

## THE AUSTRALIAN

---

### Contracts without arbiters: too far?



Bird & Bird law firm partner Hamish Fraser.

HAMISH FRASER THE AUSTRALIAN 12:00AM November 25, 2016

As a society, we place many things in the hands of trusted authorities and it's not always appropriate, or even possible, to remove them. We trust our government. We trust our courts. We trust our GP.

Take the example of the court system. We give courts the power to order that, if something is wrong, it should be undone.

A contract can be undone by the stroke of a judge's pen — the Latin term *void ab initio* is taught in Contracts 101 in all university law degrees. And this is an important societal concept.

There are times when a contract must be undone, for example when it was entered into as the result of misleading representation before the contract was created or a fraud or a mistake.

Facts are rarely cut-and-dried and many cases will see conflicting evidence of the facts.

When these things happen, our courts have no difficulty saying a contract is void or something is wrong. And nor should they.

In a world of smart contracts using a technology known as blockchain what does this mean?

The blockchain contract self-executes. Blockchain is a means to authenticate something (in the case of Bitcoin it authenticates money) without the need for a trusted third party.

Because the blockchain is a public ledger it can be verified across all other copies of it to confirm its truth.

In addition, and importantly, a blockchain transaction is irreversible. Each transaction once complete must, by definition, be absolute as there is no trusted authority to turn to if things go wrong.

The significance of this absence of a trusted authority should not be underestimated or overlooked.

It certainly stands to revolutionise many things we do; disruption to be sure, but are there times when we need that trusted authority?

It makes no sense for a blockchain contract to be void — because, since it self-executes, no human is needed — and there is no room for disputed facts.

What is more, the blockchains attached to the contract will still exist and be able to be verified: so how do we undo the verification of a public register when the whole system depends on it being a verifiable public register?

At the very least, these matters need to be thought through carefully and we need to recognise that perhaps some things — things that are not easily reversed — are not suited to a blockchain. Perhaps we value having that trusted third party in some situations.

When it's just money, it's perhaps more manageable — although if it's a lot of money, it might create a different problem). Money is fungible; if I wrongfully gain \$100 from you, I can give you back \$100 — it doesn't need to be the same note.

However, what about shares?

Shares are different to money. If I hold, or perhaps held, share No. 562 and for whatever reason a court says I do not, what happens then?

If I still hold it, I can transfer it back to whomever it belongs. But what if it never should have been issued, or someone else owns it?

The blockchain attached to that share, verifiable on the public register, shows that share No. 562 is still out there and verified.

The Australian Securities & Investments Commission and the Australian Securities Exchange are trusted third parties that verify transactions. In the blockchain era who will protect investors' interests?

Trust and trusted parties are an important part of our social contract. Blockchain is a fascinating and revolutionary way to sidestep the need for trust in every situation, but it is perhaps not the perennial panacea.

*Hamish Fraser is a partner and head of Australian Technology and Communications practice of international law firm Bird & Bird.*

