
3. Каждый оракул перед поставкой данных в смарт-контракт формирует сообщение M, содержащее необходимые параметры и вычисляет подпись:
   $$\sigma = H(M)^d \bmod n, \text{ где } H - \text{хеш-функция (например, SHA-256);}$$
4. Передача оракулом смарт-контракту пары (M, σ);
5. Вычисление смарт-контрактом $H(M)$ и проверка подписи с помощью заранее переданного публичного ключа:
   $$\text{Если } \sigma^e mod\ n = H(M), \text{ то данные корректны}$$

Такой способ позволяет аутентифицировать оракул, проверить целостность поставленных данных, а также защититься от повторного использования старых сообщений.

XI. Тестирование разработанной модели

Предположим, что в эксперименте участвуют 4 оракула O_1, O_2, O_3, O_4. Для каждого оракула заданы параметры текущей корректности q_i, исторической надежности $\hat{p}_i$, задержки поставки данных Δt_i (в секундах) так, что:

Таблица 1. Инициализация параметров эксперимента

Параметр / Оракул	q_i	$\hat{p}_i$	Δt_i
O_1	0.95	0.92	0.05
O_2	0.9	0.88	0.06
O_3	0.85	0.85	0.07
O_4	0.8	0.8	0.08

Вычислим нормализованные веса w_i на основе исторической надежности:

- Сумма исторических надежностей:
$$\hat{p}_1 + \hat{p}_2 + \hat{p}_3 + \hat{p}_4 = 0.92 + 0.88 + 0.85 + 0.8 = 3.45;$$
- Тогда нормализованные веса оракулов:
$$w_1 = \frac{0.92}{3.45} \approx 0.2667;$$
$$w_2 = \frac{0.88}{3.45} \approx 0.2551;$$
$$w_3 = \frac{0.85}{3.45} \approx 0.2464;$$
$$w_4 = \frac{0.8}{3.45} \approx 0.2319;$$

Если допустить, что $p_i = \hat{p}_i$ на данной итерации оценки производительности t, то $P_{agg}^t \approx 0.9633$, что говорит о крайне высокой точности системы.

Определим варьируемые входные параметры системы чувствительности к несогласованности, нормировочной константы для индекса скорости и параметр влияния скорости как $\theta = 100$, $S_0 = 1.0$, $\mu = 1$ соответственно.

Вычислим взвешенное среднее текущей корректности:

$$\bar{q} = \sum_{i=1}^{4} w_i q_i ;$$

Получим:

$$\bar{q} \approx 0.2667 * 0.95 + 0.2551 * 0.9 + 0.2464 * 0.85 + 0.2319 * 0.8 = 0.8778;$$

Рассчитаем взвешенную дисперсию оценок корректности:

$$D(q) = \sum_{i=1}^{4} w_i (q_i - \bar{q})^2 ;$$

- Для O_1:
$$0.2667 * (0.95 - 0.8778)^2 = 0.2667 * 0.005213 = 0.00139;$$
- Для O_2:
$$0.2551 * (0.9 - 0.8778)^2 = 0.2551 * 0.0004928 = 0.000126;$$
- Для O_3:
$$0.2464 * (0.85 - 0.8778)^2 = 0.2464 * 0.0007728 = 0.00019;$$
- Для O_4:
$$0.2319 * (0.8 - 0.8778)^2 = 0.2319 * 0.006053 = 0.001403;$$

Суммарная дисперсия:

$$D(q) = 0.00139 + 0.000126 + 0.00019 + 0.001403 = 0.003109;$$

Расчет индекса скорости. Примем за эталонное значение задержку в 0.05 секунды:

$$S_i = \frac{q_i * \hat{p}_i * S_{target}}{\Delta t_i};$$

Для каждого оракула:

- Для O_1:
$$S_1 = \frac{0.95 * 0.92 * 0.05}{0.05} = 0.874;$$
- Для O_2:
$$S_2 = \frac{0.9 * 0.88 * 0.05}{0.06} = 0.66;$$
- Для O_3:
$$S_3 = \frac{0.85 * 0.85 * 0.05}{0.07} = 0.516;$$
- Для O_4:
$$S_4 = \frac{0.8 * 0.8 * 0.05}{0.08} = 0.4;$$

Для всего кластера:

$$S_{cluster} = \sum_{i=1}^{n} w_i S_i ;$$

$$S_{cluster} = 0.2667 * 0.874 + 0.2551 * 0.66 + 0.2464 * 0.516 + 0.2319 * 0.4 = 0.233 + 0.168 + 0.127 + 0.093 = 0.621;$$

Обобщенная оценка качества системы:

$$Q_{total}^{(t)} = P_{agg}^{(t)} * \bar{q}^{(t)} * \exp\left(-\theta D^{(t)}(q)\right) * (S_{cluster})^{\mu};$$

$$Q_{total}^{(t)} = 0.92 * 0.8778 * 0.733 * 0.621 = 0.368;$$

Полученное $Q_{total} \approx 0.368$ свидетельствует об уровне эффективности системы ниже среднего уровня, однако показатели частных параметров:

- $P_{agg} = 0.92$ означает высокую вероятность правильного агрегированного ответа;
- $\bar{q} \approx 0.8778$ демонстрирует высокое качество ответов;
- Низкая дисперсия $D(q) \approx 0.003109$ указывает на согласованность между оракулами кластера;
- $S_{cluster} = 0.621$ говорит о том, что данные поставляются недостаточно оперативно и данная метрика требует особого внимания в улучшении производительности системы.

