УДК: 343.1, 343.9, 004.75
DOI: 10.24411/2312-3184-2019-00021

Судницын Алексей Борисович
начальник кафедры уголовного процесса Сибирского юридического института МВД России
кандидат юридических наук, доцент
E-mail: ab_sudnitsyn@mail.ru

Молоков Вячеслав Витальевич
начальник кафедры информационно-правовых дисциплин и специальной техники Сибирского юридического института МВД России
кандидат технических наук, доцент
E-mail: vvmolokov@mail.ru

Sudnitsyn Aleksey Borisovich
professor head of the Department of Criminal Procedure Siberian Law Institute of the MIA of the Russian Federation
candidate of juridical sciences, associate
E-mail: ab_sudnitsyn@mail.ru

Molokov Vyacheslav Vitalyevich
professor head of the Department of Information and Legal Disciplines and Special Equipment Siberian Law Institute of the MIA of the Russian Federation
candidate of technical sciences, associate
E-mail: vvmolokov@mail.ru

ОТДЕЛЬНЫЕ ВОЗМОЖНОСТИ ПОЛУЧЕНИЯ И ИСПОЛЬЗОВАНИЯ СВЕДЕНИЙ ОБ ОПЕРАЦИЯХ С КРИПТОВАЛЮТОЙ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Введение: широкое использование расчетов криптовалютой со стороны лиц, причастных к совершению преступлений, в том числе в сфере незаконного оборота наркотических средств и психотропных веществ, потребовало проработки потенциальных возможностей использования сведений о таковых финансовых операциях в раскрытии и расследовании преступлений.

Материалы и методы: были изучены отдельные положения криминалистики, специальной техники, уголовного процесса, оперативно-розыскной деятельности, примеры правоохранительной деятельности, использован комплекс общих и частных научных методов исследования в целях определения возможностей получения сведений о расчетах криптовалютой и их использования в раскрытии и расследовании преступлений.

Результаты исследования: авторы пришли к выводу, что в целях раскрытия и расследования преступлений могут быть использованы предложенные потенциальные возможности выявления уязвимостей и деанонимизации владельцев электронных кошельков, используемых при операциях с криптовалютой.

Выводы и заключения: по результатам исследования предложены направления использования информации, связанной с проведением расчетов криптовалютой, в целях раскрытия и расследования преступлений: автоматизи-

рованный анализ транзакционной сети, получение значимой информации из открытых источников путем эффективного поиска и применения инструментов интернет-разведки, использование компьютерно-технических экспертиз устройств, применявшихся для операций с криптовалютами, деанонимизация владельца криптокошелька посредством сотрудничества с криптовалютными биржами и обменниками.

Ключевые слова: Интернет, криптовалюта, технология блокчейн, раскрытие и расследование преступлений.

SOME OPPORTUNITIES FOR OBTAINING AND USING DATA ON CRYPTO-CURRENCY OPERATIONS DURING DISCLOSURE AND INVESTIGATION OF CRIMES

Introduction: widespread use of cryptocurrency calculations by persons involved in the commission of crimes, including in the sphere of illicit trafficking in narcotic drugs and psychotropic substances, requires the development of potential possibilities of using data on financial transactions in detection and investigation of crimes.

Materials and methods: certain provisions of criminalistics, special equipment, criminal procedure, operational-search activity, examples of law enforcement activities have been studied, a set of general and private scientific research methods were used to determine the possibilities of obtaining information on cryptocurrency calculations and their use in the detection and investigation of crimes .

Results: the authors concluded that in order to detect and investigate crimes, the proposed potential for identifying vulnerabilities and deanonymizing the owners of e-wallets used in operations with cryptocurrency can be developed.

Summary and conclusions: the directions of using information related to the execution of cryptocurrency calculations for the purpose of disclosing and investigating crimes have been proposed. Among them, automated analysis of the transactional network, obtaining relevant information from open sources through effective search and use of Internet intelligence tools, use of computer-technical expertise of devices used for operations with cryptocurrencies, deanonymization of the owner of the cryptocell through cooperation with cryptocurrency exchanges and exchangers.

Key words: Internet, cryptocurrency, blockchain technology, disclosure and investigation of crimes.

К настоящему времени лица, совершающие преступления, не только широко используют технические средства, компьютерные технологии, информационно-телекоммуникационную сеть Интернет, но и осуществляют специфические формы расчетов криптовалютой. Следует отметить, что использование криптовалют в мире набирает большую популярность и немалую долю в спросе на них породил растущий в 2017–2018 гг. курс криптовалюты Bitcoin. По данным ана-

литического сервиса Coinmarketcap[1] в десятку наиболее востребованных криптовалют с высоким курсом и уровнем капитализации входят: Bitcoin, Ethereum, Monero, Litecoin, NEM, XRP и др. Основная тенденция растущей популярности использования криптовалют для осуществления криминальных финансовых операций кроется в принципах их функционирования. В основе организации любой криптовалюты находится технология блокчейн (непрерывная последовательная цепочка блоков). Построенная на принципах децентрализации и приватности архитектура блокчейн обеспечивает высокую степень надежности, анонимности и скорости проведения операций. Таким образом, анонимность расчетов в криптовалютах, низкая проработанность возможностей использования в раскрытии и расследовании преступлений сведений об операциях с ними, потребность правоприменителей в соответствующих рекомендациях указывают на острую теоретическую и практическую актуальность обозначенных аспектов.

Несмотря на появление в сравнительно недавнее время отдельных исследований, касающихся вопросов криптовалюты, встречающиеся работы рассматривают ее как новое социально-экономическое явление, объект возможного правового контроля. Авторы определяют природу криптовалюты, вычленяют характерные ее признаки, в том числе широкую возможность использования при совершении преступлений, прорабатывают проблемы контроля за оборотом криптовалюты, обозначают основные направления совершенствования правоохранительной деятельности в соответствующей части (В.Б. Батоев и В.В. Семенчук [1, с. 9–15], А.Г. Волеводз [2, с. 66–75], Э.С. Маркарян [3, с. 176–187], А.Л. Пермяков [4, с. 129–135] и др.). Вместе с тем комплексных уголовно-процессуальных и технико-криминалистических исследований, посвященных вопросам получения данных о расчетах криптовалютой и их использования в раскрытии и расследовании преступлений, в современной литературе немного. Сложившееся положение требует обращения к соответствующей тематике.

Методологическую основу исследования составил комплекс общих и частных научных методов исследования (формально-логический, сравнительно-правовой, логико-юридический, интервьюирование и др.), позволивших на базе имеющейся правовой основы и практики правоохранительной деятельности, в том числе международной, выработать предложения по получению сведений о расчетах электронной наличностью и их использованию в раскрытии и расследовании преступлений.

Рассмотрим отдельные этапы операций с криптовалютами с позиций выявления уязвимостей и возможности деанонимизации владельцев электронных кошельков в интересах раскрытия и расследования преступлений. В качестве примера будем использовать наиболее популярную криптовалюту биткойн с объемом рыночной капитализации более семи триллионов долларов.

Основное преимущество организации операций с криптовалютами кроется в механизме децентрализации вычислений. Информация о транзакциях передаётся случайно выбранными узлами P2P (peer-to-peer сети с одноранговой децентрализо-

[1] URL: https://coinmarketcap.com (дата обращения 24.09.2018).

ванной структурой) сети. Несмотря на то, что биткойн-узлы соединяются друг с другом в сети Интернет посредством IP-адресов, однозначно установить, была ли полученная транзакция создана передавшим информацию узлом или он являлся всего лишь ретранслятором на настоящий момент не представляется возможным. Вместе с тем предполагается использование особенностей такой архитектуры вычислений по следующим ключевым уязвимостям:

1. Наличие технического контроля за несколькими узлами сети биткойн предоставляет возможность получения достаточных для выявления источника конкретной транзакции сведений.

2. Важнейшая особенность биткойн – все транзакции абсолютно прозрачны и доступны – дает возможность реализации алгоритмов глубокого анализа данных.

Ввиду открытости информации о транзакциях в сети биткойн были предложены алгоритмы группировки и привязывания к конкретным кошелькам операций с входными и выходными узлами. В частности, в сети Интернет опубликован алгоритм, основанный на процессе кластеризации, который анализирует данные базы блокчейна и объединяет несколько адресов криптовалютных кошельков, связанных с одним пользователем, в единый кластер [5]. По сути задача кластерного анализа транзакционных сетей сводится к нахождению нескольких входов, объединенных в одну транзакцию, что позволяет сделать вывод о едином источнике контроля. На этой основе в интересах правоохранительных органов и финансовых организаций компания Bitfury Group представила общественности новый инструмент для исследований биткоин-блокчейна – Crystal. Данный инструмент способен работать с информацией о потоках и транзакций в сети блокчейн, выявляя подозрительные операции и связывая их с объектами. Тем самым он способен деанонимизировать отдельные объекты и финансовые взаимоотношения между криминальными личностями[1].

