

Interface with Rachel Botsman

MODERN MONEY

It's the preferred payment method of drug dealers but cryptocurrency Bitcoin is finding favour with legitimate businesspeople, too.

AT THE end of 2010, Mat Holroyd, an Australian web developer, read about a new digital currency called Bitcoin. A few days later, he heard someone at a party talking about this “new cryptographic money”. So Holroyd started to do his own research on what bitcoins were and how the system worked.

The first thing he learned and liked was this new virtual currency cut out all the usual financial middlemen and is not tied to any country or economy. The coins are exchanged electronically, person-to-person, with no banks, companies or governments involved, at least for now.

“The value of the decentralised nature of Bitcoin was what immediately appealed to me and set it apart from all other currencies,” he says.

Holroyd had been reading about the history of money and gold around the time of the financial crisis. He was trying to figure out why we had come to give so much power to fiat currencies such as the US and Australian dollars or euros, which are quite simply national currencies government issue “by law”. Governments and/or central banks can adjust money supply at will (usually in favour of inflation) and this gives them a lot of control over, well, just about everything.

“What jumped out about Bitcoin was no central authority had the power to print more money,” Holroyd says. “It would be more resilient to inflation and difficult to shut down.”

A few months later, Holroyd purchased his first \$50 of bitcoins.

“At the time, I thought this could drop to zero tomorrow so for the first year, I didn’t put a lot of money on the line.”

His original \$50 of bitcoins is now worth more than \$7000. Fast forward to today, Holroyd is the founder of BitPiggy, a currency trader in Australia: “I am a bit like a market trader on eBay but I sell and buy only one product, bitcoins.”

So what’s the big deal with this new currency? I admit that when I first started hearing about



Bitcoin I thought it was a geeky and powerful idea but, honestly, I didn’t quite get it. Was this simply a gold rush for nerds? There seemed to be so much insider parlance, from “miners” to “block chains” to “Mt Gox”. So I decided to write this column a little differently; the challenge I have set myself is to try to give you non-jargon answers to all the questions I asked to understand how exactly Bitcoin works, why we seem to be in a craze, and the future financial revolution it could represent.

Who invented Bitcoin?
Nobody knows. The mystery creator was a coder and mathematical genius (possibly a group) that went by the pseudonym of Satoshi Nakamoto. On November 1, 2008, he or she published a white paper on The Cryptography Mailing List detailing the idea of how a decentralised, untraceable digital crypto-currency could work. On January 3, 2009, when the world was reeling from the global financial crisis, Nakamoto “mined” the first

50 bitcoins, now known as the “genesis block”.
How is it different from other virtual currencies?
From Facebook Credits to Beenz or Linden Dollars, there have been various attempts to build viable virtual currencies. However, these other currencies are centralised and controlled by a corporation, whether Second Life or Facebook
Where do bitcoins come from?
This is one of the hardest parts to get my head around because no central body decides when to issue bitcoins and there they have no physical representation. Instead, they’re created, traded and controlled by the user community. The digital coins themselves are algorithm-based mathematical constructs, created by developer Nakamoto. More currency is gradually introduced into the market when transactions are processed and verified. That’s where miners come in.

Who are miners?
When we talk about the “mining industry”, it has to do with digging up ore from the ground. All over the world, mathematicians, retired scientists, software engineers and general computer enthusiasts have discovered a new, sometimes lucrative hobby, known as “mining” bitcoins. Instead of diggers or shovels, personal computers use specialised software to find and solve the complex maths problems generated and distributed by the software on the peer-to-peer network. To give you a simple analogy; imagine a room full of people who are verifying trades happening between two people. Whichever miner solves the code to process a transaction is rewarded with bitcoins.

Have people really built mining rigs?
Just like gold, this currency is not an infinite resource. The system is designed so only 21 million bitcoins will ever be created. The current supply recently passed 11 million, meaning more than half the bitcoins that will ever exist have been created. The last coin is set to be created in 2140, and then there will be nothing more to mine. So people are spending tens of thousands of dollars on custom-built computers, known as application-specific integrated circuits, that can find the currency and perform the calculations faster.

How does the system prevent a gold rush?
Aside from the supply of coins being capped, the system is designed so the rate of creation is controlled. This is clever in two ways: firstly, the codes become harder to find and crack; secondly, the rewards halve every four years, so when people first started mining in 2009, they would receive 50 bitcoins per block; the rate is now around 25. This is kind of like Milton Friedman’s dream realised: an automated system that produces a limited, pre-determined supply of money at a known rate that is publicly available.

