Techlicious

Bitcoin 101: Understanding the Basics

By Natasha Stokes
November 03, 2014

You may have read about the hackers who made off with $406 million worth of the virtual currency bitcoin. And perhaps you've heard of bitcoin's skyrocketing and plummeting values, often within a two-day window.

Though it's been associated with the murkier depths of the online world, bitcoin digital currency is edging into the mainstream as U.S. authorities and big business start to recognize this virtual asset. This month, the Commodity Futures Trading Commission met to discuss bitcoin regulation. The New York Department of Financial Services is already working on BitLicense regulation for bitcoin businesses.

Retailers from Dell to Home Depot now accept bitcoin, and a raft of services are springing up to make using bitcoin as simple as sending email. The question is, is using bitcoin a smart move for you?

Bitcoin basics

Bitcoin allows direct payments between two individuals without a middleman such as a bank, credit card company or PayPal. Cutting out a centralized authority creates one of the currency's defining features: near-complete anonymity when making payments online.

Bitcoin payments are also an attractive alternative for international transfers. Without an intermediary, the costs involved in sending money are reduced, and payments can be instant.

Bitcoin's significance extends beyond this, though. It's been hailed as the first feint at digital cash. Civil liberty advocates support its ability to maintain financial privacy. For early adopters, it's a high-risk, high-return investment as well as a better way to make anonymous online purchases.

"The technology of bitcoin and the possibilities it raises are quite intriguing," says economist George Selgin, director of the Center for Monetary and Financial Alternatives at the Cato Institute, an independent think tank based in Washington, D.C. "This is a potential money that could provide a safe, sound medium of exchange that is independent of any government."

How bitcoins are created

New bitcoins are produced by a vast network of computers that whir away at cracking difficult math problems in order to validate other bitcoin transactions. Bitcoin is known as a cryptocurrency because encryption techniques are used to create bitcoins and to exchange them. Every transaction is added to a public ledger called the blockchain. The process of running a program to solve these problems is called mining.

An algorithm that controls the complexity of the math problems to be solved caps the total number of bitcoins produced at 21 million. The closer the total bitcoins mined comes to 21 million, the more complex the math problems that are created and the more processing power computers need to solve them.

When the first bitcoins were mined in 2009, a personal computer could have turned out a couple of hundred bitcoin in a few days.

Today, 13.36 million bitcoins have been mined, or 64% of the total supply. Miners need customized rigs designed to do nothing but solve blocks of bitcoin problems. Miners usually join forces with a pool of other miners. A reward of 25 bitcoins goes to the miner or mining pool that solves a block first, something that occurs roughly every 10 minutes.

Where to get bitcoins

Unless you can afford a specialized computer for mining bitcoins (and are technical-minded enough to tend to it), this DIY approach to scoring them isn't an option. Luckily, a nascent infrastructure has sprung up around the bitcoin currency, with numerous providers helping you buy, sell, store and spend bitcoins.

To buy bitcoins, you need a virtual wallet. This wallet is a string of text that people can use to send you bitcoins. It's a bit like a bank account number; the only difference is that it isn't linked to any identifying information about you.

Signing up for a wallet is as easy as signing for a new email account. All you need is an email address to receive a verification link.

Blockchain, used by 2.3 million bitcoin holders, recently raised over $30 million in funding from investors including Virgin Group founder Richard Branson.

Coinbase is both wallet and bitcoin exchange. It can link to your bank account and, for a 1% fee, act as your proxy to exchange dollars for bitcoins.

Once you have a wallet, you can go to an exchange site such as LocalBitcoins, BitStamp or CoinCafe to purchase some bitcoins. Depending on the site and the seller, payment can be made by bank transfer, money order or even cash in person. Sellers often stipulate a minimum amount of bitcoins per sale – at least 0.1 bitcoins, which cost roughly $33 at the time this article was published. Transactions normally complete minutes after the payment clears.

Dozens of U.S. cities now have bitcoin ATMs that will take cash and convert it into bitcoins deposited into your virtual wallet. Using these ATMs requires a fair amount of verification, including handprint scanning and a government-issued ID card. If you want a simple, immediate way to turn dollars into bitcoins, though, this is it.

Where to spend bitcoins

“Merchants recognize that there is a market out there of devoted users,” Selgin says.

According to Coinmap.org,

3,300 shops in North America accept bitcoin payments, including law offices, restaurants and a Roman Catholic church.

You can spend your bitcoin online on a computer from Dell, discount department store goodies at Overstock.com or electronics from Newegg.com. Virgin Galactic accepts bitcoin to pay for its space flights, or you can gamble away your bitcoin fortune at the Cloudbet online casino and sports bookie.

Other services act as a gateway to major retailers that don't have much incentive to offer a payment method that’s still employed by only a small section of society. eGifter allows customers to buy giftcards in bitcoin that can be spent via iOS/Android app at major retailers including Home Depot, Kmart and CVS, with a loyalty point reward for using the cryptocurrency.

Similarly, Gyft sells gift cards that can be used at retailers like Target, Victoria's Secret and Amazon. It accepts bitcoin as a payment method and offers a 3% discount when bitcoin is used.

So why the incentive for customers to pay by bitcoin? “We don't have to worry about credit card fees or costs from fraud chargeback,” says Gyft CEO Vinny Lingham. Unlike credit cards or PayPal, bitcoin payments can't be reversed if customers dispute a charge.

And where credit card companies take a 3% processing fee, merchants accepting bitcoin can use bitcoin processors such as BitPay, which doesn't charge for transactions. BitPay also allows retailers to cash out immediately to bank accounts, protecting them from the currency's notorious fluctuations.

What makes a secure bitcoin wallet

If your computer or phone is hacked, thieves can steal all your bitcoins simply by copying the string of text identifying your wallet and its decryption key. Whoever has this information can spend the bitcoins, just like stolen paper money.

“The blockchain [public ledger of transactions] only registers which bitcoin amount is in which wallet, not who owns the wallet,” says Sophos senior security advisor Chester Wisniewski. So it's imperative to use a bitcoin wallet that requires at least one offline means of logging in, making it more difficult for online thieves to hack in.

“Before trusting a bitcoin wallet with my bitcoins, I'd make sure it offers good encryption with a second factor authentication,” Wisniewski says. “The less convenient it is to access, the more secure it generally is.”

It's a good idea to hold mulitple wallets. Use one for daily trading that contains only some of your total holdings and is quicker to log into, with the rest in a wallet that is held offline, or in “cold storage”.

For example, BitStash generates three tiers of virtual wallet – one that is encrypted on your mobile to contain small amounts for quick spending; another that is stored on a BitStash authentication device Bluetooth paired to your computer; and a third stored on a USB drive that is only accessible when plugged into the BitStash. Since it's offline, it's not hackable. Plus, BitStash holds a backup of all the wallets, so if you lose the data on the other devices, you haven't lost all your bitcoins. (Take the unfortunate incident of the man who tossed a USB stick with $7.5 million worth of bitcoins that he'd mined in 2009.)

Similarly, Xapo offers a mobile wallet app, an additional vault option with multi-factor authentication and even a debit card linked to your bitcoin account. In the event of a hack, you could reclaim the value of your loss, as vaults are insured by the Meridian Insurance Group for an annual fee of 0.12% of your deposit.

An insured option with no annual fee is Circle, which provides a mobile or desktop wallet with two-factor authentication.

Bitcoin – not quite digital cash yet

Though Bitcoin has drawn many comparisons to digital cash, it's not entirely untraceable. ”Many people think that Bitcoin is more private than it actually is,” says Rainey Reitman, activism director at the Electronic Frontier Foundation.

Because all transactions are public in the blockchain, it's possible to track the payments made and received by a particular wallet and build a profile based on where bitcoins are spent, especially if they happen to be spent at a real-world retailer or cashed out to a bank account.

