The Economist
April 2013
How does Bitcoin work?

BITCOIN, the world's "first decentralised digital currency", was launched in 2009 by a mysterious person (or persons) known only by the pseudonym Satoshi Nakamoto. It has been in the news this week as the value of an individual Bitcoin, which was just $20 at the beginning of February, hit record highs above $250, before falling abruptly to below $150 on April 11th. What exactly is Bitcoin, and how does it work?

Unlike traditional currencies, which are issued by central banks, Bitcoin has no central monetary authority. Instead it is underpinned by a peer-to-peer computer network made up of its users' machines, akin to the networks that underpin BitTorrent, a file-sharing system, and Skype, an audio, video and chat service. Bitcoins are mathematically generated as the computers in this network execute difficult number-crunching tasks, a procedure known as Bitcoin "mining". The mathematics of the Bitcoin system were set up so that it becomes progressively more difficult to "mine" Bitcoins over time, and the total number that can ever be mined is limited to around 21m. There is therefore no way for a central bank to issue a flood of new Bitcoins and devalue those already in circulation.
The entire network is used to monitor and verify both the creation of new Bitcoins through mining, and the transfer of Bitcoins between users. A log is collectively maintained of all transactions, with every new transaction broadcast across the Bitcoin network. Participating machines communicate to create and agree on updates to the official log. This process, which is computationally intensive, is in fact the process used to mine Bitcoins: roughly every 10 minutes, a user whose updates to the log have been approved by the network is awarded a fixed number (currently 25) of new Bitcoins. This has prompted Bitcoin fans to build powerful

computers, or even to hijack other people's computers, for use in Bitcoin mining.

Bitcoins (or fractions of Bitcoins known as satoshis) can be bought and sold in return for traditional currency on several exchanges, and can also be directly transferred across the internet from one user to another using appropriate software. This makes Bitcoin a potentially attractive currency in which to settle international transactions, without messing around with bank charges or exchange rates. Some internet services (such as web hosting and online gambling) can be paid for using Bitcoin. The complexity and opacity of the system means it also appeals to those with more nefarious purposes in mind, such as money laundering or paying for illegal drugs. But most people will be reluctant to adopt Bitcoin while the software required to use it remains so complex, and the value of an individual Bitcoin is so volatile. Just as BitTorrent was not the first file-sharing service and Skype was not the first voice-over-internet service, it may be that Bitcoin will be a pioneer in the field of virtual currencies, but will be overshadowed by an easier-to-use rival.