BIZCOMMUNITY

So you think you need a blockchain?

By Cayle Sharrock

5 Mar 2020

It's 2020, and we're still in hype overdrive about blockchain. If the conventional wisdom is to be believed, blockchain is going revolutionise and disrupt every industry known to humankind, but does every industry actually need a blockchain?

Cayle Sharrock is Head of Engineering at Tari Labs

Let’s take an objective look at two of the most aggressively touted use cases for blockchain to see if it’s all it’s cracked up to be.

Before we do this, let’s remind ourselves about the four pillars of blockchain technology and what they give you: tamper-evident logs (the blockchain); cryptographic proof of ownership (digital signatures); public accountability (the distributed public ledger); and corruption resistance (proof of work).

If we use these four features as a checklist, we can evaluate any proposed use case of blockchain technology and decide whether the potential is genuine, or whether it’s just buzzword bingo.

Banking

There have been hundreds of headlines over the past four years proclaiming how Bank Y will use blockchain to disrupt the industry. Usually, what they claim is that they can perform interbank settlements at a fraction of the cost of what the incumbent monopoly, SWIFT, provides.

So does blockchain work for the banking sector?

Clearly, tamper detection of the transaction history is a must-have here. What about digital signatures and proof of ownership? Without a doubt. Multiple signatures? The more the merrier.

Bitcoin was conceived as trustless money – and with banks, we have a fairly small community that is heavily regulated, and that do actually trust each other to some degree. Essentially, banks use governments' big stick instead of proof-of-work to keep everyone honest. This works most of the time. Except when it doesn't. The 2008 crisis and the 2012 Cypriot haircuts are just two examples.

How about Public Accountability from distributed public records? No, public accountability has never been the banking sector's strong suit. That means the banks' ideal "blockchain" is just tamper detection, plus digital signatures. This sounds like a bunch of databases that have tightly controlled access along with strong cryptographic signatures.

The banks actually gave this non-blockchain blockchain a name: Distributed Ledger Technology. And it's pretty much what SWIFT already does.

Verdict: Do banks need blockchain? Nah. They want a cheaper alternative to SWIFT.

Supply chain management

Blockchain technology is going to revolutionise the supply-chain management (SCM) industry, we're told. BHP Billiton was one of the first large companies to announce in 2016 that they were implementing blockchain for their core sample supply chain. We've heard similar stories about the diamond industry.

Whether you think a proof-of-work blockchain makes sense for SCM is really secondary to the challenge of The Oracle problem: blockchains are brilliant at letting you know when data in the system has been compromised. But they have zero sense whether that data is true or not.

The Oracle problem arises whenever you need to bring the concept of truth, or providence from the real world into a trustless system like blockchain. How does the core sample data get onto the blockchain ledger? Does a guy type it in? Does he never make mistakes? Can he be bribed to type in something else? If it's a totally automated system, can it fail? Be hacked?

Maybe we solve this by having two systems running and we compare the results. Or three. Or four. Now we have the problem of having to ship our samples to different labs around the world and be sure they weren't tampered with in transit. If only we had a blockchain-based SCM system to secure our blockchain-based SCM system ...

Verdict: The Oracle problem is really hard, and torpedos a lot of tangible good-based blockchain proposals.

So, back to our original question: do you need a blockchain? Ultimately, the future of blockchain applications (beyond money) lies in whether the benefits of having a decentralised, public record secured by proof-of-work outweighs its costs. There are plenty of really encouraging use cases emerging – think ticketing, for example, or trading in any digital assets. But for most industries, the jury's still out.

ABOUT THE AUTHOR

Cayle Sharrock is Head of Engineering at Tari Labs