UC SANTA BARBARA

THE Current

March 10, 2014

Shelly Leachman

Pure Speculation: Bitcoin or Bust?

Depending on whom you ask or what you read — and when — bitcoin, the so-called "cryptocurrency," is either days from extinction or destined to give central banking a run for its money.

With implications for computer security, business, the economy and our culture, predicting the future of bitcoin is practically a cottage industry all its own. Pervasive media coverage and public debates about its worth (both literally and figuratively) have become *de rigueur* for today's prevailing digital tender, which is alternately characterized as a revolutionary innovation on par with the Internet or a flash in the pan that can't possibly survive.

"Central banks are not threatened unless bitcoins become popular, but bitcoins won't become popular unless, in effect, they become popular," said Benjamin J. Cohen, the Louis G. Lancaster Professor of International Political Economy at UC Santa Barbara, a currency expert and author of several books on the subject. "It's a chicken-or-the-egg problem.

"A currency becomes powerful in proportion to the size of the network of transactors that are prepared to accept it," Cohen added. "But very few people are willing to accept something unless they think others are going to accept it, and others aren't going to accept it until they think you are. So who's going to do it first?"

There is seemingly no shortage of those willing to try.

From independent restaurants and retailers to the NBA's Sacramento Kings and Tesla Motors, a growing number of businesses large and small are now accepting bitcoin as payment. Just last week, the well-heeled Winklevoss brothers (of suing-Facebook's-Mark-Zuckerberg fame) used bitcoin — they're big believers and investors in the nascent currency — to book two tickets on would-be space airline Virgin Galactic. There are now Bitcoin ATM machines in Vancouver, London and Austin, Texas.

The ubiquitous crypto-cash is decidedly en vogue. And it's a hot commodity. Since the Bitcoin network launched in 2009, the value of a single bitcoin has rocketed from less than a dollar to more than $1,200 in late 2013. It currently sits just south of $700. Its volatility is both part of its problem and part of its allure. Speculators see it as a potentially major moneymaker; experts say bitcoin can't evolve into a true currency until and unless it stabilizes.

And so it goes with bitcoin and its ilk (there are a multitude of competitors), which attract some people and repel others for identical reasons.

Bitcoin's champions herald its fixed supply (only 21 million bitcoins will ever be put into virtual circulation) and its elimination of the proverbial middle man (read: banks) and related transaction fees. Detractors cite the same characteristics in forecasting its ultimate failure as a true, dollar-competing currency.

"I think it will be very difficult for electronic currencies to replace the currencies we have now because there are so many fundamental issues," explained UCSB professor of economics Douglas G. Steigerwald, who said that in a growing economy, a finite supply of currency would trigger deflation. "Suppose we had dollars that are electronic, all controlled by banks, backed in the same way, by the same policy. I have no problem with the currency being electronic versus physical. The question is: Who controls the supply of the currency and how is it altered?

"We recognize the dollar's value because we believe it has value," Steigerwald added. "Why gold? Because we value gold and consider it a rare commodity. These are things in human culture that we value. Are we going to fix on bitcoins? Is it better than the U.S. dollar or the Japanese yen for someone who lives in Zimbabwe? That's not at all transparent. There are problems with bitcoin as a currency: deflation, the transparency of who holds what and what backs up the value of bitcoins."

And then there’s a different brand of backup to worry about: the computer security kind. Bitcoins, of course, aren’t coins at all. They exist in lines of code — and so does their value — making their protection a more complex process than stashing cash under your mattress.

Leave your wallet on an airplane and you might have to cancel your credit cards — a nuisance, but not catastrophic. Get your laptop stolen out of your car, however, and any bitcoins sitting on your hard drive will be gone forever. Once a bitcoin is “mined” (a computing process by which the funds are obtained), it stays where you store it. Whether it’s on your local network or online, hacking is a major concern.

“Bitcoins are for hackers, fundamentally, and it’s a big stage,” said Giovanni Vigna, an Internet security expert and UCSB computer science professor. “You have to understand the implications and how the cryptography works. Someone breaks into your computer and they can steal all your money. So now you have to go and put your computer in the bank so nobody can break the computer? It’s a complicated issue.

“As a security person, I would never invest in bitcoin,” Vigna added. “The cryptography seems solid enough, but when cryptography is associated with dollar values, suddenly a lot of people are spending nights looking at the code. There are a lot of checks in place for the banking industry to prevent disaster. Bitcoin doesn’t have that. If somebody breaks the cryptography one day, it’s all gone.”

Bitcoin was, in fact, based and built on cryptography, which is partly what’s made it simultaneously intriguing and troubling. Can it survive long-term in the face of cyberattacks and rapidly changing technology?

Only time will tell, asserted UCSB cryptographers Huijia “Rachel” Lin and Stefano Tessaro, assistant professors of computer science and founding faculty of the campus’s inaugural cryptography research group.

“Bitcoin is a very intriguing idea in the sense that cryptography is trying to replace trust,” said Lin. “It is using mathematics to replace trust, which is kind of a radical idea, but it makes sense from a high level. A bank is not a magic fortress. It also uses databases, has doors, is connected with the Internet.”

“If there were a metric to compare it to the banking system, I think bitcoin would win,” added Tessaro. “I suspect it’s probably easier to break into the local bank. The

general problem with electronic cash is making sure that you don’t spend the same money twice. And the Bitcoin network is designed to prevent that.”

Not that it can’t happen outside the network. Leading bitcoin exchange Mt. Gox went dark in recent weeks — an estimated $500 million in stored bitcoin lost — and has now filed for bankruptcy. A hack that used just such a duplication technique (geek term: transaction malleability) has been identified as the most likely culprit in that demise.

With all its promise — and its problems — the nascent currency is also increasingly polarizing. China moved to regulate bitcoin in late 2013, banning bitcoin transactions by financial companies. Japan recently announced it would tax bitcoin transactions and regulate bitcoin trading. The U.S. is still in the regulatory research and development phase, but such measures are widely deemed to be inevitable.

So then, is this digital dough the greatest thing since sliced bread — or just pie in the sky?

“You can find other algorithms, different versions that work on the same mathematical principles as bitcoin,” said Ben Zhao, an associate professor of computer science. “Bitcoin is unique in that it was the first to prove it could be done. And it’s likely going to be the first to be regulated and widely accepted — and it will probably dominate the market.

“Bitcoin has a lot of technological benefits that fundamentally change how people use money, and that’s what’s interesting to me,” Zhao said. “It is a potentially world-changing disruptive technology.

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.