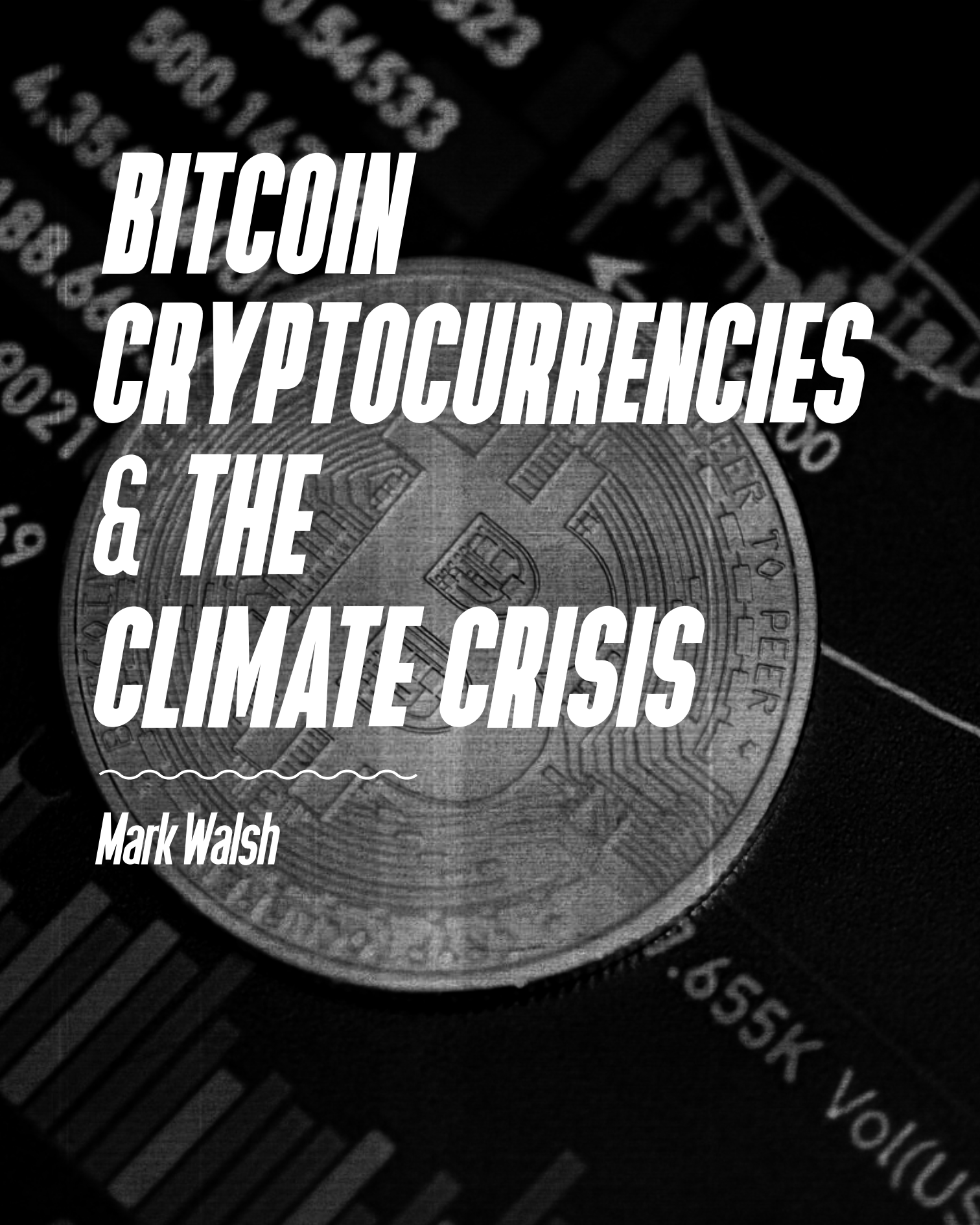

BITCOIN CRYPTOCURRENCIES & THE CLIMATE CRISIS

Mark Walsh

Bitcoin, Cryptocurrencies and the Climate Crisis

Mark Walsh

Today, almost all of the world's money is digital: data on a hard drive, numbers on a screen. Increasingly, electronic forms of payment have replaced paper ones, something which the recent pandemic has further accelerated. Indeed by 2023, Sweden aims to be the first completely cashless society.[1] Thus, when we speak of digital currencies, it is important to be precise. Over the last two decades, as all our conventional notions of money and banking were migrating to the electronic domain, we have seen the rise of certain 'alternative forms of currency'. These are variously called digital currencies or cryptographic (crypto) currencies, and unlike our traditional notions of money these have only ever had an online existence. The earliest and most well known of these is Bitcoin, although there are now thousands of such entities with new ones arising every day. They have names like LiteCoin, NameCoin, PeerCoin and Ethereum.

