What is Bitcoin cryptocurrency?

Cryptocurrency has become the fastest-growing segment of the global financial world. Anyone who bought cryptocurrency before 2017 will have made astronomical gains.

But cryptocurrency trading has also drawn criticism – apart from the association of money laundering, susceptibility to hacking, fraud and theft, governments and central banks worry about loss of control over regulation and money supply if virtual currency were to become the norm.

But love it, fear it, hate it, cryptocurrency is set to become a part of the new world economy in the 21st century.

WHAT IS BITCOIN, OR RATHER, CRYPTOCURRENCY?

It is a digital currency that uses an open source protocol encryption network that is totally independent from any central authority. You can send or receive cryptocurrency via a computer or a smartphone. All you need is an address, an identifier string with numbers and letters that works like a bank account.

October 2008
Mysterious bitcoin creator Satoshi Nakamoto published a paper on a peer-to-peer electronic cash system. No one was able to confirm if Satoshi Nakamoto is a person or a group.

January 2009
Satoshi Nakamoto released the first bitcoin software. The first bitcoin transaction took place between him and Hal Finney, a programmer.

October 2009
Bitcoin receives an equivalent value in traditional currency, US$1 = 1.309 BTC. The equation includes the cost of electricity.

May 2010
An Internet lore is born when a programmer used 10,000 BTC to pay for two pizzas worth US$25. To commemorate the transaction, May 22 is dubbed Bitcoin Pizza Day.

August 2010
The bitcoin system is hacked with 184 billion bitcoins generated in a transaction. The bug is fixed.

January 2011
The Silk Road, a notorious drugs marketplace, is established, using bitcoin currency as an untraceable way to buy and sell drugs online.

December 2017
Bitcoin crosses US$17,000 milestone.

HOW TO BUY AND SELL DIRECTLY*

One way is physically, such as using a bitcoin machine, but options are limited. There is a bitcoin machine in Singapore, but no machines exist here for other digital currencies. Another is to set up an account on an online cryptocurrency exchange. The exchange will often ask for identification documents, and require bank transfers of money, before it lets users buy cryptocurrency through it.

RISKS

Unregulated. Scams abound; caveat emptor applies.

Extremely high volatility, no clear fundamentals for most price movements.

Exchanges' systems and websites can go down anytime, especially during large price movements, which will make it difficult for users to trade or withdraw funds.

CRYPTOCURRENCIES TO WATCH

Bitcoin (BTC)
The most well-known cryptocurrency, designed by a pseudonymous creator as a peer-to-peer payment network without a central authority.

Litecoin (LTC)
Aims to offer faster transaction processing than the bitcoin network, and is fully compatible with the bitcoin system.

Ethereum (ETH)
Launched in 2015, it is backed by Microsoft, JPMorgan and Intel. It allows users to run "smart contracts", essentially turning legal contracts into code. Smart contracts can automatically facilitate or enforce the agreement.

Ethereum Classic (ETC)
The competing version of the Ethereum platform is created after a major Ethereum project was attacked, which prompted Ethereum's creators to modify the project code.

Iota (IOTA)
Designed for the Internet of Things, to let connected devices trade resources and store sensor data securely, does not use a blockchain.

Ripple (XRP)
The Google-backed Ripple grew out of a project older than bitcoin that started in 2004. Designed for enterprise use, it offers banks and payment providers another way to source liquidity on demand for cross-border transactions.

Zcash (ZEC)
Uses zero-knowledge cryptography, which allows an entity to prove it knows something about hidden information without having to reveal that information.

NEM (NEM)
The popular platform in Japan provides services such as payments and messaging.

Monero (XMR)
Intended to be secure, private and untraceable, making it extremely unlikely that a transaction can be linked to a particular user.

BITCOIN MINING MALWARE

As the price of bitcoin soars, hackers are finding ways to mine bitcoins using malware installed on websites and visitors' computers.

The websites that host coin-mining programs, or such scripts, would use the visitors' computer resources for unauthorised mining. As a result, computer users will notice their computers slowing down significantly.

