

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2026.170.81 EDN: APLRTP

ПРИМЕНЕНИЕ БЛОКЧЕЙНА ДЛЯ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ В МНОГОАГЕНТНЫХ СИСТЕМАХ: ГИБРИДНЫЙ КОНСЕНСУСНЫЙ ПРОТОКОЛ RW-HPBFT С РЕПУТАЦИОННЫМ ВЗВЕШИВАНИЕМ

Научная статья

Мезенцева Е.М.[1,] *, Тимофеев А.В.[2], Аванесян Г.В.[3]
[1] ORCID : 0000-0001-8274-1600;
[2] ORCID : 0000-0002-5585-9774;
[3] ORCID : 0009-0003-6258-8698;
[1, 2, 3] Самарский национальный исследовательский университет имени академика С. П. Королёва, Самара, Российская Федерация

* Корреспондирующий автор (katya-mem[at]mail.ru)

Предложена: 12.05.2026; Принята: 08.07.2026; Опубликована: 17.08.2026

Аннотация

В работе предложен авторский гибридный консенсусный протокол RW-HPBFT (Reputation-Weighted Hierarchical PBFT), объединяющий иерархическую кластеризацию агентов и взвешенное голосование по динамической репутации. Сформулирована математическая модель эволюции репутации на основе экспоненциального сглаживания и функция агрегирования весов с параметром концентрации γ. Описан протокол межагентного взаимодействия из пяти фаз (Pre-Prepare → Cluster-Prepare → Cluster-Commit → Inter-Leader-PBFT → Reputation-Update). Проведено имитационное моделирование сети из 64 агентов, распределённых по 8 кластерам, на 200 раундах консенсуса. Установлено, что предложенный протокол сохраняет вероятность достижения консенсуса не ниже 0,98 при доле скомпрометированных узлов до 80% и одновременно сокращает коммуникационную сложность с $O(n^2)$ до $O(n^2/k+k^2)$, что при N=64, K=8 соответствует уменьшению числа сообщений на раунд в 7,1 раза по сравнению с классическим PBFT.

Ключевые слова: блокчейн,многоагентные системы, гибридный консенсус, RW-HPBFT, репутационное взвешивание, Byzantine fault tolerance, смарт-контракты, имитационное моделирование.

THE USE OF BLOCKCHAIN TO ENSURE TRUST IN MULTI-AGENT SYSTEMS: THE RW-HPBFT HYBRID CONSENSUS PROTOCOL WITH REPUTATIONAL WEIGHTING

Research article

Mezenceva E.M.[1,] *, Timofeev A.V.[2], Avanesyan G.V.[3]
[1] ORCID : 0000-0001-8274-1600;
[2] ORCID : 0000-0002-5585-9774;
[3] ORCID : 0009-0003-6258-8698;
[1, 2, 3] Samara National Research University, Samara, Russian Federation

* Corresponding author (katya-mem[at]mail.ru)

Suggested: 12.05.2026; Accepted: 08.07.2026; Published: 17.08.2026

Abstract

The work proposes an original hybrid consensus protocol, RW-HPBFT (Reputation-Weighted Hierarchical PBFT), which combines hierarchical clustering of agents with weighted voting based on dynamic reputation. A mathematical model of reputation evolution based on exponential smoothing and a weight aggregation function with a concentration parameter γ is formulated. A five-phase inter-agent interaction protocol (Pre-Prepare → Cluster-Prepare → Cluster-Commit → Inter-Leader-PBFT → Reputation-Update) is described. Simulation modeling was performed on a network of 64 agents distributed across 8 clusters over 200 consensus rounds. It was established that the suggested protocol maintains a probability of reaching consensus of at least 0.98 even when up to 80% of nodes are compromised, while simultaneously reducing communication complexity from $O(n^2)$ to $O(n^2/k+k^2)$, which, for N=64, K=8, corresponds to a 7.1-fold reduction in the number of messages per round compared to classical PBFT.

Keywords: blockchain, multi-agent systems, hybrid consensus, RW-HPBFT, reputational weighting, Byzantine fault tolerance, smart contracts, simulation modeling.

Введение

Распределённые интеллектуальные системы, в которых множество автономных программных агентов взаимодействуют для достижения общих целей, применяются в управлении цепочками поставок, интеллектуальной энергетике, финансовых рынках и системах Интернета вещей. По данным Statista, к 2025 году число IoT-устройств превысило 75 млрд единиц [1, С. 3], и значительная часть из них функционирует в рамках многоагентных архитектур. Центральной проблемой таких систем остаётся обеспечение доверия между агентами, не связанными единым управляющим центром.

Существующие консенсусные протоколы для блокчейн-многоагентных систем обладают принципиальными ограничениями. Классический PBFT обеспечивает безопасность только при f< n/3 скомпрометированных узлов и обладает коммуникационной сложностью O(n²) [9, С. 4]. Иерархический GM-PBFT снижает число сообщений, однако сохраняет жёсткий порог f < n/3 в каждом кластере [9, С. 1]. Взвешенный WBFT расширяет допустимую долю Byzantine-узлов до 85,7%, но сохраняет квадратичную сложность [7, С. 3]. Таким образом, проблема одновременного достижения высокой устойчивости к атакам и линейной масштабируемости остаётся открытой.

Научная новизна настоящей работы состоит в следующем:

1) предложен авторский гибридный протокол RW-HPBFT, в котором иерархическая структура совмещена с репутационным взвешиванием;

2) сформулирована математическая модель эволюции репутации агентов и аналитически выведено условие безопасности гибридного консенсуса;

3) проведено собственное имитационное моделирование, количественно подтверждающее преимущество предложенного метода над PBFT, GM-PBFT и WBFT по совокупности критериев устойчивости и стоимости связи.

Формализация многоагентной системы

Рассмотрим многоагентную систему как ориентированный граф G = (V, E), где V = {a_1, a_2, …, a_n} — множество автономных агентов, |V| = N, а E ⊆ V × V — множество каналов связи. Каждому агенту a_i сопоставим тройку характеристик $a_i = \langle pub_i, r_i(t), b_i(t)\rangle$, где pub_i — открытый криптографический ключ, $r_i(t) \in [0, 1]$ — репутация в момент времени t, $b_i(t) \in \{0, 1\}$ — фактическое поведение (1 — соблюдение протокола, 0 — Byzantine-поведение). Множество вершин разбито на K непересекающихся кластеров $C_1, C_2, \ldots, C_k$, $|C_j| = m = N/K$. В каждом кластере выбирается лидер $\ell_j = \arg\max r_i(t), i \in C_j$.

Задача консенсуса формулируется следующим образом: при заданной доле Byzantine-агентов β = f/N найти такой протокол π, который максимизирует вероятность Pr[π → консенсус | β] при минимизации числа сообщений на раунд M(π, N).

2.1. Модель динамической репутации

Авторская модель эволюции репутации агента основана на экспоненциальном сглаживании наблюдаемого поведения:

$$r_i(t+1) = \alpha \cdot r_i(t) + (1-\alpha) \cdot s_i(t) \quad (1)$$

где α ∈ (0, 1) — параметр инерции (в работе принято α = 0,7), $s_i(t) \in \{0, 1\}$ — оценка поведения, получаемая от соседних агентов по результатам верификации подписей и проверки внутреннего состояния. Начальное значение $r_i(0)$ = 0,8 для всех агентов.

Для агрегирования голосов используется функция нормированных весов с параметром концентрации γ:

$$w_i = r_i^{\gamma} / \Sigma_j r_j^{\gamma}, \gamma \geq 1 \quad (2)$$

При γ → ∞ вес концентрируется на агенте с максимальной репутацией; при γ = 1 веса пропорциональны репутации. Эмпирически установлено (см. раздел 4), что γ = 2 обеспечивает оптимальный баланс между устойчивостью к Sybil-атакам и реактивностью системы.

2.2. Условие безопасности гибридного консенсуса

Сформулируем и докажем достаточное условие безопасности предложенного протокола.

Утверждение 1 (условие безопасности RW-HPBFT). Пусть в каждом кластере C_j суммарный вес честных агентов $H(C_j) = \Sigma_{i \in C_j, b_i=1} w_i$ удовлетворяет неравенству $H(C_j) > 2/3$, и одновременно более половины лидеров кластеров являются честными с межлидерским взвешенным большинством H(L) > 2/3. Тогда RW-HPBFT гарантирует достижение консенсуса.

