DIGITAL
LAW
ASSOCIATION

SUBMISSION

Law Commission Smart contracts - Call for evidence

7 April 2021

Disclaimer and Copyright

While the DLA endeavours to ensure the quality of this publication, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this publication.

Contents

ABOUT THIS SUBMISSION 3
EXECUTIVE SUMMARY 4
WHAT IS A SMART CONTRACT (CHAPTER 2)........ 6
FORMATION OF SMART CONTRACTS (CHAPTER 3)........ 23
INTERPRETATION OF SMART CONTRACTS (CHAPTER 4)........ 37
REMEDIES & SMART CONTRACTS (CHAPTER 5)........ 42
CONSUMERS & SMART CONTRACTS (CHAPTER 6)........ 49
JURISDICTION & SMART CONTRACTS (CHAPTER 7)........ 56
FINAL QUESTIONS (CHAPTER 8) 63

ABOUT THIS SUBMISSION

The Digital Law Association is an organisation dedicated to the promotion of a fairer, more inclusive, and democratic voice at the intersection of technology, law and policy.

Our mission is to encourage leadership, innovation, and diversity in the areas of technology and law by:

- bringing together the brightest legal minds in the profession and in academia to collaborate; and
- developing a network that promotes digital law, and particularly female leaders in digital law.

This document was created by the Digital Law Association in consultation with its members listed below. The compilation of this submission was led by Susannah Wilkinson. This submission has been contributed to by the following Digital Law members:

- Aaron Lane
- Alex Sims
- Amiinah Dulull
- Ana Pochesneva
- Ariane Garside
- Byron Turner
- Daniel Banik
- David Lee
- Faith Obafemi
- Georgie Hoy
- Iris Rad
- Joel Smalley
- Joni Pirovich
- Kathryn Roach
- Mark Abbott
- Muthusi Evans
- Natasha Blycha
- Sarah El-Atm
- Soraya Pradhan
- Stephen Alexander
- Susannah Wilkinson

In addition, the following have endorsed this submission:

- Ariane Garside
- Natasha Blycha
- Susannah Wilkinson
- Joni Pirovich

Submission Process

In developing this submission, our members have engaged through email correspondence and virtual discussions relating to the questions posed by the Law Commission smart contract Call for evidence. This is to ensure everyone has had the opportunity to provide input on these issues.

EXECUTIVE SUMMARY

The Digital Law Association is pleased to provide this submission to the Law Commission's Call for Evidence in relation to Smart Contracts. The Digital Law Association is an organisation dedicated to advancing a fairer, more inclusive and democratic voice at the intersection of technology, law and policy (https://digitallawassociation.com). With global membership in the thousands (when including our cross-platform social media following), we identify the need for clear and appropriate guidance for the legal and technology sectors in relation to the understanding, use, requirements and enforceability of smart contracts.

Smart contracts have evolved from a technology-led push to automate transactions, and in many cases to avoid intermediaries. We see this as part of the broader movement towards digitising contracts, with integration of active coded components that allow for automation and 'self-performance' at the more complex end of that digitisation spectrum.[1] By integrating legal language and agreements of legal status into and alongside the code of a smart contract we can form legally binding contracts (or, smart legal contracts). [2] It is important that the digital evolution of these new digital, but also legally binding contracts (with their consequential wide-scale impact on the practice of law and the broader economy) is not shaped solely by technological and commercial drivers (for which legal precedent and certainty must wait for legal judgments), but is shaped by well-established legal principles, duties, legal oversight and an eye to the rule of law as well as technology governance standards grounded in ethics.

Enhancing legally enforceable contracts at scale through automation, structured data, and digital connectivity will unlock significant value for the economy. Smart contracts have the capacity to enhance both efficiency and transparency in the rapidly emerging realm of the digital economy notwithstanding the existing and new risks that need to be managed and mitigated. Smart contracts can enhance the rule of law by allowing parties to use existing forms of structuring legal relationships to enhance their digital activities, and vice versa. Integrating the protections and coherence of legal contracting, instruments and agreements directly into the digital economy via smart contracting brings with it many opportunities to enhance the governance of data and the digital realm, and the ability of economic actors to allocate the risks and rewards of digital activity as between themselves, through legally enforceable agreements. Last but not least, the more contracts that an entity makes 'smart' through the incorporation of code, connections and data flows, the greater insights that entity

[1] See further under our response to paragraph 2.12. For more on the nature of different forms of digitisation and 'smart' elements of smart contracts, see:
Wilkinson, Susannah and Giuffre, Jacques, Six Levels of Contract Automation: The Evolution to Smart Legal Contracts - Further Analysis (March 30, 2021). Available at SSRN: https://ssrn.com/abstract=3815445

[2] For a detailed analysis of how smart contracts can integrate the legal and digital, see: Blycha N., and Garside A., 'Smart Legal Contracts: A Model for the
Integration of Machine Capabilities Into Contracts', (2020) publication forthcoming. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3743932.

can derive from its dealings and the business relationships that are packaged within such a smart (and legal) contracting framework.

More organised, understandable and interrogable data on both contracts, and the activities they govern, provides many economic benefits, and will help to minimise harms or negative impacts of particular forms of structuring relationships that may otherwise go unnoticed. The contract, enhanced in this way, becomes a form of digital asset, providing not just the bundle of legal rights and obligations of a legal instrument, but also the value of its ability to automate workflows, collect organised data and structure business relationships and activities that occur through, or are measurable by, digital systems and data.

