Научная статья
УДК 336.7
DOI: 10.25683/VOLBI.2025.71.1331

Ekaterina Ivanovna Dyudikova
Doctor of Economics,
Associate Professor of the Department of Banking and Monetary Regulation of Faculty of Finance,
Financial University
under the Government of the Russian Federation
Moscow, Russian Federation
ekidyudikova@fa.ru

Екатерина Ивановна Дюдикова
д-р экон. наук,
доцент Кафедры банковского дела и монетарного регулирования Финансового факультета,
Финансовый университет
при Правительстве Российской Федерации
Москва, Россия
ekidyudikova@fa.ru

КОНТРОЛЬ НАД АКТИВАМИ В ЭПОХУ WEB3: ОТ БАНКОВСКИХ СЧЕТОВ К КРИПТОВАЛЮТНЫМ КОШЕЛЬКАМ

5.2.4 — Финансы

Аннотация. *Настоящее исследование посвящено эволюции механизмов контроля над активами в условиях становления парадигмы Web3. Современные криптоактивы (включая монеты и токены), основанные на технологии распределенных реестров (DLT), формируют принципиально новый класс цифровых активов, бросающий вызов традиционной банковской системе. В отличие от классических банковских счетов, где контроль над средствами делегирован финансовым организациям, Web3-кошельки обеспечивают пользователям полный суверенитет над активами посредством криптографических механизмов. В центре внимания находится сравнительный анализ двух принципиально различных моделей управления активами: традиционной банковской системы и инновационных Web3-кошельков. Автор исследует ключевые различия между этими инструментами, уделяя особое внимание вопросам обеспечения безопасности, децентрализации и степени участия пользователя в финансовых операциях. В работе подробно рассматриваются структурные элементы, функциональные возможности и механизм Web3-кошельков, включая их роль в экосистеме децентрализованных финансов (DeFi), а также проводится их типологизация по критериям управления ключами, режима доступа к сети и функциональной насыщенности. Особый акцент сделан на компромиссах между автономией и ответственностью, возникающих при переходе от централизованных финансовых моделей к децентрализованным. На основе проведенного анализа делается вывод о том, что Web3-кошельки представляют собой новую парадигму владения и передачи стоимости, основанную на принципах самоуправления и криптографической безопасности. Статья подчеркивает необходимость пересмотра традиционных экономических моделей в условиях цифровой трансформации и предлагает четкие терминологические градации для современных финансовых инструментов.*

Ключевые слова: *банковский счет, децентрализация, открытый ключ, приватный ключ, технология распределенных реестров, типология, управление криптоактивами, цифровая валюта, seed-фраза, Web3-кошелек*

Для цитирования: Дюдикова Е. И. Контроль над активами в эпоху Web3: от банковских счетов к криптовалютным кошелькам // Бизнес. Образование. Право. 2025. № 2(71). С. 178—186. DOI: 10.25683/VOLBI.2025.71.1331.

Original article

ASSET CONTROL IN THE WEB3 ERA: TRANSITIONING FROM BANK ACCOUNTS TO CRYPTOCURRENCY WALLETS

5.2.4 — Finance

Abstract. *This study explores the evolution of asset control mechanisms within the emerging Web3 paradigm. Modern crypto assets (including coins and tokens), built on distributed ledger technology (DLT), constitute a fundamentally new class of digital assets that challenge the traditional banking system. Unlike conventional bank accounts, where control over funds is delegated to financial institutions, Web3 wallets grant users full asset sovereignty through cryptographic mechanisms. The focus lies on a comparative analysis of two fundamentally distinct asset management models: the traditional banking system and innovative Web3 wallets. The author examines key differences between these tools, with particular attention to security, decentralization, and user involvement in financial operations. The paper delves into the structural components, functionalities, and mechanisms of Web3 wallets, including their role in the decentralized finance (DeFi) ecosystem, and classifies them based on key management criteria, network access modes, and functional breadth. Special emphasis is placed on the trade-offs between autonomy and responsibility inherent in the shift from centralized to decentralized financial models. The analysis concludes that Web3 wallets represent a new paradigm of value ownership and transfer, grounded in self-governance and cryptographic security. The article highlights the need to rethink traditional economic models amid digital transformation and proposes clear terminological distinctions for modern financial instruments.*

Keywords: *bank account, decentralization, public key, private key, distributed ledger technology, typology, crypto asset management, digital currency, seed phrase, Web3 wallet*

For citation: Dyudikova E. I. Asset control in the Web3 era: transitioning from bank accounts to cryptocurrency wallets. *Biznes. Obrazovanie. Pravo = Business. Education. Law*. 2025;2(71):178—186. DOI: 10.25683/VOLBI.2025.71.1331.

Введение

С появлением технологии распределенных реестров (*Distributed Ledger Technology*, *DLT*) наблюдается фундаментальная трансформация финансовой экосистемы, приводящая к переосмыслению роли традиционных банковских институтов. В данном контексте *Web*3-кошельки, функционирующие на основе криптографических алгоритмов, приобретают особую значимость, выступая в качестве инструмента децентрализованного управления активами и предоставляя пользователям беспрецедентный уровень автономии.

Современные криптоактивы, включающие в себя как монеты, так и токенизированные активы, формируют принципиально новый класс цифровых ценностей, существующих исключительно в рамках *DLT*-инфраструктуры. Вопреки распространенному заблуждению, криптоактивы не хранятся непосредственно в кошельках, а представляют собой зашифрованные записи в распределенном реестре — децентрализованной базе данных, консенсус в которой достигается за счет взаимодействия множества независимых узлов сети.

*Web*3-кошельки представляют собой инновационный инструмент, который способствует более четкому концептуальному разграничению между цифровыми валютами и традиционными безналичными денежными средствами. Их ключевая особенность заключается в возможности четкого разграничения цифровых валют и традиционных безналичных денежных средств, что приобретает особую **актуальность** в условиях современной цифровой трансформации. Однако, несмотря на значимость данного критерия, в научной литературе отсутствуют комплексные исследования, посвященные анализу *Web*3-кошельков как инструмента демаркации между этими формами активов.

