WHY ON EARTH DO PEOPLE USE BITCOIN?

Catherine Martin Christopher*

I. INTRODUCTION .......................................................... 2
II. DISCUSSION .............................................................. 3
   A. Speculation/Investment .............................................. 3
   B. Trust in Algorithms ............................................... 5
   C. Spending Power .................................................... 7
   D. Money Laundering .................................................. 8
III. CONCLUSION ............................................................ 10

ABSTRACT

Bitcoin is making near-daily headlines, whether about its volatile exchange rate, the regulatory issues it raises, or its criminal associations. As the public becomes familiar with the idea of virtual currencies, many people struggle to understand why users exchange government-backed (“real”) currencies for Bitcoin. This article explores the appeal and danger of investing in Bitcoin for speculative gain, for moral purposes, for its spending power, and for its criminal applications.

* Assistant Professor, Texas Tech University School of Law. J.D., University of Pittsburgh. The author wishes to thank Eric A. Chiappinelli and Steven I. Friedland for their advice and friendship in the writing of this piece.
I. INTRODUCTION

Since I began reading, writing, and speaking about Bitcoin, I often find myself describing it to people who’ve never heard of it. “It’s a digital currency,” I explain. “It exists solely on the Internet. It’s not backed by any government, or a company, or by the price of gold. It’s a computer code that’s run on thousands of computers, all networked together over the Internet.

“The code solves a series of math problems,” I continue. (I have my spiel pretty well down by now.) “All the computers networked together work to solve these really complicated math problems, and the solution to each problem is a long string of letters and numbers that is a bitcoin.” Once a bitcoin is generated, it is randomly awarded to one of the computers in the network, and the code starts in on solving the next math problem.”

I then explain “mining” versus buying: “If you want to, you can download the Bitcoin software onto your computer and contribute your computing power to solving the math problems. You might do this in the hopes of being rewarded with a bitcoin once it’s generated. That’s called ‘mining’ for bitcoins. But it would probably take you a couple of years to mine a bitcoin from your home computer, so if you don’t want to wait that long, you can just buy some from a website—a digital currency exchange.” You give them dollars, and they give you bitcoins.

If I’m really testing the boundaries of Bitcoin newbies’ patience, I’ll also throw in, “You may have heard of a big FBI bust of a website called Silk Road in early October 2013. Silk Road was a website that matched up buyers and sellers—kind of like eBay, except that there were illegal drugs and weapons for sale—so long as the parties transacted in Bitcoin. Silk Road used Bitcoin because a Bitcoin account doesn’t have a name attached to it.”

Plenty of people look pretty shell-shocked by this point in my talk, so this is where I usually pause for questions. “People spend real money on

---

2. The capitalized word “Bitcoin” is typically used to refer to the currency system as a whole, but the un-capitalized word “bitcoin” refers to the units of virtual currency.
5. See id.
7. See id.
8. See id.
WHY ON EARTH DO PEOPLE USE BITCOIN?

Why on earth do people use Bitcoin? Why bother mining for bitcoins? Why exchange your salary or savings for an intangible digital currency—an intangible currency with a wildly fluctuating exchange rate and criminal associations, to boot?

II. DISCUSSION

A. Speculation/Investment

Many individuals invest in Bitcoin specifically to take advantage of its price fluctuations. The old standby of “buy low, sell high” applies to Bitcoin as well as it does to anything else, and plenty of people buy bitcoins because they believe that the current price is less than the price will be in the future. For example, Kristoffer Koch spent about $27 in 2009 to buy 5,000 bitcoins, which increased to $886,000 by late 2013.

The Winklevoss twins (vilified in the movie The Social Network for suing Facebook founder Mark Zuckerberg) own a large share of bitcoins, seeking to gain a return on their investment as the value and usage of

Bitcoin expand in coming years. They announced in April 2013 that they owned about $11 million in bitcoins, which at the time were valued at approximately $165 apiece. To do a back-of-the-envelope calculation, that means they owned about 66,667 bitcoins. Assuming they still held that number when the price of bitcoins reached $1,124.76 on November 30, 2013, their holdings were worth $75 million.

