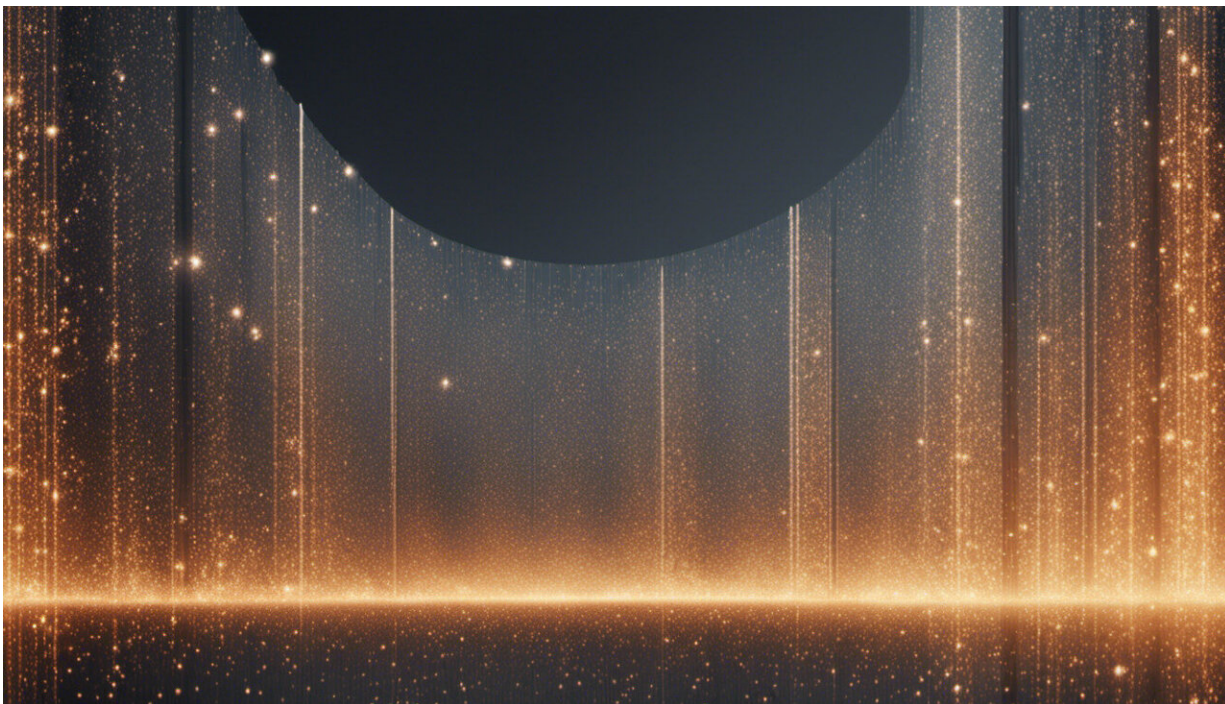# What's holding up the blockchain?

June 8 2017, by Philippa Ryan

Credit: AI-generated image ([disclaimer](#))

It's not technology or regulation holding back the blockchain—software that stores and transfers value or data across the internet—we just haven't figured out the next big use case. [Two reports](#) released this week by the CSIRO's Data61 not only inject some well-researched gravitas into the conversation, they also provide insight into why some of the major blockchain projects have stalled.

Since 2015, banks, regulators, tech giants and startups all over the world have raised billions of dollars to explore the blockchain.

But the only really successful, scaleable use of the blockchain remains cryptocurrencies like Bitcoin. Bitcoins currently trade at almost AU$4,000, with a total market equivalent to thirty times the GDP of Australia.

Think of the blockchain as a type of transparent spreadsheet or "public ledger". When someone transfers a Bitcoin, for example, the transaction is verified by "miners", encrypted and a "block" is added to the spreadsheet. Mining takes a lot of computing power, and so miners are incentivised to participate in the system with a reward of bitcoin.

It's finding a way to put all these pieces together for purposes other than cryptocurrencies that has yet to be figured out.

Because of all the computing power required to verify and encrypt new blocks, running a blockchain network is expensive and consumes a lot of electricity. For this reason, a blockchain should only be used if it solves particular problems. For example, a blockchain could allow users to see each other's ledgers and transactions, negating the need for a trusted third party to manage risk. The blockchain itself, through sophisticated cryptography, would provide privacy and trust.

Conversely, if there is already a central third party managing trust between users and verifying transactions (something banks already do for consumers), then a blockchain is probably not needed at all. Failing that, a sophisticated database or expert system would be a cheaper and simpler alternative.

Opportunities and risks

The [Data61 reports](#) describe some of the possible opportunities for the blockchain in Australia, including monitoring the outbreak of pests or animal and plant diseases, border surveillance, tracking intellectual property, and identity systems that provide greater certainty over entitlements, benefits, and tax obligations. The reports also identify some of the risks.

The risks include both business and technical risks. For example, public ledgers do not afford privacy and blockchains generally are not suitable for storing large volumes of [high speed data](#). Bitcoin's blockchain has been suffering from [this very problem](#) for more than a year. Finding a solution is a priority for any developers wanting to attract the number of users needed to make running a network profitable.

The use of blockchain in financial transactions also poses problems for compliance with [anti-money laundering legislation](#), which requires that anyone providing financial services (for example) must satisfy themselves as to the identity of their client or customer.

These shortcomings may explain why a number of high-profile blockchain projects have recently stalled. For example, last week, the Bank of Canada [announced](#) that its blockchain project, Jasper, is not yet fit to handle settlements. Citing transparency and privacy issues, the bank found that the benefits of using blockchain did not outweigh the risks.

But risk is not the only reason that blockchain projects are stalling.

In February 2017, the [R3CEV consortium](#) of banks and technologists announced after more than 18 months of investment, innovation, and testing, that they would not be using blockchain for their project because they did not need it.

Meanwhile, in a speech delivered to the Africa Blockchain Conference in March 2017, Andreas Antonopoulos warned that many recent "blockchain" projects are fraudulent attempts to raise capital under the guise of innovation and disruptive technologies.

The blockchain's holy grail

While bitcoin has proven what the blockchain can do, the technology still needs a killer app to justify the hype. The most likely contender is currently a "smart contract". Smart contracts are programmable transactions with complex internal logic that can interact with internet-enabled devices and other smart contracts.

At this time, the problem with smart contracts is that they are susceptible to manipulation. What is needed to test the capacity of the blockchain is a small-scale low-stakes low-risk smart contract that (for example) regulates energy consumption, manages permissions, or ensures payment on supply.

Data61's Smart Contracts Report lists some contenders, but first we need to manage the risk of fraud, breach of privacy, and blockchain bloat. Once these risks have been reduced to nil or negligible, the real work can resume.

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

Provided by The Conversation