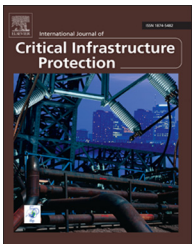
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Discussion

The promise and perils of digital currencies

Tyler Moore

Computer Science and Engineering Department, Lyle School of Engineering, Southern Methodist University, P.O. Box 750122, Dallas, Texas 75275-0122, USA

Interest in digital currencies, especially Bitcoin, has exploded over the past year. The cryptocurrency Bitcoin was created in 2009 by an anonymous entity operating under the pseudonym Satoshi Nakamoto. Using cryptographic primitives to create a digital currency is not particularly new – David Chaum proposed electronic cash nearly thirty years ago. What is different about Bitcoin is its success in gaining adoption. More than $1 billion of Bitcoin currency is in circulation, while Bitcoin startups are attracting tremendous interest from venture capitalists.

But not all the attention attracted by digital currencies is positive. In 2011, two U.S. Senators asked that Bitcoin be shut down after they learned that it was used to pay for hard drugs in an underground marketplace called The Silk Road. Recently, the Costa-Rica-based digital currency, Liberty Reserve, was closed down because it allegedly laundered more than $6 billion on behalf of cyber criminals who had turned to the currency as a favored means of exchange. Bitcoin itself is frequently targeted by hackers, who exploit operational security failures to steal from the "wallets" of consumers and firms.

1. Why is there so much interest in digital currencies?

One big reason is that digital currencies offer the prospect of substantially reduced transaction fees for online purchases. Nearly all online payments are made via payment-card networks. These payment platforms are so dominant that they can charge high fees despite low operating costs. Responding to consumer outrage, the United States recently passed legislation limiting debit card interchange fees. The European Union has proposed similar limits. The backers of new digital currencies believe they can offer lower transaction fees through technological innovation rather than regulation. Of course, it remains to be seen if they can overtake the entrenched payment networks of Visa and MasterCard.

The second reason is that digital currencies provide greater anonymity than credit cards. In Bitcoin, for example, accounts are pseudonymous and the protocol is designed to encourage the use of new account numbers for each transaction. These features are touted by Bitcoin supporters as a guarantee of anonymity, which has drawn privacy-conscious consumers – and criminals – to the currency. But they are mistaken. Associating identities with Bitcoin addresses is possible, particularly when interacting with online currency exchanges.

The third reason is the decentralized design of Bitcoin and other digital currencies that protects against inflation. Traditional currencies rely on a central bank to regulate the money supply, introducing new money into circulation as needed. The quantitative easing policies adopted by the U.S. Federal Reserve have attracted criticism about potentially causing inflation. Bitcoin, in contrast, uses cryptography to guarantee a relatively fixed money supply, which is allowed to grow at regular intervals. Periodically, the amount of money introduced is halved, until no more Bitcoin currency is brought into circulation. Hence, instead of central bank decisions driven by human prognostications, Bitcoin relies on an algorithm to limit the growth of the money supply. This approach is very appealing to inflation "hawks" who have literally bought into Bitcoin.

2. So what are the risks?

The principal risk is that digital currencies are highly susceptible to abuse by criminals.

E-mail address: tylerm@smu.edu

1874-5482/$ - see front matter © 2013 Published by Elsevier B.V.
http://dx.doi.org/10.1016/j.ijcip.2013.08.002

Merchants who sell dodgy goods or services using the traditional payment system must avoid excessive chargeback rates or they will be forced to pay higher transaction fees or perhaps even be dropped altogether by their payment processors. Criminals peddling fake antivirus software are known to pay close attention to their chargeback rates, even refunding bilked customers later in the month to stay under the radar of payment processors. Unlicensed online pharmacies are also ever fearful of being targeted by law enforcement who shut down their access to payment processors.

Given these obstacles, many criminals have moved to digital currencies to process payments. Before its closure by the FBI in October 2013, The Silk Road underground marketplace sold schedule drugs and narcotics without prescription, relying on Bitcoin for all transactions. Thousands of online Ponzi schemes called high-yield investment programs (HYIPs) rely on obscure digital currencies such as Perfect Money and, until it was shut down, Liberty Reserve.

Criminals also have begun to (ab)use digital currencies as a platform for exchange. Like all of us, criminals desire reliable bank accounts. But they want to register these accounts without providing identifying information so that their victims cannot seek recompense. Some less reputable digital currencies gladly meet this requirement. Criminals in underground forums frequently paid each other for goods and services using the now-defunct Liberty Reserve. When it was operational, Liberty Reserve was the "coin of the realm" for many criminal entities. Notably, there has been almost no evidence of criminals using Bitcoin for this purpose on a large scale.

