THE TIMES

Could these weird coins transform our lives?

Matt Ridley

Published at 12:01AM, September 29 2014

The electronic bitcoin may one day replace flawed currencies and make banks, and even governments, redundant

Amid the hurly-burly of war, disease and politics, you might be forgiven for not paying much attention to bitcoin, the electronic form of money favoured by radical libertarians and drug dealers. Yet it is possible that when the history of these days comes to be written, bitcoin's story will loom large. Unnoticed except by the tech-obsessed, the technology behind bitcoin may be slowly giving birth to a brave new world, with eventual implications well beyond money.

So argues a new book (*Bitcoin: The Future of Money?*) by the financial commentator and comedian Dominic Frisby. He makes the case that it is just possible that bitcoin and its rivals — known as altcoins — and the "blockchain" technology that lies behind them have the potential to spark a radical decentralisation of society itself. They could change the way governments finance themselves, make banks redundant and transform the ways companies are run. In the words of Jeff Garzik, a bitcoin developer, bitcoin could be "the biggest thing since the internet — a catalyst for change in all areas of our lives".

If he is right, then the founder of bitcoin will take his place alongside the great inventors. So who is he? To this day he remains carefully anonymous, and though Frisby makes a strong case for having unmasked him, the man he has identified is scarcely more visible than the disguise he uses. It is an alluring thought that history could be changed anonymously.

Bitcoin went live in January 2009, on the day that the British government announced a second bailout of the banks, an event referred to in a segment of computer code hidden inside the first bitcoins: it quoted a headline from *The Times*: "Chancellor on brink of second bailout for banks". That is significant for

two reasons. Satoshi Nakamoto, the pseudonym of bitcoin's founder, was clearly of the view that bitcoin's purpose was to replace a flawed system of banking and currency, and he was also hinting that he was British and read *The Times*.

Satoshi's Britishness extends to his language, which uses British phrases and spelling, and to the fact that his various messages are always time-stamped in Greenwich Mean Time. In fact he was doing his utmost not to sound like the American he is. The timing of his postings on a bitcoin forum suggested he was either a late riser on the US east coast or an early riser on the west coast.

Meanwhile "cypherpunks" were a group of programmers who had come together in Santa Cruz under the auspices of the computer pioneer Tim May in 1992. Their aim was to undermine what they saw as creeping government and corporate control over the nascent internet by inventing methods of encryption that people could use. "Arise! You have nothing to lose but your barbed wire fences," May told them. One of their first obsessions was a reliable form of electronic cash, a substance that the economist Milton Friedman had predicted would be the internet's most important gift to humanity.

Satoshi seems to have emerged from this group, which narrows Frisby's search. After analysing Satoshi's writing style, typing habits, computer coding skills and likely age, he eventually concludes that the main and perhaps only person behind Satoshi is a Californian with a degree in computer science and a doctorate in law named Nick Szabo. Of course, Szabo has denied it on Twitter.

Before his writing dried up around the time that bitcoin was being created, Szabo wrote a long essay on the history of money, called *Shelling Out*. In it he explored a throwaway remark by the evolutionary biologist Richard Dawkins that "money is a formal token of delayed reciprocal altruism", and drew upon other books in evolutionary psychology (including one of mine).

What Szabo was after and what Satoshi achieved was to emulate online the difficulty of mining precious metals. It requires vast amounts of computing power to "mine" each bitcoin today — and mining consists of the solving of massive mathematical puzzles by hard computer grind. He also set out to emulate the trustworthiness of paper money without a third party such as a bank or government to verify it, which is the real genius of bitcoin.

Furthermore, the system is designed so it cannot produce more than 21 million bitcoins, so debauching the currency by printing money is impossible. The number that can be mined halves every four years. Approximately 13 million have been mined so far, worth $6 billion today. Satoshi owns a large chunk of them and has not cashed in lest it reveal his identity.

How does bitcoin achieve these feats? Frankly, I don't fully understand it (I am not sure anybody outside computer science does) and they seem unable to translate it

into simple English. But in very broad outline, bitcoin is in effect a public ledger — a compendium of previous transactions, stored by bitcoin users all over the world. To participate in mining bitcoins you create a new block in that ledger and share it with others in encrypted form. This then makes bitcoin infallible as a register of who has transferred value to whom: every bitcoin carries its ancestral history in its code as verification that it is what it says it is. No third party is involved.

A new currency is just one application of such an idea. The blockchain's special feature is that it cuts out the need for somebody else to verify that something is what it says it is. This opens the possibility of self-enforcing "smart contracts" and "distributed autonomous organisations", which the digital expert Primavera de Filippi describes as networks that "once they have been created and deployed on to the blockchain . . . no longer need (nor heed) their creators".

A simple and primitive example is Twister, a blockchain-based social network with no corporate headquarters that a repressive regime might shut down. The next step might be this: imagine in the future summoning a taxi that is not only driverless but ownerless. It belongs to a network that has raised funds, signed contracts and taken delivery of vehicles autonomously, even though its "headquarters" is distributed all over the net.

Perhaps you can now see why Satoshi Nakamoto would not want to take credit for all this. Governments get jealous of people who make them look irrelevant. Look what happened to Bernard von NotHaus, who started openly selling tokens called "liberty dollars" in 1998 to people who wanted a hedge against inflation. As the economist Kevin Dowd recounts, after nine years of tolerating this, suddenly the US federal government arrested and prosecuted him on the flimsiest of grounds for counterfeiting, fraud and conspiracy. His real crime was to show the devaluing of real dollars. No wonder Satoshi keeps his head down.