Publication: Today , p 56
Date: 07 September 2017
Headline: Blockchain security not all that watertight

Blockchain security not all that watertight

FROM **KELVIN LOW FATT KIN**

A serious, albeit common, misrepresentation of blockchain technology is that it is impervious to fraud.

Bitcoin and its ilk are often referred to as cryptocurrencies because of the cryptographic protocols that underlie the blockchain technology.

However, it is important to realise that the cryptography simply entails the use of a public key and private key cryptographic system. For bitcoin, this means that your bitcoin is secure only if your private key is secure.

If you lose your private key, you lose access to your bitcoins. If someone acquires knowledge of your private key, that person acquires access to your bitcoins.

Much of the protocol behind bitcoins, as explained by the White Paper by the mysterious Satoshi Nakamoto, is concerned only to prevent double spending by end users, not secure their private keys against unauthorised access.

The problem of hacking that holders of cryptocurrencies face has been highlighted by other publications, most recently in The New York Times.

While many within the cryptocurrency investment community assume that the risks involved in losing one's private key are the same as losing one's bank PIN or Internet banking password, the two entail different risks.

Briefly, bank statements, whether issued on paper or available online digitally, are not legally authoritative of the outstanding debts owed by a bank to its customer. They are mere records that, if proven incorrect, can be corrected.

So the risk of a hack is not entirely borne by a customer but is shared between a customer and its bank.

> For bitcoin, this means that your bitcoin is secure only if your private key is secure. If you lose your private key, you lose access to your bitcoins. If someone acquires knowledge of your private key, that person acquires access to your bitcoins.

However, because cryptocurrencies purport to do away with so-called trusted third parties, the risk of any hack is borne exclusively by the holder of the cryptocurrency.

In a well-regulated banking system, depositing money with banks will often carry less risk of a total loss than investing in cryptocurrencies.

This will of course be different in a poorly managed system, but both, indeed all, systems entail exposure to risk arising from fraud.

As blockchain technology entails the use of distributed ledgers — copies of the same record kept throughout the network — this provides security in the sense that there is no single point of failure resulting in a complete loss of the records.

But the distributed ledger system provides zero protection from hackers acquiring a user's private key. Once spent, the record of the expenditure is simply replicated throughout the network.

Those looking to invest in bitcoin or any assets underpinned by blockchain technology, as promised by a rash of initial coin offerings, must remember this risk (Be wary of digital token investments: Police, MAS; Aug 11).

Other risks include the viability of the particular offering and its legality, as many initial coin offerings would be securities offerings regulated by the Monetary Authority of Singapore.