Still, digital currencies such as Bitcoin pose many risks to consumers. Consumers looking to use digital currencies for legitimate transactions can be bitten badly.

The biggest risk facing Bitcoin users is exchange-rate risk. The Bitcoin-dollar exchange rate has fluctuated wildly. During its first few years of operation, exchange rates fluctuated between $5 and $15. However, beginning in January 2013, the currency rose inexorably, reaching a peak of over $250 in early April before falling sharply. The currency has stabilized somewhat in recent months, hovering around $100. While Bitcoin's rise has benefited early adopters, consumers are fearful of holding or spending the currency because its value can change so rapidly.

Another risk for consumers is that, unlike traditional online payments, many digital currencies (including Bitcoin and Liberty Reserve) are designed to have irreversible transactions. This is attractive to merchants because it can reduce chargeback rates. But for consumers, the potential for harm is substantial because fraudulent transactions cannot be undone. Millions of consumers flocked to credit cards starting in the 1970s because strong government regulation required credit card companies to reimburse disputed transactions. Absent such protection, digital currencies could see very low adoption rates except in the minority of cases where other benefits outweigh the risk.

Another related problem is that hackers who gain unauthorized access to Bitcoin wallets can steal money, leaving victims without any recourse. Several high-profile Bitcoin thefts have targeted currency exchanges and other entities that hold large amounts of the currency. This is significant because many consumers, fearful of taking possession of their Bitcoin assets, choose to leave their newly-acquired currency in the control of the very exchanges from which they purchased the currency.

This points to another Bitcoin-specific hazard: exchange-closure risk. Since 2010, at least 40 currency exchanges that convert Bitcoin to and from hard currencies for a small fee have opened. Unfortunately, eighteen of these exchanges have subsequently closed, leaving their Bitcoin depositors in the lurch. Regression analysis has shown that increased trading volume is associated with longer operating lifetimes for exchanges. But trading volume is also positively correlated with suffering security breaches – profitable exchanges make valuable targets. Unfortunately, in the "Wild West" of Bitcoin's ecosystem, consumers have no protection against these and other risks.

3. Are there regulatory remedies that can protect consumers?

Given the widespread criminality facilitated by digital currencies and perpetrated against consumers, one might expect that little could be done by regulators and law enforcement to mitigate the threats. But the prospects for oversight and control are actually quite decent.

While Bitcoin was designed to be completely decentralized, the reality is that a relatively small number of currency exchanges facilitate most transactions. These exchanges are essential to the functional operation of the Bitcoin ecosystem because they are responsible for all transfers into and out of Bitcoin from hard currencies. Most of these exchanges operate in countries with substantial financial oversight – the largest exchange, Mt. Gox, is based in Japan.

Governments have begun to flex their muscle. The U.S. Department of Homeland Security recently temporarily cut off Mt. Gox's account with its U.S.-based payment processor Dwolla for non-compliance with currency-exchange regulations. The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) recently issued guidance to digital currencies on compliance with the Bank Secrecy Act.

Bitcoin exchanges have strong incentives to cooperate with regulators in efforts such as these. One reason is purely existential – a closure such as that of Liberty Reserve is a future that no exchange desires to emulate. It is also quite possible that exchanges will compete by providing better protection of customer accounts. Mt. Gox has suffered multiple security breaches, but in every case, it repaid consumers and absorbed the loss. However, it is not clear that such behavior would persist in the aftermath of a massive breach.

Another reason Bitcoin and other digital currency exchanges will likely work with regulators and law enforcement is that taking a stand against crime may well drive criminals to use more lax currencies. The pessimistic corollary is that, even if Bitcoin and other digital currencies do not become criminal havens, less responsible currencies will happily provide sanctuary, just like eGold, WebMoney and Liberty Reserve did in the past. While regulators can exert influence on the more responsible currencies, they will

doubtless play a never-ending game of "whack-a-mole" with the dodgier currency operators.

The bottom line is that digital currencies are a disruptive technology. They can lower online payment fees and even offer cryptographic guarantees about the money supply. But the risks they introduce – from abuse by criminals to widespread customer fraud – are substantial.

Technologists, policymakers and consumers must work together to overcome the many risks and tame what is most definitely another "Wild West."

Tyler Moore is an Assistant Professor of Computer Science and Engineering at Southern Methodist University, Dallas, Texas. His research interests include the economics of information security, the study of electronic crime, and the development of policy for strengthening security. He is a Director and Vice President of the International Financial Cryptography Association (IFCA) and Vice Chair of the IFIP 11.10 Working Group on Critical Infrastructure Protection.