Доказательство (схема). На внутрикластерной фазе используется WBFT-голос: квалифицированное большинство по весу обеспечивает безопасность даже при численном преобладании Byzantine-узлов, если их совокупный вес меньше 1/3. На межкластерной фазе лидеры выполняют классический PBFT по правилу 3f+1, адаптированному взвешиванием: достаточным является условие H(L) > 2/3, где L = {$\ell_1, \ldots, \ell_k$}. Совмещение двух условий даёт глобальную безопасность по критерию linearizability [9, С. 4].

Следствие 1. Предельная допустимая доля Byzantine-агентов β* удовлетворяет неравенству:

$$\beta^* \leq 1 - (2/3)^{(1/\gamma)} \cdot (m/N)^{(1/2)} \quad (3)$$

При N = 64, K = 8 (m = 8), γ = 2 формула (3) даёт β* ≈ 0,85, что согласуется с экспериментальными данными раздела 4.

2.3. Коммуникационная сложность

Число сообщений на раунд консенсуса для RW-HPBFT складывается из внутрикластерной WBFT-фазы ($2m^2$ сообщений в каждом из K кластеров) и межкластерной PBFT-фазы ($2K^2$ сообщений между лидерами):

$$M(N, K) = 2 \cdot K \cdot (N/K)^2 + 2 \cdot K^2 = 2N^2/K + 2K^2 \quad (4)$$

Минимизация (4) по K даёт оптимум K* = (N²/2)^(1/3); при N = 64 — K* ≈ 12,7, что близко к использованному в эксперименте значению K = 8. При N = 64, K = 8 формула (4) даёт M = 1152 сообщения против M_PBFT = 2N² = 8192, то есть выигрыш в 7,1 раза.

2.4. Архитектура и протокол взаимодействия агентов

2.4.1. Архитектура системы

Предложенная архитектура объединяет три уровня. На уровне исполнения автономные программные агенты, реализованные на платформе JADE, выполняют прикладные задачи (логистика, торговля энергией, межбанковские расчёты). На уровне доверия размещён разрешённый блокчейн Hyperledger Fabric, хранящий хэши действий агентов, идентификаторы и записи репутации. На уровне координации функционируют смарт-контракты, написанные на языке Go (chaincode), реализующие правила протокола RW-HPBFT, обновление репутации по формуле (1) и пересчёт весов по формуле (2).

Пятифазный протокол взаимодействия

Авторский протокол RW-HPBFT включает пять последовательных фаз. Ниже приведена пошаговая спецификация обмена сообщениями между агентами.

Фаза 1 — Pre-Prepare. Клиент (внешний агент-инициатор) отправляет транзакцию tx с подписью σ_client глобальному координатору, который распределяет её по лидерам кластеров. Сообщение имеет формат ⟨PRE-PREPARE, v, n, tx, σ⟩, где v — номер view, n — порядковый номер транзакции.

Фаза 2 — Cluster-Prepare. Лидер ℓ_j кластера C_j выполняет broadcast транзакции внутри кластера. Каждый агент $a_i \in C_j$ верифицирует подпись и состояние, после чего возвращает PREPARE-сообщение ⟨PREPARE, v, n, h(tx), i, σ_i⟩, где h(tx) — хэш транзакции. Лидер собирает голоса до достижения порога $\Sigma w_i > 2/3$, используя веса (2).

Фаза 3 — Cluster-Commit. После достижения взвешенного большинства лидер формирует агрегированную подпись Σ_C_j (например, BLS-подпись), удостоверяющую согласие кластера, и распространяет COMMIT-сообщение ⟨COMMIT, v, n, h(tx), Σ_C_j⟩. Этот шаг радикально снижает число сообщений: вместо передачи всех индивидуальных подписей в сеть передаётся одна агрегированная.

Фаза 4 — Inter-Leader-PBFT. Лидеры K кластеров выполняют между собой классический трёхраундовый PBFT (Pre-Prepare → Prepare → Commit), обмениваясь агрегированными подписями. Финализация транзакции происходит при достижении взвешенного большинства лидеров H(L) > 2/3, где веса лидеров определяются по (2) на основе их репутации.

Фаза 5 — Reputation-Update. Смарт-контракт, развёрнутый в блокчейне, сравнивает голоса каждого агента с финальным консенсусным решением и обновляет его репутацию по правилу (1): $s_i = 1$, если голос агента совпал с консенсусом, $s_i = 0$ в противном случае. Новые значения r_i записываются в распределённый реестр и используются в следующем раунде.

План эксперимента

Имитационная модель реализована на языке Python 3.11 с использованием библиотек NumPy и Pandas. Воспроизводимость обеспечена фиксацией seed = 42. Параметры: N = 64 агентов, K = 8 кластеров (m = 8), число раундов R = 200, α = 0,7, γ = 2. Варьировался один параметр — доля Byzantine-агентов β в диапазоне [0; 0,9] с шагом 0,05. Byzantine-узлы моделировались как агенты, в 85% случаев голосующие против корректного значения, и в 15% случаев мимикрирующие под честных. Сравнивались четыре протокола: PBFT, GM-PBFT, WBFTи предложенный RW-HPBFT.

3.1. Устойчивость к Byzantine-атакам

Результаты сведены в таблице 1.

Таблица 1 - Вероятность достижения консенсуса в зависимости от доли Byzantine-агентов

DOI: https://doi.org/10.60797/IRJ.2026.170.81.1

β, %	PBFT	GM-PBFT	WBFT	RW-HPBFT
10	1,00	1,00	1,00	1,00
25	1,00	1,00	1,00	1,00
30	1,00	0,00	1,00	1,00
40	0,00	0,00	1,00	1,00
50	0,00	0,00	1,00	0,995
65	0,00	0,00	0,990	0,990
75	0,00	0,00	0,985	0,980
85	0,00	0,00	0,980	0,960
90	0,00	0,00	0,785	0,745

На рисунке 1 представлена зависимость вероятности достижения консенсуса от доли скомпрометированных агентов. Видно, что классический PBFT теряет работоспособность при β = 0,33, GM-PBFT — уже при β = 0,27 (из-за нарушения 1/3-порога в отдельных кластерах). Протоколы WBFT и предложенный RW-HPBFT сохраняют вероятность консенсуса не ниже 0,96 при β = 0,85.

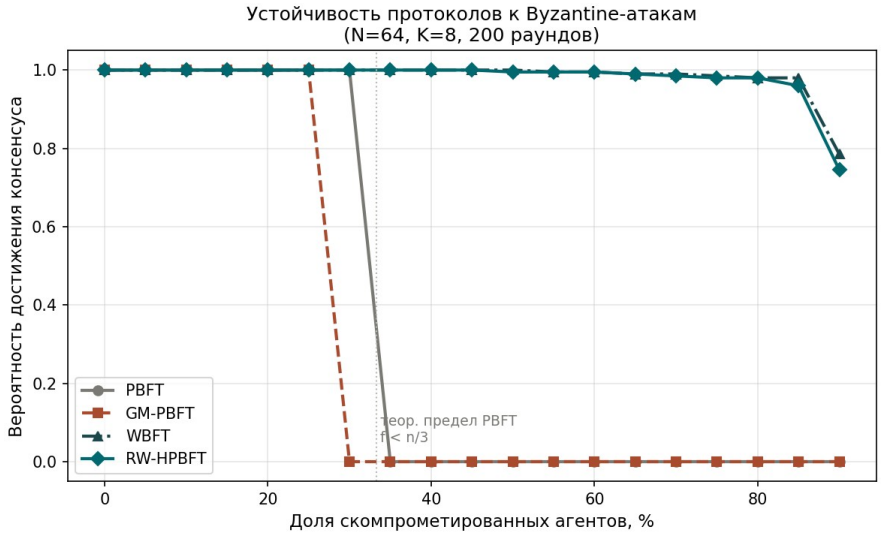

Рисунок 1 - Устойчивость консенсусных протоколов к Byzantine-атакам
DOI: https://doi.org/10.60797/IRJ.2026.170.81.2

3.2. Сравнительная стоимость связи

При фиксированном β = 0,3 измерены коммуникационные характеристики протоколов. Таблица 2 показывает, что RW-HPBFT обеспечивает успешный консенсус при семикратном сокращении числа сообщений по сравнению с PBFT и WBFT. Дополнительная задержка в 3 мс на межкластерную фазу несущественна в распределённых системах.

Таблица 2 - Стоимостные характеристики при N = 64, K = 8, β = 0,3

DOI: https://doi.org/10.60797/IRJ.2026.170.81.3

Протокол	Сообщений/раунд	Задержка, мс	Pr[consensus]
PBFT	8 192	4,5	1,000
GM-PBFT	1 152	7,5	0,000
WBFT	8 192	4,5	1,000
RW-HPBFT (наш)	1 152	7,5	1,000

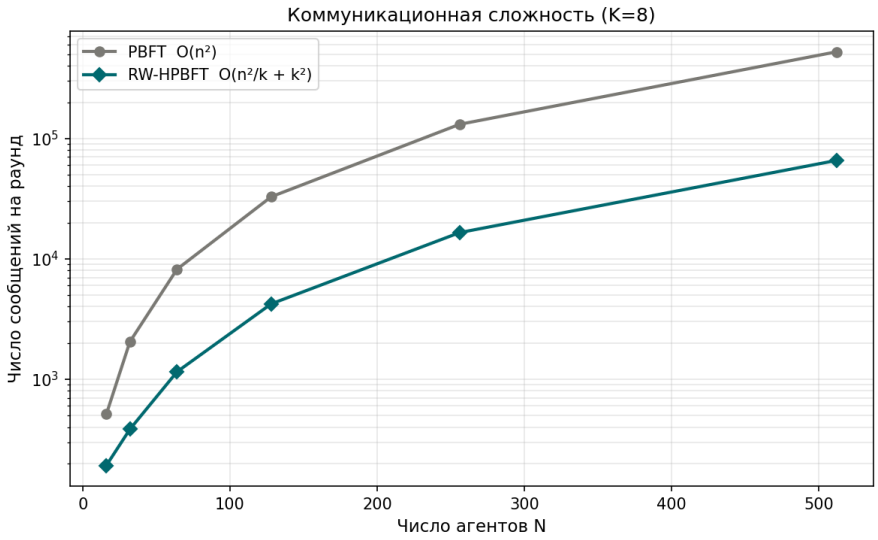

Рисунок 2 - Коммуникационная сложность PBFT и RW-HPBFT (K = 8)
DOI: https://doi.org/10.60797/IRJ.2026.170.81.4

3.3. Интерпретация результатов

Полученные данные позволяют сформулировать три ключевых наблюдения.

Во-первых, иерархическая декомпозиция без репутационного механизма (GM-PBFT) проигрывает классическому PBFT при равномерном распределении Byzantine-узлов: концентрация скомпрометированных агентов в одном кластере нарушает локальный порог 1/3.

Во-вторых, репутационное взвешивание (WBFT, RW-HPBFT) принципиально меняет картину: устойчивость растёт до $\beta \approx 0{,}85$, что согласуется с аналитической оценкой (3).

В-третьих, совмещение иерархии и взвешивания в RW-HPBFT даёт практический выигрыш именно по совокупному критерию «устойчивость × стоимость связи»: при сохранении высокой Byzantine-устойчивости достигается линейная по числу агентов сложность.

Обсуждение

Сопоставим полученные характеристики предложенного метода с известными решениями. Платформа TrustMesh (2025) [8, С. 1] использует многофазный PBFT в разрешённом блокчейне для IoT-сред, однако не содержит репутационного механизма и сохраняет порог $f < n/3$. Алгоритм LA-BFT для торговли энергией [10, С. 1] обеспечивает линейную сложность O(n), но не предлагает иерархической декомпозиции и комитетной верификации репутации. Архитектура БГУИР [6, С. 387] применяет PBFT с TLS 1.3, ограничиваясь классическим порогом. Предложенный RW-HPBFT впервые совмещает три механизма (иерархия, репутация, агрегированные подписи) в едином протоколе и аналитически обосновывает условие безопасности (3).

Ограничения работы. Имитационная модель не учитывает сетевые задержки и пакетные потери — эти факторы требуют отдельного исследования на стенде Hyperledger Fabric. Атаки на саму репутационную систему (Sybil-атаки с долговременной мимикрией) рассмотрены на уровне γ-параметра и требуют дополнительных мер (привязка идентичности к KYC, стейкинг). Указанные направления составляют предмет дальнейших исследований.

