Защита на инвестиции в криптовалута

Способен ли е законът да осигури такава

адв. Иво Александров и адв. Яна Лазарова | Камбуров и съдружници

През изминалата година понятието криптовалута зае централно място в икономическите новини. Все още е рано да се оцени дали прогнозите на експерти, че се касае за явление, сравнимо по мащаб с появата на интернет през 90-те, са верни. Към момента обаче е ясно, че криптовалутите са част от бизнес средата и с нарастването на популярността й тази нова разменна единица навлиза в много сфери на обществения живот.

Основното им предимство се базира на технологията на блокчейн веригата - децентрализирано управление на транзакции в peer-to-peer система, която за разлика от транзакциите с традиционни валути не подлежи на сериозна регулация и контрол от правителствата, поне за момента. Привлекателността на криптовалутите е свързана с анонимността и сигурността на блокчейн технологията, които произтичат от самата й конструкция.

При неограничения достъп на участници в системата обаче надеждността й е нарушена. 1/4 от транзакциите с криптовалути се извършват именно заради анонимността на трансфера. Като се прибавят и плащанията за нелегални дейности в т.нар. тъмен интернет (darknet), доверието в отношенията между участниците придобива друг смисъл. Индикация в тази насока са сигналите на правоприлагащи органи от цял свят, които подчертават невъзможността за идентифициране на виртуални плащания в криптовалути, което ги прави привлекателен инструмент за изпиране на пари. В същото време примерите за пробиви в системи, считани за сигурни, са ежедневие.

Към април 2018 г. броят на действащите криптовалути е 1565, нараства и броят на хората, инвестиращи в тази сфера. Това поражда много правни въпроси като как да се адаптират законовите механизми против изпирането на пари, как да се регулират инвестициите в ICO проекти, блокчейн договорите и др. От всички аспекти на криптовалутите, които правото следва да обхване, най-съществена за момента изглежда сигурността.

Какви са начините за съхранение

Двата основни варианта за съхранение са чрез платформа за търговия с криптовалути или в личен портфейл. Съществуват различни типове портфейли: онлайн, хардуерни, хартиени и т.н. Личните портфейли не съхраняват самата криптовалута, тъй като тя няма материален еквивалент. Предметът на съхранение е уникалният криптиран код (ключ) в съответната блокчейн верига. Ключът може да се запамети на физическо устройство (USB), което съхранява ключа локално и не е свързано с интернет. Алтернатива на физическото устройство е съхранението в цифров портфейл онлайн или локално на смартфон или компютър, но този вид съхранение може да бъде обект на хакерски атаки. Ако предпочитаният подход е офлайн съхранение на портфейла, вместо на хардуер, уникалният криптиран код може да бъде записан и на обикновен лист хартия.

Как се краде криптовалута и какви мерки за сигурност да използваме

Според Ерик Ларшевек, управител на Ledger Wallet, "всички хакери по света насочват усилията си към криптовалутите". През 2015 г. от европейската платформа Bitstamp бяха откраднати 19 000 биткойна. През 2016 г. 120 000 биткойна бяха откраднати от базираната в Хонконг Bitfinex. В края на 2017 г. група хакери осъществи пробив в системата на NiceHash, откъдето са откраднати около 4700 биткойна на стойност над 70 млн. долара. През януари 2018 г. бе съобщено, че криптовалута на стойност над половин милиард долара е била откраднатата от японската борса Coincheck.
Зачестяват и случаи на хакерски атаки с цел заразяването на компютри с програми за майнинг на криптовалута. Съобщава се и за кражби на специализирана техника за добив на криптовалута (от декември насам в Исландия са откраднати 600 сървъра). Появи се и случай, в който крадци влизат в частен дом в Англия и принуждават с оръжие да им бъдат преведени притежаваните от собственика биткойни. Коментираните ситуации очертават

основните рискове за собствениците на криптовалути:

- Трето лице се сдобива с паролата ви в услуга за съхранение на криптовалута. Ако използвате услуга като Coinbase, не ви се налага да запаметявате публичен и частен ключ. Услугата наподобява електронно банкиране, за което са нужни потребителско име и стандартна парола. Тази система позволява кражба на вашата парола. Най-често това се случва, като трето лице получи достъп до вашия имейл и изпрати искане до съответната платформа за промяна на паролата, в резултат на което получава директен достъп до средствата ви.
Бихте могли да предотвратите този риск, като заключите с двустепенна автентификация имейл профила си, както и профила в съответната платформа, с приложение от рода на Google Authenticator. Препоръчително е да не използвате SMS парола като втори етап на автентификацията, тъй като съобщенията могат да бъдат прихващани.

- Неволно предоставяте достъп до частния ви ключ. Този риск съществува, когато не използвате специална платформа. В този случай е възможно някой да види частния ви ключ, ако го съхранявате в имейла си или на място, достъпно за трети лица. Препоръката на експертите е да съхранявате частния си ключ на сигурно място, задължително офлайн.

- **Хакер се представя за получател на криптовалута.** Най-често това може да се наблюдава при ICO кампании. Чрез фалшив уебсайт хакери се представят за компания, лансирала ICO процедура, и убеждават инвеститорите да превеждат средства в различен портфейл. За да избегнете този риск винаги проверявайте дали адресът, на който превеждате средства, е истински.

- Несигурна трета страна. Касае се за платформи, предлагащи услуги в сферата на криптовалутите, чиито системи за киберсигурност могат да бъдат преодолени от хакери. Проблем в този случай е фактът, че често такива платформи не гарантират възстановяване на откраднатите средства или компенсация за потребителите си. Внимателният подбор на компаниите, с които работите, би могъл да ограничи този риск.

- Преустановяване на услуга за съхранение. Съществуват множество платформи, където потребителите могат да съхраняват своите криптовалути. Съобщава се за случаи, в които дадена платформа изчезва, като често твърди, че е станала обект на хакерска атака. В действителност понякога се касае за измама, при която собствениците на платформата изчезват от интернет заедно със средствата на клиентите си. Обичайно подобни измами се наблюдават в darknet и специалистите съветват да се избягват сделки с криптовалута в тази част на интернет пространството.

- Изгубвате достъп до средствата си. Инвеститорите наблюдават също загуба на достъп до електронния портфейл поради засилените мерки за сигурност при съхранението. Счита се, че към януари 2018 г. има над 3000 безвъзвратно изгубени биткойна, или около 14% от тази криптовалута. Според Кристофър Алън, един от

главните архитекти на Blockstream компания с фокус в сферата на сигурността, никога не сме прекалено подсигурени. Препоръчително е съхранение на паролата за достъп в криптосейф cryptosteel. Друга препоръка е винаги да имате back up на първоначалния back up.

Какво може да се предприеме в случай на кражба?

В случай че криптовалутата се съхранява в платформа за търговия с криптовалути, ако при хакерска атака или неразрешен от вас достъп до портфейла ви изгубите активи, би следвало да се обърнете към платформата с искане за възстановяване стойността им. Практически обаче съществуват редица препятствия преди довеждането на това начинание до (успешен) край. Първо, трябва да се изследват общите условия на съответната платформа и да се установи какви механизми и гаранции за възстановяване на активите се предлагат.

Най-често онлайн платформите застраховат активите, които държат, като осигуряват възможност за възстановяване на стойността при кражба, която е резултат от нарушение на сигурността на платформата, хакерска атака, кражба на служител или измамно прехвърляне към чужд портфейл. Този тип гаранция обаче не покрива загуби, произтичащи от неоторизиран достъп до вашия личен профил, като изрично се сочи, че е задължение на държателя да защитава личните си пароли и да контролира устройствата си за влизане в системата. Следва да се отбележи, че повечето платформи са ситуирани извън България, съответно се прилага правото на юрисдикцията, в която оперира платформата. В случай че това се случва в САЩ например криптовалутите не подлежат на защитата на правилата за застраховане на депозити или за защита на инвеститорите в ценни книжа.

В случай че вашият уникален криптиран код бъде физически откраднат, може да сезирате правозащитните органи – полиция, прокуратура. Тук се навлиза в непознати територии, където въпросите са много, а възможните отговори - още повече. На първо място, възможно ли е уникалният криптиран код да се третира като право на интелектуална собственост, притежаваща характеристиките на програмен код, и ако да, кой състав на престъпление следва да се приложи?

От друга страна, отнемането на ключа (независимо дали е на физическо устройство или хартиен носител) от ваше владение и без ваше съгласие отговаря на престъпния състав на кражба в Наказателния кодекс. Усложненията тук са много. Анонимността в блокчейн веригата е минус в конкретния случай, тъй като много трудно бихте могли да докажете собствеността върху конкретния ключ. Възможно решение е оставянето на писмена следа с достоверна дата, удостоверяваща, че конкретният ключ е ваша собственост. Тази писмена следа трябва да се предаде за съхранение при доверено лице, в сейф или при нотариус. Проследяването на откраднатия ключ също повдига много въпроси.

Първо, необходими са високи технологични познания и капацитет за боравене в тази иновативна среда и, второ, анонимността на транзакциите води до трудно установяване на наказателно отговорното лице. Поради огромния потенциал на криптовалутите и генерираната от тях стойност безспорно ще расте и ролята им в икономическия и социален живот. Защитата на правата и законните интереси на лицата следва да бъде гарантирана, а това изисква развитие на правото и нов подход на държавните институции и правоприлагащите органи към тази чувствителна материя.