Bitcoin – A Primer

by Sava Mihic, Quant Analyst

Bitcoin has recently captured popular attention by exceeding the US$10,000 per coin mental barrier. Discussion has been extremely polarised, with some claiming it is the biggest bubble since the Tulip while others claim we are seeing the start of a new paradigm.

This article will discuss what it is, some perspectives, and what the future may look like.

What is Bitcoin?

Bitcoin is the first of a new breed of digital tokens labelled "cryptocurrencies" (or simply "cryptos"). The core idea is that it has a public record of all transactions, called a "blockchain". New transactions are recorded by adding transaction record blocks to the existing chain, with specific rules around who can add blocks, how new blocks are recognised, the types of blocks and the rate at which they are *meant*[1] to be added.

Bitcoin follows a "proof-of-work" requirement in order to add a block to the blockchain. This means that the right to record the next block is attained by doing work – also known as "mining". The work required, in the case of Bitcoin, is testing a large number of random numbers until you happen upon one that produces a specific outcome. By making the numbers random, the playing field is levelled, with anybody able to jump in and mine. The more miners there are testing random numbers, and the more computing power they use, the faster somebody finds the correct random number. Miners that control more computing power are more likely to be the first to find the solution, with their rate of success being proportional to their share of computing power. Making mining simple means it isn't dominated by any one party, preventing a malicious party from consistently adding fraudulent transaction blocks.

Once a new block is mined, the miner will broadcast it to the network. The network will confirm that the random number the miner chose does indeed generate the required outcome, and will append it to all the other blocks in the Bitcoin blockchain. One Bitcoin block is meant to be added every 10 minutes – the idea being that prescribing 10 minute intervals makes it less likely for two miners to independently find and broadcast competing solutions to the network at the same time. If mining activity increases and blocks start to be added faster, the difficulty of mining will increase in order to keep the rate at one block per 10 minutes.[2] Conversely, the difficulty will decrease if there is less mining. Each block can at present accommodate around 2,000 transactions.

Of course, people need to be incentivised to do the work required to record transactions, so Bitcoin has an incentive system to encourage mining. There are two parts to the incentive system, and both go to the miner that solves the block first:

1. The first part is the block reward. Currently set at 12.5 Bitcoin and halving every four years, it will increase Bitcoin supply up to a maximum of 21 million Bitcoin and will therefore end in 2140 if all goes to plan. This amount isn't paid by anybody in particular, but rather is inflationary. Essentially, it is partially funded by everybody that owns Bitcoin.
2. The second part is the transaction fee, which is a variable amount and depends on how much Bitcoin users are willing to pay in order to have their transaction included in the next block. Users bid a transaction fee, and miners then decide which transactions to include in the block they are mining. As Bitcoin has risen in popularity, transaction fees have moved from being around 0.1 Bitcoin to 2 Bitcoin per block, with this cost borne by the parties initiating transactions.

Chart 1 on the following page shows the price of Bitcoin on a log scale, and puts into perspective just how extreme the initial boom in 2013 was. While it got a lot of attention then, it didn't get the same level of attention as the latest boom, primarily because the total value of all outstanding Bitcoin peaked at US$10 billion at the time, whereas we are now looking at US$250 billion. See our commentary in *The Journal* on the 13th of January 2014 for further thoughts at the time.[3]

A lot has changed since the early days of Bitcoin. Nobody thought Bitcoin prices would reach the stratosphere when it first started, and there were so few miners at the time that mining could be done by a home PC. Today, mining has become so intense that it requires specially designed hardware, huge amounts of electricity and heavy cooling. Bitcoin has been able to rise through a combination of

