



# What To Know About Cryptocurrency and Scams

Confused about cryptocurrencies, like bitcoin and Ethereum? You're not alone. Before you use or invest in cryptocurrency, know what makes it different from cash and other payment methods, and how to spot cryptocurrency scams or detect cryptocurrency accounts that may be compromised.

- [What To Know About Cryptocurrency](#)
- [Paying With Cryptocurrency](#)
- [How To Avoid Cryptocurrency Scams](#)
- [How To Report Cryptocurrency Scams](#)

## What To Know About Cryptocurrency

### What is cryptocurrency?

Cryptocurrency is a type of digital currency that generally only exists electronically. There is no physical coin or bill unless you use a service that allows you to cash in cryptocurrency for a physical token. You usually exchange cryptocurrency with someone online, with your phone or computer, without using an intermediary like a bank. Bitcoin and Ether are well-known cryptocurrencies, but there are many different cryptocurrency brands, and new ones are continuously being created.

**Cryptocurrency Scam** 

**If you see a tweet** (or a text, email, or other message on social media) **that tells you to pay with cryptocurrency, that's a scam.**

Report scams: [reportfraud.ftc.gov](https://reportfraud.ftc.gov)

The graphic features a dark blue background with a smartphone and a Bitcoin wallet. Several gold Bitcoin coins are shown floating above the phone. A yellow warning triangle with a red exclamation mark is positioned to the right of the title.

## How do people use cryptocurrency?

People use cryptocurrency for quick payments, to avoid transaction fees that regular banks charge, or because it offers some anonymity. Others hold cryptocurrency as an investment, hoping the value goes up.

## How do you get cryptocurrency?

You can buy cryptocurrency through an online exchange platform. Some people earn cryptocurrency through a complex process called “mining,” which requires advanced computer equipment to solve highly complicated math puzzles.

## Where and how do you store cryptocurrency?

Cryptocurrency is stored in a digital wallet, which can be online, on your computer, or on an external hard drive. But if something unexpected happens — your online exchange platform goes out of business, you send cryptocurrency to the wrong person, you lose the password to your digital wallet, or your digital wallet is stolen or compromised — you’re likely to find that no one can step in to help you recover your funds. And, because you typically transfer cryptocurrency directly without an intermediary like a bank, there is often no one to turn to if you encounter a problem.

## How is cryptocurrency different from U.S. Dollars?

There are important differences between cryptocurrency and traditional currency.

- **Cryptocurrency accounts are not backed by a government.** Cryptocurrency accounts are **not** insured by a government like U.S. dollars deposited into a bank account. If you store cryptocurrency with a third-party company, and the company goes out of business or is hacked, the government has no obligation to step in and help get your money back.
- **Cryptocurrency values change constantly.** The value of a cryptocurrency can vary rapidly, even changing by the hour. It depends on many factors, including supply and demand. An investment that’s worth thousands of dollars today might be worth only hundreds tomorrow. And, if the value goes down, there’s no guarantee it will go up again.

# Paying With Cryptocurrency

If you're thinking about paying with cryptocurrency, know that it's different from paying with a credit card or other traditional payment methods.

- **Cryptocurrency payments do not come with legal protections.** Credit cards and debit cards have [legal protections](#) if something goes wrong. For example, if you need to [dispute a purchase](#), your credit card company has a process to help you get your money back. Cryptocurrencies typically do not.
- **Cryptocurrency payments typically are not reversible.** Once you pay with cryptocurrency, you can usually only get your money back if the person you paid sends it back. Before you buy something with cryptocurrency, know the seller's reputation, where the seller is located, and how to contact someone if there is a problem. Confirm these details by doing some research before you pay.
- **Some information about your transactions will likely be public.** People talk about cryptocurrency transactions as anonymous. But the truth is not that simple. Some cryptocurrencies record some transaction details on a public ledger, called a "blockchain." That's a public list of every cryptocurrency transaction — both the payment and receipt sides. Depending on the cryptocurrency, the information added to the blockchain can include details like the transaction amount and the sender's and recipient's wallet addresses. A wallet address is a long string of numbers and letters linked to your digital wallet. Even though you can use a fake name to register your digital wallet, it's possible to use transaction and wallet information to identify the people involved in a specific transaction. And when you buy something from a seller who collects other information about you, like a shipping address, that information can be used to identify you later on.

## How To Avoid Cryptocurrency Scams

Scammers are always finding new ways to steal your money using cryptocurrency. **One sure sign of a scam is anyone who says you have to pay by cryptocurrency.** In fact, anyone who tells you to pay by [wire transfer](#), [gift card](#), or cryptocurrency is a scammer. Of course, if you pay, there's almost no way to get that money back. Which is what the scammers are counting on. Here are some cryptocurrency scams to watch out for.

### Investment and business opportunity scams

- Some companies promise that you can earn lots of money in a short time and [achieve financial freedom](#).
- Some scammers tell you to pay in cryptocurrency for the right to recruit others into a program. If you do, they say, you'll get recruitment rewards paid in cryptocurrency. The more cryptocurrency you pay, the more money they promise you'll make. But these are all fake promises, and false guarantees.
- Some scammers start with unsolicited offers from supposed "investment managers." These scammers say they can help you grow your money if you give them the cryptocurrency you've bought. But once you log in to the "investment account" they opened, you'll find that you can't withdraw your money unless you pay fees.
- Some scammers send unsolicited job offers to help recruit cryptocurrency investors, sell cryptocurrency, mine cryptocurrency, or help with converting cash to bitcoin.
- Some scammers list [scam jobs](#) on job websites. They'll promise you a job (for a fee), but end up taking your money or personal information.

Look for claims like these to help you spot the companies and people to avoid:

- **Scammers guarantee that you'll make money.** If they promise you'll make a profit, that's a scam. Even if there's a celebrity endorsement or testimonials. (Those are easily faked.)
- **Scammers promise big payouts with guaranteed returns.** Nobody can guarantee a set return, say, double your money. Much less in a short time.
- **Scammers promise free money.** They'll promise it in cash or cryptocurrency, but free money promises are always fake.
- **Scammers make big claims without details or explanations.** Smart business people want to understand how their investment works, and where their money is going. And good investment advisors want to share that information.

Before you invest, check it out. Research online for the name of the company and the cryptocurrency name, plus words like "review," "scam," or "complaint." See what others are saying. And read more about other common [investment scams](#).

## Blackmail emails

Scammers will often send emails that say they have embarrassing or compromising photos, videos, or personal information about you. Then, they threaten to make it public unless you pay them in cryptocurrency. Don't do it.

This is blackmail and a criminal extortion attempt. Report it to the [FBI](#) immediately.

## Social media scams

If you read a tweet, text, email, or get a message on social media that tells you to send cryptocurrency, it's a scam. That's true even if the message came from someone you know, or was posted by a celebrity you follow. Their social media accounts might have been hacked. Report the scam immediately to the social media platform, and then tell the FTC at [ReportFraud.ftc.gov](#).

## How To Report Cryptocurrency Scams

Report fraud and other suspicious activity involving cryptocurrency to

- the FTC at [ReportFraud.ftc.gov](#)
- the Commodity Futures Trading Commission (CFTC) at [CFTC.gov/complaint](#)
- the U.S. Securities and Exchange Commission (SEC) at [sec.gov/tcr](#)
- the cryptocurrency exchange company you used to send the money