CRYPTOCURRENCY SCAMS

BBB study finds lack of regulation and consumer education results in dramatic increase in fraud and financial losses

BETTER BUSINESS BUREAU
INTERNATIONAL INVESTIGATIONS INITIATIVE

ISSUED: MARCH 2022

CRIMINALS ARE FINDING NEW METHODS WITH THE CRYPTOCURRENCY MARKET, LIKE BITCOIN AND ETHEREUM, TO STEAL FROM UNSUSPECTING INVESTORS OR VICTIMS OF COMMON SCAMS.

As Bitcoin and other types of cryptocurrencies gain attention in the news for their volatility, novelty and celebrity investors, scammers are quickly discovering how to use people's lack of knowledge about the system to rip off investors and dress up old scams.

Early entrants into the market made enormous amounts of money, and later others rushed in with hopes of similar gains. The total value of all bitcoins in the world is estimated at $1.03 trillion. A single bitcoin, worth $2,000 in 2017, reached an all-time high of $67,549 in 2021. But Bitcoin is volatile, and the value can swing wildly. After hitting a high in 2021, it declined to $35,484 in early 2022. Purchasing power of a bitcoin can vary day-to-day. Nonetheless, cryptocurrency — a digital payment system that does not rely on banks to verify transactions — has now grown into a major worldwide industry. New York, Arkansas, Brazil, and Puerto Rico expressed interest in becoming attractive locations for the cryptocurrency industry. However, in the spring of 2021 China banned cryptocurrency. It was the second largest country using cryptocurrency.

A virtual tug of war exists between the legitimate and fraudulent use of cryptocurrency.

This study examines digital currencies and the scams that use them. It provides background on key terms and concepts, examines cryptocurrency's susceptibility for large-scale scams, and notes the risks and provides tips for common investors and others using cryptocurrency as a payment method.

CRYPTOCURRENCY SCAMS ARE ON THE RISE

Better Business Bureau® (BBB®) reports received about fraudulent activity involving cryptocurrency have tripled in the past three years.

The cryptocurrency payment method accounted for the second-highest scam losses reported to the Federal Trade Commission (FTC) in 2021 with losses of $750 million, only slightly behind bank-to-bank wire transfers.

The FBI's Internet Crime Complaint Center (IC3) received 35,229 complaints in which victims used cryptocurrency in 2020, with reported losses of $246 million, a 64% increase from 2019 when they reported losses of $159 million.

The Canadian Anti-Fraud Centre (CAFC) describes similar trends. Losses reported nearly tripled from $8.3 million in 2019 to $22.8 million in 2020 and then skyrocketed to $75 million in 2021. Many of those reports used Bitcoin. It was the payment method in 9,445 instances while the use of other forms of cryptocurrency was negligible.

Because there is so much money in this system, and it is relatively anonymous, there is widespread fraud and victims are losing millions. Many people report being duped into using Bitcoin when payment was demanded for ransomware, Bitcoin mining, Ponzi schemes and more. This year, a U.S. married couple was arrested for allegedly conspiring to launder $4.5 billion in Bitcoin and are accused in the U.S.'s biggest-ever cryptocurrency theft case.

While BBB Scam Tracker® shows the number of victims reporting financial losses through cryptocurrency nearly tripled between 2019 and 2021 and monetary loss amounts more than tripled during the past two years, the actual number of victims is much higher as most fraud victims do not report it. The FTC found that fewer than 5% of fraud victims report scams to BBB or law enforcement.

YEAR	COMPLAINTS REPORTING MONETARY LOSS	AMOUNT DISPUTED
2019	451	$4,915,838
2020	906	$5,438,407
2021	2,465	$7,933,424

Two categories emerged from Scam Tracker reports — investment frauds and cryptocurrency — as new methods of getting money from victims in traditional frauds. There were also victim reports of Ponzi schemes, hacking, malware, and ransomware attacks.

There is a clear trend that scammers are using cryptocurrency and it appears likely to continue. According to the 2021 BBB Scam Tracker Risk Report, cryptocurrency scams have become the second riskiest type of scams that victims encounter.

For consumers, the line is blurry between losses to outright scams and losses to legitimate companies. Over the past three years, nearly 4,000 complaints to BBB have claimed losses of more than $18 million to companies involved with cryptocurrency, with more complaints that don't mention specific losses. At least 1,028 negative reviews were filed about cryptocurrency companies. One of the largest contributors to BBB cryptocurrency complaints is Coinbase, with a BBB "F" rating and more than 3,000 complaints in the last three years.

Victims cited social media and celebrity promotions as the top means of contact for this type of scam. California victims reported twice as many complaints as Texas or number three Florida. The two largest age groups disclosing cryptocurrency scams fell into the 25- to 34-year-old age bracket at 29% and the 35-44 age range at 27%. Almost equal numbers of men and women reported cryptocurrency-related scams.

Several other trends appear from this data. Romance scammers have shifted from requesting money for supposed emergencies to now conning people into investing in cryptocurrency. The CAFC found that the number of romance fraud victims asked to invest in cryptocurrency doubled in 2021. The availability and increase in Bitcoin ATMs or kiosks make it easy for victims to send cryptocurrency to scammers. Now located at nearby convenience stores and big box stores, victims need only feed in $20 bills and scan a QR code the scammer provides to have the money sent directly to them.

BBB SCAM TRACKER

YEAR	REPORTS	LOSSES
2019	444	$7,399,704*
2020	572	$2,897,170
2021	1215	$7,953,502

**A single Scam Tracker report claimed $4 million in losses.*

BBB NEGATIVE REVIEWS ABOUT CRYPTOCURRENCY COMPANIES

YEAR	REVIEWS
2019	155
2020	250
2021	579

I have a Coinbase account with several thousand dollars in it. I have a new telephone with a new authenticator. I submitted my photo ID and picture to prove my identity in order to use the new authenticator. Coinbase has not responded to me to acknowledge and set up the new device. There are no working points of contact on the Coinbase website. No phone numbers, no email addresses and the chat function does not work. Without working authentication, I cannot access my account.

- from a consumer complaint to BBB

INDUSTRY KEY CONCEPTS AND DEFINITIONS

What is cryptocurrency? It is a digital payment system that does not rely on banks to verify transactions. It is a form of digital money that uses encryption technology that can enable anyone anywhere to send and receive payments. It does not exist in physical form, like paper money. It exists as lines of computer code digitally signed each time it travels from one owner to another.

To understand the fraudulent aspects of this industry, it is necessary to provide background on common terminology and an understanding of how this system works. Most cryptocurrency fraud and complaints involve Bitcoin. Another form of cryptocurrency is Ethereum. There are thousands of new types of cryptocurrencies, but they all operate with blockchain technology. The essential concepts are the same.

Bitcoin was developed in 2009 by Satoshi Nakamoto, who may or may not be a real person. It operates wholly over the internet. There is an open-source code for the programs that operate it and a governing committee that sets the basic rules for the system. This allows person-to-person sharing anywhere in the world without any central authority, such as a bank, tracking transactions or reporting to any government agency. Importantly, transactions are not reversible. They do not offer many of the safeguards which protect users of traditional financial systems.