Изученность проблемы. В академической литературе широко исследуется проблематика *Web*3-кошельков и их значимость в контексте развития криптоиндустрии. Так, вопросы безопасности, включая классификацию атак и систематизацию сопутствующих рисков, рассматриваются в работах Y. Erinle, Y. Kethepalli, Y. Feng, J. Xu [1], S. Houy, Ph. Schmid, A. Bartel [2], H. Guo и X. Yu [3]. Аспекты деанонимизации пользователей и анализ механизмов повышения приватности кошельков детально изучены в исследованиях H. Kim и S. Park [4], G. Fanti и P. Viswanath [5], R. Balu, T. Furon и S. Gambs [6]. Проблемы эрогономичности и правового регулирования работы с ними освещаются в трудах O. Alqaryouti, N. Siyam, Z. Alkashri, K. Shaalan [7] и M. Finck [8]. Кроме того, P. Tasca, C. J. Tessone [9], S. M. Werner с соавторами [10] уделяют внимание функциональной роли кошельков в качестве ключевых элементов доступа к *DeFi* и системам децентрализованной идентификации.

Научная новизна заключается в систематизации подходов к анализу *Web*3-кошельков как инструмента демаркации между цифровыми валютами и традиционными безналичными средствами. Автор предлагает комплексный сравнительный анализ банковских счетов и *Web*3-кошельков, выделяя ключевые различия в контроле над активами, уровне децентрализации, безопасности и участии пользователя. Также представлена типология кошельков на основе критериев управления ключами, режима доступа к сети и функциональных возможностей, что способствует структурированию знаний в этой области.

Цель работы — исследовать эволюцию механизмов контроля над активами в условиях перехода от традиционных банковских систем к децентрализованным финансам, а также провести сравнительный анализ этих моделей для выявления их принципиальных различий и преимуществ.

Задачи исследования включают: проведение сравнительного анализа банковских счетов и *Web*3-кошельков по ключевым параметрам; представление типологии *Web*3-кошельков на основе моделей управления ключами, режимов доступа к сети и функциональных возможностей; анализ кейсов использования *Web*3-кошельков для верификации теоретических выводов; определение роли кошельков в экосистеме *DeFi* и их влияние на трансформацию традиционных экономических моделей.

Теоретическая значимость исследования заключается в развитии теории криптоэкономики за счет предложения четкой терминологической градации и концептуальных основ для понимания *Web*3-кошельков. Работа систематизирует знания о новых парадигмах владения и передачи стоимости, основанных на принципах самоуправления и криптографической безопасности. Результаты могут служить основой для дальнейших научных изысканий в области *DLT* и цифровых валют. **Практическая значимость** исследования заключается в предоставлении инструментов для выбора оптимальных решений в управлении криптоактивами. Результаты исследования могут быть полезны пользователям криптовалют для понимания преимуществ и рисков различных типов кошельков; финансовым институтам для адаптации к новым технологическим вызовам и разработки гибридных решений; регуляторам для формирования нормативной базы, учитывающей особенности *DeFi*. Статья также подчеркивает необходимость пересмотра традиционных экономических моделей в условиях цифровизации, что актуально для бизнеса и государственных структур.

Основная часть

Методология. В рамках настоящего исследования был применен комплекс методов, направленных на всестороннее изучение эволюции механизмов контроля над активами в условиях перехода от традиционных банковских систем к *DeFi*. Методологическая база исследования включает следующие подходы:

• ***Сравнительный анализ***: проведено детальное сопоставление традиционных банковских счетов и *Web*3-кошельков по ключевым параметрам. Данный метод позволил выявить принципиальные различия между анализируемыми моделями.

• ***Типологический анализ***: представлена классификация *Web*3-кошельков на основе таких характеристик, как модель управления приватными ключами, режим сетевого доступа, функциональные возможности и тип используемого устройства, что способствовало структурированию существующего многообразия решений.

• ***Криптографический анализ***: исследованы базовые принципы функционирования *Web*3-кошельков, включая алгоритмы генерации и хранение ключей, процессы подписания транзакций, а также методы обеспечения безопасности.

• ***Анализ практических кейсов***: рассмотрены примеры распространенных *Web*3-кошельков с целью демонстрации их функциональных особенностей и верификации теоретических выводов.

• ***Обзор научной литературы и нормативных документов***: исследованы современные публикации, посвященные криптоактивам и децентрализованным технологиям, а также нормативные акты, регулирующие их использование. Это позволило выявить актуальные тенденции и нерешенные вопросы в данной области.

Результаты исследования основаны на синтезе теоретических и эмпирических данных, что обеспечило комплексный анализ рассматриваемой проблемы. Применение указанных методов способствовало не только систематизации существующих знаний, но и разработке новых концептуальных подходов к пониманию роли *Web*3-кошельков в современной финансовой экосистеме.

Результаты. ***Web3-кошелек vs банковский счет.*** Криптовалютный кошелек или *Web*3-кошелек служит основным инструментом взаимодействия пользователя с распределенным реестром, обеспечивая управление криптоактивами посредством криптографических ключей [11]. В отличие от банковского счета, где контроль над средствами осуществляет финансовое учреждение, *Web*3-кошелек предоставляет пользователю полный суверенитет над активами. При этом закрытый ключ, необходимый для доступа к криптоактивам, не хранится в явном виде в кошельке, а либо временно загружается в процессе работы, либо активируется с использованием *seed*-фразы.

Функционально *Web*3-кошелек можно рассматривать как цифровой аналог физического кошелька, представляющий собой клиентскую часть приложения и выполняющий следующие ключевые задачи: отображение текущего баланса; предоставление интерфейса для формирования и подписания транзакций; взаимодействие с *DLT*-сетью для передачи транзакций на обработку; ведение истории операций; настройка комиссий и приоритетов исполнения транзакций.

