

УДК 336.74: 004.75

151. ОСОБЕННОСТИ КРИПТОВАЛЮТНЫХ ОПЕРАЦИЙ В СЕГМЕНТЕ P2P

*Масальский А. И. – студент гр.578104, Бабков М. М. – ассистент кафедры ЭИ
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Ефремов А. А. – канд. экономических наук, доцент

Аннотация. В статье анализируется трансформация глобальной финансовой архитектуры через призму развития P2P-технологий. Рассматриваются преимущества децентрализации и ключевые различия между кастодиальными и некастодиальными моделями расчетов. Особое внимание уделено киберугрозам нового поколения, включая использование генеративных нейросетей, и методам их нейтрализации. Исследуется опыт правового и потенциал токенизации реальных активов. Обосновывается концепция безопасности как фундаментального фактора масштабирования сектора. Делается вывод, что синергия доверия к коду и адаптивного регулирования обеспечит полную интеграцию P2P-систем в глобальную экономическую систему.

Ключевые слова. Криптовалюта, P2P-транзакции, кибербезопасность, смарт-контракты, децентрализация, некастодиальные платформы, социальная инженерия, доказательство с нулевым разглашением (ZKP), нормативное регулирование, финансовая инклюзивность.

Глобальная финансовая архитектура вступает в фазу необратимой децентрализации. Традиционные механизмы межбанковских расчетов – включая систему SWIFT – демонстрируют критическую неэффективность: чрезмерные задержки (время обработки платежей достигает 3–5 рабочих дней), многоуровневые комиссии банков-корреспондентов, а также растущий риск политически мотивированного замораживания активов. На этом фоне одноранговые (P2P) транзакции трансформировались в системно значимый механизм обеспечения ликвидности. Так, например, для стран Глобального Юга P2P-сети стали единственным жизнеспособным средством доступа к мировому рынку капитала в условиях жесткого валютного контроля.

Ключевое преимущество P2P-архитектуры заключается в отсутствии централизованных точек отказа, что делает сеть устойчивой к внешним санкциям и техническим сбоям со стороны посредников. Однако децентрализация переносит операционные риски непосредственно на программную логику смарт-контрактов и уровень компетентности конечного пользователя. Учитывая, что 1,4 миллиарда человек классифицируются Всемирным банком как «неохваченные банковскими услугами» (unbanked), и что объем P2P-платформ ежегодно растет на 20–25%, надежность этих шлюзов становится вопросом глобальной экономической стабильности. Текущий этап требует разрешения противоречия: системы должны сохранять операционную гибкость, не жертвуя при этом безопасностью, необходимой для привлечения капитала.

Доверие в среде гарантируется алгоритмами эскроу, которые минимизируют риски «двойного расходования» и мошенничества со стороны контрагентов. В современной практике доминируют две архитектурные парадигмы: кастодиальная модель и некастодиальные решения.

В первую очередь будет описана кастодиальная модель. Централизованные платформы (Binance P2P, Bybit, OKX) хранят активы на своих внутренних биржевых кошельках. Это позволяет использовать централизованные системы арбитража, в рамках которых споры разрешаются оператором на основе внешних данных о фиатных средствах (например, выписок из банковских приложений или SMS-подтверждений). Основным риском в данном случае является риск контрагента. Взломы бирж, внутренняя коррупция или оперативное исполнение предписаний о заморозке активов делают эту клиентскую модель уязвимой для государственного контроля – несмотря на высокую скорость разрешения споров.

Некастодиальные платформы (DEX, Bisq, HodlHodl) используют протоколы Hashed Timelock Contracts (HTLC) и мультисиг-счета. Активы блокируются в блокчейне с помощью математических «замков», условия разблокировки которых строго определены программным кодом. При такой транзакции средства перечисляются покупателю только после предъявления криптографического секрета, подтверждающего факт оплаты. Это позволяет исключить риски, связанные с участием посредников, однако требует от пользователя строгого соблюдения правил «цифровой гигиены». Ошибки при управлении сид-фразами или закрытыми ключами приводят к безвозвратной утрате средств без какой-либо возможности их возврата.