Cryptocurrencies are, in a sense, internet currencies, emerging in an internet subculture suspicious of governments and financial institutions. They take the form, roughly, of data on a computer network, and can be exchanged online, according to certain protocols, between willing participants who regard them as having value. Intrinsically, they are completely worthless and obtain value only as far as people see them as valuable. In a sense, that is true of all currencies. However, a defining feature of a cryptocurrency is that, unlike a conventional currency such as the US dollar or the Euro, it is designed to be independent of any state, central bank, or financial authority. Indeed, it is designed to be independent of any sort of central authority (something which is not quite true as we will see), a so-called 'decentralised currency'. This, claim proponents (who include some on the left), puts cryptocurrencies and their underlying technology in a position to revolutionise monetary transactions and indeed capitalism itself.

For most people, though no doubt they are aware of the existence of such entities, digital currencies are the stuff of mystery. This is hardly surprising. The financial sphere is already filled with technical, often deliberately obscure language; mass ignorance about the inner workings of financial markets suits those raking in the cash. When one adds to this a virtual currency, replete with notions from mathematics and computer science (in particular cryptography—the mathematics of codes and secrecy), it is hardly surprising that most people have neither the time nor the stamina, nor even the confidence to explore further. Indeed, it seems likely that many, if not most, of those persuaded to invest their savings in the cryptocurrency market have no real idea of what it is they are gambling on (although this is probably true for investors in all sorts of commodities).

With all of this in mind, the primary purpose of this article is to provide a reasonable description of what a cryptocurrency is and how they operate. This will necessarily be done in a somewhat idealised sense, restricted to the best-known cryptocurrency, Bitcoin, although all the salient ideas apply more generally. A secondary purpose will then be to discuss some of the implications of this supposedly revolutionary technology, in particular its effects on our environment.

What is Bitcoin?

In October 2008, a person or persons under the pseudonym of Satoshi Nakamoto published a paper to a cryptography mailing list entitled 'Bitcoin: A Peer-to-Peer Electronic Cash system'.[2] The paper, subsequently referred to as the 'Bitcoin White Paper', defined what a bitcoin was and laid out a protocol for

financial transactions involving this newly conceived form of virtual currency. The following January, Bitcoin was launched with a starting 'block' of 50 bitcoins, the first decentralised digital currency. To get an idea of what any of this means, and to understand the problem solved in the white paper, it is worth starting with a very simple example which we will then generalise to something which is akin to Bitcoin itself. It should be stated that the example below, and much of the explanation that follows, draws heavily from a fascinating video available on the mathematics YouTube channel *3Blue1Brown*.[3]

Imagine you are part of a small group of friends who meet regularly on a social basis, say a book club, and in the process buy each other food, drink and other items. Rather than exchanging cash every time, the group decides to record all transactions in a club ledger, the idea being to settle up once every couple of months, say. A typical ledger extract might look like: 'Karl pays Rosa 25 Euro, James pays Fred 16 Euro, etc' When time comes to settle up, the process simply involves each member working out whether they have given or taken more from the entire group and redressing the balance from the common pot. This is far simpler than a complicated criss-crossing of cash transactions between pairs of group members.

This all sounds straightforward enough, and with a small group of trusted friends dealing with relatively modest amounts, is not likely to run into any serious difficulty. Of course, this is just a warm-up example. So, let's consider now expanding to allow for an arbitrarily larger group, one containing many mutual strangers, spread across many nations, and where matters of trust become much more pressingThere are many potential problems but let's just focus on three.

> **Problem One:** How does one prevent a group member from running up a massive debt, unpayable when time comes to tally up?
>
> **Problem Two:** How does one verify that a transaction written in the ledger is legitimate? What is to stop James claiming, illegitimately, that Fred owes him fifty euro?
>
> **Problem Three:** Expanding on Problem Two, who 'hosts' the ledger? Do we trust one group member or some outside source to maintain the record of transactions accurately? And how do we prevent the record from being 'hacked' in some way?

