[1]Е. Флоря, [2]Л. Шаргу

[1]Комратский государственный университет, Республика Молдова, г. Комрат, email: florya@yahoo.com

[2]Европейский Университет Молдовы, Республика Молдова, г. Кишинёв

КРИПТОМОНЕТЫ ZCASH И DASH КАК КРИМИНОГЕННЫЙ ФАКТОР

Ключевые слова: Zcash, Dash, криптовалюта, анонимность, блокчейн, Биткоин, даркнет, миксер, майнинг, мастерноды.

В статье рассматриваются криптомонеты с повышенной анонимностью Zcash и Dash с точки зрения тех криминальных рисков, которые влекут за собой данные цифровые активы. Автор отмечает, что оба проекта заметно уступают криптоактиву Monero как по популярности, так и по технической разработанности. В то же время стабильный спрос на монеты с повышенной анонимностью будет толкать создателей Zcash и Dash к усовершенствованию своих разработок, что, в свою очередь, закономерно вызовет ответную реакцию со стороны регуляторов, которые либо сумеют обеспечить прозрачность осуществляемых транзакций, либо выведут их за правовое поле. Очевидно, что представители криминалитета также крайне заинтересованы в анонимности осуществляемых транзакций и внимательно отслеживают все технологические новшества в данной сфере. Задачей органов, призванных бороться с преступностью, в этой связи является максимально оперативное реагирование на возникновение новых криминальных угроз в этой сфере и своевременная разработка мер, направленных на их предупреждение и предотвращение.

[1]E. Florya, [2]L. Shargu

[1]Comrat State University, Republic of Moldova, Comrat, email: florya@yahoo.com

[2]University of European Studies of Moldova, Republic of Moldova, Chisinau

ZCASH AND DASH CRYPTOMONETS AS A CRIMINOGENIC FACTOR

Keywords: Zcash, Dash, cryptocurrency, anonymity, blockchain, Bitcoin, darknet, mixer, mining, masternodes.

The article studies Zcash and Dash, crypto coins with enhanced anonymity, from the point of view of the criminal risks that these digital assets entail. The author notes that both projects are noticeably weaker than Monero crypto asset both in popularity and technical sophistication. At the same time, the ongoing demand for coins with enhanced anonymity will push Zcash and Dash teams to improve their products, which, in turn, will naturally cause a backlash from regulators, who will either be able to ensure the transparency of the transactions carried out, or will take them out of the legal field. Obviously, criminals are also extremely interested in the anonymity of the transactions carried out and closely monitor all technological innovations in this area. In this regard, the task of the bodies that are fighting crime is to respond as fast as possible to the emergence of new criminal threats in this area and to develop prompt and adequate preventive measures.

Помимо криптомонеты Monero, которая является безусловным лидером среди анонимных криптомонет как по популярности среди пользователей, так и по степени технической проработанности, современный рынок цифровых активов представлен также и другими монетами, ставящими во главу угла анонимность и этим обстоятельством привлекающих внимание преступников. Рассмотрим технические особенности и возможные криминогенные риски, связанные с двумя из них, а именно Zcash и Dash.

Цель исследования

Целью исследования является криптомонеты с повышенной анонимностью Zcash и Dash с точки зрения тех криминальных рисков, которые влекут за собой данные цифровые активы. В соответствии с целью исследования были поставлены следующие задачи:

1.Провести сравнительный анализ некоторые технологические особенностей криптомонеты с повышенной анонимностью Zcash и Dash

2.Изучить методы распознавания

Объектом исследования является криптомонеты с повышенной анонимностью Zcash и Dash.

Результаты и их обсуждение

1. Сеть Zcash *(ZEC)* [1] была официально запущена 28 октября 2016 года. По мнению бывшего агента ЦРУ Эд-

варда Сноудена, данный проект «может стать ответом на риски, которые несут открытые и доступные любому желающему записи в блокчейне Биткоина» [2]. Изначально ZEC разрабатывался как протокол в рамках Биткоина, обеспечивающий его повышенную анонимность. Однако вскоре создатели протокола решили запустить собственную криптовалюту. Фактически речь идёт о форке Биткоина с функцией AEC (Форк (от англ. to fork – ответвляться) – создание новой независимой версии продукта на основе кодовой базы другого программного проекта. Основная цель таких ответвлений – реализация идей и возможностей, которых не было в основном проекте. AEC – аббревиатура термина Anonymity Enhanced Coin, т.е. криптомонета с повышенной анонимностью).

Необходимо отдельно отметить, что команда разработчиков Zcash имеет солидную научную подготовку и, в целом, по нашему мнению, является одной из лучших в индустрии. Над подготовкой и реализацией проекта работали и продолжают работать четыре группы блокчейн-инженеров, представляющих Массачусетский технологический институт, Университет Джонса Хопкинса, Технион (израильский технологический институт), Университет Тель-Авива, Университет Беркли [3]. В отличие от проекта Monero, разработчики которого предпочли сохранить анонимность, на официальном сайте Zcash можно найти подробную информацию о создателях данного проекта [4].

Укажем некоторые технологические особенности ZEC. Если в сети Биткоина содержится информация об отправителе, получателе и сумме транзакции, то при использовании Zcash в блокчейн вносятся лишь данные о факте осуществления транзакции, без указания её сторон и суммы. Каждая монета ZEC имеет чистую историю, поэтому, в отличие от BTC, нельзя отследить, использовалась ли она для осуществления незаконных операций или нет. Другой особенностью Zcash является возможность выбора уровня конфиденциальности транзакций. Если при использовании Monero данный параметр задан по умолчанию и не может быть произвольно изменён, то в сети ZEC пользователь сам решает, использовать ли монету как Биткоин либо включить функцию анонимности. Для этого применяются два типа адресов – публичные, которые работают по аналогии с Биткоином (*public address*), и скрытые (*shielded address*), которые функционируют с применением опции нулевого разглашения. При этом возможны как полностью публичные платежи, так и частично скрытые, когда анонимными остаются только адрес отправителя или только адрес получателя платежа. (см. рис. 2) Очевидно, что переключение с одного типа адреса на другой оставляет возможность для внешнего отслеживания осуществляемых платежей. Важно отметить, что по умолчанию используется публичный адрес, тогда как защищённый требует активации.

Исследователи отмечают, что монета, не смотря на свои свойства анонимности, значительно уступает XRM и BTC по объёмам платежей в даркнете. Всего 0.09 клиентов Zcash прибегают к функции нулевого разглашения для своих сделок с монетой [6, p. 8]. Исходя из того, что Биткоин может предоставить такой же функционал, как и отрытые платежи в Zcash, скорее всего, подавляющее большинство пользователей ZEC просто не до конца понимают, как работает технология защищённых платежей в данной системе. Нельзя также исключать тот факт, что непопулярность анонимных транзакций в сети связана со значительно более высокими комиссионными платежами. Кроме того, необходимо отметить, что даже скрытые транзакции в блокчейне Zcash далеко не столь анонимны. Этот факт был подтверждён в рамках эвристического анализа системы ZEC, проведённого учёными Университетского колледжа Лондона [7, p. 463-477]. Поэтому неудивительно, что 8 июня 2020 года компания Chainalysis заявила о добавлении функции отслеживания ZEC в один из своих продуктов (Reactor) [8].

Тем не менее, многие игроки криптовалютного рынка поспешили поставить Zcash в один ряд с Monero и отказались от использования этой монеты, что не могло не сказаться на её стоимости. На момент исследования монета занимает 57 место в рейтинге криптовалют с ценой в $ 138 и рыночной капитализа-

цией в $ 1.579 млрд., хотя всего через три дня после запуска (1 ноября 2016 года) её цена доходила до $ 1445 [9].

2. *Dash (DASH)* [10]. Практически все первые криптовалюты так или иначе связаны с Биткоином. Как и Zcash, данная монета является форком продукта Сатоши Накамото с упором на анонимность. Проект был запущен 18 января 2014 года американским программистом Эваном Даффилдом (*Evan Duffield*), но история разработки идеи уходит в 2010 год, когда Даффилд, впечатлённый концепцией Биткоина, стал задумываться о том, как добавить первой монете анонимности. Разработанные им предложения были отвергнуты Биткоин-сообществом, желавшим сохранить базовый протокол первой криптовалюты неизменным. Это и стало толчком для создания программистом собственного проекта [11].

Несколько раз разработчики меняли название своего продукта. Изначально это была монета XCoin (XCO). Однако у проекта возникла серьёзная проблема, состоявшая с том, что не до конца была продумана концепция скорости создания монет. Это привело к инстамайну, т.е. чрезвычайно быстрому майнингу (Инстамайн (Instamine) – термин произошёл от слияния двух английских слов *instant* и *mining* и представляет собой процесс сравнительно быстрой эмиссии существенного объема монет, который происходит при выпуске новой криптовалюты, когда майнинг монет в первые несколько дней или часов осуществляется слишком быстро. Как правило, подобное возникает из-за ошибок в программном коде, где динамически изменяемая сложность корректируется неправильно).

В течение первых 48 часов после запуска проекта, было добыто около трети от всего предусмотренного в программном коде объёма монет [12]. Идея проекта была скомпрометирована, поэтому, после устранения возникшей проблемы, было принято решение о переименовании проекта в *Darkcoin*. Однако и от этого названия разработчики вскоре решили отказаться, так как не желали ассоциировать свой продукт с даркнетом. В результате появилось нынешнее название DASH, что представляет собой аббревиатуру от Digital cASH.

Технические особенности Dash имеют сходство с Zcash, состоящее в опциональной анонимности, которую необходимо задействовать. Анонимность монете обеспечивает механизм «PrivateSend» и мастерноды.

Принцип работы PrivateSend построен на технологии CoinJoin из названия которой следует, что она подразумевает объединение монет. На деле происходит смешение средств нескольких клиентов, чтобы скрыть связь между отправителем и получателем. (см. рис. 2)

Эта процедура скрывает потоки движения средств и ограничивает возможности прямого отслеживания сделок. Транзакция дробится на несколько фиксированных частей, которые перемещаются между мастернодами от 2 до 8 раз и лишь после этого в полном объеме отправляются получателю. (см. рис. 2)

Мастерноды – это специальные сверхмощные узлы (серверы), которые обслуживают сеть, работают на децентрализованной основе и контролируются волонтерами из разных точек земного шара. Для обеспечения повышенной защиты и исключения вероятности подключения злоумышленников, подключение к мастерноде требует внесения залога в размере 1000 DASH (около $ 190 тыс по курсу на 25 марта 2021 года) [13]. На сайте проекта отмечается, что мастерноды обеспечивают функционирование сервисов InstantSend, PrivateSend и системы аккаунтов пользователей проекта на блокчейне, а в награду за это владельцы узлов получают регулярные выплаты, формирующиеся за счёт комиссионных, которые уплачиваются при осуществлении сделок [14]. На момент написания работы разработчиками указывалось более 4.5 тысяч действующих нод [15].

Как и в случае с Monero и Zcash, рассматриваемая монета попала под череду запретов и делистингов, что не могло не отразиться на её общих экономических показателях. В декабре 2016 года стоимость одной монеты Dash доходила до $ 1.5 тыс., однако сегодня монета находится в конце пятого десятка криптовалют с общей капитализацией чуть менее $ 2 млрд. и стоимостью около $ 190 [16].

