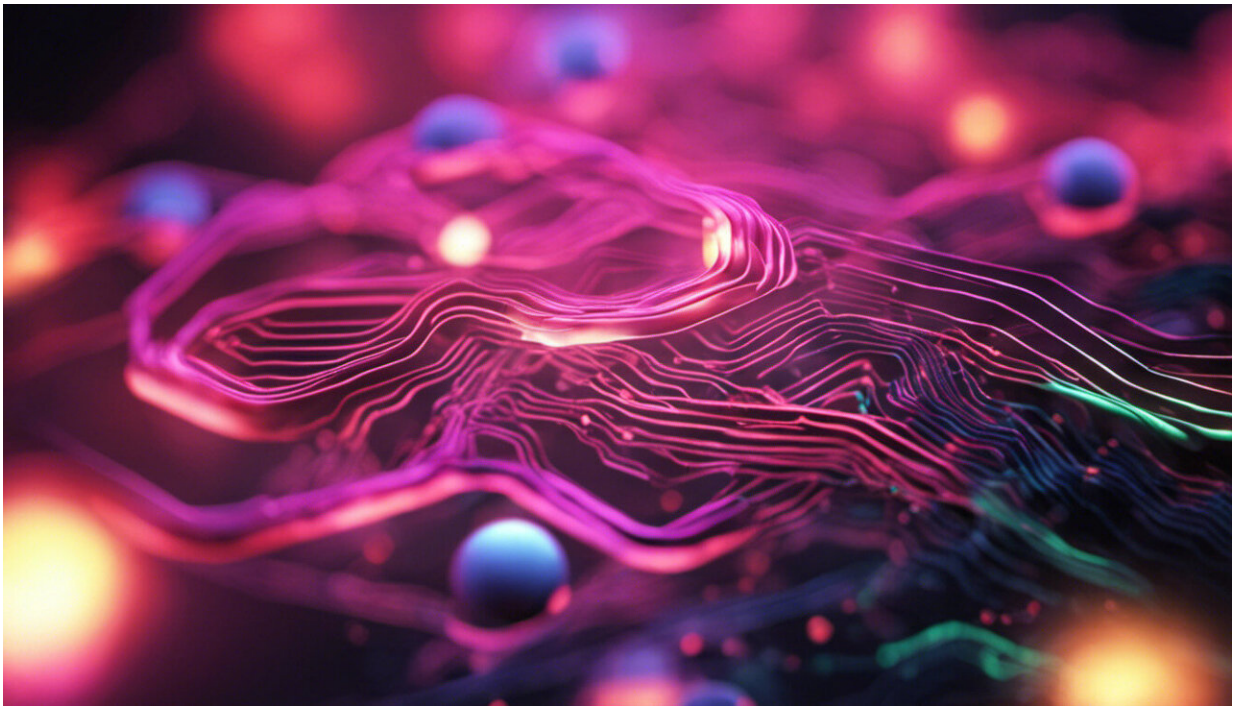
OPINION: Blockchain really only does one thing well

July 20 2016, by Stephen Wilson



Credit: AI-generated image (disclaimer)

No new technology since the dawn of the internet has captured the imagination like blockchain.

Designed to run unregulated electronic currency, the blockchain is promoted by many as having far broader potential in government,

identity, voting, corporate administration and healthcare, to name just some of the proposed use cases. But these grand designs misunderstand what blockchain actually does.

Blockchain is certainly important and valuable, as an inspiration for brand new internet protocols and infrastructure. But it's a lot like the Wright Brothers' Flyer, the first powered aeroplane. It's wondrous but impractical.

Not quite eight years ago, in November 2008, a mysterious and still unknown developer going by the pseudonym Satoshi Nakamoto launched bitcoin –- the first practical electronic cash that didn't rely on a digital reserve bank. A decentralised crypto-currency scheme requires global consensus on when someone spends a virtual coin, so she cannot spend it again. Blockchain's trick is to broadcast every single bitcoin transaction to the whole community, which then in effect votes on the order in which transactions appear. Any attempt to "double spend" (move the same bitcoin twice), or to introduce a counterfeit coin that hasn't been seen on the network before, is detected and rejected.

With no umpire, the continuous arbitration of blockchain entries requires a massive peer-to-peer network in order to resist distortion or manipulation.