XII. Недостатки разработанной модели

Хотя в разработанной модели входными данными являются формальные показатели работы оракулов, она требует инициализации некоторых параметров вручную. Например, такими параметрами являются чувствительность к дисперсии θ, влияние скорости μ, эталонное значение латентности S_{target}. Последствия некорректно выбранных параметров (значительно отличающихся от исторических или рекомендованных) повлечет за собой искаженный обобщенный показатель Q_{total}.

С другой стороны, преимуществом данного подхода является возможность варьировать эти параметры, основываясь на исторических показателях

системы, что повысит релевантность обобщенного показателя качества относительно программного и технического оснащения всей системы.

Для точного вычисления показателя агрегированной корректности P_{agg} используется суммирование по всем подмножествам оракулов, удовлетворяющих пороговому условию. При увеличении числа оракулов в системе число таких подмножеств экспоненциально возрастет, что приведет к большим вычислительным затратам.

Предложенный алгоритм цифровой подписи RSA поможет аутентифицировать данные на этапе взаимодействия оракул – смарт-контракт, но позволяет злоумышленнику устроить «атаку посередине» на этапе источник данных – оракул. Для обеспечения защиты на всех этапах взаимодействия сущностей системы необходимо организовать защиту и со стороны поставщика данных, что может быть довольно затруднительно, ведь, как правило, поставщиками данных являются третьи лица, не заинтересованные во вмешательстве в безопасность своей системы. Этот вопрос рассмотрен в работе Mik Eliza «Smart Contracts and the «Oracle Problem» in the Context of InsurTech» [10,11].

XIII. Заключение

Описанная модель оценки производительности кластера оракулов может быть использована в системах с самоисполняющимися смарт-контрактами как способ внутреннего аудита оценки качества системы.

Проведенный анализ актуальности проблемы достоверности поставленных данных и полученные результаты эксперимента позволяют судить о практической пользе разработки.

Представленный подход позволяет не только оценить производительность кластера оракулов, но и выявить слабые места в их работе, что является важным условием для повышения безопасности и надежности смарт-контрактов.

Несмотря на выявленные недостатки системы в виде присутствия параметров, которые при первичной инициализации системы должны быть заданы вручную на основе эмпирических данных, разнородности показателей производительности, образующих обобщенную оценку качества, возможности злоумышленником устроить «атаку посередине» на этапе сообщения оракула с источником данных, модель остается актуальной и открытой для дальнейших исследований и улучшений. Технологии нулевого разглашения (ZKProofs) смогут дополнить или заменить алгоритм цифровой подписи, а разбиение модели на отдельные сегменты разнородных показателей позволит получать более полные, точные и релевантные данные по результатам оценки определенных параметров системы [12].

Библиография

[1] Федосеев С.В. "Информационные и программные аспекты разработки и применения смарт-контрактов" // Правовая информатика. 2021. №3. DOI: 10.21681/1994-1404-2021-3-25-33

[2] Жихарев А.Г., Киданов В.В., Фефелов О.С. "К вопросу о безопасности обработки информации с использованием смарт-контрактов" // Научный результат. Информационные технологии. 2023. №1. DOI: 10.18413/2518-1092-2022-8-1-0-4

[3] Etherscan. "Ethereum Daily Deployed Contracts Chart" [Online]. Available: https://etherscan.io/chart/deployed-contracts

[4] Беликова К.М. "Исследование теоретических вопросов внедрения сетевых договоров (смарт-контрактов) на примере России и зарубежных стран" // Социально-политические науки. 2020. №5. DOI: 10.33693/2223-0092-2020-10-5-95-105

[5] Cong, Lin; Prasad, Eswar S.; Rabetti, Daniel. "Financial and Informational Integration Through Oracle Networks" (December 1, 2023) DOI: http://dx.doi.org/10.2139/ssrn.4495514

[6] Chainlink. "Chainlink Whitepaper" [Online]. Available: https://chain.link/whitepaper

[7] Кацко И.А., Швырёва О.И., Киёк М.О. "Моделирование современных тенденций риск-ориентированного аудита с применением теоремы Байеса" // Научный журнал КубГАУ. 2016. №115.

