Научная статья
УДК 343.98
DOI 10.33184/vest-law-bsu-2024.24.15

Гайсин Нурсултан Ильгизович
Уфимский университет науки и технологий, АО «ПОЛИЭФ», Уфа, Россия,
nursultan9703@mail.ru

К ВОПРОСУ О НЕОБХОДИМОСТИ КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ РАССЛЕДОВАНИЯ ХИЩЕНИЙ КРИПТОВАЛЮТНЫХ АКТИВОВ

Аннотация. В настоящее время широко распространено хищение криптовалютных активов. Однако достаточными знаниями для проведения эффективного предварительного расследования таких хищений обладает очень узкий круг сотрудников правоохранительных органов. В статье рассмотрено значение знаний о технологии блокчейн, о некоторых инструментах, благодаря которым развивается и распространяется криптовалютная сфера, для предварительного расследования хищений криптовалютных активов.

Ключевые слова: блокчейн, криптовалюта, смарт-контракт, децентрализованное приложение, мнемоническая фраза, публичный ключ, приватный ключ, токен, хищение

Для цитирования: Гайсин Н.И. К вопросу о необходимости криминалистического обеспечения расследования хищений криптовалютных активов / Н.И. Гайсин. – DOI 10.33184/vest-law-bsu-2024.24.15 // Вестник Института права Башкирского государственного университета. – 2024. – № 4. – С. 154–160.

Original article

Gaisin Nursultan Ilgizovich
Ufa University of Science and Technologies, JSC “POLIEF”, Ufa, Russia,
nursultan9703@mail.ru

THE NEED FOR FORENSIC SUPPORT IN INVESTIGATING CRYPTOCURRENCY ASSET THEFT

Abstract. The theft of cryptocurrency assets is now widespread. However, a very narrow range of law enforcement officers have sufficient knowledge to con-

duct an effective preliminary investigation of such thefts. The article considers the importance of knowledge about blockchain technology, about some of the tools with the help of that the cryptocurrency sphere develops and spreads, for the preliminary investigation of theft of cryptocurrency assets.

Keywords: blockchain, cryptocurrency, smart contract, decentralised application, mnemonic phrase, public key, private key, token, theft

For citation: Gaisin N.I. The Need for Forensic Support in Investigating Cryptocurrency Asset Theft. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta = Bulletin of the Institute of Law of the Bashkir State University,* 2024, no. 4, pp. 154–160. (In Russian). DOI 10.33184/vest-law-bsu-2024.24.15.

Мы живем в эпоху зарождения, развития, широкого распространения и признания криптовалюты в качестве средства платежа, сбережения и инструмента для инвестирования. Например, ряд государств осуществляют либо собираются осуществлять международные расчеты посредством криптовалюты.

Данная сфера является новой и по этой причине на законодательном уровне должным образом не урегулирована. Кроме того, криптовалюта обладает рядом свойств, которых нет у безналичных денежных средств:

1) расчеты осуществляются без посредничества и контроля третьих лиц;

2) пользователи могут не раскрывать свою личность (имеется возможность владения, распоряжения и пользования без идентификации личности);

3) пользователи могут свободно перевозить криптовалюту в любую точку мира, в том числе без использования материальных носителей, обменивать ее на национальную валюту любого государства при наличии лиц, желающих произвести такой обмен.

Все указанное создает благоприятные предпосылки для хищения криптовалютных активов.

Некоторые способы хищений мало чем отличаются от старых и современных способов хищения безналичных денежных средств, а некоторые целенаправленно разработаны для хищения криптовалютных активов.

Поскольку способы хищения криптовалютных активов имеют свою специфику, а некоторые из них обладают новизной, современная наука криминалистика не оснащена достаточными знаниями о том, какие способы хищения криптовалютных активов существуют, об организационных особенностях первоначального этапа расследования, типичных следственных версиях и ситуациях, действиях, которые необходимо предпринять на том или ином этапе расследования, а также о том, как произвести эти действия наиболее эффективно. Для того чтобы начать формирование этих знаний, необходимо иметь представление о технологии, благодаря которой стало возможным появление

криптовалюты, а также об инструментах, благодаря которым происходит ее распространение и развитие: блокчейн, смарт-контракты, децентрализованные приложения и токены.

Основополагающей технологией, лежащей в основе криптовалюты, является блокчейн. Большинство ее сторонников полагают, что классический блокчейн представляет собой одноранговую (децентрализованную, основанную на равноправии участников) сеть с управляемым доступом для осуществления безопасной записи информации в распределенный реестр, нефиксированное множество копий которой может прийти к окончательно консистентному (согласованному, непротиворечивому) состоянию, используя заданный алгоритм консенсуса [1].

А.И. Савельев полагает, что блокчейн представляет собой «децентрализованную распределенную базу данных ... обо всех подтвержденных трансакциях, совершенных в отношении определенного актива, в основе функционирования которой лежат криптографические алгоритмы» [2, с. 96].

Е.В. Былинкина опираясь на дефиницию, данную в стандарте ISO 22739:2020 «Технологии блокчейн и распределенного реестра. Словарь», где блокчейн определяется в качестве распределенного реестра с подтвержденными блоками, организованными в последовательную цепочку только для добавления с использованием криптографических ссылок, предложила собственное определение: «Блокчейн есть разновидность распределенного реестра, предназначенного только для добавления информации, данные в который записываются блоками с использованием криптографических алгоритмов таким образом, что каждый новый блок включает информацию о предыдущем блоке. Безопасность данных в блокчейне обеспечивается за счет децентрализованного хранения информации и применения криптографических алгоритмов» [3, с. 146].

В.А. Вайпан обозначает блокчейн в качестве «сквозной цифровой технологии, явления экономической жизни», требующего нового нормативно-правового регулирования [4, с. 7].

На наш взгляд, блокчейн можно определить как распределенный реестр или базу данных, в которой хранится постоянно актуализирующаяся информация о переводах криптовалюты между пользователями без посредников и контроля третьих лиц.

Блокчейн имеет два основных свойства:

1) история трансакций на блокчейне сохраняется навсегда и доступна всем пользователям;

2) кошельки на блокчейне не привязаны к личности (доступ обеспечивается с помощью мнемонической фразы или приватного ключа).

Благодаря первому свойству можно отследить любые трансакции в блокчейн-обозревателе, который представляет собой сайт в сети Интернет. Данная возможность крайне важна для предварительного расследования, поскольку благодаря ее использованию можно получить информацию о совершенных трансакциях.

Говоря о ключевых элементах при работе с криптовалютой, важно знать, что такое публичный ключ. Он представляет собой набор латинских букв и цифр. Если привести аналогию, то это то же самое, что номер расчетного счета. Указав в блокчейн-обозревателе публичный ключ, можно отследить все трансакции, которые когда-либо совершал пользователь. Узнать публичный ключ можно в ходе допроса (получения объяснения), а также в ходе осмотра устройства, на котором установлен криптовалютный кошелек с искомым публичным ключом.

Второе свойство может показаться неблагоприятным для расследования. Однако следует иметь в виду, что криптовалюта представляет собой ценность, которую можно приобрести в обмен на национальную валюту, и наоборот – криптовалюта может быть обменена на национальную валюту. Наиболее часто встречающийся способ обмена подразумевает банковский перевод безналичных денежных средств на банковские счета лиц, которые осуществляют деятельность по обмену криптовалюты на национальную валюту и наоборот. То есть, проведя ряд оперативно-разыскных мероприятий и следственных действий, можно установить личности тех, с чьих банковских счетов произведен перевод денежных средств и на чьи счета поступили денежные средства в обмен на криптовалюту.

Возвращаясь к ключевым элементам при работе с криптовалютой, важно также знать о том, что такое мнемоническая фраза и приватный ключ. Первое представляет собой набор слов в определенной последовательности, а второе – набор латинских букв и цифр. Имея что-то одно, злоумышленник может получить доступ к чужой криптовалюте и распорядиться ею по собственному усмотрению. С точки зрения проверки сообщения о преступлении и предварительного расследования эти знания важны, так как позволяют наиболее эффективно провести допрос потерпевшего либо получить объяснение. По результатам указанных процессуальных действий следователь (дознаватель) будет иметь понимание о том, совершено ли хищение, а также о способе его совершения.

Криптовалюта не является чем-то вещественным. Это лишь цифровая запись в распределенном реестре. То есть криптовалюта – метод учета балансов внутри блокчейна. Вне блокчейна она существовать не может.

Необходимо отличать основную криптовалюту от токена. Токен тоже криптовалюта, которая создается «поверх» существующего блокчейна и мо-

жет иметь определенный функционал. Токен может создать любое лицо. Этот процесс намного проще, чем создание основной криптовалюты, поскольку в данном случае не нужно разрабатывать блокчейн. С токенами тоже можно совершать трансакции по блокчейну (при уплате комиссии в основной криптовалюте).

Поскольку создание токена намного проще, чем создание основной криптовалюты, существует множество токенов, созданных с целью хищений, под видом того, что они имеют какой-то полезный функционал или потенциал роста в цене.

Токены могут быть созданы только на тех блокчейнах, которые имеют поддержку смарт-контрактов. Смарт-контракт можно определить как программный код, изготовленный на блокчейне и выполняющий набор команд по заданным условиям.

Существует мнение, что смарт-контракт является договором в электронной форме, исполнение прав и обязательств по которому осуществляется путем совершения в автоматическом порядке цифровых трансакций в распределенном реестре в строго определенной реестром последовательности и при наступлении определенных им обстоятельств [5, с. 100–101].

Также существует мнение, что смарт-контракт – это компьютерная программа (или компьютерный код), которая может быть использована только совместно с технологией блокчейн и позволяет автоматически заключать, исполнять и прекращать различные договоры в момент наступления заранее установленных юридических фактов [6]. Это определение является более точным.

Самый первый блокчейн – биткойн – не поддерживает функцию смарт-контрактов. Однако существует ряд более новых блокчейнов, которые имеют поддержку смарт-контрактов и на которых возможно создание токенов лицами, имеющими соответствующие навыки. Например, это блокчейны Ethereum, Binance Smart Chain, Tron, Cosmos, Solana и др.

Поскольку смарт-контракт является программным кодом, он позволяет создавать не только токены на блокчейнах, но и различные приложения, которые принято называть децентрализованными приложениями. Злоумышленники тоже активно пользуются данными возможностями и анонимно создают децентрализованные приложения, с помощью которых совершаются хищения криптовалютных активов. Технически это происходит следующим образом: введенный в заблуждение пользователь подключает свой криптовалютный кошелек к децентрализованному приложению и подтверждает какое-либо действие (то есть запускает в работу смарт-контракт), на первый взгляд не являющееся подозрительным, но на самом деле направленное на получение согласия на распоряжение криптовалютой или перевод криптовалюты на кошелек злоумышленника.

Знания о том, что такое смарт-контракт и децентрализованное приложение, необходимы для проверки сообщения о преступлении и предварительного расследования. Они позволят осуществлять процессуальные действия наиболее эффективно. Знающий следователь (дознаватель) сможет определить в ходе допроса и (или) осмотра, при помощи какого децентрализованного приложения произошло хищение криптовалюты, принадлежащей потерпевшему. Полученная информация может послужить отправной точкой, стартовав с которой, можно успешно провести предварительное расследование.

Подводя итог, следует отметить, что в настоящее время имеется острая необходимость в активном обеспечении следователей (дознавателей) знаниями о способах совершения преступлений в рассмотренной сфере, а также в разработке тактики производства отдельных следственных действий и методики расследования хищений криптовалюты. Однако для начала необходимо уяснить как в теории, так и на практике, на чем базируется рассмотренная в данной работе сфера, из каких элементов состоит и какие инструменты в ней используются.

Список источников

1. Родикова В.А. Блокчейн-технологии и персональные данные граждан: перспективы правового регулирования / В.А. Родикова // Российская юстиция. – 2023. – № 5. – С. 72–80.

2. Савельев А.И. Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву / А.И. Савельев // Закон. – 2017. – № 5. – С. 94–117.

3. Былинкина Е.В. Блокчейн: правовое регулирование и стандартизация / Е.В. Былинкина // Право и политика. – 2020. – № 9. – С. 143–155.

4. Вайпан В.А. Основы правового регулирования цифровой экономики / В.А. Вайпан // Право и экономика. – 2017. – № 11. – С. 5–18.

5. Зенин С.С. Правотворчество в условиях алгоритмизации права / С.С. Зенин, Д.Л. Кутейников, О.А. Ижаев, И.М. Япрынцев // Lex Russica. – 2020. – № 7 (164). – С. 97–104.

6. Ефимова Л.Г. Правовая природа смарт-контракта / Л.Г. Ефимова, О.Б. Сиземова // Банковское право. – 2019. – № 1. – С. 23–30.

References

1. Rodikova V.A. Blockchain Technologies and Personal Data of Citizens: Prospects for Legal Regulation. *Rossijskaya yusticiya = Russian Justice,* 2023, no. 5, pp. 72–80. (In Russian).

2. Saveliev A.I. Some Legal Aspects of the Use of Smart Contracts and Blockchain Technologies under Russian Law. *Zakon = Law,* 2017, no. 5, pp. 94–117. (In Russian).

3. Bylinkina E.V. Blockchain: Legal Regulation and Standardisation. *Pravo i politika = Law and Politics,* 2020, no. 9, pp. 143–155. (In Russian).

4. Vaypan V.A. Fundamentals of Legal Regulation of the Digital Economy. *Pravo i ekonomika = Law and Economics,* 2017, no. 11, pp. 5–18. (In Russian).

5. Zenin S.S., Kuteinikov D.L., Izhaev O.A., Yapryntsev I.M. Lawmaking in the Context of Algorithmization of Law. *Lex Russica,* 2020, no. 7 (164), pp. 97–104. (In Russian).

6. Efimova L.G., Sizemova O.B. Legal Nature of a Smart Contract. *Bankovskoe pravo = Banking Law,* 2019, no. 1, pp. 23–30. (In Russian).

Информация об авторе

Гайсин Нурсултан Ильгизович *– аспирант кафедры криминалистики Института права; юрист АО «ПОЛИЭФ»*

Information about the Author

Gaisin Nursultan Ilgizovich *– Postgraduate Student of the Chair of Criminalistics, Institute of Law, Lawyer of JSC «POLIEF»*

Статья поступила в редакцию 18.09.2024; одобрена после рецензирования 25.10.2024; принята к публикации 25.10.2024.
The article was submitted 18.09.2024; approved after reviewing 25.10.2024; accepted for publication 25.10.2024.