*Web*3-кошелек и банковский счет представляют собой разные модели учета и распоряжения активами, основанные на противоположных подходах к доверию, контролю и участию пользователя в финансовых операциях. Банковские счета функционируют в рамках изолированных электронных систем, где движение средств отражается в виде бухгалтерских проводок, вносимых кредитными организациями на основании принятых распоряжений к исполнению от владельцев счетов [12]. Ключевыми особенностями выступают следующие аспекты:

– *косвенное участие пользователя*: владелец счета не имеет прямого доступа к системе учета, а взаимодействует с ней исключительно через интерфейс, предоставляемый банком;

– *посредническая роль банка*: все транзакции требуют согласования с финансовым учреждением, которое выступает доверенным оператором и контролирует исполнение распоряжений клиента;

– *централизованный контроль*: банк обладает полномочиями замораживать средства, отменять операции или ограничивать доступ к счету в соответствии с регуляторными требованиями.

В отличие от банковского счета, *Web*3-кошелек обеспечивает прямой доступ к активам через механизмы *DLT*, имея следующие основные характеристики:

– *прямое участие пользователя*: записи о транзакциях создаются и подтверждаются самим владельцем кошелька (или лицами, которым напрямую предоставлены права доступа) и фиксируются в распределенном реестре без посредников;

– *криптографическая аутентификация*: каждая операция требует цифровой подписи с использованием закрытого ключа, что исключает необходимость доверенных третьих сторон;

– *полный суверенитет над активами*: пользователь самостоятельно управляет средствами, а отсутствие централизованного контроля делает невозможным необоснованное обезличенное внешнее вмешательство в транзакции (заморозку, отмену или цензуру).

Наиболее значимое различие между двумя моделями заключается в распределении контроля над активами. В банковской системе активы клиента фактически принадлежат не клиенту, а банку, который фиксирует обязательства перед владельцем, но сохраняет полномочия по управлению и ограничению доступа к средствам (рис. 1). В отличие от этого, *Web*3-кошелек обеспечивает прямое и исключительное владение активами через криптографические ключи, а их движение регулируется алгоритмами децентрализованных сетей на основе *DLT*. Данное различие демонстрирует, что *Web*3-кошелек не является функциональным аналогом банковского счета, а представляет собой новую парадигму владения и передачи стоимости, основанную на децентрализации и самоуправлении (табл. 1).

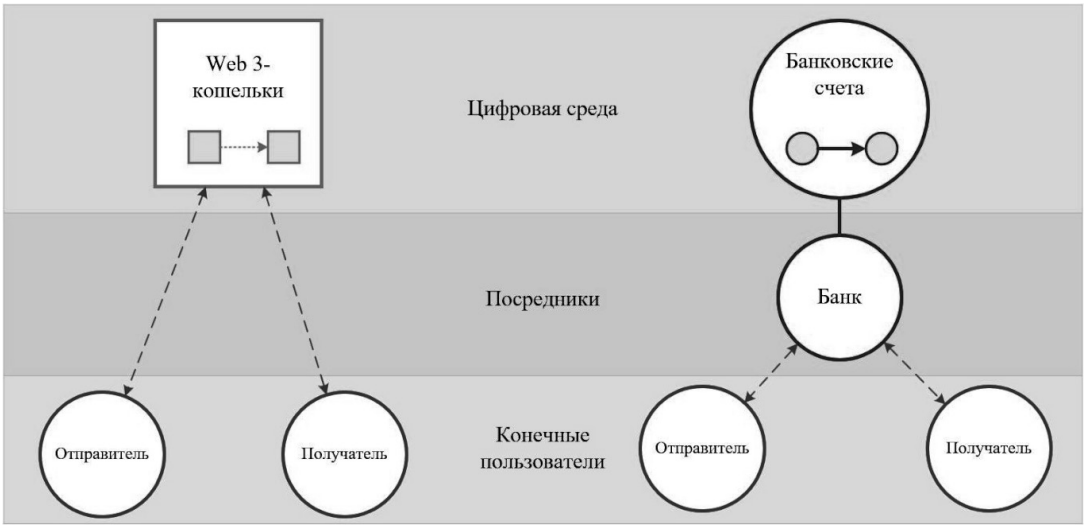

Рис 1. Фундаментальный сдвиг в управлении криптоактивами в парадигме *Web*3 (составлено автором)

Таблица 1

Сравнительная характеристика банковских счетов и *Web*3-кошельков

Критерий	Банковский счет	Web3-кошелек
Контроль над активами	Опосредованный (банк управляет средствами, может заморозить счет)	Прямой (полный контроль через приватные ключи, нет цензуры)
Централизация	Централизованный (банк выступает посредником)	Децентрализованный (нет единого управляющего органа, сеть узлов)
Доступ к средствам	Через банковские системы (отделения, дистанционное банковское обслуживание, карты)	Через приватные ключи / seed-фразу (чаще всего нет восстановления при потере)
Реестр операций	Внутренние базы данных банка (закрытые, изменяемые)	DLT (публичный/приватный распределенный реестр, неизменяемый, прозрачный)
Анонимность	Регулируемая (KYC/AML, идентификация личности)	Псевдоанонимность
Комиссии за транзакции	Устанавливаются тарифами банков / платежных систем	Зависят от нагрузки сети (gas fee, priority fee)
Скорость транзакций	Зависит от банка и платежной системы (минуты — дни)	Зависит от DLT (секунды — часы)
Гарантии возврата средств	Возможны (страхование вкладов, оспаривание операций, возврат платежа)	Невозвратность (транзакции необратимы, смарт-контракты исполняются автоматически)
Использование в DeFi	Ограничено (требует интеграции)	Полная совместимость (доступ к смарт-контрактам, DEX, стейкингу, лендингу)
Программируемость	Нет	Да
Регулирование	Подчиняется нормам национального и международного правового поля	Зависит от юрисдикции, но в основном слабо регулируется
Доступность	Требует документов (паспорт, подтверждение дохода, операций и пр.)	Доступен любому (только необходим доступ в Интернет и регистрация в сети)
Географические ограничения	Есть	Нет (кроме единичных блокировок со стороны централизованных сервисов)
Риски	Финансовая цензура, мошенничество и «банковские кризисы»	Потеря ключей и мошенничество

Примечание: составлено автором.

Банковские счета функционируют в рамках доверительной модели, где контроль делегирован финансовым институтам, тогда как *Web*3-кошельки опираются на криптографические механизмы и принцип *self-custody*. Это влечет за собой компромисс между автономией и ответственностью: пользователи *Web*3 получают полную финансовую суверенность, но несут риски, связанные с сохранностью ключей, в то время как банки предлагают защиту в регулируемой среде, ограничивая при этом степень прямого распоряжения средствами.

*Web*3-кошельки выступают критерием дифференциации новой формы денег, отделяя цифровые валюты (включая *CBDC*) от традиционных безналичных средств. Их ключевые атрибуты — программируемость, децентрализованное управление и прямая распоряжаемость — позволяют рассматривать такие активы не как производные от существующих денежных систем, а как самостоятельную категорию, сочетающую свойства «цифровых (аналоговых) наличных» с функциональностью *DLT*. Таким образом, *Web*3-кошельки трансформируют не только механизмы взаимодействия с расчетно-платежными системами, но и концептуальные основы денег, способствуя пересмотру традиционных экономических моделей в условиях цифровизации. Их распространение подчеркивает необходимость четкой терминологической и функциональной градации при анализе современных финансовых инструментов.

Элементы Web3-кошельков. Структура *Web*3-кошелека основана на связке из публичного и приватного ключей, а также seed-фразы, выполняющих различные функции в процессе взаимодействия с *DLT*.

Публичный (открытый) ключ — уникальный адрес кошелька, представленный в виде длинной строки случайной последовательности букв и цифр, используемый для идентификации пользователя в сети, отражения средств и совершения переводов. Публичный ключ находится в открытом доступе, не предоставляя доступ к управлению средствами в кошельке. При совершении транзакций криптоактивы не перемещаются физически, а лишь изменяют запись в распределенном реестре, отражаясь на новом адресе.

Приватный (закрытый) ключ — секретная фраза-пароль доступа к кошельку для управления средствами, подтверждения транзакций и авторизации переводов, поэтому необходимо обеспечивать его сохранность и конфиденциальность. Приватный ключ может быть представлен в разных форматах: мнемонические фразы, *QR*-коды и пр. Утеря или компрометация приватного ключа приводит к безвозвратной потере доступа к криптоактивам. Некоторые кошельки предоставляют возможность резервного копирования приватного ключа для минимизации рисков его утраты.

Seed-фраза (мнемоническая фраза) представляет собой последовательность 12—24 случайных слов, генерируемую при создании *Web*3-кошелька. Ее назначение в восстановлении доступа за счет регенерации приватного ключа в случае его потери — при утрате *seed*-фразы восстановить кошелек невозможно.

Функционирование *Web*3-кошелька основано на асимметричной криптографии и консенсусных алгоритмах распределенных реестров. Процесс создания кошелька включает следующие этапы:

1) генерация приватного ключа и *seed*-фразы:

– пользователь инициирует создание кошелька, в результате чего генерируется криптографически безопасный приватный ключ (случайное число высокой энтропии);

– на основе приватного ключа формируется *seed*-фраза;

2) приватный ключ формирует публичный ключ с использованием эллиптической криптографии;

3) публичный ключ = *DLT*-адрес (уникальный идентификатор, на который поступают криптоактивы).

Транзакция в *Web*3-кошельке выполняется по следующему алгоритму (рис. 2):

– отправитель криптоактивов инициирует перевод суммы из своего кошелька в кошелек получателя, указывая его адрес (открытый ключ) и сумму для перевода (этап 1);

– данные о транзакции (сумма, адреса сторон и пр.) структурируются в определенной форме (блок/запись) и подписываются закрытым ключом отправителя, что подтверждает ее подлинность (этап 2);

– сформированный блок/запись отправляется в сеть для проверки и подтверждения узлами (этап 3);

– участники сети идентифицируют каждую из сторон операции путем проверки их публичных ключей, достаточности средств и подтверждают транзакцию в автоматизированном режиме (этап 3);

– получатель своим закрытым ключом расшифровывает адресованное ему сообщение и получает перевод (этап 4);

– блок/запись, проверенный и подтвержденный всеми участниками сети, добавляется в распределенный реестр (этап 4).

Для взаимодействия с *dApps* используется стандартный процесс авторизации и подтверждения транзакций. Он обеспечивает безопасность и децентрализацию, поскольку пользователь никогда не передает свои приватные ключи приложению. Перед использованием *dApp* необходимо авторизоваться через кошелек, что можно сделать двумя способами: через браузерное расширение (*MetaMask*) или *WalletConnect*. После *dApp* запрашивает подпись транзакции или вызов смарт-контракта, что подтверждается приватным ключом.

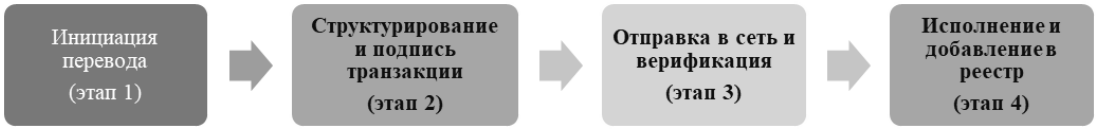

Рис. 2. Алгоритм выполнения транзакции

В контексте функционирования *Web*3-кошельков применяются криптографические методы верификации транзакций, обеспечивающие их аутентичность и целостность. Используются два основных механизма цифровой подписи: 1) *ECDSA* представляет собой стандартизированный метод формирования и проверки цифровых подписей, широко применяемый в *DLT*-сетях; 2) *Multisig* (мультиподпись) – механизм, требующий согласованного подтверждения транзакции несколькими сторонами. Выбор механизма подписи транзакций зависит от требований к безопасности и сценарию использования. В то время как *ECDSA* обеспечивает эффективное подписание для индивидуальных пользователей, *Multisig* применяется в корпоративных системах и *DeFi*, где критически важен распределенный контроль над активами.

Функциональные возможности. *Web*3-кошельки представляют собой не просто инструменты для управления криптоактивами, а играют ключевую роль в экосистеме *Web*3. Они обеспечивают взаимодействие пользователей с распределенными реестрами, *dApps*, *NFT*, *DeFi*, *DAO* и другими сервисами *Web*3.

К базовому функционалу кошельков относятся «хранение» криптоактивов; управление приватными ключами (некастодиальный подход, обеспечивающий полный контроль пользователя над средствами); осуществление транзакций, включая *P*2*P*-переводы, спотовую торговлю и настройку комиссий (*gas fee*). Вместе с тем современные *Web*3-кошельки предлагают широкий спектр дополнительных функций, выходящих за рамки базового управления активами:

– взаимодействие с *dApps*: доступ к *DeFi*-сервисам; работа с *NFT*-маркетплейсами (покупка, продажа и управление NFT на *OpenSea*, *Rarible*); интеграция с играми и метавселенными (*Axie Infinity* и *Decentraland*);

– мультичейн-поддержка: совместимость с различными *DLT*-сетями через *RPC*-настройки; возможность добавления кастомных сетей (*Trust Wallet*); формирование кросс-чейн мостов (*Synapse* и *Wormhole*);

– управление токенами и *NFT*: поддержка разных стандартов токенизации; просмотр и управление *NFT*-коллекциями в интерфейсе кошелька;

– аппаратная интеграция — подключение аппаратных кошельков (*Ledger*, *Trezor*) для повышения уровня безопасности;

– поддержка приватных транзакций через специализированные *privacy*-сервисы (*Zcash*, *ZK-rollups*);

– взаимодействие со смарт-контрактами (подтверждение транзакций в DeFi) и подпись сообщений для верификации без комиссий (смарт-подписи);

– токенизированная идентификация: использование децентрализованных идентификаторов (*Ethereum Name Service*) и авторизация в *dApps* без паролей;

– цифровая конверсия — обмен криптоактивов (в т. ч. в фиатные средства);

– аналитические инструменты и безопасность: мониторинг рынка, «умный анализ» данных, трекеры балансов, защита от фишинга и мошенничества — и др.

Таким образом, криптовалютные кошельки трансформировались в многофункциональные платформы, обеспечивающие не только хранение и передачу криптоактивов, но и интеграцию с широким спектром децентрализованных сервисов, что делает их ключевым элементом инфраструктуры *Web*3.

Типология Web3-кошельков. Криптовалютные кошельки характеризуются существенной вариативностью, обусловленной различиями в способах хранения ключей, уровнях безопасности, типах используемых устройств и функциональных возможностях. Указанные параметры формируют широкий спектр решений, адаптированных для различных сценариев применения в условиях децентрализованной экосистемы.

В зависимости от модели управления ключами выделяют кастодиальные и некастодиальные кошельки (табл. 2). Первая модель включает кошельки, которые предусматривают

наличие сервисов по стороннему управлению ключами пользователей (третьими лицами). В этом случае пользователь не имеет полного контроля над своими закрытыми ключами и зависит от сервиса посредника для доступа к собственным криптоактивам. При этом кастодиальные кошельки, как правило, не анонимны и могут иметь расширенный функционал. Так, в криптопространстве выделяют биржевые кошельки, которые открываются пользователю криптобиржами для хранения активов, полученных на этих платформах. Отметим, что биржи являются централизованными организациями, которые контролируют и управляют своими закрытыми распределенными реестрами. Они осуществляют хранение открытых и закрытых ключей клиентов путем размещения на своем сервере, а пользовательский доступ предоставляют по логину и паролю. Некастодиальные кошельки — *Web*3-кошельки, закрытые ключи которых полностью единолично контролируются их владельцем и к его криптоактивам отсутствует доступ у третьих лиц.

Таблица 2

Сравнительная характеристика кастодиальных и некастодиальных *Web*3-кошельков

Критерий	Кастодиальные кошельки	Некастодиальные кошельки
Контроль над средствами	Средства контролируются третьей стороной	Полный контроль у пользователя (приватные ключи хранятся локально)
Приватные ключи	Хранятся у провайдера	Хранятся только у пользователя
Безопасность	Зависит от безопасности платформы (риск взлома, блокировки аккаунта)	Зависит от пользователя [риск потери ключей, фишинга, вредоносного программного обеспечения (далее — ПО)]
Восстановление доступа	Возможно, через поддержку	Только через seed-фразу
Анонимность	Требует верификации (KYC)	Анонимность (не требует идентификации)
Примеры	Binance, Coinbase, Kraken	MetaMask, Ledger, Trezor, Phantom, Keplr
Удобство	Простота использования, восстановление пароля, интеграция с системами (+ институциональными)	Требует больше ответственности (нужно хранить seed-фразу и следить за безопасностью)
Делегирование управления	Возможно (стейкинг через биржу)	Полная самостоятельность (подписывание транзакции и управление активами)
Комиссии	Могут взиматься дополнительные комиссии за вывод и обслуживание	Обычно только сетевые комиссии (gas fees)
Поддержка DLT-сетей	Зависит от платформы (мульти-чейн, но не все сети доступны)	Зависит от кошелька (MetaMask — EVM-сети; Phantom — Solana и т. д.)
Использование в DeFi	Ограничено (не все кошельки поддерживают прямое подключение к dApps)	Полная интеграция с DeFi, NFT-маркетплейсами, dApps и пр.

Примечание: составлено автором.

В зависимости от режима доступа к сети кошельки могут быть горячими и холодными [13]. Горячие кошельки постоянно подключены к сети «Интернет». Они доступны через *web*-браузеры или мобильные приложения, иногда имея расширенный функционал. С одной стороны, данный вид кошельков представляется наиболее удобным и доступным, с другой — именно они в большей степени подвержены хакерским атакам. Холодные кошельки — тип кошельков с физическим воплощением (аппаратные и бумажные), которые большую часть времени находятся в *offline*. Такие кошельки считаются наименее уязвимыми для взлома и вредоносных программ, при этом высокая безопасность достигается за счет автономного хранения. Основные различия между горячими и холодными *Web*3-кошельками представлены в табл. 3.