The first problem is not difficult to solve. One solution is to simply begin by insisting that all group members pay into the common pot a certain starting amount. The idea is to put an upper bound on each group member's spending. This would be written in the ledger at the beginning, with each person paying into the group; for example: 'Karl pays in 1000 euro'. Thus, Karl is not permitted to make a transaction leading him to owe more than 1000 euro to the common pot. Perhaps he buys a bicycle from Emilia for 600 euro and a couch from Claire for 400 euro, leading to the lines 'Karl pays Emilia 600' and 'Karl pays Claire 400' being added in the ledger. Any further payment from Karl (without any compensatory transaction in the opposite direction) would be deemed illegitimate.

Notice now that, provided this upper bound rule is satisfied (and ignoring the other problems we have mentioned), ledger transactions can proceed without any need to settle up. In this sense, the ledger itself becomes its own currency! Of course, the original act of contributing euros to the pot provides a link from this ledger currency back to the conventional currency. But as there is no necessity to settle up, ledger transactions can proceed indefinitely. One might even decide to drop the reference to euros in the ledger (as was subtly done in the previous paragraph) and refer to this currency simply as LedgerCoins (LC). In the case of Bitcoin itself, which our LedgerCoins are an allusion to, the case is even clearer, as we will see. There was no original injection of real cash and so the coins should be viewed as existing in the form of entries on a ledger in their own right. Crucially, this means that a bitcoin has zero intrinsic value! Its worth is entirely determined by what people are prepared to pay for it.

Returning to our hypothetical ledger, we now turn our attention to Problem Two. A first attempt at solving it is to insist that each member signs off on each payment that they make. Thus, if Karl pays Rosa fifty LC, he signs his name to that entry in the ledger. As signatures can be forged, this is hardly

a comprehensive solution. One way around this is to use something called a 'digital signature'. (At this point we are assuming that the ledger is hosted online. We will come to the hosting issues of Problem Three shortly.) Now, a digital signature is quite a sophisticated entity and, for reasons we will shortly outline, it is unfeasibly difficult to forge. Indeed, the mathematical principles behind it arise in solving the third of our problems and are at the heart of how Bitcoin works. Thus, it is worth taking a short mathematical digression.

There are two notions we must introduce, the second following on from the first. We begin with large numbers. The physicist George Gamow, in his marvellous popular science book *One, Two, Three ... Infinity*, recounts the legend of King Shirham of India.[4] Shirham, delighted with the invention by his grand vizier of the game of chess, offers the vizier a reward. With seeming modesty, the vizier requests only that there should be placed on the first square of the chess board a single grain of rice, followed by two on the second, four on the third, and so on doubling the number of grains until the final sixty-fourth square. The rice on the final square is all he requires. The king, astonished at what he perceives as so humble a request, eagerly agrees. Of course, such a rate of growth, which we call 'exponential', is something we know only too well in a time of pandemic. The sequence proceeds: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024 … By the time we reach the thirty-first square, which is not even halfway, the required number of grains has already surpassed a billion. By the end, the required debt owed by King Shirham was so large that it would take several millennia of harvesting all of the rice grown in the world today in order to meet it! Such numbers are called powers of two. And we write 2^n to represent two multiplied by itself n times. Thus, King Shirham owed his vizier 2^{63} grains of rice (the first square required 2^0=1 grain), an astonishingly large number.

Powers of two will play an important role in our discussion for the reason that the computational information we are dealing with often appears in binary form, i.e. as a sequence of 0s and 1s. The number of ways of writing a sequence of n such 'letters', given that there are two choices for each letter, is precisely 2^n. Thus, there are 2^5=32 ways of writing a sequence of length five, i.e. numbers like 01101, 00111, 10101, etc. As the length of n increases, the number of possible 'words' of length n that can be formed from 0s and 1s grows exponentially. Of particular importance in our story is the case when n=256. The number 2^{256}, the number of strings of 0s and 1s of length 256, is an utterly astoundingly large number. Words simply do not do this number justice. As a feeble attempt at conveying its immensity, it should be noted that 2^{256} is a little more than 500 times greater than current estimates for the number of atoms in the known universe![5]

The second notion we must introduce has a rather alarming name and the reader should not worry too much about this. It is an example of something called a 'cryptographic hash function n', and more precisely called SHA256. The initials SHA stand for secure hash algorithm. So, what does it do? Well, quite simply, it is a computational creature (algorithm) which 'eats' a message of arbitrary length (some list of words and numbers like a set of ledger transactions for example) called an input, and spits out one of these strings of 256 0s and 1s we met in the previous paragraph, the output. Such an output is often called a hash. Thus, SHA256 takes in an input message and makes a hash of it! The term 'function' means that for any input one feeds into SHA256, there is precisely one corresponding output string of 0s and 1s (the same one every time) associated to that input, which the creature spits out. So, each input results in one well-defined hash. Now, it is perfectly possible for two distinct input messages to produce the same output, although finding a pair which does that is an extraordinarily difficult task.

