

Remaking money

The technology behind bitcoin was built to fix finance. What could possibly go wrong, asks Douglas Heaven

IN SEPTEMBER, on a luxurious carpet-covered stage at a hotel in New York City, the boss of the biggest investment bank in the US launched a savage attack on a notorious upstart. Bitcoin is a “fraud”, declared Jamie Dimon, CEO of JPMorgan Chase, useful only for get-rich-quick speculators and drug dealers. “Honestly, I am just shocked that anyone can’t see it for what it is.”

Plenty of responsible, law-abiding citizens were quick to disagree – and bitcoin’s value reached new heights in November, when it breached the \$8000 mark for the first time. But whatever your view on the world’s most famous cryptocurrency, Dimon’s last comment inadvertently highlights something that often goes unsaid: no one really knows what bitcoin is, or what it is destined to become. The same goes for the technology on which it is based, known as the blockchain, hailed in some quarters as an engine of disruption on a par with the internet.

As things stand, bitcoin is all things to all people. But the community of software developers and “miners” that maintain it are engaged in a civil war, a clash of ideologies that will go a long way to deciding its fate. Meanwhile, the banks it was designed to sidestep seem to be toying with the idea that its underlying technology could be useful. Given the extent to which we are all at the mercy of the financial system, how it plays out has consequences for everyone. Can bitcoin rebuild the very idea of money? Will the blockchain make finance fairer? And what could possibly go wrong?

Bitcoin was born out of the embers of the global financial meltdown of 2008. Its mysterious inventor, or inventors, known only as Satoshi Nakamoto, saw the role of the big banks in that fiasco and decided enough was enough. They would create a truly peer-to-

peer electronic currency – a way for people to store and exchange digital coins without the need for banks or any other central authority.

The money most of us use every day has value because it is backed by a government. Take that away and the £10 note in your pocket is only worth the paper it is printed on – pretty much zilch. Its value is based entirely on faith in the institutions that back it. But as the 2008 crash demonstrated, the institutions in which we place our faith are liable to let us down.

Nakamoto spelled out the problem with these so-called fiat currencies in a short post online when bitcoin launched in 2009: “The root problem with conventional currency is all the trust that’s required to make it work. The

“If we can use blockchains to create binding contracts, we could bypass estate agents”

central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.”

Take quantitative easing, where central banks try to kick-start the economy by creating more money and handing it to the banks so they can lend it. “There is no worse thing you could do to exacerbate the gap between the rich and the poor than pump a bunch of free money into the system that only wealthy people could get their hands on,” says Nolan Bauerle, director of research at cryptocurrency news website Coindesk. This currency manipulation is exactly the sort of thing bitcoin was invented to avoid.

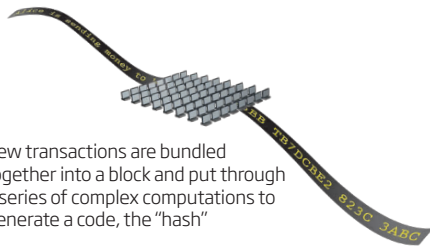
Nakamoto’s solution was to derive trust not from banks but from a new piece of software called the blockchain (see “Inside the trust machine”, page 38). This public ledger records every bitcoin transaction and is shared ▶

between everyone who uses the currency. Thanks to some nifty cryptography techniques, any new transaction added to the ledger is practically impossible to tamper with, and since it is public it can be viewed by anyone at any time. The result is a currency that is trustworthy without being backed by any one organisation.

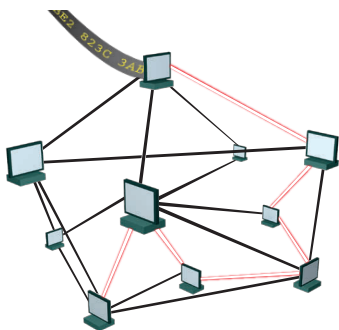
Since 2009, bitcoin has boomed, bombed, then boomed again. In its early days, its use in dark-web drug markets gave it an image problem. But that is changing, partly due to its soaring value and partly because its potential uses for law-abiding people have become apparent. It has also inspired a menagerie of other cryptocurrencies, each building on blockchain technology in different ways.

Inside the trust machine

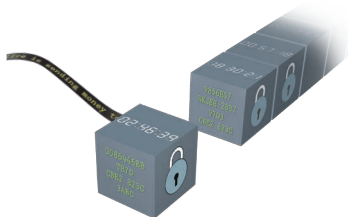
The blockchain is a digital ledger that uses cryptography and distributed computing to maintain an unalterable record of transactions



New transactions are bundled together into a block and put through a series of complex computations to generate a code, the “hash”



This hash is broadcast to all the computers on the blockchain network. Any attempts to alter transaction data would produce a completely different hash, which would be obvious to the network



Only when the hash is verified can it be added to the chain – a shared database that is practically tamper-proof

These days, there are more than 1000 of them, says Garrick Hileman at the University of Cambridge, who studies digital money.

But for all that, it still isn't clear what bitcoin is. Many see it as something more akin to gold than money: an asset that may be tricky to exchange for goods but has intrinsic value. Like gold, bitcoin takes time and energy to extract by mining (see “How bitcoins are made”, below right), and scarcity is guaranteed because the system is designed so there can never be more than 21 million bitcoins.

One thing is clear: it isn't yet a currency that most of us can spend. True, you can use it to buy pizzas, cars and holidays from a select few online vendors. But take it into your local grocery store or pub and the best you can hope for is a blank stare. The truth is that “it won't become [a form of currency] until people are paid in it”, says Hileman. And that means governments will probably need to recognise it first. For the time being then, the most likely way for bitcoin to go mainstream is to compete with the likes of Visa and PayPal as an electronic payment system in which bitcoins, rather than fiat currency, are exchanged.

That is certainly the view of one faction in the bitcoin community. To make this happen, they want to change the underlying software so it can support more transactions. Other members see things differently. They insist that such changes would raise barriers to entry, concentrate power in the hands of a few mining groups – and thus betray the very aims on which the whole venture was founded.

In August, the dispute escalated into a civil war and led to a split. The end result was a new version of bitcoin, called Bitcoin Cash, that supports more concurrent transactions. Which version wins will go a long way to deciding whether bitcoin will ever be more than a niche phenomenon.

Then again, there is another scenario in which it could affect everyone – and perhaps not in a good way. As the infighting continues, the banks that bitcoin was set up to subvert are sniffing around. This July, the US Commodity Future Trading Commission granted a bitcoin trading platform called Ledger X the first licence to operate as a clearing house for derivative contracts – in which value is derived from the price of an underlying financial product – that are settled with bitcoin. The respectability associated with a licensed platform should attract more investors, who would hold on to their bitcoins and thereby take more of them out of circulation, which could in turn dampen volatility. Or it could just inflate a bubble that is already fit to burst.



Bitcoins are “mined” in warehouses where computers run 24/7

What really has some observers' alarm bells ringing, however, is the notion that bitcoin might quietly get woven into the intricate web that links different parts of the financial system. In an interview with US news channel CNBC in October, Joe Saluzzi at Themis Trading said that the trading of bitcoin-linked products reminds him of the financial crisis. “I have a problem that on Wall Street the innovators are trying to package something up and put a derivative label on it when they really don't know what's underneath.”

In the run-up to the 2008 crash, traders were passing around newfangled financial products that masked the collapsing value of the risky mortgages at their heart. Similarly, the value of financial products packaged around bitcoin would be hard to determine if the cryptocurrency at their core, prone to wild fluctuations, were hidden.

One thing that made the collapse of the “sub-prime” mortgage market so devastating was that so many parts of the financial system were interconnected, with loans and debts stacked and bundled together in ever more complicated ways. As financial journalist Matt Lynn has pointed out, we don't really know how banks are experimenting with blockchains or which derivatives have been hitched to what cryptocurrency. If one bubble bursts, the shock waves could again spread far and wide.

But the promises and perils of cryptocurrencies go way beyond money. Many believe that the underlying blockchain

متن کامل مقاله

دریافت فوری ←

ISIArticles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات