What to make of cryptocurrencies and blockchains

Cryptocurrencies and their underlying technology, blockchains, have been hyped to the skies. Tim Cross offers a realist's guide.
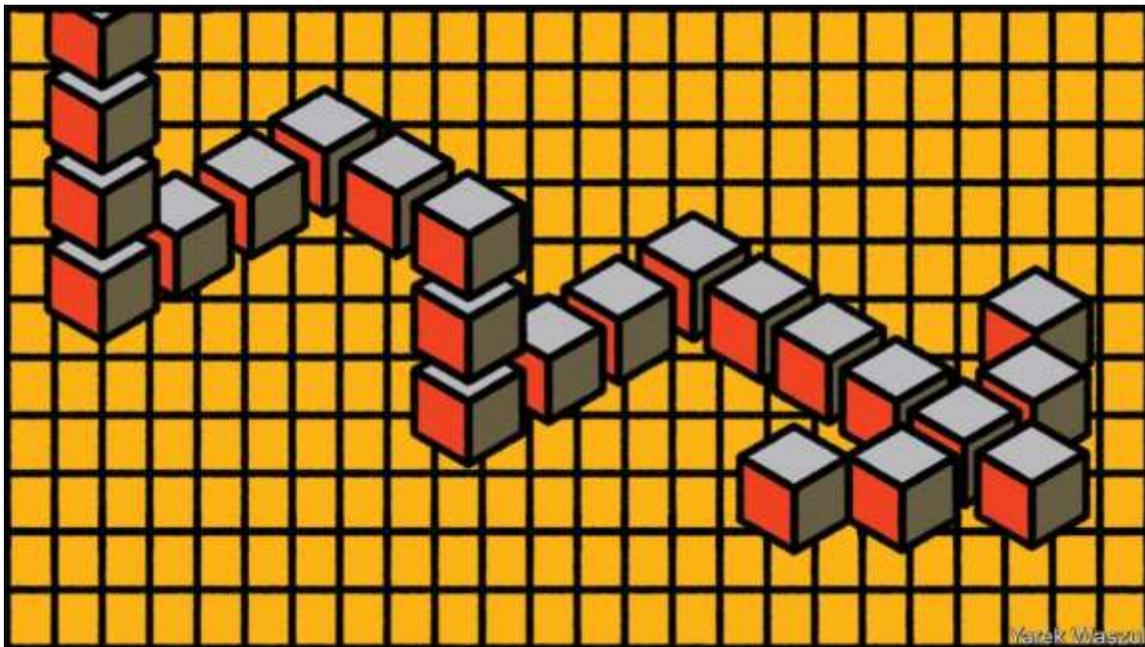
Print edition | Technology Quarterly

Aug 30th 2018

JOSEPH KENNEDY, John F. Kennedy's father, supposedly said that when he started getting share tips from his shoeshine boy, he knew it was time to sell. That was in the late 1920s. One investor in cryptocurrencies recalled that remark when he saw advertisements on the London Underground that seemed to suggest pensioners invest in bitcoin. "Be More Brenda," said the poster, featuring a white-haired lady claiming to have bought bitcoin in under ten minutes.

Cryptocurrencies are everywhere. According to one survey, 5% of Americans hold some cryptocurrencies—not bad for a financial product that is only a decade old.

Bitcoin is the best-known, and in 2017 the dramatic rise in its price—from $3,000 in September to almost $19,000 by December—made headlines.

It was invented in 2008 by a reclusive cryptographer going by the name of Satoshi Nakamoto. He was dissatisfied with the conventional financial system, so he wanted to create an electronic version of cash that did not rely on a central operator and was free from direct control by a government or central bank. The idea took off. These days anyone who wants to get into cryptocurrencies can weigh the relative merits of bitcoin, ether, Monero, Dash, Litecoin and thousands of others. Many of those who bought in early have, on paper at least, made astonishing gains. Bitcoin's price in 2010 was around 6 American cents. Even at its current price of $6,470, it would provide an early investor with a handsome profit—though not nearly as handsome as if he had sold at the peak last December.

In keeping with their do-it-yourself image, cryptocurrencies have given rise to initial coin offerings (ICOs), a way for cryptocurrency companies to crowdfund themselves. Cash is pouring in. According to one estimate, from Coinschedule, a firm that tracks such things, by early August 706 ICOs had raised almost $18bn from a mix of institutional investors and individuals this year. That compares with just 221 ICOs in the whole of 2017, raising $3.7bn.

