

The  
Economist

You are now logged in

Can cryptocurrencies recover?

# Flaws in Bitcoin make a lasting revival unlikely

*The latest boom and bust invite comparisons with past financial manias*



Max Löffler

Print edition | Finance and economics

Mar 28th 2019



“Be more Brenda,” said the ads for CoinCorner, a cryptocurrency exchange. They appeared on London’s Underground last summer, featuring a cheery pensioner who had, apparently, bought Bitcoins in just ten minutes. It was bad advice. Six months earlier a single Bitcoin cost just under \$20,000. By the time the ads appeared, its value had fallen to \$7,000. These days, it is just \$4,025 (see chart)

**The Economist**

As Bitcoin was soaring, big financial institutions such as Barclays and Goldman Sachs flirted with opening cryptocurrency-trading desks. Brokerages sent excited emails to their clients. The Chicago Board Options Exchange (CBOE), one of the world’s leading derivatives exchanges, launched a Bitcoin futures contract. Hundreds of copycat cryptocurrencies also soared, some far outperforming Bitcoin itself. Ripple rose by 36,000% during 2017.

OGLAŠEVANJE



Ponovi

inRead invented by Teads

The bust has been correspondingly brutal. Those who bought near the top were left with one of the world’s worst-performing assets. Cryptocurrency startups fired employees; banks shelved their products. On March 14th the CBOE said it would soon stop offering Bitcoin futures. Bitmain, a cryptocurrency miner, appears to have pulled a planned IPO. (Miners maintain a cryptocurrency’s blockchain—a distributed transaction database—using huge numbers of specialised computers, and are paid in newly minted coins).



## The Economist

The speed with which the bubble inflated and then popped invites comparisons with past financial manias, such as the Dutch tulip craze in 1636-37 and the rise and collapse of the South Sea Company in London in 1720. Cryptocurrency enthusiasts like to claim a more flattering comparison—with the 1990s dotcom bubble. They point out that, despite the froth, viable businesses emerged from that episode. But the cryptocurrency fiasco has exposed three deep and related problems: the extent of genuine activity is hugely exaggerated; the technology does not scale well; and fraud may be endemic.

Consider the overstatement of activity, first. Ten years after their invention, using cryptocurrencies to pay for goods and services remains a niche pastime. Bitcoin is the original cryptocurrency and still the most popular. In January Satoshi Capital Research, a cryptocurrency firm, declared that

Bitcoin transactions in 2018 added up to \$3.3trn, more than six times the volume handled by PayPal. But such figures include an awful lot of double-counting, mostly related to the way Bitcoin handles change, says Kim Grauer at Chainalysis, a firm that analyses Bitcoin's blockchain. Strip that out, and Chainalysis reckons that Bitcoin accounted for around \$812bn of genuine transfers of value.

**The Economist** You are now logged in  
Grauer reckons, only a fraction was used to buy things. Around \$2.4bn went to payment providers, which handle payments for businesses—a piffling sum compared with the \$15trn of transactions in 2017 on Alipay and WeChat Pay, two Chinese payment apps. Darknet markets, which sell stolen credit-card details, recreational drugs, cheap medicines and the like, made up \$605m, and gambling sites \$857m. Most of the rest was related to speculation.

Even for speculators, business is less brisk than it seems. “Wash trading”, in which traders buy and sell to each other (or themselves) to create the illusion of volume, is widespread. Bitwise Asset Management, a cryptocurrency-fund manager, analysed 81 cryptocurrency exchanges for a presentation on March 20th to the Securities and Exchange Commission, an American financial regulator. The firm estimated that 95% of trading volume could be artificial. The Justice Department is investigating claims of price manipulation.

The second problem is that the technology is too clunky to operate at scale. Cryptocurrencies are unlikely ever to achieve mass adoption, says Nicholas Weaver, a computer scientist at the University of California, Berkeley. Unlike Alipay or WeChat Pay, cryptocurrencies are intended as new financial systems rather than extensions to the current one. But they have serious design flaws.


Bitcoin's pseudonymous creator, Satoshi Nakamoto, wanted it to be resistant to control by tyrannical governments and banks. Payment records are therefore not held centrally, but broadcast to all users. A new batch of Bitcoin is issued every ten minutes on average. That limits the network to processing about seven transactions per second (Visa, by contrast, can handle tens of thousands per second). In 2017, as the crypto-bubble was inflating, the system became clogged. To ensure that transactions went through, users had to pay miners—at one point, as much as \$50 per transaction.

Moreover, Bitcoin is designed such that only 21m Bitcoins will ever be created, making it inherently deflationary. Mining, essentially a self-adjusting lottery in which participants compete to buy tickets, is energy-hungry. At the height of the boom it was thought to consume as much electricity as Ireland (these days, it merely consumes as much as Romania).

The final problem is fraud. Transactions are irreversible—a boon for con-artists. Ponzi schemes are common, as is incompetence. Cryptocurrency exchanges often collapse or are hacked. In February Quadrigacx, a Canadian exchange, filed for bankruptcy, saying it had lost \$165m in deposits when its founder, Gerard Cotton, died, since only he had known the encryption keys protecting Quadriga CX's deposits. But on March 1st Ernst & Young, which was appointed to handle the bankruptcy, said that the deposit addresses seem to have been empty for at least eight months before the date Mr Cotton is said to have died.

## When Lambos?

Attempts are under way to get round some of these limitations. Some Bitcoin enthusiasts are testing an add-on called the Lightning Network, which tries to speed things up by moving many transactions off the blockchain. Stablecoins, whose value is supposedly pegged to something else, are touted as a way to rein in speculation. Once again, promise often falls short of reality. On March 20th, the most popular stablecoin, with \$2bn-worth in circulation, said that it might not be worth dollars after all. None has achieved even Bitcoin's limited take-up.

 You are now logged in  
Most fans simply want cryptocurrency prices to start rising again. In 2017 John McAfee, a cryptocurrency enthusiast who made his money in antivirus software, said that if Bitcoin was not worth \$1m in 2020 he would eat an intimate part of his anatomy on television. On March 20th he tweeted that losing that bet was "not mathematically possible". Last year Jack Dorsey, Twitter's boss, said he thinks Bitcoin will be the world's "single currency" within a decade. Facebook is working on some kind of cryptocurrency project. Market analysts and pundits provide cheery reassurance that the currency will soon soar again.

Mr Weaver is sceptical, at least in the short term. The very visible boom and bust, and more attention from regulators, have probably cut the number of willing new punters, he says. But boosters are trying their best. They have taken to referring to the post-bust period as a "crypto winter". The intended analogy is with artificial intelligence: the "AI winters" were funding crunches in the 1970s and 1980s after hype outstripped reality. The implication is that, one day, summer will return.

*This article appeared in the Finance and economics section of the print edition under the headline "The madness of crowds"*