International Journal of Information Technology Project Management
Volume 10 • Issue 2 • April-June 2019

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

DOI: 10.4018/IJITPM.2019040103

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

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[1]. Ultimately, it is human to err[2].

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[3] 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).

THE CONTRACTUAL NATURE OF PUBLIC CONTRACTS AND SMART CONTRACTS

In the first part of this article, the contractual nature of both the smart contract and the public contract will be assessed. There is no doubt that public contracts form part of the contractual realm, but doubt has been cast as to whether smart contracts can be considered as a contract.

The most basic principle on which the national contract law is built is the freedom to contract. The authority of the law is placed in the will of the parties – a person is bound because s/he wants to be bound. The principle is entrenched in Article 992(1) of the Civil Code (Chapter 16 of the Laws of Malta). Contract law lists the specific elements that need to be adhered to for the state to recognise the contract as valid and for a court to confirm its execution. According to Article 966 of the Civil Code (Chapter 16 of the Laws of Malta).

The following are the conditions essential to the validity of a contract:

1. Capacity of the parties to contract;
2. The consent of the party who binds himself;
3. A certain thing which constitutes the subject-matter of the contract;
4. A lawful consideration.

As the Court of Appeal (Superior Courts of Malta) (2014) explained in its judgement to the case between Victoria Sciberras and Sr Adelaide Gauci noe et, if the contract satisfies these requirements, it cannot be declared null or without effect, since this contract reflects the parties' legitimate will and the parties' will is supreme, according to the rules of interpretation Article 1002 and sequitur of the Civil Code set out. Two elements need to be examined in further detail to confirm the case for a public contract to be transformed into a smart contract.

Capacity

An individual must (i) have the natural capacity to contract, which depends on the use of reason and the age of the individual, and (ii) not be inhibited from contracting due to a legal prohibition. In relation to smart contracting, Article 973 of the Civil Code (Chapter 16 of the Laws of Malta)[4] may prove critical. Pursuant to this provision of the law, it is only the invalid individual who can annul a contract on the ground of his/her own incapacity. The same ground cannot be put forward by the other contracting party.

Werbach and Cornell (2017) raise an interesting point in relation to the requirement of capacity of the parties in a smart contract. They note that the parties to a smart contract at a technical level are not individuals, but cryptographic private keys. The private key is assumed to represent the individual, based on a mathematical relationship with the associated public key. The fact that one requires the private key to generate a valid digital signature against a given public key is the basis of electronic identity systems. However, the authors note major issues when adopting these concepts to smart contracts: (a) Even if a key uniquely belongs to an individual, the two are not the same; (b) an individual may possess different digital identities which are backed by different private keys; (c) the key may designate a persistent digital identity hiding the real individual (pseudonymity) or no information at all (anonymity) (Werbach & Cornell, 2017). The author dares add that other issues might arise in relation to the public key infrastructure operating the digital identity. For example, in the event that the revocation system of the public key infrastructure does not function properly, then the trust in the identity of both the physical individual and technical counterpart (the private key) is inevitably shattered. This issue will probably be fully addressed through appropriate legal intervention[5] in the same manner as the legal recognition of digital certificates that have been given legal equivalence to handwritten signatures through legislation.

Consent

The Maltese Civil Code does not have a specific definition of consent. Through the work of jurists and jurisprudence, the elements that need to coexist for consent to be confirmed are the following:

1. There is no defect to the consent and there is identity between the two consents, in order for the two consents to meet.

Werbach and Cornell (2017) assess this requirement when they examine the problem that might arise when the intentions of the parties are not the same when executing a smart contract. They use the example of a smart contract regulating the delivery of cotton by a ship named Peerless, where more than one ship has the name Peerless. If the name of the ship is not adequately described in a traditional contract, error can be claimed as a vice of consent leading to the unenforceability of the contract being declared by the court. The smart contract will, however, be executed with the possibility of having an executable smart contract that does not satisfy the legal conditions for mutual consent.

The International Swaps and Derivatives Association (ISDA) (2017) raised an important question in this regard: "How do I know the code as written in the contract reflects my intentions if I cannot read it?" (p.16). They note that the code might not be as readily understandable to an average reader as natural human language. Although one resolution is for the lawyer to have learnt the relevant language used to write the code, smart contracts seem to inevitably require the effort of the legal and technical persons of both contracting parties[6]. However, this solution does not do much to reduce the current administrative costs relative to contract drafting. From a technical perspective, Alharby and Van Moorsel (2017) identified three solutions in an attempt to write correct smart contracts: (i) Semi-automation of the contracts by translating human-readable contract representations to smart contract rules; (ii) provide developers with guidelines to aid them write correct smart contracts; or (iii) the adoption of formal verification techniques to detect unintended behaviours of smart contracts.

2. There is both an offer and acceptance.

A public contract is a perfect example of the second scenario. Following a public call, interested parties submit their offers to the call. The offers are evaluated by the contracting authority, which then awards the contract based on the published award criteria. The public call on its own does not create a contractual arrangement; the contract that ensues between the contracting authority and the tenderer following a final award constitutes the fully-fledged contract.

3. Consent is manifested externally.

In relation to the external manifestation of consent, national law generally recognises three vehicles that can be utilised to contain the four elements that create a contract: public deed, private writing, or verbal arrangement. Public contracts normally take the form of private writings – a signed document between the contracting authority and the economic operator. Other vehicles have been investigated by the court including technical vehicles which emanate from the legal framework resulting from the European digital agenda.

Directive 2000/31/EC (European Parliament and Council, 2000) and Directive 1999/93/EC (European Parliament and Council, 1999)[7] formed part of the digital agenda propelled by the EU[8]. They have led to important legal inroads, such as:

1. Article 9(1) of Directive 2000/31/EC requires that the legal requirements which are applicable to the contractual process neither create obstacles for the use of electronic contracts nor result

in such contracts being deprived of legal effectiveness and validity on account of having been made by electronic means;

2. Article 5(1) of Directive 1999/93/EC requires that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
    a. Satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data;
    b. Are admissible as evidence in legal proceedings.

This legal framework acted as an enabler for the conclusion of contracts utilising electronic means. The electronic communication does not create the contractual arrangement per se, but specific aspects of the contract are transformed into electronic data, as in the case of the electronic signature. The innovative aspect of smart contracts is the fact that the electronic data constitute the contract itself.

Werbach and Cornell (2017) contend that nothing prevents an expression of mutual assent from being formulated in code, once mutual assent can take such a variety of forms. Von Haller Gronbaek (2016) observes that the contract law principles are so fundamental that “it would be counterproductive if these could be circumvented alone by subjecting to the fait accompli of a fully automated and self-enforcing smart contract” (p.4). However, similarly to the legal initiatives which are taken in relation to electronic contracting and signatures, legal certainty might require regulatory provisions to be in place to clarify the contractual issues the author identified above and which are specific to smart contract[9].

SMART PUBLIC CONTRACTS?

The objective of this second part of the article is to assess the barriers that exist for a public contract to be transformed into a smart contract and possible resolutions.

The subject-matter of public contracts can be complex and they may include terms such as “best effort,” “best endeavours,” and “commercially reasonable endeavours”, resulting from possible negotiations between the contracting parties. Lim et al., (2016) note, while a smart contract may contain some part of the “database of obligations” between the parties in its instructions, it is unlikely to be a comprehensive catalogue of all obligations, particularly where these are complex since:

1. The terms are not capable of being assessed deterministically by a computer program (not capable of Boolean expression and an algorithmic determination, but instead requiring human judgement);
2. In order to be sufficiently expressive, obligations may import indeterminate concepts of reasonableness or appropriateness that again are not suited to algorithmic determination;
3. The expression of an obligation in code may not accurately reflect the agreement between the parties (for example because of error or omission); and
4. The contract may itself contain a further agreement to agree, or a mechanism for amending the contract which is not in itself algorithmically deterministic (p.3).

This last point is particularly relevant for public contracts. A public contract that includes an implementation plan for the economic operator to follow may be subject to more elaborate clauses that provide for the possibility of a correction plan in the event of a default by either party.

One proposal Lim et al. (2016) put forward is to split the current agreements into two, by automating those contractual provisions that are suited to algorithmic determination and retaining the traditional contract for those terms that are not suitable for execution through a smart contract. Another recommendation is for the traditional contract to incorporate the smart contract code by reference into the contract, but the former should take priority over the code, in case of conflict. They also suggest a legal counter-part to the hard fork action taken by the blockchain community:

> *A "fail-safe" in the smart contract code that allows the code to be terminated in certain agreed scenarios by any party to the contract (e.g., by trusted authorities with multi-signatory keys). Consequences of the use of the "fail-safe" (whether appropriate or not) would be resolved by the parties, in accordance with the legal wrapper and within the framework of the law. The "fail-safe" could also allow parties to amend the smart contract code, when there is a contract variation or where a party chooses to waive certain rights under the contract. (p.5)*

R3 and NRF (R3 and Norton Rose Fullbright, 2016b) also mention this option. They refer to the "split contracting model" whereby "non-human performance is encoded into computer code, and wider human obligations, remedial and other provisions are written into natural language, the two components operating together as a cohesive contract." (p.13)[10]

In another paper, NRF (Norton Rose Fullbright, 2016a) note:

> *There may already be technical solutions to work around this problem. For example, where the exercise of discretion (or a decision of some kind) is required of one of the participants to a smart contract, it could be accommodated by building in a mechanism to halt performance of the smart contract temporarily while input from the participant (or a third party empowered to verify a state of affairs) is sought. To build in such a dependency: (a) runs the risk of undermining a key virtue of a smart contract: lack of dependency on a participant / third party agency; and (b) means that the parties can no longer be certain that an event (for example, the release of payment) will happen on an irrevocable basis once the smart contract is put in place. (p. 12)*

Three matters require attention, when considering public contracts as a potential candidate to be transformed into a smart contract:

1. The type of distributed ledger that may be utilised by governments for this purpose;
2. The handling of contract modifications;
3. The resolution of disputes.

DISTRIBUTED LEDGER TECHNOLOGY

R3 and NRF (2016b) identify three forms of DLT that are currently available:

1. Permissionless DLTs allow anyone to freely download the software, submit messages for processing and/or be involved in the process of authentication, verification, and reaching consensus. This is the main principle of blockchain technology - achieving consensus over a set of shared facts through the community without any dependency on the authority of a single entity;
2. Permissioned (private) DLTs allow participants to be preselected or subject to conditional entry on satisfaction of certain requirements or on approval by an administrator of the DLT. In fact, such DLTs provide for agreement on the facts of each transaction to be reached "by decision of a single trusted third party or designated administrator or a consensus of distributed shared and voting "notary servers" built for just that purpose" (Norton Rose Fullbright and R3, 2016b, p. 9). In such instance, governments may have the option to create an independent authority to act as an administrator for its smart contracts;

3. Hybrid DLTs allow for different variables to be applied from the previous DLTs, such as the degree of centralisation that those responsible for setting up a distributed ledger wish to achieve. One specific example provided is for a permissionless DLT having encryption of transactions and supported with a strong identity framework (Norton Rose Fullbright and R3, 2016b).

Even in relation to DLTs, identity will play a crucial role and, as the author explained above, it will be important for the validity of smart contracts in order to establish the basic element of consent. Although electronic identity has gone through an overhaul through the EIDAS Regulation, DLTs will offer new challenges to the legal provisions which have been agreed so recently (International Swaps and Derivatives Association, 2017).

Confidentiality of data and the protection of personal data will be key aspects that need to be considered when contracting authorities choose the type of DLT for their smart public contracts. A number of public contracts can easily pass the confidentiality test, since most of the information included in the public contract is already publicly available through the tender document and the award notice, besides meeting the test of greater transparency in public procurement. Companies submitting confidential technical information as part of their offer would prefer a permissioned DLT. The same reasoning applies to the protection of personal data. Europe has stringent legal requirements on the processing of personal data which are coded in the General Data Protection Regulation (European Parliament and Council, 2016) and the increased rights given to data subject, in particular the right for rectification and the right to stop and erase data processing, must be implemented within DLTs. Alharby and Van Moorsel (2017) point out the two main privacy issues they encountered: The lack of transactional privacy, considering that all transactions and users' balances are publicly available to view, and the lack of data feeds privacy once requests for data feeds from a third party are exposed to the public on the blockchain[11]. Von Haller Gronbaek (2016) confirms that, if a blockchain database holds personal data in clear text, this information will be copied on all distributed copies of the ledger to all nodes. He questions: Who are these nodes? Who are data controllers and data processors?

Contract Modifications

Complementing the first provision of Article 992 of the Civil Code (Chapter 16 of the Laws of Malta) is its second provision: Contracts "may only be revoked by mutual consent of the parties, or on grounds allowed by law". Freedom to contract implies that the contracting parties are free to amend the terms of the contract. In relation to this right, both public and smart contracts raise exceptions. Variations to public contracts need to be handled in a special manner in view that the ensuing contract between the contracting authority and the economic operator is the result of a public call. The requirements of the public call and the price against which the contract is being awarded are published to enable any interested party to appeal the decisions the contracting authority is taking and hence ensure transparency in the process.