That's not to say you can't make transactions much harder to track.“You could a create new wallet for every transaction, transferring only the payment amount,” Wisniewski says.

Bitcoin laundering sites, called tumblers, anonymize bitcoin transactions by collecting pools of bitcoin amounts and mixing them up before sending them on.

DarkWallet, a wallet app currently in development, also launders your coin by mixing up your transaction amounts with those of other DarkWallet users before sending them off.

The benefits of Bitcoin

Digital currencies such as Bitcoin have the potential for truly private online trading. “There are benefits to having certain transactions take place without having a huge long data shadow behind you,” says Reitman.

Paying for goods or services online with credit or debit cards means sensitive info is stored in the databases of retailers and banks that have been hacked, and yet another facet of your online behaviour painted into a profile for advertisers to track.

Paying by bitcoin can be a boon when making purchases you don't want appearing on your credit card statement; or for public figures wishing to donate to controversial organizations privately.

For digital rights advocates, it's also a means to push back against heavy-handed censorship by banks or other financial intermediaries. “Paypal, Visa and Mastercard shut down transactions to the website Wikileaks even though Wikileaks was not charged with a crime,” Reitman says. “But you could always transfer bitcoin, because there's no PayPal or Visa intermediary that needs to approve it.”

As an investment, entrepreneurs and speculators believe the currency will offer great return. “I think there will be another three or four years of volatility but the trend is upwards,” Gyft's Lingham says. At its height in December 2013, a single bitcoin was worth US$1,151. It’s since plummeted, with the value of a single bitcoin worth $329 at the time of publishing.

“The bitcoin currency will be volatile as long as a big proportion of transactions continue to come from the black market,” Wisniewski says. For example, when the founder of online black market Silk Road was arrested and his stash of 144,000 Bitcoins (worth US$28.6 million at the time) auctioned off by FBI officials, the value of a Bitcoin fell to $560 from around $670 earlier that month, due to a loss of confidence in the privacy of Bitcoin, Wisniewski says.

Should you buy bitcoin?

“Buying bitcoin remains a very risky proposition,” Selgin says. Many bitcoin owners are speculators, whowant return, not stability. This makes the currency more volatile as speculators will buy or sell in anticipation of spikes and dips, thus causing sharp fluctuations.

However, as more retailers open up to bitcoin, its value could steady. “The more that legitimate purchases like coffee, clothing or games outweigh the non-legitimate, the more stability that will bring,” Wisniewski says.

Perhaps as significant is the use of bitcoins as a privacy-friendly alternative to corporate banking. “People should think about the fact that as we become an increasingly digital world, we have less and less financial privacy,” Reitman says. “Bitcoin has the potential to reinstate that privacy.”

In many African countries, where there is a paucity of banking services, bitcoin is a low-barrier way to send and receive money. In Venezuela, where currency controls make it hard to get cash, bitcoin is rising as a medium of trade.

However, Selgin doesn't believe Bitcoin can or will be the digital currency that the world uses. “If bitcoin were universally treated as a medium of exchange, the growth in demand for it could only be accommodated by deflation because of its limited supply [at 21 million],” he says. “Prices denominated in bitcoin units would have to fall so that each bitcoin can command more purchasing power.” That's great for speculators, but not for anyone who wants to be able to depend on using bitcoins to buy or sell things.

Instead, Bitcoin is paving the way for a future digital currency that can offer all its benefits with some of its wrinkles ironed out. “We're at an early stage of digital currency,” Selgin says. “The progress of bitcoin shows experimental currencies could get far.”

Other digital currencies such as Dogecoin and Litecoin are worth less and are easier to mine, but are less widely accepted – for now.

“There's definitely the potential for the widespread adoption of digital currency as long as more innovative services are offered – and if governments don't try to over-regulate this industry,” Reitman says.

There's no guarantee that bitcoins will be worth anything in a few years (or that they won't!), and you may never be able to spend them at your local coffee shop. But, as the first step towards global digital money, Bitcoin is blazing a path.