Fundamental to achieving these kinds of benefits, is ensuring that well-understood and tested legal protections, norms and principles of contracting can still be relied upon, even with the incorporation of coded components, automation, data connections and other ‘smart’ elements into a contract. A clear thread runs through our submission, advocating for methods of smart contracting and well-designed platform(s), that allow for a true integration of legal language (or at least legal principles of contracting) with the digital elements of code. Rather than aiming to exclude or minimise the legal status of a smart contract (and all the consequential protections and implications legal status as a contract provides), we believe that the most practical, and beneficial way forward for the digitisation of contracting is integration of legal language and code. This has the accompanying, and equally important impact of ensuring interrogability. Where code is linked – through whatever methodology – to legal language, smart contracting becomes more accessible to, and less risky, for a broader spectrum of people and economic actors who might otherwise be excluded from this innovation.

Our submission is based on the underlying premise that the most appropriate way forward for smart contracts is (a) to develop methodologies and legal approaches that enable them to be legal contracts, (b) enable them to be understandable to humans as well as by machines (particularly as artificial intelligence takes a more active role); and (c) for formal legal bodies and governments to be involved in (sovereign) platform and application solutions that support the rule of law and global low energy approaches[3], particularly if the market alone fails to deliver solutions that promote (a) and (b).

[3] Many public, permissionless DLT platforms (by virtue of their current consensus protocols), used for smart contracts have high energy footprints which the DLA considers should be a barrier to their use and promotion.

WHAT IS A SMART CONTRACT (CHAPTER 2)

1. What kinds of contractual obligations can currently be automated using computer programs? Please provide specific examples where possible. (Paragraph 2.12)

Before directly answering this question, we provide the following introductory comments to contextualise the two ends of the spectrum from which this question can be answered:

- Ethereum-based smart contracts, particularly those used in decentralised finance (**DeFi**), are intended to represent the entirety of legal and contractual rights and obligations between the user and the Ethereum blockchain (a concept colloquially referred to as "code is law", as opposed to "code of law" which refers to our existing domestic and international legal regimes). No natural language version of the smart contract code (a .sol file) is generally produced although smart contract code audits (when commissioned and made publicly available) are written in natural language and specify the cyber risks identified and what action has been or will be taken to mitigated the identified risks.
- An entire, traditional legal contract (not just a particular obligation – or a part of a contract) can be made machine readable and can be tagged to structure and generate data. This is a useful first step in digitising contracts, even if the contract does not contain any code or other automation-enabling features[4] and is also the most logical form of contracts that do contain automations.

More specifically, an entire, traditional legal contract can be:

- machine readable (that is, to have the text of its legal language searchable and reviewable by machine systems); and
- stored on an appropriate digital platform that provides a single source of truth between counterparties.

The inherent complexity of contracts and the natural interaction of different rights and obligations inside a traditional contract, means that a particular obligation should not be considered in isolation from the agreement as a whole. This dependency is relevant in considering the impact of automation on a particular obligation within the broader digitised and machine-readable agreement.

That is, once a baseline machine-readable and digitally accessible contract is live, parties can also choose to automate performance of certain obligations under a contract, connect the contract to, or allow the contract to be, a source of data and extend the contract through digitally adding automations or structured data that are of value to one or more parties.

[4] That is, unless and until natural language processing systems become sophisticated enough to take action based on regular legal language in a contract.

As noted above, our submission is based on the underlying premise that the most appropriate way forward for traditional legal contracts to become smart contracts is to (a) develop methodologies and legal approaches that enable them to be legal contracts, and (b) enable them to be understandable to humans as well as machines. With that in mind, to understand what kinds of contractual obligations can be automated, it is useful to consider two different ways that discrete automations (sometimes referred to as smart clauses) can be embodied within a contract to allow parts of the contract to be accessible to both human and machine. These are:

1. drafting appropriate clauses in machine readable code and logic to enable deterministic logic of the obligation to be processed by machine (Unified Method); and

2. extending a natural language clause by pairing (tagging or linking) the clause with coded automation (Paired Method).

In the case of a hybrid contract, a simplistic way to describe the difference between the methods is that the former provides a way to express a particular obligation in a unified way so that it is accessible to both computer and human, effectively the two ways to express the provision are two sides of the same coin. Whereas the latter provides a way to attach the benefits of automation to a natural language expression through pairing code with a relevant term or clause in the natural language contract.

The method of creating the smart contract, including both the platform and the user interface will be influencing factors in determining which method is used, and what parts of a contract can be subject to automation. We expect market solutions to include the option for both methods.

The **Paired Method** provides that the natural language expression of a particular provision/obligation is extended by virtue of being paired (connected, tagged or linked) to a corresponding coded expression of a related automation, but the two expressions do not need to necessarily match (in terms of completeness or logic). The pairing is relevant only for contractual/legal reasons not for technical functionality. For example, a natural language clause that states ‘The delivery date under the contract is 1 July 2021 and liquidated damages will be payable for every day delivery is late’, can be extended simply by pairing the clause with code that provides an automated notice advising the purchaser if delivery has not been received by 5:00pm on 1 July 2021. In this case, the automation could, but does not necessarily need to go further and address calculation and payment of liquidated damages to mirror all of the elements of the natural language clause. Rather the parties to the contract have freedom to choose where automation or the collection of shared data indicating or measuring performance adds value to the contract management process.

This method is very flexible and versatile and theoretically there is no natural language obligation that cannot be extended through automation of paired or linked code, provided the parties have appropriate technical inputs and outputs they are willing to use in respect of a given contractual process or obligation. For example, any part of a contract from the party names, definitions, calculations, business days, operative provisions etc can be extended through the tagging of a notice, payment, API call or a calculation. This provides counterparties the flexibility to determine on a clause, and subclause, level whether the natural language or the code should take priority, and other key matters in relation to the performance of the automated provision. This also allows for unilateral internal automation from the contract into a counterparties' internal systems that could sit outside the scope of the legally enforceable contract, in addition to shared automation that the parties may agree to form part of the contract. Shared automation is a new concept to the legal industry and the sharing of upside benefit or downside risk in the event an automation does not function properly or is subject to a cyber-attack are new matters for the legal industry to resolve.