Income earned from Bitcoin transactions is presumably taxable, though the Internal Revenue Service is struggling to identify and explain Bitcoin-derived tax liability to taxpayers.

Of course, there are risks involved in using Bitcoin as a speculation or an investment vehicle beyond the obvious possibility that the price of Bitcoin will go down instead of up.

Bitcoins are susceptible to theft, via good old-fashioned hacking. Hackers can obtain a Bitcoin user’s private key (akin to an ATM PIN) and use it to transfer some or all of the bitcoins in the user’s digital wallet (e-wallet) to another location. The private key is a validation process to ensure that Bitcoin transactions are authorized, but there is no way to ensure that the e-wallet’s owner is the one doing the authorizing. The potential for hacking is not helped by the facts that (1) encryption and protection of an e-wallet is left to the user, and (2) transactions are irreversible. Just as with physical cash, once bitcoins have been stolen, they are effectively untraceable and unreturnable.
Along with theft of bitcoins, hacker attacks on digital currency exchanges drive down the price of bitcoins across the system. If bitcoins can be stolen, or if transactions cannot be completed, what is a bitcoin worth? A massive hacker attack on Mt. Gox (formerly the currency’s largest exchange) in June 2011 resulted in the theft of 25,000 bitcoins, valued at the time at approximately $8.75 million, which drove the exchange value of a bitcoin from $17.50 to a single penny.

After all, without the backing of a government or other guarantor, bitcoins have no intrinsic value; bitcoins are valuable only because users believe they are, just as the U.S. dollar is only valuable because users believe it is.

Worth noting, however, is the fact that although Bitcoin wallets and exchanges can be hacked, bitcoins themselves have thus far been proved impervious to counterfeiting. The Bitcoin code contains a public ledger of each bitcoin’s transaction history, showing that bitcoin X moved from account A to account B. Once that transaction is completed, account A cannot spend that bitcoin again because the ledger demonstrates that account A no longer holds that coin. Likewise, a user cannot fabricate a new bitcoin by making up a long string of letters and numbers, because the code does not recognize that string as an answer to any of the previous math problems.

B. Trust in Algorithms

In the white paper introducing the currency, computer programmer Satoshi Nakamoto wrote, “We have proposed a system for electronic...
transactions without relying on trust.”

The math-problem-solving process by which new bitcoins are generated is transparent (even if the math itself is difficult), and the rate at which bitcoins are generated is generally predictable. The code will stop producing new bitcoins once there are 21 million in existence.

Some individuals find comfort in the Bitcoin currency precisely because it is mathematically driven and not manipulated by central bankers. Such Bitcoin users mistrust central banking institutions and their authority to print more money and, instead, prefer a currency operated with computerized, pre-determined precision to a currency backed by a government but regulated by fallible humans.

The transparent, algorithm-driven, no-central-bankers model holds significant appeal in the wake of the 2008 global financial crisis. In the first part of the 2000s, U.S. subprime mortgage loans became the shaky foundation upon which trillions of dollars of derivatives business was built. When it became apparent that no one, not even financial experts, appropriately understood the derivatives products or the magnitude of the economic danger, the U.S. government stepped in, rescuing some firms with spectacular, taxpayer-funded bailouts while letting other firms fail without much explanation. To many laypeople, the mysterious machinations of the financial services industry were infuriating, and the simple transparency of Bitcoin transactions seemed far more equitable.

Relatedly, some individuals feel a libertarian pleasure in utilizing Bitcoin; they feel that storing wealth in Bitcoin rather than, say, U.S. dollars is somehow subverting the U.S. government. Bitcoin users’ enthusiasm is also related to some people’s faith in gold. Historically, gold has been more than just a scarce commodity; it has been money. Bitcoin appeals to these gold bugs’ “libertarian politics” because, as in societies that used gold

33. Cohen, supra note 27.
34. See id.
35. See Grinberg, supra note 1, at 172.
36. See Popper & Lattman, supra note 12 (quoting Tyler Winklevoss as saying, “We have elected to put our money and faith in a mathematical framework that is free of politics and human error[.]”).
37. See id.
39. See id. at xvi.
40. See Popper & Lattman, supra note 12.
41. Dion, supra note 4, at 169 (“The currency may also have been favored by those who viewed American monetary policy as unconstitutional and therefore illegitimate. Their investment in Bitcoin is a political demonstration of the feasibility of a private legal currency.”).
42. Floyd Norris, One Man’s Currency is Another Man’s Bet, N.Y. TIMES, April 19, 2013, at B1.
43. Id.
as currency, more money cannot simply be created by governmental decision.  

C. Spending Power

A basic function of any currency is to operate as a medium of exchange: one party can give currency to another in exchange for goods and services. In the U.S., the dollar serves as the default medium of exchange, and it is legal tender in the U.S. because merchants are required to accept it for payment. Bitcoin is not legal tender in the U.S. or anywhere else, which means that merchants are not required to accept it. Merchants may choose to do so, however, and among those merchants, Bitcoin is a viable medium of exchange.

It is perfectly possible to buy goods and services with bitcoins, both in the U.S. and abroad. Bitcoins can be used to buy electronics, jewelry, paintball equipment, and clothing, and to pay for health care, technical support, hotel rooms, and restaurant meals. Infamously, bitcoins can also be used to purchase illegal items, such as the drugs and guns for sale on Silk Road. Since Bitcoin accounts do not require names or other identifying information, they provide a level of anonymity when purchasing drugs, weapons, or pornography. Purchasing over the Internet also reduces or eliminates geographic restrictions of supply and demand.

Bitcoin users share information online about which merchants are willing to accept payments in Bitcoin. Institutions such as WikiLeaks,

46. Id. at 113–14.
47. See 31 U.S.C. § 5103 (2012); see also Grinberg, supra note 1, at 162, 165–66 (discussing the basics of Bitcoin).
48. See Grinberg, supra note 1, at 166.
50. See Trade, BITCOIN Wiki, https://en.bitcoin.it/wiki/Trade (last visited Oct. 29, 2014) (scroll down for a list of retailers currently accepting payment in Bitcoin). Interestingly, a warning on this page provides that “Products or services illegal in [the] US or Japan are not fit to be listed here—such links will be removed immediately.” Id.
accept contributions in Bitcoin, and vendors that decide to accept payment in Bitcoin often make a splash in the news, such as the university in Cyprus that now accepts tuition payments in bitcoins.

Bitcoin has liquidity problems that other currencies do not, however. Bitcoin advocates may crow about thousands of vendors accepting bitcoins as payment, but bitcoins still cannot be used generally to pay for things like rent. Bitcoin’s association with infamous vendors, such as Silk Road (selling illegal drugs and weapons) and WikiLeaks (an organization flirting with the distinction between heroic whistleblowers and criminal anarchists), may contribute to legitimate, lawful retailers’ reluctance in adopting Bitcoin as a viable means of payment.

D. Money Laundering

Because of Bitcoin’s anonymity and the Internet’s ability to facilitate trade around the globe, Bitcoin is being used as a medium of exchange in drug trafficking, terrorist financing, human trafficking, and a host of other criminal activities. In addition to those crimes, Bitcoin can also be used for laundering the proceeds of those activities, adding another layer of criminal liability.

Physical cash has long been the ideal medium of money laundering: it is “anonymous, untraceable, requires no intermediary, is widely accepted, and provides for immediate settlement.” On the other hand, cash presents several significant difficulties, namely the physical, logistical, and geographic problems of possessing and transporting large amounts of cash.

