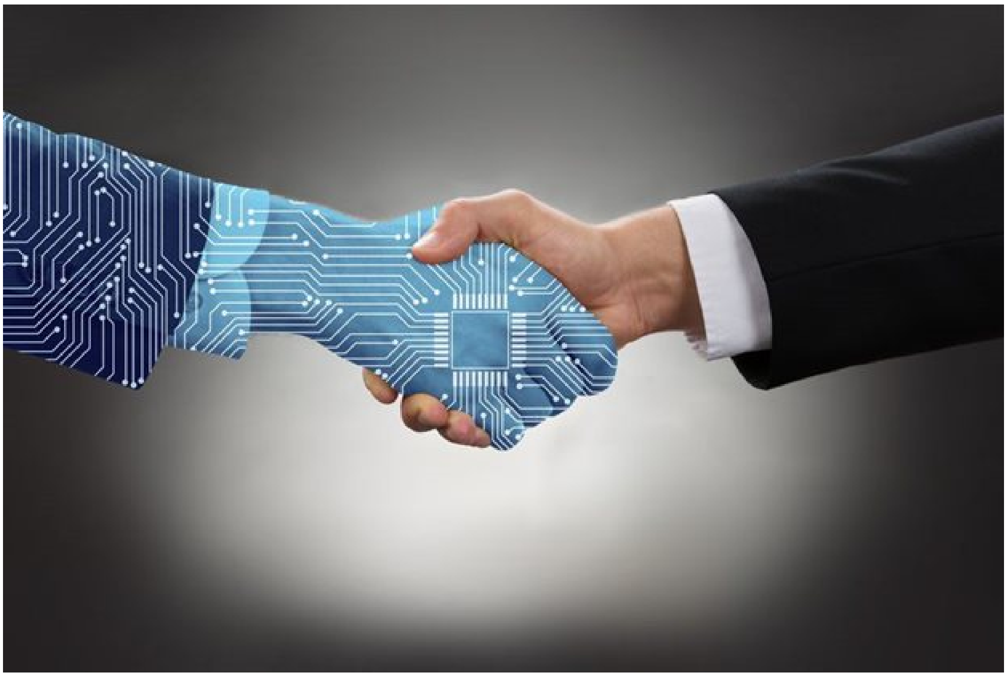
BIZCOMMUNITY

# Smart contracts adoption could be tripped up by legal validity and privacy laws concerns

By Wendy Tembedza

28 Oct 2020

Covid-19 forced businesses to accelerate the rate at which they adopt and adapt to technological change. Many businesses are looking to conclude agreements by taking advantage of technology platforms that promise efficiency and cost-savings; including using smart contracts. Although the opportunities for smart contracts are vast - issues related to their legal validity and compatibility with growing data protection laws may create real stumbling blocks for their use.



© Andriy Popov – 123RF.com

Smart contracts have continued uncertainty regarding their enforceability. Within the context of data protection, questions arise as to whether smart contracts are compatible with privacy laws. However, in the context of the fourth industrial revolution, we need to acknowledge the interplay between technology and the law and identify ways to facilitate it.

Any legal discussion related to smart contracts must be operationally contextualised. Smart contracts operate on distributed ledger technology (DLT) that allows users to create a database or record of information that is distributed among the users on the network and is subject to shared management by the users. DLT facilitates the secure recording, validation and sharing of data. Smart contracts benefit from a specific implementation of DLT made famous by Bitcoin, being the blockchain. In the blockchain, the unique software and data structure provides increased security controls for data through encryption and hashing technology. The immutable nature of blockchain also means that any transaction recorded in a smart contract is guaranteed to be concluded and can be easily traced. Transparency as a result of the distributed nature of the blockchain also means that parties to a smart contract are held accountable for performance.

Although smart contracts provide great benefits for contracting parties, the novel way in which they are created and recorded (being a contract in software form), raises questions about their enforceability in the traditional contracting world. The ability of parties to enforce smart contracts will impact on the rate of their adoption. Developments in other jurisdictions, set out below, suggest that there may well be a future where smart contracts form part of the contracting lexicon in South Africa.

On 18 November 2019, the UK Jurisdiction Task Force issued a legal statement on the legal status of crypto assets and smart contracts, finding that:

- the nature of smart contracts does not preclude them from recognition under English law and
- smart contracts can have legal force – as they possess, albeit in a unique form, the characteristics of traditional contracts and can be interpreted, subject to some adjustment, by the same means used to interpret traditional contracts.

Although the statement of the Task Force is not binding legal authority, given that the UK and South Africa are both based on the common law system of law, the prevailing approach in the UK may be a harbinger for the position which could be taken in South Africa on the contractual validity of smart contracts.

## Legal issues

In addition, the International Swaps and Derivatives Association, Inc. (ISDA) recently published four whitepapers analysing the legal issues associated with using "smart derivatives contracts" from a French, Irish, Japanese and New York law perspective. Although these white papers do not delve into the enforceability of smart contracts (this has been examined in previous guidelines published by ISDA); they do examine issues related to how to determine which law governs the smart contract and which jurisdiction applies in the event of a dispute arising from the smart contract. These issues become prevalent when derivatives are traded on a cross-border basis.

Wendy Tembedza

Although these developments suggest that there may well be a future for smart contracts in South African law - when assessing the use-case for smart contracts, the requirements of privacy laws must be considered. Due to the nature of their creation and existence, smart contracts have a multitude of use-cases, including the ability of smart contracts to facilitate the storage of vast amounts of data and personal information. Following from this, the question to ask is whether smart contracts are compatible with data protection laws.

## SA data protection laws

In South Africa, the President announced that the majority of the remaining provisions of the Protection of Personal Information Act, 2013 (POPIA) came into effect on 1 July 2020. This means that, subject to the compliance grace period ending on 31 June 2021, responsible parties will be required to comply with the eight conditions of lawful processing set out in POPIA, which are aimed at protecting data subject's personal information by establishing minimum thresholds for the processing of personal information. Some of these conditions raise issues in relation to the use of smart contracts. The conditions that pose potential difficulties are set out below:

**Condition 1 - Lawfulness:** POPIA requires that the responsible party ensure that the conditions for lawful processing are complied with, both at the time of determining the purpose and means of processing the personal information, and during the actual processing. This means that the responsible party must play an oversight role in observing the personal information processing activities to ensure compliance with the eight conditions. Given that smart contracts do not rely on one central authority to store information, and that everyone on the network has the exact same copy of the data, the question arises as to who is the responsible party in this context. Potentially, all parties on the network can be considered responsible parties, however, this makes the enforcement of any rights under POPIA by a data subject particularly difficult given that a network could consist of hundreds (if not more) of users.

**Condition 3 - Purpose specification:** POPIA states that personal information must not be retained for longer than is necessary for achieving the purpose for which it was collected, unless such retention can be justified under POPIA. The immutable nature of smart contracts means that once the contract has been created, it cannot, save with some extreme intervention, be amended or deleted. It is difficult to see how smart contracts can be reconciled with POPIA in respect of the requirement that any continued retention of personal information must be justifiable. It remains to be seen whether this has the effect of reducing the use-cases for smart contracts and in fact precludes their use in relation to, for example, storage of large volumes of personal information by landlords.

**Condition 5 - Information quality:** POPIA requires responsible parties to ensure that they maintain accurate records of personal information. This means updating personal information where necessary. Due to the immutable nature of smart contracts and the difficulty in amending them, a responsible party be would not be able to maintain accurate records within a smart contract given that information that is stored cannot be changed. Most likely, a new smart contract would have to be created with the corrected information included. The practicalities of this may not be worth the potential time required to ensure up-to-date records in some instances.

## ABOUT THE AUTHOR

Wendy Tembedza, Senior Associate at Webber Wentzel