Также можно отметить, что биткойн-адрес можно попытаться связать с конкретными людьми, если их личная информация была каким-либо образом отождествлена с ним. Например, если использовался биткойн-адрес для депозитного счета, снятия денег с регулируемой биржи (кошелька) или с помощью биткойн осуществлялся расчёт в интернет-магазине и т.п., то в открытом доступе находится адрес для перечислений монет. В этом случае глобальный поиск по всем информационным ресурсам (социальные сети, блоги, сайты даркнета и т.п.) с ключевым признаком номера кошелька может позволить выявить определенное лицо.

Перечисленные выше методы получения значимой для раскрытия и расследования преступлений информации отражают возможности, находящиеся «на верхнем уровне абстракции». Но у операций с криптовалютами существуют и элементы, которые могут быть выявлены на стадии конвертации. В качестве та-

[1] Bitfury выпустила Crystal – блокчейн-инструмент для финансовых расследований. URL: http://cryptowiki.ru/news/bitfury-vypystila-crystal-blokchein-instryment-dlia-finansovyh-rassledovanii.html (дата обращения 26.09.2018).

ковых могут выступить данные об отдельных этапах перемещения криптовалюты (приобретение, продажа в различных формах).

Как правило, процесс приобретения или обмена криптовалют осуществляется на виртуальных торговых площадках – криптобиржах. Сотрудничество с организаторами криптобирж в рамках раскрытия и расследования преступлений может способствовать выдаче правоохранительным органам информации о банковских счетах обмена криптовалют, IP-адресах пользователей в сети Интернет и иную персональную информацию. Предпринимаются попытки, направленные на обеспечение получения требуемой информации, в том числе деанонимизации расчетов криптовалютой. Например, Европейский парламент утвердил пакет новых мер по борьбе с отмыванием средств в странах Евросоюза, в числе которых он усилил контроль над биткойном и другими виртуальными валютами. После указанных мер платформы обмена, виртуальные кошельки и банковские учреждения обязаны осуществлять контроль клиентов, включая требования к проверке информации о них, что способствует предотвращению анонимности криптовалют[1].

Важную для расследования информацию можно получить на компьютерных устройствах, используемых при осуществлении операций с криптовалютами. Обоснованный вывод о предполагаемом месте нахождения такой компьютерной техники позволит принять решение о проведении обыска (выемки), по результату которого обнаружить и изъять соответствующие технические устройства и информационные носители.

Обратим внимание, что для покупки, обмена, продажи криптовалюты требуется наличие электронного кошелька (Wallet), управление которым происходит с помощью программы, клиента сети биткойн. Факт использования этого, а также и иного программного обеспечения, связанного с криптовалютой (при наличии в нашем распоряжении изъятой компьютерной техники: компьютер, ноутбук, смартфон, планшет и пр.), может быть обнаружен путем производства осмотра предметов, а также в последующем при исследовании компьютерной информации. В связи с этим рекомендуется фиксировать посещенные пользователем веб-сайты и установленное программное обеспечение, имеющее отношение к операциям с криптовалютами, в том числе программы анонимизации (например, браузер Tor), причем не только путем указания в протоколе, но и с помощью скриншотов с экрана устройства.

Сведения, полученные в ходе осмотра, могут быть подтверждены в результате исследования компьютерной информации, содержащейся на изъятых технических устройствах. Характерным для сети Биткойн считается наличие на информационном носителе файла wallet.dat. Операции с таким файлом могут способствовать получению информации о балансе найденного кошелька с использованием другого устройства. Ввиду применения программой кошелька криптоалгоритмов и подтверждения транзакций пользователя секретным клю-

[1] Евросоюз вводит верификацию владельцев криптовалют для деанонимизации транзакций. URL: https://forklog.com/evrosoyuz-vvodit-verifikatsiyu-vladeltsev-kriptovalyut-dlya-deanonimizatsii-tranzaktsij (дата обращения 25.09.2018).

чом его наличие также является неотъемлемым. Криптоключ может находиться в зашифрованном контейнере, на аппаратном кошельке либо напечатан на бумажном носителе. Напомним, что утеря секретного ключа приведет к безвозвратной утрате монет в кошельке биткойн, а в этом вряд ли заинтересован сам владелец. Кроме того, путем производства экспертизы могут быть обнаружены дополнительные данные, а также сделаны выводы, подтверждающие операции с криптовалютой.

