Never one to let a bandwagon pass by, Greg Medcraft, the Chairman of the Australian Securities and Investments Commission (ASIC), has enthusiastically hopped onto the Blockchain wagon. Mr Medcraft has seen the light and recently proclaimed

Blockchain is an important technology development that has the potential to change fundamentally the world's capital markets

This is a hugely extravagant claim for what is a basic, if very elegant, piece of computer code. And Mr Medcraft is not alone. None other than Arthur Levitt the esteemed ex-Chairman of the Securities and Exchange Commission (SEC) has also been converted . And banks, such as Commbank
, have eagerly embraced this 'next big thing'.

It is about time for someone to critically examine this particular king's new clothes.

First, what Blockchain is not!

Blockchain is not about so-called cryptocurrencies, such as Bitcoin . Sure, the original Blockchain was the technology underlying Bitcoin but the debate on whether such unregulated currencies have a role in international finance is independent of the Blockchain concept. Blockchain has long since broken the shackles of Bitcoin and is ready to fly on its own.

Nor are the majority of the technologies underlying Blockchain particularly innovative. Concepts such as strong cryptography goes back to the work of Duffie and Hellman in the mid 1970s. Hashing, or compressing a piece of information into a short key that is hard to tamper with, was developed for the US National Security Agency (NSA) in the early 2000s and a similar concept has been used in the transmission of financial messages since the 1970s. Even the underlying technical problem of implementing distributed consensus has been solved since the 1980s.

What is unique about Blockchain is how data representing financial transactions is stored. Unlike conventional databases, data is not held in a single place, but as a so-called ‘distributed ledger’ where data is copied and replicated in many computers which, to quote Mr Medcraft, are not “controlled or owned by any single entity”.

Blockchain is the free-market’s Holy Grail. But like that golden chalice, the purported benefits of Blockchain are elusive.

In his ‘op-ed’ piece Mr Medcraft presented the arguments of the Blockchain spruikers. His assertions are however debatable.

First, the Holy Grail, “Blockchain automates trust and eliminates the need for ‘trusted’ intermediaries”.

Sounds noble but trusted intermediaries, such as stock exchanges and high value payments systems such as SWIFT, are widely used precisely because they are trusted and have been proven to be so for many years. Their track record of technology excellence and stability far exceeds that of the banks and firms vying to replace them. These intermediaries are trusted because they work and they work but they are single, focused and importantly well-regulated entities.

The proponents of Blockchain confuse ownership of a technology with its operations.

Organizations, such as SWIFT and settlement agencies, already operate a ‘distributed trust’ model. They are owned by their members and operated by a separate organisation that is highly transparent as to its policies, rules and operations. The multiple members (owners) do not have to keep a copy of every transaction to trust each other - all they need to do is, individually and collectively, ensure that the independent entity is operating within the agreed rules. It is a form of distributed trust that is efficient and proven to work.

Nor is a distributed trust model completely immune from corruption. For example, the mechanism for assigning credit ratings to securities prior to the GFC was a classical model of

distributed trust in that separate and distinct firms (S&P, Moody's and Fitch) were permitted to assign credit ratings independently. As the official commission into the GFC noted that "the credit rating agencies abysmally failed in their central mission to provide quality ratings on securities for the benefit of investors". The agencies had been corrupted by the incentives provided by external parties, the large investment banks that created the securities, who played one agency off against another to gain advantage.

Another example of distributed trust, which broke down spectacularly, was the recent FX benchmark manipulation scandal. There is no central authority in the global Forex market, yet rampant manipulation of the market went undetected for years. Unfortunately, the Blockchain model does not take into account systemic pressures that affect all of the parties in a particular market.

The second claim made by Blockchain spruikers, such as Mr Medcraft, is that of superior efficiency and speed. The speed argument is pure nonsense. The Blockchain mechanism has been set up *deliberately* to be hard to break, and even its proponents admit means that it is resource intensive and expensive. How can it be faster to interrogate multiple sources of data spread across multiple networks and computers than to retrieve data from one secure and trusted source? Luckily in the real world, the laws of physics and queuing theory still apply.

With an evangelical glint in his eye, Mr Medcraft argued that "when investors now buy and sell securities they generally rely on settlement and registration that takes several days to settle and even longer with cross-border deals. Blockchain can automate this whole process". Of course he should know better - and he probably does when not intoxicated by the technology.

Sure it takes too long to settle securities today but that is not because settlement notes are being sent by carrier pigeon. It is because, in order to settle real securities (as opposed to artificial Bitcoins) with real money, the exchange of information has to be standardised. Names and codes for securities, counter-parties and currencies all have to be agreed before the exchange will work. This is not a technical problem but one of hard work, analysis and communications that takes time. The fairy dust of Blockchain will never speed up this convoluted process.

One of the many fanciful claims made by spruikers of Blockchain is that the technology will result in massive cost savings. This thinking confuses systems with infrastructure. Blockchain is an infrastructure and has nothing to do with how the data it holds is processed. In order to

gain the efficiencies so longed for by Blockchain acolytes, not only do the standards mentioned above have to be developed and agreed but more importantly the computer systems that process the information have to be built. This involves enormous software development costs - far outweighing the costs of the underlying data storage technology.

Blockchain is like the mythical unicorn that appears to give its free-market adherents a vision of a perfect world where economic agents can interact directly with one another freely and without friction. In the real world, building robust financial technology is hard and panaceas, such as Blockchain, thankfully come and go at regular intervals.

Blockchain is an elegant solution to a very specific problem, albeit one that protects the identities of potential drug runners, tax dodgers and money launderers (who incidentally ASIC should be trying to unmask). Its inherent performance limitations means that the technology does not have a meaningful part to play in the trillion dollar, million transactions per day world of real finance.

After the long holidays, Mr Medcraft should concentrate in clearing out the in-tray of issues that has built up in recent years for ASIC, such as completing ongoing investigations into financial benchmark manipulation , rather than chasing technology unicorns.

Read more http://theconversation.com/blockchain-a-regulatory-unicorn-52673