How is Bitcoin created? "Miners" solve incredibly complex mathematical problems and receive Bitcoin as a reward. Despite the use of the term "token," Bitcoin only exists electronically. The originating protocols of this system allow for creation of a maximum of 21 million Bitcoin. Mining currently accounts for 18.7 million Bitcoins. The mathematical problems are increasingly more complex, and the rewards for mining decrease with time. As a result, there is a limited supply of Bitcoin available.

It takes specialized computers to perform the enormous number of calculations needed to mine, consuming massive amounts of electricity, a criticism of the industry. Miners create the "blocks" in the blockchain and act as auditors to write the ledgers, making sure the same Bitcoin is not used twice. This prevents double spending and counterfeiting. Miners are compensated with Bitcoin.

Bitcoin mining occurs all over the world. Because all cryptocurrencies rely on blockchain and require mining, some cryptocurrency businesses offer investments in mining operations. Some hackers use the others' computers to surreptitiously run mining programs — an act called cryptojacking.

What is blockchain? Blockchain is what makes cryptocurrencies possible. All cryptocurrencies employ it. It is an open record of every Bitcoin transaction and serves as a ledger of all transactions and includes a time stamp. This decentralized system is distributed among computers all over the world that validate and record transactions. Every few minutes, miners add "blocks," which cannot be edited. Proponents believe there is great potential in blockchain technology, but there are few situations where it operates outside the realm of cryptocurrency. It is not clear who would pay for the mining necessary to support other uses of the blockchain technology.

How can I buy Bitcoin?

Bitcoin and other types of cryptocurrencies can be purchased at Bitcoin ATMs (kiosks) or at Bitcoin exchanges with various apps. Exchanges permit the purchase of cryptocurrency through almost any method, including bank wiring, credit cards, and even with gift cards. Cash App, a popular smartphone application backed by banks, is another option.

Bitcoin ATMs

Because many people are unfamiliar with cryptocurrency, one might expect that they would be reluctant to pay scammers that way. With the advent of Bitcoin ATMs, victims can now go to a convenient place near them to easily and quickly send Bitcoin.

Where can I find Bitcoin near me?

Bitcoin ATMs, or kiosks, have expanded very rapidly and are now found at nearby locations across the U.S. and Canada. In January of 2020 there were 4,212 of these machines in the U.S. But now there are over 30,000 in the U.S. and 2,235 in Canada, the second most in the world. There is even a website that can locate one near you. Bitcoin ATMs are commonly located at gas stations/convenience stores such as Circle K and at many Walmart stores.

How does a Bitcoin ATM work?

Most Bitcoin ATMs allow a user to register an account at the machine. One company stated for amounts under $250, consumers just need to enter a phone number to register an account. Other companies may have different requirements. Consumers load the Bitcoin into a "wallet" they have created (or set up at the ATM) or send it to someone else's Bitcoin wallet. The FBI warns that scammers provide victims with a QR code to their phone, representing the "address" of the Bitcoin wallet receiving the funds. The machine scans the code and the money goes into the blockchain. The recipient can cash it out in just a few minutes after the blockchain is updated.

One use for Bitcoin ATMs is simply to purchase Bitcoin, store it in a wallet, and hope it appreciates in value. Bitcoin ATMs may also be used to send money to family members in other countries. These remittances are a major source of income for Mexico and other countries. They are an important part of the business for companies like Western Union and MoneyGram. There is more privacy in sending money through Bitcoin, and fees can be lower.

Some Bitcoin ATMs have warning signs on them. Those operated by Bitcoin Depot have a sign reading:

WARNING! Have you received a phone call from someone demanding payment with Bitcoin? THIS IS LIKELY A SCAM. All Bitcoin transactions are irreversible. Send to your own wallet only. NOT SURE if you are being scammed? Call us for assistance at...

There is a free phone at the Bitcoin ATM for consumers to call for assistance with their transactions or to report a possible scam. Some machines also have security cameras recording videos of those at the machines.

How are Bitcoin ATMs regulated?

Bitcoin ATMs are regulated by FinCEN in the U.S. and Fintrack in Canada. In the U.S. registration is required. The ATM must comply with the Bank Secrecy Act and its anti-money laundering standards (AML), such as Know Your Customer (KYC) requirement to identify who is sending money. There are also currency transaction reports (CTRs) which must be completed if someone tries to send more than $10,000 or in total sums calculated to evade these controls. Owners of these systems must also provide the government with Suspicious Activity Reports (SARs) about certain transactions.

There are reports about problems with scammers seeking money through Bitcoin ATMs.

The FBI warns of an increase in scammers asking victims to pay through Bitcoin ATMs for government impostors, those impersonating utility companies or law firms, and for lottery frauds. Scammers ask victims to withdraw cash from bank or retirement accounts. CAFC also reported that scammers ask victims to go to Bitcoin ATMs to send money, as has the FTC.

These machines also may be subject to state licensing and regulation as Money Services Businesses like Western Union and MoneyGram. The State of New Jersey issued a report in February 2021 warning of unlicensed ATMs operating with few safeguards to protect the public.

These unlicensed sites were used for fraud. The New Jersey investigation also found that one third of the ATMs operating in the state had not registered with FinCEN. State Police had prosecuted an individual who received $600,000 in payment in Bitcoin from victims who "purchased" nonexistent vehicles.

In 2020, the Justice Department dismantled a network of Bitcoin ATMs that laundered up to $25 million at ATMs in California. These machines were not registered, and the owner knew they were used for illegal activity. He was sentenced to two years in prison.

What is a crypto wallet?

Because Bitcoin and other tokens have no physical existence, owners control the encrypted cryptocurrency passwords, which are like incredibly complicated PINs. The codes are stored in "wallets." Those can be stored at Bitcoin exchanges, on a personal computer or other device, like a thumb drive. Bitcoin exchanges also offer wallets. Many people store cryptocurrency in apps on their smart phones. But scammers can supply victims with corrupt apps they control, and bogus apps can be found on the App Store and Google Play.

What can I buy with cryptocurrency?

While there are reports that retailers are considering accepting Bitcoin and other cryptocurrencies for payment, it is unclear that many do currently. Tesla said some transactions are accepted using Dogecoin to purchase merchandise like belt buckles, but that form of payment cannot be used to buy a car.

PayPal now allows people to pay for purchases with Bitcoin, but not directly. PayPal converts Bitcoin to dollars at a rate they determine after converting the cryptocurrency. This is due to the volatility of cryptocurrency. Merchants are understandably reluctant to take payments in a currency which may quickly drop in value.

Charitable enterprises do accept donations in Bitcoin, and BBB Wise Giving Alliance has developed a system that allows for donations in many kinds of cryptocurrency.

How do I track cryptocurrency?

Because the blockchain is a ledger of all transactions, it is possible to trace the path of a cryptocurrency payment from where it began to where it went. Chainalysis is one company that offers a service to track Bitcoin and other cryptocurrency. Ciphertrac and Elliptic are other cryptocurrency tracking services.

Once cryptocurrency goes into a scammer's wallet, consumers may not know who owns that wallet. Scammers can quickly cash out the cryptocurrency into dollars or other national currencies — referred to in the cryptocurrency field as "fiat currency" — or quickly move the money by trading it for other kinds of cryptocurrency.

