УДК 336.741.1 (045)

Специальные инструменты выявления и противодействия недобросовестным практикам с цифровыми финансовыми активами

А. Г. Коринной

Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, Российская Федерация, 198206, Санкт-Петербург, ул. Летчика Пилютова, 1

Для цитирования: *Коринной А. Г.* Специальные инструменты выявления и противодействия недобросовестным практикам с цифровыми финансовыми активами // Бюллетень результатов научных исследований. — 2023. — Вып. 1. — С. 125–132. DOI: 10.20295/2223-9987-2023-1-125-132

Аннотация

Цель: В статье рассматриваются концептуально новые подходы противодействия использованию криптовалют и электронных средств платежа в недобросовестных практиках. В результате установлено, что все они нацелены на выявление подозрительных транзакций и деанонимизацию личностей, причастных к незаконной деятельности. Обосновывается вывод о том, что информационно-аналитические системы являются перспективными специальными инструментами для эффективного контроля криптовалютного рынка и блокчейн-сетей. Теоретическую основу исследования составили научные публикации экспертов, специализирующихся на вопросах вовлечения, технологии блокчейна, распределенных реестров и криптовалют при расследовании преступлений, а также применяемые иностранные программные инструменты в области обеспечения безопасности блокчейн-сетей. **Методы:** В исследовании автор опирается на методы дедукции, системного анализа, обобщения и синтеза. **Результаты:** Определение возможностей зарубежных и отечественных специальных инструментов в сфере деятельности провайдеров виртуальных кошельков и операторов обмена (типа «крипотвалютных бирж» и пр.). **Практическая значимость:** Представлен механизм функционирования специальных инструментов по деанонимизации транзакций с целью противодействия использования криптовалют и электронных средств платежа в недобросовестных практиках.

Ключевые слова: Цифровые финансовые активы, криптовалюта, электронных средств платежа, недобросовестные практики, блокчейн-сети, деанонимизация, специальные инструменты, информационно-аналитические системы, машинное обучение.

Введение

В настоящий момент виртуальное пространство стало полем деятельности организованных преступных групп. Об этом можно судить по обобщенным результатам исследований криминалистических практик, где электронное средство платежа стало одним из основных средств финансовых расчетов в сфере незаконного оборота наркотических средств [1], психотропных и психоактивных веществ, оружия, финансирования террористической и экстремистской деятельности [2, 3]. Сюда же можно добавить предоставление российскими юридическими лицами услуг по обмену криптовалют на рубли и иностранную валюту, а также на

предметы роскоши, работы (услуги). В целом все подобное положение дел позволяет сделать вывод о масштабе и актуальности угрозы незаконного использования в целом цифровых финансовых активов (далее — ЦФА) в осуществлении сомнительных операций в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма [4]. Как правило, при транзакциях преступники используют криптовалюту [2]. Согласно отчету FATF, наиболее популярными являются Bitcoin, Ethereum, Monero. Правда, последний имеет сомнительную репутацию из-за своего анонимного статуса и повышенной конфиденциальности протокола.

Методы исследования

Для достижения цели исследования автор, используя метод дедукции, переходит от общего вопроса противодействия криминализации экономической сферы ЦФА к предметному набору специальных инструментов, доступных органам исполнительной власти, осуществляющим функции по обеспечению экономической безопасности. Метод анализа и обобщения был применен для описания свойств специальных инструментов по выявлению подозрительных транзакций и деанонимизации личностей, причастных к незаконной деятельности. Материалами для анализа послужили существующие инструменты аналитических компаний, специализирующихся в области использования технологии распределенных реестров и на вопросах безопасности протоколов блокчейн-сетей и криптовалют. Также с помощью метода синтеза была построена схема функционирования специальных инструментов деанонимизации применительно к процессу функционирования систем и программ обеспечения деанонимизации.

Результаты исследования

В данной статье внимание акцентируется на деанонимизации как инструменте предотвращения преступных практик с криптовалютой. Для противодействия анонимизации криптовалют и электронных средств платежа необходим широкий спектр мер воздействия на причины, их порождающие, с целью устранения или нейтрализации их последствий. Прежде всего необходимо идентифицировать личности участников и реальных бенефициаров, причастных к незаконной деятельности. На это неоднократно указывалось в официальных обзорах и криминалистической литературе [5, 3].

Для достижения целей исследования следует определить две группы инструментов по деанонимизации. Первая — универсальные инструменты — предназначена для снижения криминального потенциала криптовалюты путем видоизменений правил рынка и программного кода валют. То есть применительно

к экономической сфере эти инструменты воздействуют на экономику валюты в целом. По своей сути универсальные инструменты предназначены для проблем гораздо более глобального уровня, чем те, о которых идет речь в данной статье [6].