Таблица 3

Сравнительная характеристика горячих и холодных *Web*3-кошельков

Критерий	Горячие кошельки	Холодные кошельки
Подключение к Интернет	Постоянное, online-доступ	Отсутствует (offline-хранение)
Безопасность	Уязвимы к кибератакам (фишинг, вредоносное ПО, взлом серверов)	Высокая защищенность (ключи не подвержены удаленным атакам)
Хранение ключей	Приватные ключи хранятся на подключенном к сети устройстве (персональный компьютер, смартфон, браузер)	Ключи хранятся на изолированном устройстве (аппаратный кошелек, бумажный носитель)
Удобство использования	Высокое (быстрые транзакции, интеграция с dApps, DeFi, NFT)	Ограниченное (требуется подключение для подписания транзакций)
Доступность	Бесплатные, легко создать	Требуют покупки аппаратного кошелька / дополнительных носителей
Примеры	MetaMask, Trust Wallet, Phantom	Ledger, Trezor, бумажные кошельки
Риск потери средств	Высокий (из-за экспозиции в Интернет)	Низкий (при условии сохранности seed-фразы и устройства)
Использование в DeFi	Полная интеграция (подписание транзакций в один клик)	Требуется ручное подтверждение через аппаратное устройство
Скорость транзакций	Мгновенная	Замедленная (необходимость физического подтверждения)
Восстановление доступа	Зависит от типа кошелька	Только через seed-фразу (потеря устройства не критична при ее наличии)
Стоимость	Бесплатно	Платно
Анонимность	Зависит от кошелька (некастодиальные — анонимны)	Высокая (отсутствие цифрового следа)

Примечание: составлено автором.

Говоря о поддержке *DLT*-сетей необходимо выделить:

– мультичейн-кошельки поддерживают взаимодействие с несколькими *DLT*-сетями через единый интерфейс, предоставляя возможность управления активами в разных *DLT* без переключения между кошельками и использования кросс-чейн сервисов (мосты, агрегаторы);

– одноцепочечные кошельки специализированы на работе в рамках одной сети, что позволяет оптимизировать функционал под ее особенности.

В табл. 4 систематизированы ключевые различия между мультичейн- и одноцепочечными кошельками по следующих критериям: функциональность, совместимость, удобство использования и безопасность.

Распространенный критерий классификации *Web*3-кошельков — степень их функциональной насыщенности. Так, базовые кошельки ограничиваются минимальным набором операций, включая отправку и получение транзакций; смарт-кошельки обеспечивают расширенную функциональность за счет поддержки смарт-контрактов, мультиподписи и социального восстановления доступа; *MPC*-кошельки применяют криптографические протоколы распределенного управления ключами, исключая наличие единой точки отказа.

Таблица 4

Сравнительная характеристика мультичейн- и одноцепочечных *Web*3-кошельков

Критерий	Мультичейн-кошельки	Одноцепочечные кошельки
Поддержка DLT-сетей	Множество сетей (EVM, Solana, Cosmos и др.) в одном интерфейсе	Только одна DLT-сеть (MetaMask — Ethereum, Phantom — Solana)
Универсальность	Подходят для работы с кросс-чейн активами, мостами и мультисетевыми dApps	Оптимизированы под конкретную экосистему и могут иметь уникальные функции для нее
Удобство управления	Единый кошелек для разных активов (меньше seed-фраз и аккаунтов)	Требует создания отдельного кошелька под каждую сеть
Интеграция с dApps	Широкая, но возможны ограничения в поддержке специфических функций некоторых сетей	Глубокая интеграция с dApps своей сети (Solana-кошельки для Solana DeFi)
Примеры	Trust Wallet, Exodus, Atomic Wallet	MetaMask (EVM), Phantom (Solana)
Безопасность	Зависит от реализации: риски утечки ключей при взаимодействии с множеством сетей	Меньше векторов атак (ограниченная поверхность взаимодействия)
Сложность настройки	Требует ручного добавления сетей (RPC) в некоторых случаях	Простота использования (автоматическая настройка под сеть)
Кросс-чейн транзакции	Встроенные мосты и свопы (Trust Wallet)	Требуют сторонних мостов или мультичейн-кошельков-посредников
Производительность	Возможны задержки из-за поддержки множества сетей	Оптимизированы под свою сеть (быстрые транзакции)
Делегирование и стейкинг	Поддержка в нескольких сетях (Exodus)	Только в native-сети (Keplr для Cosmos)
Популярность	Высокая среди пользователей с диверсифицированным портфелем	Доминируют в своих экосистемах и используются для узкоспециализированных задач

Примечание: составлено автором.

В зависимости от используемого устройства для хранения ключей кошельки подразделяются на пять основных категорий [14; 15]: аппаратные, бумажные, мобильные, десктопные и браузерные.

Аппаратные кошельки представляют собой специализированные физические устройства, предназначенные для *offline*-хранения закрытых ключей. Их основное преимущество — высокая устойчивость к кибератакам благодаря изолированности от сети. Конструктивно они выполнены в виде компактных устройств (аналогичных *USB*-накопителям), оснащенных защищенной памятью и специализированным ПО для управления ключами, а также хранения сопутствующих данных. Подключение к Интернет осуществляется исключительно в момент проведения транзакций, что минимизирует риски компрометации. Дополнительные механизмы безопасности включают многофакторную аутентификацию, резервные *seed*-фразы, биометрическую верификацию и аппаратные средства защиты. Несмотря на высокую степень надежности, данный тип кошельков отличается относительно высокой стоимостью и потенциальной уязвимостью к сбоям встроенного программного и аппаратного обеспечения. С точки зрения классификации по режиму доступа к сети аппаратные кошельки относятся к холодному хранению.

Бумажные кошельки представляют собой метод *offline*-хранения, при которой закрытый и открытый ключи, а также *seed*-фраза фиксируются на физическом носителе (бумаге) в виде текста/*QR*-кодов. Этот способ обеспечивает полную защиту от цифровых угроз, включая хакерские атаки и вредоносное ПО, поскольку хранение осуществляется вне сети. Основное преимущество — максимальная устойчивость к кибератакам, что делает бумажные кошельки оптимальным решением для долгосрочного хранения криптоактивов. Однако ключевой недостаток — уязвимость к физическому уничтожению или потере носителя: без резервных копий восстановление доступа невозможно. Для снижения рисков рекомендуется использовать дополнительные меры защиты, такие как ламинирование документа или хранение в сейфовых ячейках. По классификации доступа бумажные кошельки также относятся к холодному хранению.

Мобильные кошельки — это приложения для смартфонов и планшетов, обеспечивающие управление криптоактивами в режиме горячего хранения (постоянно подключены к Интернет через мобильное устройство). Они поддерживают широкий спектр операций, включая транзакции, стейкинг и взаимодействие с *dApps*. Ключи могут храниться локально на устройстве (в зашифрованном виде) или в облачных сервисах с дополнительной аутентификацией. Некоторые решения используют встроенные функции безопасности смартфонов, таких как биометрическая идентификация (*Face ID*, *Touch ID*) и защищенные элементы (*Secure Enclave*). Основные преимущества мобильных

кошельков включают удобство использования (быстрый доступ к средствам в любое время); мульти функциональность (поддержка различных *DLT*, токенов и *DeFi*-сервисов) и дополнительные уровни защиты (*PIN*-коды и 2*FA*). Однако они подвержены рискам, связанным с кибератаками (фишинг, вредоносное ПО, взлом устройства); потерей/поломкой устройства (без резервной копии *seed*-фразы доступ невозможен) и зависимостью от операционной системы (уязвимости *iOS*/*Android* могут компрометировать безопасность).

Десктопные кошельки представляют собой программные решения для персональных компьютеров и ноутбуков, обеспечивающие локальное хранение закрытых ключей на жестком диске в зашифрованном виде. В зависимости от режима работы они могут функционировать как в горячем, так и в холодном хранилище (при отключении от сети). Они подразделяются на «толстые», когда предполагается хранение на пользовательском устройстве криптографических ключей и копии всего распределенного реестра (требуя значительного объема памяти), и «тонкие» — программа-клиент не хранит весь распределенный реестр. Десктопные кошельки предоставляют полный контроль над активами и поддерживают расширенные функции: от базовых транзакций до взаимодействия с полными узлами сети, сложных смарт-контрактов и поддержки мультиподписи. Их преимущества включают повышенную безопасность по сравнению с *online*-решениями и отсутствие зависимости от третьих сторон. Однако они уязвимы к вредоносному ПО, компрометации из-за небезопасности компьютера и требуют регулярного резервного копирования.

Браузерные кошельки представлены программными расширениями или *web*-приложениями, интегрируемыми в интернет-браузеры. Они функционируют исключительно в режиме горячего хранения, обеспечивая быстрый доступ к *dApps*, *DeFi*-платформам и *NFT*-маркетплейсам. Ключи хранятся в зашифрованном виде в локальном хранилище браузера, а доступ защищается паролями или *seed*-фразами. Основные преимущества — удобство использования, поддержка *EVM*-совместимых сетей и отсутствие необходимости в отдельной установке. Недостатки включают уязвимость к фишингу, взлому браузера и ограниченную функциональность по сравнению с автономными решениями.

Отдельно остановимся на гибридных *Web*3-кошельках, которые сочетают функциональность нескольких типов хранилищ (аппаратных, мобильных, десктопных и браузерных), обеспечивая синхронизацию между устройствами без потери безопасности. К их особенностям относятся мультиплатформенность (поддержка различных операционных систем и *web*-интерфейсов); гибридное хранение ключей (возможность выбора между горячим и холодным режимами); интеграция с аппаратными модулями безопасности (*HSM*); расширенная функциональность (мультиподпись, кросс-чейн, доступ к *DeFi* и пр.).

Заключение

*Web*3-кошельки представляют собой не просто инструменты для хранения и передачи криптоактивов, а фундаментальный элемент новой финансовой парадигмы, основанной на децентрализации и самоуправлении. В отличие от банковских счетов, которые функционируют в рамках доверительной модели с централизованным контролем, *Web*3-кошельки обеспечивают прямой доступ к активам через криптографические ключи, исключая необходимость в посредниках. Однако эта автономия сопряжена с повышенной ответственностью пользователей за сохранность ключей и защиту от мошенничества. Разнообразие типов кошельков — от кастодиальных до некастодиальных, от горячих до холодных — позволяет адаптировать их под различные сценарии использования, от повседневных транзакций до долгосрочного хранения. Распространение криптовалютных кошельков подчеркивает необходимость пересмотра традиционных экономических моделей и разработки четких терминологических градаций для современных финансовых инструментов. Их дальнейшее развитие будет способствовать углублению интеграции децентрализованных технологий в глобальную финансовую систему.

СПИСОК ИСТОЧНИКОВ

1. Erinle Y., Kethepalli Y., Feng Y., Xu J. SoK: Design, Vulnerabilities, and Security Measures of Cryptocurrency Wallets // arXiv. 2307.12874. DOI: 10.48550/arXiv.2307.12874.

2. Houy S., Schmid Ph., Bartel A. Security Aspects of Cryptocurrency Wallets—A Systematic Literature Review // ACM Computing Surveys. 2023. Vol. 56. Iss. 1. Art. 4. DOI: 10.1145/3596906.

3. Guo H., Yu X. A survey on blockchain technology and its security // Blockchain: Research and Applications. 2022. Vol. 3. Iss. 2. Art. 100067. DOI: 10.1016/j.bcra.2022.100067.

4. Kim H., Park S. Cryptocurrency recovery framework using pre-signed transaction // International Journal of Information Security. 2025. Vol. 24. Art. 84. DOI: 10.1007/s10207-025-00994-5.

5. Fanti G., Viswanath P. Deanonymization in the Bitcoin P2P Network // Advances in Neural Information Processing Systems 30 (NIPS 2017). URL: https://proceedings.neurips.cc/paper_files/paper/2017/hash/6c3cf77d52820cd0fe646d38bc2145ca-Abstract.html.

6. Balu R., Furon T., Gambs S. Challenging Differential Privacy: The Case of Non-interactive Mechanisms // Computer Security - ESORICS 2014 : 19th European Symposium on Research in Computer Security / eds. M. Kutyłowski, J. Vaidya. Cham : Springer, 2014. Pt. II. Pp. 146–164. (Lecture Notes in Computer Science; Vol. 8713). DOI: 10.1007/978-3-319-11212-1_9.