Transparency would be circumvented, if the contracting authority was allowed to make unauthorised or illegal modifications following the publication of the original award price. As a result, variations to public contracts are regulated in detail by the procurement regulations. Once again, smart contracts will not really impact the modifications rules, but any contractual modifications must be clearly documented to ensure traceability for auditing purposes.

Although a smart contract is immediately executable, a number of authors point to the possibility and the importance of including code within the smart contract that enables modifications to the smart contract. Lim et al. (2016) emphasise:

> *A smart contract…. must also be amenable to rectifications where it no longer satisfies the requirements of law or fails to reflect the obligations agreed by the contracting parties. Where a smart contract is designed in a way that cannot achieve this, it may result in misalignment between rights recognised by law and rights recognised by the public. (p. 4)*

One possible solution would be incorporating the modification in a separate smart contract in the form of an addendum to the first smart contract.

Gauci (2017) proposes another solution: the use of oracles. Oracles are trusted third parties, such as courts, authorities, or other entities that can determine real-life instances, variables, laws, and conditions into the smart contracts to cater for a flexible and lawful outcome[12]. One instances would be allowing court to stop a transaction in certain instances or to enforce precautionary measures (Gauci, 2017).

Resolution of Disputes

According to Werbach and Cornell (2017):

> *Smart contracts will not replace contract law. Contract law is a remedial institution. Its aim is not to ensure performance ex ante but to adjudicate grievances that may arise ex post. Smart contracts bring into sharper relief this core function of contract law. They eliminate the act of remediation by admitting no possibility of breach. The needs that give rise to contract law do not however disappear. (p. 4)*

Any disputes arising in relation to a public contract are regulated through its dispute resolution provisions. The standard position of the government of Malta in relation to the resolution of disputes arising from its public contracts requires the reference of the dispute to the Courts of Malta, unless the parties agree to refer the matter to the Malta Arbitration Centre.

As against public contracts, which have a long-standing tradition of dispute resolution, the executable nature of smart contracts has made the subject of dispute resolution a matter of discussion. If the DLT chosen allows pseudonymous transactions and a dispute arises, how would an aggrieved participant identify the other party to a smart contract in order to bring legal proceedings against it? Do such transactions have legally binding effect, if it is simply not possible to identify the contracting party (R3 and Norton Rose Fullbright, 2018b).

Luckily for analysts (but unluckily for the aggrieved persons), smart contracts have already been put to the test. A flaw in the code of the smart contract on the Ethereum project resulted in the creation of two Ethereum platforms and the coding vulnerability in the smart contract of the Parity wallet resulted in an exploit that compromised millions of cryptocurrencies. Werbach and Cornell (2017) observe that the fact that smart contracts are immediately executable increases the importance of ex-post adjudication of grievances[13]. Courts are the ultimate forum where an aggrieved party may seek remedy and to act as the final competent authority in case of a dispute between parties.

According to Bacon and Bazinas (2017), having a formal redress system to resolve issues or disputes arising from the blockchain:

> *…offers a two-fold advantage over the informal and unilateral approach taken by Ethereum. First, it transfers legal authority to an independent and experienced arbitrator who is qualified to hear and rule on disputes. Second, it elevates computer code to binding contractual provisions and provides a legal platform for recognising and enforcing legal rights in a smart contract. (p. 2)*

Alternative dispute resolution may be considered as an answer to the immediate enforceability and executability of smart contract.

Considering that the legislation regulating DLTs is currently embryonic and that governments are reluctant to be subject to the laws and courts of another state, a smart public contract needs to include provisions on the applicable law and jurisdiction. Adair (2017) notes that "a contract involving blockchain technology should assign responsibility to parties with regards to monitoring for changes in laws and regulations, as well as associated costs from implementing resultant changes to the contract" (p.2). Regulation 524/2013 (European Parliament and Council, 2013)[14] may provide a helpful tool to resolve disputes related to smart contract that are concluded within the EU. This regulation provides for the establishment of an EU-level online dispute resolution platform for business-to-consumer disputes about contractual obligations arising from online sales and service contracts.

However, R3 and Norton Rose Fullbright (2016b) identify a further problem. There may be difficulties in proving the existence or content of a smart contract in court proceedings where evidence exists only in electronic format on a distributed ledger or elsewhere. In this digital age, courts are already facing numerous problems when electronic evidence is submitted as proof, particularly in the event that the evidence is collected in a foreign jurisdiction. Laws governing the production of evidence and their interpretation in court are not harmonised and largely depend on national legal systems. This is a hurdle that still needs to be faced by smart contracts[15].

Another interesting point which will need to be determined by the court is whether the institute of prohibitory injunctions will become redundant within the context of smart contracts. According to Article 873(1) of the Code of Organisation and Civil Procedure (Chapter 12 of the Laws of Malta), the object of a warrant of prohibitory injunction is to restrain a person from doing anything which might be prejudicial to the person suing out the warrant. In view of the immediate execution of smart contracts, it might not be possible to restrain an individual from executing the smart contract. Again, the role of courts to provide ex-post adjudication of grievances becomes even more critical.

CONCLUSION

On the assumption that the smart contract is considered as a legally enforceable contractual arrangement, a possible use case of smart contracts may be within the context of framework agreements. A framework agreement is a public contract awarded by contracting authorities to either one supplier for the procurement of multiple supplies / services or to multiple suppliers for the provision of multiple supplies / services. The procurement process of framework agreements has already been largely automated through the use of the dynamic purchasing system. It is considered achievable to also automate the post-award stage of the framework agreement using a split contracting model. A framework agreement has the advantage of having most of the contracting terms included in a master supply or service contract. The multiple purchases are then incorporated in respective purchase orders that reflect the specific purchasing terms. Once these terms are performance based, they can easily be codified as smart contracts with the more legalistic terms agreed in the master contract than retains the form of the natural language agreement.

Local public contracts have an easy resolution to possible legal disputes emanating from the immediate execution of the contract. Bank guarantees accompany most of the public contracts and are payable on demand to the contracting authority in case of breach of the contractual terms. The guarantee takes the form of a commitment by a third party, the guarantor, that is normally a commercial bank. If public smart contracts are utilised, then one option is to put into practise performance guarantees that are not applied on a per-contracts basis, but are instead provided by and binding on the economic operator through a single bank guarantee, independently of the number of contracts which are awarded to the economic operator. A further interesting option would be having the guarantee in the form of smart contract code as well.

Specifically, in relation to contract management, IBM's (2017) report notes that the current environment does not detect in a timely manner those vendors that breach the contract. Blockchain provides more complete and trusted data to enable government organisations to take better decisions about where to focus their attention. Vendors' performance monitoring is captured on the blockchain focusing attention on a vendor's reputation and trustworthiness. Blockchain is also credited with making fraudulent activity more easily detectable. The report suggests that smart contracts could automatically penalise contractors with a history of repeat offences.

As Hyman and Digesti (2017) observe, blockchain technology has taken the legal community back to the 1990s, when the community had to work through the legal implications of the then new technology, the Internet. One legal issue that caused innumerable headaches was the status of electronic signatures. As electronic transactions increased both in number and in value, the legal community had to bow to the technological advances and adapt by giving legal recognition to electronic signatures. As use cases for smart contracts continue to be identified and implemented (Chamber of Digital Commerce, 2016), the legal community will again need to adapt and, as soon as the issues identified in this article are surmounted, public procurement contracts will easily become candidates to be transformed into smart contracts.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. I would like to thank Dr. Lalit Garg B.E. (Bark.), P.G.D.I.T (IIITM), Ph.D. (Ulster) Senior Lecturer, Computer Information Systems, Faculty of Information and Communication Technology, University of Malta for the opportunity he gave me to submit the research paper and for his assistance in preparing the research paper.