[8] Egberts, Alexander. "The Oracle Problem - An Analysis of how Blockchain Oracles Undermine the Advantages of Decentralized Ledger Systems" (December 12, 2017) DOI: http://dx.doi.org/10.2139/ssrn.3382343

[9] Бакаева О.А., Барабошкин Д.А. "Разработка протокола передачи данных на основе комбинированного алгоритма их шифрования" // Программные продукты и системы. 2023. №3. DOI: 10.15827/0236-235X.142.493-502

[10] Смирнов Д.В., Сотников А.И., Асеев А.Ю. "Обеспечение безопасности системы электронной почты от типа атак 'человек посередине' на основе блокчейна" // Вестник Череповецкого государственного университета. 2018. №4 (85). DOI: 10.23859/1994-0637-2018-4-85-4

[11] Mik, Eliza. "Smart Contracts and the 'Oracle Problem' in the Context of InsurTech" (Feb 13, 2023) DOI: http://dx.doi.org/10.2139/ssrn.4390271

[12] Черемушкин А.В. "Системы с открытыми ключами на основе идентификационной информации" // ПДМ. 2023. №61. DOI: 10.17223/20710410/61/4

Статья получена 26 февраля 2025.

Булгаков В.Д. – Белгородский государственный технологический университет имени В. Г. Шухова (e-mail: bulgakovvlad@yandex.ru).
Гвоздевский И.Н. – Белгородский государственный технологический университет имени В. Г. Шухова (e-mail: Gvozdevskiy.in@bstu.ru).

Performance evaluation model for oracles in self-executing smart contracts

Vladislav Bulgakov, Igor Gvozdevsky

***Abstract* - The article presents a model for evaluating the performance of oracles used in self-executing smart contracts. Performance is defined as a composite of parameters including data delivery speed, accuracy of transmitted information, and the security level of the oracle cluster. The proposed model integrates weighted data aggregation mechanisms, the application of asymmetric penalties for inaccurate results, as well as formal methods for assessing oracle quality using probabilistic models and statistical analysis. The study analyzes existing approaches to ensuring the reliability of data provided by oracles. It examines both consensus mechanisms-which allow the aggregation of information from multiple independent sources-and approaches based on the use of trusted data sources selected manually. The analysis emphasizes that traditional evaluation methods often fail to capture the dynamic nature of the system and lack the necessary flexibility to adapt to changing conditions. As a solution, an internal audit methodology for oracle clusters is proposed, enabling both quantitative and qualitative assessment of their reliability and effectiveness, which is particularly relevant for governmental and corporate blockchain systems.**

***Keywords* - oracle, blockchain, smart contract, performance, model, evaluation.**

REFERENCES

[1] Fedoseev, S.V. “Information and Software Aspects of the Development and Application of Smart Contracts” // Legal Informatics. 2021, No. 3. DOI: 10.21681/1994-1404-2021-3-25-33.

[2] Zhikhariev, A.G.; Kidanov, V.V.; Fefelev, O.S. “On the Issue of Information Processing Security Using Smart Contracts” // Scientific Outcome. Information Technologies. 2023, No. 1. DOI: 10.18413/2518-1092-2022-8-1-0-4.

[3] Etherscan. “Ethereum Daily Deployed Contracts Chart” [Online]. Available: https://etherscan.io/chart/deployed-contracts (accessed: 24.02.2025).

[4] Belikova, K.M. “A Study of Theoretical Issues of Implementing Network Contracts (Smart Contracts) Using the Example of Russia and Foreign Countries” // Social and Political Sciences. 2020, No. 5. DOI: 10.33693/2223-0092-2020-10-5-95-105.

[5] Cong, Lin; Prasad, Eswar S.; Rabetti, Daniel. “Financial and Informational Integration Through Oracle Networks” (December 1, 2023). DOI: http://dx.doi.org/10.2139/ssrn.4495514.

[6] Chainlink. “Chainlink Whitepaper” [Online]. Available: https://chain.link/whitepaper (accessed: 24.02.2025).

[7] Katsko, I.A.; Shvyryova, O.I.; Kiyok, M.O. “Modeling of Modern Trends in Risk-Oriented Auditing Using Bayes’ Theorem” // Scientific Journal of Kuban State Agrarian University, 2016, No. 115.

[8] Egberts, Alexander. “The Oracle Problem – An Analysis of How Blockchain Oracles Undermine the Advantages of Decentralized Ledger Systems” (December 12, 2017). DOI: http://dx.doi.org/10.2139/ssrn.3382343.

[9] Bakaeva, O.A.; Baraboshkin, D.A. “Development of a Data Transmission Protocol Based on a Combined Encryption Algorithm” // Software Products and Systems. 2023, No. 3. DOI: 10.15827/0236-235X.142.493-502.

[10] Smirnov, D.V.; Sotnikov, A.I.; Aseev, A.Yu. “Ensuring the Security of an Email System Against ‘Man-in-the-Middle’ Attacks Based on Blockchain” // Bulletin of Cherepovets State University. 2018, No. 4 (85). DOI: 10.23859/1994-0637-2018-4-85-4.

[11] Mik, Eliza. “Smart Contracts and the ‘Oracle Problem’ in the Context of InsurTech” (February 13, 2023). DOI: http://dx.doi.org/10.2139/ssrn.4390271.

[12] Cheremushkin, A.V. “Systems with Public Keys Based on Identification Information” // PDM. 2023, No. 61. DOI: 10.17223/20710410/61/4.