Anyone at all is free to join the blockchain network, as a holder and spender of currency, and/or as a node contributing to the consensus process. The incentive to participate comes in the form of a random reward paid whenever the ledger is settled, which is roughly every 10 minutes. The odds of a node winning the reward go up with the amount of computing power it adds to the network, and so running a node is dubbed bitcoin "mining".

The only authoritative record of anyone's bitcoin balance is held on the

blockchain. Account holders operate a wallet application, which shows their balance and lets them spend it, moving bitcoin to other accounts. Counter-intuitively, these "wallets" hold no money; all they do is control account holders' private keys, and provide a user interface to what's in the blockchain.

In fact bitcoin is entirely ethereal, with not even virtual coins. The Blockchain only records the movement of bitcoin in and out of account holders' wallets, and calculates virtual balances as the difference between what's been spent and what's been paid.

The only way to spend your balance is to use your private key, to digitally sign an instruction to the network, specifying the amount to move, and the address (that is, the public key) of where to move it to. If a private key is lost or destroyed, then the balance associated with that key is frozen forever and can never be spent. Ever.

There has been a string of notorious mishaps where computers or disk drives holding bitcoin wallets have been lost, together with millions of dollars of value they controlled. And predictably, numerous pieces of malicious software have been developed specifically to steal bitcoin private keys and balances.

The enthusiasm for crypto-currency innovation has proven infectious; the feeling is that if blockchain "squared the circle" in payments, then it must have untold powers in other domains.

In particular, many commentators have promoted blockchain for identity management.

The conspicuous thing about proposals to put "identity on the blockchain" is that they overwhelmingly come from blockchain advocates and not identity management experts. What's missing in the

great majority of blockchain-for-identity proposals – and indeed in most of the non-payments use cases – is a careful statement of the problem and proper analysis of why distributed consensus is important.

What the blockchain can't do

Sadly, when you look closely, the blockchain just doesn't do what most people seem to think it does. There is nothing "on" the blockchain. All it holds is a record of bitcoin movements and associated metadata. The metaphor of recording anything "on" it belies the need for additional technologies and processes over and above blockchain, to decide how to represent physical items in code and to oversee the assignment of those codes. These necessitate extra key management, registration of ownership, and governance.

Blockchain does nothing about these realities, neither does any other distributed ledger technology that has followed in bitcoin's wake. Blockchain was expressly designed to manage crypto-currency without any key management or registration. No one is trusted in the naked bitcoin world. No administrator and no third party is needed to vouch for any wallet holder or network node. The lack of friction is great for the unbanked (as well as illicit users) and it also helps build the peer-to-peer network, which must be maintained at a huge scale in order to guard against those untrusted participants conspiring against the system.

And it's best to remember that the incentive to run blockchain nodes comes from the mining reward. Take bitcoin away from non-payment use cases and it's unclear who will pay for the infrastructure, and how. The original blockchain is not separable from bitcoin. Now, there is certainly plenty of fresh research and development being done on alternative consensus mechanisms and participation models. But nothing yet is up and running like the established public blockchain, and nothing else has yet been proven with blockchain's security properties.

Blockchain does just one thing: it establishes the order of entries in a distributed ledger, so as to prevent double spend without an umpire. The truth of the contents of the ledger is an entirely different matter. Blockchain doesn't magically make the entries themselves trustworthy, let alone the people that created them.

Despite the hype, blockchain is not a "trust protocol"; it's actually the opposite. Just think about it: it's not as though paying by bitcoin stops you from being ripped off. For anything of value other than bitcoin to be transacted via the blockchain requires additional layers of agents, third parties and auditors – things that just don't square with the trust-free architecture.

Lofty claims are made for blockchain's ability to decentralise all sorts of things. But in truth, blockchain only decentralises the adjudication of the order of entries in a ledger. It is not a general or native "Internet of Value" as claimed by authors like Don and Alex Tapscott. It was expressly designed for electronic cash; it has no *native* connection to real world assets.

Few businesses have escaped the call to evaluate blockchain technologies. If you've been persuaded to have a look, then as a first step, re-examine your security and record keeping needs. Take the time to understand what blockchain does, and all the things it leaves to be done by other systems. If your business is decentralised and your assets are purely digital, then blockchain has a lot to offer, but otherwise, it's just another database.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation