The trust machine

The technology behind bitcoin could transform how the economy work

Bitcoin has a bad reputation. The decentralised digital cryptocurrency, powered by a vast computer network, is notorious for the wild fluctuations in its value, the zeal of its supporters and its degenerate uses, such as extortion, buying drugs and hiring hitmen in the online bazaars of the “dark net”.

This is unfair. The value of a bitcoin has been pretty stable, at around $250, for most of this year. Among regulators and financial institutions, scepticism has given way to enthusiasm (the European Union recently recognised it as a currency). But most unfair of all is that bitcoin’s shady image causes people to overlook the extraordinary potential of the “blockchain”, the technology that underpins it. This innovation carries a significance stretching far beyond cryptocurrency. The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. Simply put, it is a machine for creating trust.

To understand the power of blockchain systems, and the things they can do, it is important to distinguish between three things that are commonly muddled up, namely the bitcoin currency, the specific blockchain that underpins it and the idea of blockchains in general. A helpful analogy is with Napster, the pioneering but illegal “peer-to-peer” file-sharing service that went on line in 1999, providing free access to millions of music tracks. Napster itself was swiftly shut down, but it inspired a host of other peer-to-peer services. Many of these were also used for pirating music and films. Yet despite its dubious origins, peer-to-peer technology found legitimate uses, powering internet startups such as Skype (for telephony) and Spotify (for music streaming)—and also, as it happens, bitcoin.

The blockchain is an even more potent technology. In essence it is a shared, trusted, public ledger that everyone can inspect, but which no single user controls. The participants in a blockchain system collectively keep the ledger up to date: it can be amended only according to strict rules and by general agreement. Bitcoin’s blockchain ledger prevents double-spending and keeps track of transactions continuously. It is what makes possible a currency without a central bank.

Blockchains are also the latest example of the unexpected fruits of cryptography. Mathematical scrambling is used to boil down an original piece of information into a code, known as a hash. Any attempt to tamper with any part of the blockchain is apparent immediately—because the new hash will not match the old ones. In this way a science that keeps information secret (vital for encrypting messages and online shopping and banking) is, paradoxically, also a tool for open dealing.

Bitcoin itself may never be more than a curiosity. However blockchains have a host of other uses because they meet the need for a trustworthy record, something vital for transactions of every sort. […] Bitcoin fanatics are enthralled by the libertarian ideal of a pure, digital currency beyond the reach of any central bank. The real innovation is not the digital coins themselves, but the trust machine that mints them—and which promises much more besides.

Published in The economist. Oct 31st 2015

http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine