BW|BUSINESSWORLD

FINANCE 19 Feb, 2014 11:25 IST

Gaining Currency

Bitcoins have shown promise, but an unregulated market is cause for concern

Abraham C. Mathews

Illustration by Champak Bhattacharjee

Let us assume that much of the blame for the economic problems in the developing world today lies with the excessive printing of dollars by the US Federal Reserve. And, you wish to make its just-retired chairman, Ben Bernanke, pay. Or, let us assume you want the president of a Western power taken to task for his country's presence in Afghanistan. Or, maybe, you have another politician in your crosshairs, one you do not wish to see become premier. What do you do?

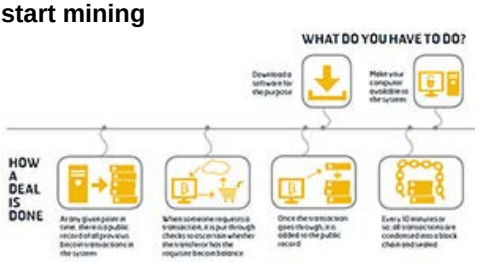
A website that cropped up late last year (and has since shut down) allowed you to contribute to the assassination fund for any person of your choice. It is the brainchild of a person who identified himself as Kuwabatake Sanjuro, a pseudonym he gave Forbes magazine. You can name any person you want assassinated and, with others who think alike, contribute to his assassination fund. Whoever carries out the hit (with advance notice to the administrator) gets the corpus. Are you committing a crime by participating in such a scheme? Under law, yes. But, if you are using a sufficiently safe crypto-currency like a bitcoin, you will remain anonymous, and safe.

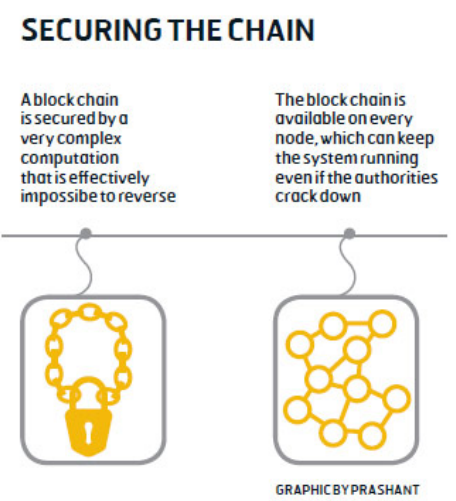
Welcome to a new financial world. One conceived by geeks, where money is minted on your home computer, and transacted solely through the Internet. "Bitcoins will revolutionise finance, just the way the Internet changed communications," says Nishith Desai of Nishith Desai Associates, a law firm. With bitcoins, you can pay for anything as long as the seller agrees to accept them. You do not need a bank, as your money is stored digitally in your own bitcoin wallet. Most importantly, the system (like a computer programme), runs itself. As long as you don't disclose details, even the government cannot trace your transactions.

Bitcoins also serve as an asset, a very volatile asset albeit. Their value appreciated astronomically last year. Through 2013, the value of a bitcoin rose 40-fold from around $25 to a high of $1,000. And then dramatically, in late December, as well as again in February, the currency crashed after questions were raised about its acceptability. The currency now trades around $600. In early January, a survey by bitcoin information portal CoinDesk suggested that a majority of bitcoin users expect the virtual currency to only increase in value in 2014. At the height of the bitcoin's value, the bounty on Bernanke's head had touched $120,000 (120 Bitcoins); haters of the Western leader had put a $50,000 price on his in bitcoins.

BIT BY BIT

Anybody with access to a computer can make money, at least of the bitcoin kind. All you need to do is plug in and start mining





Then again, what happens if after a well-thought-out assassination, the assassin finds that the promised funds have not reached him? How does he stalk an anonymous geek in his parlour, the virtual world? Who does he complain to? For all

you know, the Assassination Market is just a ploy to get the gullible to part with their money.

What The Fuss Is All About

To geeks, the bitcoin is today what the Internet was in the nineties. To lesser mortals, it is just a virtual currency, derived out of a complex software program they do not understand, regulated by none and, thus, unsafe. The geeks are on a different plane altogether. Global dominance is what they anticipate. It is best described as, to quote Sherlock Holmes: "You do see. You just don't observe." Its inevitability is beyond doubt. Says bitcoin trader Vishal Gupta, who runs bitterco.in, a bitcoin mouthpiece: "Whether you like it or not, you will soon have to accept the reality of bitcoins."

Bitcoins present the prospect of a world in which the state will cease to have a role. Can the state step in and put an end to it? "It will be a veritable nightmare to shut down the system. It will be the online equivalent of knocking on each and every door in the country to catch a thief. Virtually impossible," says Benny Samuel, a Bangalore-based software expert and bitcoin enthusiast.

Let us take a step back to process that. The bitcoin system is unlike any other technological product which works out of central servers, explains Mihir Parikh, head of Research and Knowledge Management at Nishith Desai Associates. In fact, individual computers of bitcoin users act as servers. All the data in the network, including the record of all previous transactions, is condensed into what they call a 'hash function' and passed through every node (computer) on the network. Such a hash function is sealed for good every 10 minutes or so, as a block chain. While it is possible for a malicious programmer to go back and alter such a program, according to Desai, it is immensely tedious, and the reward is not be worth the effort. And that seems to have been the goal of bitcoin founder Satoshi Nakamoto (most certainly a pseudonym, as 'he' continues to remain anonymous) — to keep his baby out of the reach of any government.

So, we have a software that is practically incorruptible and difficult to block (because a government would have to individually find IP addresses on which the software is running, unlike, say, a blog, for which it has to just clamp down on the server hosting the blog). Neither is it possible to track down transactions. While the block chain keeps a publicly available record of every transaction, "it is impossible to tie a bitcoin wallet to a real person by monitoring bitcoin transactions, if this person does not disclose his identity in other ways", says Sergei Lozhkin, senior security researcher at Kaspersky Labs, an anti-virus software maker. However, Tokyo-based bitcoin exchange Mt. Gox, in a recent statement said: "It has detected unusual activity on its bitcoin wallets and performed investigations during the past weeks. This confirmed the presence of transactions which need to be examined more closely." It has stopped withdrawls for an indefinate period.

HOW A BITCOIN IS MINED

Bitcoin generation happens when a computer solves an algorithm, a process known as mining. Unlike what the name suggests, mining does not involve digging or searching. All you need to do is connect your processor (yes, even you can mine — no permits needed, and definitely no fear of auctions) to the system by downloading a software, which will do the job for you.

A new set of 25 bitcoins is generated at a frequency of around 10 minutes. The process includes solving what is considered to be a progressively complicated algorithm (as more and more miners join the system, the algorithm is designed to become tougher to crack). The first to crack the algorithm wins the bitcoins.

If bitcoins gain wider acceptance, they could become the currency of the future. The problem is, so far, despite all the noise, it has not. According to blockchain.info, the average number of transactions every 10 minutes is estimated to be around 600, hardly significant for what purports to be a tour de force. In India, hardly any bitcoins are traded on a daily basis, says Gupta. He blames the government's indifference and uncertainty over its legal status. Besides, the global bitcoin traders have little, if any, holdings in the country.

This raises a larger question. What is the fuss all about? One possible answer lies in tracing who the beneficiaries will be. In an effort to protect the currency from deflation, the protocol that gave rise to bitcoins was designed so as to create only 21 million units of the currency, with a provision that after the first 10.5 million over four years, half that, or 5.25 million, would be released over the next four years, and so on.

A bulk of the 12 million or so bitcoins in circulation were mined in the first four years, when it was still an unheard of commodity. It is entirely reasonable to imagine that the bulk of these are owned by a small group of people or organisations who came into the game first (or, as sceptics say, designed the game). Many bitcoin traders admit that they were given the currency free (again not a crime — it can be put down to market creation).

If bitcoins do take off, the limited supply could take their value to a different orbit. You now begin to understand the logic of hardselling bitcoins as the currency of the future.

Free For All

Something cannot be dubbed illegal or wrong just because it disproportionately benefits its founders. For example, the biggest beneficiary of the surge in the price of the Facebook scrip in the past year has been its founder, Mark Zuckerberg. Going back even further, people who owned land (such as those under the zamindari system), a finite commodity, were the ones who did not have to fight the odds of the system to acquire wealth.

A senior official of India's Serious Fraud Investigation Office says crypto-currencies — or virtual currencies that have only a digital presence and are not managed by a regulator — are not a new concept. Take, for example, the case of

MMM, a scheme (originated in Russia in the nineties) which encouraged people to deposit real money in exchange for a crypto-currency called the Mavro. The value of a Mavro would increase by 30 per cent every month, representing the amount a depositor would become entitled to withdraw in real currency. As long as the value of new money being deposited went up by 30 per cent every month, the system would work. That was improbable and so, eventually, the scheme folded up, leaving many investors in the lurch.

The authorities, admittedly, cannot foretell what can go wrong with bitcoins. Yet, on the face of it, it seems fishy to them. For one, it lacks a central regulator. Bitcoin traders have been crying themselves hoarse about the need for regulation. But, how do you regulate a currency that runs on a technology that is designed to protect it from outside interference, and facilitates anonymous transactions?

'If tomorrow something goes wrong, who do you go after? What jurisdiction does this (bitcoin market) fall under?'

ROHIT MAHAJAN
Head, Forensic Practice, Deloitte India

'The bitcoin system is not like any other technological product that works out of central servers'

MIHIR PARIKH
Head, Technology, Nishith Desai Associates

The Bitcoin Foundation, a non-profit organisation based in Montreal, Canada, is the currency's public face. Its vice-chairman Charlie Shrem was arrested in January on charges of knowingly facilitating the sale of bitcoins to those trading on Silk Road, a platform for the world's largest black market, selling drugs in exchange of bitcoins. Hardly a picture of trust!

The Silk Road experience presents the other big challenge to authorities. The anonymity that such platforms promise gives rise to the trade in contraband such as drugs and pornography. Last year, the Federal Bureau of Investigation (FBI) arrested Ross William Ulbricht, alleged Dread Pirate Roberts, the brain behind Silk Road. He is said to have a stash of 600,000 bitcoins (worth $600 million at the time of his arrest, and now the property of the FBI).

Misuse is not the only risk that the currency faces. Bitcoins can be duplicated with slight variations. The bitcoin architecture is based on an open source code (like the operating system Linux which, as opposed to Windows, users can modify to their requirements) that anybody can modify to create their own virtual currency. So, while the number of bitcoins is programmed to be finite, you can have other versions of the currency which are infinite. Around 70 versions of the currency have been created already, with varying degrees of popularity, says Samuel.

THE UNANSWERED QUESTIONS

1. How will the Bitcoin Foundation protect the people who have invested in the currency, if it is declared illegal?
2. One of the biggest concerns of governments seems to be that it is impossible to trace a bitcoin transaction to its transactor. Is there any way the foundation can assuage their concerns by enabling such traceability?
3.How will the proliferation of other crypto-currencies impact the value of bitcoins?
4. How many bitcoin users are there currently, and what is the average value of daily transactions in bitcoins?
5. In what capacity is the foundation acting? Has there been an official transfer of the code or any such 'asset' from Satoshi Nakamoto to the foundation?
6. What is the identity of Satoshi Nakamoto? Is he currently a part of the foundation in any capacity?

In the works is laxmicoin, the brainchild of IIT-Delhi graduate and Silicon Valley programmer Mitts Daki (a pseudonym, as he requested anonymity). Laxmicoin is different in the sense that you have somebody taking ownership of the concept, as opposed to bitcoin's creator, who has not revealed himself. Daki is awaiting Reserve Bank of India (RBI) approval to launch his currency. The wait seems in vain. "It is almost akin to asking RBI to permit a rival currency," says Samuel. Daki hopes to make his money by retaining around 25 per cent of laxmicoins (like Satoshi's million or so bitcoins), and encashing them when they get valuable.

The virtual currency has economists spooked too. Is there a central authority you can approach to encash bitcoins, asks Madan Sabnavis, chief economist at Care Ratings. The value of a rupee note is guaranteed by the RBI governor, he points out. While you may argue that the governor, when asked to redeem your rupee notes, would not be able to pay you in anything other than rupee notes, yet there is an implicit trust that his guarantee inspires.