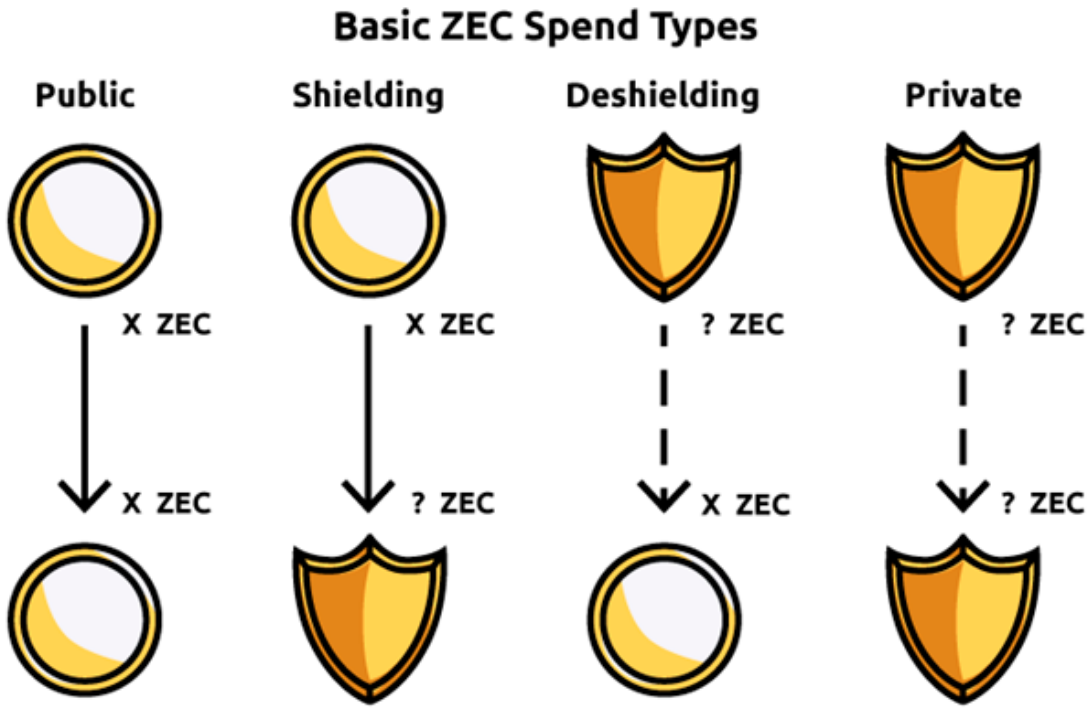

Рис. 1. Виды транзакций в системе Zcash [5]

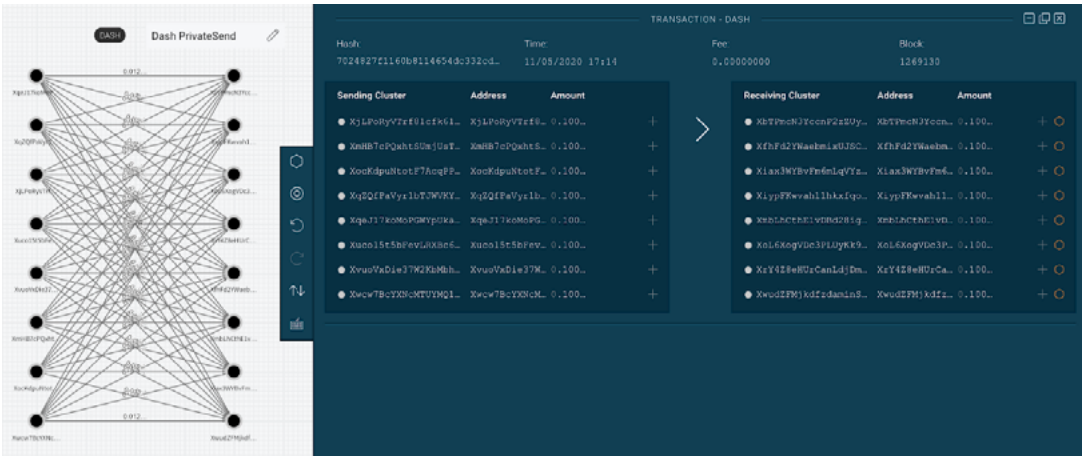

Рис. 2. Принцип функционирования механизма PrivateSend в системе Dash [8]

Анонимные свойства Dash, на которых фактически строится весь проект, вызывают определённые вопросы. Этим грамотно воспользовались представители компании Chainalysis, которые добавили возможность отслеживания транзакций в сети этой монеты. Как отмечается в пресс-релизе по случаю включения Dash в список отслеживаемых, «с технической точки зрения функциональность конфиденциальности Dash не больше, чем у Биткоина» [8], поэтому относить Dash к категории “анонимные монеты” не совсем верно. Не смотря на функцию перемешивания монет, электронные адреса, как и в случае BTC находятся в публичном доступе, а это значит, что денежные потоки в сети вполне можно отследить.

Выводы

В качестве главного вывода следует подчеркнуть, что стабильный спрос на монеты с повышенной анонимностью будет толкать создателей Zcash и Dash к усовершенствованию своих разработок, что, в свою очередь, закономерно вызовет ответную реакцию со стороны регуляторов, которые либо сумеют обеспечить прозрачность осуществляемых транзакций, либо выведут их за правовое поле. Очевидно, что представители криминалитета также крайне заинтересованы в анонимности осуществляемых транзакций и внимательно отслеживают все технологические новшества в данной сфере. Задачей органов, призванных бороться с преступностью, в этой связи является максимально оперативное реагирование на возникновение новых криминальных угроз в этой сфере и своевременная разработка мер, направленных на их предупреждение и предотвращение.

Библиографический список

1. Zcash official website [Электронный ресурс]. Режим доступа: https://z.cash/ (дата обращения: 22.03.2021).

2. SOUTHROST J. Snowden: Anonymous 'Zcash' Could Solve Bitcoin Surveillance Risks // Bitcoin.com – 07.06.2016 [Электронный ресурс]. Режим доступа: https://news.bitcoin.com/snowden-zcash-bitcoin-risks/ (дата обращения: 08.02.2022).

3. Built on rigorous science // Zcash official website [Электронный ресурс]. Режим доступа: https://z.cash/ (дата обращения: 08.02.2022).

4. Founding Zcash scientists // Zcash official website [Электронный ресурс]. Режим доступа: https://z.cash/ (дата обращения: 08.02.2022).

5. PETERSON P. Anatomy of A Zcash Transaction // Electric Coin Co. – 23.11.2016. [Электронный ресурс]. Режим доступа: https://electriccoin.co/blog/anatomy-of-zcash/ (дата обращения: 08.02.2022).

6. YE. C., OJUKWU Ch., HSU A., HU R. Alt-Coin Traceability. Carnegie Mellon University, 18.05.2020. [Электронный ресурс]. Режим доступа: https://eprint.iacr.org/2020/593.pdf (дата обращения: 08.02.2022).

7. KAPPOS G., YOUSAF H., MALLER M., MEIKLEJOHN S. An Empirical Analysis of Anonimity in Zcash // 27th USENIX Security Symposium. August 15–17, 2018. Baltimore, MD, USA. – P. 463-477. [Электронный ресурс]. Режим доступа: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kappos.pdf (дата обращения: 08.02.2022).

8. Introducing Investigation and Compliance Support for Dash and Zcash // Chainalysis Team – 08.06.2020. [Электронный ресурс]. Режим доступа: https://blog.chainalysis.com/reports/introducing-chainalysis-investigation-compliance-support-dash-zcash (дата обращения: 08.02.2022).

9. Zcash // CoinMarketCap [Электронный ресурс]. Режим доступа: https://coinmarketcap.com/ru/currencies/zcash/ (дата обращения: 08.02.2022).

10. Dash official website [Электронный ресурс]. Режим доступа: https://www.dash.org/ (дата обращения: 08.02.2022).

11. The birth of Darkcoin // Dash.org – 29.03.2014 [Электронный ресурс]. Режим доступа: https://www.dash.org/forum/threads/the-birth-of-darkcoin.162/ (дата обращения: 08.02.2022).

12. ЯНИТОС И. Что Такое Криптовалюта Dash // AltCoinLog – 28.01.2020. [Электронный ресурс]. Режим доступа: https://altcoinlog.com/what-is-dash/ (дата обращения: 08.02.2022).

13. Dash // CoinMarketCap – 25.03.2021. [Электронный ресурс]. Режим доступа: https://coinmarketcap.com/ru/currencies/dash/ (дата обращения: 08.02.2022).

14. Как работают мастерноды // Dash Official website. [Электронный ресурс]. Режим доступа: https://www.dash.org/ru/masternodes/ (дата обращения: 08.02.2022).

15. Deterministic Masternodes Monitoring // DASH Ninja [Электронный ресурс]. Режим доступа: https://www.dashninja.pl/ (дата обращения: 08.02.2022).

16. Dash // CoinMarketCap – 25.03.2021. [Электронный ресурс]. Режим доступа: https://coinmarketcap.com/ru/currencies/dash/ (дата обращения: 08.02.2022).