Password security

Each transaction is recorded on the blockchain. They are encrypted, and an electronic code or key to use cryptocurrency is required. Lose the key, and you lose the money. There is a famous story of Gerald Cotton, who died at age 30 and never revealed the key to $250 million worth of cryptocurrency. This led to speculation that this was a scam, and he did not really die.

Scammers actively attempt to hack these keys. Hackers seek access to wallets where cryptocurrency is stored, and online exchanges have usernames and passwords to protect these keys. Many of these passwords require two-factor authentication, often by text message. Scammers attempt to engage in SIM swapping — transferring a phone number to themselves so that they receive those text messages. In one recent case, a New York man pleaded guilty to SIM swapping, which he used to steal $20 million in cryptocurrency. In addition, phishing scams appearing to come from legitimate exchanges are a significant issue, since the stolen credentials can lead to identity theft and cryptocurrency loss.

Be careful with QR code links

Quick Response or QR codes are square barcodes that a smartphone camera scans and reads to quickly lead the user to a website. A QR code can also be used to send or receive Bitcoin from one person to another. A scammer may send a victim a QR code that they can scan at a Bitcoin ATM, and it provides the address the Bitcoin is to be sent. The FBI warns consumers that "cybercriminals are taking advantage of this technology by directing QR code scans to malicious sites to steal victim data, embedding malware to gain access to the victim's device, and redirecting payment for cybercriminal use."

What are Bitcoin exchanges?

People often store Bitcoin in wallets held by exchanges, where one can buy, sell, or trade cryptocurrency. An account must be set up to authenticate identity, but some exchanges, particularly those located in other countries, may require less information about a person's identity. Those accounts have passwords, and those must be secure.

An exchange can simply store Bitcoin with hopes it appreciates in value, but it can also track the value in an account, trade it for other types of cryptocurrencies or convert it to U.S. dollars or fiat currency. Exchanges charge a transaction service fee.

What is Ethereum?

The second most common cryptocurrency after Bitcoin is Ethereum, which can be bought and sold as investments. Like all cryptocurrency, it uses blockchain, but the codes stored on the block can contain decentralized applications, known as dApps.

What are non-fungible tokens (NFTs)?

Non-fungible tokens are part of the Ethereum blockchain system. They are trending up in popularity. Ethereum "smart contracts" can record ownership of a digital asset, such as a digital picture or music, and this ownership can be recorded on the blockchain ledger.

A piece of digital art can be sold and ownership of it is recorded; however, it does not mean it is protected from copyright violations, despite the recent increase in popularity.

The Wall Street Journal reported: "In 2020, just over $100 million worth of NFTs changed hands. Last year Chainalysis estimates that grew to $44.2 billion."

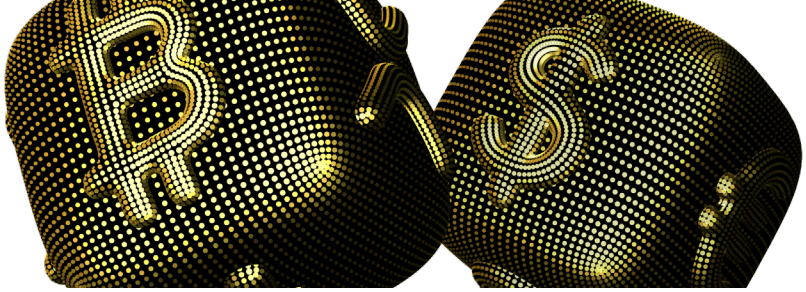
NFTs can then be sold, or the original owner can get a royalty every time it changes hands. NFTs are used frequently for digital art and music and for video games. The Morning Brew noted, "The Bored Ape Yacht Club (BAYC), a collection of 10,000 ape avatars that individually act as tickets to an online social club, has become one of the most prominent brands in the NFT space."

The U.S. Treasury Department recently warned that NFT's are increasingly used to launder money and threatened to make them subject to regulation.

What is Decentralized Finance (DeFi)?

Decentralized Finance allows the Ethereum cryptocurrency system to lend money, buy insurance and trade assets in ways other financial systems currently perform, but without the use of intermediaries such as banks. This system works primarily through Ethereum. People offer "smart contracts" stored in the blockchain. The contracts have simple specific terms, which allow those who accept them to have a concrete agreement. Using DeFi and a decentralized finance application (dApp), a consumer enters their loan needs and an algorithm matches the needs with a loan with acceptable terms. The consumer would need to agree to those terms to receive the loan.

This system is still in its infancy. Problems include the volatility in prices and regulatory issues. Although this system shows much promise, there are few reports discussing successful uses of this technology in fields outside cryptocurrency. Reports indicate over the last two years, the amount of money deposited at DeFi services has spiked from just $500 million to $247 billion. And more than $10 billion was stolen from them in 2021.



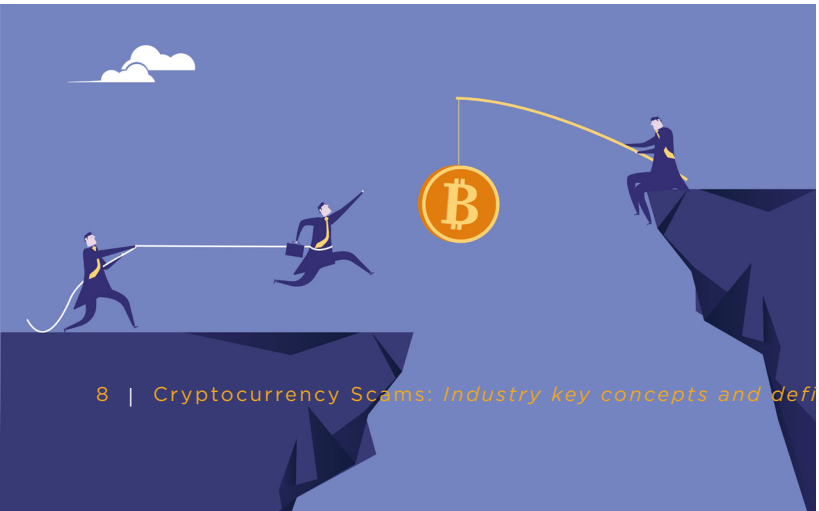
What are stablecoins and other types of cryptocurrencies?

The wide swings in the value of cryptocurrency are an issue. One solution is to attach the coins to a fiat currency such as the dollar. This is being explored, and the U.S. government issued a report framing how this might work and the necessary regulations.

There are now hundreds of other types of cryptocurrencies. All operate on blockchain and there is a lure to get in on the ground floor for maximum appreciation like Bitcoin. In addition, the Department of Justice (DOJ) reports that some are more difficult to trace than others.

What are Central Bank Digital Currencies (CBDCs)?

There is much discussion about governments having to issue CBDCs, digital currencies which would be backed by central banks. Some 91 countries reportedly are examining this possibility. China banned cryptocurrency, and reportedly is working on one tied to the Yuan for internal purposes in China. The U.S. Federal Reserve recently issued a policy paper on the subject. The hope is that these cryptocurrencies could simplify and expedite financial transactions. The paper expresses serious concerns about crime surrounding the effort and would require "robust rules" that address money laundering and terrorist financing. These transactions would require record keeping and reporting requirements.



Is cryptocurrency "real"" money?