7. Alqaryouti O., Siyam N., Alkashri Z., Shaalan K. Users' Knowledge and Motivation on Using Cryptocurrency // Information Systems. EMCIS 2019 : 16th European, Mediterranean, and Middle Eastern Conference / eds. M. Themistocleous, M. Papadaki. Cham : Springer, 2019. Pp. 113—122. (Lecture Notes in Business Information Processing; Vol. 381). DOI: 10.1007/978-3-030-44322-1_9.

8. Finck M. Blockchain Regulation and Governance in Europe. Cambridge University Press, 2018. 214 p. DOI: 10.1017/9781108609708.

9. Tasca P., Tessone C. J. A Taxonomy of Blockchain Technologies: Principles of Identification and Classification // Ledger. 2019. Vol. 4. Pp. 1—39. DOI: 10.5195/ledger.2019.140.

10. SoK: Decentralized Finance (DeFi) / S. M. Werner, D. Perez, L. Gudgeon et al. // arXiv. 2101.08778. DOI: 10.48550/arXiv.2101.08778.

11. Семьянов П. В., Грезина С. В. Анализ криптографической защиты криптокошелька Bitcoin Core // Проблемы информационной безопасности. Компьютерные системы. 2023. № 2. С. 82—91. DOI: 10.48612/jisp/mrx7-m1rk-2316.

12. Дюдикова Е. И., Куницына Н. Н. Парадоксы имплементации цифрового рубля в денежный оборот // Вопросы экономики. 2024. № 4. С. 148—158. DOI: 10.32609/0042-8736-2024-4-148-158.

13. Прасти Н. Блокчейн. Разработка приложений : пер. с англ. СПб. : БХВ-Петербург, 2018. 256 с.

14. Ситник А. А. Технология блокчейн в платежных системах // Актуальные проблемы российского права. 2021. Т. 16. № 5. С. 42—54. DOI: 10.17803/1994-1471.2021.126.5.042-054.

15. Милованов В. В. История развития цифровых валют: от электронных денег к криптовалютам // Азимут научных исследований: экономика и управление. 2024. Т. 13. № 1. С. 84—89.

REFERENCES

1. Erinle Y., Kethepalli Y., Feng Y., Xu J. SoK: Design, Vulnerabilities, and Security Measures of Cryptocurrency Wallets. *arXiv*. 2307.12874. DOI: 10.48550/arXiv.2307.12874.

2. Houy S., Schmid Ph., Bartel A. Security Aspects of Cryptocurrency Wallets—A Systematic Literature Review. *ACM Computing Surveys*. 2023;56(1):4. DOI: 10.1145/3596906.

3. Guo H., Yu X. A survey on blockchain technology and its security. *Blockchain: Research and Applications*. 2022;3(2):100067. DOI: 10.1016/j.bcra.2022.100067.

4. Kim H., Park S. Cryptocurrency recovery framework using pre-signed transaction. *International Journal of Information Security*. 2025;24:84. DOI: 10.1007/s10207-025-00994-5.

5. Fanti G., Viswanath P. Deanonymization in the Bitcoin P2P Network. *Advances in Neural Information Processing Systems 30 (NIPS 2017)*. URL: https://proceedings.neurips.cc/paper_files/paper/2017/hash/6c3cf77d52820cd0fe646d38bc2145ca-Abstract.html.

6. Balu R., Furon T., Gambs S. Challenging Differential Privacy: The Case of Non-interactive Mechanisms. *Computer Security — ESORICS 2014. 19th European Symposium on Research in Computer Security*, Lecture Notes in Computer Science; Vol. 8713. M. Kutyłowski, J. Vaidya (eds.). Cham, Springer, 2014;2:146–164. DOI: 10.1007/978-3-319-11212-1_9.

7. Alqaryouti O., Siyam N., Alkashri Z., Shaalan K. Users' Knowledge and Motivation on Using Cryptocurrency. *Information Systems. EMCIS 2019. 16th European, Mediterranean, and Middle Eastern Conference*, Lecture Notes in Business Information Processing; Vol. 381. M. Themistocleous, M. Papadaki (eds.). Cham, Springer, 2019:113—122. DOI: 10.1007/978-3-030-44322-1_9.

8. Finck M. Blockchain Regulation and Governance in Europe. Cambridge University Press, 2018. 214 p. DOI: 10.1017/9781108609708.

9. Tasca P., Tessone C. J. A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger*. 2019;4:1—39. DOI: 10.5195/ledger.2019.140.

10. Werner S.M., Perez D., Gudgeon L. et al. SoK: Decentralized Finance (DeFi). *arXiv*. 2101.08778. DOI: 10.48550/arXiv.2101.08778.

11. Semianov P.V., Grezina S.V. Bitcoin Core Cryptocurrency Wallet Cryptographic Security Analysis. *Problemy informacionnoj bezopasnosti. Kompyuternye sistemy = Information Security Problems. Computer Systems*. 2023;2:82—91. (In Russ.) DOI: 10.48612/jisp/mrx7-m1rk-2316.

12. Dyudikova E. I., Kunitsyna N. N. Paradoxes of the digital ruble implementation in monetary turnover. *Voprosy Ekonomiki*. 2024;4:148—158. (In Russ.) DOI: 10.32609/0042-8736-2024-4-148-158.

13. Prasti N. Blockchain. Application Development. Transl. from English. Saint Petersburg, BKhV-Petersburg, 2018. 256 p. (In Russ.)

14. Sitnik A.A. Blockchain Technology in Payment Systems. *Aktual`nye problemy rossiiskogo prava = Actual Problems of Russian Law*. 2021;16(5):42—54. (In Russ.) DOI: 10.17803/1994-1471.2021.126.5.042-054.

15. Milovanov V.V. The History of Digital Currencies: From E-Money to Cryptocurrencies. *Azimut nauchnykh issledovanii: ekonomika i upravlenie = Azimuth of Scientific Research: Economics and Administration*. 2024;13(1):84—89. (In Russ.)

Статья поступила в редакцию 05.05.2025; одобрена после рецензирования 29.05.2025; принята к публикации 02.06.2025.
The article was submitted 05.05.2025; approved after reviewing 29.05.2025; accepted for publication 02.06.2025.