The Economist

Bitcoin

The magic of mining

Minting the digital currency has become a big, ruthlessly competitive business

Jan 10th 2015 | BODEN, SWEDEN | From the print edition

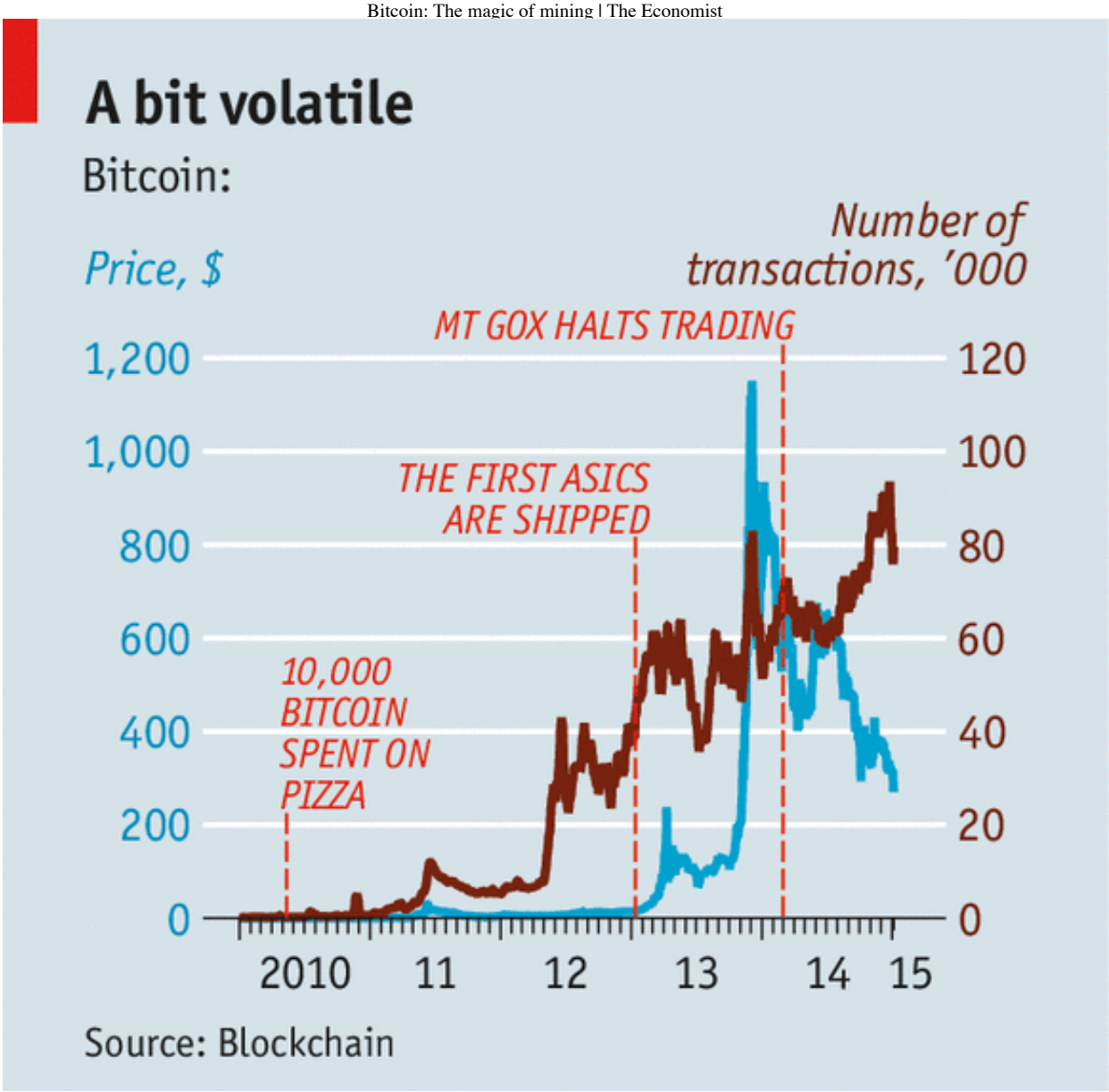
Deep down in the bitcoin mine

A HUGE aircraft hangar in Boden, in northern Sweden, big enough to hold a dozen helicopters, is now packed with computers—45,000 of them, each with a whirring fan to stop it overheating. The machines (pictured) work ceaselessly, trying to solve fiendishly difficult mathematical puzzles. The solutions are, in themselves, unimportant. Yet by solving the puzzles, the computers earn their owners a reward in bitcoin, a digital "crypto-currency".

The machines in Boden are in competition with hundreds of thousands more worldwide. The first to solve a puzzle earns 25 bitcoins, currently worth $6,900. Since bitcoin's invention in 2008 by a mysterious figure calling himself Satoshi Nakamoto, people have increasingly traded it for real money, albeit at a wildly varying price (see chart). Although there are only $3.8 billion-worth of them in circulation—about twice the value of Paraguayan guaraníes in use—bitcoins have three useful qualities in a currency: they are hard to earn, limited in supply and easy to verify.

But stability is important too: just over a year ago a bitcoin was worth four times as many dollars as now. But then Mt Gox, the crypto-currency's biggest exchange, collapsed and the bitcoin bubble burst. Critics make comparisons with 17th-century "tulip mania", and predict that bitcoin mania will fizzle out in similar fashion. On January 5th Bitstamp, another bitcoin exchange, halted operations and reported that 19,000 of the currency units had vanished in an apparent hacking attack.

The price collapse and the exchanges' woes do not tell the whole story, though: increasing numbers of businesses are accepting payment in bitcoin, including Time Inc and Microsoft; and



whatever the fate of bitcoin, the technology may spawn a range of alternative crypto-currencies and provide the basis for other businesses involving such things as the transfer of assets.

When Mr Nakamoto announced his invention (but not his true identity, see article (http://www.economist.com/news/business-books-quarterly/21638093-rise-and-fall-crypto-currency-good-news-authors-least-much)), several digital-cash schemes, including DigiCash and e-gold, had failed, or were in their death throes. But whereas some had tried to create the electronic equivalents of bills and coins, bitcoins only exist as entries in a giant electronic ledger called the "blockchain". This contains the history of every transaction in the coin, and copies of it are held on many computers around the world. What this means is that unlike conventional currencies and earlier digital ones, bitcoins do not need trusted third parties to handle flows of money or a "central bank" to issue it.

The computers that solve the puzzles also process transactions in the currency and update the blockchain. Every ten minutes each machine or group of machines takes a block of pending

transactions, and uses it as the input for a mathematical puzzle. The first to find a solution announces it to the rest, which check that it is right, and that the transactions are valid. If a majority approve, the block is cryptographically attached to the ledger and the computers move on to a new set of transactions.

If a fraudster wanted to spend a bitcoin twice, he would need to disguise it by rewriting the ledger. To do this he would single-handedly have to control more than half of the network's computing capacity. But such a "51% attack" would be prohibitively expensive: Coinometrics, a data provider, reckons it would cost $425m in equipment and electricity.

The enigmatic Mr Nakamoto designed the system to keep everybody honest. For instance, successful miners have to wait for a further 99 blocks of transactions to be processed before they get their rewards—so there is a constantly refreshed pool of participants with an interest in ensuring that everyone else keeps to the rules.

The system of rewarding successful miners with bitcoin has proved an effective way to get the currency into circulation. Operators of conventional payment systems live on transaction fees, but that business model would not have worked for bitcoin in its early days, because of a lack of users. However, as bitcoin becomes more popular, the idea is that miners will be able to start charging significant transaction fees, and that these will become their main source of income. It will need to: the system cuts the reward for solving puzzles every four years or so.

Despite the slump in bitcoin's value—last year it performed even worse than the Russian rouble and Ukrainian hryvnia—the combined mining power on the network is still increasing, and some miners are still investing in upgrading their machines, making this one of the fastest-moving parts of the IT industry.

Brew your own money

In the crypto-currency's early days, most miners were small-scale, trying to mint money on their home computers. This was Mr Nakamoto's libertarian dream: home-brewed money, without the need for central authorities. But as bitcoin's value rose, it all became more businesslike. Individual miners started to combine their computing power and share the rewards. Most mining today is provided through such "pools".

Startups from all over the world began building specialised hardware powered by custom-built chips, known as application-specific integrated circuits (ASICs). Leaving the amateurs behind, these firms soon became locked in a digital arms race. Microprocessors usually double their power every 18 months, a rhythm called Moore's law. In the case of mining ASICs, this doubling has occurred every six months.

Mining has also moved into the cloud. Firms have started selling online mining capacity in "gigahashes per second", or Gh/s—that is, for a fee they will provide enough computing power to make one billion attempts a second to solve a "hash function", as the puzzles are called. For instance, Genesis Mining charges $702 for 1,000 Gh/s plus a small fee for electricity.

Given the nature of the business, one would expect the bosses of bitcoin-mining firms to be super-geeks. But instead of coming from Silicon Valley, they typically hail from places like Sweden and Georgia—and talk (and often look) more like real miners. "I'm no libertarian but a businessman," says Sam Cole, the "C" in KnCMiner, the operator of the giant mining facility in Boden and a maker of mining computers.

Like other energy-intensive industries such as smelting aluminium, minting bitcoins is more efficiently done at scale, and in places where electricity is cheap and reliable. It also helps to be somewhere cold, to reduce the cost of cooling the machines. KnCMiner's hangar is near the Arctic Circle and right next to a hydroelectric dam.

The makers of mining computers benefit from the way the bitcoin system adjusts the difficulty of the puzzles, every two weeks, according to how much computing power is hooked up to the system. In theory the difficulty can be adjusted in both directions: upwards, to ensure that the system does not get swamped by an excess of prize-seeking machines; and downwards, to encourage miners to keep their machines online when things get too quiet. But until now the difficulty has mostly gone upwards: since the first ASIC chips were introduced in early 2013, it has increased by a factor of 10,000. As a result, new mining computers, which each cost several thousand dollars, have been becoming obsolete in a matter of months.

When the bitcoin price was rising, many of its fans thought investing in mining equipment was a better bet than simply buying and holding the currency. They were willing to plunk down top dollar months ahead of delivery of the computers. These advance payments allowed KnCMiner and other makers to manage without having to raise any financing.

What happens in the wake of the bitcoin price collapse is unclear. The long queues for mining rigs have dispersed. Demand for renting cloud-based hashing-power is stagnant. Many equipment-makers have ended up running the machines for their own benefit—and selling some of their stock of bitcoins to cover costs. Some people say this is why the currency has kept falling.

People in the industry are already discussing at what price mining becomes unprofitable. But Mr Cole is unfazed. Where others see a weak price, he just sees all the bitcoin yet to be mined, and lots of struggling rivals set to exit the business. He recently raised $14m in venture capital, looking forward to a bigger slice of a less competitive market. If other miners do give up, the difficulty of the puzzles may fall—so winning bitcoins would get easier.

Perhaps it is a good thing that the breakneck growth of a year ago has ended: had it continued, the system would soon have hit the limits of its capacity. The bitcoin protocol in its current form can only process seven transactions per second—nothing compared with the capacity of conventional payment systems such as Visa, which can handle 10,000.

Not very green

A more fundamental worry is that digital-currency mining, like other sorts of mining, has environmental costs: all that number-crunching uses a lot of electricity, and not all of it comes from renewable sources, as it does in Boden. The rapid development of the ASICs chips has made the machines more efficient, but even if all mining worldwide were carried out in modern facilities like Boden's, the combined electricity consumption would be 1.46 terawatt-hours per year—the consumption of about 135,000 average American homes.

A bigger concern is that, as the mining pools have got bigger, it no longer seems inconceivable that a bunch of miners might amass enough capacity to dominate the system and become capable of mounting a 51% attack. Last June one pool, GHash.IO, had the bitcoin community running scared by briefly touching that level, before some users switched to other pools.

Such is the complexity of the system that some analysts wonder if it might be possible for a rogue pool to launch an attack with a much smaller share. And the truth is that no one is sure how concentrated the industry already is. About a fifth of mining power is classified as "unknown", meaning it is not clear who owns it.

Chances are that many of these mystery machines live in China. At any rate, mining is likely to grow rapidly there. Miners in Inner Mongolia—where electricity is cheap thanks to abundant coal, over-investment in power plants and lax environmental rules—are reportedly building data centres much bigger than any in the West. "I've always feared that mining will concentrate in a few countries," says Yifu Guo, a founder of Avalon, a designer of mining chips. He even worries that a hostile government might seize control of the bitcoin system. Others worry that it might, at least, end up as a monopoly.

Whether the bitcoin system can avoid such outcomes will depend on whether its participants can agree on reforms to stop it becoming too concentrated. However, it may have become too successful for its own good: when billions are at stake, vested interests tend to defend the status quo.

As with the internet, the governance of bitcoin follows the principle of "rough consensus and running code". Everybody can pitch in on online forums. If there is general agreement and the solution has proved workable, the system's software code is updated by one of its five main developers—who "emerged" as pre-eminent figures during bitcoin's early days.

Then follows the real test: whether miners accept the changes. They "vote" in favour of a software update by installing it on their machines. And it only becomes part of the system if a large majority do so. That has not been a problem so far. But miners may still balk at any future changes they fear could cost them money. Gavin Andresen, one of the five main developers, is optimistic this can be avoided. If miners did block better solutions, there would be a "fork", meaning that a part of the bitcoin community would start a new currency.

Some groups have already launched their own crypto-currencies. Many of these "altcoins" are the bitcoin equivalent of stockmarkets' highly speculative "penny stocks". But some offer real innovation: Ripple and Stellar do away with mining altogether and use other mechanisms, such as voting, to create the currency and update the blockchain. Now there is much talk about "side-chains", new blockchains pegged to that of bitcoin in such a way that the currency and other assets can be transferred between them, which could unleash even more experimentation.

Other groups are using the blockchain in ways Mr Nakamoto never intended. Some, such as CoinSpark, are offering services to transact in any asset over the network, including stocks and bonds, or use it for notarised messaging (by embedding the location and a summary of the message in a bitcoin transaction).

Where all this may lead to is a constellation of linked crypto-currencies and blockchains, with all sorts of uses: stores of value, means of exchange, mechanisms for transferring assets and verifying transactions, whatever. The original bitcoin may remain at the centre of this constellation—or not. Whether its price recovers from last year's slump may not matter. Whoever and wherever he is, Mr Nakamoto can be proud of having unleashed a wave of financial innovation, and founded what looks set to become a sizeable new branch of the global IT industry.

From the print edition: Business