Understanding Cryptocurrency

Crypto currencies have become increasingly popular over the past several years. At the moment, there are more than 6,700 of them being traded, and the number is constantly growing.

With that has come an increase in people wanting to understand more about them, but are sometimes too embarrassed to ask.

To that end, and because I haven't really covered crypto currencies much in my previous blogs (except for the 'Building The New PayPal' article last year), I thought it might be time to put some foundations down and get together a basic introduction covering what crypto currency is and why it's becoming more and more important.

Currency: A Brief History

In the caveman era, people used the barter system, in which goods and services are exchanged among two or more people. For instance, someone might exchange seven apples for seven oranges. The barter system fell out of popular use because it had some glaring flaws:

- People's requirements have to coincide - if you have something to trade, someone else has to want it, and you have to want what the other person is offering.
- There's no common measure of value - you have to decide how many of your items you are willing to trade for other items, and not all items can be divided. For example, you cannot divide a live animal into smaller units (unless you also happen to be a butcher!).
- The goods cannot be transported easily, unlike our modern currency, which fits in a wallet or is stored on a mobile phone.

Once people realised the barter system didn't work very well, currency went through a few iterations:

The first known currency was created by King Alyattes in Lydia, now part of Turkey, in 600BC. The first coin ever minted features a roaring lion. In 110 B.C., an official currency was minted; in A.D. 1250, gold-plated florins were introduced and used across Europe; and from 1600 to 1900, paper currency gained widespread popularity and ended up being used around the world - This is how modern currency as we know it came into existence.

Modern currency includes paper currency, coins, credit cards, and digital wallets, (for example, Apple Pay, Amazon Pay, Paytm, PayPal, and so on). All of it is controlled by banks and governments, meaning that there is a centralised regulatory authority that limits how paper currency and credit cards work.

Traditional Currencies vs. Crypto Currencies

Imagine a scenario in which you want to pay a friend who you have just bought a second hand car from, by sending money online to his or her account. There are several ways in which this could go wrong, including:

- The financial institution could have a technical issue, such as its systems are down or the machines aren't working properly.
- Your or your friend's account could have been hacked—for example, there could be a denial-of-service attack or identity theft.
- The transfer limits for your or your friend's account could have been exceeded.

There is a central point of failure: the bank.

This is why the future of currency could lie with crypto currency…

Now imagine a similar transaction between two people using the bitcoin app. A notification appears asking whether the person is sure he or she is ready to transfer bitcoins. If yes, processing takes place: The system authenticates the user's identity, checks whether the user has the required balance to make that transaction, and so on. After that's done, the payment is transferred and the money lands in the receiver's account. All of this happens in a matter of minutes.

