ERA Forum (2020) 21:209–220
https://doi.org/10.1007/s12027-020-00617-7

ARTICLE

Regulating Blockchain, DLT and Smart Contracts: a technology regulator's perspective

Joshua Ellul[1] · Jonathan Galea[2] · Max Ganado[3] · Stephen Mccarthy[4] · Gordon J. Pace[5]

EUROPÄISCHE RECHTSAKADEMIE
ACADEMY OF EUROPEAN LAW
ACADEMIE DE DROIT EUROPEEN
ACCADEMIA DI DIRITTO EUROPEO
TRIER · TREVES · TREVIRI

Published online: 30 June 2020

Abstract Blockchain, Smart Contracts and other forms of Distributed Ledger Technology provide means to ensure that processes are verifiable, transparent, and tamperproof. Yet the very same enabling features that bring decentralisation also pose challenges to providing protection for the various users and stakeholders. Most jurisdictions which have implemented regulatory frameworks in this area have focused on regulating the financial aspects of cryptocurrency-based operations. However, they have not addressed technology assurance requirements. In this paper we present a world-first technology regulatory framework.

Keywords Blockchain · Regulation · DLT · Smart Contracts

✉ J. Ellul
joshua.ellul@um.edu.mt

J. Galea
jonathan.galea@bca.com.mt

M. Ganado
mganado@ganadoadvocates.com

S. Mccarthy
stephen.mccarthy@mdia.gov.mt

G.J. Pace
gordon.pace@um.edu.mt

[1] Inaugural Chairperson of the Malta Digital Innovation Authority and Director of the Centre for Distributed Ledger Technologies, University of Malta, Msida, Malta

[2] Managing Director of Blockchain Advisory Limited, VFA Agent, and lawyer specialising in DLT and cryptocurrencies since 2013, San Gwann, Malta

[3] Senior Partner, Ganado Advocates, Valletta, Malta

[4] Inaugural CEO, Malta Digital Innovation Authority, Mriehel, Malta

[5] Professor of Computer Science, University of Malta, Msida, Malta

1 Introduction

Over the past few years, many jurisdictions have looked into regulating cryptocurrency related operations. We have seen regulators take different approaches on how to go about this. Approaches have included outright bans of cryptocurrencies and Initial Coin Offerings (ICOs), using a case-by-case vetting and approval process of such activities, and clear guidelines regarding whether a particular activity can operate and eventually receive regulatory approval—while other jurisdictions still have not decided on whether to provide for any regulation of such activities. In reality, a jurisdiction has three paths it can take regarding regulation in this area: (i) it can ban and/or try to restrict the use of such cryptocurrencies;[1] (ii) it can decide not to implement any regulation; or (iii) it can provide clarity and a regulatory framework regarding how such activities can operate within the jurisdiction. Whilst a jurisdiction could choose to ban such activity, given the decentralised nature of the underlying types of systems, it is extremely hard, if not impossible, to enforce such a ban. While a jurisdiction can also choose to wait to see how matters play out – in the meantime subjecting itself to a severe risk of unregulated, possibly illegal, activity taking place in its territory—the legal uncertainty which can emerge from the absence of any regulation will only drive away any stakeholders in the sector who may fear that operating within such a jurisdiction could impose risks that can be mitigated by moving to a jurisdiction with a regulatory framework in place. Therefore it seems that providing a regulatory framework should be a necessity for jurisdictions seeking to protect themselves from abuse, while recognising that legal certainty can also be provided through a regulatory regime which will, in turn, enable the sector to flourish. At the same time providing a regulatory framework will also give consumer protection to investors and stakeholders whilst providing assurances and imposing requirements on operators to follow rules established so as to combat illegal activity.

Many jurisdictions around the world have introduced regulatory frameworks which provide assurances regarding due diligence on individuals, entities and the financial operations surrounding a regulated entity's activities. However, as we will demonstrate in this paper, it is not only the financial operations which require high levels of assurances in the sector, but also the technology. Seeing cryptocurrencies simply as assets whose provision and use is to be regulated fails to take into consideration the point that the underlying technologies used do more than just enable the assets, but rather bring into play new challenges in regulating them and their use. One can argue that such assurances regarding technology are as important, if not more important than other assurances being provided. In this paper we make a case for the requirement of technology assurances of not only cryptocurrencies but also other sectors or applications that are deemed to be high-risk or safety-critical and which make use of Decentralised Ledger Technologies (DLT) such as Blockchain and Smart Contracts.

[1] There is, as yet, no standard definitions for different forms of assets stored in digital form on a decentralised platform—terms such as tokens, coins and cryptocurrency are used in different ways by different authors and mean different things in different jurisdictions. In the paper, we will be using the term *cryptocurrency* to refer to all forms of such assets in order to remain as terminology-agnostic as possible.

2 Background technology

Traditionally, the technology which enables a regulated financial product or service is considered to be outside the purview of the law—it is the actions of the parties involved in providing or using the services that are to be regulated. It suffices to look at legislation addressing digital money pre-DLTs to see how legislation is technology-agnostic, and identifies subject persons responsible for the activity. And yet, certain technologies are more disruptive than others, and we argue that certain features of DLTs give rise to situations where traditional legal tools are impotent to act.

In particular, we identify the following features which, although not shared by all DLT implementations, are shared by many, particularly public DLT implementations for which no permissions have been given:

- *network decentralisation:* the peer-to-peer nature of DLTs ensures that the network is resilient against direct attempts to shut it down.
- *governance decentralisation:* governance of the content on a DLT is itself decentralised, in that no single party may impose decisions taken on the content stored, transactions processed, *etc*.
- *redundancy through decentralisation:* data stored on a DLT is stored in multiple locations, in order to ensure resilience through redundancy.
- *immutability of past data:* information written on the DLT cannot be changed, overwritten or deleted.
- *irreversibility of transactions:* most DLTs primarily store one form of data, typically transactions between parties invloving assets stored in digital form. The immutable nature of DLTs implies that such transactions are irreversible and cannot be affected *a posteriori*.
- *user anonymity:* although different forms of DLTs exist, the decentralised nature of the technology allows for anonymous (or, at least, pseudonymous) participation in the transactions.
- *automated aspect:* DLT-based smart contracts allow for automation on a DLT to go beyond execution of transactions, but also to enable the execution of arbitrary code in a decentralised, tamperproof manner which cannot be manipulated by any single party.
- *reactive nature of the execution model:* the underlying execution model of most DLTs is a reactive one, in that the platform reacts to external stimuli (*e.g.*, the initiation of a transaction or the invocation of a smart contract), rather than an active one in which actions can be initiated by the DLT itself.

Although a number of these technological features have been seen before, the combination of them leads to various new regulatory challenges. In particular, it is worth noting that the automated aspect of DLTs together with the immutability of data provides them with a degree of autonomy, in that once instructions are recorded, they can be executed, but cannot be interfered with—either at the smart contract (thanks to immutability), or at DLT level (due to the resilience of the network and data redundancy). These features bring about a number of novel regulatory challenges, as discussed below:

- *data violations:* although peer-to-peer networks have long been known, the immutability introduced by DLTs means that data cannot be removed or changed, even if authorities require it to be. Furthermore, the decentralised governance implies that authorities cannot filter what is written on the DLT.
- *anonymity violations*: removing anonymity has typically been addressed through regulatory requirements on service providers, but the decentralised governance of DLTs does not give a regulatory framework a foothold it can use to remove anonymity.
- *illegal actions:* actions arising from executable code written to and executed on a DLT may result in breach of law. In some cases blame can be assigned to the party provoking the behaviour (*e.g.*, a party using a smart contract to perform a transaction in return for an illegal service), although there still lies the challenge of anonymity. However due to the decentralised nature of DLTs, it is not always clear how parties can be identified.
- *violations due to inaction:* due to the reactive nature of the many DLT platforms operating without permission having been given, progress may be stalled due to actions which cannot be performed unless initiated by an external party, which may lead to a breach of the law due to inaction, and with no party being obliged to trigger the smart contract.
- *violations due to code errors:* whilst automation can be considered an advantage, in that the code prescribes behaviour, one has to take into account errors in code, and obfuscated code which indicates one form of behaviour but stealthily performs another. Where the responsibility for causing such behaviour lies is unclear, since the code does prescribe one form of behaviour, even though the user may have expected another.

Over and above these types of violations, there lies the overarching challenge of addressing what is to be done when a breach of law occurs. The immutability of the recorded information and immortality of the underlying platform severely handicap the power of the law to intervene.

3 An overview of regulatory frameworks

The field of cryptocurrency has brought technology closer to finance. Even though not all DLT platforms provide (or require) a cryptocurrency, they have been intertwined or at least, closely associated in the minds of many. Therefore, before focusing on aspects relevant to the underlying technology, we will give an overview of the cryptocurrency regulatory frameworks that have been proposed.

It can be said that the need for regulatory frameworks was spurred by two main factors—concern over the use of cryptocurrencies for illicit purposes, and the need to protect retail, professional and enterprise users of various platforms providing services akin to financial services. The first high-profile, large-scale illicit activity and money laundering case involving cryptocurrencies was the notorious Silk Road case, where Ross William Ulbricht, was found guilty of running, operating and administering an underground e-commerce marketplace on the dark web for illicit ‘victimless products' [8] such as drugs and other substances, as well as malicious hacking software, forged documents such as licences and passports, and assassin hiring services, among other items. The first major case of a service provider which resulted in significant losses for users was the Mt. Gox cryptocurrency exchange incident, where some sources claim that up to 750,000 BTC were lost through unsolicited attacks by unknown third parties [9].

These two landmark incidents intertwine in a sense as they led lawmakers in most developed jurisdictions to undertake an approach that can be seen as a common one. Certain service providers, specifically those which act as a bridge between fiat and cryptocurrencies such as exchanges, and those who hold in custody the private keys granting access to one's cryptocurrencies, were brought within the remit of anti-money laundering and financial service frameworks. In case of the latter, extensions of existing frameworks such as in the case of the United States [7] and Luxembourg,[2] or the creation of new ad-hoc ones serve first and foremost to provide investor and user protection, and also to ensure that any entities providing such services are properly screened and vetted prior to the commencement of operations. Indeed, some regulators have seen fit to include an assessment of certain technological aspects in the mentioned vetting process.

Anti-Money Laundering concerns in general also led to the Fifth EU Anti-Money Laundering Directive,[3] including requirements for exchanges that offer conversion of fiat currencies to cryptocurrencies and vice-versa, and service providers holding custody of cryptocurrencies on behalf of clients. Apart from classifying such entities as subject persons under the Directive, Member States are also required to mandate the registration of such entities with the competent local authorities, namely financial intelligence units and/or the financial services authorities. This has forced EU Member States, at a bare minimum, to regulate such service providers, with Member States such as France effectively regulating other service providers as well, very much in the spirit of the regulations enacted by the Maltese authorities. Likewise, the *Autorité des Marchés Financiers* requires its licensees to disclose implemented internal cybersecurity measures.

One can also see that other jurisdictions have also started to undertake steps towards implementing regulations, or at least introducing standards, in relation to the use and development of DLT in general. Earlier this year, the People's Bank of China implemented the Financial Distributed Ledger Technology Security Specification.[4] The purpose of this security specification is to provide a common base standard for the development of financial services using DLT, specifically to ensure that security remains the main underpinning principle when delving further through the possible use-cases of DLT. The published specification document addresses various aspects of such systems such as basic hardware and software, cryptographic algorithms, protocols, smart contracts, and operational and maintenance requirements.

The European Union Blockchain Observatory and Forum, an initiative of the European Commission, has prepared a report on a *Legal and Regulatory Framework*

[2] https://www.siliconluxembourg.lu/cryptocurrencies-in-luxembourg-current-regulatoryapproach/.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843.

[4] https://news.bitcoin.com/china-adopts-security-standards-blockchain/.

of Blockchains and Smart Contracts[5] in which they highlight challenges, potential solutions and various paths forward for DLT and the law. The report highlights the following points which are most relevant to the discussion being presented herein: (i) the importance of identifying central points which can be used to apply regulation to, such as miners, core software developers, end users, and even enabling governmental or regulatory players to be potential blockchain participants; (ii) issues of identifying liability, for example that of core software developers; (iii) the challenges that the immutability and lack of update-ability of smart contracts brings; and (iv) the need for quality assurance and technology audit processes. We provide solutions regarding the above points in our innovative technology arrangements regulatory framework which will be described further in Sect. 5.