Economist and Nobel laureate Paul Krugman writes in his New York Times blog: “Whenever I ask how a bitcoin can be a store of value, they come back to me saying it is a terrific medium of exchange.” A store of value without an underlying asset — it is reminiscent of the 2008 financial crisis to most. Increasingly complex financial products were designed and traded by investment banks, backed by assets whose value was, at best, dubious. Only, in the case of bitcoins, it is worse. There is no underlying asset, dubious or otherwise.

According to bitcoin.org, “nobody owns it and nobody controls it”. However, recently, it emerged that a Ukrainian mining pool, ghash.io, has acquired over 46 per cent of the entire bitcoin processing capacity, sending the community into a tizzy. The worry was that any entity with control of 51 per cent of the nodes on the network could, theoretically, alter the protocol to its advantage. It may or may not have sinister intentions, but what is to stop a malicious programmer from taking over a few dominant miners to upset the entire system. It is where a regulator can play a role.

Rohit Mahajan, head of Deloitte’s forensics practice in India, reminds you of the National Spot Exchange fiasco. “If tomorrow something goes wrong, who do you go after, what jurisdiction does this fall under,” he asks. “The National Spot Exchange was a classic case of the risks of an unregulated market without oversight.”

Proper regulation can still do the trick, says Mahajan. So far, regulators are choosing to ignore the possibilities. Samuel makes a case for the government to consider this seriously. Payments are not the be-all and end-all of the system, he adds. Technology that can facilitate verification is easily adoptable, he points out.

BW|Businessworld sent multiple emails to the Bitcoin Foundation seeking its position on several issues, including the regulatory risks, possibility of dilution, and the identity of Satoshi Nakamoto. After an initial mail to the effect that the foundation would get back, there was no further response to any of the questions.

Selective Appeal

The buzz around bitcoins has been gaining in decibel levels since late last year. Taylor and Ross Winklevoss, who claim to have introduced the idea of Facebook to Zuckerberg, have launched the Winklevoss Bitcoin Trust to invest in bitcoins. More and more retailers are beginning to accept the digital currency, which helps them save on transaction charges of up to 10 per cent on cash transfers. NYSE-listed Zynga, which makes the popular Farmville games on Facebook, has announced it will soon start accepting payments in bitcoins, as did overstock.com, an online retailer. The NBA team Sacramento Kings said it will accept bitcoins as payment for its products. Even a UK public university has said it will accept bitcoins as tuition fees for two new courses examining the role of complementary currencies.

The growing acceptance of bitcoins has led to formation of consortia for mining the currency. For example, a company such asButterfly Labs now allows you to invest in mining pools — rather than mine independently on your personal computer. As a consortium, you stand a better chance of finding a quick solution to the algorithm, and winning new bitcoins. Butterfly Labs did not respond to BW ’s queries.

Ask any economist and he will tell you, a currency is one which is used by a substantial number of people for regular business. For the masses to take to bitcoins, it will take nothing less than a seal of approval from the government. And, so far, governments are refusing to play ball.

RBI, for example, warned people about the risks of using bitcoins — the lack of a centralised regulatory agency, no underlying asset to support its value, lack of clarity regarding its jurisdictional status, and the susceptibility to hacking — in late December.

Just two weeks earlier, the People’s Bank of China had gone a step further by banning banks from handling bitcoins. Bernanke, in a written deposition before the US Senate, washed his hands of the currency, saying the Fed could only regulate currencies issued by it.

And, indeed, at the moment, when the nature of the beast is still unknown, the authorities must tread with caution. If the problem of anonymity can be solved and, if a proper regulator has control over the currency, including the power to recall transactions or even shut them down temporarily, bitcoins hold promise. But, then, those very safeguards would kill its appeal.

Or, perhaps, as Mahajan says, “we will be sitting here three years from now discussing how bitcoins have transformed the way we look at the future”.

abraham@businessworld.in;
matabrahamc@gmail.com;
twitter@ebbruz