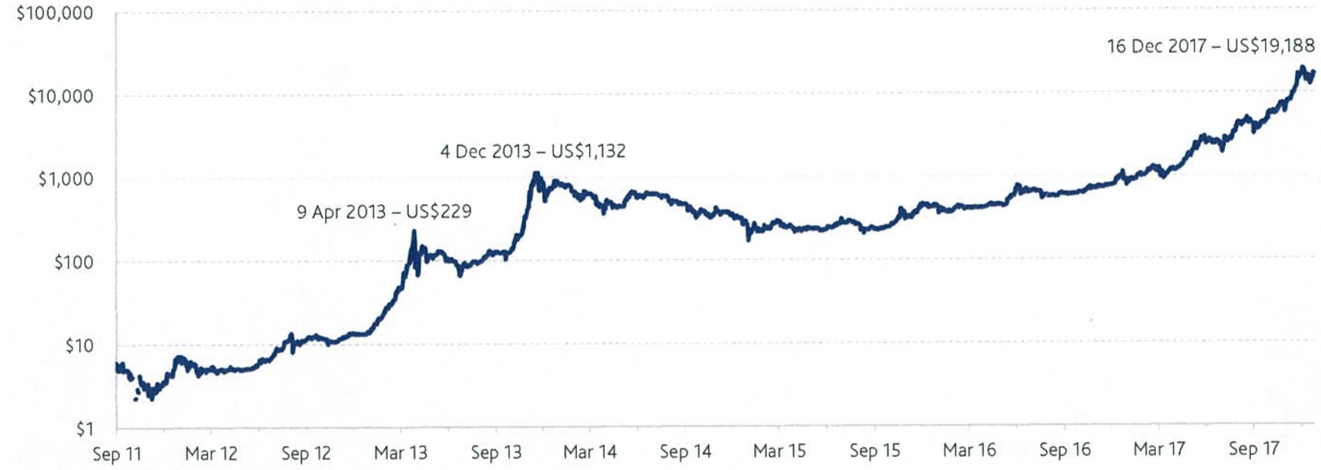
[1] Bitcoin blocks require testing random numbers to process, so a block can take more or less than the 10 minute target depending on miner luck. That is why processing time is *meant* to be 10 minutes, rather than *is* 10 minutes.

[2] Difficulty is increased by requiring more random numbers to be tested by miners before a solution can be found.

[3] https://www.platinum.com.au/Insights-Tools/The-Journal/The-Fantastic-Rise-of-Bitcoin

Chart 1 – Bitcoin Price History

BitStamp (USD) – Closing Price – Daily (Log Scale)



Source: https://bitcoincharts.com

fulfilment of needs, strong promotion, and a healthy dose of speculative exuberance. Some of these are discussed in the following sections. The price of US$15,000, which is current at the time of writing, will be used in numbers quoted below.

Bitcoin as a Medium of Exchange?

One of the early hopes was the idea that Bitcoin could be used as a cheap means of transaction that circumvents the banking system. As things stand today, however, this is not a realistic proposition unless some significant changes are made to the Bitcoin protocol. The reason is that transaction costs on the Bitcoin network are simply too high – today the block reward, i.e. the socialised cost of a transaction, is about US$100 at the 2,000 transactions per block rate (see Chart 2). Additionally, the specific transaction cost borne by the transacting parties is about US$15. Add to this the fact that each block takes 10 minutes to process,[4] and you will be waiting quite a while to confirm your $25 coffee order. The Bitcoin blockchain simply cannot be used to process small transactions as it is currently configured.

Bitcoin as a Store of Value?

With the reality that it cannot be used as a medium of exchange recognised, the narrative has shifted to Bitcoin being a store of value, with gold being used as an analogue. Proponents argue that the limited total supply of Bitcoin creates scarcity value, and that the mining of Bitcoin, similar to the mining of gold, takes work. In the case of gold, the price is often underpinned to some extent by the cost of mining it, and mining costs generally increase over time as the geology becomes more difficult. In contrast, no such analogue can be drawn in Bitcoin, because the difficulty of mining is proportional to the amount of processing power being expended. High Bitcoin prices incentivise more processing power and therefore higher costs, but the reverse is also true, which implies that there is little pricing support when Bitcoin prices fall.

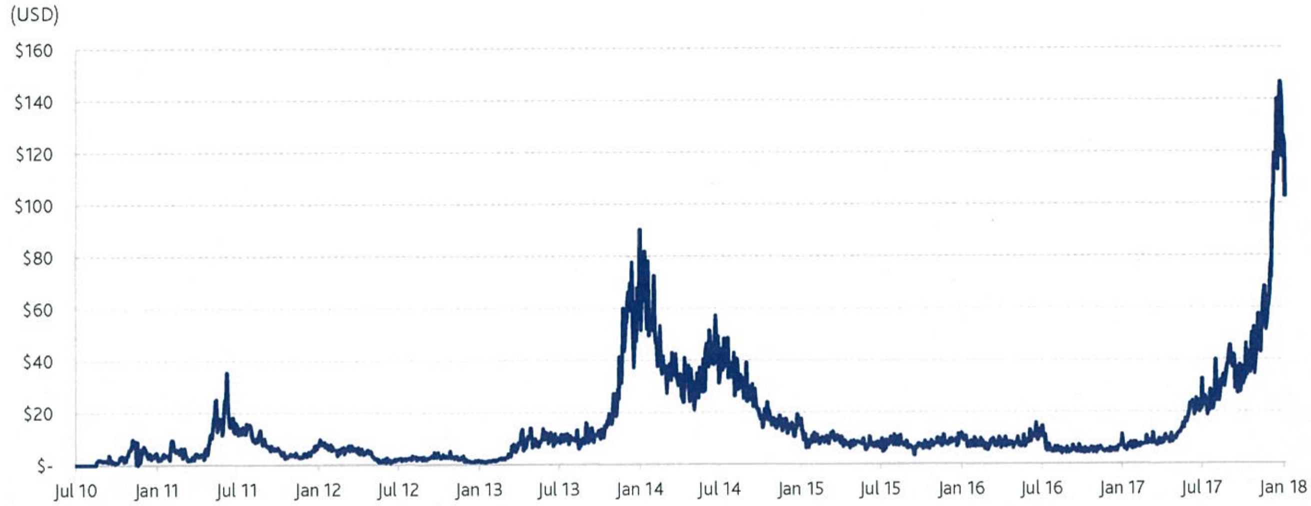
ICOs and "Forks"

But what about scarcity value? While Bitcoin supply is limited (unless the code is changed), there has been an enormous proliferation of copycats[5] – the count of recognised cryptocurrencies stands at 1324 as of today. Coinschedule.com indicates that in 2016 a total of US$96 million was raised in 46 "Initial Coin Offerings" (ICOs), and in 2017 the number has jumped to 235 ICOs, raising a total of US$3.7 billion – a 39 fold increase in money raised.

[4] There is a backlog, which varies in size, but currently has over 100,000 unconfirmed transactions, which would take over 8 hours to process assuming no further transactions are recorded. Even with no backlog, one would generally require several blocks to be added after the block processing one's transaction, to ensure that the transaction is embedded in the blockchain.

[5] An example of a copycat is Ether, which is similar to Bitcoin, but has the added use of being able to pay for "smart contracts" on the Ethereum network, which are payment contracts that are executed automatically. For example, a smart contract may have an address, and when something is paid into that address, it may be split among two different addresses automatically in a certain share, like a royalty. The Ethereum network can also be used to issue ICOs. Another example is Ripple, which, instead of using proof of work like Bitcoin and Ether, relies on consensus among trusted parties to approve transactions, thereby removing the costs of proof of work, but also to some extent the decentralisation. If Ripple, which has some institutional backing, were to advance from concept to a fully functioning network, it may represent an efficient payment system. Among the many less popular tokens is UET, the "Useless Ethereum Token". The "ICO disclosure" of UET, "the world's first 100% honest Ethereum ICO", says that it has "no value, no security and no product. Just me, spending your money."

Chart 2 – Cost per Transaction



Source: https://blockchain.info

In an ICO, the promoter profits by selling tokens to the public. Generally the promoter will start by publishing a "whitepaper" to explain the token and getting backing from a few high net worth investors that are willing to fund the advertising of the token. Then the promoter will selectively groom some initial investors, for example, by setting up a Slack channel in which he chats with them directly, convincing this group that they are "in the know". This "special" group will take a pre-ICO placement of tokens to distribute ownership and some will then proceed to spread the word on the ICO and how great it is. Finally, after a strong burst of advertising, and once interest is judged to be at peak, the promoter will issue as many tokens as there is demand for while cashing out, usually significantly.

The other angle is "forking", which involves creating a new cryptocurrency and issuing the tokens to the owners of an existing cryptocurrency. Fork promoters tend to be involved in cryptocurrency mining and/or the running of cryptocurrency exchanges. They bet that the more widely distributed a token is the more valuable it is likely to be. So, instead of staging an ICO, which is likely to attract only a limited number of investors, they freely give the new tokens to everyone who is listed as an owner of Bitcoin (or some other well-known token) at a certain point in time, hoping to profit by being the trading hub where their token is traded, earning transaction fees. There have been two significant forks using the Bitcoin blockchain – Bitcoin Cash and Bitcoin Gold. While the names may give the impression that these tokens are somehow the offshoots of Bitcoin, in reality they are not – these are entirely unrelated cryptocurrencies created by those seeking to take advantage of Bitcoin's popularity and wide ownership base.