Назначение второй группы инструментов более конкретно: это обеспечение принудительной деанонимизации. Таким образом, мы имеем специальный инструментарий, напрямую воздействующий на теневой сектор криптовалютной экономики с помощью комплекса систем. Специальные инструменты, в отличие от универсальных, четко ориентированы на борьбу с недобросовестными практиками на аналитическом и оперативном подуровнях. Сюда входят инструменты, связанные с деятельностью Росфинмониторинга, финансово-кредитных организаций и правоохранительных органов. Оптимизация в этой сфере в конечном результате должна повысить результативность борьбы с определенными видами недобросовестных практик, а также обеспечить своевременное реагирование соответствующих структур о неединичных преступлениях такого рода [7].

Собственно, сами специальные инструменты обладают не слишком широкими возможностями влияния на процесс анонимизации и чаще всего представлены информационно-аналитическими системами и сетевыми разработками. Это относится как к российским, так и к иностранным производителям (в качестве примера можно привести «Прозрачный блокчейн», Crystal, Chainalysis, Elliptic) [8].

Сочетание разных методов и инструментов и уровня их воздействия на блокчейн-системы определяется не видимыми, «лежащими на поверхности» закономерностями, а гораздо более глубинными. Кроме того, они могут быть использованы в целях расследования предикатных преступлений и предоставления общей аналитической информации о состоянии криптовалютной сферы в России.

Разработанная в России по заказу Росфинмониторинга система «Прозрачный блокчейн» предназначена для мониторинга и анализа движения цифровых активов, в основном с использованием наиболее распространенных в России криптовалют (типа «биткоин» и пр.). Эксплуатация системы органами экономического и правоохранительного обеспечения должна решить следующие значимые задачи:

– осуществлять анализ, а также прослеживать движение цифровых активов;

– осуществлять сбор и хранение сведений определенных адресов сети блокчейна (виртуальных кошельков), владеющих виртуальными активами, а также, возможно, вовлеченных в противоправную деятельностью;

– осуществлять наблюдение за деятельностью участников криптовалютного рынка и блокчейн-сетей;

– осуществлять налогообложение операций в сети блокчейна;

– оформлять профили участников транзакций и оценивать их роль в экономической деятельности.

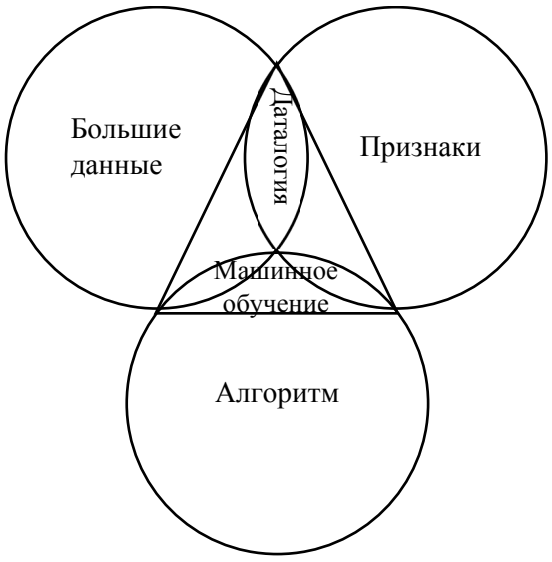
Однако также следует обратить внимание и на западный опыт в части имеющихся на рынке информационных систем [9, 10]:

– коммерческий программный продукт от сервиса Crystal дает возможность внутренним службам операторов обмена криптовалют прослеживать пути перемещения подозрительных транзакций до конечного получателя или точки вывода криптовалюты. Такой тип инструментов можно отнести к аналитическому типу: он не дает оценок законности транзакций, однако допускает сбор и обработку подробной информации сотрудникам правоохранительных органов или внутреннему пользователю;

– Chainalysis, ИТ платформа занимающаяся криптовалютными расследованиями. Программный продукт для блокчейн-сетей под названием Know Your Transaction (KYT) предоставляет обратную связь по транзакциям в реальном времени и отправляет соответствующую информацию операторам обмена на «движок обработки транзакций». Таким образом, руководители площадок видят «рискованных» пользователей и получают возможность отслеживать их подозрительные действия [3]. Инструмент может показать свою эффективность в отслеживании людей, которые участвуют в незаконной деятельности, связанной с криптовалютами. Как пример использования — наличие в списках западных санкций граждан РФ. Инструмент активно применяют иностранные правоохранительные органы США (ФБР и Управление по борьбе с наркотиками) и ЕС (Европол);

– Elliptic представляет собой комплексный скрининг возможных рисков в обеспечении соответствия требованиям деанонимизации и объединяет поток транзакций клиентов и их криптоактивов в сетях блокчейн, иллюстрируя всю криптосферу. Он также укажет на угрозу, независимо от актива или анализируемого блокчейна. Как прогностический инструмент он может использоваться в качестве системы предоставления прогностических показателей и построения прогностических моделей, позволяющих в дальнейшем снизить риски использования криптовалют и электронных средств платежа в схемах легализации.

