Bloomberg Law®

White Collar Crime Report™

DIGITAL CURRENCY

Three Kobre & Kim lawyers discuss how the use of cryptocurrency to store and transfer value creates new challenges and new opportunities for practitioners trying to recover assets. The authors explain how asset recovery methods will need to evolve and develop as cryptocurrencies gain greater adoption among businesses and everyday users.

INSIGHT: Did Someone Steal Your Crypto? Here's How to Get it Back



By David H. McGill, Benjamin J.A. Sauter, and Jake Chervinsky

The booming cryptocurrency market has attracted attention from a wide variety of constituents, including traders, regulators, hackers and thieves. As bitcoin and other digital currencies have skyrocketed in value, they have become an appealing target for criminals seeking to defraud honest market participants. Fortunately for victims, and contrary to common assumptions, there are effective options available to recover lost or stolen funds.

New Challenges and New Opportunities

The use of digital currency to store and transfer value creates new challenges and new opportunities for practitioners trying to recover assets. These new challenges and opportunities arise from the blockchain technology on which cryptocurrencies are based, as compared to the financial infrastructure underlying more traditional currencies.

Out With the Old The traditional financial system employs numerous safeguards to facilitate asset recovery and prevent thieves and fraudsters from making off with ill-gotten gains. In most jurisdictions, financial institutions are subject to strict due diligence requirements that call for identifying the owner and the source of specific assets. As a result, if a criminal attempts to deposit stolen funds into a regulated bank account, the bank will collect information about the deposit and record any transactions involving the account. These measures create a paper trail that facilitates the tracing of stolen funds no matter where in the world they travel. And once stolen assets are found, they can often be frozen and returned to their rightful owner through an appropriate legal process.

Of course, the financial system is not perfect at restricting the flow of illicit proceeds, and it has notably struggled to keep up with the forces of rapid globalization. For years, criminals have successfully sheltered

 ISSN 1559-3185

stolen funds in certain offshore banking centers and other jurisdictions with lax banking regulations. Criminals have also taken advantage of complex corporate devices to launder and reintroduce stolen funds into regulated institutions. Yet, with the passage of tighter laws such as the Foreign Account Tax Compliance Act, many more institutions have come into compliance with the global financial system, and criminals have found it increasingly difficult to hide stolen funds from their victims or creditors.

In With the New Digital currencies currently operate outside, or on the fringes, of the traditional financial system. Unlike funds that are held in accounts controlled by regulated financial institutions, cryptocurrencies like bitcoin are stored on decentralized public ledgers that, by definition, are immune to control by third parties. This feature is called ''censorship resistance,'' meaning once funds have been transferred and recorded on a digital currency's ledger, those funds cannot be frozen, returned, or transferred by anyone except their new owner.

At the heart of every digital currency is a simple ledger—a record of transactions between different accounts. The ledger is maintained by a vast network of computers that uses an extraordinary amount of processing power to ensure that the ledger is accurate and tamper-proof. The ledger is a permanent, immutable record; except for new transactions, the ledger's history can never be altered. (This describes the function of a particular type of distributed ledger: a blockchain using a proof-of-work consensus algorithm. This technology is used by bitcoin, the most popular digital currency, but there are many other types of distributed ledgers that use different methods to accomplish roughly the same goals.)

Typically, anyone can create an address (often called a ''wallet'') on a digital currency's ledger without providing any information about who or where they are. Each wallet is typically defined solely by two numbers called ''keys''—a public key that operates as the wallet's identification number and a private key that operates as the wallet's password. Any person who knows a wallet's public key can check the wallet's balance or send currency to the wallet, but no person can transfer currency out of the wallet without the private key.

Crucially, a wallet's public and private keys share a mathematical relationship, but it is impossible to use a wallet's public key to determine its private key. (This is the ''cryptographic'' aspect of cryptocurrency). Thus, as long as a wallet's owner keeps his private key secret, no person or entity will ever be able to find it. (For maximum security, public-private key pairs can be generated offline so that an account owner's private key is never exposed to the internet. An account that's held entirely offline is referred to as ''cold storage.'') This means that unlike under the traditional financial system, it is often impossible for a bank, government or court to freeze or transfer any of a digital currency wallet's funds, even if those funds represent the proceeds of criminal activity. This characteristic is what makes cryptocurrencies censorship-resistant.

digital currency proponents applaud censorship resistance, touting its ability to enable peer-to-peer, cash-like transactions over the internet, free from interference by totalitarian governments. This feature is particularly important in dictatorial countries like Venezuela, where the ruling regime often uses asset seizure as a weapon of political oppression. Yet despite the benefits that censorship resistance offers to unstable regions in the world, it also greatly complicates the ability of theft and fraud victims to recover stolen digital assets.

Methods for Tracing and Recovering Stolen Digital Currency

Victims of digital currency fraud have two primary methods to recover their funds. The first method applies existing asset recovery practices to the digital currency space: using a legal or judicial process to freeze assets that a thief or fraudster has deposited with a third party. The second method involves obtaining judgments that can be executed against other traditional assets wherever they reside. A successful asset recovery strategy will likely require some combination of both methods.

Tracing and Recovering Stolen Digital Assets Deposited With a Third Party One benefit of most digital currencies is that their ledgers are public, which makes tracking the movement of funds a much simpler task than in the traditional financial system. If a criminal deposits stolen digital assets into a digital currency exchange—a company that enables users to purchase and trade assets through an online platform akin to Vanguard or E-Trade—the deposit can typically be found through an analysis of the asset's ledger. There are some technologies that can attempt to obscure the flow of digital funds, but in general, cryptocurrencies offer a remarkable improvement in the transparency and auditability of financial transactions.

At present, some of the largest holders of digital assets are digital currency exchanges. Importantly, when a user deposits funds into a digital currency exchange, the user does not control the private key for the wallet in which the funds are stored. Instead, for security reasons, the exchange typically combines all of its users' funds into a small number of wallets and keeps the private keys for those wallets to itself. The exchange then maintains a separate record showing the amount of funds that belong to each user, and if a user wants to withdraw funds, he must ask the exchange to transfer those funds for him.

This means that a digital currency exchange can play the same role as a bank in the traditional financial system: it can freeze a criminal's assets and thereby prevent him from spending or transferring ill-gotten gains.

But if a digital currency exchange can freeze its users' assets, why would a criminal deposit stolen funds into an exchange in the first place? The primary reason is to convert the funds into fiat currency to be withdrawn, or a different type of currency that *cannot* be tracked: a so-called privacy coin. Unlike bitcoin and many other cryptocurrencies with entirely public ledgers, some currencies employ technology that offers private and untraceable transactions. Popular privacy coins like Monero and Zcash allow users to transfer funds without revealing the amount transferred or the wallet to which the funds were sent. As a result, if a criminal successfully converts stolen digital assets into one of these currencies, the assets may be very difficult to follow.

The likelihood of success in convincing a digital currency exchange to freeze a user's assets depends on the jurisdiction where the exchange is located and no small measure of skillful advocacy. Several of the largest and most reputable exchanges—such as Coinbase and Bittrex—are based in the United States, and are thus subject to the U.S.'s well-developed legal and judicial framework for asset recovery. For example, our firm was recently able to freeze approximately $1 million worth of digital currency assets that had been stolen from a client and deposited with an exchange only days earlier. Other mature jurisdictions with popular exchanges include Korea (home to Upbit and Bithumb), China (home to OKEx and Huobi) and Hong Kong (home to Bitfinex), where our firm's local offices have also had success recovering stolen assets with the assistance of law enforcement agencies and the courts. In all instances, persuading exchanges and authorities to freeze assets before they dissipate requires advocates with the right combination of technical acumen, credibility, and—critically—speed.

Even the most capable asset recovery specialists must confront jurisdictional barriers to retrieving stolen assets. Indeed, some prominent exchanges have set up in jurisdictions with lax regulations that provide little recourse for victims of digital currency theft or fraud. For example, Binance—one of the largest exchanges in the world by trading volume—recently announced that it would relocate from China to Malta, largely in response to a crackdown on digital currency trading by regulators in Beijing. The government of Malta has positioned the country as a ''crypto-friendly'' jurisdiction, actively pursuing partnerships with digital currency companies and passing legislation that simplifies the issuance of new digital assets.

While Malta's progressive approach to cryptocurrencies may be a benefit for exchanges like Binance, the country lacks a strong mechanism for recovering stolen assets. Tellingly, the Maltese government established its Asset Recovery Bureau in 2015 to trace and recover the proceeds of criminal activity, but three years later, the bureau is still not up and running. (*See* https://www.timesofmalta.com/articles/view/20180220/local/malta-sending-message-that-serious-financial-crimes-go-unpunished.671253.) Consequently, victims whose funds end up in a Binance account must consider creative mechanisms for retrieving stolen assets, including leveraging Malta's status as a member of the European Union to obtain recognition and enforcement of foreign judgments in the aid of asset recovery. Ultimately, the general trend of exchanges setting up in less-regulated jurisdictions means that victims of fraud will become increasingly reliant on advocates with the specialized expertise to design and execute on cross-border asset recovery strategies.

Moreover, the rapid advancement of decentralized exchanges may further complicate matters for victims of theft or fraud. One of the potentially disruptive applications of digital currency technology is the ability to run software—usually called a ''smart contract''—on the network of computers that maintain the currency's ledger. This would be similar to running software in the cloud, except there is no third party in control of the software once it has been launched. Several blockchain technology startups are now working on decentralized exchange protocols (such as AirSwap, IDEX, and the 0xProject), which would enable users to purchase and trade digital assets without ever depositing funds into a wallet controlled by a third party. If this technology works as advertised, criminals could convert stolen funds into untraceable privacy coins without ever relinquishing control, making the funds very difficult to recover.

Obtaining and Enforcing Judgments Against Traditional Assets If digital currency assets are gone for good, there is still a second method of recovery: obtaining a judgment against the thief or fraudster and enforcing it against traditional assets that cannot be hidden. This method only works if the criminal's identity can be ascertained *and* he owns property in a jurisdiction where asset recovery is feasible. If a victim's funds are stolen by an anonymous party, or if the offender keeps all his assets in certain offshore jurisdictions, it may not be possible to obtain or enforce a traditional judgment.

In the brief history of financial crime in the digital currency space, the identities of the offenders have rarely been discovered. The largest theft of digital currency to date was announced in February 2014, when the Mt. Gox exchange reported that a hacker had stolen approximately 850,000 bitcoins, today valued at more than $5 billion. In July 2017, a joint U.S.-Interpol task force arrested Alexander Vinnik for allegedly laundering a portion of the proceeds from the Mt. Gox theft, but the identity of the hacker remains unknown. Similarly, in July 2016, a hacker was able to steal 3.6 million Ether tokens, today valued at approximately $1.5 billion, by exploiting a flaw in a smart contract called The DAO on the Ethereum network. The DAO hacker was never identified even though he or she posted repeatedly on social media about the theft in the days after it occurred. Indeed, the list of anonymous hackers who have stolen millions of dollars in digital currency without being caught is long and growing.

That said, fraud victims are often well-acquainted with those who steal from them, and in the digital age, forensic analysis can glean much from a relatively small amount of information. For example, the victim of a phishing attack may be able to track an offender using an email address or other useful metadata. digital currency exchanges that play by the rules in certain jurisdictions will also likely maintain ''know-your-customer'' information about their account holders, and that information can be obtained through a subpoena or other court processes, as our firm has demonstrated. Here again, the technical acumen of practitioners is critical to a successful asset recovery strategy.

The Upshot

Asset recovery methods will need to evolve and develop as cryptocurrencies gain greater adoption among businesses and everyday users. For now, the best advice for theft and fraud victims is to immediately seek help from practitioners with the right combination of skills and experience to move quickly in tracing the flow of their stolen funds, identify the perpetrator, and mobilize the appropriate strategy to recover their assets before it is too late.

Author Information

David McGill is a litigator and investigator with Kobre & Kim whose practice resides at the intersection of

finance and technology, frequently handling disputes involving crypto-assets. Benjamin Sauter is a Kobre & Kim litigator who focuses on cutting-edge financial products and services disputes, including all manners of digital-currency-related disputes. Both are part of the Digital Currency & Ledger Defense Coalition, a group of over 50 lawyers dedicated to protecting U.S. blockchain innovators. Jake Chervinsky is a Washington DC- based litigator at Kobre & Kim.