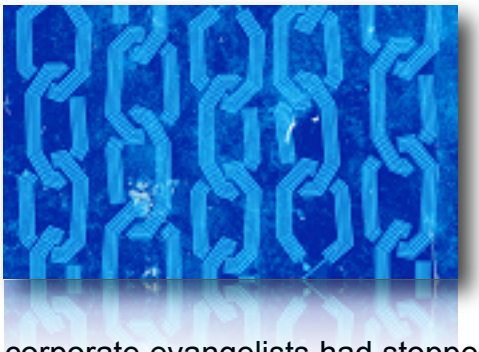
theguardian
Winner of the Pulitzer prize

Gian Volpicelli
Saturday 10 March 2018

Does blockchain offer hype or hope?

For many tech insiders, the most exciting thing about bitcoin is the thing that allows it to function: blockchain. What is it and what other uses might it have?



'The question many are asking now is whether there is much to blockchain apart from hype and speculation.' Illustration: Bryan Mayes

These days, bitcoin is front-page news, as its price's vertiginous ups and downs elicit glee and despondency by turns among investors. It was not always this way: the now-definitely-in-a-bubble cryptocurrency is making a comeback following years in which its association with crime and *darknet* drug markets kept it away from the spotlight. During that period, technologists and corporate evangelists had stopped touting the qualities of bitcoin, turning instead to a technology that underpinned the cryptocurrency without being tainted by dodgy connections: *blockchain*.

The blockchain was born as the digital scaffolding for cryptocurrency transactions. When devising bitcoin, pseudonymous inventor Satoshi Nakamoto's aim was to create a stateless virtual currency, not controlled by any bank or government.

But without any third-party acting as a guarantor, how could you ensure users did not cheat and spend their immaterial coins more than once? The solution was to entrust oversight to the whole network: all transactions are etched on a public log – the blockchain – maintained by a peer-to-peer swarm of computers (or *"nodes"*), each holding an identical copy of the ledger. When users spend their coins, nodes take note and update the ledger.

The decentralised structure ensures that there is no single point of failure, making it nearly impossible to hack the network, forge transactions, or freeze them for legal purposes.

Nakamoto added a further wrinkle to the system – *"mining"*: transactions are clustered in *"blocks"* and added to the ledger by powerful computers (*"miners"*), which earn the right to do so after solving mathematical puzzles through an electricity-consuming series of random attempts.

The narrative that started spreading at some point in 2013 was that blockchain technology should be decoupled from bitcoin, and used for more than exchanging digital currency. Cryptocurrency units could be inscribed with additional information and transformed into tokens representing anything from diamonds to title deeds; in this way blockchains could be repurposed as devices to verify property rights, or track products as they changed hands throughout the supply chain. Every sector could adopt a blockchain to move value or information among a multitude of parties, without the need for a mediator.

Blockchain would lead to efficiency, transparency and security.

Don Tapscott, an academic and businessman, and author of messianic book The Blockchain Revolution, has called blockchain technology "the trust protocol".

> "You don't need intermediaries to ensure parties will act with integrity, because the very platform you're transacting on does that for you," he says. "Trust is not achieved by middlemen but by cryptography, collaboration and clever code."

New blockchains emerged. Banks and financial institutions – bitcoin's original designated victims – started experimenting with their own private ledgers, in the hope that they could streamline the transfer of stocks and financial products.

It's never the first generation of a technology that delivers the hit, always the second – or the third

A blockchain called Ethereum came to dominate the open-source landscape: launched in 2015 by Russian-Canadian programmer Vitalik Buterin, it allowed developers to code and run "decentralised autonomous organisations" – applications selling their services in exchange for cryptocurrency, and self-managing themselves according to sets of automatically enforced rules dubbed "smart contracts".

Advocates recast blockchain as a tool for decentralising the internet itself. The Facebooks and Amazons of the future would be autonomous companies living on Ethereum, and they would store user information across the network, rather than in a data centre in Oregon – an arrangement that would make them less exposed to both cybercrime and government censorship.