The Federal Reserve Bank of Boston proposes a 'supervisory node' [2], a blockchain node set up to undertake supervisory roles which forms part of blockchains which the regulator is supervising. The general architecture describes that the 'supervisory node' can undertake many roles "beyond the Fed's regulatory supervisor role, such as an auditor, payments network rule-enforcer, or data reporting entity." It is unclear whether the responsibility will be that of the regulator to integrate with the different blockchain platforms under supervision, or whether they will provide a number of platform-specific blockchain implementations which operators will be obliged to integrate with. The former puts a significant burden on the regulator to develop various 'supervisory node' implementations to be able to successfully connect and interact with the various types of DLT platforms that may eventually exist out there, and further puts the onus on the regulator to ensure that the implementation is correct (for each different platform) so as to ensure that the particular operator or activity can be supervised adequately. The latter case of requiring operators to integrate with limited supported platforms: (i) puts a greater burden on the operator to integrate with the 'supervisory node'; (ii) acts as a potential technology barrier to certain activities from operating within the regime if the operator's DLT system is not technologically capable of such interaction; and (iii) also may put the regulator's implementation into question when things go wrong, if the operator claims that some error occurred due to the incorrect behaviour of the "supervisory node" (which is more of a worry for smaller DLT networks). Later in Sect. 5, we present the innovative technology arrangement regulatory framework's 'Forensic Node' and 'Technical Administrator' respectively, which provide a solution to supervision and potential intervention, but do not pose the challenges listed above.

Besides the Malta Digital Innovation Authority's technology regulatory features alluded to above and further described in Sect. 5, the Malta Financial Services Authority (MFSA), issued guidelines on cybersecurity measures to be implemented by all operators within the jurisdiction, namely those issuers conducting public offerings of virtual financial assets (VFAs), as well as those offering services in relation to such assets [1]. The Financial Intelligence Analysis Unit (FIAU) also mandates issuers of virtual financial assets and service providers to implement tools that tap into the resourcefulness of DLT when it comes to tracking and tracing cryptocurrencies and the origin thereof, commonly termed as crypto-forensic tools. Malta can therefore be

[5] https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf.

seen as a prime example of where regulators place emphasis on technological aspects of DLT and cryptocurrencies, encouraging the use and adoption of solutions in order to safeguard end users and investors.

4 The case for technology assurances

The various cryptocurrency and DLT regulatory frameworks that have been proposed around the globe (with the exception of that of Malta) require either no or bare minimal features aimed at providing technology assurances. In this section we build a case as to why technology assurances are essential.

Since its debut, software has become ubiquitous whilst at the same time is notoriously known to suffer from bugs – whether this be software used on traditional computers or firmware used in embedded devices inside homes or cars or in relation to other facets of life. Bugs are often of minor consequence. However, some can have more serious implications, such as the infamous NASA Spirit Rover which became unresponsive due to a bug that resulted in files not being deleted [5]; or the Therac-25 bug [3] which resulted in a radiation therapy machine overdosing six (known) patients causing their death.

To ensure that bugs are minimised in deployed systems, quality assurance processes are followed which typically include: (i) developer support tools that help to minimise errors whilst writing code; (ii) testing, which is often undertaken by independent programmers or teams; (iii) verification techniques used to ensure that software is checked for correct operation prior to deployment; and (iv) when all else fails and bugs still manage to make it into deployed systems, once found, a bug will be fixed in a new version of the code and updated on the running system.

For some types of systems the above tools and processes are sufficient. However, for systems which are safety-critical in nature or which may result in large losses if incorrect behaviour occurs, the above is not good enough. Moreover, in software systems which do not allow for code to be updated, like smart contracts, deploying a system with a bug is detrimental. Such types of systems, which are safety critical in nature and/or do not allow for software updates, existed before the advent of blockchain and cryptocurrencies. Consider the aviation industry, where a bug in airplane software could result in loss of many lives. To raise the levels of assurances in aviation software, such software goes through independent audits. This is really not just about software. Many industries require independent audits where failure is not an option—*e.g.*, this is required for critical physical infrastructure such as bridges. For the very same reasons, software that is used for applications that are critical or of a high risk nature, be it smart contracts, blockchain networks, other distributed ledgers, or even traditional software, should undergo independent audits to ensure that the systems are implemented correctly, so as to avoid detrimental consequences. The question then for the cryptocurrency and DLT sector, which we address now, is: *if the system fails, could the losses be substantially large or detrimental?*