Following our earlier discussion, it is hopefully clear that the numbers of possible inputs and outputs involved here are colossal. What is more, SHA256 is designed in such a way that even when input messages are similar (say differing only in one digit or character), their corresponding outputs will look nothing like each other. This means, and this is very important, that if one wanted to reverse the process and find an input which SHA256 sends to a given output, one would have no better way of doing this than guessing! Remember, getting an output from an input is easy. SHA256 just spits it out. Trying to go in the reverse direction and find an input from an output

is very, very hard and can only be done by guessing!

Now, modern computers can guess quickly, but given the immensity of options, finding the desired input would still be utterly unfeasible. With current technology, one would need something like billions of times the computational power available to humanity working over billions of years to even have the slightest chance of guessing the right input! This fact is at the root of encrypting (and thus protecting) the information contained in every credit card transaction in the world today. Though that does not mean that this data is invulnerable to other sorts of attack; there are all sorts of ways in which people can be tricked into divulging information!

We now return to our earlier discussion and the problem of using a signature to verify a transaction, Problem Two above. A digital signature consists of two numbers (both strings of 1s and 0s). The first of these is called a public key and, as its name suggests, is publicly available. Essentially, it forms part of the visible profile of a member of our community of LedgerCoin users. The second number, which is associated to the first in a rather complicated mathematical way which we will ignore here, is called the private key and is kept secret. Essentially, when the payer in a transaction wishes to add a message to the ledger indicating payment to another, they feed both their message and private key into SHA256 to obtain a digital signature. There is an elementary process for verifying that a given digital signature is legitimate: a function which takes in the original message, the digital signature, and the public key of the signer and returns a verdict of either true or false depending on the legitimacy of the digital signature. Given our earlier discussion on the unfeasibility of reversing the SHA256 function, it should be clear that there is no feasible *computational* way of stealing the signer's private key from such a process.

We now come to the third and most fundamental problem, the one solved in the 'Bitcoin White Paper'. The idea is to do away with a centralised ledger and the need to trust any individual or organisation with its maintenance. Decentralising the ledger involves having 'copies' of the ledger spread out throughout the community individually maintained by users. Of course, one naturally would wonder how that could possibly work! How would one guarantee that these copies coincided? Surely it would not be long before multiple versions of the ledger emerged with different histories of transactions causing the entire enterprise to fall apart?

To deal with this problem, the following protocol is adopted. Each member keeps their own copy of the ledger. Whenever a person initiates a transaction, they broadcast this publicly to the network and members update their ledgers to account for this, but with respect to a very important criterion. The ledger is organised into subsets of transactions called blocks, organised together in a chain, a so-called 'blockchain'. Adding to the ledger means gathering together a list of recently broadcast transactions to form a new block. Having assembled a block, the assembler must complete a computational task or 'do work on their block' before they can add it. This work involves a sort of simplified version of the unfeasibly difficult reversing of the SHA256 function discussed earlier. Essentially, enough extra information is given to make the 'target' of one's guesswork sufficiently large that within a short time, say about ten minutes, a moderately powerful computer processor (or set thereof) will find an appropriate number: the so-called proof of work. This number is added to the block and the block is added to the chain. Importantly, when a new block is added, the proof of work number of the previous block is stated clearly at the top, thus properly connecting the chains. Any attempt at rewriting an earlier block would undo all work done on every subsequent block!

At this point the problem of multiple conflicting ledgers arising is not yet solved. What we have are 'block builders' all around the world, listening out for transactions, creating blocks, racing to be the one complete the 'work' on the blocks, and adding them to the chain. Importantly, these block builders are incentivised to do this work by an inbuilt rewards system. Successfully verifying and adding a block yields a small quantity of additional LedgerCoin to theledger. These additional coins do not come from the existing pot but are newly minted by the underlying algorithm precisely for this purpose! Note that, by design, anyone with the requisite computing power (and an internet connection) can be a block

builder, as the broadcasting of transactions is publicly accessible.

So now we come to the key point. If a conflict arises and two chains start to differ, the protocol is to always defer to the chain that has had the most work done on it, i.e. the longest chain. This gives us an unambiguous way to determine a version of the ledger history. However, one might well ask why this gives a fair version of events. To see this, consider what it might take to subvert the true history of transactions. Suppose for example, Karl broadcasts to Rosa *alone* that he is paying her 500 LC for a bicycle but keeps this secret from the rest of the community. That way he gets Rosa's bike, she thinks he has paid her 500 LC, but as far as the rest of the world knows the payment never happened and Karl is free to spend his 500 LC elsewhere. There are now two versions of the ledger. However, in order for Karl to maintain his version, he has to stay ahead of the rest of the community in the race to add more blocks. Recall that adding blocks means doing computational work. Unless Karl alone has vastly more computational power than the rest of the community combined (a problem which under capitalism should not be discounted), it is probabilistically impossible that Karl can maintain his version of events for any significant period of time.

What we have described here, in the guise of LedgerCoin, is effectively Bitcoin. With some minor adjustments, it characterises any of the digital currencies out there. In essence, the key contribution of Nakamoto was the establishment of the blockchain, the decentralised ledger which contains a history of all Bitcoin transactions. Having set up a public/private key pairing, which provides anonymity (or at least pseudonymity), one can obtain bitcoins in one of two ways. The first is to buy them directly from an owner, which means having a line added to the ledger to that effect. As we will discuss, given its wildly fluctuating value, this is a very risky endeavour.[6] The second is one we briefly mentioned earlier. The process of verifying and adding blocks to the ledger is incentivised by assigning to the block builder/adder a certain quantity of new bitcoin for their trouble. Anybody with the appropriate software and enough computer power can do this, and indeed, part of the principle of Bitcoin is that the ledger is spread out and worked on by as many people as possible. It is in the sense that the ledger is said to be decentralised.

Built into the Bitcoin verification process is a gradual decline in the value of the incentive rewards for those checking transactions. This means that there is a finite limit on how many bitcoins will ever come into existence, some twenty-one million coins.[7] Incidentally, this is not true of all cryptocurrencies. Over the years, users have compared the process of obtaining rewards for verifying transactions to mining for gold or precious stones. There is a certain amount of 'buried' bitcoin, and the rush is on to dig it out. Thus, the process of transaction verification is commonly referred to as bitcoin mining or just mining. As we will shortly see, the analogy runs deeper than that when one considers the environmental destruction wrought by both practices.

Despite the ever-diminishing returns available to bitcoin miners from the intrinsic reward process, there is always another incentive. In order to have their transactions more rapidly added to the block, users often add a tip to the miner (some fraction of bitcoin as a sort of transaction fee). This latter aspect is very important in determining how long it might take for a transaction to go through. In general, this can vary wildly, from hours to days or even weeks. It depends on how many transactions are awaiting confirmation, the number of miners and their corresponding computational power (hash power), and most importantly, the priority miners place on a given transaction. Adding a larger tip increases the likelihood a transaction will be verified quickly. Too small a tip and, with a declining intrinsic reward, a transaction may sit unverified indefinitely.

Bitcoin in the news

In February of this year, Elon Musk's company Tesla purchased 1.5 billion US dollars' worth of the digital currency Bitcoin.[9] Tesla also promised that the company would shortly start accepting this alternative decentralised currency as payment for its products. Musk, who along with his space-race competitors Bezos and Branson must surely rank as one of the poster children for Bond-villain capitalism, cited the fact that Tesla had a lot of spare cash to invest. The

company wished to maximise returns by investing in 'reserve assets' such as digital currencies and gold bullion. This is something which speaks volumes about the current state of capitalism. Immediately, the value of an individual bitcoin spiked to its then highest level of $44,200, having seen lows of less than $5000 only twelve months previously, and having followed a rollercoaster ride of fluctuating value over the decade or so since its inception. By May, it had reached a record high of over $60,000.[10] Amid the frenzy, some commentators argued that the flagship cryptocurrency was finally breaking through into the mainstream.[11]

At the time of writing, less than two months since its record high, the value of Bitcoin stands at less than $30,000, a fall of more than 50 per cent.[12] The extent to which Musk's subsequently cooler Twitter comments are a factor is unclear; it is likely that a recent clampdown by the Chinese state on cryptocurrencies is another one. Indeed, many governments, in particular the US, fear that cryptocurrencies may be used by certain 'rogue nations' to navigate around sanctions or to destabilise more conventional currencies. In any case, what is not in doubt is that Bitcoin and the many thousands of other subsequent cryptocurrencies rank as some of the most volatile and riskiest investments going. More than this, it shows the ease with which wealthy individuals can manipulate the value of these entities.

Surrounding the cryptocurrency phenomenon is an inordinate amount of hype, impenetrable technical verbiage, and a ferocious debate. There are those who hail 'crypto', touting its independence from governments and traditional financial institutions, as the future of money. Financial transactions involving Bitcoin, for example, are accurate and, for reasons we have discussed, very difficult to hack. Many advocates speak with an evangelical devotion, suggesting that Bitcoin and its analogues represent a world-changing innovation. Indeed, there has been some support for digital currencies and the technology underlying them from figures on the left. The argument is that they represent (or at least have the potential to represent) a radically democratic form of currency and one that can be used to undermine major financial institutions. In particular, the hope is that this might allow some of the most impoverished people access to financial services that they would otherwise have no chance to obtain. Unfortunately, the evidence overwhelmingly suggests this hope is an illusion; a point we will return to.

While some of the support for cryptocurrencies is based on an appreciation of the technology involved, most of it is fuelled by 'charismatic' internet personalities attempting to get people to buy some or other cryptocurrency with the promise of an easy fortune, or new start-up companies promising to further enhance the technology underlying cryptocurrency and selling 'digital tokens' to investors as a means of raising revenue. Such digital tokens are the cryptocurrency equivalent of a voucher for a department store (one with the implied potential to grow immensely in worth). Except in this case the department store does not yet exist, and even if it materialises, the voucher may well end up of little value. This is essentially what happened to investors in the company Block.One, which netted billions from such a scheme, leaving investors holding an empty sack. The company suffered only a paltry $24 million fine from the SEC (Securities and Exchange Commission) in the US, though investors have since brought a class-action lawsuit.[13=]

The ease with which such cybercurrencies can be established makes them fertile ground for so-called 'pump and dump' scams whereby teams of investors rapidly buy up and promote a particular stock to artificially inflate its value before quickly selling it off, leaving some hapless buyers with worthless junk. Whatever value some cryptocurrencies or their underlying technology may offer, there is no doubt that the field is brimming with scams and pyramid schemes of all sorts. Another consequence of the lack of regulation and the relative anonymity of cryptocurrency transactions is that they are, inevitably, highly attractive to gangsters and money launderers of all kinds. Indeed, kidnapping and extortion become far less risky for the criminal when it is virtually impossible to trace the cash used in ransom. The recent increase in cyber ransomware attacks, such as that sustained by the Irish Health Service Executive earlier this year, is to a significant degree based on the emergence of cryptocurrency.[14]

The environmental impact

There is another fact which is undeniable and arguably the most serious objection to cryptocurrencies, at least in their current form. It is a fact which should be at the forefront of any discussion on the merits or even potential merits of this technology, and that is that cryptocurrencies have a devastating environmental impact. As the above description hopefully conveys, the brute force calculations involved in these transactions involve mind-bogglingly large numbers and necessarily require enormous computational power. This requires energy, and lots of it. And there is no way of avoiding this without significantly reinventing these entities in a very fundamental way. Recall that the 'miners' who verify transactions are rewarded for doing so by an intrinsic rewards system which generates new currency as well as in the form of transaction fees tipped by users. Provided the computer network is sufficiently powerful, the electricity costs sufficiently low, and the relevant cryptocurrency judged to be sufficiently valuable, the person running such a network is effectively printing money!

What is more, the process of mining for cryptocurrency is super competitive, which further exacerbates the ecological impact. Over the last decade, Bitcoin and other cryptocurrency mining operations have popped up all over the world, competing with each other to verify transactions and mine the reward. These 'mines' are essentially large warehouses packed with highly specialised computer processors running through tedious calculations at high speed and guzzling electricity. Verifying a lone block on the blockchain is a somewhat random hit or miss process. However, with a large-scale operation and enough computational power, statistically there will be hits. So long as the costs of running such operations (which aside from the hardware mostly involve local energy), are sufficiently low and the value of Bitcoin and the hit rate are high enough, the profits will roll in.

Up until about a year ago, some 65 per cent of these mining operations were in China.[15] Recently however, the Chinese state has shut down most of these operations. However, cryptocurrency mining is still a booming business, and in the United States it is growing rapidly. Recently, an American bitcoin mining company called Core Scientific was valued at almost $5 billion on the Nasdaq exchange. Based out of Washington State, the company successfully mined over 1600 bitcoins (worth about $53 million) in the first half of 2021.[16] British bitcoin miners Argo, who trade on the London Stock Exchange, have recently stated they intend to commence operations in the United States next year.[17] Currently 8 per cent of the world's bitcoins are mined in Iceland, where energy costs are relatively low and where the local climate means cooling costs for computer hardware are significantly reduced.[18]