Безопасность дополняет ончейн-репутация – прозрачная история транзакций, записанная в неизменяемый реестр. В отличие от банковских кредитных рейтингов, P2P-репутация формируется на основе объективных параметров: процент успешно завершенных заказов, средняя скорость ответа и объем торгов.

Киберугрозы представляют собой чрезвычайно серьезную проблему: согласно некоторым источникам, в 2025 году объем хищений в криптовалютной индустрии составил 3,4 млрд долларов [1]. Киберпреступность прошла процесс профессионализации: прямые атаки, нацеленные на уязвимости в коде, вытесняются гибридными схемами.

Один из основных методов предполагает использование генеративных нейросетей, что позволяет создавать дипфейки в режиме реального времени. Злоумышленники имитируют видеозвонки от служб безопасности или банков, манипулируя пользователями и вынуждая их подтверждать транзакции без фактического получения денежных средств. Это подрывает эффективность традиционной двухфакторной аутентификации и побуждает отрасль переходить к биометрии с нулевым разглашением (ZK-биометрии) – технологии, позволяющей верифицировать личность без передачи самих биометрических данных в облачные хранилища.

Регулирующие органы реагируют на эти вызовы посредством стандартизации. Регламент ЕС MiCA (Markets in Crypto-Assets) обязывает поставщиков услуг в сфере крипто активов внедрять строгие процедуры верификации личности, а также отделять активы клиентов от корпоративных активов.

В Республике Беларусь Декрет №8 «О развитии цифровой экономики» сформировал одну из наиболее либеральных и в то же время структурированных правовых баз для криптоактивов в регионе. Резидентам Парка высоких технологий (ПВТ) были предоставлены уникальные правовые условия для осуществления операций с токенами, включая создание криптовалютных бирж и обменных сервисов [2]. На фоне частичных ограничений доступа к международным платежным системам P2P-платформы стали для белорусского бизнеса и граждан эффективным каналом поддержания трансграничной ликвидности. Эта трансформация превратила страну в экспериментальный полигон для внедрения смарт-контрактов в реальный сектор экономики.

Более того, P2P-сети имеют глубокие социально-экономические последствия: они радикально снижают издержки, связанные с денежными переводами мигрантов. В странах Африки и Латинской Америки комиссии, взимаемые традиционными системами, достигают 8–10%. P2P-переводы с использованием стейблкоинов (например, USDT и USDC) снижают эти издержки всего до 1–1,5%, обеспечивая при этом мгновенную доставку средств [3]. В Нигерии, Вьетнаме и Аргентине «цифровые доллары», переводимые через P2P-сети, стали основным инструментом хеджирования рисков, связанных с национальными валютами.

Ключевым трендом 2025–2026 годов станет перенос прав собственности на физические активы – недвижимость, облигации и сырьевые товары – в блокчейн. P2P-платформы трансформируются в глобальные вторичные рынки для реальных активов. Согласно прогнозам, к 2030 году объем рынка токенизированных активов достигнет 10% от мирового ВВП.

Технологический прогресс, достигнутый в области бизнес-решений на основе доказательств с нулевым разглашением (ZKP), позволяет подтверждать легитимное происхождение средств или статус KYC без раскрытия паспортных данных пользователя [4]. Это разрешает противоречие между правом на неприкосновенность частной жизни и нормативными требованиями, устанавливаемыми государством, тем самым создавая условия для безопасного и анонимного взаимодействия в рамках правового поля. Практическая реализация этого баланса между надзором и свободой транзакций находит отражение в существующих экономических моделях государственного регулирования; в контексте Республики технологическая верификация сочетается с математически обоснованными фискальными стимулами.

Экономическая выгода (B) пользователя от использования P2P-инструментов в легальном поле до 2025 года описывается функцией налогового бремени:

$$B(t) = I * (1 - t) - C(I), \quad (1)$$

где

I – доход от операций;

t – ставка налога (равная 0 для физлиц по Декрету №8);

$C(I)$ – комиссия P2P-платформы, напрямую зависящая от дохода операции.

Параллельно с выгодой пользователя, целесообразность поддержки легального P2P-сектора для государства (G) в данной модели описывается функцией совокупного дохода:

$$G(t) = I * t + T_{plat} - S, \quad (2)$$

где

T_{plat} – налоговые и лицензионные отчисления самой платформы;

S – затраты государства на мониторинг и обеспечение регуляторного комплаенса.

В свою очередь, прибыль самой P2P-платформы (P) как связующего звена системы определяется эффективностью монетизации трафика:

$$P = \sum C(I) - T_{plat} - O, \quad (3)$$

где

O – операционные расходы на техническое поддержание сети.

Представленные уравнения формируют единую систему динамического равновесия, в которой интересы всех участников не просто пересекаются, а являются производными друг от друга. Эта математическая модель наглядно демонстрирует эффект синергии.

Более того, P2P-сектор представляет собой весьма привлекательное направление для инвестиций. Это обусловлено его антихрупкостью: в периоды банковских кризисов объем P2P-транзакций демонстрирует корреляцию с ростом спроса на «твердые» активы. Тем не менее инвесторам необходимо учитывать сопряженные риски – прежде всего риск ликвидности. Это означает, что в условиях экстремальной волатильности спред между ценами покупки и продажи на P2P-рынках может расширяться до 5–7%. Кроме того, неодинаковый правовой статус криптовалют в различных юрисдикциях создает правовые ловушки для участников трансграничной торговли.

Таким образом, анализ глобальных тенденций подтверждает, что фокус на развитие вместо безопасности в P2P-секторе является концептуально ошибочным. Безопасность выступает не ограничителем экспансии, а, напротив, её фундаментом. Дальнейшая эволюция P2P-систем будет зависеть от масштабирования некастодиальных решений и устойчивости к угрозам, порождаемым искусственным интеллектом.

Сбалансированный «общественный договор» между пользователями, платформами и государством позволит P2P-технологиям полностью интегрироваться в качестве фундаментального, неотъемлемого уровня глобальной финансовой системы.

Список использованных источников:

1. Отчет Chainalysis [Электронный ресурс] // Кузьмичева А., Лузгин А. – URL: <https://www.rbc.ru/crypto/news/69453c9f9a7947f3cb18874b?> (дата обращения: 04.04.2026).
2. Декрет Президента Республики Беларусь № 8 «О развитии цифровой экономики» (в редакции от 2024 г.) – пункты 2.1, 2.2.
3. Remittance Prices Worldwide Quarterly - Issue 48 [Электронный ресурс] // The World Bank. – URL: <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099053025160039576> (дата обращения: 04.04.2026).
4. Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium [Электронный ресурс] // Buterin V., Illum J., Nadler M., Schar F., Soleimani A. – URL: <https://www.sciencedirect.com/science/article/pii/S2096720923000519> (дата обращения: 04.04.2026).

THE SPECIFICS OF CRYPTOCURRENCY TRANSACTIONS WITHIN THE P2P MARKET

*Masalskiy A. I. – student of group 578104, Babkov M.M. – assistant of the
Department of EI*

*Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus*

Efremov A. A. – Candidate of Economic Sciences, Associate Professor

Annotation. The article examines the transformation of the global financial architecture through the lens of P2P technology development. It analyzes the benefits of decentralization and key differences between custodial and non-custodial settlement models. Special focus is given to next-generation cyber threats, including generative AI, and neutralization methods such as ZK-biometrics. The research explores regulatory frameworks (MiCA, Decree No. 8 in Belarus) and the potential for real-world asset tokenization. The author substantiates the concept of security as a fundamental factor for sector scaling. It is concluded that the synergy between code-based trust and adaptive regulation will enable the full integration of P2P systems into the global economic infrastructure.

Keywords. Cryptocurrency, P2P transactions, cybersecurity, smart contracts, decentralization, non-custodial platforms, social engineering, zero-knowledge proof (ZKP), regulatory framework, financial inclusion.