Risks to consumers posed by virtual currencies

What are virtual currencies? And, as a consumer, what risks should you be aware of?

You may have heard about virtual currencies like Bitcoin, XRP, and Dogecoin. You may have heard you can buy them online. In some circumstances, you can send them to other people or use them to pay for goods and services. You may also have heard that some people buy them as speculative investments or that you can "mine" them with your computer.

But what are virtual currencies? And, as a consumer, what risks should you be aware of? In a nutshell, while virtual currencies offer the potential for innovation, a lot of big issues have yet to be resolved – some of which are critical.

If you are interested in using or buying virtual currencies, you should be aware of the associated risks:

- **Hackers.** Virtual currencies are targets for highly sophisticated hackers, who have been able to breach advanced security systems.
- **Fewer protections.** If you trust someone else to hold your virtual currencies and something goes wrong, that company may not offer you the kind of help you expect from a bank or debit or credit card provider.
- **Cost.** Virtual currencies can cost consumers much more to use than credit cards or even regular cash.
- **Scams.** Fraudsters are taking advantage of the hype surrounding virtual currencies to cheat people with fake opportunities.

So before you get involved, it's important to know what can go wrong.

What are virtual currencies?

Virtual currencies are a kind of electronic money. That means when you buy a virtual currency you don't get an actual coin or bill that you can hold in your hands. Instead, you receive electronic units that many people may agree to accept and treat like dollars, euros, or other forms of money.

But virtual currencies aren't regular money. To begin with, virtual currencies are not issued or backed by the United States or any other government or central bank. No one is required to accept them as payment or to exchange them for traditional currencies. To work, they depend on the processing power of vast networks of unidentified, private computers around the world, which maintain and update a public ledger called the "blockchain." (Think of it as a public spreadsheet.)

According to online accounts, after learning about a **Bitcoin exchange** from an internet search, Nicole* transferred cash to a bank account designated by the exchange's representative, Jackson, who she had e-mailed with and even spoken to on the phone. Nicole never received her Bitcoins, however. When Nicole tried to call Jackson again, the line was disconnected.

*All names have been changed.

Further, virtual currencies are not kept in banks or credit unions. In order to use virtual currencies, you need to store them in a "digital wallet," which are identified by your "public keys." To access the virtual currency in your digital wallet, you use "private keys." (Your private keys are random sequences of 64 letters and numbers that should be kept secret; your public keys are corresponding letter/number sequences that everyone can see on the blockchain.) If you want to send someone your virtual currency, for example as payment, you use the private keys to unlock your digital wallet.

In many ways, your private keys **are** your virtual currency so keeping your private keys secret is critical to owning and using virtual currency. You can store and protect your private keys yourself or entrust them to a company called a wallet provider to protect them for you.

You can learn more about how virtual currencies work at http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html. And before you decide to use virtual currencies, here are some of the things you should consider:

If you are buying virtual currencies

Know who you're dealing with if you decide to buy.

If something goes wrong with your purchase of virtual currencies, do you know how to contact the seller? Some virtual currency exchanges do not identify their owners, their phone numbers and addresses, or even the countries where they are located. Ask yourself: In any other business transaction, would you trust these people with your money? Do you know what your contractual rights would be (or how you would enforce them) if the seller doesn't deliver what you purchased?

Virtual currency exchanges, including those using kiosks, are required to register with the Financial Crimes Enforcement Network—which is part of the U.S. Treasury Department—as money services businesses.

Before you do business with an exchange, you can verify that it has registered by checking www.fincen.gov/financial_institutions/msb/msbstateselector.html.

(Note, though, that though it is illegal for a virtual currency exchange to operate without registering with FinCEN, the registration does not, on its own, mean that an exchange is trustworthy.)

Exchanges may also need to be licensed with your State as money transmitters or currency exchanges. You can check with your State's financial regulators to make sure that an exchange is licensed.

Understand what the actual costs will be.

For example, do you know what the relevant exchange rate will be and how it was determined? Are there any mark-ups to the exchange rate or other fees? How long will the transaction take to complete? Do you know what will happen if rates change before the exchange is made?

Bitcoin "ATMs" are not ATMs at all.

Bitcoin kiosks are machines, connected to the Internet, that allow you to insert cash in exchange for Bitcoins (which they can give you as a slip of paper or by moving money to your public key on the blockchain). They may look like traditional ATMs, but unlike ATMs that you may associate with your checking and savings accounts, Bitcoin kiosks do not connect to your bank and may lack many of the safeguards you would expect. They may also charge high transaction fees – media reports describe transaction fees as high as 7% and exchange rates $50 over rates you could get elsewhere.

Be prepared to weather very large price fluctuations.

In 2013, Bitcoin's price fell as much as 61% in a single day. In 2014, the one-day price drop has been as big as 80%.

Virtual currencies are still experimental.

Virtual currencies, like Bitcoin, are still in active development. There are big issues that have yet to be resolved. In particular, the critical component of the entire system—the public ledger known as the blockchain—is maintained by vast unidentified private computer networks spread all over the world. It is possible that elements of these networks could abuse the power that comes with maintaining the ledger, for example by undoing transactions that you thought were finalized.

If it seems too good to be true, it may be.

Many criminals have seized upon the press and enthusiasm relating to virtual currency to create new versions of old scams. In early 2014, the U.S. Securities and Exchange Commission sued the organizer of an alleged Ponzi scheme in Texas that purportedly advertised an "investment opportunity" that promised up to 7% interest per week. Instead, invested Bitcoins were allegedly used to pay existing investors and the organizer's personal expenses. Like any other investment, do your due diligence before giving someone money. The U.S. Securities and Exchange Commission has issued important warnings about virtual currency investment scams, which you can read at www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf and www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html.

Bitcoin transactions may not be entirely anonymous.

Information about each and every Bitcoin transaction is publicly shared and stored forever. Persistent, motivated people will likely be able to link your transactions to, among other things, your other transactions and public keys, as well as to your computer's IP address. So it is possible that others will be able to estimate both how much Bitcoin you own and where you are.

If you store virtual currencies by yourself

You can be hacked.

If you use virtual currency, the data on your computer or phone can be an attractive target to hackers. If someone gets access to your computer (for example, using a "Trojan Horse" virus or other malware), they can get your private keys and, thereby, steal your virtual currency.

You are on your own.

With a traditional bank account or payment card, if someone breaches your account, your bank or payment card company will help you recover some or all of your funds. If you're storing your virtual currencies on your own computer, you're basically on your own if your virtual currency is stolen. There is no other party to help you.

If you lose your private keys, you've lost your funds forever.

If you store your virtual currency yourself, you can lose your funds without being hacked. If you lose your private keys, you have lost all access to your funds. No one can help you with password reminders and no one will refund your loss. Some people store their private keys offline on a USB key, external hard drive, or even paper. But if they haven't made a backup copy and they lose that USB key, hard drive, or piece of paper (or spill a glass of water on it), they lose those funds forever.

According to news reports, James mistakenly discarded a computer hard drive containing his **private keys** for 7,500 Bitcoin in 2013. As of July 2014, that amount of Bitcoin was valued at nearly $5 million. James didn't back up the drive and has not been able to locate the drive at the city dump. Consequently, he has lost all his funds.

If you trust someone else to store your virtual currencies

The government does not insure virtual currency accounts (or "wallets").

The Federal Deposit Insurance Corporation or the National Credit Union Share Insurance Fund typically protects your funds if a bank or credit union fails. But this doesn't apply to virtual currency accounts. So, if an exchange or wallet company fails—and many have failed—the government won't cover your losses.

According to media accounts, Kat had Bitcoin valued at nearly $10,000 stolen from an account she maintained with a major Bitcoin company. When it happened the first time, they refunded her money. When it happened again a month later, they told her that she didn't qualify for a refund.

