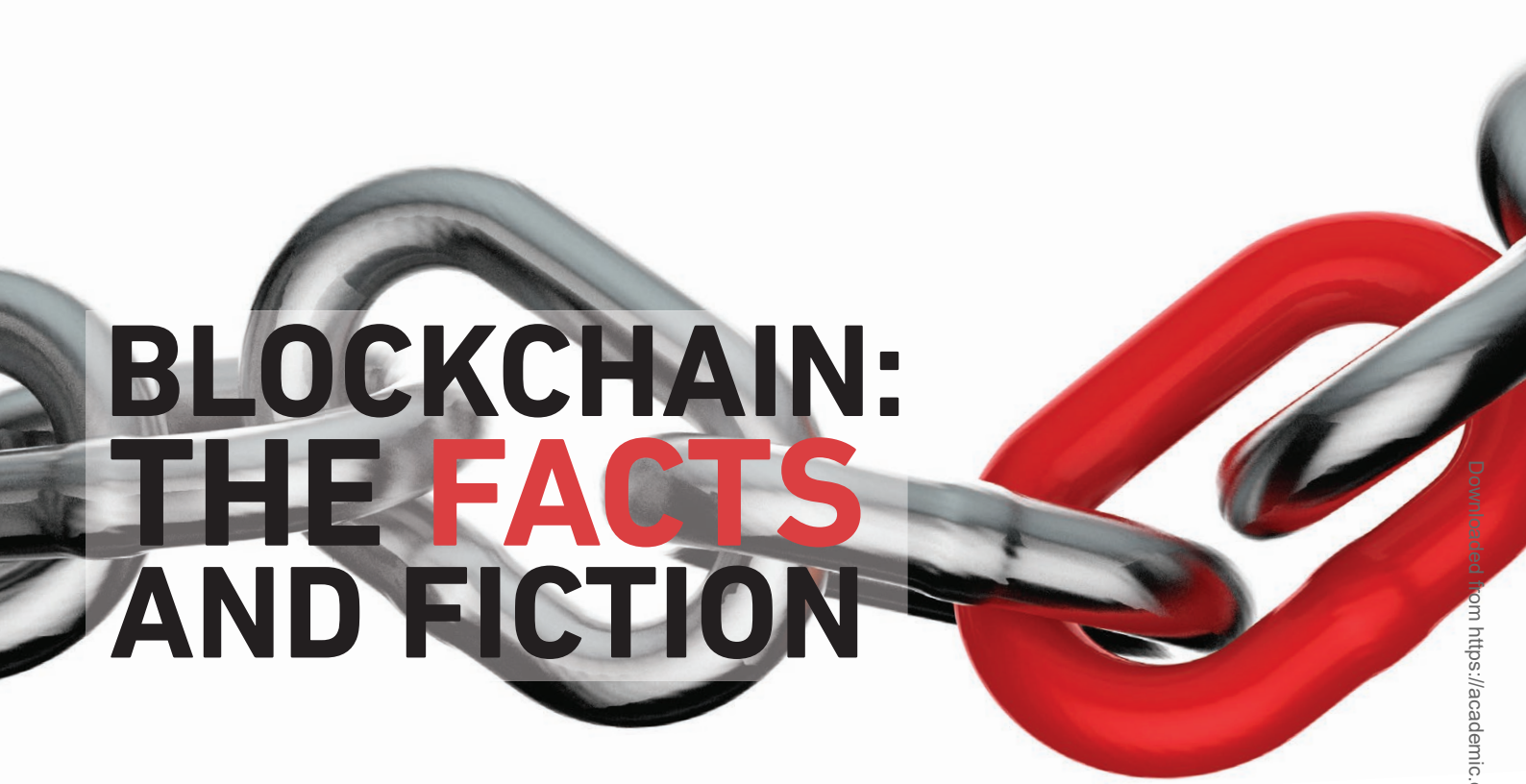

BLOCKCHAIN: THE FACTS AND FICTION

If you look at any indicator of what the data management world is interested in right now, blockchain will be at the top of the list, writes Ron Ballard, database consultant and author.

Internet searches, pronouncements by CEOs, new books published, information technology magazines, podcasts, major software companies, industry analysts, etc. All seem to be in a blockchain frenzy...

How does blockchain work?

First of all, let's take a look at how blockchains work. You can read Satoshi Nakamoto's original paper at **http://bit.ly/31oG7ba** for much more detail; this is a quick summary.

Bitcoin is what made blockchain famous. It is not the only blockchain application but it is the model for the others; it is by far the biggest, so you can assume Bitcoin in this description unless we say otherwise.

