



Property in a digital age

PART 4

> Security and adoption of bitcoin

BY BRIAN CHUNG

LAST week, we explored points to clear doubts on bitcoin technology. We also shared bitcoin entrepreneur Andreas Antonopoulos' tips and advice, bidding the authorities to think twice before making any decision on regulating bitcoin.

In this last of our four-part series, we share more of Antonopoulos' insights, including how safe it is to use bitcoin.

SAFE AND SECURE TECHNOLOGY

"The bitcoin network has been secure since Jan 3, 2009. There has not been a successful attack on the bitcoin system." Why one wonders, to which Antonopoulos says: "It's either that nobody has tried to attack it or everyone is trying to attack it."

The expert justifies the reason behind his rationale, considering that many have been trying to attack it. He says: "Everyone is trying to attack bitcoin. They have been at it continuously since 2009. Bitcoin now protects 12 billion US dollars, which is a big prize for whoever is successful in attacking it. It also serves as a lesson to teach

bitcoin and its users to be more careful as each person tries to attack it; the system adapts itself and becomes more secure. There is no one who has successfully attacked bitcoin over the past seven years; unlike regular financial institutions, where not a single bank in the world can accede to this."

It is remarkable but not magic, Antonopoulos feels; not that bitcoin has found a way to secure itself that nobody else is able to. "It is simply the result of de-centralising control among all the participants or players. So the only way to attack it is to attack everyone successfully," he said, which is quite impossible.

GOVERNMENT VIEW

In response to the emergence of "disruptive technology", the government has set up an organisation called the Malaysia Industry-Government Group for High Technology (MIGHT), to help understand new technology. MIGHT is a not-for-profit company under the purview of the Prime Minister's Department.

Its immediate role is to bring policy-makers and companies together to discuss leveraging new disruptive technologies. MIGHT and Bloktex were the two parties

which recently invited Antonopoulos to share insights on bitcoin technology. The intention was to provide the public and policy-makers with insights into this technology, and from who better than the expert himself.

MIGHT president Datuk Dr Mohd Yusoff Sulaiman shared his reason behind collaborating with Bloktex on the talk.

"Why we are very interested in working with Bloktex in this event is because we see Blockchain as the technology that will change the whole way of doing business. It will especially impact the financial and property sectors among others. I think this technology will mature and further develop and once it does, it will also affect the non-financial sectors," Mohd Yusoff shared. Another reason for hosting Antonopoulos and presenting the public with the talk on this growing new technology is to help Malaysia remain relevant and competitive among the global industry players.

Mohd Yusoff then shared about the nature of bitcoin and other disruptive technologies. "I think the nature of some of these new technologies that come under the umbrella of the fourth industrial revolution tends to be

RECOMMENDED RESOURCES AND READING FOR BETTER UNDERSTANDING OF BLOCKCHAIN AND BITCOIN TECHNOLOGY

- ▶ **Mastering Bitcoin by Andreas Antonopoulos**
- ▶ **The Internet of Money by Andreas Antonopoulos**
- ▶ **Bitcoin.org**
- ▶ **Blockchain: Blueprint for a New Economy by Melanie Swan**

multidisciplinary and brings sectors closer together, further redefining the sector in itself.

"For example, Uber itself is a combination or merging of two industries - telecommunications and transport. This is where we need to get industries and policy-makers together, to look into the future of how this new innovation is 'disrupting' our businesses and economy, hence use it to create more opportunities to improve businesses and economies," Mohd Yusoff added.

He urged the authorities, those in the financial sector, including the man on the street as well as business entrepreneurs, to look at today's modern technologies and new developments, and try to tap into these to further grow, improve and move from the traditional way of doing things.

"It is very important for us to

look at the overall technology development, not in isolation but as a bigger picture; how it will affect and change things for the better," he added.

MORE TIPS AND ADVICE

Today, bitcoin continues to impact industries, property included. However, Antonopoulos advocates the importance of fully understanding the concept of bitcoin before one "invests" into it.

"I 'speak for' bitcoin as an experimental technology that one should only invest in if one really understands the mechanics of it. You should primarily invest in learning and fully understanding the technical aspects that could turn bitcoin into an innovative industry that can lead to business start-ups and build careers," Antonopoulos said.

He reminds interested parties that bitcoin is not a stock investment. "If you hear someone tell you that this system is a sure investment, run away as fast as you can because those characteristics are shared by only one category of investment - scams."

The expert also prompts one to be alert and aware, especially in the Southeast Asian region where there are large numbers of new middle-class investors, many for the first time entering into the investment market. "Scams are extremely popular. When you hear things like bitcoin will make you rich, walk away. Bitcoin will not make you rich, but make you poor quickly. It is a volatile experimental system that comes with risks. I am advocating the understanding of this technology, not the use of it as speculative investment. Unless you need to use it and know how to use it, it is not an investment or a get-rich-quick scheme," Antonopoulos drives his point home.

Sharing Antonopoulos' sentiments, Mohd Yusoff said: "Blockchain is currently all the hype in Asia and we should look at it, learn and understand it, and relate it with the fourth industrial revolution. It is no longer business as usual as it fundamentally changes the way we work and live. Bitcoin might affect our work culture, policy and lifestyles. And MIGHT is looking at how we can and should integrate this technology into our lives." Follow our column next week featuring our monthly read on interior decor.

▶ Email your feedback and queries to: propertyqs@thesundaily.com

How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is string of letters and numbers, such as 1HULLMwZEPkjEPeCh43BeKJL1ybLCWrdpN.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Each address has its own balance of bitcoins.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's

Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair", composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

VERIFYING THE TRANSACTION

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

Gary, Garth, and Glenn are Bitcoin miners.

The miners' computers are set up to calculate cryptographic hash functions.

Hash value*
Each new hash value contains information about all previous Bitcoin transactions.
+ Nonce
= New hash value

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Cryptographic Hashes
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

Nonces
To create different hash values from the same data, Bitcoin uses "nonces". A nonce is just a random number that added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The root of all evil ???
0000 0000 0000...
Creating hashes is computationally trivial, but the Bitcoin system requires that new hash value have a particular form - specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes "coinbase" transaction that pays out 50 bitcoin to the winning miner - in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoin.

TRANSACTION VERIFIED
As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did - because any changes require a completely different winning nonce - and then redo the work of all the subsequent miners. Such a feat is nearly impossible.