УДК 336 DOI: 10.14451/1.251.291

Трансформация корпоративного управления цифровыми активами в эпоху распределённых технологий: роль искусственного интеллекта и блокчейн-систем второго поколения

© 2025 **Пискарёва Александра Юрьевна**
Студент 4 курса бакалавриата. Финансовый университет при Правительстве РФ.
E-mail: 221236@edu.fa.ru

© 2025 **Обухович Алексей Романович**
Студент 4 курса бакалавриата. Финансовый университет при Правительстве РФ.
E-mail: obukhovichforbb@gmail.com

© 2025 **Переход Сергей Александрович**
Кандидат экономических наук, Лаборатория Фининвест, Кафедры финансовых рынков и финансового инжиниринга. Финансовый университет при Правительстве РФ.
E-mail: saperekhod@fa.ru

Ключевые слова: цифровые активы, корпоративное управление, агентская теория, блокчейн 2.0, искусственный интеллект, DAO, токеномика, децентрализация, смарт-контракты, риски.

В статье исследуется трансформация корпоративного управления цифровыми активами в условиях стремительного развития технологий распределённых реестров и блокчейн-систем второго поколения. Рассматриваются проблемы агентских конфликтов, асимметрии информации и морального риска в децентрализованных автономных организациях (DAO). Анализируется роль искусственного интеллекта в мониторинге транзакций, автоматизации смарт-контрактов и снижении рисков манипуляций. Проведено сопоставление теоретических основ агентской теории с современными цифровыми экосистемами, выявлены ключевые факторы централизации власти и новые формы оппортунизма. Теоретическая и практическая значимость исследования заключается в разработке концептуальной модели интеграции ИИ и блокчейн 2.0 для повышения прозрачности, устойчивости и эффективности корпоративного управления цифровыми активами.

Введение

В последние годы наблюдается стремительный рост криптоэкономики, обусловленный развитием технологий распределённых реестров, широким внедрением блокчейн-решений и расширением применения цифровых активов в различных секторах экономики. Процессы токенизации капитала, появление децентрализованных автономных организаций и цифровых платформ, основанных на смарт-контрактах, трансформируют традиционные представления о собственности, управлении и распределении экономических ресурсов, в результате чего формируются новые модели корпоративного взаимодействия, где ключевую роль играют не институциональные структуры, а децентрализованные сети и алгоритмические механизмы принятия решений (Manakhova, Kolmykov, 2025).

Одновременно с этим развитие цифровой экономики сопровождается появлением новых рисков и специфических вызовов для корпоративного управления. Классические модели, базирующиеся на централизованной структуре принятия решений, иерархической ответственности агентов перед принципалами, оказываются недостаточно эффективными в условиях децентрализованных экосистем. Традиционные механизмы мониторинга и контроля не обеспечивают необходимой прозрачности и доверия в среде, где власть и решение распределены между участниками на основе владения токенами и механизмов консенсуса сети.

Особое значение приобретает проблема новых форм агентских конфликтов, выражающихся в манипулировании токенами, злоупотреблениях в управлении DAO, а также несанкционированных изменениях алгоритмов смарт-контрактов и использовании асимметричной информации в целях извлечения частной выгоды (Asryan, 2025). В этой связи особую актуальность приобретает исследование роли современных технологических решений прежде всего искусственного интеллекта и блокчейн-систем нового поколения в трансформации корпоративного управления цифровыми активами.

Целью настоящего исследования является анализ потенциала интеграции ИИ и блокчейн 2.0 для совершенствования корпоративного управления цифровыми активами, а также выявление их вклада в снижение агентских конфликтов и повышение устойчивости децентрализованных экономических систем.

Теоретические основы корпоративного управления и агентских отношений

Агентские отношения формируют одну из фундаментальных категорий в современной экономической науке и практике корпоративного управления. В наиболее общем виде они возникают в ситуации, когда одна сторона (принципал) делегирует другой стороне (агенту) полномочия управлять ресурсами или принимать управленческие решения от ее имени (Dulzon, 2009). Делегирование способствует повышению эффективности использования ресурсов и специализации труда, но одновременно порождает потенциальные конфликты интересов, обусловленные несовпадением целей сторон.