Bitcoin has many cash-like attributes. Most importantly, Bitcoin transactions can be effected anonymously. Bitcoin addresses and wallets

57. See Kashmir Hill, 21 Things I Learned About Bitcoin From Living on It for a Week, FORBES (May 9, 2013, 1:54 PM), http://www.forbes.com/sites/kashmirhill/2013/05/09/25-things-i-learned-about-bitcoin-from-living-on-it-for-a-week/ (“Living on Bitcoin is a great way to lose weight. As it is not widely accepted, you are prevented from spontaneous snacking.”).
58. See Chen, supra note 51 (discussing the original Silk Road conflict); Stokes, supra note 3, at 4–5.
61. Id. ¶¶ 11, 13.
WHY ON EARTH DO PEOPLE USE BITCOIN?

have no identifying information about the owner, and encryption and IP randomizers can be used to further obscure any facts that would lead to the discovery of the owner’s identity. Moreover, Bitcoin addresses are free and unlimited, making them essentially disposable. Peer-to-peer Bitcoin transactions occur instantaneously, and charge-backs (akin to disputing a credit card charge) are impossible with Bitcoin because there is no higher authority to administer a charge-back system.

In some ways, Bitcoin is even better than cash for money launderers. Moving a large amount of Bitcoin is just as easy as moving a small amount, and transactions can be made across international borders without physical or political impediments. The drawback of Bitcoin as a money-laundering vehicle is that it is not accepted everywhere. This is where digital currency exchanges come in. Digital currency exchanges are websites where users can exchange bitcoins for other currencies, including virtual currencies and government-backed currencies like the U.S. dollar.

Money laundering is its own crime, though of course the funds being laundered must be derived from criminal activity for the laundering itself to be criminal. Anti-money laundering laws are in turn enforced through a complex scheme of regulations placed on financial institutions. Under penalty of law, financial institutions are required to confirm customer identities, maintain certain records, and report certain transactions to government agencies.

Anti-money laundering regulations are likely not applicable to individual Bitcoin users, but they probably are applicable to digital currency exchange websites. If law enforcement seeks to crack down on crimes committed and denominated in Bitcoin, digital currency exchanges will probably provide valuable information about the criminals’ identities: digital currency exchanges often require more identifying information about users than the Bitcoin software does, and the digital currency exchanges

64. Stokes, supra note 3, at 3.
68. See id.
70. Hett, supra note 22, ¶¶ 7–9.
71. See id.
72. See Stokes, supra note 3, at 1.
74. Id.
75. See Christopher, supra note 69, at 6.
may be able to help law enforcement detect patterns in Bitcoin transactions that may provide additional identifying information.76

III. CONCLUSION

When I give talks about Bitcoin, I’m often people’s first introduction to it. It’s a lot of new concepts and information to absorb in a short period of time, but one of the things I often assure my listeners is, “Now that you’ve heard about it, you’ll see it everywhere.” Bitcoin is all over the news.77 (That’s not just my warped perspective on things, right?)

One thing that surprises me about my Bitcoin talks is that hardly anyone asks me if I own any bitcoins. I don’t know why I don’t get that question more often—perhaps people are too polite to pry. I don’t own any bitcoins. Neither my mortgage company nor my favorite sandwich shop accepts them, so there’s nowhere I’m interested in spending them. I don’t want them as an investment vehicle, either—the exchange rate is too volatile for my conservative finances, and I don’t get a gambler’s rush from speculating. I’m mad as hell about the abuses committed in the early 2000s that led the world into a global financial crisis, but I’m not convinced that government-less currencies are the way to prevent those mistakes from happening again.

So while there are legitimate uses for Bitcoin—investment, commerce, and moral conviction—they’re compelling only to a specialized segment of the population. Before Bitcoin can truly be widely used, it will have to become a lot more user-friendly to ordinary people. People will have to understand how it works, and the exchange rate will have to stabilize. Apps and accounts will have to be developed so that users are not responsible for their own tech support. People will have to know where they can spend their bitcoins and trust that their Bitcoin savings will retain value. In short, Bitcoin will only become widespread when people are able to stop asking, “Why on earth would anyone use Bitcoin?”