Схема 1
Принцип функционирования специальных инструментов деанонимизации



Таким образом, анализируя основные принципы функционирования систем, программ обеспечения деанонимизации и получения общей информации о состоянии криптовалютной сферы, можно прийти к выводу, что почти все они построены на инструментах науки о данных и машинном обучении. Эти инструменты во многом пересекаются, но все же они разные и у каждого свои задачи.

Рассмотрим основные свойства специальных инструментов применительно к процессу функционирования систем, программ обеспечения деанонимизации:

1. Большие данные (Big Data) — непрерывная работа с большим объемом данных, полученных непосредственно от блокчейн-сетей (операторов обмена). Это в основном выборки типовых транзакций, работе с которыми нужно обучить систему. Чем больше транзакций загружено в систему, тем лучше и точнее она будет работать.

2. Даталогия, или наука о данных (Data Science). Позволяет извлекать полезные сведения из общего потока транзакций в исследуемой сети блокчейн с целью нахождения правильного подхода для дальнейшего анализа, сортировки, выборки и поиска данных, в нее поступающих.

3. Признаки представлены в системе в виде аналитических данных о недобросовестных практиках, связанных с возможными злоупотреблениями в сфере информационных технологий и позволяющих уходить от мониторинга и идентификации источника для целей извлечения выгоды или совершения преступления по отмыванию незаконно полученных доходов [11, 12].

4. Алгоритм используется для алгоритмизации функционирования выбранного подхода как внутри подсистемы, так и между подсистемами. Подбор уникального алгоритма деанонимизации определяет задачи, которые ставятся перед системой, программой.

5. Машинное обучение (Machine learning) позволяет искусственному интеллекту делать выводы о конкретных операциях с криптовалютой и электронными средствами платежа на основании выходных данных из подсистем с учетом прописанных признаков недобросовестных операций, схем по отмыванию доходов, видов преступлений и т. д. То есть система (программа) должна найти закономерность в сложных многопараметрических задачах, выдавая таким образом более точные результаты обработки исходных данных выборки. Как результат — более точное прогнозирование.

Соответственно, выявление подозрительных транзакций и деанонимизация являются перспективными специальными инструментами предотвращения преступных практик с целью мониторинга и контроля криптовалют и электронных средств платежа, учитывающими специфику исследуемой сферы и опирающимися на принципы анализа типовых транзакций с помощью обработки больших массивов данных с использованием метода машинного обучения, подобранного с учетом особенностей поставленных задач.

Библиографический список

1. Сизов Д. А. К вопросу организации противодействия незаконному обороту синтетических аналогов каннабиноидов (по материалам УМВД России по Костромской области) / Д. А. Сизов // Труды Академии управления МВД России. — 2015. — № 3(35). — С. 125–128.

2. Батоев В. Б. Использование криптовалюты в преступной деятельности: проблемы противодействия / В. Б. Батоев, В. В. Семенчук // Труды Академии управления МВД России. — 2017. — № 2(42). — С. 9–15.

3. Земцова С. И. Криптовалюта в незаконном обороте наркотических средств: вопросы деанонимизации и ответственности / С. И. Земцова // Криминалистика: вчера, сегодня, завтра. — 2020. — № 1(13). — С. 54–63. — DOI: 10.24411/2587-9820-2020-10007.

4. Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года: Указ Президента РФ от 23 ноября 2020 г. № 733 // Информационный портал «Гарант.ру». — URL: Garant.ru (дата обращения: 15.10.2022).

5. Новоселов Н. Г. Использование системы «Прозрачный блокчейн» в борьбе с незаконным оборотом наркотиков / Н. Г. Новоселов // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XXV Международной научно-практической конференции: Красноярск, 07–08 апреля 2022 года. — Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2022. — С. 267–269. — DOI: 10.51980/978-5-7889-0334-7_2022_5_2_267.