Chain reaction

Many of those startups hope to capture the benefits of blockchains, the technology that underlies cryptocurrencies. In essence, a blockchain is a database designed to be distributed among many users, to be immutable, to work without oversight from any central authority and to dispense with the need for its users to trust each other. These qualities, it is argued, make it suitable for a huge variety of new and exciting business applications, which many companies are now trying to explore.

For example, a blockchain's immutability and distributed nature would seem perfect for streamlining supply chains. A widget manufacturer in one country, its shipping agent, its customer in another country and customs authorities on both the sending and the receiving end could all use the same database to track the widget. Another promising idea might be to provide an incorruptible record of transactions covering anything from property deeds to the provenance of diamonds.

According to Crunchbase, an industry consultancy, in the first five months of this year a total of more than $1.3bn of venture capital was invested in blockchain startups. KPMG, a large consultancy firm, reckons that the amount of money venture capitalists

want to invest in such things outstrips the opportunities to do so. Established companies are rushing to catch up. Technology firms such as IBM, Oracle and Amazon are giving their customers the chance to experiment with blockchains. KPMG offers a service to advise clients on blockchains, as do most of its rivals. Diar, a consultancy specialising in cryptocurrencies, lists dozens of blockchain-related patent applications, filed by companies as diverse as Bank of America, Intel, a chipmaker, RWE, an electricity firm, and British Telecom.

A bit of a let-down

This Technology Quarterly will take a more sceptical view. It will point out that, despite a decade of development, bitcoin has failed in its stated objective: to become a usable currency. Security is poor (according to one estimate, around 14% of the supply of big cryptocurrencies has been compromised); its decentralised nature inevitably makes it slow; there is no consumer protection; and the price is so volatile that not many people would want to use it as a means of exchange for goods and services. Other cryptocurrencies suffer from similar problems. Few merchants accept them.

At the same time the technology's built-in antipathy to regulation has attracted plenty of people who feel the same way for the wrong reasons. Some cryptocurrencies amount to Ponzi schemes, and unscrupulous ICO operators have swindled investors. America's authorities are investigating allegations of widespread price manipulation. Social-media firms have banned advertisements for ICOs amid concerns about fraud. Anyone thinking of investing in such instruments will need to do a lot of homework first.

Other drawbacks of bitcoin and such like are becoming increasingly apparent, too. The "mining" process required to verify all transactions is hugely power-hungry. Data centres have sprung up from Mongolia to Quebec, collectively consuming as much electricity as entire countries to run a system that cannot manage more than a handful of transactions per second.

The potential applications for the underlying blockchain technology look rather more attractive, but progress in developing them has been slower than hoped, and some apparent successes turn out to have been exaggerated. Because they are power-hungry and slow, the blockchains that drive cryptocurrencies have to be remodelled for use in business, which can make them less distinctive and more like other databases. Though the excitement surrounding the technology has provided a useful push to get interested parties around the table and start talking, most blockchain projects are still at the exploratory stage.

Putting a business on a blockchain is as complicated as any other big IT project. Those involved in the planning stage still have to ask the usual questions. What exactly is it meant to do? Why would an individual company want to sign up to such a shared venture? Who will design the system? Who will be in charge if things go wrong? And once a decision is made to build such a system, there will still be a lot of grunt work to be done. All this suggests that, whatever the benefits of blockchains, they will not arrive overnight.

One problem, says Gary Barnett, an analyst at GlobalData, a consultancy, is mutual incomprehension between insiders and outsiders. "There's a 'two tribes' vibe about a lot of this," he says. Because blockchains and cryptocurrencies are notoriously complicated, non-experts from other industries can end up confused by techno-speak, whereas advocates of the technologies are so excited by the potential that they give insufficient attention to important details of the industries they are aiming to revolutionise.

To understand the pros and cons of cryptocurrencies and blockchains, the best way is to start with bitcoin itself.

Read on: How to put bitcoin into perspective>>

Cryptocurrency prices correct as of August 21st

This article appeared in the Technology Quarterly *section of the print edition under the headline "A cryptic message"*