The same media accounts note that when Larry had $5,000 worth of Bitcoin stolen, his hosted wallet company would not help him with a refund because Larry hadn't set up their strongest security settings.

You still have to be prepared to protect yourself from hackers.

Are you using your wallet provider's recommended practices on securing your login and password? Are you careful to avoid sharing your access credentials, inadvertently or otherwise? Watch out for fake websites or e-mails that may try to trick you into turning over your login and password, by mimicking your wallet's website (sometimes referred to as "phishing" or "smishing"). The Federal Trade Commission offers useful additional information about phishing scams at www.consumer.ftc.gov/media/game-0011-phishing-scams.

Even if you use best practices, anything that connects to the Internet—even big companies—can be hacked.

Do you know how your wallet company stores its customers' virtual currencies or if their security systems have been audited? There have already been numerous reports of hackers successfully getting access to peoples' phones and computers, allowing them to bypass systems that require both forms of identity authentication.

If you have linked your bank account or payment card to your digital wallet, they may also be at risk.

Hackers that compromise your digital wallet account may not just empty it of your virtual currency – they may also pull funds (like U.S. dollars) from your traditional bank account if you have linked it to your digital wallet.

Read your agreement with your wallet provider carefully.

With a traditional bank account or payment card, the bank or payment card company will generally return your funds or reverse your charges if someone makes an unauthorized transfer from your account. In contrast, virtual currency wallet companies may disclaim responsibility for replacing your virtual currency if it is stolen on their watch.

Really, read your agreement with your wallet provider carefully.

If your wallet company does promise to reimburse you for unauthorized transactions, will they make the refund in virtual currency or U.S. dollars? What happens if there's been a big exchange rate increase or decrease in the interim – who gets the benefit of the difference in exchange rates, you or your wallet provider? If your wallet provider offers insurance, what exactly does the insurance cover and what does it provide when the coverage applies?

In February 2014, Japanese Bitcoin exchange Mt. Gox froze customers' Bitcoin accounts and the Mt. Gox website disappeared, as was widely reported in the news. Shortly thereafter, Mt. Gox announced that it had lost almost $400 million of customer funds, which was nearly 6% of all Bitcoin then in circulation. Customers' only recourse was to file claims in Mt. Gox's later bankruptcy proceeding. To date, customers have not recovered any of the missing funds.

If you use virtual currencies to pay for things or send funds to other people

Mistakes can be extremely costly.

When using virtual currencies to pay for goods or services, if you don't enter the recipient's 64-character public key perfectly, you will send the funds to the wrong person. If you're not using a hosted wallet provider (a service that helps manage your private keys), there's no mechanism for stopping the payment or getting the money back. And if you do use a hosted wallet provider, the provider may disclaim responsibility for helping you get your funds back.

Virtual currencies don't have status as legal tender in any jurisdiction.

No party is required by law to accept payment in virtual currencies. While the number of stores and online retailers that accept virtual currencies as payment is increasing, the current universe is still very limited.

Also, the tax treatment can be complicated. If you spend (or sell) your virtual currency, you have to keep track of your taxable gains (and possibly your losses) so you can report them on your tax filings. The Internal Revenue Service has issued important guidance relating to virtual currencies, which you can access at www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance.

If you pay for things with virtual currencies, know how the merchant does business.

If you buy something with virtual currency you may be paying more than you would pay if you paid in dollars. Know how the merchant sets its exchange rate and look for mark-ups or other fees. Further, not all merchants that accept virtual currency have policies outlining guarantees for consumers when purchases go wrong. If you request a refund, are they going to reimburse you in virtual currency or U.S. dollars? Again, who gets the benefit of a large exchange rate spike or drop in the interim – you or the merchant?

If you encounter a problem with virtual currency or a virtual currency company, let us know. Submit a complaint online at www.consumerfinance.gov/complaint. Submitting a complaint takes only a few minutes.