Smart contracts, blockchain and DLT node implementations are indeed software—and software is prone to having bugs. Numerous examples of bugs have resulted in large financial losses. A few notable cases of smart contract related bugs include:

the infamous Parity bug [6] that ended up losing and locking away USD 200 million worth of Ether (the cryptocurrency provided on the Ethereum blockchain); the infamous Decentralised Autonomous Organisation (DAO) hack [4] which allowed for a malicious user to steal USD 50 million worth of Ether of other users' funds; and more recent cases which saw a decentralized lending protocol hacked in two days[6] resulting in just under USD 1 million being stolen, and a decentralised exchange bug which allowed for a hacker to get away with more than USD 250,000.[7]

Whilst it is impossible to get rid of bugs in smart contracts (unless a way has been factored in to replace smart contracts), blockchains do allow for software updates provided that the nodes in the network install the update. Such updates could cause 'hard forks' in the network, whereby those nodes that do not choose to accept the update would no longer be part of the 'new' blockchain with the updated code, but would remain part of the 'old' blockchain with the original unpatched code. For large networks, coordinating such an update could take time, within which there would be a lack of clarity regarding what users should do. Should they continue to use the unpatched blockchain? Should they wait for the new version to be deployed? What losses could they incur due to not being able to transact? A notable instance of such a bug that was active in the wild includes a Bitcoin bug that would have allowed malicious users to mint more bitcoin than the maximum 21 million bitcoin limit.[8]

Wallet software bugs can also result in large losses. A recent bug in an IOTA (a popular DLT) software wallet resulted in USD 2 million being lost, and the IOTA network being taken down [9] for nearly a month.

As can be seen from the use cases above, providing assurances that such software being used is not faulty is crucial, and the failure to do so could result in very substantial losses. Therefore, technology assurances for such high-risk operations should be required. In the next section we present the Malta Digital Innovation Authority's regulatory framework, which aims at instilling higher levels of assurances within such technology.

5 The Malta digital innovation authority and the innovative technology arrangement regulatory framework

The Malta Digital Innovation Authority (MDIA) was set up in 2018, having as its explicit purpose "*to promote consistent principles for the development of visions, skills, and other qualities relating to technology innovation, including distributed or decentralised technology, and to exercise regulatory functions regarding innovative technology, arrangements and related services and to make provision with respect to matters ancillary thereto or connected therewith.*"[10] We will first highlight the

[6] https://cointelegraph.com/news/decentralized-lending-protocol-bzx-hacked-twice-in-amatter-of-days.

[7] https://www.coindesk.com/hacker-exploits-flaw-in-decentralized-exchange-bisq-tosteal-250k.

[8] https://www.coindesk.com/the-latest-bitcoin-bug-was-so-bad-developers-kept-its-fulldetails-a-secret.

[9] https://blog.iota.org/trinity-attack-incident-part-3-key-learnings-takeawaysc933de22fd0a.

[10] Malta Digital Innovation Authority Act (MDIAA), Chap. 591, Laws of Malta.

strategy and policy decisions which led to the regulatory framework and thereafter highlight specific features of the framework.

The first policy action was to create a new regulator for *innovative technology arrangements* (ITAs) defined to be "*the intrinsic elements including software, codes, computer protocols and other architectures which are used in the context of DLT, smart contracts and related applications...as may be further defined in the Innovative Technology Arrangements and Services Act*." The Authority was not set up to regulate cryptocurrencies or such assets, but to address technology arrangements constituting blockchain, other DLT or smart contracts (which very well may be used within cryptocurrencies or other virtual currencies).

The bigger policy issue is whether one should have a regulator for these new technologies and what any such regulator should do. Many disagree that technology should be regulated at all, let alone have a self-standing regulator for an "innovative" sector when we all know that innovation never stops. The reason why the decision to take this step was made relates to the fact that this technology has features of decentralised governance and automation which go beyond anything we have known before. These two features create a dependence of users on the technology itself without obvious recourse to an owner or controller who can be held liable for detrimental outcomes.

Most importantly, the Government of Malta recognised that once deployed, the technology could cause a loss or be in breach of the law—such as those on the prevention of money laundering, on privacy, on taxation and on consumer rights. Some form of redress was therefore needed. The outcome of this law was to ensure that the technology passed some quality tests on important aspects or features which cover vulnerabilities, many of which were noticed.

The creation of the Malta Digital Innovation Authority also addresses a resource problem for Malta, which has a small population of under 700,000. It was important to ensure that limited resources in this field are concentrated under one roof with a clear and consistent agenda. This would avoid overlap with the many other regulatory authorities which already exist, thus avoiding regulator competition for talent in a small market. It also seeks to avoid duplication and contradictory strategies, while at the same time maintaining expertise on a subject matter (*e.g.*, financial services, health) combined with knowledge and awareness of the strengths and weaknesses of DLT and smart contracts. It allows one regulator to focus on the quality of the technology solution using DLT with the other regulator relying on the first to ensure that the goals of the second are achieved in its areas of expertise.

The Innovative Technology Arrangements and Services Act (ITASA) is the law which introduced the initial licences for which one could apply. The law does not say one needs a licence to design, develop and deploy blockchain, DLT or smart contracts—as that would be absurd. The deployment of technology has even been assimilated to freedom of expression. What the Act seeks to do is to offer certification to a developer of an innovative technology arrangement which should provide a level of trust in the market. It is voluntary and one can apply for it if one wishes to meet the standards of the law and obtain confirmation of such compliance.

The voluntary nature of certification seeks to address two issues. The first is that this is newly-charted territory—a developer going to a state entity and asking for the technology to be checked for standards and quality is something new. Why should one do that? In the private software context, anyone offering software facilities will naturally warrant their qualities as part of the offering for sale or lease. That creates liability for deficiencies and a buyer of the software or a lessee will be able to rely on the warranty (assuming wording which implies consumer rights) and sue for damages if the software fails.

System Auditors and Subject Matter Experts Systems auditors, entities that will audit the technology developed in order to determine whether the innovative technology arrangement meets the standards required, are registered with the Malta Digital Innovation Authority, following an application process involving a review and a due diligence exercise including the vetting and scrutiny of their various subject matter experts. Once registered they can—provided that they are independent of the developer or applicant of an innovative technology arrangement—be engaged by a developer or indirectly through the technology arrangement (through the technology arrangement's internal governance structure) to review the software and its features and capacities. That will then lead to certification by the Authority if the requisite standards are met.

Certification of an innovative technology arrangement can take any of the following forms (currently): for DLT alone, DLT with some smart contracts, or smart contracts on their own. The certification will state, on the face of it, what is being certified. This will enable a third party user to understand what is covered by it and what is not.

Technical Administrator Another crucial service provider is the technical administrator. The systems auditor has been conceived as being pre-deployment assurance, leading to certification, while the technical administrator has been conceived as playing a potential role post-deployment and certification.

Without going into too much detail, the technical administrator is a person engaged by the technology arrangement applicant, and need not necessarily be independent as long as he subscribes to duties which are of a fiduciary nature in favour of the users as a whole. Basically, the technical administrator must be the last point of recourse should there be a loss or a breach of law taking place which is not addressed through the governance structure of the arrangement.

If no-one acts to address a problem of loss or breach of law, then the technical administrator, on being notified of the problem and seeing lack of action, must intervene. To be able to intervene effectively, the software must give him some powers to intervene and modify the software and perhaps, in an extreme case, a kill switch. Although having such a power may be seen to be controversial (in the DLT-sphere), it has been adopted in order to address the fact that technology may have points of failure and, without powers of intervention and modification. It would be contrary to acceptable levels of integrity to allow certification of such a platform. Such intervention will vary depending upon the type of arrangement. However, this could vary from the ability to update smart contract logic (which could be based upon a governance structure), to the issuing of software updates to be published on the various nodes in the DLT.