Are bitcoins worth anything?
Unlike other items once used as currency – salt, shells, tobacco, grain or even cows – bitcoins have no value in their own right. What gives the currency its value is people believing it has value. The exchange rate is based on simple supply and demand: when the number of bitcoins wanted is higher than that available, their values soar, making them highly volatile risk assets. The market price climbed to an all-time high of \$266 on April 10 2013, then plunged below \$80 a week later. Some argue the surge was caused by the crisis in Cyprus where people started to convert euros into bitcoins. Currently, there are more than 11.6 million bitcoins in circulation, which puts the value of the Bitcoin economy worldwide at over \$1.3 billion.
How can you buy and store bitcoins?
To get started, you simply download some open-

BITCOINS ARE HIGHLY VOLATILE RISK ASSETS. THE MARKET PRICE CLIMBED TO AN ALL-TIME HIGH OF \$266 ON APRIL 10 2013, A WEEK LATER IT PLUNGED BELOW \$80.

source software on a site like www.weusecoins.com and then sign-up for a digital wallet service such as Coinbase or MyWallet. Instead of containing notes and coins, digital wallets contain all your “private keys” (see below), which you can use to make payments. OK, now you need to get Bitcoins. If mining is out of the question you can use exchanges such as Bitpiggy or find local bitcoiners on a site like TradeBitcoin. If you want to make larger purchases, you need to go to services such as Bitstamp or Mt Gox, the world’s largest Bitcoin exchange, based in Tokyo that handles approximately 60 per cent of exchange volume.
How does a transaction work?
Two users, let’s call them Mary and John, have bitcoin wallets on their computer. Mary wants to pay John 150 bitcoins. John’s wallet creates a new address, basically a string of digitally encrypted letters and numbers, for Mary to send payment to. The cryptographic process involves a combination of a freely-available “public key” and a secret “private key” that belongs to one individual owner and proves their right to spend bitcoins from a specific digital wallet. A transaction looks something like this:

Pay to: 13e5HeX976tUFg3496Dee587’
Amount: 150 BC
From: 56Hhet840JUiklae3990CacewRR22
Unlike traditional bank accounts, each user does not have one address, but many addresses designed to keep funds secure. Miners verify all transactions (this part of the process is technically complicated, involving “cryptographic hash functions”) and, once verified, it shows up in your receiver’s wallet as paid. Every payment that has ever occurred on the network can be publicly viewed on services such as BlockExplorer.com. Think of the public “block chains” as a real-time ledger of all transactions. However, the personal identity of bitcoin owners is kept anonymous.

So what can you spend bitcoins on?
Even though the currency only exists online it can be traded for real goods and services. A growing number of merchants accept bitcoins as payment for everything from Amazon gift cards to dating website fees or online retailers. There are a growing number of options in Australia. These include Honestbeef.com.au where you can pay 0.079 BTC per kg for home beef delivery. In September, The Old Fitzroy in Sydney became the first local pub to accept bitcoins. Australian realtor, Paul Osborne accepted bitcoins for his fees from an entrepreneur on the sale of his Melbourne terrace.
What happens to Bitcoin after the Silk Road bust?
Given the anonymous nature of the currency, it didn’t take long for it to become a preferred form of payment on Silk Road. On October 2 the FBI shut down the drug bazaar, arrested the man who is alleged to be behind it, Ross Ulbricht, and seized \$US3.6 million in bitcoins. However, Ulbricht may have another \$US80 million stashed away but the government can’t get its hands on the money because it doesn’t have the passwords to verify the transactions. The Bitcoin market took a steep dive, but only briefly after the arrest and has now rebounded back to almost its same value as before the Silk Road shakedown.

What about government regulation?
In short, it’s a nightmare for governments because technology has basically outpaced the law. Existing regulations don’t provide a good framework because there really isn’t a clear category that Bitcoin fits into, and because it’s decentralised, it’s a difficult system to control. In Australia, an act passed in 2006 states the key requirement of an e-currency is that it must be backed by something such as precious metal, bullion or “a thing of a kind prescribed by the AML/CTF Rules”. This is good news for the likes of Mat Holroyd. “The irony is that because bitcoin is not classed as an e-currency by Australian law, I am not burdened by AML/CTF reporting.” **B**