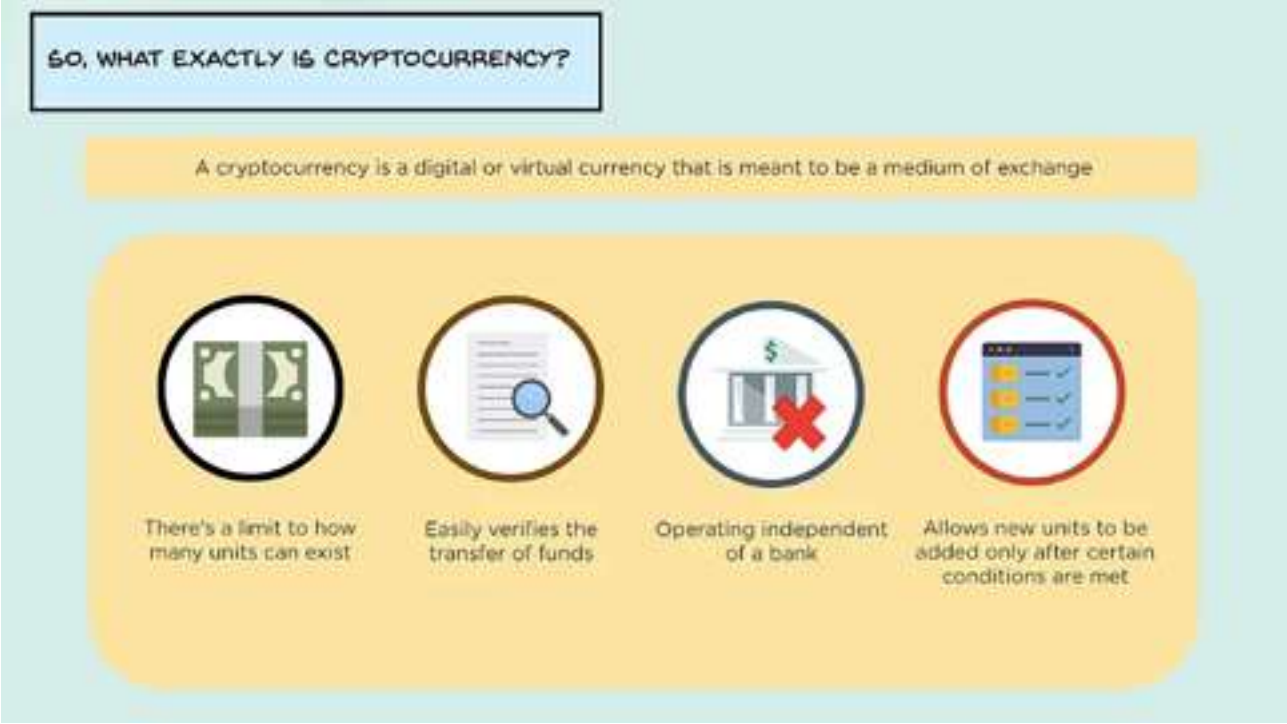
In this way, crypto currency removes all the problems of modern banking: There are no limits to the funds you can transfer, your accounts cannot be hacked, and there is no central point of failure Considering how much growth they're experiencing at the moment, there's a good chance that there are plenty more to come.

What is Crypto Currency?

A crypto currency is a digital or virtual currency that is meant to be a medium of exchange. It is quite similar to real-world currency; except it does not have any physical embodiment, and it uses something called cryptography to work.

Because crypto currencies operate independently and in a decentralised manner, (without a bank or a central authority), new units can be added only after certain conditions are met. For example, with Bitcoin, only after a 'block' has been added to the 'blockchain' will the 'miner' (bear with me) be rewarded with bitcoins; and this is the only way new bitcoins can be generated.

The limit for bitcoins is 21 million; after this, no more bitcoins will be produced.



Benefits of Crypto Currency

With crypto currency, the transaction cost is low to nothing at all - unlike, for example, the fee for transferring money from a digital wallet to a bank account. You can make transactions at any time of the day or night, and there are no limits on purchases and withdrawals.

And anyone is free to use crypto currency, unlike setting up a bank account, which requires documentation and other paperwork.

International crypto currency transactions are faster than wire transfers too. Standard electronic transfers take anything from half a day to a week for the money to be moved from one place to another. With crypto currencies, transactions take only a matter of minutes or even seconds.

What is Cryptography?

Cryptography is a method of using encryption and decryption to secure communication in the presence of third parties with ill intent - that is, third parties who want to steal your data or eavesdrop on your conversation.

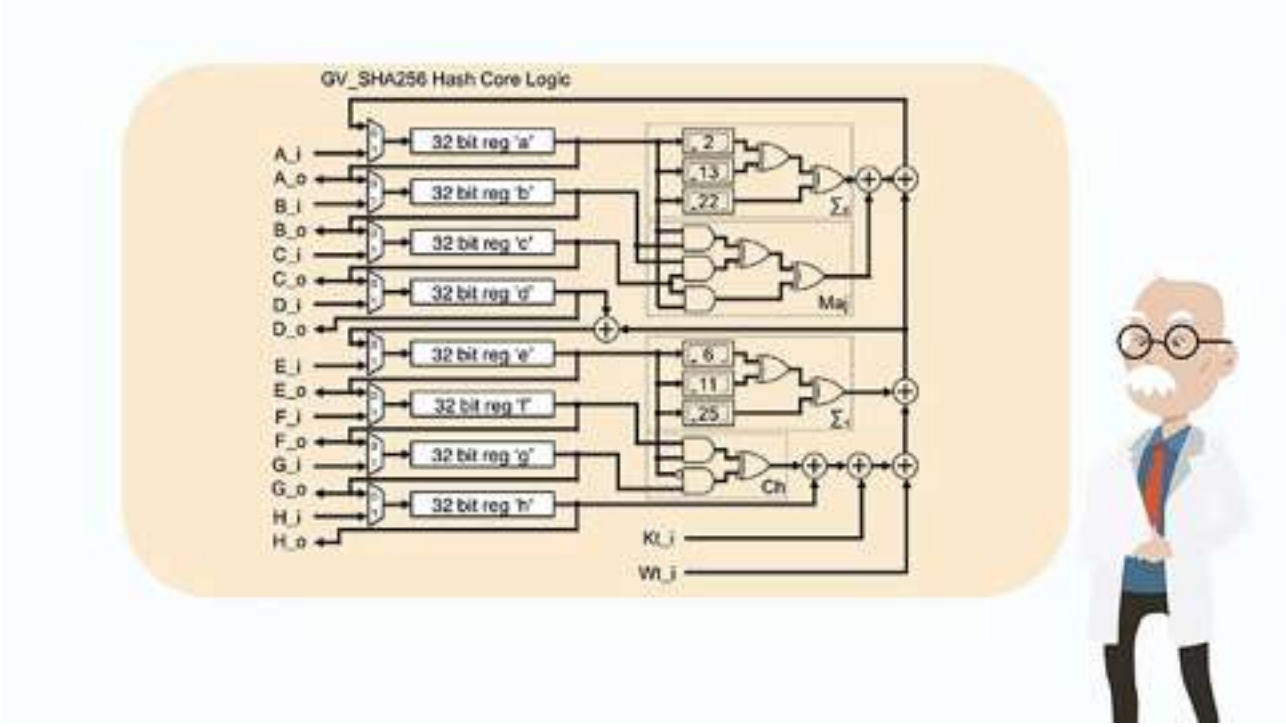
Cryptography uses computational algorithms such as SHA-256, which is the hashing algorithm that Bitcoin uses; a public key, which is like a digital identity of the user shared with everyone; and a private key, which is a digital signature of the user that is kept hidden.

Cryptography in Bitcoin Transactions

In a normal Bitcoin transaction, first, there are the transaction details: who you want to send the bitcoins to, and how many bitcoins you want to send. Then the information is passed through a hashing algorithm.

The output is then passed through a signature algorithm with the user's private key, used to uniquely identify the user. The digitally signed output is then distributed across the network for other users to verify. This is done by using the sender's public key.

The users who check the transaction to see whether it's valid or not are known as miners. (I always keep my promises!) After this is done, the transaction and several others are added to the blockchain, where the details cannot be changed. The SHA-256 algorithm looks something like in the image below.



You can see how complicated it is, meaning it's safe to say that the encryption is very difficult to hack.

The Future of Crypto Currency

The world is clearly divided when it comes to crypto currencies.

On one side are supporters such as Bill Gates, Al Gore and Richard Branson, who say that crypto currencies are better than regular currencies. On the other side are people such as Warren Buffet, Paul Krugman, and Robert Shiller, who are against it.

Krugman and Shiller, who are both Nobel Prize winners in the field of economics, call it a Ponzi scheme and a means for criminal activities.

In the future, there's going to be a conflict between regulation and anonymity. Since several crypto currencies have been linked with terrorist attacks, governments would want to regulate how crypto currencies work. On the other hand, the main emphasis of crypto currencies is to ensure that users remain anonymous.

Futurists believe that by the year 2030, crypto currencies will occupy 25 percent of national currencies, which means a significant chunk of the world would start believing in crypto currency as a mode of transaction.

There is no doubt that it's going to be increasingly accepted by merchants and customers, and it will continue to have a volatile nature in the short to medium term, which means prices will continue to fluctuate, as they have been doing for the past few years.

To Conclude…

It really does need to be taken into account that crypto is a form of currency that has been in existence for only just over 10 years.

It isn't gold and it isn't fiat. This is brand new technology that has already illustrated its ability to fundamentally disrupt the global financial system. But it isn't perfect by any stretch.

Crypto, or digital, or virtual currencies have created a paradigm shift in the way we look at money. The way we look at potentially buying it. The way we look at potentially spending it.

For now I would just say; “be careful buying it”.