The Paired Method may be particularly useful where existing agreements are to be automated, as automation can be gradual and evolutionary (i.e., the business concerned is not reinventing the wheel and can develop its automation over time). This will be particularly helpful where one party is dealing on standard terms where there is little room for negotiation, as the contract, once codified, will only require certain known variables to be changed for each iteration of the agreement. This may be particularly useful in the context of business to consumer transactions. In addition, the regulatory environment within which such contracts exist (noting the imbalance of bargaining power between a business and a consumer) could provide comfort to the consumer that should there be a mismatch between the written word of the agreement and the automation, an appropriate remedy would be available. This could lessen the risks to the consumer and could encourage smart contract adoption where it may otherwise seem an additional risk.

By contrast, the **Unified Method** requires that a particular provision is expressed in a unified representation of the parties' agreement whether through some derived, formal language or intermediary language which provides the machine-readable logic. This may involve a clause 'stack' where multiple files relating to a clause are combined such as the approach used in Clause (where a text, model and logic file are combined into a single '.cta' file for a given unified clause).

From a legal drafting perspective, the Unified Method is more restrictive in that it requires both the natural language and coded expression of a particular clause to be either the same expression, or very closely correlated. This means that only clauses that can be expressed in a closed loop manner can be extended through automation, for example payments, calculations, notices with strict parameters and so on; or which can be triggered by an appropriate input (for example, an external 'oracle' providing a trusted input). While this is valuable, it is potentially limiting in terms of the functionality available in respect of a given clause under a contract. This model may be beneficial where a business is designing new processes from the ground up, is aware of the potential limitations and can alter its processes to compensate.

Of the provisions in a contract that can be expressed in computational logic or paired to computational logic, we anticipate that the parties will ultimately need to do a cost benefit analysis particularly as there will likely be an increasing cost profile, behavioural and training shifts, and increasing complexity in the first instance for additional automations added to a contract that will need to be weighed against efficiencies and risk requirements.

Common features identified across use cases include increased transparency and security, improved data control, authentication procedures, certainty in performance or title or asset transfer.

Key factors in deciding what should be automated include:

- The technical assessment of ability to automate – is it practical and viable to automate in a meaningful way (often dependent on whether a particular step, event or process set out by a contract can be meaningfully and reliably measured and translated into one or more data points);

- A commercial assessment of the value of outcomes produced – in particular any impacts on individuals arising from the automation (either as a result of unintended impacts of the automation or the automation going wrong,[5] or as a result of job displacement), what is the return on investment, financial value, gains in economic efficiency, but also less direct quantifiable metrics such as the value of information-sharing between parties and, from perspective of legal practice, facilitation of collaborative legal practice, avoidance of future disputes, etc; and

- The ability to reuse the same automations in multiple agreements. The initial cost and time incurred in automation is unlikely to be attractive if the entire process has to be repeated on a bespoke basis for each agreement. However, if there is an element of consistency and the changes can be reduced to variables that merely need to be completed for each agreement (i.e. the core logic of the agreement/code does not change), then the benefits of automation are likely to be more readily achieved.

The extent to which automation is achievable also depends on the interaction between the smart or automated contract and third party systems or records. For a simple example, the triggering of a payment would involve the smart contract being connected with the banking solution to trigger an automated payment. To achieve the full benefits of automation, this would have to be capable of being completed without manual human review, but an intermediary step may be the generation of automated payment instructions with a human review before final instruction of the transfer. This can be achieved programmatically, and automated connections with the bank's computer systems enable direct communication to effect the transfer. This approach can also be extended to situations where a definitive ownership record which can be updated by the smart contract exists – for example, title to land which is recorded on a land register, and the smart contract can instruct a transfer of title from one party to another, which is then recorded on the register.

[5] For discussion of the technical causes and potential impacts of algorithmic decision making and automation on individuals, see for example the same discussion in respect of artificial intelligence by the Australian Human Rights Committee: 'Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias', available at: https://humanrights.gov.au/our-work/rights-and-freedoms/publications/using-artificial-intelligence-make-decisions-addressing

Greater difficulties arise where the action requires an action in the real world, or where the action cannot be definitively achieved by a computer system with which the smart contract can interact. For example, the ownership of many assets is by possession or chain of title rather than a definitive ledger, and where certain assets such as cars are registered, such registrations are not definitive evidence of ownership. Automation then relies on either trusted third parties holding the asset concerned (for example, title to certificated shares) or interaction with the physical world (such as physical delivery of an asset), and would therefore be dependent on certain codified, triggering actions occurring to enable completion of the smart contract. This may require changes to the existing methods of carrying on business, some of which may be beneficial in the longer term, while some may not be attractive and therefore would limit smart contract adoption.

2. Do you agree that the Law Commission's scoping study on smart contracts should be limited to contracts which use distributed ledger technology? If not, please provide details of other technologies which are used to support smart contracts, and their prevalence. (Paragraph 2.26)

Distributed ledger technology (**DLT**) is a name that can be applied to a broad church of architectures and platforms some private, some public, some with channels, some with a single ledger, and some permissioned.

Given that smart contracts are shared and may often be or become highly valuable or critical digital assets, DLT architecture in its broadest sense is the most suitable given its immutability and its distributed nature. Having said this, this may not always be the case and other technologies may arise in time that are more suitable. We note that the less nodes involved in securing the network, the greater the actual or perceived risk of censorship and the more nodes (and thus, decentralisation) involved, the greater the actual or perceived benefits of censorship-resistance (i.e. true immutability).

It is helpful to consider through a legal lens, the preferred features and characteristics of a suitable digital platform required to best support the successful hosting and operation of traditional contracts as software. We have seen the emergence of various smart contracting platforms for specific use cases, however a more efficient course forward for enterprise and government use may be to develop national industry-agnostic digital infrastructure (rather than an industry vertical) that provides a cyber-secure, interoperable protocol for contracting and legal instruments. The *Digital Infrastructure Integrity Protocol for Smart and Legal Contracts* (DIIP 2021) sets out the "minimum best practice requirements and recommendations for any high integrity digital infrastructure or enterprise platform (**EP**) intended to support smart legal contracts"[6] which include:

> ***"1. Confidentiality, Privacy and Permissioning***

[6] Garside, Ariane and Wilkinson, Susannah and Blycha, Natasha and Staples, Mark, DIGITAL INFRASTRUCTURE INTEGRITY PROTOCOL FOR SMART AND LEGAL CONTRACTS DIIP 2021 (March 30, 2021). Available at SSRN: https://ssrn.com/abstract=

The EP should enable appropriate permissioned access to, and actions in respect of, the contract.

If an EP is hosting a Smart Legal Contract for a party, the EP should allow all authenticated parties to the Smart Legal Contract to be able to, at a minimum, have a reasonable access to view the contractual rights and obligations of that contract, whether expressed in natural language or in code (or in both).

The EP should allow all parties to agree how to control and manage data generated by the Smart Legal Contract.

The EP should support robust and rigorous identity access management with appropriate controls and standards applicable to the use of any sensitive data (including biometric data) or special classes of people (including those not legally able to contract).

The EP should ensure confidentiality of the contract including in respect of the contract's existence, contents, history and controls. The EP should also implement controls to preserve the privacy of parties identified in the contract, and not share their personal information without consent with third parties.

2. Access

An EP does not have an obligation to host any contracts that are outside its commercial or technical domain of speciality or business model, however if all other DIIP and EP requirements are met, the EP should host any or all contract(s) uploaded and paid for by a user.

3. No change to contract without counterparty agreement.

The EP should ensure that no party to a Smart Legal Contract can form, vary or amend the contract without the agreement of the other parties.

4. Data

The EP should collect and record only the minimum amount of individual user data that is required to run the EP and the Smart Legal Contracts it hosts. To the extent possible, the EP should minimise the use of data other than for the purposes intended by the parties.

If the EP collects and uses data for the purposes of internal systems and processes, those systems and processes should be in accordance with minimum standards and sound practice guidelines.

5. Cybersecurity

The EP should have appropriate levels of cybersecurity for the nature and contents of the Smart Legal Contracts it hosts, and to enable their proper performance without unauthorised third party interference.

The cybersecurity of the EP should be supported by practices, procedures, and systems compliant to ISO 27001 (or its equivalent).

> *The EP should implement industry-standard safeguards and procedures to prevent unauthorised access to and the destruction, loss, misuse or improper alteration of information managed by the EP.*
>
> ***6. Portability, Interoperability, Reliability, Availability & Suspension***
>
> *The EP should provide a technical capability for portability of the contract (including natural language, connected code, and data that form part of the contract) and interoperability with other platforms and digital systems, including platforms in other jurisdictions.*
>
> *The EP must make available to users information about expected and target hosting service reliability and availability, and recommend to parties to establish a business continuity capability if there are unexpected service outages, regardless of how the party's inability to access to the service arises.*
>
> *The EP should give weight to the special status of the contract before terminating the hosting of a Smart Legal Contract. If an EP account is not paid on time and in full, and the parties have not communicated consent for an EP account to be terminated or a contract or contracts digitally destroyed, the EP should take reasonable steps prior to suspending or terminating an account or contract to give notice to the party or parties informing them of the coming suspension, termination or destruction.*
>
> ***7. Legal & Jurisdictional***
>
> *The EP should be compliant with all applicable laws within the relevant jurisdiction, including consumer laws, cybersecurity, privacy, data collection and breach and other regulatory requirements. This includes laws that apply to the EP itself and to any extent applicable to the digital assets on the platform, including the Smart Legal Contract."*

These features may also provide courts with a useful framework for relevant issues to consider when making determinations about the context, running and enforceability of smart contracts, as the choices made by the parties in respect of the platform or system that runs a smart contract, as well as the nature of the platform or system itself, will influence interpretation of the contract.

We anticipate that the rules and governance of a platform will necessarily influence to some degree the terms of a smart contract running on that platform. For example, a permissioned platform's requirements in terms of access, permissioning, and authentication of users may impact on a party's ability to freely novate a contract on that platform. Or whether a contract can be amended to reverse or suspend a particular part of the code will indicate whether the contract's running is intended to be irreversible and immutable (similar to, for example, smart contracts on the Ethereum blockchain). In the same way that clauses that specify the jurisdiction import certain legal obligations or requirements into the terms of a contract, so too in time, could the platform design and platform rules impact the terms of the contract.

3. When, and why, do parties to smart contracts decide to use: (1) permissioned DLT systems; (2) permissionless DLT systems? (Paragraph 2.29)

Different systems will appeal to different use cases. Permissioned systems are generally used when there is no issue of trust between the parties, and all of the parties are identified and granted access to the system. This can commonly be seen through the evolution of existing processes which parties are already confident meet their requirements (i.e. they are already entering into the relationships on the basis of reputation and regulation to ensure trust). Smart contracts are used in permissioned systems for improved efficiency and lower transactional risk that can arise from human error or single human misdemeanour. However, there will typically be a gatekeeping process where a permissioned system is only made available to trusted counter-parties – i.e. trust is not the issue being solved.

Permissionless systems are used where there is systemic mistrust, i.e. in jurisdictions and situations where there is little faith in the integrity of the parties nor in the regulatory system or public institutions.

Permissionless systems are designed to avoid the need for trust in the first place – for example, a bitcoin wallet can be identified from the wallet address and the balance checked against the state of the distributed ledger. The private key is supposed only to be known to the holder of the wallet, and the design of the system is such that transactions signed by the private key are definitive. As such, in a simple payment transaction, there is (theoretically) no need to prove that the owner of the wallet is the owner (this is verified, in theory, by knowledge of the private key) and that the wallet has the requisite amount in it to complete the transaction (this is ascertainable from the ledger).

While this avoids the need for a central authority trusted to maintain the ledger, the disadvantage to this approach is it requires a level of transparency which may be unattractive (i.e. everyone can see all the transactions – albeit pseudonymous transactions – on the ledger) and a wide consensus is required to ensure the ledger is not manipulated by an individual party. The pseudonymous nature of the permissionless system started with a libertarian idea that the ledger is definitive and free from outside interference. However, this presents practical difficulties in constructing and maintaining a system which is both definitive, and provides remedies for abuse and privacy.

Looking to the future of wide-scale adoption by businesses and government in general commercial use, we expect the unique benefits of permissioned DLT systems to be a deciding factor in choice of system.

For further reference, see also our discussion of some critical features and principles of a smart contracting platform in our response to paragraph 2.26, as these may influence the choices of contracting parties.

4. Which of the three forms of smart contract discussed in para 2.32 of the call for evidence are most commonly used in existing smart

contracts or smart contracts which are in development? Please provide examples of how these forms of smart contract have been used in practice (Paragraph 2.39)

The three forms of smart contracts proposed in the Call for Evidence are a useful starting point for the analysis of smart contracts, however further distinctions may be useful for completeness. For example, the assessment is not necessarily one of degree of automaticity agreed between the parties, but rather agreement as to whether and where the boundaries of the legally enforceable agreement are drawn between the natural language and code.

The three forms of contracts proposed stem from an assumption that each clause should *either* be expressed in natural language or in code. We understand there to be an additional approach that allows a given provision to be both expressed in natural language and mirrored or extended (wholly or partially) by code, providing additional flexibility and freedom for the parties to legally agree associated matters relating to the code such as risk allocation, and in particular whether the code or the natural language take priority in terms of legal obligation.

The distinction should be made under the form of hybrid contracts between the Paired Method and Unified Method (see response to question 1). This will also help to address the confusion that can be generated when classifying the contract as a whole, rather than a decision between parties as to whether, on a clause by clause basis, the code or the natural language would take priority. Indeed, as indicated above, often code or automation is designed around a contractual process that may touch on several clauses (e.g. form of notice, delivery requirements, consequential payment requirements and milestones may each be set by a differing clause, but a single piece of coded automation allows for the tracking of a delivery, notification and consequential payment for a given delivery, and identification that a project milestone has been achieved based on delivery status, recognising that each of the relevant clauses may also contain legal content and obligations that are not captured in that coded process).

Natural Language contract – in which some or all of the contractual obligations are performed automatically by the code of a computer program deployed on a distributed ledger. The code itself does not record any contractual obligations, but is merely a tool employed by the parties to perform those obligations.
This form would apply where performance of at least part of the contractually agreed terms expressed in natural language are subject to some automation, but the parties agree that such code does not constitute part of the contract capable of breach.

This form and approach may have some appeal in the early days of contract digitalisation due to the fact that the code effectively sits outside the bounds of the legal agreement and is simply a means of performance, not capable of breach. This avoids the legal complexity of many of the questions raised in this Call for Evidence as any coded performance of contractual obligations would be akin to that under traditional contracts (e.g. direct debit payments).

The consequence of this approach though is to pass up the opportunity for parties to apply the flexibility and rigour of contractually agreed parameters in relation to the automated elements of their agreed performance. In other words, if the coded elements form part of the contract, key matters in respect of how the code operates in the performance of obligations can be contractually agreed and therefore legally enforceable between the parties (e.g. what happens if the data source fails, failure of code to execute as intended, who owns data generated by the execution of the code etc.).

Over time, the increased degree of separation between increasingly complex code and natural language will become progressively more problematic from the perspective of legal enforceability. This presents an unfavourable outcome in the mid to long term where the legal entity of the contract as evidence of agreement is divorced from the practical real-world digital performance of the same contractual terms.

Hybrid – in which some contractual obligations are recorded in natural language and others are recorded in the code of a computer program deployed on a distributed ledger (to varying degrees).

We note it is possible for hybrid contracts to cover situations where a given clause or obligation is expressed either in natural language, or code, or both. Where the hybrid contract sits on this spectrum of natural language and code will depend on the contract itself, for example, whether parties have elected, either wholly or on a clause by clause basis whether or not either expression of the obligations is legally binding and within the bounds of the contract. It will be vitally important for certainty and enforceability of smart contracts, for parties to make such elections clear in the drafting of the contract. See generally *‘Smart Legal Contracts: A Model for the Integration of Machine Capabilities Into Contracts’*.[7]

We see benefit in preserving the natural language components of a contract alongside the ‘smart’ components such as code, connections and other forms of contract automation, as the natural language provides a mechanism to provide certainty, including as between the parties of how to resolve potential conflict between natural language and code. Without clarity as to this, the risks of mistake or mismatch between the natural language and executing code have the potential to create issues in contractual interpretation, with parties taking differing positions on the impact of the natural language on the code and vice versa. This is particularly so given code – particularly in the Paired Method (see response to Question 1) – is unlikely to exactly align to the natural language. Code that is inconsistent with the natural language agreement may be construed as forming part of the ‘relevant facts’ informing interpretation, or where there are non-code elements of the contract which are relevant for determining the appropriate remedy, particularly where value judgements (which are difficult to codify) may be relevant. In addition, the entirety of the agreement reached between the parties can be recorded and stored in the same form – such that there is an audit trail which could be referred to in construction of the contract/considering disputes.