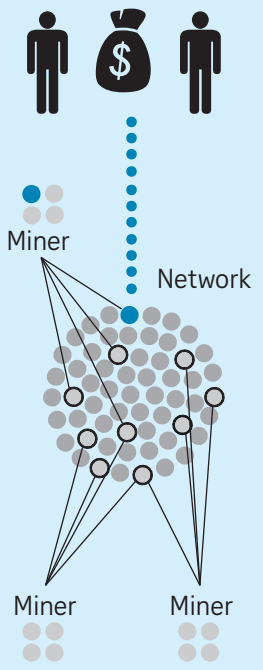
To protect against such attacks, users should use anti-virus software and firewalls, and not click on suspicious links.

BITCOIN BLOCKCHAIN

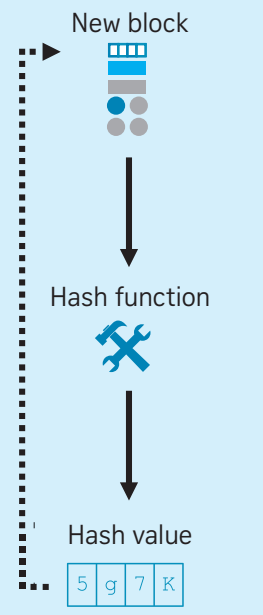
Most cryptocurrencies are built on blockchain technology, although new ones have emerged that do not use blockchain. A blockchain is a public ledger in which each update comprises new data and a full description of the database before the current update. When applied with certain rules and protocols, the blockchain makes it feasible to have an open database in which users always have the most updated version of the database, there is confidence in the integrity of the data, and many parties may independently update the data.

1 A buyer who wants to pay with cryptocurrency declares to the network how much he plans to transfer and to whom, and that declaration joins a network-wide pool of announced transactions.

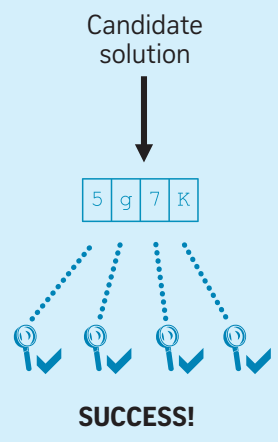
2 Miners working independently of each other race to create a new blockchain by adding a new block to a number of transactions from the pool and validate them to create a block of a predefined size. Each miner may pick whichever transaction to include in a block. To increase the chances of being picked, buyers may include a transaction fee amount of their own choosing that the miner can keep if he successfully provides an update to the blockchain. Anyone can be a miner.



3 A block of new transactions is combined with the current version of the blockchain, some other required information and a number called a nonce, and then run through an algorithm called a hash function to generate a hash value. There is a predetermined range to limit the pace of new bitcoin creation. If the miner's hash value falls outside of that range, the hashing is repeated with different values of the nonce until an acceptable hash value is obtained.



4 When a miner obtains an acceptable hash value, that hash value and all of the data that were fed into the hash function are broadcast to the bitcoin network, where other miners will verify the solution. If the majority accepts the new hash function as correct, the candidate will become the latest version of the blockchain.



BLOCKCHAIN USERS

• **Trade finance ledgers**
DBS Bank and Standard Chartered have teamed up to share records for trade finance contracts and transactions. By having a distributed ledger, the banks hope to avoid falling victim to companies that pledge a single contract or asset to more than one lender.

• **Trade settlement and clearing**
The Australian Securities Exchange is trying to develop a blockchain-based clearing and settlement system as a way to reduce administrative and reconciliation costs.

TWO SIDES OF THE SAME COIN

Coindesk estimated that about 85 per cent of the world's bitcoin trading volume came from China. Ordos, the famed ghost town of Inner Mongolia province, is now the centre of bitcoin mining facilities. However, the Chinese government is tightening its control over domestic cryptocurrency trading.

The Financial Services Agency, a Japanese government agency and an integrated financial regulator responsible for overseeing banking, securities and exchange, has recently issued operating licences to 11 bitcoin exchanges.

Source: COINMARKETCAP.COM, BITCOIN.ORG, ETHEREUM.ORG, RIPPLE.COM, LITECOIN.COM, COINDESK.COM, NEM.IO, IOTA.ORG STRAITS TIMES GRAPHICS