That futuristic vision did not survive the appearance of the first decentralised autonomous organisations – unmanned venture capital fund the DAO was launched and immediately hacked in spring 2016. But that did not stop other, more conventional startups from popping up with the promise to crack one of the multiple problems with blockchain.

More recently, an Ethereum feature that allows anyone to mint and sell their own mini-currencies was bent into a crowdfunding tool: developers just had to float their idea for a blockchain venture and sell their tokens with the understanding that they would be of some use on a yet-to-be-built platform. Initial coin offerings (ICOs) were born, unleashing a speculative craze that would foreshadow the current bitcoin resurgence.

The question many are asking now is whether there is much to blockchain apart from hype and speculation. The technology is still too slow to be used on a large scale: Ethereum can only process about 15 transactions per second compared, for instance, to Visa's 2,000. Mining, the verification process that keeps blockchains trudging on, is a carbon-generating disgrace – Iceland uses more electricity for mining bitcoin than it does in powering its households. And some wonder what exactly a blockchain does, that a centralised tamper-proof digital ledger – a decade-old technology – does not.

> "I have seen no use cases for blockchain; there's nothing that a blockchain in particular brings to the party," says David Gerard, author of crypto-sceptic book Attack of the 50 Foot Blockchain. "The only use case I found for blockchain is cryptocurrency, and the only use for cryptocurrency is illicit transactions. And even for that, bitcoin is too slow."

Anarcho-libertarians of the Satoshi Nakamoto type might value blockchain for its imperviousness to state interference but Gerard sees no reason why conventional businesses should adopt one. Others think it is just a matter of waiting for the technology to mature. Jamie Burke, CEO and founder of the blockchain-focused fund Outlier Ventures, believes that, in the long run, blockchain could make several industries more automated, transparent and decentralised, and that the ICO model might allow teams behind open-source projects to make a profit. Current scaling hurdles are simply par for the course for a technology that is still in its late infancy.

“I don’t think any meaningful application will be built on the blockchain for at least two or three years,” he says. “But then again it’s never the first generation of a technology that delivers the blockbuster hit. It’s always the second, or the third. This is the reality of how technologies are adopted: the only difference is that with blockchain, this cycle is happening very publicly, because of the cryptocurrency hype.”

Linked in: alternative applications for blockchain

Catalan demonstrators in Barcelona, 2017. Photograph: Credit: Matthias Oesterle / Alamy Live News/Alamy Live News.

Voting

Funnily enough, one of the areas where blockchain technology could make the biggest impact has little to do with business, and much to do with politics: voting. Some think the ledger’s decentralised, tamper-proof nature make it safe enough to allow fraud-free online elections: voters would just get vote tokens and transfer them in order to signal their preference. The idea has already been proposed by Ethereum-powered nonprofit organisation Sovereign, and actually piloted and green-lighted in Estonia – although in the apolitical context of e-voting in corporate shareholder meetings. Even the European parliament devoted a short white paper to assessing blockchain-based electronic voting.

More recently, during a talk in Barcelona, bitcoin developer and anarchist firebrand Amir Taaki proposed using blockchain technology for rerunning the Catalan independence referendum online, a method which, he argued, would neutralise the repression of Spain’s central government.

Adding blockchain to the election process could change the way we think about voting, says Michael Mainelli, director of financial thinktank Z/Yen. For instance, he says, blockchain could allow for “continuous voting” – the casting of voting every week or month – and “transferable voting”.

> “The idea is that I have a vote but I don’t know enough about a topic, so I give my vote to someone who knows a lot about that, and let them make the choice,” Mainelli says. “Of course, this would also work in corporate governance.”