[7] Blycha, Natasha and Garside, Ariane, Smart Legal Contracts: A Model for the Integration of Machine Capabilities Into Contracts (December 7, 2020). Available at SSRN: https://ssrn.com/abstract=3743932 or http://dx.doi.org/10.2139/ssrn.3743932

Inclusion of boilerplate terms – similar to interpretation provisions – that provide for primacy of either the code or natural language to the extent of any inconsistencies will help to mitigate this problem, though contracts are likely to be interpreted by the court on a case by case basis such that these provisions – while of assistance – will not necessarily be the final word.

Code only – a contract that is recorded solely in the code of a computer program deployed on a distributed ledger. No natural language version of the agreement exists: all the contractual obligations are recorded in, and performed by, the code.

We do not see the third form of contract being likely to form a standalone legally binding and enforceable contract for enterprises and institutions in the near future unless lawyers are involved in the drafting or review of smart contract (and the broader schemes that they form part) to ensure sufficient legal wording is added in natural language text to the smart contract as well as other information and marketing dissemination interfaces such as websites and social media accounts.

Code only smart contracts may well have a significant role to play in automation of performance of obligations, but may fail as legally binding contractual representations Even where such instruments may form contracts (to a greater or lesser degree) the design of such smart contracts creates issues for contracting parties with different levels of understanding of the coded language, may cause unfair terms or low accessibility arising from the complexity and of the code (when not tied to or governed by more understandable and certain – to human parties – language) and is subject to limitations associated with programming languages, meaning this approach is largely only applicable to simple, highly deterministic agreements. In DeFi, a suite of smart contracts are generally designed to offer financial products to individual consumers (i.e. similar to business to consumer legal relationships) rather than between sophisticated enterprises and governments.

In summary, care should be taken to clarify, but not to oversimplify, the classifications. Applications will warrant individual consideration of what obligations should be automated, and parties will need to agree whether the automation is within the bounds of the terms of the agreement, capable of breach, and to agree related issues (such as control of data, ownership of IP, recourse and responsibility in case of API, code or system failure and so on). Naturally, most agreements will demand a hybrid approach, however this encompasses a broad range of agreements with varying degrees of integration and associated nuances.

5. How do code and natural language interact in hybrid smart contracts currently in existence or in development and which terms are generally coded? (Paragraph 2.40)

See answer to question 1 in relation to discussion of Paired and Unified Methods.

Other factors that may interact with the code and natural language are:

- the nature of the platform the smart contract runs on - see answer to question 2 in relation to the influence of platform on the terms of the contract; and

- the act of a lawyer reviewing and adding natural language text to a code only smart contract to assist with legal validity and interpretation of the smart contract – see answer to question 4 in relation to code only contracts.

6. What process do the parties follow (or plan to follow) in negotiating, drafting and entering into a smart contract?[8] (Paragraph 2.41)

Note: Please initially refer to our answer to question 1 in relation to discussion of Paired and Unified Methods, and question 4 on the three types of contracts as those include detailed consideration of key aspects of these issues.

There are multiple factors that will influence the process followed in negotiating, drafting and entering into a "smart" traditional contract. These include the nature of the "smarts", the history between counterparties, whether it is a bespoke contract, or adopting modular precedent or standardised clauses that have been tested and used previously.

In a bespoke business to business agreement, each party would likely have their own advisers (initially both legal and technological, though some convergence in time is to be expected) and therefore the costs for bespoke agreements are likely to be high until such time as model or standard clauses become accepted norms. However, as "smart" traditional contracts become more prevalent, established practice and model clauses and code will help reduce this burden, potentially with a final audit review prior to execution to give comfort to both parties that the agreement does what it says it will do, and has no unintentional consequences. By so doing, the burden of preparing a smart contract could be significantly reduced, and when considered with the potential lifetime savings brought by automation, incentivise their wider use.

In contrast, business to consumer or other contracts conducted on standard terms could see the benefit of automation more quickly, as the substantive logic of the agreement does not change from one transaction to the next. As such, these types of contract are more likely to see earlier adoption as there is a greater scope to realise the benefits of automation in the short term.

If the smart contract is modified within the relevant platform from inception to final execution, there is also the advantage that all changes would be tracked within the system for the lifetime of the contract, potentially with additional contextual information (such as the information provided by the parties prior to entry into the smart contract) being recorded if required. This would then be signed by the parties using their own private keys.

As an alternative to each party having their own advisers, it may become market practice to rely on a platform to provide the technical infrastructure and tools for the

[8] The call for evidence specifically asks to please explain in particular: (1) where all the contractual obligations are contained in a natural language agreement and the code is intended merely to perform those obligations, the practical steps involved in coding the parties' rights and obligations contained in the natural language agreement; (2) where the parties intend that there will be a hybrid contract or a code only contract, the practical steps involved in drafting, negotiating and agreeing the code of the smart contract; (3) where there is a hybrid contract, whether the natural language element and the coded element are entered into contemporaneously or at different times; and (4) the role played by third party service providers (such as computer coders and software firms) in this process

parties to achieve automation without the requirement for advanced technological skills. While initially contracts would likely be bespoke, once a library of standard clauses is created, there is an increased opportunity for ‘DIY’ platforms using these pre-vetted modules to construct agreements.

A further critical issue from a traditional law firm perspective is the practical implication of risk allocation, insurance coverage and contractual structures where assisting with coding internally or outsourcing coding. In particular, whether coding will be offered as part of an integrated service by law firms or by third party service providers, or technical expertise within the client. Multi-disciplinary insurance coverage will be key here, and the appetite from insurers around the world in relation to emerging technologies and their risks is still extremely conservative.

We submit that there is strong grounds for an approach to drafting in the Paired approach, that is, a conjoined manner, that links code to natural language where the natural language is contractually agreed to have primacy over the corresponding code. This will be required for commercial or enterprise grade contracting in the broad sense allowing for certainty and understanding in relation to the intention of the parties.

7. Are you aware of any examples of use cases for smart contracts beyond those we give in the call for evidence, or variations on the use cases we give, which are being developed, are at proof of concept stage or are already operational? (Paragraph 2.64)

We do not have direct knowledge of smart contracts in operation beyond those in the Call for Evidence. There are various examples in the market of unilateral automation but we could not consider these to be smart contracts in the way that term is defined for the purpose of this Call for Evidence. Some examples of such initiatives that may merit further review that we come across through publicly available information include:

- Smart flood insurance – example given by Lloyd’s of a smart insurance ecosystem. This is intended not only to automate payments/calculation of premiums, but also to operate as a personal risk management mechanism by way of a system of notifications sent to the insured.[9]
- Leasing - facilitating automated payments, for example rent and return of bonds, as well as verification (highly valuable in lease market).[10]

[9] See Lloyd’s, *Triggering innovation: How smart contracts bring policies to life* (Emerging Risks Report, 2019), page 18.

[10] Robert Size, ‘Taking Advantage of Advances in Technology to Enhance the Rule of Law’ (2017) 91 *Australian Law Journal* 575, 580-581. Note: at the time of drafting this submission we are unsure how developed this application is, though there is some industry commentary: https://deloitte.wsj.com/cfo/2018/01/03/blockchain-and-smart-contracts-could-transform-property-transactions/. See also https://www.lexology.com/library/detail.aspx?g=b257ef57-4296-4f2a-a327-f34441a58b5d

- Insurance-linked securities transactions – 2016 Allianz trial involving natural catastrophe swap transaction.[11]

8. What benefits and cost savings can smart contracts provide compared with traditional contracts? Will increased use of smart contracts lead to any additional costs? Please provide details and any available qualitative and quantitative evidence (Paragraph 2.66)

In principle, the implied benefits of any machine-readable and rule-based self-executing contract, including ledger-based smart contracts, lie within the realm of automation efficiencies, speed of transaction or actions taken in response to a specified trigger, immutable record-keeping, structured data generation and capture, process optimisation, standardisation, risk mitigation, and value creation.

Assuming that open, interoperable standards become established (and adopted) so as to enable contracts to be accessible, a key benefit will be that all the parties associated with the contract would have secure unfettered access to the contractual record, and have certainty as to the true version and status of a contract.

In the case of a single static agreement where any amendments, additions or access logs would usually be infrequent, and which does not have any automation or code, then the cost-benefit of the smart contract is less significant at a micro level, but may offer value at a macro, enterprise level as it enables stronger record hygiene, searchability and analysis capabilities across the contract load. The cost-benefit analysis of including code and automation in a single contract must be done on a case by case basis, and acknowledging the higher costs of creating those initially when platforms, skills and precedents are less developed. However, if most of the construction of the contract can be automated and the use of an open library containing tried and tested contract formulas, including pre-formatted articles in both natural language and computer code, then the unit cost could drop dramatically and the quality of the contract increases.[12]

Based on our experience of current vendor development and market readiness, the most likely and accepted end-state for commercial-scale adoption is centred around the notion of a living, dynamic smart contract that contains agreed executable rules and decision-based logic between multiple parties within the context of an end-to-end business process containing multiple procedures. The executable actions can be a mix of digital automation and human tasks, but the intention in some cases is to minimise or eliminate human intervention, labour or error rates. The key benefit of this aspiration becoming realised centres around real time, frictionless, secure and faultless processing. Should this vision be fully realised where the smart contract becomes the single point of truth as between the parties, then the cost-benefit for an appropriate use case is significant. Apart from dramatically reducing the transaction costs of mutable market supply chains, the time frame of completion involving multiple stages of, say, purchasing a property could be, according to vendors, reduced from months to

[11] See Jonathan Gould, 'Allianz Expects Blockchain Tech to Expedite Cat Bond Deals', *Insurance Journal* (Web Page, 15 June 2016) <https://www.insurancejournal.com/news/international/2016/06/15/416971.htm>

[12] For example https://www.openlaw.io/ is working towards such outcomes.

seconds. This approach also negates the need for a supply chain to pay the very high cost of centralised system integration of all the computer systems associated with the tasks prescribed within the smart contract.

Beyond the practical-level benefits outlined above, on the macro-scale the key benefit that a well-integrated, well-functioning smart contract economy will provide is the capacity of the smart contract to integrate law and legal structure into the evolving digital architectural landscape which our economics are becoming significantly and systemically dependent upon. A wicked problem currently exists that inhibits our cities and regions from benefiting from the ongoing digital transformation journey of economic activities. This problem centres around moving from the waypoint of interconnectivity we enjoy today, towards fully automated, efficient, and effective sectors where digitised market liquidity becomes a possibility. The construction of digitally-created tradeable assets, through legal instruments such as smart contracts, can produce new types of capital to strengthen our fragile post-COVID economies, whilst laying down the foundations for greater resilience to shock, as they enable stronger data flows and reaction times to allow economic activity to prepare for and respond to such shocks.

What is still required, however, is evidence of meaningful, validated impacts upon individual actors, business, market sectors and economies of the claimed benefits within the broader context of the use of smart contracts. Without such evidence, it is important that any regulations or legal structures created to deal with smart contracts are structured to accommodate a broad range of methodologies that achieve similar outcomes, rather than being limited to a particular conception or preconception of ‘smart contracting’, in particular one that is founded on use of blockchain or DLT systems.