6. Грачев А. В. Организационно-экономические инструменты противодействия криминализации общества (на примере органов внутренних дел): дисс. … канд. экон. наук / А. В. Грачев. — СПб., 2007. — 206 с.

7. Соловьев В. И. О возможности осуществления контроля за оборотом цифровых финансовых активов / В. И. Соловьев, В. К. Конторович, В. Г. Феклин // Проблемы экономики и юридической практики. — 2022. — Т. 18. — № 5. — С. 242–247. — DOI: 10.33693/2541-8025-2022-18-5-242-247.

8. Крыгин С. В. Инструментарий деанонимизации криптовалют / С. В. Крыгин, С. И. Кувычков, С. Н. Сухов // Государство и право в изменяющемся мире: конвергенция частных и публичных интересов: материалы Всероссийской научно практической конференции, Нижний Новгород, 26 марта 2020 года. — Нижний Новгород: Автор, 2021. — С. 227–232.

9. History Has Its Eyes on Crypto. Let’s Prove It’s on the Right Side. — URL: www.blog.chainalysis.com/reports/sanctions-screening-tools/ (дата обращения: 15.09.2022).

10. URL: http://cbr.ru (дата обращения: 12.11.2022).

11. Коринной А. Г. Об отдельных элементах механизма регулирования оборота криптовалюты / А. Г. Коринной // Вестник экономической безопасности. — 2022. — № 1. — С. 271–276. — DOI: 10.24412/2414-3995-2022-1-271-276.

12. Концепция противодействия недобросовестным действиям на финансовом рынке // Официальный сайт ЦБ РФ. — URL: http://cbr.ru (дата обращения: 09.10.2022).

Дата поступления: 16.12.2022
Решение о публикации: 21.02.2023

Контактная информация:
КОРИННОЙ Александр Геннадьевич — адъюнкт; koorish@mail.ru

Special Instruments to Reveal and Resist Unfair Practices with Cryptocurrencies and Digital Financial Assets

A. G. Korinnoy

Saint Petersburg University of Russian Federation Internal Affairs Ministry, 1, Letchika Pilyutova str., Saint Petersburg, 198206, Russian Federation

For citation: Korinnoy A. G. Special Instruments to Reveal and Resist Unfair Practices with Cryptocurrencies and Digital Financial Assets. *Bulletin of scientific research results*, 2023, iss. 1, pp. 125–132. (In Russian) DOI: 10.20295/2223-9987-2023-1-125-132

Summary

Purpose: The article discusses conceptually new approaches to resist using cryptocurrencies and electronic payment means in unfair practices. As a result, it was found that all of them are aimed at revealing suspicious transactions and deanonymized individuals involved in illegal activities. The conclusion is substantiated that information and analytical systems constitute promising special tools for effective control of cryptocurrency market and blockchain networks. The research theoretical basis comprises scientific publications of the experts specialized in the issues of involvement, blockchain technology, distributed registries and cryptocurrencies at the investigation of crimes as well as foreign software tools, applied in the field of blockchain networks security. **Methods:** In the research, the author relies on deduction, generalization, synthesis and system analysis methods. **Results:** Determination of the capabilities of foreign and domestic software special tools in the field of virtual wallet providers and exchange operators (such as "crypto-currency brokers' board", etc.). **Practical significance:** The mechanism of functioning of special software tools for deanonymization of transactions in order to resist the use of cryptocurrencies and payment electronic means in unfair practices is presented.

Keywords: Digital financial assets, **c**ryptocurrency, electronic payment means, unfair practices, blockchain networks, deanonymization, special tools, informational and analytical systems, machine learning.

References

1. Sizov D. A. K voprosu organizatsii protivodeystviya nezakonnomu oborotu sinteticheskikh analogov kannabinoidov (po materialam UMVD Rossii po Kostromskoy oblasti) [On the issue of the organization of counteraction to the illicit trafficking of synthetic analogues of cannabinoids (based on the materials of the Ministry of Internal Affairs of Russia in the Kostroma region)]. *Trudy Akademii upravleniya MVD Rossii* [Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia]. 2015, Iss. 3(35), pp. 125–128. (In Russian)

2. Batoev V. B., Semenchuk V. V. Ispol'zovanie kriptovalyuty v prestupnoy deyatel'nosti: problemy protivodeystviya [The use of cryptocurrencies in criminal activity: problems of counteraction]. *Trudy Akademii upravleniya MVD Rossii* [Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia]. 2017, Iss. 2(42), pp. 9–15. (In Russian)