Supply chain

Scanning a tin of tuna using the Provenance app. Photograph: provenance.org

How to make sure that the shirt we are wearing was not manufactured using child labour, or that the jewel in our wedding ring is not a blood diamond? Tracking a product's history through the global supply chain is a tantalising task, given the multitude of parties involved. Some companies think blockchain technology could help make it easier. London-based Provenance, for instance, labels products such as fish or cotton with radio-frequency identification (RFID) tags that guarantee its ethical and safe sourcing; as the product changes hands, each step of its journey is automatically added to the blockchain; the end customer can then verify the object's origins through a mobile app. Provenance claims to work with over 100 businesses, including large brands such as Sainsbury's, and its architecture relies on Ethereum and Linux Foundation's blockchain Hyperledger. Still, founder Jessi Baker thinks that public blockchains

> "have a long way to go before they can be applied at scale".

To solve the problem, some of the logging is conducted without relying on a blockchain.

Another London-based company, Everledger, uses the blockchain to guarantee the provenance of diamonds: each stone is assigned a blockchain-based ID, which follows it from mine to jeweller, chronicling its history. This makes it possible to spot and root out diamonds whose provenance is unclear – which are often sourced in conflict zones. Over a million diamonds have gone through the Everledger treatment so far.

Finance and payments

A board at the Australian Securities Exchange, which now uses blockchain. Photograph: Bloomberg via Getty Images

The Australian Securities Exchange announced in December 2017 that it would start using a blockchain to keep track of shareholdings and carry out equity transactions. Its blockchain, though, is to be very different from bitcoin's or Ethereum's public ledger: it will be a private, invitation-only network, run by the exchange in compliance with law and regulation.

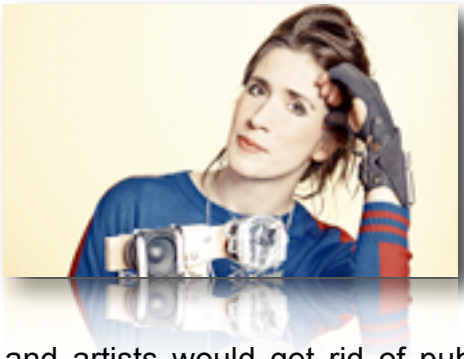
Although finance seems like an obvious field for applying blockchain technology, it is only partially so. In nearly all cases, big banks and financial institutions dabbling in blockchain have ditched the decentralised element and the mining mechanism, preferring – perhaps reasonably – to create a closed, private digital transaction record book.

Something similar happened when companies harnessed blockchain technology to power payments in real-world currency. Take Ripple, a payment system backed by several banks including Unicredit, UBS and Santander. Its open-source ledger is powered by tokens standing in for fiat money – which can be transferred cross-border in a cheaper and quicker fashion than remittances. Ripple's protocol does not use mining and is pretty centralised; it also allows for payments to be "frozen" for legal reasons.

> "Our mission is not to apply blockchain to payments, but to make payments better. We use blockchain only insofar as it provides benefits," says Ripple's chief technology officer Stefan Thomas. "Blockchain is going to solve trust problems in transactions, but it comes at

a cost: it's more expensive and harder to coordinate. And it's not always worth it: how often has your bank stolen money from you?"

Music



Singer-songwriter Imogen Heap, who wants to use blockchain to tackle royalties. Photograph: Phil Fisk for the Observer

British singer Imogen Heap has been at the forefront of an effort to improve the music industry through blockchain. The problem Heap set out to tackle in 2015, through her initiative Mycelia, was that of music royalties.

Heap's initial vision was one of total decentralisation: musicians and artists would get rid of publishers, producers and labels and get paid directly by consumers, through the blockchain.

Over the following three years, though, Mycelia's mission has shifted, and to less revolutionary aims. Today, it is working on promoting a "creative passport": a digital document containing a musician's personal information, professional biography, discography and background – or, as Mycelia head of research Carlotta De Ninni defines it,

> "a beacon of verified information".

These passports are to be stored on a decentralised tamper-proof blockchain and could incorporate smart-contract elements for quick direct payments.

> "Imogen, for instance, receives tens of emails every day from people who want to play her songs at weddings or other similar contexts; answering them all is tiring," Di Ninni says.

> "A smart contract included in a creative passport could specify the terms of use for some songs, and automatically authorise the use after payment."

The organisation plans to launch the creative passport later this year but has not decided on which blockchain platform the project is to run.