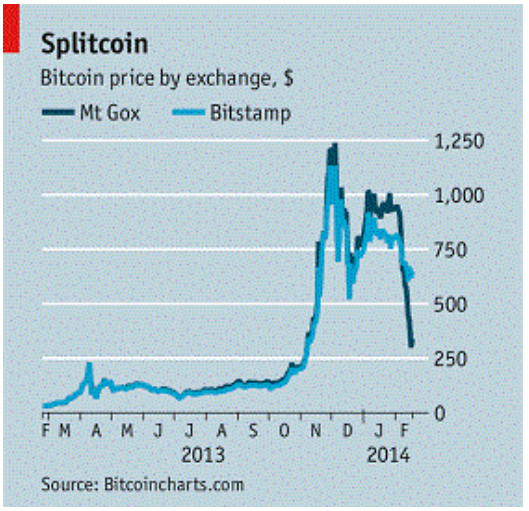
The Economist - Main report: February 22nd 2014

Cryptocurrencies: The great hiccup

Bitcoin is growing too fast for its technology to keep up

IN MOST businesses, a small coding error is a minor problem. With Bitcoin, an online "cryptocurrency", a fairly simple flaw seems to have cost $5.3 billion. That is how much the value of all of the Bitcoin in the world has fallen over the past two weeks, after a bug caused several Bitcoin exchanges to halt withdrawals temporarily. The price of a Bitcoin, which peaked at about $1,200 in December, is now about $630 on Bitstamp, one of the exchanges that has resumed trading. On Mt Gox, another exchange based in Tokyo, coins that still cannot be withdrawn are selling for far less (see chart).



The problems began with the discovery of a flaw in Bitcoin's code at the start of February. Bitcoin is, in effect, a giant shared transaction ledger, recording who owns each individual unit of the currency at any one time. Everyone must use the same copy of the ledger--known as the "blockchain"--to prevent the same coins from being spent twice. The flaw, known as "transaction malleability", muddles up the ledger so that successful Bitcoin payments do not appear to have been made. This could make it possible for hackers to trick badly-coded software--such as the proprietary Bitcoin wallets used by some exchanges--into sending money repeatedly.

To avoid any losses, most exchanges ceased all withdrawals while they checked that their software was secure. That sparked a panic as rumours spread that Bitcoin was fundamentally broken or that hackers had made off with customers' money. And then on February 14th about $2.5m of Bitcoin was apparently stolen from Silk Road 2.0, a website which is used to trade mainly illegal drugs. The site's administrators blamed transaction malleability for the hack.

Mike Hearn, a prominent Bitcoin developer, says the flaw is far from fatal. Indeed, Bitcoin's programmers have known about transaction malleability since 2011. What's surprising is that big exchanges such as Mt Gox were unprepared for it. Fixing it is technically simple but harder in practice, as it means getting a large majority of those running Bitcoin to accept new rules at about the same time. In the meantime, vigilance--and safer wallets--can prevent hackers.

Bitcoin's weakness stems from its success: speculators flocked to it long before it was ready for serious use. "There are still plenty of ways you can interfere with the Bitcoin network" says Mr Hearn. Sending vast numbers of small transactions slows the network down, for example. Other vulnerabilities are sure be discovered. One strength of Bitcoin is that its programming is "open source", meaning anyone can check it for flaws and suggest ways of fixing them as bugs arise. Yet it is also unsettling to rely on the work of volunteers when large amounts of money are involved.

Bitcoin has recovered from worse: since 2011 dozens of exchanges including Mt Gox have been hacked, and some have been robbed of millions of dollars. Its price has crashed by more than half several times. As crises go, this one is probably manageable.