**Source:** *The Sunday Times,* pB17
**Date:** 5 August 2018

# Five common bitcoin myths demystified

## Learning the associated jargon, sorting fact from fiction will help avoid potential financial losses

**Emir Hrnjic and Nikodem Tomczak**

Misinformation, myths and misnomers abound in the world of technology, frequently amplified on social media due to a lack of credible sources.

The emergence of cryptocurrencies, and bitcoin in particular, is no exception, with the promise of fast fortunes to be made helping to fuel the speed with which these myths spread.

Yet misinformation about how a technology works can hamper its adoption and use, and expose users to significant risk.

Here are five common bitcoin myths demystified.

### 1. BITCOIN TRANSACTIONS ARE ANONYMOUS

Perhaps one of the most ubiquitous myths about bitcoin is that it is anonymous in nature, and hence is widely used for illegal activities.

In fact, in any transaction, the addresses of bitcoin senders and receivers must be revealed, allowing law enforcement to easily track and trace them.

Bitcoin therefore would more accurately be described as pseudonymous, since all the transaction records, including times, amounts and addresses, are traceable.

In addition, any illegally acquired bitcoins have to be eventually cashed out via real-world transactions typically connected to a crypto exchange or a bank account.

Since banks and most of the popular exchanges follow strict anti-money-laundering and know-your-customer laws, these "cash-out" transactions effectively reveal bitcoin holders.

### 2. 'MINERS' ARE DISCOVERING OR CREATING BITCOINS

Mining refers to the process of recording, validating and adding new blocks of transactions to the bitcoin blockchain. This process prevents double spending, secures the network, and in return incentivises the miners by paying them for their work with newly created bitcoins.

The bitcoin code generates 12.5 bitcoins every 10 minutes, awarded to the miner that is first to validate the most recent block of transactions. In 2020, this award will reduce to 6.25 bitcoins per block, after which it will then halve every four years until the supply reaches a maximum of 21 million.

What this means is that, as more miners emerge and competition heats up, the chances of winning newly created bitcoins will diminish.

Security of the network notwithstanding, increasing or decreasing the number of miners has no influence on the bitcoin creation process since all the bitcoin miners compete for the same reward. But only one miner can be rewarded at a time.

Consequently, the miners are not discovering or creating bitcoins – the new coins are simply a reward for securing the network.

Therefore, rather than modern-day versions of Wild West gold prospectors, this makes bitcoin miners more akin to competitive accountants.


Bitcoin – with its logo seen here at the Consensus 2018 blockchain technology conference in New York City in May – is not discovered or created by "miners". Rather, they get new coins as a reward for securing the network. PHOTO: REUTERS

### 3. BITCOINS ARE SCARCE

The perceived gold-like scarcity of bitcoin stems from the fact that its computer code will generate bitcoins at regular intervals until the total number reaches a maximum of 21 million bitcoins.

Nevertheless, bitcoin's code properties are not rigid and the maximum coin supply can potentially be raised by majority consensus among miners, especially since newly minted bitcoins are crucial to incentivise mining.

Furthermore, bitcoin spin-offs such as bitcoin cash, bitcoin gold, and bitcoin private – essentially new currencies – have been created by a so-called "fork" in the blockchain.

These forks result from a radical change in the protocol, resulting in a group of miners creating a new offshoot of the chain.

These forks effectively increase the supply since they create additional bitcoin-like currencies. More importantly, there are already almost perfect bitcoin substitutes available such as litecoin – a tweaked bitcoin protocol with 84 million coins – effectively increasing the supply.

### 4. BITCOIN WALLETS HOLD BITCOINS

While real-world wallets hold real-world banknotes, crypto-wallets hold only the keys needed to access cryptocurrency that itself resides on the blockchain.

To be able to initiate a transaction, a user needs to know the public account address (derived from the public key) and sign the transaction using the corresponding private key, without revealing it.

In this context, wallets are software applications that hold the user's keys to access their bitcoins. Since bitcoin is virtual, the balance does not reside in the wallet but on the blockchain.

Furthermore, since losing access to the wallet means losing access to the monetary value stored on the blockchain, misplaced private keys account for a significant fraction of lost coins.

In 2013, for example, one early bitcoin miner accidentally threw away a hard drive with keys to 7,500 bitcoins, losing roughly US$65 million (S$89 million) at current prices.

### 5. BITCOIN IS IMPOSSIBLE TO HACK

The bitcoin network itself has never been hacked or compromised, unlike more traditional and well-established financial platforms such as Swift or Visa.

In fact, bitcoin's underlying software and consensus protocols are so secure that the closest potential threat lies in the development of quantum computing, and even that remains some time off.

But this is beside the point. Due to the way bitcoin is transacted, the real weakness in the system lies with careless bitcoin owners, incompetent app developers, poorly designed cryptocurrency exchanges and dishonest crypto companies.

Together, these account for nearly all of the hacked or lost bitcoins.

### GET YOUR INFORMATION STRAIGHT

The rapid emergence of bitcoin and other cryptocurrencies has been accompanied by an explosion of misinformation about them.

Correcting this and narrowing the knowledge gap is vital to improving understanding, strengthening user security and protecting novices from manipulation and exploitation.

As with all new technologies, learning the associated jargon and sorting fact from fiction are key to avoiding potentially heavy financial losses.

• Emir Hrnjic is a visiting senior research fellow at the Centre for Asset Management Research & Investments at NUS Business School. Nikodem Tomczak is a research scientist and adjunct associate professor at the National University of Singapore (NUS). The opinions expressed are those of the writers and do not represent the views and opinions of NUS.