Money, as we know it, has value in its own right. It may represent the right to tangible goods, and it is backed by a government. Paper dollar bills have little inherent value but are backed by the full faith and credit of the United States government. Paper money is used to pay all debts, public and private. The U.S. Treasury holds real assets, such as gold. Banks are backed by collateral assets such as real estate or stock in companies. There is no collateral backing cryptocurrency.

This all works when people have confidence in the monetary system. If people lose confidence, the system could collapse. In the 1600s the Dutch financial system was the most powerful in Europe. Speculation grew in tulip bulbs, and prices increased to dizzying heights. However, this "tulip bubble" crashed, costing many their life savings.

The Bank of England warned cryptocurrency could become worthless. Some have suggested the entire system is little more than a Ponzi scheme.

Is cryptocurrency protected by financial systems?

There are many safeguards and regulations built into standard financial systems to remedy abuses or other problems experienced throughout history. Despite the efforts of regulators to apply those safeguards to cryptocurrency worldwide, many do not apply or are not followed. This adds increased risks.

Two common protections do not apply to cryptocurrency:

- Bank deposits are backed by the Federal Deposit Insurance Corporation (FDIC). If a bank makes a bad loan, the owners embezzle funds, or the bank is robbed, you are insured, and your money is protected.
- Credit cards offer chargeback protection. If you buy something over the internet with your credit card and scammers do not send anything or send counterfeit goods, you can contact your bank and get your money back. The credit card system holds a reserve account of money, and they can assess fines or take some of that money.

CRIME IN CRYPTOCURRENCY MARKETS

Criminals use Bitcoin and other cryptocurrency to support enormous amounts of criminal conduct. Because this conduct can involve huge sums of money and because some actions affect the stability of the cryptocurrency market, they deserve mention. Chainalysis reports $14 billion was lost to cryptocurrency fraud in 2021. This is double the $7.8 billion lost in 2020. DOJ details the types of criminal conduct involved in cryptocurrency markets and sketched out efforts to combat it.

Darknet marketplaces operate in parts of the Internet not accessible by search engines. These markets allow criminals to buy and sell illegal drugs, firearms, child pornography, counterfeit passports and other documents. Payment for these goods and services is mainly in cryptocurrency. DOJ is concerned about some "anonymity enhanced cryptocurrencies" that are difficult to track with non-public blockchains like Monero, Zcash, and Dash.

DOJ has acted against some of these dark web markets. In 2017, DOJ indicted a Russian and a large digital currency exchange for laundering $4 billion in illicit proceeds from ransomware, hacks, and narcotic sales. In 2019, DOJ indicted the owners of DeepDotWeb, a site that facilitated money payments for fentanyl, heroin, crystal meth, firearms, hacking tools, and stolen credit cards using cryptocurrency. One member was sentenced to prison. Similarly, the Government Accountability Office (GAO) reported cryptocurrency markets are increasingly used to fund sex trafficking operations and to buy and sell illegal drugs.

Fake websites are used by scammers who often send "phishing" emails impersonating real banks and other organizations which ask victims to "confirm" their log in information. This happens to cryptocurrency wallets and now it has spread to Google. Victims searching Google for a cryptocurrency app such as phanto**m**.com find a site for phanto**n**.com. When they set up a wallet on the fake website, which looks quite professional and authentic, they unwittingly transfer their money into a scammer-owned wallet. Reports from the fall of 2021 show fraudsters used these tactics and stole $500,000.

Rug pulls are another major form of fraud in the cryptocurrency ecosystem. In this scheme, users find investors who provide financial support for new cryptocurrency projects by trading in their cryptocurrency to fund a new kind of token, anticipating expansion and value appreciation. These new tokens are created on the Ethereum blockchain and listed on decentralized exchanges. Sometimes the new type of cryptocurrency does not really exist, and the investors lose all their money. Chainalysis reports rug pulls accounted for 37% of all cryptocurrency scam revenue in 2021.

The Squid Game rug pull is an example. Developers launched a new token following the popular Netflix series and claimed the tokens could be used on online games then traded for other types of cryptocurrencies. The token's developers took an estimated $3.3 million.

Money laundering is a concern of law enforcement in the cryptocurrency field. Through various means, criminals can transfer cryptocurrency through a variety of other cryptocurrencies and into fiat money. This conduct can include tax evasion and disguising criminal profits. In 2021 DOJ got a guilty plea in a case against Helix, which used mixers and tumblers to launder over $300 million from narcotics and other criminal transactions.

Rogue nations can also use this system to evade financial sanctions. For example, the U.S. issued sanctions against a Russian exchange that laundered money for ransomware and other crimes.

Stolen cryptocurrency and hacking are common. In 2021, Chainalysis reports $3.2 billion in cryptocurrency stolen, with $2.3 billion taken from DeFi protocols, a 516% increase from 2020. Other kinds of large-scale thefts occur in cryptocurrency markets. In 2021, Thodex, a large centralized exchange, disappeared after the exchange stopped investors from withdrawing funds. The result: a loss of $2 billion in cryptocurrency. Pakistanis recently lost $100 million in investments in a local Bitcoin exchange.

Hackers also direct their efforts to cryptocurrency exchanges. Reports show hackers attacking cryptocurrency exchanges and DeFI platforms stole $4 billion in 2021. Hackers from North Korea reportedly stole $400 million by hacking centralized exchanges. There are many more cases where cryptocurrency exchanges have been hacked and money stolen. In February 2022, the U.S. announced the arrest of two people for laundering $3.6 billion in cryptocurrency stolen in an earlier hack of a cryptocurrency exchange.

VICTIMS SHARE EXPERIENCES

Cryptocurrency investment fraud

As long as people have invested money, there has been fraud. Cryptocurrency simply opens new opportunities for the repackaging of common investment frauds. With the development of new types of cryptocurrencies after the success of Bitcoin, there are more opportunities for investment fraud. Various investor protections developed through government regulation are less effective to those who are victims of this type of fraud.

Shanell works in the finance department of a university in St. Louis. In the summer of 2021, she heard about making money from Bitcoin investing. She watched a YouTube video about how Bitcoin investments work and noticed several comments on the video by people claiming that they made money successfully with Graham S. Cassidy Trading Services. Shanell reached out through WhatsApp and contacted Graham. Shanell was told to buy Bitcoin through Cash App and send $1,500. Though it stretched her financially, she sent the money. After ten days, she received a screenshot that showed her account increased to $7,345.56.

When Shanell decided to withdraw her earnings, she was first told that she had to pay a 10% commission of $734.56 and then a broker's fee of $812.45. After she paid both, an email requested an additional $1,167.88 to withdraw her money, which she did not pay. Shanell concluded it was a scam and reported it to BBB.

Though large investors lose large sums, these scams are increasingly aimed at the public and small investors. Investment frauds are a major portion of cryptocurrency reports to BBB Scam Tracker, doubling between 2019 and 2021. In addition, both the FTC and the CAFC report a substantial number of cryptocurrency investment complaints and millions of dollars lost to these schemes.

The Chairman of the U.S. Securities and Exchange Commission (SEC) recently testified to Congress describing cryptocurrency investment field as the "wild west" riddled with fraud and investor risk. The SEC issued a warning about this topic. State securities regulators similarly expressed serious concerns about investment in cryptocurrency, as have securities regulators in Canada.

ROMANCE SCAMMERS ASK VICTIMS FOR CRYPTOCURRENCY INVESTMENTS

Romance scams are one of the costliest frauds operating around the world. For 2020, the FBI's IC3 reported they were second in reported losses only to Business Email Compromise frauds in terms of money lost. For the first six months of 2021 the IC3 reported 1,800 romance scam complaints with losses of $133.4 million. The FTC recently reported that romance scam victims reported losses of $547 million in 2021, the most of any fraud category.

The nature of romance scams is explained in the BBB's romance scam study. Scammers using fake profiles and stolen photos contact individuals on dating sites or social media, and then quickly move victims to other methods of communication. They groom victims and build trust with them for several months, and then extract money from them by feigning an illness or another emergency, claiming a temporary need for funds due to a business issue, or for the financial means to visit the victim in person, often claiming marriage plans.

Over the past two years, romance scammers began convincing victims to invest in cryptocurrency. The CAFC reports in 2018 and 2019 they had 85 romance victims who paid with cryptocurrency. In 2020, this rose to 178. In May of 2021, an analysis by the FTC found in the previous six months 20% of lost money through romance scams was to cryptocurrency investments. And for 2021, the FTC had 2,985 reports of romance scams where money was lost through cryptocurrency, with losses of $139 million.

Both the FBI and Interpol report scammers are asking romance scam targets to download bogus cryptocurrency apps, assuring them of great returns on the investments. These sophisticated fake apps pretend to be from the Apple App store or from Google Play. The apps allow victims to check the bogus online accounts and have live customer service personnel to answer questions. Victims may be allowed initially to take out money, but then are encouraged to invest more. Some romantic interests claim to have invested, which provides a sense of shared risk and legitimacy. Online accounts appear to show funds rapidly increasing in value. But if the victim tries to remove money, they are locked out of the account money unless they pay additional fees. The romantic interest disappears, and the money is gone.

COMMON TYPES OF INVESTMENT FRAUDS REPORTED TO SCAM TRACKER AND ACTIONS TAKEN BY ENFORCEMENT AGENCIES IN THE CRYPTOCURRENCY REALM INCLUDE:

Investment fraud reported to BBB

BBB Scam Tracker Reports include victims of Ponzi schemes, mining investments and rug pulls. However, most reports assert these investment scams began on social media and some report the victim relied on the endorsement of a celebrity when they became involved.

Ponzi schemes

Ponzi schemes, named for Charles Ponzi and most recently made newsworthy by Bernie Madoff, offer initial investors high returns on their investment. These earnings draw in more new investors, whose money is used to pay the returns to early participants, not from any increase in value. But at some point, there is not enough new money coming in to pay investors, and the system collapses. The SEC has warned investors about this type of scam. In one case the SEC alleged that cryptocurrency lending platform BitConnect was a Ponzi scheme which cost investors $2 billion. The owner of BitConnect has since been indicted.

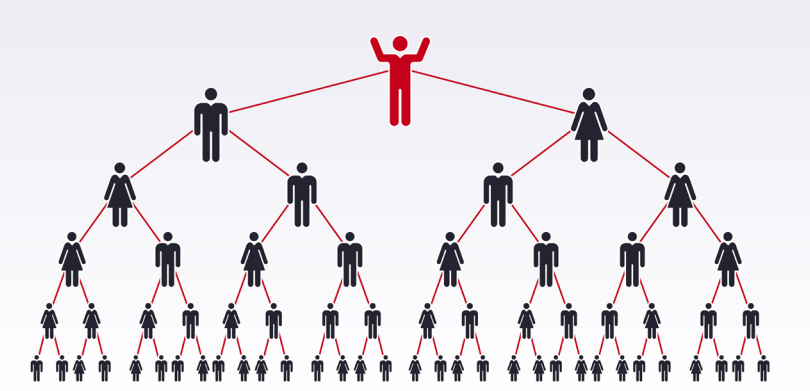
Initial Coin Offerings (ICOs)

With ICOs, some investors are interested in funding the launch of a new kind of cryptocurrency token and are led to believe they can get in on the ground floor with such an investment. Often these are just rug pulls, and the organizers simply disappear with the money from investors.

Bitcoin mining

In these scams, victims are encouraged to invest in Bitcoin mining. The Texas securities commissioner sued one fraudulent operation that promised a 10% return within 30 days.

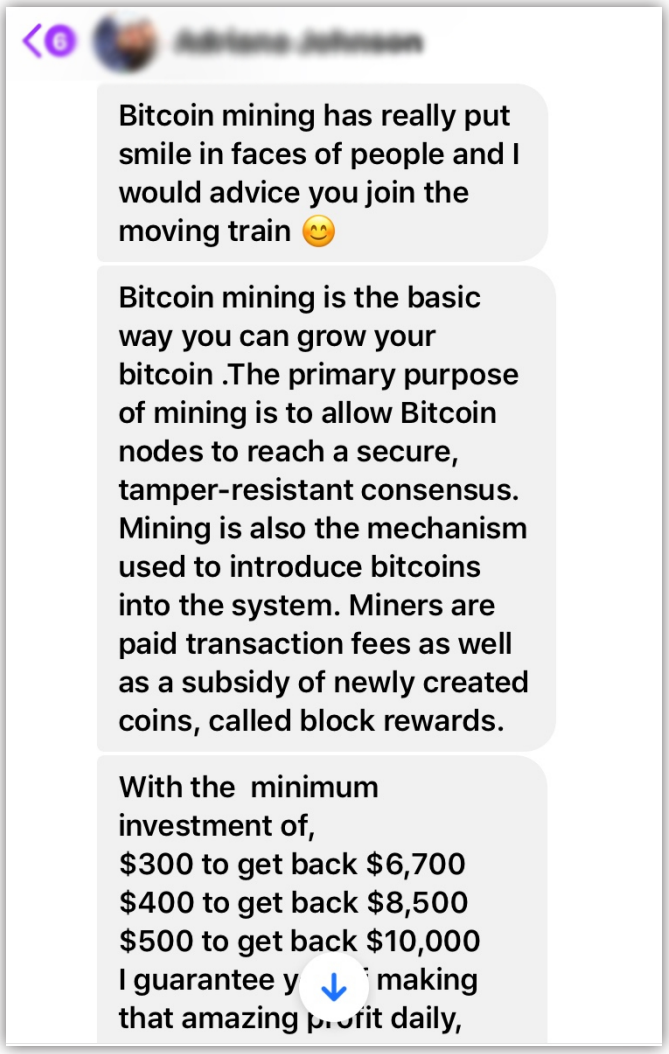
Keishae lives in the Bay Area and works at a hospital, though she is planning to go back to school soon. In September 2021, she got a message from a person she thought was a friend on Facebook. The "friend" told her that she could instantly increase an investment by ten times with Bitcoin through Coinbase. She initially sent $50 through Cash app to the wallet the friend specified. She got a screen shot showing that the money increased to $500, and when she asked about withdrawing her money she was told there was a $200 processing fee, but that she would also get ten times the investment on that money. She complied and was told there was still another processing fee to be paid. This continued, and eventually Keishae had paid $1,300. She was never able to get any money back. She complained to the "friend" on Messenger and started receiving X-rated videos. She reached out directly to her Facebook friend and learned she had not really been communicating with her. The account was hacked. She complained to BBB and called the police, who told her to go to the FBI. She filed a complaint online with the FBI.



Social Media

BBB Scam Tracker data show that social media is the most common place victims find cryptocurrency scams. The FTC reports that 25% of all scams in 2021 began on social media.

In a common tactic, scammers impersonate friends on Facebook who then tell victims about their success in making money and urge victims to follow suit. Other common Facebook posts tell people they can quickly double their money or steer people to "investment advisors."



Text message from a scammer to a targeted investor

MORE VICTIM EXPERIENCES

Lori lives in Chicago, and put some money into Bitcoin before, so she had a wallet. In September of 2021, she was on Instagram and met "Melissa Snart", who messaged Lori that she was with crytotradeFX and that money could be made in funding Bitcoin mining and get ten times the investment over a brief period. Lori initially sent $500, hoping to grow it to $5,000. Melissa told her that the minimum investment was $1,000. So Lori sent another $500 in Bitcoin, hoping to get $10,000. The company told her it would charge 15% for the service which would come out of the earnings. It seemed odd to Lori that there was no "p" in "crytotradeFX," the name of the website.

Lori was provided with an account at the website and she had a password for access and to review the status of her account. In six days, the site said her account increased to $11,000. So Lori decided to take out her money. First the company said that she had to pay the 15% fee with additional money, and it could not come out of her account. So she sent an additional $1,500 and submitted a withdrawal request. They then asked her to send a picture of herself holding her driver's license and to send an additional $600 for insurance and taxes. She requested proof that these additional requirements were needed, and they refused. Lori realized this was a scam and told the company that they were criminals. She filed complaints with BBB, the FBI and the FTC. She lost a total of $2,500.

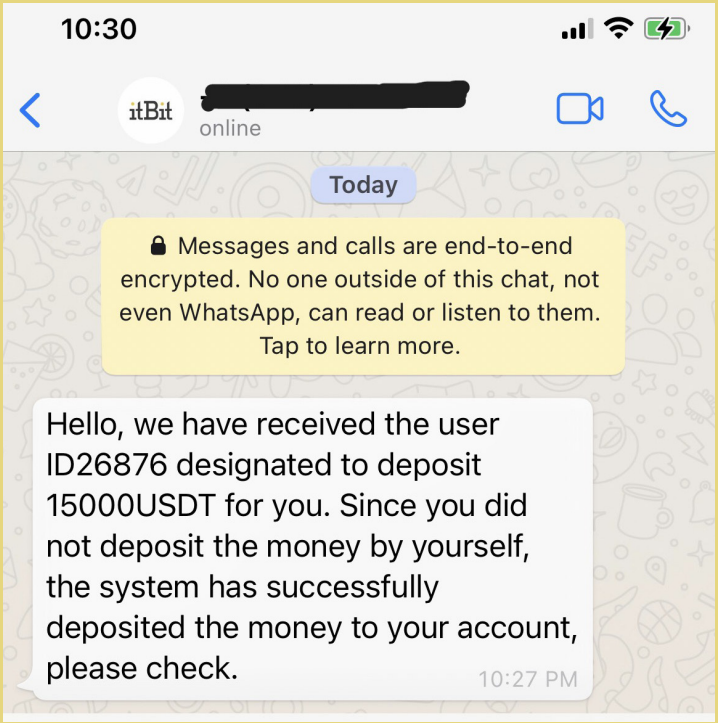
Hunter is a college student in Kansas, where she is studying sports administration. In November 2021, she was contacted by a "friend" on Instagram Messenger. The friend told her that she had made a lot of money trading in cryptocurrency and withdrew her earnings. She sent Hunter some links and other information about the cryptocurrency investment, and it appeared legitimate. The friend recommended an app to buy cryptocurrency, and Hunter did some research to show that the app was legitimate. So Hunter bought about $4,000 in Bitcoin and transferred that to marketmasteroptions.com. The site asked her to create a username and password which allowed her to check her balance at any time. Within a few weeks, she made $35,000 on her investment.

Hunter decided to withdraw her money. She contacted the company, and they told her there was a fee to withdraw the funds. She paid the fees. When she still did not receive her money, she contacted the company again, and was told that she had to pay $2,000 to the company for taxes. Hunter knew this is not how the IRS works, so she refused to pay. She called the IRS, which encouraged her to file a complaint with BBB and law enforcement. Hunter also contacted her friend on Instagram. She learned her friend's Instagram account was hacked and had not talked to Hunter in several months.

Myra is as an accountant in Dallas. In October 2021, she met Jinghua on a dating site; he said he lived in Dallas, but they never met in person. They communicated through WhatsApp. Myra had also invested a little money in Bitcoin before and she had a wallet at Coinbase. Jinghua told her that he invested with cryptocurency and she could make a good return, too.

He sent her a link to an app for investing which she downloaded onto her phone, and he deposited money to her account. There also was a website she could check and she set up a user name and password. As time passed, the website changed its name several times. They impersonated a real company, ItBit by Paxo. She then invested more money for a total of $40,000. Over the next month, she continued to check her account and saw that it increased to $400,000.

Myra decided it was time to withdraw some of her earnings. She communicated with customer service for the site. She learned she needed to pay $70,000 for taxes. She had to send in that amount and it could not come from her earnings. She knew from previous experience in investing that she did not have to pay taxes to the companies but only to the IRS. She didn't pay. Jinghua contacted her and urged her to pay the taxes. She realized that this was a scam and reported this to the BBB and the FTC.



Text message sent to a victim by a scammer

WHAT SCAM TRACKER CRYPTOCURRENCY INVESTMENT SCAM REPORTS HAVE IN COMMON

Most Scam Tracker complaints allege the victim was convinced to invest in cryptocurrency and sent Bitcoin to an investment operation. Victims report these scams have very professional looking websites and look quite legitimate. These sites offer live customer support through chat functions. The sites require usernames and passwords. Victims then use the site to track investment returns, which usually appear to increase dramatically. These sites often impersonate the websites of legitimate cryptocurrency companies and exchanges.

But when victims attempt to withdraw money, they learn they must pay substantial fees for taxes or other purposes to withdraw earnings and cannot use the funds in their accounts for this purpose. Those who pay this additional money are asked to pay still more. Then the original investment vanishes, the "earnings" are nonexistent, and victims lose even more money.

How do scammers develop such professional-looking websites? **Scamadviser** and volunteer scam fighting group **AA419** report there is a huge worldwide underground system that can cheaply create and host fraudulent websites for scammers. These typically claim to be a company registered in the UK, but those registrations are often fake. Registering a real one only costs $17, and the domain names can be purchased for as little as $1. Hosting the websites only costs $2.50. The scam website creators are very prolific, creating fake websites for banking, escrow, and shipping, which they employ in a variety of other frauds.

In January 2019, Facebook and Instagram banned ads for cryptocurrency investments, but the company now allows them. Facebook had been developing its own cryptocurrency system, but abandoned those efforts.