To put all of this in perspective, in 2014 it was estimated that the total yearly energy cost of mining bitcoin alone (not counting other digital currencies) was equivalent to that of Ireland's total yearly energy consumption.[19] Since then, the problem has greatly worsened. In February of this year, research at Cambridge University concluded that the yearly energy consumption of bitcoin mining was on the order of about 121 terawatt-hours per year.[20] This means that if bitcoin mining was a country, it would rank in the top thirty energy consuming nations in the world, lying just above Argentina. And while bitcoin mining will likely peek in value at some point (although it is unclear when), this is to say nothing of the multitude of other cryptocurrencies and the ecological impact they will have. Amid the gravity of the environmental crisis our species faces, it is difficult to imagine a more absurd and parasitical form of energy consumption than this.

The problem of cryptocurrency mining is at the extreme end of a much larger and more complicated problem. That is the considerable and growing energy cost of processing the gigantic quantities of data which have become such an intrinsic part of all our lives. This relates not just to the financial realm but to mobile phone use, email and social media sites, businesses of every shape and size, along with state institutions. Much of this data is stored in so-called data centres. These are essentially warehouses hosting vast complexes of computing and digital storage systems, servers, routers, and firewalls. Such facilities, like those used to mine cryptocurrencies,

require enormous quantities of electricity. Dublin hosts one of Europe's largest concentrations of such data hubs, which in 2020 accounted for close to 2 per cent of Ireland's total carbon emissions.[21] Such is the strain this imposes on the electrical grid that the regulators in Ireland have warned of the threat of possible blackouts in the near future. This rapidly growing sector is dominated by big players like Facebook, Amazon, Google, and Microsoft. Some of these organisations have formed a lobby group within IBEC called Cloud Infrastructure to oppose any moratorium on data centre construction and to prioritise their access to the national grid.[22]

Aside from the heavy hitters, more and more organisations and businesses are seeing the need to increase their online presence as a means of survival. This is especially true in the light of the pandemic. Dealing with this problem is not easy. The processing and storage of data plays a very important function in a modern society, and most of us depend on this to some extent. Many of those hailing Ireland's transformation into one of Europe's key data centre economies will say that an increasing proportion of this energy comes from renewable sources. However, such claims are notoriously unreliable. Moreover, while it is possible for big corporations like Amazon to buy large swathes of energy from wind farms, this still begs the question as to whether the purposes Amazon puts this energy to are really the optimal ways such energy can be used. And while it is certainly the case that most of us rely on or at least benefit from the ability to hastily send and store vast quantities of data, what is unclear however is how much of this data is not only useless to most of us but downright hostile. For example, how much data is stored purely for purposes of marketing, advertising, and mass manipulation? How much data is collected and stored by states as a means of tracking and controlling their citizenry? And what say do the majority of us have in what is stored and how it is used?

This takes us to the fundamental problem. A technology like blockchain (which underlies Bitcoin), or the internet, or any of the myriad technological innovations our species has developed, arises not in a vacuum but in a social and historical context. How an idea develops and how a technology is deployed is something which is heavily determined by the interests of those in power. It is certainly the case that blockchain contains within it some intriguingly clever notions. The economist Yanis Varoufakis, incidentally a highly competent mathematician, argues that blockchain is a brilliant innovation. Interestingly though, he has described it as 'the answer to a problem that does not yet exist' and has gone on to issue fairly withering denunciations of Bitcoin and other cryptocurrencies.[23]

Varoufakis's position on this is worth exploring. It is certainly the case that a decentralised ledger system which takes control of financial transactions away from private banks sounds, in principal, like a wonderful thing. Indeed, such a ledger, where all major monetary transactions are publicly available (and where it is possible for everyone to know how much money is in the system) should be a necessary part of any democratic society. Indeed, Varoufakis argues, a Bitcoin-style currency based on something like blockchain technology is likely the sort of currency that any fledgling socialist society would want to adopt. But we do not live in a socialist society. And under capitalism, the form and application of such a technology has a radically different consequence.

While it is difficult to obtain precise data, studies show that at least 75 per cent of all bitcoins are in the hands of the top 2 per cent of owners.[24] Some studies suggest this number is as high as 95 per cent.[25] Most investment in Bitcoin is speculative, and so owners are unlikely to part with their coins, at least when the value is climbing. This coupled with the cap on the total number of coins, something which those holding even modest quantities of the currency have a strong interest in maintaining, makes it very difficult to conceive of Bitcoin playing the role of a real currency. Instead, along with other cryptocurrencies, it is mostly just a source of speculative mania, of an exploding number of scams and Ponzi schemes, and, fundamentally, an opportunity for the wealthiest and most destructive elements in our society to hide their wealth and further enrich themselves.

Capitalism necessarily creates concentrations of wealth and power. Over time these concentrations can become ever more extreme, sucking in more wealth and power in the manner of a black hole singularity. The effect of this is to distort and turn upside down the means to which technological innovations are put. When a new technology emerges, it is those best placed to utilise it who will determine how it is deployed. Moreover, while states and governments under capitalism are there to manage and facilitate the interests of the ruling capitalist class, forms of deregulation rarely benefit the majority. Often the regulations that do exist, such as those concerning health, safety, and the environment, or those concerning financial markets, have been hard fought for and provide us some protection from the most vicious aspects of the system. Thus, deregulation almost always favours those with the means to take advantage. It is the absurd nature of that system, worse when unchecked, that allows individuals to accumulate vast wealth for doing nothing more than setting energy intensive machines to work doing utterly pointless calculations. Whatever theoretical advantages it may one day offer, the reality is that the short history of cryptocurrency is one of powerful people and nefarious interests riding roughshod over the needs of the many.

In its early years, many, including some on the left, felt that the internet would have a profoundly positive and democratising influence on our world. As we sit firmly in the information age, it is abundantly clear that, like all such technological developments, the internet reflects the deeply unequal and undemocratic society we live in. And while those of us wishing to challenge the power structures of the world have made use of this technology, and found places in which to operate, the overwhelming benefits of the internet and all its corollary technologies like cryptocurrencies have been predictably harvested and deployed by those who rule. There is a lesson here. How a technological breakthrough may a change a society is a deeply political matter. There is absolutely no guarantee that scientific innovation alone will improve our world. Indeed, in a system such as ours, the opposite is very often the case. It is only in a system based on genuine democratic principles and the shared and ecologically responsible stewardship of the earth's resources that we can rationally control and optimally enjoy the fruits of our hard-won scientific knowledge.

Acknowledgement: The author is grateful to Professor David Malone of the Hamilton Institute at Maynooth University, an expert in these matters, for a several clarifying conversations.

NOTES

1. https://www.npr.org/2019/02/11/691334123/swedens-cashless-experiment-is-it-too-much-too-fast?t=1627833691540
2. https://bitcoin.org/bitcoin.pdf
3. https://www.youtube.com/watch?v=bBC-nXj3Ng4
4. George Gamow, *One, Two, Three,... Infinity*, Bantam Science and Mathematics, April 1963, Ch 1, p 7.
5. https://www.livescience.com/how-many-atoms-in-universe.html
6. https://www.statista.com/statistics/326707/bitcoin-price-index/
7. https://www.statista.com/statistics/802775/worldwide-cryptocurrency-maximum-supply/
8. https://www.bbc.com/news/business-55939972
9. https://www.statista.com/statistics/326707/bitcoin-price-index/
10. https://www.vox.com/recode/22383757/bitcoin-coinbase-ipo-crypto-ethereum-cryptocurrency
11. https://www.bbc.com/news/business-57549543
12. Alizart, M. *Cryptomcommunism,* Polity.
13. https://www.sec.gov/news/press-release/2019-202
14. https://www.theguardian.com/commentisfree/2021/jul/10/how-bitcoin-and-putin-are-enabling-the-ransomware-spree
15. https://www.youtube.com/watch?v=bBC-nXj3Ng4
16. https://www.cnbc.com/2021/06/15/chinas-bitcoin-miner-exodus-.html
17. https://www.forbes.com/sites/jonathanponciano/2021/07/21/bitcoin-miner-core-scientific-to-go-public-at-4-billion-valuation-as-us-crypto-mining-gains-steam-on-china-crackdown/?sh=6feb8c92599f

18. https://www.vanityfair.com/news/2019/11/the-big-bitcoin-heist
19. O'Dwyer, M., *Bitcoin Mining and its Energy Footprint,* ISSC 2014, Limerick
20. https://www.bbc.com/news/technology-56012952
21. https://www.irishtimes.com/business/energy-and-resources/number-of-operational-data-centres-in-ireland-up-by-quarter-report-finds-1.4562274
22. https://www.irishtimes.com/news/ireland/irish-news/big-tech-lobbying-coalition-against-curbing-data-centres-1.4617306
23. https://www.wired.co.uk/article/yanis-varoufakis-bitcoin-bubble-interview
24. https://insights.glassnode.com/bitcoin-supply-distribution/
25. Ibid