По результатам проведенных мероприятий в группе следственных действий – обыск-осмотр-экспертиза – должна четко прослеживаться связь сведений, подтверждающих операции с криптовалютой. Аналогичное содержание должно быть прослеживаемо и в допросах лиц.

Круг вопросов, выясняемых в ходе допросов лиц, причастных к операциям с криптовалютой, определяется конкретной следственной ситуацией, сложившейся к этому моменту расследования. Обобщение результатов следственной и судебной практики демонстрирует, что в показаниях указанных лиц внимание акцентируется на деталях финансовых операций, связанных с переводом денежных средств в криптовалюту, а затем обратно. На эти же особенности обращается особое внимание и в других доказательствах.

Обозначенные способы использования сведений об операциях с криптовалютой в доказывании по уголовным делам являются типичными. Их применение может иметь место как при расследовании преступлений в сфере незаконного оборота наркотических средств и психотропных веществ, так и преступлений из иных сфер.

Другие формы установления сведений об операциях с криптовалютой и их дальнейшее использование в доказывании гипотетически возможно. Однако данная возможность в большинстве случаев упирается в непреодолимую на настоящий момент технологию шифрования данных как заложенную в суть криптовалюты, так и применяемую при обеспечении анонимного нахождения абонента в сети Интернет. Так, лицам, преследующих цель обеспечить анонимность своих транзакций с криптовалютой, в качестве рекомендации, исходящей от соответствующих заинтересованных лиц, для достижения той же цели предлагается использовать биткойн-миксер. Как привило, это сайт, принимающий биткойны множества лиц, использующий алгоритмы для их смешивания и отправки по разным кошелькам. Такой миксер не позволяет связать транзакции с определенным лицом. Высокую степень анонимности предоставляет сеть Tor, что также способствует скрытию IP-адреса абонента и его трафика в сети Интернет. Вместе с тем представляются перспективными ряд возможностей использования сведений об операциях с криптовалютой в раскрытии и расследовании преступлений.

Одной из главенствующих задач в рассматриваемых случаях является выявление лица, его идентификация в информационной среде сети Интернет (интернет-биржи, форумы, сайты и др.). В качестве средств достижения данной задачи могут выступить нижеприведенные предложения и примеры.

Автороведческий анализ (исследование, экспертиза) позволит установить автора текста, размещенного в информационной среде. При этом в силу огромного массива информации, хранящейся во всемирной паутине, следует уделять первоочередное внимание автоматизации процесса распознания авторства текста. Подобные разработки уже имеются[1] [6].

Кроме того, не следует забывать о современных возможностях технико-оперативно-аналитической работы. Так, примером подобной работы можно назвать установление, последующее задержание и осуждение Росса Уильяма Ульбрихта (Ross William Ulbricht) – владельца анонимной торговой площадки (подпольной биржи) Silk Road, указавшего свой адрес электронной почты, позволившей выявить совпадения в его онлайн-деятельности [7].

Другой успешный пример: сотрудники управления по контролю за распространением наркотиков США (далее – DEA) выдали себя за продавца наркотических средств, получили в качестве оплаты биткойны, изобличили Эрика Дэниеля Хьюза (Eric Daniel Hughes). Указанному лицу вменили незаконную трату собственности, покупку незаконных веществ. Указанная операция была осуществлена на подпольной бирже Silk Road, как предполагается, путем создания сотрудниками DEA подставного аккаунта [8].

Подобные методы работы могут быть «взяты на вооружение», благодаря чему возможно установление и последующее привлечение к ответственности лиц, совершающих преступления и использующих при этом расчеты посредством криптовалюты. Безусловно, при подобных операциях в действиях сотрудников правоохранительных органов не должно содержаться признаков провокации или иных преступлений.

На основании проведенного исследования предлагаются следующие выводы, позволяющие формализовать методы и средства получения информации, представляющей ценность для раскрытия и расследования преступлений, связанных с использованием операций с криптовалютами:

1. Технология блокчейн обеспечивает анонимность владельца адреса кошелька криптовалюты, но не исключает автоматизированный анализ всей транзакционной сети.

2. Методы эффективного поиска и инструменты интернет-разведки дают возможность получения значимой информации из открытых источников.

3. Компьютерно-техническая экспертиза устройств, используемых для операций с криптовалютами, позволяет решить ряд задач по обеспечению доказательной базы.

4. Сотрудничество с криптовалютными биржами и обменниками в рамках расследования по уголовным делам может решить задачу деанонимизации владельца криптокошелька.

Приведенные выводы подтверждают, что даже при наличии препятствий технического характера (некоторые из них непреодолимы на настоящий мо-

[1] Деанонимизация во всемирной сети – все ближе и ближе. URL: https://habrahabr.ru/post/165435 (дата обращения 15.09.2018).

мент), сведения об операциях с криптовалютой могут быть получены при раскрытии преступлений разнообразными способами (в том числе «в обход» технических проблем).

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

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

2. Волеводз А. Международное сотрудничество в сфере уголовного судопроизводства по делам о преступлениях, совершенных с использованием криптовалюты: постановка проблемы // Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования: сб. материалов междунар. науч.-практич. конф. / редкол.: А.В. Гришин [и др.]. – Орел: ОрЮИ МВД России им. В.В. Лукьянова, 2018. – С. 66–75.

3. Маркарян Э.С. Особенности получения данных о механизме следообразования при расследовании преступлений, совершенных с использованием криптовалют // Библиотека криминалиста. Научный журнал. – 2017. – № 4 (33). – С. 176–187.

4. Пермяков А.Л. Криптовалюта в механизме преступления: предмет, средство или способ? // Вестник Восточно-Сибирского института Министерства внутренних дел России. – 2018. – № 2 (85). – С. 129–135.

5. Dmitry Ermilov, Maxim Panov, Yury Yanovich Automatic Bitcoin Address Clustering. URL: https://bitfury.com/content/downloads/ clustering_whitepaper.pdf (дата обращения 25.09.2018).

6. Nicole Perlroth Software Helps Identify Anonymous Writers or Helps Them Stay That Way // The New York Times. URL: https://bits.blogs.nytimes.com/ 2012/01/03/software-helps-identify-anonymous-writers-or-helps-them-stay-that-way (дата обращения 10.09.2018).

7. Danny Bradbury Silk Road fell due to a catalogue of errors by owner Ross Ulbricht // CoinDesk, Inc URL: https://www.coindesk.com/ross-ulbrichts-silk-road-head-smacking-rookie-errors (дата обращения 20.09.2018).

8. Brian Cohen, Adam B. Levine Users Bitcoins Seized by DEA // The LTB Network: URL: https://letstalkbitcoin.com/post/53700133097/users-bitcoins-seized-by-dea (дата обращения 15.09.2018).

BIBLIOGRAPHIC REFERENCE

1. Batoev V.B., Semenchuk V.V. The use of cryptocurrency in criminal activity: countermeasures // Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. – 2017. – No. 2 (42). – pp.9–15.

2. Volevodz A. International cooperation in the field of criminal proceedings in cases of crimes committed using cryptocurrency: problem statement // Collection of materials of the international scientific-practical conference "Modern criminal procedure law - the lessons of history and the problems of further reform", October 18–19, 2018 / editorial board: A.V. Grishin [and others]; Orel Law Institute of the Ministry of

Internal Affairs of Russia named after V.V. Lukyanov. – Orel : OrLI of the Ministry of Internal Affairs of Russia. – 2018. – 430 p.

3. Markaryan E.S. Features of obtaining data on the mechanism of tracing in the investigation of crimes committed using cryptocurrencies // Library of the criminologist. Science journal. – 2017. – No. 4 (33). – pp. 176–187.

4. Permyakov A.L. Cryptocurrency in the mechanism of crime: the subject, means or method? // Bulletin of the East-Siberian Institute of the Ministry of Internal Affairs of Russia. – 2018. – No. – 2 (85). – pp. 129–135.

5. Dmitry Ermilov, Maxim Panov, Yury Yanovich Automatic bitcoin address clustering // bitfury.com. URL: https://bitfury.com/content/downloads/clustering_whitepaper.pdf (accessed: 25.09.2018).

6. Nicole Perlroth Software helps identify anonymous writers or helps them stay that way// The New York Times URL: https://bits.blogs.nytimes.com/2012/01/03/software-helps-identify-anonymous-writers-or-helps-them-stay-that-way (accessed 10.09.2018).

7. Danny Bradbury Silk road fell due to a catalogue of errors by owner Ross Ulbricht // CoinDesk, Inc URL: https://www.coindesk.com/ross-ulbrichts-silk-road-head-smacking-rookie-errors (accessed 20.09.2018).

8. Brian Cohen, Adam B. Levine Users bitcoins seized by DEA // The LTB Network URL: https://letstalkbitcoin.com/post/53700133097/users-bitcoins-seized-by-dea (accessed 15.09.2018).