Bitcoin’s future

Hidden flipside

How the crypto-currency could become the internet of money

Mar 15th 2014 | From the print edition

THE father has been found in time for his child’s funeral. That would appear to be the sorry state of affairs in the land of Bitcoin, a crypto-currency, if recent press coverage is to be believed. On March 6th Newsweek reported that it had tracked down Satoshi Nakamoto, Bitcoin’s elusive creator. And on March 11th Mt Gox, the Japanese online exchange that had long dominated the trade in the currency before losing $490m of customers’ Bitcoins at today’s prices, once more filed for bankruptcy protection, this time in America.

In reality, things are rather different. Evidence is mounting that Dorian Satoshi Nakamoto, whom Newsweek identified as Bitcoin’s father, is not the relevant Satoshi. More importantly, Bitcoin’s best days may still be ahead of it—if not as a fully fledged currency (see article), then as a platform for financial innovation. Much as the internet is a foundation for digital services, the technology behind Bitcoin could support a revolution in the way people own and pay for things. Geeks of all sorts are getting excited—including a growing number of venture capitalists, who know a new platform when they see one.

To understand the enthusiasm in this modern currency, it helps to think about a very old one. Until the early 20th century the people on Yap, an island in the Pacific Ocean, used large stone disks (pictured) as money for big expenses, such as a daughter’s dowry. Being very heavy, they were rarely moved when spent. Instead, they simply changed owners. Every transaction became part of an oral history of ownership, which allowed islanders to know the proprietor of each stone and made it difficult to spend the same stone twice.

Bitcoins also don’t move around when they are transferred. They are best understood as entries in a
giant ledger, the “blockchain”, which contains the transaction history for every Bitcoin in circulation. It is kept up to date with the help of cryptography and copious computing power, provided by a global network of tens of thousands of computers. Again, openness helps the system remain secure: the blockchain is public so every participant can check whether a transfer comes from the rightful owner.

This set-up is the first workable solution to one of the more nagging problems of the digital realm: how to transfer something of value from one person to another without middlemen having to make sure that the item is not copied or, in the case of money, spent more than once? And Bitcoin does the trick while being open (unlike conventional payment mechanisms, which aim for security by shielding themselves from outsiders). This means that third parties can make use of Bitcoin’s features without having to ask anyone for permission—as is the case with the internet.

Such “permissionless innovation”, in the jargon, should in time result in a cornucopia of applications. Bitcoin’s technology could be used to transfer ownership both in other currencies and of any kind of financial asset. This, in turn, would allow the creation of decentralised exchanges which let asset holders trade directly. And money could be “programmed” to come with conditions: for instance, it might be released only if a third person agrees.

Some want ownership of devices—a car, say—to be represented by a Bitcoin, or a tiny fraction of it. The car would work only when turned on with a key that includes the Bitcoin token. This would make managing ownership of and access to physical assets much easier: the token could be sold or rented out temporarily, enabling flexible peer-to-peer car-rental schemes. Such “smart property” would turn the blockchain into a global registry of ownership in physical assets.

All that may sound like science fiction, but a growing number of startups are working on bringing such applications to market. Coloured Coins and Mastercoin will soon release software that enables trade in other financial assets, including stocks and bonds. The most ambitious project is Ethereum: it will launch a new blockchain, similar but unrelated to Bitcoin, with a programming language to encode financial instruments and other contracts.

Although banks have mostly steered clear of Bitcoin as a currency, they too have started exploring how they could use the technology in other ways. They are unlikely to move fast, but there are plenty of possibilities. Global banks could, for instance, use Bitcoin-like systems to move money between subsidiaries. They could even issue their own crypto-currencies.

But turning Bitcoin into a platform comes with risks. Some geeks fret that the network will reach its maximum capacity of 300,000 transactions per day as new applications come online. Another worry is that as the blockchain, which has already trebled in size to 15 gigabytes over the past year (see chart), continues to grow, fewer of the network’s participants will store it.

Yet if history is any guide, the blockchain will be fine. Two decades ago, when millions went online...
after the invention of the web browser, pundits predicted the internet’s collapse. Technical fixes repeatedly saved the day. And even if Bitcoin were to break down, another similar system would most likely take its place.

From the print edition: Finance and economics