Text message sent from a scammer in response to a request for more information

CELEBRITIES

Cryptocurrency scams on social media often use the names of celebrities to support their claims of legitimacy. Ads on Facebook feature photos of celebrities who supposedly want to share their experiences with cryptocurrency investments. In May 2021, the FTC found people had sent over $2 million in six months to Elon Musk impersonators. Many of these ads promote links to fake websites.

Also in May 2021, Twitter announced that scammers had hacked the Twitter profiles of Joe Biden, Kanye West, Barack Obama and others. The fraudulent tweets sent from these accounts stated "all Bitcoin sent to the address below will be sent back doubled! If you send $1,000, I'll send back $2,000. Only doing this for 30 minutes."

In addition, a UK television investment personality, Martin Lewis, complained to Facebook about thousands of ads on the Facebook site using his name to promote investments without his authority. He eventually sued Facebook, which settled for £3 million, which went to a UK charity that assists consumers. Facebook also set up a dedicated team to handle complaints from the UK about scam ads. More recently, Australian mining magnate Twiggy Forest, the richest man in Australia, pressed criminal charges against Facebook for allowing his name to be used in cryptocurrency scams.

In January 2022, a class action lawsuit was filed against Kim Kardashian, Floyd Mayweather, and several other social media "influencers" alleging they were paid to promote a new cryptocurrency token which subsequently collapsed.

Other celebrities, such as Matt Damon and Reese Witherspoon, endorse presumably legitimate cryptocurrency companies.

HOW SCAMMERS TAKE PAYMENTS WITH CRYPTOCURRENCY

Victims are increasingly asked by scammers to pay using cryptocurrency. Cryptocurrency is popular with scammers because it is quick, easy and hard-to-trace. Many existing scams use cryptocurrency instead of more traditional payments previously used such as Western Union and gift cards. Scammers' requests for cryptocurrency as payment methods are rapidly expanding. The FTC advises: *"Nobody from the government, law enforcement, utility company, or prize promoter will ever tell you to pay them with cryptocurrency. If someone does, it's a scam, every time."*

Fraudulent sales of goods online

Both BBB Scam Tracker and the CAFC report this is the most reported problem by victims who paid by cryptocurrency. There are reports that major retailers are likely to accept payment through Bitcoin in the near future, especially with online purchases. Reports indicate victims who have a wallet and want to buy hard-to-find items, like a PlayStation, are asked to pay with Bitcoin. Once the funds are sent, they are lost forever, and no goods are shipped.

The reports to Scam Tracker about online purchases using cryptocurrency reported are primarily about pet scams. In this scenario, a photo of a pet is posted online. Scammers demand a series of payments for air transport, special crates, shots, or care. But no pets are ever delivered.

Advance fee loans

This scam offers loans to individuals and small businesses with poor credit. Once the province of classified ads, these have now moved online. This is the third-most common scam reported to Scam Tracker asking for payment through cryptocurrency.

In these scams victims are offered loans, but the scammer requests money up front for plausible reasons such as insurance. Victims send money for these fees, but no loan ever appears.

Employment scams

This is the second-most common scam reported to BBB Scam Tracker and the CAFC. These scams take two forms.

In one scam, people respond to employment ads for positions like "Financial Transfer Agent." But the job is really laundering money, receiving and cashing out Bitcoin, and otherwise handling money as a "money mule." It is unlikely that they will ever be paid for their work.

Another employment scam uses fake checks and is the subject of another BBB study. These scams offer people jobs working from home. They are told to pay a third-party for a laptop, phone, or software to perform the job. The scammers provide the victim with a business check to pay for the equipment. The victim deposits the check and the bank credits the funds to the account. At this point the victim feels protected because they believe the check has cleared and they have the money. Victims then send money to the third-party. Scammers now ask victims to send this money by cryptocurrency. The check is counterfeit, the bank removes the funds from the victim's account and no equipment is ever shipped.

Extortion scams

A common scam involves email messages sent directly to individuals claiming that the sender hacked their computer and has video of them watching pornography. The scammers threaten to broadcast this to friends and family and support the hacking claims by providing an old password the victim has used. It is a bluff. They simply have an old file of passwords from a prior data breach and no consequences ever follow from failure to pay. The CAFC received 5,815 reports of this type of scam in 2020.

Government impostors

One of the most frequent contacts people have with scammers is through calls claiming to be from Social Security or the IRS (Service Canada or Revenue Canada in Canada). Callers claim the victim's Social Security Number is suspended because it is tied to a murder or drug theft. Victims talk to someone claiming to be a criminal investigator who says their bank accounts will be frozen. They are advised to protect their funds by transferring them to a "safe" account with the government. Scammers threaten to arrest the victim immediately if they hang up. Read BBB's study on government imposter scams.

Increasingly, these scammers ask for payment with cryptocurrency. The FTC reports that in 2021, it received 1,392 complaints about cryptocurrency used in government impostor scams with losses of $22,510,938. The CAFC reports that in 2020 it received 2,890 complaints about this fraud, with losses reported of $1,361,737.

Other scams

There are recent reports of victims asked to pay taxes by cryptocurrency to receive lottery winnings, pay for tech support work -- remoting into a computer, finding "problems" that do not exist, and demanding money to fix them -- and for payments to be eligible for free government grants, which never materialize. In addition, the FBI warns that payment is requested in cryptocurrency by scammers impersonating a legal office or a utility company.

RANSOMWARE

This is the scam that is most troublesome to governments. With the growth of Bitcoin, ransomware exploded in recent years. Often a hospital, school system, local government or major corporation fall victim to it. When malicious software is installed on the computer system, it allows these frauds to encrypt all data on the computer system, making it gibberish. Victims receive a popup telling them how to contact the fraudsters to pay the ransom and recover the data. Payments are almost always made through Bitcoin, and the scammers walk victims through the steps in making payments. A video by McAfee explains how this works.

In 2020 the IC3 received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million. Not all ransomware situations are reported to the IC3. These figures do not reflect the costs of business disruption and recovery, which can easily exceed the cost of the ransom itself. One study by Chainalysis found ransomware costs globally increased 311% in 2020 to $350 million in cryptocurrency.

Some ransomware operations perform the full range of "services," installing malware, encrypting files and collecting the ransom. But these scams have now developed ransomware as a service (Raas). One set of parties develops the encryption software and may receive ransom and decrypting files. But the ability to spread malware is being franchised. The encryption enterprise takes 20% to 30% of the ransom that is paid. This allows far more enterprises to attack computers.

