Transforming Public Procurement Contracts Into Smart Contracts

Pauline Debono, Malta Information Technology Agency, Malta

ABSTRACT

The terms governing the provision of supplies, services, or works by an economic operator to a governmental entity are set into a public contract that is signed, following a procurement process. This article explores whether the public administration can utilise smart contracts to incorporate the terms governing the provision of supplies, services, or works. The fundamental elements of a contract are assessed, in order to determine whether a smart contract can be considered as fulfilling these requirements. Following this assessment, the main hurdles to the use of smart contracting are examined and a possible solution proposed. The case for utilising smart contracting within the realm of public procurement is finally advocated.

KEYWORDS
Economic Operator, Elements of Contract, Public Procurement, Smart Contracts

INTRODUCTION

Over the past months, the debate on smart contracts has gathered momentum, as attention on the use of smart contracts has increased globally. The definition of smart contracts which is most often considered is that Nick Szabo (1996) has created: “A set of promises, including protocols within which the parties perform on the other promises. The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics, thus these contracts are “smarter” than their paper-based ancestors. No use of artificial intelligence is implied.” Norton Rose Fulbright (NRF) and R3 (2016b) list the characteristics of smart contracts as follows:

- **Digital form**: Code, data and running programs;
- **Embedded**: Contractual provisions are embedded as computer code in software;
- **Performance**: Mediated by technological means;
- **Irrevocable**: Once initiated, the outcomes for which a smart contract is encoded to perform cannot typically be stopped (unless an outcome depends on an unmet condition).

As with other technological innovations, the pace of the legal debate on the nature of smart contracts is relatively slower, compared to the more popular assertions on the economic benefits of smart contracts. As enthusiasts project smart contracts as the ultimate solution to the bureaucratic
web which has been created by a state’s administration, the legal profession threads carefully, in view of the inevitable impact that regulatory or judicial intervention can have on the development path of innovation (Adair, 2017; Werbach & Cornell, 2017).

The enthusiasts’ proclamation that smart contracts will do away with both regulators and lawyers, together with the legal structures that support all human relationships, is very difficult to sustain. The capture of the legal system will be inevitable, as the operation of smart contracts requires either clarification, due to misunderstandings, or the resolution of disputes in human relationships. Although smart contracts are the currently most advanced stage of electronic contracting, the action underlying the smart contract is incepted by a human, the code is also written by a human, and humans are susceptible to misunderstandings and mistakes. Ultimately, it is human to err.

Considering that smart contracts will not be immune to government and court intervention, the counter proposal can be worth investigating – what if the government itself makes use of smart contracts in its administration of the state? Contracting by governments is a complex and sensitive subject in view of the fact that the majority of elected representatives have the power to utilise public money for state administration. Mishandling of public money is often the outcry of corrupt practices. Moreover, it is a well-known fact that public procurement is a key component of the global economy. The Public Procurement Directive 2014/24/EU (European Parliament and Council, 2014a), regulating public procurement within the European Union (EU), was intensely negotiated by Member States representatives in view of its inevitable impact on the recovery of the states from the late 2008 economic crisis.

For these reasons, public procurement is often put under the magnifying lens. A myriad of regulations and processes try to ensure that government achieves the best value for money, whilst at the same time applying fair competition and transparency between the participants in the process. The process for the selection of the economic operator until the final award of the public contract is governed by financial administration rules. The subsequent signature and execution of the public contract is regulated by the national contract law. Whereas it is not foreseen that smart contracts will impact the public procurement process leading to the selection of the economic operator, it is the objective of this article to consider whether public contracts, in their whole or part, can be transformed into smart contracts. Can the cost savings and efficiency gains which are often attributed to smart contracts be utilised to the advantage of both government, suppliers and ultimately the citizen within the context of public procurement?

A recently published report by IBM (2017) considers the counter façade of government’s involvement in distributed ledger technology (DLT). The report hits the nail on the very issue which the author identified above and which is at the heart of public procurement – transparency. In the words of the Institute: “To build trust, most government organizations strive to be as open, transparent and collaborative as possible. Too often, they fall short of their own ambitions. Blockchain, the technology underlying distributed ledgers, offers a new approach to transparency and collaboration” (p.2).

Various governments already adopt some form of electronic contracting and cryptography. Although the Maltese government does not utilise electronic contracting yet to process its public contracts, it has adopted an electronic identity card which is based on a system of public and private keys. Cryptography is also an enabler, once distributed ledgers use hashing, digital signing, and other cryptographic techniques to identify participants, to find consensus between their views of facts, and to lock consensus into records for the permanent log (R3 and Norton Rose Fullbright, 2016b). However, the main difference will lie in the fact that trust will not depend on a single certification authority that is entrusted with the issue and processing of the digital certifications, but it will depend on the distributed ledger. Adopting smart contracts will be the leap forward, as smart contracts are seen as representing the fusion of these two lines of technological development: electronic contracting and cryptography (Werbach & Cornell, 2017).
Related Content

Challenges in Modelling Healthcare Services: A Study Case of Information Architecture Perspectives
www.igi-global.com/chapter/challenges-in-modelling-healthcare-services/135759?camid=4v1a

The Software Engineering Discipline
www.igi-global.com/chapter/software-engineering-discipline/28179?camid=4v1a
Information Architecture: Case Study
Cláudio Roberto Magalhães Pessoa, Monica Nassif Erichsen, Renata Maria Abranches Baracho and George Leal Jamil (2016). Handbook of Research on Information Architecture and Management in Modern Organizations (pp. 424-438). www.igi-global.com/chapter/information-architecture/135779?camid=4v1a

Topic Effects on Process Gains and Losses in Electronic Meetings