3. Zemtsova S. I. Kriptovalyuta v nezakonnom oborote narkoticheskikh sredstv: voprosy deanonimizatsii i otvetstvennosti [Cryptocurrency in illicit drug trafficking: issues of deanonymization and responsibility]. *Kriminalistika: vchera, segodnya, zavtra* [Criminalistics: yesterday, today, tomorrow]. 2020, Iss. 1(13), pp. 54–63. DOI: 10.24411/2587-9820-2020-10007. (In Russian)

4. Ob utverzhdenii Strategii gosudarstvennoy antinarkoticheskoy politiki Rossiyskoy Federatsii na period do 2030 goda: Ukaz Prezidenta RF ot 23 noyabrya 2020 g. № 733 [On approval of the Strategy

of the state anti-drug policy of the Russian Federation for the period up to 2030: Decree of the President of the Russian Federation of November 23, 2020 № 733]. *Informatsionnyy portal "Garant.ru"* [Information portal "Garant.ru"]. Available at: Garant.ru (accessed: October 15, 2022). (In Russian)

5. Novoselov N. G. *Ispol'zovanie sistemy "Prozrachnyy blokcheyn" v bor'be s nezakonnym oborotom narkotikov. Aktual'nye problemy bor'by s prestupnost'yu: voprosy teorii i praktiki : materialy XXV Mezhdunarodnoy nauchno-prakticheskoy konferentsii: Krasnoyarsk, 07–08 aprelya 2022 goda* [The use of the "Transparent blockchain" system in the fight against drug trafficking. Actual problems of combating crime: questions of theory and practice: Materials of the XXV scientific and practical International Conference. In 2 parts, Krasnoyarsk, 07–08 April 2022]. Krasnoyarsk: Sibirskiy yuridicheskiy institut Ministerstva vnutrennikh del Rossiyskoy Federatsii Publ., 2022, pp. 267–269. DOI: 10.51980/978-5-7889-0334-7_2022_5_2_267. (In Russian)

6. Grachev A. V. *Organizatsionno-ekonomicheskie instrumenty protivodeystviya kriminalizatsii obshchestva (na primere organov vnutrennikh del): diss. ... kand. ekon. nauk* [Organizational and economic tools to counter the criminalization of society (on the example of internal affairs bodies): diss. … cand. economy Sciences]. St. Petersburg, 2007, 206 p. (In Russian)

7. Solovyov V. I., Kontorovich V. K., Feklin V. G. O vozmozhnosti osushchestvleniya kontrolya za oborotom tsifrovykh finansovykh aktivov [On the possibility of controlling the turnover of digital financial assets]. *Problemy ekonomiki i yuridicheskoy praktiki* [Problems of Economics and legal practice]. 2022, vol. 18, Iss. 5, pp. 242–247. DOI: 10.33693/2541-8025-2022-18-5-242-247. (In Russian)

8. Krygin S. V., Sukhov S. N. *Instrumentariy deanonimizatsii kriptovalyut. Gosudarstvo i pravo v izmenyayushchemsya mire: konvergentsiya chastnykh i publichnykh interesov: materialy Vserossiyskoy nauchno prakticheskoy konferentsii, Nizhniy Novgorod, 26 marta 2020 goda* [Tools for deanonymization of cryptocurrencies. State and law in a changing world: convergence of private and public interests: Materials of the All-Russian Scientific and Practical Conference, Nizhny Novgorod, March 26, 2020]. Nizhny Novgorod: Avtor Publ., 2021, pp. 227–232. (In Russian)

9. History has set its eye on cryptography. Let's prove that it's on the right side. Available at: www.blog.chainalysis.com/reports/sanctions-screening-tools (accessed: September 15, 2022).

10. Available at: http://cbr.ru (accessed: November 12, 2022).

11. Korinnoy A. G. Ob otdel'nykh elementakh mekhanizma regulirovaniya oborota kriptovalyuty [On the individual elements of the mechanism for regulating the turnover of cryptocurrencies]. *Vestnik ekonomicheskoy bezopasnosti* [Bulletin of Economic Security]. 2022, Iss. 1, pp. 271–276. DOI: 10.24412/2414-3995-2022-1-271-276. (In Russian)

12. Kontseptsiya protivodeystviya nedobrosovestnym deystviyam na finansovom rynke [The concept of counteraction to unfair actions in the financial market]. Ofitsial'nyy sayt TsB RF [Official website of the Central Bank of the Russian Federation]. — URL: http://cbr.ru (accessed: October 09, 2022). (In Russian)

Received: December 16, 2022
Accepted: February 21, 2023

Author's information:
Alexandr G. KORINNOY — Postgraduate Student; koorish@mail.ru