Some argue that these ICOs and forks will fade over time, and that people will refocus on Bitcoin, thereby retaining its scarcity value. For now, the proliferation is massive.

Black Market Demand

One of the initial use cases of Bitcoin was black market activity, because Bitcoin addresses[6] have no identifying information, allowing criminals to stay anonymous. While there is no doubt that underground activity remains a significant part of the actual transactions using Bitcoin, which is considered the currency of the dark web, it is probably not playing as large a part in Bitcoin's recent run as it may have done previously.

The Miners

Around 300,000 Bitcoin transact each day using the blockchain, representing US$3.5 billion at the moment. Of that, miners are earning around 2,200 Bitcoin per day, for revenues of about US$33 million per day or US$12 billion per year. There are estimates that mining electricity costs are around 16% of mining revenues today, with total power consumption up 25% in December alone and approaching one-seventh of Australia's national energy consumption.[7] Currently miners are very profitable, but in the past they have suffered large losses when the price fell, as they were unable to recoup the significant capital outlay for the custom mining chips they operate. The chips used for mining are called ASICs (application-specific integrated circuits), and they have no use

[6] Bitcoin addresses are digital keys that represent the location at which Bitcoin are held by an individual, similar to a bank account number, and are usually in the format of a string of random letters and numbers.

[7] https://powercompare.co.uk/Bitcoin/ has great data.

outside of mining Bitcoin, resulting in Bitcoin miners being unable to sell them during the last crash. The most popular Bitcoin mining ASICs, Antminers, are developed by the biggest Chinese crypto mining company, a privately held firm called Bitmain.

The Exchanges

A cryptocurrency exchange is an entity through which a customer can exchange Dollars for Bitcoin or another cryptocurrency, or exchange one cryptocurrency for another.[8] This is how most Bitcoin are bought. When a customer buys Bitcoin on an exchange, it does not go to their private wallet immediately; rather, it is held in custody by the exchange, where the customer can sell it. Moving Bitcoin between an exchange and one's private wallet, in either direction, will incur the blockchain fee. This means that customers holding Bitcoin in a private wallet run the risk of not being able to return their Bitcoin to the exchange in a timely manner if they wish to sell it, as there tends to be a large backlog to process transactions through the blockchain during times of heavy trading. Regulation on Bitcoin exchanges is currently minimal – the market has grown too fast for legislation to catch up.[9]

Impressively, the exchanges bear no mining costs but are, in aggregate, trading around US$10 billion[10] in Bitcoin per day, more than double the daily transaction volume on the blockchain itself. Taking a 1% clip (0.5% on each side) of that US$10 billion means that the Bitcoin exchanges are pulling in US$100 million per day at the current pace – annualising fees of US$36.5 billion,[11] with relatively low overheads. If one adds the exchange trading of other cryptocurrencies to the mix, total annualised fees exceed US$60 billion. To put this in perspective against conventional exchanges, Intercontinental Exchange, a group that operates the New York Stock Exchange among other regulated exchanges and clearing houses and has a market capitalisation of US$46 billion, is expected to produce revenue of US$4.6 billion in 2017.

If you ever wondered who funded all of the Bitcoin and cryptocurrency ads that you saw, now you know – the crypto exchanges are the true winners in the Bitcoin phenomenon, bearing none of the risk and earning outsize profits. It is somewhat ironic that these exchanges, which have none of the proof of work or decentralisation features that give Bitcoin its appeal, actually transact twice as much Bitcoin as the blockchain!

Bitcoin as Gambling Arbitrage

So how did the exchanges get so big? Part of the answer is gambling arbitrage. In Japan and South Korea gambling is heavily regulated. Japan has no casinos and pachinko parlours, the traditional gambling outlets, have been curtailed by regulation over time. The extreme volatility that has occurred in Bitcoin, coupled with its unregulated nature and high turnover, makes it an ideal avenue for gambling. A large Japanese cryptocurrency exchange plays the sound of pachinko machines as the prices of cryptocurrencies move up and down, as well as when trades are done, triggering all the necessary endorphins.

Bitcoin as a Tool to Circumvent Capital Controls

China has strict capital controls. It also dominates the crypto mining industry, having the largest share of mining as well as of the market for designing custom mining chips. The initial driver of the recent boom in Bitcoin occurred in China – Bitcoin, with its anonymity, allowed some capital to circumvent the traditional currency controls and flee the country. Seeing this, the Chinese government banned ICOs from being sold to Chinese nationals and shut down domestic crypto exchanges by preventing the exchange of Renminbi for cryptocurrencies.[12] Volumes observably related to China are now a tiny fraction of what they used to be.

Bitcoin and Decentralisation

Another of the initial hopes for Bitcoin was its potential to be a decentralised system, with a frequent argument being that it can disintermediate transactions by removing the need for "trusted" centralised institutions such as banks. To date, Bitcoin has not realised this decentralisation, and is becoming more rather than less centralised. For example, a small group of programmers, known as Bitcoin Core, still write the software that the network runs. Bitcoin mining, which was supposed to be democratised by the brute force "proof-of-work" that anybody can do, is instead being dominated by a few Chinese mining pools as institutionalised ASIC-based mining makes individual PC-based mining unprofitable. Mining ASIC design itself is also dominated by Chinese mining pool operator Bitmain, and Bitcoin trading is dominated by cryptocurrency exchanges, which are centralised institutions. Even Bitcoin ownership is highly

[8] The main exchange for Australians is BTC Markets. There one can purchase Bitcoin using Australian Dollars. If one then wants to buy one of the more exotic cryptocurrencies, one could convert their Bitcoin to Ether and send the Ether to an offshore exchange that offers trading in other cryptocurrencies. Using Ether to fund the alternate exchange account is sensible as the transaction cost is lower and transaction confirmation is faster.

[9] The government of South Korea has indicated concern around unsophisticated investors being too involved in cryptocurrency trading and is therefore considering regulating their exchanges. China has banned the exchange of Renminbi for cryptocurrency on exchanges.

[10] https://coinmarketcap.com/ has aggregation data regarding trading on all of the popular crypto exchanges.

[11] This annualises current turnover with the current elevated Bitcoin price. If the price falls, their annual take would fall proportionally.

[12] Not all regulation has been negative – Japan has taken the most positive stance, approving Bitcoin as a means of payment.

centralised, with 1500 addresses (of a 28 million total) owning 38% of all Bitcoin. The number of parties that must be trusted therefore makes the argument that Bitcoin can be used for "trustless" disintermediation difficult.

Bitcoin as a Ponzi Scheme

Some argue that the structure of Bitcoin is an exact replica of a Ponzi Scheme. Nobody can see Bitcoin or make anything out of it and there is no utility value to holding Bitcoin (unlike, say, gold, which is used to make jewellery and has some limited industrial uses). Bitcoin generates no income, and an owner of Bitcoin can only make money by selling the Bitcoin at a higher price to another investor. Bitcoin buyers are attracted by the very high appreciation apparently on offer, and the continuation of the scheme is dependent upon current holders[13] continuing to hold! Encouraging holding, there are some barriers to moving Bitcoin held off an exchange onto an exchange, such as slow transaction time and high transaction costs, making selling more difficult. To cap things off, the whole process is facilitated by the exchanges, which act as the cashed-up manager of the scheme, pumping out unregulated advertising promoting the wonderful returns on offer.

The Future of Bitcoin

The future of Bitcoin is unclear, but it is unlikely to become a medium of exchange in its current form, and further regulation is likely on the horizon. Whether that regulation removes demand for some of the uses of Bitcoin, and whether it stifles unregulated advertising, is yet to be seen, and its ultimate future will depend on that.

Telling also is the fact that long discussions among enthusiasts on the future uses of Bitcoin have given way to hopes and dreams around how soon one can become rich – one is told to resist the "fud" (fear, uncertainty, doubt), be one with the "fomo" (fear of missing out) and just "hodl" (hold). Amongst many buyers understanding of how Bitcoin works and whether it can be used for anything is minimal. People questioning the long-term value of Bitcoin are promptly banned from online crypto forums, although predictions around short-term declines are allowed. With Bitcoin having made the front cover of Barron's, there is no doubt that things are very frothy today, and while the madness of crowds has taught us that bubbles can persist for some time, ultimately, like every euphoria before it, Bitcoin will come crashing down.

[13] Or, as they like to refer to themselves, "HODLers" – a famous misspelling of "hold" by a drunk Bitcoin user trying to calm people down during a crash.