Классическая агентская теория получила своё формальное оформление в работе Дженсена и Меклинга (1976), где доказано, что разделение собственности и контроля в корпорациях порождает проблемы агентских конфликтов, проявляющихся в расхождении между стремлением акционеров к максимизации долгосрочной стоимости компании и желанием менеджеров максимизировать собственные выгоды и влияние (Levanova, 2017). Вследствие возникает необходимость в системах мониторинга и стимулирования, направленных на ограничение поведения агентов, не согласующегося с интересами собственников.

Элементы классической формулировки проблемы агентских конфликтов:

- Информационная асимметрия.
  Управленец обладает большей полнотой информации о деятельности компании, чем её собственники, затрудняя объективную оценку управленческих решений
- Моральный риск.

Возможность агента действовать в своих интересах, пользуясь ограниченностью механизмов контроля.
- Неблагоприятный отбор.
  Сложность оценки агента на этапе заключения контракта, что требует организационных издержек на мониторинг и мотивацию.

Расширение теоретического инструментария агентской теории связано с признанием неполноты контрактов (Grossman, Hart) и анализом многофакторных моделей мотивации (Holmström, Milgrom,) (Antras, 2011, Holmström, 1991). Данные подходы акцентировали внимание на ограничениях контрактного регулирования и необходимости комплексных систем стимулирования, обеспечивающих оптимальный баланс между вознаграждениями и санкциями. Современное применение агентской теории выходит за рамки корпоративного управления, охватывая государственное управление, финансы, образование и здравоохранение, что свидетельствует о ее универсальной аналитической ценности.

В российской экономической науке отдельное внимание уделяется институциональным аспектам агентских отношений в условиях трансформационной экономики (Bakhareva, 2024). Н. А. Южакова доказывает, что слабость правовых институтов и недостаточная прозрачность усиливают оппортунистические риски и увеличивают агентские издержки, включая затраты на мониторинг и регулирование деятельности менеджмента (Yuzhakova, 2025).

Классическая агентская теория, несмотря на фундаментальный вклад, встречает ограничения, связанные с допущением рационального поведения участников и акцентом на иерархические структуры. Однако современные экономические процессы характеризуются ростом значимости сетевых и децентрализованных форм организации, где традиционные модели требуют переосмысления с учётом цифровизации и технологий распределенных реестров, а также влияния когнитивных искажений и иррациональных факторов в принятии решений.

Границы между принципалом и агентом становятся размытыми, а участники сообщества могут одновременно выполнять функции собственников и управляющих. В этих условиях алгоритмическое управление снижает потребность в доверии, но открывает новые риски — от уязвимостей кода до концентрации влияния у крупных держателей токенов. Следовательно, классические подходы требуют доработки и адаптации к современной цифровой среде.

Агентские конфликты в условиях криптоэкономики и децентрализованных систем

В децентрализованных автономных организациях (DAO) функции собственника и менеджера часто пересекаются, поскольку участники одновременно выступают инвесторами, разработчиками и управляющими. Такая множественность ролей порождает новые формы конфликтов интересов, обусловленные различиями в оценке рисков, сроков и приоритетов распределения ресурсов. Традиционные агентские модели, основанные на централизованном управлении и наличии единого принципала, оказываются недостаточными для DAO, где отсутствует централизованный механизм контроля, а функции мотивации реализуются через алгоритмические правила, токеномику и репутационные механизмы. Агентские издержки в таких условиях смещаются из контрактной плоскости в протокольные и сетевые взаимодействия, что требует новых теоретических подходов, учитывающих особенности коллективного и программно-фиксированного управления. Важное значение приобретает децентрализация блокчейна, где права распределены между многочисленными держателями токенов управления. Однако концентрация токенов в узком кругу инвесторов может воспроизводить иерархию, противоречащую принципам децентрализации, и способствовать манипуляциям при коллективных решениях. Отсутствие эффективных механизмов консенсуса и разрешения споров чревато стагнацией деятельности DAO. Эти особенности отражены в современных исследованиях правового и организационного статуса DAO, демонстрируя необ-

ходимость адаптации управления к уникальным вызовам децентрализованных структур.

Статистика крупнейших DAO подтверждает устойчивое доминирование крупных держателей (whales) в структуре владения. Так, исследования показывают, что в 2025 году у ведущих DAO, таких как MakerDAO, Uniswap и Aave, около 78% governance-токенов сосредоточены у топ-20 участников, а в некоторых случаях топ-10 держателей контролируют от 40% до 58% голосов, что характерно для Uniswap и ENS DAO. Анализ 100 крупнейших DAO выявил, что коэффициент Джини распределения голосов обычно превышает 0,7, что соответствует значительной концентрации по стандартам политэкономии (Fritsch, 2024). В частности, в MakerDAO один прокси-депутат аккумулировал свыше 9% всей власти, а для изменения протокола Uniswap достаточно было собрать 4% голосов, что регулярно использовалось крупными инвесторами и фондами венчурного капитала (Bongaerts, 2025).

Для снижения риска «захвата власти» внедряются инновационные механизмы: quadratic voting (квадратичное голосование), делегирование голоса (proxy/delegated voting), системы репутации и NFT-бейджи «добросовестных участников». Квадратичное голосование стало стандартом в более чем 100 DAO: стоимость дополнительного голоса для whale растет экспоненциально, что снижает отдачу от концентрации токенов и позволяет миноритариям оказывать реальное влияние (например, Gitcoin, CryptoUnicorns). Делегированное голосование и veto right (например, Lido, ENS DAO, Curve) усиливают коллективный контроль и позволяют сообществу блокировать отдельные инициативы крупных игроков. На практике, однако, большинство DAO продолжают использовать чисто пропорциональную модель, где каждый токен дает один голос, что и порождает оборотную проблему власти whale-депозиторов [24].

Крупные манипуляции или атаки (governance attacks) со стороны whale-держателей неоднократно фиксировались и приводили к значительным убыткам для мелких инвесторов. По данным научного анализа рынка DAO за 2020–2024 годы, прямые финансовые потери инвесторов от подобных атак превысили $613 млн, а общее падение капитализации протоколов вследствие governance exploit может доходить до $1,3 млрд (атаки на Compound, BadgerDAO, Curve, Sushiswap). В ряде случаев (Curve, август 2023) три крупнейших адреса проголосовали за изменение протокола, приведшее к падению цены токена на 18% и многомиллионным потерям розничных держателей. Прецеденты голосования немотивированной массы (governance apathy) в Uniswap и Lido также вызывали sell-off порядка $30–50 млн на фоне конфликтных решений, вынесенных при кворуме всего 3–7% участников (Sharma, 2025).

Несмотря на декларируемую прозрачность блокчейн-инфраструктуры, она создаёт новые типы рисков для участников финансовой экосистемы (Piskareva, 2024). Данные о транзакциях открыты и доступны, что формально должно снижать информационную асимметрию, однако одновременно увеличивает уязвимость пользователей, в результате чего информационная асимметрия не исчезает, а трансформируется, принимая новые формы.

Финансовые последствия этих рисков особенно заметны в секторе децентрализованных финансов. Только за первую половину 2025 года потери от фишинговых схем превысили 410 миллионов долларов США, а отдельные инциденты, такие как атака на Venus Protocol, привели к потере 13,5 миллиона долларов с одного кошелька пользователя [25]. Современные фишинговые атаки всё чаще используют сгенерированный искусственным интеллектом контент для имитации легитимных платформ, достигая показателя переходов по ссылкам на уровне 54%, что значительно выше результатов традиционных методов фишинга. В случае с Venus пользователь одобрил вредоносную транзакцию через поддельный интерфейс, что спровоцировало падение нативного токена протокола на 6% и сокращение совокупного объёма заблокированных средств в сети BNB Chain на 9,2%.

Такие каскадные эффекты показывают, что киберугрозы, в частности фишинг, перестают быть изолированным явлением и становятся системным фактором риска для устойчивости и доверия к экосистеме DeFi [7]. Особое значение в криптоэкономике приобретает токеномика — архитектура распределения токенов и система стимулов для участников проекта (Jermann, 2025). Непродуманная структура вознаграждений способна обострить агентские конфликты: если разработчики оставляют за собой чрезмерную долю токенов, они получают возможность влиять на курс и управленческие процессы в ущерб остальным участникам. В то же время недостаток долгосрочных стимулов может привести к «бросовым» проектам, когда команда быстро извлекает выгоду и покидает экосистему, оставляя инвесторов с обесцененными активами.

Распределение токенов между разработчиками, инвесторами и сообществом — ключевой параметр сбалансированности стимулов в криптопроектах. Эмпирические исследования показывают, что значительная концентрация (более 25–35%) в руках core team приводит к риску манипуляций и снижению вовлеченности пользователей, тогда как проекты с равномерным распределением и значительными пулами для публичного стейкинга, грантов и governance демонстрируют более устойчивую экосистему. Анализ структуры распределения в DAOs указывает: если на ранних этапах доля развития и фонда команды превышает 40–50%, это сопряжено с последствиями misalignment — слабеет долгосрочный интерес участников и занижается качество обратной связи в управлении (Messias, 2025).

Согласно данным Elliptic и других криптобезопасных платформ, частота мошенничества в сети (exit scam) и rug pull составляет в среднем 1–3% от общего числа запущенных проектов в год, но среди DeFi-проектов эти показатели иногда доходят до 7–10%. В отчете Elliptic за 2024–2025 годы общий объем потерь пользователей в результате мошенничества и скам-проектов только в США составил $9,3 млрд — по миру до $2–3 млрд ежегодно, причем средний прямой ущерб для инвестора в отдельно взятом случае варьируется от $40 тыс. до $1,7 млн в зависимости от размера пула и вовлеченных средств [11]. При этом нарастает доля сложных смешанных схем: кража частных ключей, фиктивные ICO и кроссчейн-проекты с premine.

Для снижения агентских рисков и стимулирования долгосрочного участия наилучшие результаты демонстрируют многоступенчатые схемы вестинга, где разблокировка токенов для команды и инвесторов происходит в течение 1–5 лет и привязана к проектным либо управленческим метрикам. Наиболее успешные стимулы сочетают линейный вестинг с milestone-based unlock, публичным аудитом казначейских кошельков и опциями для заново распределяемых токенов. Эффективные модели предполагают внедрение прозрачности (on-chain мониторинг, внешние аудиторы), автоматизацию через смарт-контракты и участие сообщества в калибровке кривой стимулирования, что заметно в кейсах Uniswap, Aave, MakerDAO [11].

Согласно данным SolidityScan's Web3HackHub за 2024 год, общий ущерб от атак составил 1,42 миллиарда долларов США в 149 задокументированных случаях. Ключевые типы атак включают: уязвимости контроля доступа ($953,2 млн), логические ошибки ($63,8 млн), атаки повторного входа ($35,7 млн), использование flash-кредитов ($33,8 млн), недостаточную проверку входных данных ($14,6 млн), манипуляции с ценовыми оракулами ($8,8 млн) и непроверенные внешние вызовы ($550,7 тыс.) [22].

В 2025 году OWASP представила Smart Contract Top 10 — список ключевых уязвимостей, включающий контроль доступа, манипуляции с ценовыми оракулами, логические ошибки, недостаточную валидацию входных данных, атаки повторного входа, непроверенные внешние вызовы, флешкредитные атаки, переполнение целых чисел, ненадежную генерацию случайных чисел и DoS-атаки. Несмотря на прозрачность блокчейна, смарт-контракты остаются источником системных рисков, где безопасность зависит не только

от качества кода, но и от квалификации участников. Для минимизации угроз рекомендуются регулярные аудиты, автоматический анализ кода, обучение разработчиков и надежные механизмы контроля доступа и аутентификации [20].

Современные эмпирические исследования указывают на значительное количество и частоту конфликтов в крупных DAO, что в ряде случаев приводит к потере устойчивости или даже к форкингу и распаду проектов. По метаисследованию Han et al. (2025), только за 2021–2024 гг. в крупнейших 100 DAO было зафиксировано более 370 существенных конфликтных ситуаций, из которых 41 завершились fork (разделением цепочки или сменой команды управления), а 62 сопровождались governance attack с резким снижением TVL или капитализации. Анализ разовых и периодических кризисов (например, Luna crash, FTX collapse) выявил, что DAOs с высокой долей конфликтов интересов и централизованного голосования теряли в среднем на 18,9% TVL больше, чем средний рынок, а в периоды внешних шоков (2022–2023) потери достигали 44,6% TVL. Устойчивость платформ повышалась при высоком вовлечении мелких держателей и наличии эффективных процедур разрешения споров, тогда как рекуррентные внутренние конфликты почти всегда приводили к снижению рыночной капитализации и оттоку участников.

Пути снижения агентских конфликтов в криптоэкономике тесно связаны с развитием корпоративного и технического регулирования, среди которых ключевое значение приобретают независимые аудиты смарт-контрактов с публичным раскрытием их результатов для инвесторов. Устойчивость децентрализованных организаций обеспечивается за счет внедрения прозрачных процедур голосования, многоуровневых систем согласования и эффективных механизмов разрешения споров, гарантирующих равноправное участие всех сторон. Одновременно требуется выработка сбалансированной регуляторной политики, которая эффективно защищала бы инвесторов и ограничивала возможности злоупотреблений, не препятствуя развитию инноваций и отрасли в целом. Особое внимание уделяется внедрению искусственного интеллекта для мониторинга блокчейн-транзакций и обнаружения аномалий, что существенно повышает качество контроля и снижает риски манипуляций.

Итак, с одной стороны, децентрализация и прозрачность обладают потенциалом для снижения традиционных агентских издержек, связанных с мониторингом и обеспечением исполнения обязательств. С другой стороны, они создают новые формы асимметрии и новые возможности для злоупотреблений. В отличие от классических моделей, где противостояние ограничивалось дуализмом «принципал — агент», в децентрализованных системах возникает более сложная сеть конфликтов между множеством участников.

Перспективы использования искусственного интеллекта и блокчейн 2.0 в управлении цифровыми активами

Массовые случаи мошенничества с ICO, внутренние конфликты в DAO, уязвимости смарт-контрактов и рыночные манипуляции подтверждают необходимость поиска новых инструментов управления и контроля.

Алгоритмы машинного обучения могут автоматически выявлять уязвимости в смарт-контрактах, моделировать сценарии атак и прогнозировать их последствия. В условиях, когда в первой половине 2025 года совокупные потери Web3-проектов от атак и уязвимостей превысили 3,1 миллиарда долларов США, развитие подобных систем становится критически важным. При этом лишь проблемы с контролем доступа в смарт-контрактах привели к убыткам в размере более 950 миллионов долларов, что подтверждает масштаб угроз [23].

Помимо аудита, искусственный интеллект используется в мониторинге транзакций. Технологии анализа больших данных позволяют в режиме реального времени отслеживать подозрительные операции, выявлять схемы отмывания средств или манипулирования рынком. Данные инструменты способны существенно снизить

моральный риск и информационную асимметрию, которые в классической агентской теории рассматриваются как ключевые источники конфликтов. Не менее перспективным направлением является внедрение технологий блокчейн 2.0, которые выходят за рамки простого хранения транзакций и позволяют создавать децентрализованные платформы для управления цифровыми активами. Если блокчейн первого поколения обеспечивал лишь прозрачность и неизменность данных, то блокчейн 2.0 дополняет эти характеристики функционалом смарт-контрактов, интеграцией с системами искусственного интеллекта и возможностью построения более гибких моделей управления.

Однако статистические данные показывают, что даже децентрализованные механизмы сталкиваются с проблемой концентрации власти. В 2025 году насчитывалось более 13 тысяч DAO, контролирующих активы на сумму порядка 21,4 миллиарда долларов США. Тем не менее анализ распределения токенов управления демонстрирует, что менее 1% участников контролируют около 90% голосов. Такая диспропорция создаёт предпосылки для серьёзных агентских конфликтов, поскольку решения принимаются ограниченным числом крупных держателей, что подрывает интересы широкого круга инвесторов.

Для иллюстрации данной проблемы был проведён эксперимент на основе синтетических данных, моделирующих распределение токенов между участниками DAO. В качестве показателя концентрации власти применялся индекс Джини, а для визуализации использовались кривые Лоренца. На рисунке 1 представлены три сценария: исходное распределение токенов, усиление позиций топ-5 держателей и равномерное распределение за счёт выпуска новых токенов.

Анализ результатов моделирования показал, что в исходном сценарии индекс Джини составляет 0,64, это указывает на высокий уровень неравенства. Усиление крупных держателей (топ-5) приводит к росту индекса до 0,71, подтверждая тенденцию к централизации власти. Напротив, равномерное распределение новых токенов снижает индекс до 0,39, что отражает более справедливое участие сообщества в управлении. Результаты эксперимента подтверждают, что без применения дополнительных инструментов концентрация власти в DAO имеет тенденцию усиливаться, тогда как механизмы перераспределения и автоматизированный мониторинг способны снизить риски централизации.

Таким образом, использование алгоритмов анализа распределения токенов и прогнозирования концентрации власти позволяет выявлять потенциальные угрозы ещё до того, как они приведут к кризисным ситуациям, что подтверждает роль искусственного интеллекта не только как инструмента мониторинга, но и полноценного элемента корпоративного управления в условиях блокчейн 2.0 (Rane, 2025).

Далее предлагается модель управления, объединяющая ключевые компоненты и процессы ИИ и блокчейн 2.0.

Предложенная модель опирается на ядро блокчейн 2.0, обеспечивающее хранение и исполнение договоров с повышенным уровнем безопасности и управлением правами. Искусственный интеллект, интегрированный в эту систему, добавляет возможности интеллектуального анализа и предсказаний, что позволяет осуществлять адаптивное управление и своевременно выявлять риски. Смарт-контракты второй версии обеспечивают гибкое управление правами и автоматическое исполнение операций с цифровыми активами, включая использование внешних данных через оракулов. При этом постоянный мониторинг и аудит с помощью ИИ гарантируют безопасность, прозрачность и соблюдение нормативных требований. Важным элементом модели является взаимодействие с другими платформами и сетями, что расширяет функциональность и повышает ликвидность цифровых активов. Такая концептуализация может быть представлена как схема с потоками данных и управленческих процессов либо как таблица, раскрывающая архитектуру управления цифровыми активами с применением ИИ

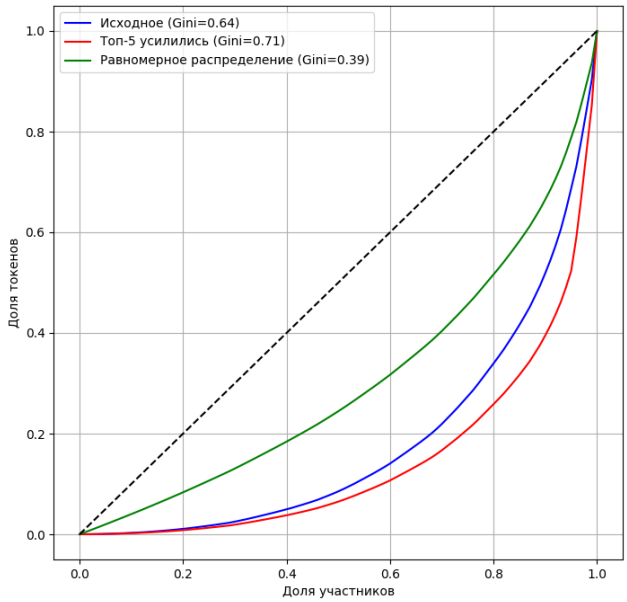

Рис. 1. Кривые Лоренца для распределения токенов в DAO в Python-модели. Источник: составлено авторами.

и блокчейн 2.0, отражая современные технологические тренды и достижения. Вместе с тем, несмотря на преимущества этих технологий, они не являются универсальным решением: случаи атак даже после аудитов смарт-контрактов подтверждают необходимость непрерывного совершенствования алгоритмов защиты и формирования комплексной регуляторной среды. Избыточное регулирование способно сдерживать инновации, тогда как отсутствие контроля создаёт риски злоупотреблений, поэтому оптимальной представляется разработка сбалансированных моделей регулирования, основанных на прозрачности, стандартизации процедур и усилении ответственности участников цифровых экосистем.

Таблица 1. Концептуальная модель управления цифровыми активами с ИИ и блокчейн 2.0.

Компонент модели	Описание и функции	Технологическая основа	Роль в управлении цифровыми активами
Хранилище цифровых активов	Децентрализованное распределённое хранилище, обеспечивающее неизменность и прозрачность данных	Блокчейн 2.0 (с улучшенной безопасностью)	Обеспечивает надёжное хранение и учёт права собственности
Управление доступом	Гибкое управление правами доступа к активам и операциям через смарт-контракты 2.0	Смарт-контракты 2.0 с правами доступа	Контроль и разграничение полномочий участников системы
Автоматизация операций	Автоматизированное исполнение транзакций и операций через смарт-контракты с учётом правил и условий	Смарт-контракты 2.0, оракулы для внешних данных	Повышает эффективность и снижает операционные риски [10].

Продолжение на следующей странице

Таблица 1. Концептуальная модель управления цифровыми активами с ИИ и блокчейн 2.0. (Продолжение таблицы)

Компонент модели	Описание и функции	Технологическая основа	Роль в управлении цифровыми активами
Прогностический анализ	Аналитика и моделирование состояния активов, прогнозирование трендов и рисков с помощью машинного обучения	Искусственный интеллект, алгоритмы ML	Поддержка принятия управленческих решений, выявление аномалий
Мониторинг и аудит	Непрерывный мониторинг, обнаружение аномалий, автоматический аудит операций	ИИ и блокчейн с неизменяемой историей	Обеспечение прозрачности, безопасности и соблюдения правил
Взаимодействие с экосистемой	Обеспечение совместимости и интеграции с другими блокчейн-сетями и цифровыми платформами	Межсетевые протоколы, API, оракулы	Расширяет возможности использования и ликвидность активов
Безопасность данных	Использование криптографических методов, защиты данных и предотвращения взломов	Криптография, алгоритмы консенсуса PoS/PoA	Повышение защищённости и доверия к системе

Источник: предложено авторами.

Таким образом, использование искусственного интеллекта и блокчейн 2.0 открывает качественно новые возможности для управления цифровыми активами и минимизации агентских конфликтов. Перспективным направлением является сочетание технологических инструментов с эффективным управлением сообществом и продуманной регуляторной политикой. Внедрение таких подходов позволит не только снизить агентские издержки, но и обеспечить устойчивое развитие криптоэкономики в долгосрочной перспективе.

Библиографический список

1. *Асрян А. С.* Смарт-контракт: перспективы применения в банковском секторе // Journal of Monetary Economics and Management. — 2025. — № 1. — URL: https://cyberleninka.ru/article/n/smart-kontrakt-perspektivy-primeneniya-v-bankovskom-sektore.
2. *Бахарева Я. Д.* Влияние цифровизации на процессы стратегического управления в современных организациях // Вестник науки. — 2024. — 12 (81). — URL: https://cyberleninka.ru/article/n/vliyanie-tsifrovizatsii-na-protsessy-strategicheskogo-upravleniya-v-sovremennyh-organizatsiyah.
3. *Дульзон А. А.* Разработка управленческих решений : учебник. — Томск : Издательство Томского политехнического университета, 2009. — 295 с. — ISBN 5-98298-330-6.
4. *Леванова Л. Н.* Развитие системы корпоративного управления в России : монография. — Саратов : Амирит, 2017. — 312 с. — ISBN 978-5-6040143-2-5.
5. *Манахова И. В.*, *Колмыков К. А.* Цифровые финансовые активы на современном финансовом рынке: систематизация опыта и трендов в России // Известия Саратовского университета. Новая серия. Серия Экономика. Управление. — 2025. — № 2. — URL: https://cyberleninka.ru/article/n/tsifrovye-finansovye-aktivy-na-sovremennom-finansovom-rynke-sistematizatsiya-opyta-i-trendov-v-rossii.
6. *Пискарева А. Ю.*, *Криничанский К. В.* Блокчейн-технологии в процессах расчетов и клиринга на фондовом рынке // Финансовые рынки и банки. — 2024. — № 12. — С. 279—286. — EDN MLUWLE.
7. Риски фишинга в DeFi: что инвесторы должны делать для защиты своих активов / Bitget. — URL: https://www.bitget.com/ru/news/detail/12560604949099 (дата обр. 25.10.2025).
8. *Южакова Н. А.* Формы внутреннего оппортунизма и его влияние на деятельность компании // Финансы и управление. — 2025. — № 2. — URL: https://cyberleninka.ru/article/n/formy-vnutrennego-opportunizma-i-ego-vliyanie-na-deyatelnost-kompanii.