REFERENCES

Adair, M. (2017, June 16). Navigating the blockchain legal landscape. *Mason Hayes & Curran*. Retrieved from https://www.mhc.ie/latest/blog/navigating-the-blockchain-legal-landscape

Alharby, M., & Van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. Retrieved from https://arxiv.org/ftp/arxiv/papers/1710/1710.06372.pdf

Bacon, L., & Bazinas, G. (2017, June 2). Smart contracts: The next big battleground? *Clydeco*. Retrieved from https://www.clydeco.com/insight/article/smart-contracts-the-next-big-battleground

Chamber of Digital Commerce. (2016, December). Smart contracts: 12 use cases for business and beyond. Retrieved from http://www.the-blockchain.com/docs/Smart%20Contracts%20-%2012%20Use%20Cases%20for%20Business%20and%20Beyond%20-%20Chamber%20of%20Digital%20Commerce.pdf

Choy, W., & Teng, P. (2017, December 22). When smart contracts are outsmarted: The parity wallet "freeze" and software liability in the Internet of value. *Blockchain and the Law*. Retrieved from https://www.blockchainandthelaw.com/2017/12/when-smart-contracts-are-outsmarted-the-parity-wallet-freeze-and-software-liability-in-the-internet-of-value/

Civil Code. (Chapter 16 of the Laws of Malta). (1874). Retrieved from http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8580&l=1

Code of Organisation and Civil Procedure. (Chapter 12 of the Laws of Malta). (1855). Retrieved from http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8577&l=1

De Ridder, C., Tunstall, M., & Prescott, N. (2017, January 6). Recognition of smart contracts. *Pillsbury Law*. Retrieved from https://www.pillsburylaw.com/en/news-and-insights/recognition-of-smart-contracts.html

Electronic Transactions Act. (Chapter 26 of the Laws of Arizona). (n.d.). Retrieved from https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/44/07061.htm

European Parliament and Council. (1999). Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093&from=EN

European Parliament and Council. (2000). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

European Parliament and Council. (2014a). Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0024&from=EN

European Parliament and of the Council. (2013). Regulation 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0001:0012:EN:PDF

European Parliament and of the Council. (2014b). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

European Parliament and of the Council. (2016). Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Gauci, I. (2017, November 28). Demystifying smart contracts. *GTG Advocates*. Retrieved from https://www.gtgadvocates.com/demystifying-smart-contracts/

Grigg, I. (2004). The Ricardian contract. In *Proceedings. First IEEE International Workshop on Electronic Contracting 2004* (pp.25-31). IEEE doi:10.1109/WEC.2004.1319505

Hyman, G., & Digesti, M. (2017, August). New Nevada legislation recognizes blockchain and smart contract technologies. *Nevada Lawyer*. Retrieved from https://www.nvbar.org/wp-content/uploads/NevadaLawyer_Aug2017_Blockchain-1.pdf

IBM Institute for Business Value with the support of the Economist Intelligence Unit. (2017). Building trust in government, exploring the potential of blockchains. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03801USEN&

International Swaps and Derivatives Association. (2017). Smart contracts and distributed ledger – A legal perspective. Retrieved from http://www2.isda.org/functional-areas/infrastructure-management/market-infrastructure-and-technology/

Lessing, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books.

Lim, C., Saw, T. J., & Sargeant, C. (2016, July 11). Smart contracts: Bridging the gap between expectation and reality. Faculty of Law, University of Oxford. Retrieved from https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality

Norton Rose Fulbright. (2016a, March). Smart contracts: Coding the fine print. Retrieved from http://www.nortonrosefulbright.com/knowledge/publications/137955/smart-contracts-coding-the-fine-print

Norton Rose Fulbright. (2017, October). Arbitrating smart contract disputes. Retrieved from http://www.nortonrosefulbright.com/knowledge/publications/157162/arbitrating-smart-contract-disputes

Norton Rose Fulbright and R3. (2016b, November). Can Smart contracts be legally binding contracts? Retrieved from http://www.nortonrosefulbright.com/knowledge/publications/144559/can-smart-contracts-be-legally-binding-contracts

Szabo, N. (1996). Smart contracts: Building blocks for digital markets. Retrieved from https://nakamotoinstitute.org/smart-contracts-glossary/#selection-109.1-109.326

Vittoria Sciberras et vs Sr Adelaide Gauci noe et, Judgement delivered by the Court of Appeal (Superior Courts of Malta) on the 29th October 2014. Retrieved from http://justiceservices.gov.mt/courtservices/Judgements/search.aspx?func=pdftext

Von Haller Gronbaek, M. (2016, June 16). Blockchain 2.0 smart contracts and challenges. Retrieved from https://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges

Werbach, K., & Cornell, N. (2017). Contracts Ex Machina. *Duke Law Journal*, 67, 313–328. Retrieved from https://ssrn.com/abstract=2936294

ENDNOTES

[1] Norton Rose Fulbright (2016a) in their paper *Smart contracts: Coding the fine print* note the possibility of machine-to-machine smart contracts: “Devices connected to the Internet of Things that will be entering into smart contracts, rather than humans” (p. 10).

[2] Those who wish to use or establish smart contracts will have to deal with issues which have existed for many years in the ‘dumb’ world…. Smart contracts will have the added complication that their compilation will require the involvement of both a legal and a technical person. (Lim, Saw, & Sargeant, 2016, p. 3)

[3] The term “smart contract” within this paper refers to smart contract code, rather than legal smart contracts.

[4] Article 973: “Persons capable of contracting may not set up the nullity of the contract on the ground of the disability of those with whom they have contracted”

[5] Section 44-7061 of the Electronic Transactions Act (Chapter 26 of the Laws of Arizona) is the first statutory law that gives legal effectiveness to smart contracts in a similar way as electronic records and signatures. Paragraph (c) states that “smart contracts may exist in commerce. A contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term”

[6] The famous quote by Lawrence Lessig (Code and Other Laws of Cyberspace, 1999) “online code is law” is often referred to, in this regard. Martin von Haller Gronbaek (2016) expands that coders will become akin to lawyers drafting “traditional” contracts, and coders will be assisted by lawyers who are specialised in the language and mechanics of smart contracts.

[7] This Directive has now been replaced by Regulation (EU) No 910/2014 (European Parliament and Council, 2014b) on electronic identification and trust services for electronic transactions in the internal market, with the aim of strengthening the cross border use of national electronic identification schemes and creating an internal market for trust.

[8] https://ec.europa.eu/digital-single-market/en/digital-agenda-europe-key-publications

[9] Besides the statutory provisions enacted by Arizona through the Electronic Transactions Act (Chapter 26 of the Laws of Arizona), other legislative initiatives are mushrooming principally in the United States. According to de Ridder, Tunstall, and Prescott (2017), Delaware had taken the lead in 2016 by starting the Delaware Blockchain Initiative. In 2016, Vermont also passed a bill making it possible for blockchain-registered digital records to be admissible in court. Following Arizona's Electronic Transactions Act, Nevada followed the same example by amending its Electronic Transactions (Uniform Act) (Chapter 719 of the Laws of Nevada) and additionally forbids governmental entities from charging money or requiring licenses for using blockchain technology or smart contract.

[10] The White Paper also refers to the "Ricardian contract" These use an identifier (a "hash") to link a natural language contract indelibly to some form of activity within smart contract architecture, such as payment. The smart contract architecture administers the data-driven performance components of the arrangement (Grigg, 2004).

[11] Alharby and Van Moorsel (2017) also refer to technical solutions that have been developed to address privacy issues. The literature the authors quote refers to encryption as well as a tool that has been developed to write privacy-preserving smart contracts without the need of implementing cryptography.

[12] Alharby and Van Moorsel (2017) note that the dependency on a third party has created two classifications of smart contracts, namely a deterministic smart contract, which is one that, when it runs, does not require any information from an external party, and a non-deterministic one, that depends on information from an external party. Specifically, in relation to oracles, they also note the possibility of a security issue with the lack of trustworthiness of data feeds. They refer to a Town Crier solution, which is proposed in the technical literature the authors reviewed and which acts as a trusted third party between external sources and the smart contract to authenticate data feeds for the contract.

[13] In relation to the Parity incident, Choy and Teng (2017) note that software liability will need to be revisited particularly in view that blockchain and a number of its applications use open source licenses. Parity utilised GNU General Public License v3.0, which states that the software is provided as is, and disclaims warranties and liabilities.

[14] The European online dispute resolution platform has been operational as of 15 February 2016 (see https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home.chooseLanguage).

[15] In another article, Norton Rose Fullbright (2017) note that arbitration may also be automated through blockchain by referring the dispute to a central blockchain administrator with the power to determine disputes and insert remedial transactions into the blockchain as necessary.

Pauline Debono holds the position of Legal Advisor with the Malta Information Technology Agency. For the past thirteen years she has been mainly involved in ICT law issues that have a bearing on the functions of the Agency in particular providing advice and ensuring compliance to legal and regulatory requirements and securing the Agency's interests in its dealings with both existing and prospective suppliers and clients. Dr Pauline Debono served as a member of the Board of Directors of the Lotteries and Gaming Authority for five years. She has an LL.D and a Magister Juris (European and Comparative Law) from the University of Malta.