Blockchain combines two mature technologies: the chain and the hash.

Simple chain structure

The chain structure has been used for at least 50 years in data management sofware. The simple chain shown here is not 'blockchain', it is just a chain of blocks.

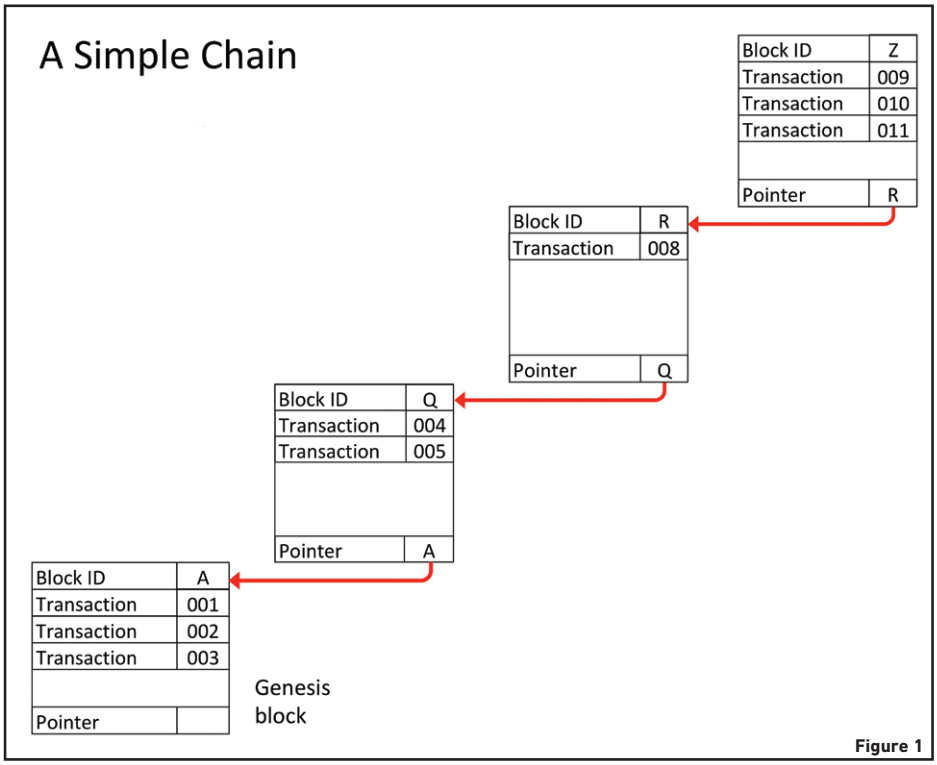

Figure 1

Each block is linked to the previous one by having a pointer value that matches the block ID of the previous block. If we want to change a simple chain, we can: we just add the new block and adjust the pointers.

But blockchain wants to make the chain 'immutable' so that once a block has been added to the chain it cannot be changed. Blockchain achieves this by making it very expensive to change the chain, as we shall see.

Hashing

The hash is also a very old computer sofware concept, going back at least to 1953.

A hash is a value that is calculated by applying some function to the series of bytes that make up a field, a block or even a whole file. The hash value is usually a number. Using a particular hash function the same input will always give the same output. Let's start with a very simple example. We could take the UTF-8 value of each character in the input, add them all up, divide the result by 256 and take the remainder as our hash. This is what we get for a few different strings as shown in **Table 1**.

This hash function is very simplistic and can produce only 256 values, so we do get some collisions, as in the last two rows of this table.

The hash function used in blockchains is usually SHA-256. In this case '256' refers

doi:10.1093/itnow/bwaa039

to the number of bits in the hash, so we get 2^{256} or 10^{77} possible values and the chance of a collision is unimaginably small.

Input	UTF-8 values	Sum of UTF-8 values	Remainder (our Hash)
Ron	82, 111, 110	303	47
Relational datatbases for Agile developers	82, 101, 108, 97, 116, 105, 111, 110, 97, 108, 32, 68, 97, 116, 97, 98, 97, 115, 101, 115, 32, 70, 111, 114, 32, 65, 103, 105, 108, 101, 32, 68, 101, 118, 101, 108, 111, 112, 101, 114, 115	3893	53
Netezza	78, 101, 116, 101, 122, 122, 97	737	225
NonStop SQL	78, 111, 110, 83, 116, 111, 112, 32, 83, 81, 76	993	225

Table1

A blockchain

Now we can combine the simple chain and the hash to make a blockchain. This example is simplified but it still shows the main feature that makes blockchains 'immutable'.

The first step is to make our block ID 'A' the 'genesis block'. We make a SHA-256 hash of the contents of the block:

'Block ID|A|Transaction|001|Transaction|002|Transaction|003|Pointer||'

Which gives us the SHA-256 hash: dfdba2bdb97e68127d817502c192f94cd251e5a5024aed96fb72864e.

We now use this as the identifier of the block. We use the block hash of the genesis block as the pointer in the next block (our block ID 'Q').

So now, we make a SHA-256 of block ID 'Q' including the pointer to the genesis block:

'Block ID|Q|Transaction|004|Transaction|005|Pointer|dfdba2bdb97e68127d8175ea200be502c192f94cd251e5a5024aed96fb72874e|'

Which gives us the SHA-256 hash: 3c4374099d09d10d36545c5bf10db1eb2dbe36b936312b95ce9803c923d82c60.

We use the hash of block ID 'Q' as the pointer in block ID 'R' and include the pointer to block 'Q' in the block hash of block 'R'. We continue up the chain as shown in **Figure 2**.

If we change just one byte in the data of block ID 'Q', then the hash of block ID 'Q' will have to change to make this block valid.

Now block ID 'Q' has a different block hash. So, to make block ID 'R' valid, we have to change its pointer so that it points to our new version of block ID 'Q'.

We have to calculate a new block hash for block ID 'R', which means we have to change the pointer in block ID 'Z' and so on until the end of the chain.

So, you can change a blockchain but if you do, then you have to change every block that follows, which costs as much as creating all the blocks in the first place.

Since blockchain is immutable, there are other requirements that make it even more difficult to change. These include 'proof of work' and a 'peer-to-peer network' to validate the blockchain.

The 'proof of work' is an arbitrary calculation that is done for every block that is added. The calculation is what produces the block hash and it is more complicated than the example given. In fact, thousands of hash calculations are required to produce the block hash.

Bitcoin adds other complications to the 'proof-of-work' so that it really is very expensive to carry it out. The first peer to do this successfully gets to create the block

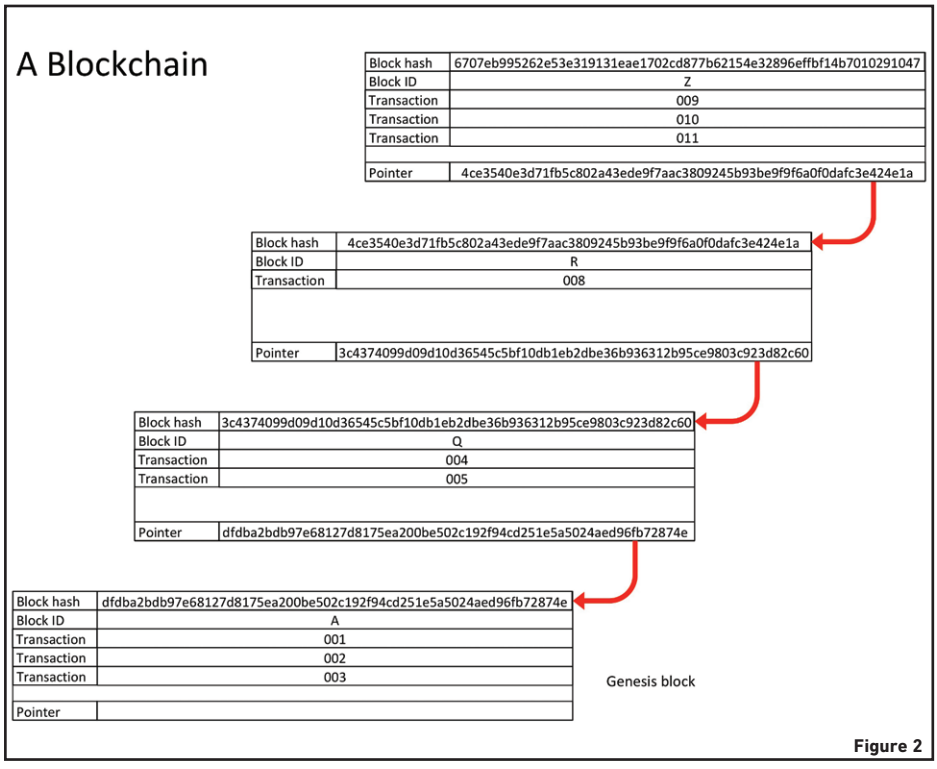

Figure 2

Figure 3

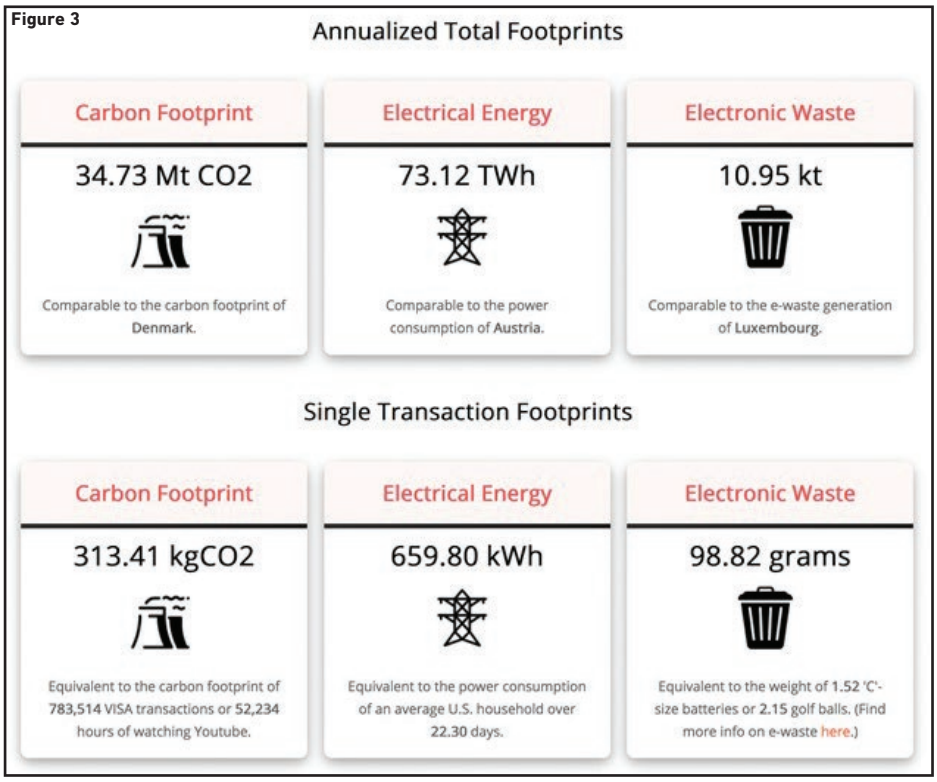

Image: digiconomist.net

and claim the reward.

Claims about blockchain

There are many claims made about blockchain. Most of them fall into the vacuous marketing-hype category, such as:

'Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system.' — bitcoin.org

'From frictionless supply chains to food we can really trust, learn how industries are revolutionising business with IBM blockchain. Let's put smart to work.™' — IBM

'Create smarter, more efficient supply chains, reduce fraud, verify transactions more quickly and create disruptive new business models with Azure blockchain services.' — Microsoft

'Improve trust and efficiencies in a network-driven world with blockchain technologies.' — SAP

'Oracle blockchain platform securely extends your business processes and applications while enabling you to process business transactions much faster.' — Oracle

'For the United Nations to deliver better on our mandate in the digital age, we need to embrace technologies like blockchain that can help accelerate the achievement of sustainable development goals'. — António Guterres, United Nations Secretary General.

There are many breaches of truth in these statements. There are also some specific and testable claims:

- Immutable ledger ('tamper evident');
- low transaction fees;
- cryptographic proof;
- worldwide payments;
- fast peer-to-peer transactions;
- enables 'smart contracts'.

Before we look at these claims specifically, though, we must consider the show-stopper for blockchain and that is the massive damage it is doing to the environment.

Sustainability

We are in a climate emergency. To waste an amount of electricity equivalent to that used by Austria is a crime against our planet. **Figure 3** gives several measures of the scale of this crime.

The statistics are for Bitcoin only, although; most other cryptocurrencies work in the same way. Ethereum is the next biggest digital currency and although it is significantly smaller than Bitcoin, it is still very damaging, using the same amount of electricity as Luxembourg.

The organisations that create new blocks ('miners') are based where there is a large and cheap supply of electricity. For most miners that means China, where electricity is cheap and mostly produced using the worst method for the environment: coal.

Blockchain 'miners' are in a massive international arms-race with one another. Those who can deploy the most computing power get to add the most blocks to the blockchain and earn the most Bitcoins.

Proponents of Bitcoin say that the machines that do the work will become more efficient. But if they double in efficiency, the energy use will still be obscene. And they also say that the number and size of blockchains will increase dramatically.

If the technology is used as widely as the hype suggests, then Bitcoin (and blockchain generally) will be significant factors in the climate change disaster because they use so much power.

This is enough of a reason to put blockchain in the technology waste bin right now and really does make the statement by the UN secretary general very problematic: he should know better.

Other claims

I cannot imagine an advantage of any software system that would be great enough to make it worth the environmental cost of blockchain, but let's see if any of them come close:

Immutable ledger

There are two problems with the immutable ledger:

1. It is not immutable.
2. It does not solve the problem of fraud.

There were supposed to be many independent anonymous peers keeping the blockchain from corruption. However, you can watch blocks being added to the

doi:10.1093/itnow/bwaa039

Bitcoin blockchain at **https://bitaps.com/**.

You don't have to watch for long to see that most blocks are committed by 'mining pools'. If you can't spare the 10 minutes or so that it takes to check this, then scroll down on the webpage to see the pie chart that shows most blocks being committed by mining pools.

These pools are mostly in China where the state's influence over business is much more powerful than it is in most other countries. The idea of independent peers has been subverted, so the blockchain is now vulnerable to an attack by a controlling miner.

There have been many multi-million dollar frauds involving blockchain (see **https://bit.ly/2vExPjV**). The 'immutability' does not protect against fraud. Most frauds occur outside the computer system, in the real world.

If the blockchain faithfully records a fraudulent transaction, then that transaction is still fraudulent. The 'immutable ledger' is a blinkered techie approach which assumes that fixing the computer system will fix a problem out there in the real world. It doesn't.

Low transaction fees

When you submit a request for your transaction to be added to the blockchain, you specify the transaction fee. The miners then choose the transactions with the highest fees to add to the next block. The more you pay, the sooner you get your transaction in a committed block. So, transaction fees are very variable and can be high if you are in a hurry.

But the transaction fees are tiny compared with the block reward and this shows the real cost of blockchain transactions. The block reward is currently about £100,000. Sometime around May this year, the block reward will be halved – this is part of the Bitcoin/blockchain design and has happened twice before. The value of Bitcoin increased each time.

We don't know what it will do to the economics of mining this time, but a decrease in transaction fees does not seem a likely outcome.

Cryptographic proof

Hash algorithms are used in cryptography; to provide a check on the content of a chunk of data; as a type of indexing and simply to provide a unique key in a distributed database. The blockchain is not encrypted. The term 'crypto' (with or without a suffix) appears to serve only the purpose of sounding cool and high-tech, when in fact the technology is not very sophisticated and is certainly not cool.

'The "immutable ledger" is a blinkered techie approach which assumes that fixing the computer system will fix a problem out there in the real world. It doesn't.'

Worldwide payments

Bitcoin can do this. So can many other payment systems. The transaction fees may or may not be less with Bitcoin, but the environmental cost is several orders of magnitude higher with Bitcoin.

Fast peer-to-peer transactions

The peer-to-peer statement is just untrue. When you make a transaction with Bitcoin, you deal with miners, who can arbitrarily accept or ignore your transaction. You also deal with the blockchain software, probably via an app. There is still a 'middleman', but you don't know who it is.

As for 'fast', it takes an average of about ten minutes to get your transaction committed, assuming you paid a big enough transaction fee to get it into the next block. Typical international credit card payments are completed in less than a second. How does ten minutes qualify as 'fast'?

Enables 'smart contracts'

There doesn't seem to be much evidence of smart contracts actually existing at present. And there is no reason why such things cannot be implemented with other technologies. I have various automated payments using my bank accounts and credit cards: variable direct debits for example. The 'smart contract' appears to be more marketing fluff and is certainly not something enabled only by blockchain.

In summary

Blockchain is not a silver bullet, as the big vendors claim. They can make money out of blockchain consultancy, but if they had any integrity, they would advise their clients to avoid blockchain completely.

There are no exciting uses that could not be covered by any previous payment system. Even money-laundering is still possible with other payment systems, although it is easier with Bitcoin/blockchain. Is this actually an advantage of blockchain?

Gambling on a highly volatile currency is what has sustained blockchain and allowed it to set about trashing the environment.

Blockchain implementations that use the original proof-of-work (that is most of them) are a climate-change disaster and should be stopped. It is hard to see how they can be stopped now, but they should be. As individuals we can:

- Avoid any use of blockchain-based currencies.
- Write to politicians, charities (especially green charities), newspapers, climate-change activists, to make sure they understand the environmental cost.
- Refuse to support charities that accept Bitcoin donations — move those donations to more responsible charities.
- Do not buy or commission a blockchain-based system (this is easy — you will save money too).
- Don't say: 'leveraging the power of blockchain' or other such marketing nonsense.
- Do say: 'how, exactly, does blockchain help?'

The views in this article are the views of the author and are his own personal views that should not be associated with any other individuals or organisations.