Cryptocurrency Questions, part 2

Cryptocurrencies, and the blockchain technology many of behind them, are here to stay. They are incredibly flexible and have many uses. In this FAQ we dig a little deeper …

Frequently Asked Questions part 2 – how do cryptocurrencies work?	
What's the difference between a cryptocurrency and a blockchain?	Blockchain is a technology and cryptocurrency is an early application of it. Blockchain is a powerful type of database to manage any chain of transactions. Each use is different and many businesses have sprung up to make use of the technology. Up until 2018, they are mostly financial services fintech businesses. Note that some cryptocurrencies do not use blockchain and some blockchain applications are not currencies.
What is forking?	One way to create a new currency is to copy an old one. This can happen when two sets of users disagree about a change of rules so one group takes a copy of the blockchain of transactions and creates a similar currency with a new name. They fork in different directions and trade in parallel. This is called a hard fork - Bitcoin did this several times in 2017 and the new currencies proved controversial as they fought for legitimacy and market share. A soft fork is when a number of blocks are bypassed, maybe due to a bug or a hack, and the currency continues from there.
Can cryptocurrencies be changed?	As they are made of software, it is possible for the developers to change the features of a blockchain or a cryptocurrency. Currently, major changes are agreed by consensus between the developers, miners and key users. But there is nothing to prevent changes being made without consensus, so they can be controversial, as with forking.
It is said that cryptocurrencies are transparent, anonymous, public and private. But which?	That's the magic of crypto. All of them! The transactions and balances are in the public domain but the usernames are encoded. Hence the ledger is transparent to maintain confidence but the user identities are anonymous to maintain privacy. The blockchain data structure holds a sequence of transactions, for instance who paid how much currency to whom and what the new balances are. When combined with cryptography, it holds the data securely and when decentralised it can eliminate the involvement of intermediaries, such as banks.
Can a blockchain replace an 'end to end business process' in a secure way without the need for a central owner?	No - a blockchain is only a sequential list of transactions; most of the end to end business process is managed off-chain. Bitcoin, for example, has numerous business processes and protocols to make it work and the blockchain is just the published transaction list at the end of the process.
What are 'ICOs'?	These are the launch of new currencies – *Initial Coin Offerings* to fund new tech projects and for investors to buy in to. They are a way of the developers recouping their costs (or cashing out) and a

	way of investors joining a tradeable market. These new currencies could appreciate and become the digital currencies of the future, or they might disappear as quickly as they were created.
How could I buy into a Cryptocurrency?	You can purchase the currency from a Crypto Exchange. There are dozens, each offering a different selection of currencies and each with a different track record of service and security. Many of the currencies can only be bought with Bitcoin or Ethereum so you would need to buy Bitcoin first and then exchange it. Alternatively, you could use a Forex spread betting platform which means you invest in the value of the currency rather than owning it personally, but the risks/costs may be higher. There are pros and cons of each. This is not investment advice!
Are Cryptocurrencies safe?	Not fully. The technology is very new and some of the fundamental issues are still being resolved. Although cryptography is a robust science, there are bugs in some of the currencies, exchanges and wallets, hacking is rife and users are still learning their way around the system. Governments are now getting involved and starting to regulate cryptocurrencies in many countries. This will legitimise them but also place additional rules on them. This is a necessary pre-cursor to widespread adoption and will tame the wild-west nature of the market.
Can a Blockchain be hacked?	In terms of the security, the blockchain cryptography has never been successfully hacked. As a digital currency, a design feature had to be that a Bitcoin is impossible to copy/paste/duplicate, so every Bitcoin wallet balance maintains its integrity. The main blockchain was designed to be so secure that it is vanishingly unlikely that any private key/public key combination can be guessed in the next million years. As far as we know this has been entirely successful. The main technical risks are therefore bugs (eg. one incident in 2010 due to an overflow bug, but the transaction was successfully bypassed by the miners via a 'soft fork') or a mining group taking over the network by buying over 51% of the computing power, but that would be incredibly expensive and the value of every Bitcoin would plummet so it would be counter-productive.
Can a user be hacked?	Yes. Users must keep safe their own private keys (think of a random 34-character password) in a pair with their public wallet number (think of a bank account number). Anyone can send coins to a wallet but only the private key holder can send funds from a wallet. Unfortunately, users can lose the keys or have them discovered by hackers. A lost private or public key means lost access to the funds – this has happened a lot but only affects individual users. When Exchanges are hacked, the hackers get access to a large number of private/public keys, enabling them to perform unauthorised transfers – this happens fairly regularly and is high profile due to the total amounts involved. It gives rise to an interesting philosophical/ethical dilemma. If they spot it quickly, the

	miners (if they act together) could refuse to process any transactions on the hacker's wallet. But that goes entirely against the decentralised anonymous design of Bitcoin and would make them the 'central authority' that they have sworn to dispense with.
Why do the price graphs look so dramatic?	Because the price rises and falls have been so dramatic. The older Cryptocurrencies have up to 9 years of trading history so you can view their ups and downs. However, these graphs are easy to mis-interpret – if a currency has been trading for a long time, any recent peak will look highly exaggerated against the right-hand margin. To get a more accurate visual comparison, set each price graph to the last 12 months so they can be seen on the same scale.
If it rises, what price will Bitcoin top out at?	There is no telling; it all depends on demand. Some people are forecasting $100k, others $1m or even more.
If it falls, what price will Bitcoin bottom out at?	There is no telling; it all depends on confidence. Some people are forecasting $10k, others $1k or even less.
So, is cryptocurrency in a bubble or not?	There is no consensus. Some people point to obvious comparisons with previous investment bubbles and predict a full-blown crash in 2018. Others say the valuations are justified as cryptocurrencies will come to dominate financial services in the future. Both views may yet be right!
How does it compare to the dot com industry in the year 2000?	In terms of the market narrative, there are many similarities. Dot coms promised to revolutionise industry. Thousands of businesses started up with little more than a glossy brochure and huge optimism. eCommerce share prices rocketed in 18 months but the eCommerce industry took 18 years to develop the business models and cash flows to justify them. Hence there was a severe crash in between. In the crypto world in 2017, all we know is that the exponential spike was higher and quicker than in 2000. We don't know if it will continue, level out or crash, or whether the ultimate market cap of the currencies will be higher or lower than now.
What is a market cap and how is it valued?	The market capitalisation is simply how much a Cryptocurrency is worth in total – the price per coin multiplied by the number of coins in circulation. There is no consensus on how to assess a future market cap (unlike a share price which is based on future earnings, dividends and growth). Optimists say that the market cap can be equated with the total of transactions, making comparisons with a company's turnover. Pessimists say that there is no intrinsic value, so it could be zero.
Will the newer cryptocurrencies increase in value as much as Bitcoin has?	It is a possibility that a small number will see massive growth but Bitcoin's market lead is so strong it continues to tower over all of the others. Ultimately the most popular are likely to be the ones with the best utility. The pace of innovation will remain high for some

	time, both in terms of technical architecture and business model. You ain't seen nothing yet.
If I buy a coin, how would I keep it safe?	Most Exchanges allow you to hold your coins in your account, but this is normally only recommended for small holdings as some have been hacked in the past. Moving the coins to an electronic wallet on your PC or phone is an alternative, but this also has risks due to loss or data corruption. You could also print the records out on paper, but don't lose the paper!
If I make a mistake in a crypto transaction, can my bank reverse it?	No. Transactions are irreversible once they are added to the blockchain. That is part of the security of the system; no bank owns it or runs it, so cannot change it.
If I make a profit, do I pay tax?	That depends. If you buy currency as an asset (on an Exchange) you are probably liable for tax. If you trade it as a spread bet (banned in the USA) then probably not, but each country's regulations are different.
Does the mafia really own Cryptocurrency?	The mafia own a chunk of every currency, so no surprise there. Maybe they even own Cryptokitties. The anonymity of cryptocurrencies is particularly appealing so criminals are buying and selling with renewed confidence. The cryptocurrencies will become mainstream over time, so Regulators are starting to crank up the pressure on money laundering.
What the hell are Cryptokitties?	Cryptokitties is an online game released in 2017. It's a great example of blockchain technology that isn't a currency. Users breed animated kittens. The blockchain technology works in a similar way to DNA, allowing users to breed pairs of kittens to achieve the traits they want. Kittens can then be bought and sold for Ethereum currency. The game came to prominence 6 weeks after its release when a Cryptokitty was sold for 247 Ethereum, worth well over $100k.

James Crawford, Touchpoint Change Consulting.
January 2018.
james.crawford@touchpointchange.co.uk Tel. 0777 55 90192.