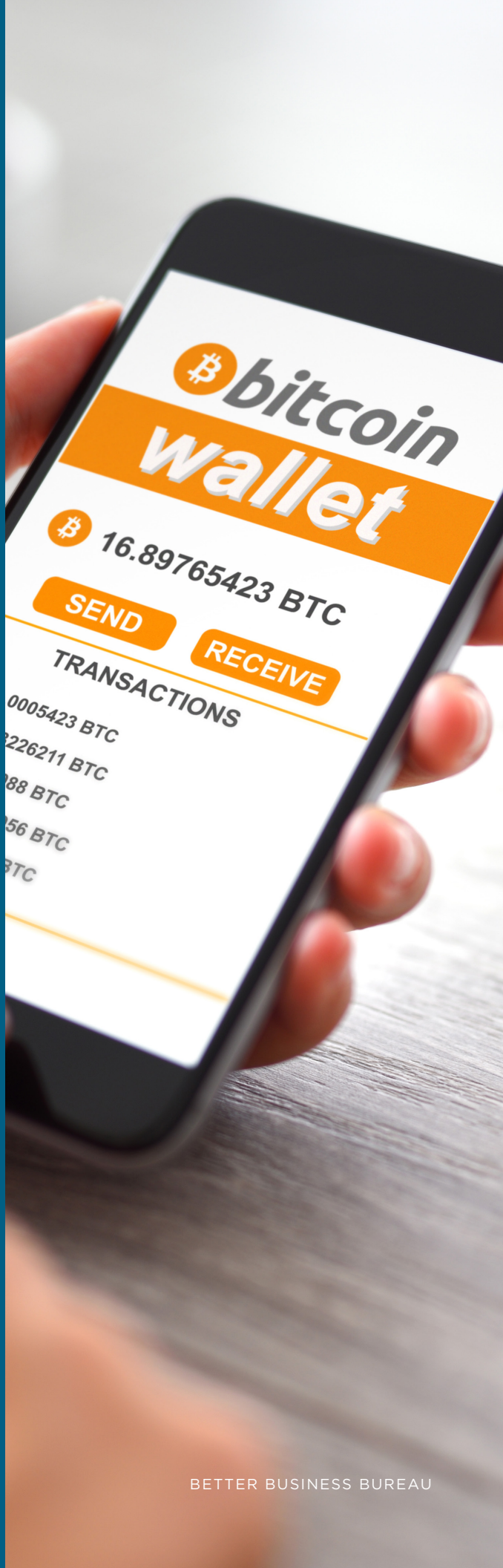
In addition, many believe that some governments are developing and employing ransomware as a cyberattack. The goal of the ransomware may not even really be designed to collect ransom. For example, Symantec says it is "highly likely" North Korea was behind the WannaCry ransomware attack. Total money paid as ransom in WannaCry attack, was only $50,000 — but there were billions more in damages. Similarly, experts believe Petya ransomware was an attack, not really an effort to obtain ransom.

The main way of transmitting a virus is through email attachments, some of which appear safe, but have a virus contained in a PDF or Word document. There are also reports of scammers attempting to bribe employees to install ransomware on systems. For example, a Russian man was recently convicted of trying to bribe an employee of Tesla to install ransomware. Reports indicate that bribery attempts are increasing. Scammers have also begun mailing USB devices to organizations, which insert them into a device to learn what they are and why they were sent and then become infected or spread a virus throughout the company's network.

Ransoms paid are typically in Bitcoin and presumably traceable through the blockchain, but few ransomware scammers have been prosecuted. Recently, however, the FSB in Russia busted the group behind the REvil ransomware operation. The U.S. collects all its ransomware resources at Stopransomware.gov.

TIPS TO AVOID CRYPTOCURRENCY SCAMS

- **Guard your wallet.** If you buy cryptocurrency, the security of the wallet is of prime importance. If you lose the key, then your funds are gone permanently.
- **Look carefully at email addresses and website addresses.** Phishing scams often try to trick people into logging in and then capture the log in credentials. Those then can be used to steal money. Looking for an exchange with an internet search engine may lead to fake sites which advertise and impersonate real companies. Be especially careful when viewing these on a phone.
- **Do not pay for products with cryptocurrency.** Be careful if someone asks you to pay with Bitcoin or another cryptocurrency. No one with the government will ever ask for this form of payment.
- **Beware of fake recovery companies.** Scam companies sometimes claim that they can recover stolen money – for a fee. These are usually scammers.
- **Watch out for fake reviews.** Scammers often create fake reviews for their own companies.
- **Be wary of celebrity endorsements.** It can be tempting to rely on a prominent figure who has invested in cryptocurrency. But those endorsements are often not authorized and even if they are, the celebrity may be paid for the effort and may not know more about it than you do.
- **Be careful about claims made on social media.** This is the most common place for people to encounter investment scams.
- **Be wary of "friends" who reach out to you on social media** and tell you how they made money with cryptocurrency. Accounts are frequently compromised. Call your friend by phone to see if it is really them.
- **Only download apps from Google Play or the App Store.** Trusted app stores do not eliminate the threat of app scams, but they do offer a basic level of protection. Be careful with apps. Some contain malicious software.
- **Do not believe promises of guaranteed returns.** No one can guarantee how an investment will perform.
- **Seek help and support.** Cybercrime Support Network offers a free, confidential support program for romance scam survivors.



WHERE TO REPORT A SCAM OR REGISTER COMPLAINT

Better Business Bureau — file a complaint with your local BBB at BBB.org if you lost money or report a scam online at BBB.org/scamtracker.

Federal Trade Commission (FTC) — file a complaint online at reportfraud.ftc.gov or call 877-FTC-Help.

Internet Crime Complaint enter (IC3) — file a complaint online at ic3.gov/complaint and include:

- **All transaction IDs**
- **Where you sent your crypto from (private wallet, account at exchange X, etc.)**
- **Where you believed you were sending your funds (perpetrator's private wallet, arbitrage account, etc.)**
- **Any details regarding the scam and scammers.**

Canadian Anti-Fraud Centre — file a report online at antifraudcentre-centreantifraude.ca or call 1-888-495-8501.

U.S. Securities and Exchange Commission — SEC.gov/tcr

RECOMMENDATIONS

- **Social media should do more to:**
  - Prevent hijacking of profiles
  - Stop scam advertisements for cryptocurrency investment schemes
  - Prevent the illegal use of celebrity names to promote cryptocurrency scams
- **Regulators should carefully monitor Bitcoin ATMs to prevent use by scammers.**
- **BBB, media, trade groups and government agencies should continue to educate the public about risks.**
- **U.S. Department of Treasury and security regulators should provide stringent oversight and regulation of cryptocurrencies.**

About BBB

BBB is a nonprofit organization that sets and upholds high standards for fair and honest business behavior. Most BBB services to consumers are free of charge. BBB provides objective advice, free BBB Business Profiles on more than 5.3 million companies, 11,000 charity reviews, dispute resolution services, alerts and educational information on topics affecting marketplace trust.

BBB's mission is to be the leader in advancing marketplace trust. It accomplishes this by:

- **Setting standards for marketplace trust**
- **Encouraging and supporting best practices by engaging with and educating consumers and businesses**
- **Celebrating marketplace role models**
- **Calling out and addressing substandard marketplace behavior**
- **Creating a community of trustworthy businesses and charities**

Acknowledgments
This study was a joint project of Better Business Bureaus of Chicago, Dallas, Omaha, San Francisco and St. Louis. Contributions include data from BBB Scam Tracker, BBB Institute for Marketplace Trust, IABBB and various regulatory agencies.

BBB International Investigations Initiative contact information
BBB Chicago — bbbinfo@chicago.bbb.org
BBB Dallas — info@nctx.bbb.org
BBB Omaha — info@bbbinc.org
BBB San Francisco — info@bbbemail.org
BBB St. Louis — bbb@stlouisbbb.org

By C. Steven Baker, BBB International Investigations Specialist stbaker@bbbinc.org

Find more information about this study and other BBB scam studies at BBB.org/scamstudies

All images courtesy of Getty Images unless otherwise noted.