Forensic Node Another crucial requirement is that of a *Forensic Node* [11] whose aim *"is to store all relevant information to the runtime behaviour of the innovative technology arrangement in real-time including but not limited to transactions carried on the DLT-components of the ITA"*.[12] The forensic node is to be implemented by the operator (and not the Authority). At the same time it does not require that the operator abides by a specific specification, interface or other technology restriction.[13] Systems auditors are required to ensure that all relevant information is recorded faithfully in real-time without risk of omission or corruption, thus ensuring that the means of conducting an investigation exist at a later stage when required.

In this manner, Malta provided a solution which can be rendered unnecessary by dealing with any problems or vulnerabilities in the software itself.

Furthermore, the legislation seeks to address the problem of the identification of owners and controllers of the arrangement through looking at tokens which imply ownership and control in different ways from the traditional shares, partnership interests and directors or administrators found in legal organisations. Anti-money laundering laws, privacy law and consumer protection laws all assume traditional corporate operators where the process of identification is easy. Tokens have challenged all that. Some solutions have been provided in the law to support anti-money laundering. Tax guidelines were also introduced simultaneously with the legislation on the Malta Digital Innovation Authority and innovative technology arrangements in November 2018.

Blueprint, English Description and Consumer Protection The systems auditors, in undertaking their quality and assurance checks, will use a technology blueprint to determine whether an arrangement is technically sound. In the event that a discrepancy emerges between the implementation and an obligatory (English) description displayed to users, then, according to the Innovative Technology Arrangements and Services Act, the English description will be deemed to prevail over the implementation.

6 Conclusions

Recent efforts around the globe to provide legal certainty to cryptocurrency based operations, and protection to various types of users and stakeholders have been a step in the right direction. However, as has been highlighted in this paper, flaws within the technology deployed for such activities could result in large financial losses. Given the nature of Blockchain, DLT and Smart Contracts which limit the ability for software and/or data errors to be rectified, in this paper we put forward the need for technology assurances to be put in place for any safety-critical or high-risk based applications. In the interests of not stifling innovation, we propose that such technology

[11] It is worth mentioning that despite the use of the term 'node,' a forensic node may not necessarily be on-chain.

[12] Malta Digital Innovation Authority, *Forensic Node Guidelines*, 2019. Available from https://mdia.gov.mt/.

[13] Unlike the Boston Fed supervisory node described in Sect. 3.

assurances be voluntary for sectors or applications that are deemed to be low-risk. In the foregoing text we have presented the Malta Digital Innovation Authority, a world-first regulator of its type, and the innovative technology arrangements framework which currently provides for a technology assurance regulatory environment for Blockchain, DLT and Smart Contracts.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Buttigieg, C.P., Efthymiopoulos, C.: The regulation of crypto assets in Malta: the virtual financial assets act and beyond. Law Financ. Mark. Rev. **13**(1), 30–40 (2019)
2. Federal Reserve Bank of Boston: Beyond theory: Getting practical with blockchain (2019). Whitepaper
3. Leveson, N.G., Turner, C.S.: An investigation of the therac-25 accidents. Computer **26**(7), 18–41 (1993)
4. Mehar, M.I., Shier, C.L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H.M., Laskowski, M.: Understanding a revolutionary and flawed grand experiment in blockchain: the dao attack. J. Cases Inf. Technol. **21**(1), 19–32 (2019)
5. Neilson, T.: Mars exploration rovers surface fault protection. In: 2005 IEEE International Conference on Systems, Man and Cybernetics, vol. 1, pp. 14–19. IEEE Press, New York (2005)
6. Nikolić, I., Kolluri, A., Sergey, I., Saxena, P., Hobor, A.: Finding the greedy, prodigal, and suicidal contracts at scale. In: Proceedings of the 34th Annual Computer Security Applications Conference, pp. 653–663 (2018)
7. Nonaka, M., Konko, J., Gaffney, C.: FinCEN issues guidance to synthesize regulatory framework for virtual currency. J. Invest. Compliance (2019). https://doi.org/10.1108/JOIC-07-2019-0041
8. Rothstein, A.: The end of money. The New Scientist. ISBN: 9781473629530 (2016)
9. Trautman, L.J.: Virtual currencies; bitcoin & what now after liberty reserve, silk road, and mt. gox? Richmond J. Law Technol. **20**(4) (2014)