LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

TUESDAY, AUGUST 29, 2017

PERSPECTIVE

Invasion of the smart contract hackers

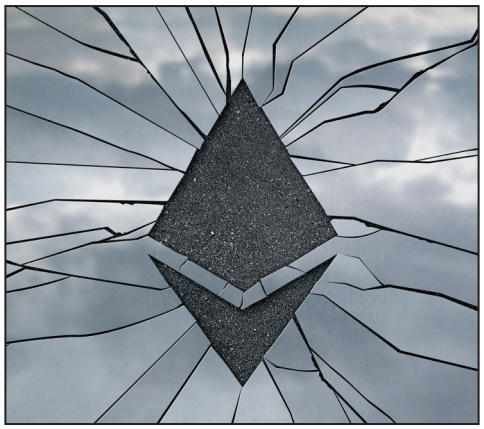
By David W. Adams
and Matthew E. Kohen

It's a story that could easily land on the desks of producers all over Southern California in the form of a sci-fi screenplay. In July, some users of the cryptocurrency ethereum were victimized by a hack of a multi-signature wallet designed by an independent software company. Unauthorized users accessed vulnerable wallets and transferred funds associated with them. These malicious actors reportedly stole over 150,000 ether, valued, as of late August, at more than $50 million. After news of the hack broke (and during the theft), a group of ethical hackers (commonly known as white hats) used the same attack vector to transfer nearly 400,000 ether from vulnerable wallets. They then placed the ether into a new, secure wallet contract designed to permit the ethers' rightful owners to reclaim their tokens.

Many see the blockchain as the wild west of today's technology sector due to its disruptive potential. As a result, developers and businesses in the space must contend with myriad legal uncertainties. These are often exacerbated by events that, all-too-frequently, seem ripped from the pages of a crime drama. This article explores two important blockchain attributes and why they cause so much uncertainty when existing law is applied.

Blockchain Technology: A Brief Background

A blockchain can be defined as a cryptographically-secured, distributed transaction ledger. The blockchain enables trustless peer-to-peer transactions by eliminating the need to rely on a centralized authority, like a bank or clearinghouse. The blockchain eliminates the need to trust third parties by distributing a copy of the ledger



Shutterstock

Etherium's logo seen in a cracked glass.

memorializing all transactions to all (or substantially all) market participants. This feature, combined with the requirement that a majority of these participants agree on the validity of a new transaction before it can be added to the ledger, makes the technology incredibly secure. Using the same complex cryptography and mathematics, the blockchain requires that market participants agree on which version of the ledger is correct. As such, absent the consensus of the participants in the protocol, past transactions cannot be modified.

Simple Transactions Give Way to Self-Executing Smart Contracts

As blockchain technology has matured, users have started to employ distributed ledgers to store and run smart contracts. Smart contracts, which are self-executing computer programs that exist on the blockchain, monitor and validate a condition to automatically determine whether the asset involved in that contract should be sent to one or more parties. Smart contracts, like peer-to-peer transactions, generally cannot be modified, repaired, stopped, or removed once they are deployed onto the blockchain, absent extreme circumstances such as a "hard fork," which is a permanent divergence from the blockchain's previous version.

A wallet contract, like the one mentioned above, is one type of ethereum smart contract. Wallet contracts are designed to permit only authorized users to send transactions. So, if a wallet contract containing a vulnerability is deployed to the blockchain, there is typically little that can be done to repair it. This happened in the case of the vulnerable wallets mentioned above — and demonstrates the white hats' purported justification for proactively draining the contents of those wallets to more secure contracts.

A New Legal Frontier

The challenges imposed by two of blockchain's most significant features — immutability and trustlessness — have profound legal implications. In many circumstances, existing laws and regulations do not account for the unique manner in which smart contract participants interact with one another.

The futility of traditional legal remedies is one significant obstacle. Ethereum provides for pseudonymous transactions. Generally, users interact with one another through a public address, which is just an alphanumeric string. Users may never know the true identity of their counterparty. So, if a user accrues an actionable legal claim — i.e., if funds are stolen from a wallet — it may be impossible to identify the culprit.

Even if a victim could identify a malicious actor and obtain a judgment or court order against that actor, there is practically very little that such a judgment or order could do. In today's traditional banking system, a court might order a bank to freeze at-risk funds before a would-be thief has the chance to abscond with them. In the blockchain's completely trustless world, there is no such authority to implement the court's protective

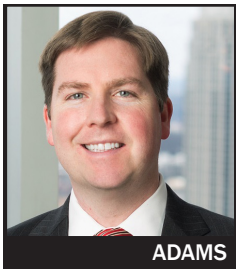
measures. Similarly, banks can often unwind or alter fraudulent transactions, such as those initiated by the victim of a scam. When settling a transaction on a blockchain, there is comparatively little that can be done once the transaction is broadcast to the network. Short of convincing a substantial majority of users to coordinate a hard fork and change prior entries to the ledger to return the stolen funds, victims are out of luck.

This futility is further exacerbated by the manner in which U.S. law treats software that contains bugs or is otherwise unusually vulnerable to attack. Theoretically, users of software that contains bugs or other vulnerabilities could accrue a civil claim against the software's creator. However, because, as a practical matter, nearly every piece of software contains some type of bug, liability for its creators is typically limited through restrictions in the licensing agreement, terms of service, etc. While these restrictions help to foster technological innovation, they may also leave victims of hacks, bugs, or other complications without recourse.

The ineffectiveness of legal remedies is only the tip of the proverbial iceberg when it comes to the legal uncertainties associated with using blockchain technology. Courts will soon have to grapple with the jurisdictional implications of assets that exist solely in the cloud, on hundreds of identical copies of a digital ledger, and are stored on computers throughout the globe. For these and other reasons, anyone curious about the blockchain and its disruptive potential should consider the effect that existing, somewhat-incompatible laws could have on society's ability to regulate this emerging technology. For now, we may have to wait for the release of a movie to generate enough interest to settle these questions.

David W. Adams *chairs Carlton Fields' FinTech practice and focuses his practice on financial institutions, payment processors and emerging technology companies. He can be reached at dwadams@carltonfields.*com and @GeorgiaLawDavid.

Matthew E. Kohen *is co-chair of Carlton Fields' Blockchain Technology and Virtual Currency Taskforce. He focuses his practice on the representation of telecommunications and technology companies, and frequently writes and speaks on a variety of technology-related topics. He can be reached at mkohen@carltonfields.com.*


ADAMS


KOHEN