July 19, 2017

Skadden

Blockchain Update

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Four Times Square
New York, NY 10036
212.735.3000

Lessons From the CoinDash Initial Coin Offering Hack

On July 17, 2017, the CoinDash initial coin offering (ICO) was hacked within minutes of its launch, resulting in numerous potential purchasers sending their money to a fraudulent address. The hack has raised many questions about the security and legitimacy of ICOs and of the blockchain more generally.

An Overview of ICOs

In recent months, ICOs, also known as token sales, have become the proverbial "coin of the realm" for blockchain startups to raise funding for their projects. According to a report by the research firm CB Insights, ICOs raised more than $1 billion in the first half of 2017, surpassing the amount raised for blockchain ventures through traditional venture financing. A company looking to raise funds through an ICO publishes a white paper setting forth its business plan and announces a day on which anyone can purchase unique tokens linked to that project. The parameters around the token sale generally specify the price of the token based on another currency, a maximum number of tokens to be sold and/or a cap on the amount to be raised, and a minimum amount to be raised (which, if not achieved, will result in the purchasers' money being refunded). For this reason, ICOs are often described as crowdsourcing for blockchain startups.

Purchasing ICO tokens likely does not provide the holder with equity in the blockchain startup that issued the tokens, any right to profits or dividends, or any voting rights in the enterprise. Rather, a token might provide the purchaser with access to, or use of, the services the blockchain company will offer. Those participating in the ICO are typically able to purchase a token at a discount with the hope that demand for the token will increase and they will able to re-sell the token at a profit. Interest in ICOs has been fueled by the amount of money many startups have been able to raise and, in some instances, by a dramatic increase in token value.

In most cases, the tokens used for ICOs — which must typically be purchased using bitcoins or ether cryptocurrencies — are a form of Ethereum token that complies with ERC-20, a standard for currencies built on the Ethereum blockchain. Using the ERC-20 protocol provides the blockchain startup with a fairly easy way to generate coins for its project. It also gives individuals who hold ether cryptocurrency through an ether "wallet" fairly easy access to ICO token purchases. Nearly all of these token sales are based on so-called smart contracts, which perform specified steps without human intervention once a set of conditions are satisfied.

Not surprisingly, many ICOs exist in the gray area of existing regulatory frameworks. Questions as to whether some ICOs should be deemed securities under U.S. law have resulted in many new ICOs being launched outside the U.S., and the expectation is that the Securities and Exchange Commission (SEC) will step in at some point and regulate these offerings. For now, purchasers of most ICOs are not presented with the robust disclosures that would accompany other regulated forms of fundraising. This lack of disclosure was noted recently by an SEC official speaking at the Consensus blockchain conference in May 2017. Valerie Szczepanik, the head of the SEC's distributed ledger group and an assistant director of the SEC's Division of Enforcement, remarked that even companies that are not regulated by the SEC have fiduciary duties to investors.

Despite a common misconception to the contrary, ICOs are not essential to raise funds for blockchain startups. All the traditional means of funding a startup exist for blockchain entities as well. However, ICO proponents note that this new approach "democratizes" the fundraising process, allowing even the smallest investors to invest directly in a startup. They assert that this is consistent with the spirit of blockchain technology generally. Critics of ICO note that while democratization of the investment process exists in theory, much of the funding remains concentrated within a relatively small group of cryptocurrency holders. Critics also note that ICO issuers are primarily motivated by the ability to obtain significant funding in a short period of time and with little or no regulatory oversight.

The CoinDash Hack

CoinDash is a blockchain startup focused on building a portfolio management platform and providing cryptocurrency social trading (*i.e.*, where investors can follow how others are trading and mimic their actions). The CoinDash token sale kicked off as planned on July 17, 2017, with a 28-day token sale window and a $12 million hard cap in CoinDash Token (CDT) sales.

Three minutes after the launch, CoinDash realized that the ICO was compromised and hackers had changed the address to which ether payments were to be sent by purchasers. This new address went straight to the hackers' own wallet. CoinDash promptly posted the following message on its website in English, Chinese and Korean:

> *This is an emergency message delivered to you in order to stop you from sending your money to an unauthorized ETH address.*
>
> *It seems like our Token Sale page was tampered and the sending address was changed. Please stop from sending your funds to any of the addresses until we say otherwise.*
>
> *We are currently examining the situation and will shortly send further instructions.*

An estimated 43,500 ether (valued around US$7.4 million) were sent to the hackers. CoinDash has stated that it will make purchasers who were compromised whole, stating: "CoinDash is responsible to all of its contributors and will send coins reflective of each contribution." The CoinDash hack is believed to be the first successful hack of an ICO.

Lessons Learned

The initial reaction among many who learned of the CoinDash hack was, "I thought the blockchain could not realistically be hacked." The CoinDash hack does not change this reality. Hacking a well-established blockchain such as the Ethereum or bitcoin network would still require such a massive amount of computing power that such a hack would be virtually impossible. It also remains unclear what the hackers would gain, since they would be stealing a cryptocurrency whose value their own hack would materially degrade.

However, while established blockchains themselves remain virtually impenetrable, applications that serve as gateways into the blockchain are not necessarily equally secure. Similarly, applications that allow the purchase of tokens do not offer blockchain-level security, even though the funding is often then used for a blockchain startup. Indeed, many have noted that the CoinDash hack was very simple to execute. Platforms to purchase tokens are not, by definition, secure, and conducting one's own diligence or relying on communitywide diligence efforts before a purchase is essential. In addition, trusted third parties are starting to emerge to vet token sales. There is no doubt that security will be one of the factors they will test for in the future.

The CoinDash hack also brings renewed focus on the unregulated state of the ICO market. While CoinDash has committed to make purchasers whole, it is not clear it was under any legal obligation to do so. The recourse that a purchaser would have against the token seller is murky at best. As noted, token sellers generally do not make disclosures or representations in any document about the security of their offering (such as, "We used industry-standard security measures to protect your token purchases.") Moreover, even if such statements were made,

purchasers would likely have little insight into whom to sue or even, given the global nature of ICOs, what jurisdiction to file such a suit in.

While much of the focus to date has been on the question of whether ICOs should be deemed securities, the hack highlights that other risks exist with respect to token sales that even a robust regulatory scheme might not have addressed. Nonetheless, a regulated offering may have included a risk factor about the potential for cybersecurity attacks. It will be interesting to see whether offerors of token sales consider adding a disclaimer regarding cybersecurity risk going forward.

It remains to be seen whether the CoinDash hack will dampen enthusiasm for ICOs, at least in the short term, or if investors will dismiss this incident as a one-off outlier. Regardless of the impact on the ICO market, there is little doubt that the hack will only increase regulatory scrutiny of this fundraising practice.