9. *Antras P.*, *Grossman G.*, *Hart O.* Goes Global: Incomplete Contracts, Property Rights, and the International Organization of Production. NBER Working Paper No. w17470. — 2011. — URL: https://ssrn.com/abstract=1935796.
10. Automated Execution of Financial Contracts on Blockchains / B. Egelund-Müller [et al.] // Business & Information Systems Engineering. — 2017. — 59 (6). — P. 457–467. — DOI: 10.1007/s12599-017-0507-z.
11. Best practices to prevent AI-enabled crime in the cryptoasset ecosystem. Elliptic report 2025. — URL: https://www.elliptic.co/hubfs/AI\%20REPORT\%202025/AI\%20best\%20practices\%20report\%20final\%20(1).pdf (visited on 09/15/2025).
12. *Fritsch R.*, *Müller M.*, *Wattenhofer R.* Analyzing voting power in decentralized governance: Who controls DAOs? // Blockchain: Research and Applications. — 2024. — Sept. — Vol. 5, no. 3. — P. 100208. — ISSN 2096-7209. — DOI: 10.1016/j.bcra.2024.100208.
13. Future of Algorithmic Organization: Large Scale Analysis of Decentralized Autonomous Organizations (DAOs) arXiv:2410.13095v1 / T. Sharma [et al.]. — 2025.
14. *Han J.*, *Lee J.*, *Li T.* A review of DAO governance: Recent literature and emerging trends // Journal of Corporate Finance. — 2025. — Apr. — Vol. 91. — P. 102734. — ISSN 0929-1199. — DOI: 10.1016/j.jcorpfin.2025.102734.
15. *Han J.*, *Lee J.*, *Li T.* A review of DAO governance: Recent literature and emerging trends // Journal of Corporate Finance. — 2025. — Apr. — Vol. 91. — P. 102734. — ISSN 0929-1199. — DOI: 10.1016/j.jcorpfin.2025.102734.
16. *Holmström B.*, *Milgrom P.* Multitask Principal-Agent Analyses: Incentive Contracts, Asset Ownership, and Job Design // Journal of Law, Economics, and Organization. — 1991. — No. 7. — P. 24–52.
17. *Jermann U.*, *Xiang H.* Tokenomics: Optimal monetary and fee policies // Journal of Monetary Economics. — 2025. — Oct. — Vol. 155. — P. 103808. — ISSN 0304-3932. — DOI: 10.1016/j.jmoneco.2025.103808.
18. *Jermann U.*, *Xiang H.* Tokenomics: Optimal monetary and fee policies // Journal of Monetary Economics. — 2025. — Oct. — Vol. 155. — P. 103808. — ISSN 0304-3932. — DOI: 10.1016/j.jmoneco.2025.103808.
19. *Messias J.*, *Ide A.* Fairness in Token Delegation: Mitigating Voting Power Concentration in DAOs. arXiv preprint / Max Planck Institute for Software Systems. — 2025. — URL: https://arxiv.org/html/2510.05830v1.
20. OWASP Smart Contract Top 10. — URL: https://owasp.org/www-project-smart-contract-top-10 (visited on 10/26/2025).
21. *Rane N.*, *Choudhary S.*, *Rane J.* Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance // SSRN Electronic Journal. — 2023. — ISSN 1556-5068. — DOI: 10.2139/ssrn.4644253.
22. SolidityScan's HackHub: Learn about Hacks & Prevent Attacks. — URL: https://solidityscan.com/web3hackhub (visited on 10/20/2025).
23. SolidityScan's HackHub: Learn about Hacks & Prevent Attacks. — URL: https://solidityscan.com/web3hackhub (visited on 10/24/2025).
24. *Sterling R.* Quadratic Voting in DAO Governance: How NFT Badges Enable Fairer Decision-Making. —. — URL: https://governancenft.com/2025/10/26/quadratic-voting-in-dao-governance-how-nft-badges-enable-fairer-decision-making.
25. Venus Protocol User Loses $13.5 Million in BNB Chain Phishing Attack / Coinspot.io. — 2025. — URL: https://coinspot.io/cryptocurrencies/altcoins/venus-protocol-phishing-attack.
26. Vote Delegation in DeFi Governance. SSRN Working Paper / D. Bongaerts [et al.]. — 2025. — URL: https://ssrn.com/abstract=5177022.