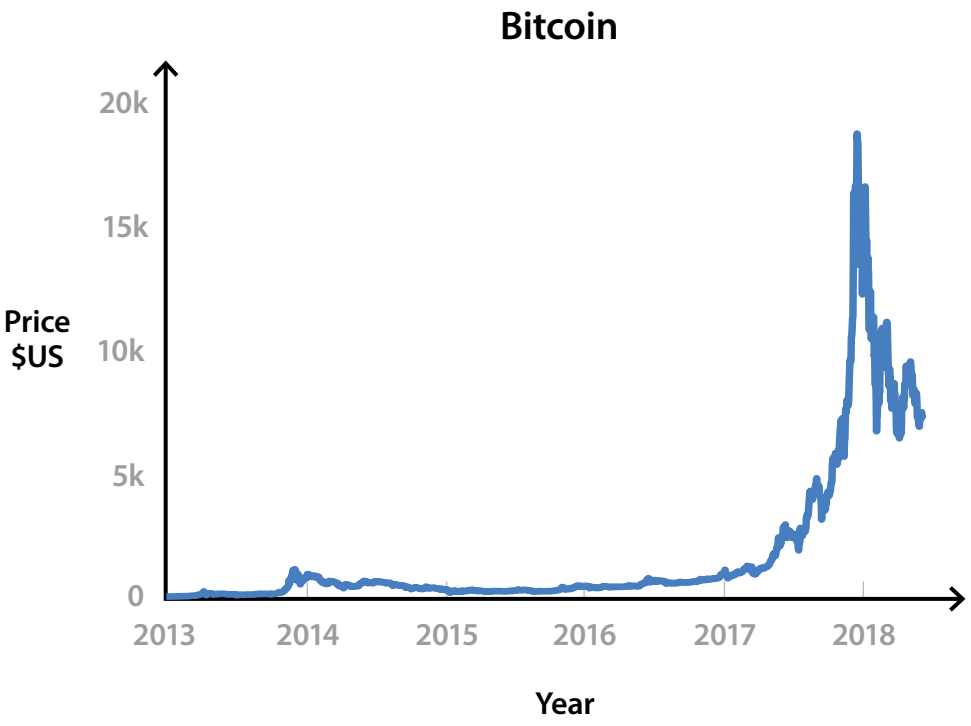
Cryptocurrencies

What are Cryptocurrencies?

Cryptocurrencies are digital tokens. They are a type of digital currency that allows people to make payments directly to each other through an online system. Cryptocurrencies have no legislated or intrinsic value; they are simply worth what people are willing to pay for them in the market. This is in contrast to national currencies, which get part of their value from being legislated as legal tender. There are a number of cryptocurrencies – the most well-known of these is Bitcoin.

Activity in cryptocurrency markets has increased significantly and prices of cryptocurrencies have risen rapidly. The fascination with these currencies appears to have been more speculative (buying cryptocurrencies to make a profit) than related to their use as a new and unique system for making payments. Related to this, there has also been a high degree of volatility in the prices of many cryptocurrencies. For example, the price of bitcoin increased from around US$1 000 at the start of 2017 to around US$20 000 at the end of 2017 before falling to around US$7 000 in early 2018. The extraordinary interest in cryptocurrencies has also seen a growing amount of computing power used to solve the complex codes that many of these systems use to help protect them from being corrupted. Despite the increased level of interest in cryptocurrencies, there is scepticism among most industry experts about whether they would ever replace more traditional payment methods or national currencies.



Source: Coindesk.com

Features of the Bitcoin System

Bitcoin was launched in 2009, a year after a report that described the Bitcoin system was released under the name Satoshi Nakamoto. The system was designed to electronically mimic features of a cash transaction. It was designed to allow peer-to-peer (or person-to-person) transactions, without the need to know or trust the other person in the transaction, and to occur without the need for a central party (such as a bank). Unlike conventional national currencies such as Australian dollars, which get part of their value from being legislated as legal tender (the law says it must be accepted as a payment), Bitcoin and other cryptocurrencies do not have any legislated or intrinsic value. Instead, the value of Bitcoin is determined by what people are willing to pay for it in the market (and, in theory, its value could fall to zero at any time).

One feature of the Bitcoin system is that the supply of bitcoins increases at a pre-determined rate and is capped at around 21 million (with each bitcoin able to be subdivided into 100 million satoshis or 0.00000001 bitcoins). Because of this the supply of bitcoins has been commonly compared to the supply of a scarce commodity, such as gold.

The Bitcoin system allows transactions to occur directly from person to person without requiring a central party (such as a bank) to verify or record the transactions. This is unlike most conventional payment methods, such as electronic bank transfers, which rely on a central party to keep and update records of transactions. For example, commercial banks maintain a record of their customers' account balances, deposits and withdrawals.

Instead, the Bitcoin system uses 'blockchain' technology to record transactions and the ownership of bitcoins. This is essentially technology that connects groups of transactions ('blocks') together over time (in a 'chain'). Each time a transaction occurs, it forms part of a new block that is added to the chain. As a result, the blockchain provides a record (or database) of every bitcoin transaction that has ever occurred, and it is available for anyone to access and update on a public network (this is often referred to as a 'distributed ledger'). The integrity of the Bitcoin system is protected by 'cryptography', which is a method of verifying and securing data using complex mathematical algorithms (or codes). This makes the system very difficult to corrupt.

Bitcoin transactions are verified by other users of the network, and the process of compiling, verifying and confirming transactions is often referred to as 'mining'. In particular, complex codes need to be solved to confirm transactions and make sure the system is not corrupted. The Bitcoin system increases the complexity of these codes as more computing power is used to solve them. A new block of transactions is compiled approximately every ten minutes. 'Miners' want to solve the codes and process transactions because they are rewarded with new bitcoins (currently 12.5 new bitcoins per block).

The increase in competition between miners for new bitcoins has seen large increases in the amount of computing power and electricity required (which is often used for air conditioning to cool computer systems). While it is difficult to calculate with precision, some estimates suggest that the annual energy consumption of the Bitcoin system is similar to that of countries like Greece, Colombia or Switzerland.

How Does a Bitcoin Transaction Work? – An Example

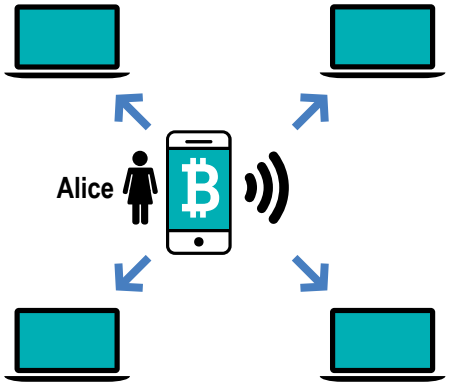
Bitcoin transactions occur through electronic messages that are sent to the entire network with instructions about the transaction. The instructions include information such as the electronic addresses of the parties involved, the quantity of bitcoins to be traded, and a time stamp.

Suppose Alice wants to transfer one bitcoin to Bob. Alice starts the transaction by sending an electronic message with her instructions to the network, where all users can see the message. Alice's transaction is one of a number of transactions that have recently been sent. Since the system is not instantaneous, the transaction sits with a group of other recent transactions waiting to be compiled into a block (which is just a group of the most recent transactions). The information from the block is turned into a cryptographic code and miners compete to solve the code to add the new block of transactions to the blockchain.

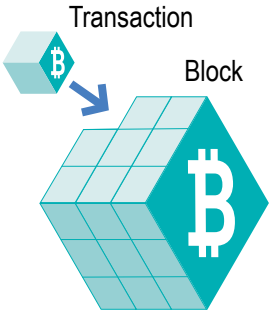
Once a miner successfully solves the code, other users of the network check the solution and reach an agreement that it is valid. The new block of transactions is added to the end of the blockchain, and Alice's transaction is confirmed. (It can take up to 60 minutes, the time taken for six blocks of transactions to be processed, for users to be certain that their transaction has been successful.)

How Does a Bitcoin Transaction Work? – An Example

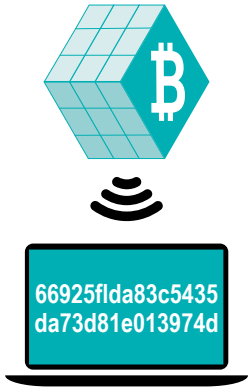
1. Alice sends **instructions** to **transfer** bitcoins to Bob. **Anyone** using the **network** can view the message.



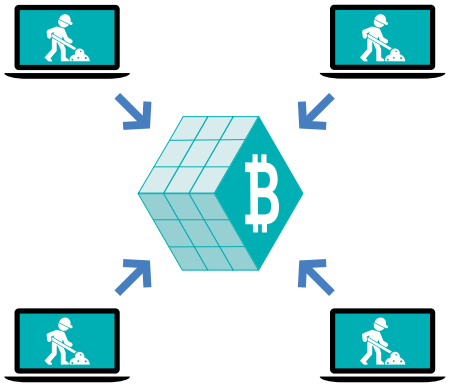
2. **Miners** group the transaction together into a **'block'** with other recently sent transactions.



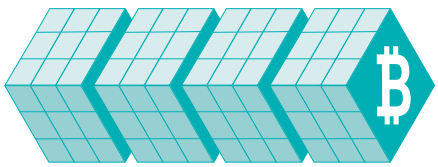
3. Information from the new **block** is transformed into a **cryptographic code**.



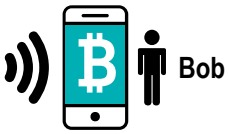
4. Miners compete to find the **code** that will add the new block to the **blockchain**.



5. Once the code is **solved**, the block is added to the **blockchain** and the transaction is **confirmed**.



6. **Bob** receives the **bitcoins**.



Is Bitcoin Money?

A frequently asked question is whether bitcoin (or cryptocurrencies more generally) can be defined as 'money'. The short answer is that bitcoin is not a form of money. To see why, we can compare bitcoin with the key characteristics of money:

- **Means of payment** – can it be used to buy and sell things? Money generally comes in the form of a nation's currency, and is widely accepted as a means of payment. While bitcoin can be used to buy and sell things, it is not widely accepted as a means of payment, and surveys suggest that only a small fraction of bitcoin holders use them regularly for payments. There are also issues around the ability of the Bitcoin system to cope with a large volume of transactions.
- **Store of value** – can its purchasing power (the ability to purchase a similar basket of goods and services) be maintained over time? Large fluctuations in the price of bitcoin reduce its effectiveness as a store of value.
- **Unit of account** – is it a common way of measuring the value of goods and services? In Australia, the prices of goods and services are measured in Australian dollars. While some businesses may accept bitcoin, it is not a primary way used to measure and compare prices.

So, while bitcoin can be used to make payments, currently its use as a means of payment is limited and it does not display the key characteristics of money.

What Are Some of the Public Policy Implications of Cryptocurrencies?

The use of cryptocurrencies more generally presents a number of issues for public policymakers, such as the Reserve Bank. This includes questions like: does the Reserve Bank intend to issue a digital form of the Australian dollar (an eAUD) in the future? The Governor of the Reserve Bank noted in his 2017 speech 'An eAUD?' that there are:

> *'… no immediate plans to issue an electronic form of Australian dollar banknotes, but that the Reserve Bank is continuing to look at the pros and cons.'* [1]

Some of the technology behind cryptocurrencies is likely to have useful applications, but it also raises a number of considerations for public policymakers. Given the anonymity provided by the Bitcoin system, and its worldwide reach, there are questions about how to limit the use of digital currencies for criminal activities. In addition, the current fascination with cryptocurrencies has potentially added to the speculative nature of these markets, and has raised concerns around consumer protection. If cryptocurrencies were to be more widely adopted, it could also present some challenges for the role of the banking sector and raise additional financial stability concerns in a crisis.

Most industry experts and observers are fairly sceptical about whether cryptocurrencies will replace more traditional payment methods or national currencies. In the above-mentioned speech, the Governor of the Reserve Bank also noted the following in regards to cryptocurrencies:

1 Lowe, Philip (2017), 'An eAUD?', Address to the 2017 Australian Payment Summit, 13 December.

'One class of technology that has emerged that can be used for payments is the so-called cryptocurrencies, the most prominent of which is Bitcoin. But in reality these currencies are not being commonly used for everyday payments and, as things currently stand, it is hard to see that changing. The value of bitcoin is very volatile, the number of payments that can currently be handled is very low, there are governance problems, the transaction cost involved in making a payment with bitcoin is very high and the estimates of the electricity used in the process of mining the coins are staggering. When thought of purely as a payment instrument, it seems more likely to be attractive to those who want to make transactions in the black or illegal economy, rather than everyday transactions. So the current fascination with these currencies feels more like a speculative mania than it has to do with their use as an efficient and convenient form of electronic payment.'

The future use of cryptocurrencies will likely depend on how well they can meet the needs of users compared with other electronic payments, such as electronic bank transfers. The extent to which there is take-up of cryptocurrencies more broadly will depend on costs, incentives and convenience for users – for any payment system to succeed it needs to be convenient and accessible for both consumers and businesses.

Disclaimer

This explainer is provided to facilitate the conceptual understanding of cryptocurrencies. It does not constitute advice, or a recommendation, to buy, trade or invest in Bitcoin or any other cryptocurrency. If you decide to trade or use cryptocurrencies you may be taking on risk for which there is no recourse.

For more information about these risks see ASIC's MoneySmart website.