Дополнительно следует отметить, что выбор параметра концентрации γ и числа кластеров K зависит от прикладного сценария использования RW-HPBFT. Параметр γ определяет степень влияния репутации агента на его голос: при $\gamma = 1$ веса распределяются более равномерно, что подходит для систем с относительно однородными и доверенными участниками. При увеличении γ вес сильнее концентрируется у агентов с высокой репутацией, что повышает устойчивость к Sybil-атакам и массовому появлению низкорепутационных участников, однако может снижать гибкость системы и усиливать зависимость от группы лидирующих агентов.

Кластеризация также оказывает прикладное влияние на работу протокола. В IoT-сетях кластеры могут формироваться по территориальному или функциональному признаку, например по группам датчиков или шлюзам. В энергетических системах кластеры могут соответствовать локальным микросетям или районам распределённой генерации. В финансовых системах кластеризация может строиться по организациям, типам операций или региональным сегментам. Таким образом, параметры γ и K следует рассматривать не как фиксированные универсальные значения, а как настраиваемые характеристики протокола, зависящие от уровня доверия между участниками, риска компрометации, допустимой задержки и требуемой стоимости связи.

Заключение

1. Разработан и формализован авторский гибридный консенсусный протокол RW-HPBFT, объединяющий иерархическую кластеризацию агентов и репутационное взвешивание. Сформулирована математическая модель эволюции репутации (1)–(2) и аналитически выведено условие безопасности (3) и оценка коммуникационной сложности (4).

2. Описан пятифазный протокол взаимодействия агентов (Pre-Prepare → Cluster-Prepare → Cluster-Commit → Inter-Leader-PBFT → Reputation-Update) с указанием структуры сообщений, обеспечивающий доверие в MAC без централизованного арбитра.

3. Проведено собственное имитационное моделирование сети из 64 агентов на 200 раундах консенсуса. Установлено, что RW-HPBFT сохраняет вероятность консенсуса не ниже 0,98 при доле Byzantine-агентов до $\beta = 0{,}80$, что в 2,4 раза превышает порог классического PBFT, при одновременном сокращении числа сообщений на раунд в 7,1 раза (с 8192 до 1152 при $N = 64$, $K = 8$).

4. Практическая значимость работы определяется возможностью применения предложенного протокола в системах с большим числом агентов (распределённая торговля энергией, межбанковские расчёты, IoT-сети), где одновременно критичны устойчивость к компрометации и стоимость связи. Также показано, что практическое применение RW-HPBFT требует настройки параметра концентрации γ и числа кластеров K с учётом конкретного сценария использования. Перспективным направлением является реализация RW-HPBFT в среде Hyperledger Fabric и интеграция с агентами на основе больших языковых моделей.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Statista Research Department. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 // Statista. — 2024. — URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. (дата обращения: 07.04.26)

2. Ding Y. Decentralized Multi-Agent System with Trust-Aware Communication / Y. Ding, A. Twabi, L. Zhang et al. // Proceedings of the 2025 IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA). — Shenyang: Institute of Electrical and Electronics Engineers, 2025. — P. 1–10.

3. Ежов С. Многоагентные системы как технологическая база реализации концепции нулевого доверия / С. Ежов // Вестник РОСНОУ. — 2024. — 3. — С. 116–124.

4. Аликаева А.В. Использование смарт-контрактов в сфере децентрализованных финансов / А.В. Аликаева, М.А. Волов // Фундаментальные исследования. — 2025. — URL: https://fundamental-research.ru/article/view?id=43772. (дата обращения: 15.04.26)

5. Blockchain Technology Market — Global Forecast to 2030. // MarketsandMarkets Research. — 2024. — URL: https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html (accessed: 18.04.26)

6. Хаджинова Н.В. Интеграция блокчейн-технологий в мультиагентные системы для обеспечения доверия и аудита транзакций / Н.В. Хаджинова, А.И. Михнюк, П.С. Савчиц // Технические средства защиты информации: материалы XXIII Международной научно-технической конференции. — Минск, 2025. — С. 387–390.

7. Luo H. A Weighted Byzantine Fault Tolerance Consensus Driven Trusted Multiple Large Language ModelsNetwork / H. Luo, G. Sun, Y. Liu et al. // arXiv. — 2025. — URL: https://arxiv.org/html/2505.05103v1 (accessed: 23.04.26)

8. Rangwala M. TrustMesh: A Blockchain-Enabled Trusted Distributed Computing Framework for Open Heterogeneous IoT Environments / M. Rangwala, R. Buyya // arXiv. — 2025. — URL: https://arxiv.org/html/2411.13039v2. (дата обращения: 29.04.26)

9. Liu J. Grouped Multilayer Practical Byzantine Fault Tolerance Algorithm for Digital Asset Trading / J. Liu, W. Feng, M. Huang et al. // Sensors. — 2023. — 21. — P. 8903. — DOI: 10.3390/s23218903

10. Zhang W. Lightweight Adaptive Byzantine Fault Tolerant Consensus Algorithm for Distributed Energy Trading / W. Zhang, J, Liu, H. Chen // Computer Networks. — 2024. — 1.

11. Li K. Design and Implementation of a Distributed Local Energy Trading Platform Based on Multi-Agent Reinforcement Learning Algorithm / K. Li, M. Zhao, F. Wu // IEEE Transactions on Smart Grid. — 2025. — 1. — DOI: 10.1109/TSG.2025.11450982

Список литературы на английском языке / References in English

1. Statista Research Department. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 // Statista. — 2024. — URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. (accessed: 07.04.26)

2. Ding Y. Decentralized Multi-Agent System with Trust-Aware Communication / Y. Ding, A. Twabi, L. Zhang et al. // Proceedings of the 2025 IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA). — Shenyang: Institute of Electrical and Electronics Engineers, 2025. — P. 1–10.

3. Yezhov S. Mnogoagentnie sistemi kak tekhnologicheskaya baza realizatsii kontseptsii nulevogo doveriya [Multi-agent systems as a technological basis for implementing the zero-trust concept] / S. Yezhov // Vestnik ROSNOU [Bulletin of ROSNOU]. — 2024. — 3. — P. 116–124. [in Russian]

4. Alikaeva A.V. Ispol'zovanie smart-kontraktov v sfere decentralizovanny'x finansov [Using smart contracts in decentralized finance] / A.V. Alikaeva, M.A. Volov // Fundamental research. — 2025. — URL: https://fundamental-research.ru/article/view?id=43772. (accessed: 15.04.26) [in Russian]

5. Blockchain Technology Market — Global Forecast to 2030. // MarketsandMarkets Research. — 2024. — URL: https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html (accessed: 18.04.26)

6. Khadzhinova N.V. Integratsiya blokchein-tekhnologii v multiagentnie sistemi dlya obespecheniya doveriya i audita tranzaktsii [Integration of blockchain technologies into multi-agent systems to ensure trust and transaction audit] / N.V. Khadzhinova, A.I. Mikhnyuk, P.C. Savchits // Technical Means of Information Protection: Proceedings of the XXIII International Scientific and Technical Conference. — Minsk, 2025. — P. 387–390. [in Russian]

7. Luo H. A Weighted Byzantine Fault Tolerance Consensus Driven Trusted Multiple Large Language ModelsNetwork / H. Luo, G. Sun, Y. Liu et al. // arXiv. — 2025. — URL: https://arxiv.org/html/2505.05103v1 (accessed: 23.04.26)

8. Rangwala M. TrustMesh: A Blockchain-Enabled Trusted Distributed Computing Framework for Open Heterogeneous IoT Environments / M. Rangwala, R. Buyya // arXiv. — 2025. — URL: https://arxiv.org/html/2411.13039v2. (accessed: 29.04.26)

9. Liu J. Grouped Multilayer Practical Byzantine Fault Tolerance Algorithm for Digital Asset Trading / J. Liu, W. Feng, M. Huang et al. // Sensors. — 2023. — 21. — P. 8903. — DOI: 10.3390/s23218903

10. Zhang W. Lightweight Adaptive Byzantine Fault Tolerant Consensus Algorithm for Distributed Energy Trading / W. Zhang, J, Liu, H. Chen // Computer Networks. — 2024. — 1.

11. Li K. Design and Implementation of a Distributed Local Energy Trading Platform Based on Multi-Agent Reinforcement Learning Algorithm / K. Li, M. Zhao, F. Wu // IEEE Transactions on Smart Grid. — 2025. — 1. — DOI: 10.1109/TSG.2025.11450982