In the absence of properly developed, (most likely private and permissioned) smart contracting platforms, clear and quantifiable smart contract efficiency data is difficult to find and cost savings on public blockchains need scrutiny (particularly if moving into enterprise complexity and large volumes of transactions). This is particularly true where the currently available technical solutions (public blockchains and off-chain solutions) are not considered safe or appropriate for smart (and legal) contracts. Yet, due to the higher cost and complexity for contracts and the associated records to be stored on a chain for some forms of blockchain, currently the majority of the data is kept off the chain.

The estimated cost ratio of programming on public blockchain systems was around one million to one when compared to programming in Java. This dichotomy presents a real problem of scalability, environmental impact and cost. The Ethereum blockchain has set out to solve this problem by increasing the number of chains, switching to a proof of stake model and eventually creating a greatly improved smart contract model. The time frame for this is not clear, but the indication is that we are a few years away from the problem being solved in respect of Ethereum or other public-style blockchains. It may be wise to determine the time frame as well as the probable costs before making any assumptions that may impact any regulation.

The acid test is how much would it cost to create and operate a live smart contract in the context of a supply chain of, say, purchasing a home when every execution of a rule or decision has to be added to the chain. Just the cost of making an addition to the chain can (historically) cost USD 20, for these styles of public chain. This then gives rise inevitably to the question of what the total cost to the industry would be when every automated transaction is charged by some sort of blockchain middleware service. We cross-reference the central bank digital currency (**CBDC**) discussion at this point to note that the data and transfers of value associated with the movement of goods and services through a supply chain could be captured by a domestic CBDC that is interoperable with other country CBDCs. Latest research by the Bank of International Settlements suggests that within the next three years, general use CBDCs will be issued to at least one third of the world's population. Absent legal certainty and clear smart contracting legal principles, perhaps inhibiting enterprise and corporate uptake of smart contracting, the momentum of CBDCs will add pressure to the need for certainty and clear principles around smart contracts that allow for the programmability of CBDCs.

Following on from these concerns, we anticipate other market (or publicly financed) solutions will emerge that leverage greater efficiency and economy to solve for this problem. In particular, styles of permissioned or hybrid DLT structures that do not require the more intensive processing power or architectural structures required to sustain the particular 'trustless' nature of public blockchains.

A traditional cost-benefit analysis cannot answer the question of '*will it work*?'. This is because a positive benefit may well be indicated, and yet, when the context of using a smart contract is factored into a value equation, the result may be a negative value to critical parties whose participation is required for a critical mass of adoption. Again, this is where we suggest that there may be a case for public investment in securing the future of platforms that support secure legal instruments. Like the governments have responsibility for road and rail infrastructure, so too is the case becoming increasingly urgent and compelling that governments should have responsibility for secure and reliable digital infrastructure.

Ultimately, while there are benefits to the utilisation of smart contracts, the practical consequences of adding contracts to a public-style blockchain with high processing power requirements is to result in significant energy resource production that, for the foreseeable future, will impede scalable adoption. A key factor in assessing the value of smart contracting moving forward will be the nature of the DLT or other systems and platforms available to enable it. For more on this, see our answer to question 2 above, which outlines some of the key requirements for any such smart contracting system of scale.

An example of how smart contracts could have a beneficial impact at scale upon the public sector centres around the need to determine the correct address when establishing an account, with such data then being used to process any customer-centric service such as eligibility, status and request.

Despite significant investment by governments worldwide on centralised identity management systems, establishing a single point of truth devoid of risk remains elusive.

This problem is exacerbated by centralised systems' inability to enable a customer to update all governments’ records of a change of address with sufficient confidence by all parties that all required legal processes or obligations have been met and recorded accurately.

A smart contract structure may enable a tell-it-once capability within a government department and allows multiple systems across government (and beyond) to interact with a single point of truth without the high establishment cost or overhead of complex systems integration.

FORMATION OF SMART CONTRACTS (CHAPTER 3)

9. In what ways can parties reach an agreement through their interactions on a distributed ledger? (Paragraph 3.13)

There is no technical reason that a bespoke and well-designed smart contract platform cannot support parties to reach legal agreement in the same way as they do now. Particularly if that well-designed solution allows for the organic interaction of natural language and code. Whilst the way parties reach agreement now is familiar, we question whether it is the best way for all members of society. The only difference between current practice and agreement on a well-designed DLT solution is that digital legal execution and performance events would be recorded, such that they would create a single source of truth of that agreement's lifecycle (audit trail). This is conceivably superior to the current analogue method and will for example, be of great use in supporting legal variations.

Much depends on the technical or legal 'rules' established by the underlying DLT, or platform, either through technical design or terms and conditions which set out how users may interact and transact with each other. Parties' level of knowledge, acceptance and use of these rules and systems will influence interpretation of whether an agreement has been reached. In contrast, in code only smart contracting platforms like Ethereum, there continues to be heavy debate between what prevails when something goes wrong: "code is law", "code of law", or "intent of code is law"? We are aware of one matter proceeding through an Australian court that is considering the applicability of "code of law" where an Australian regulator has a published view that effectively endorses "code is law".

Moving to consideration of public blockchains and how they might help (or not help) parties reach an agreement, they can technically replicate existing processes for reaching an agreement, and mimic any type of decision and rule table to fully automate the interactions between parties, including reaching an agreement. Often times though, the parties will need to include human decision making as required as part of the transaction when full automation is not possible or preferred. To date, the Ethereum-based smart contracts used in DeFi and entertainment/gaming, are purposely one-directional - there is no party to negotiate with because a person merely interacts with the smart contract code. Whilst there is no negotiation, an increasing number of consumers are attracted to the simplicity, transparency and affordability of DeFi notwithstanding the cyber risks associated with smart contracts. A suite of smart contracts can be designed and deployed to operate as a decentralised application (dApp). Decentralised models of governance have become the mechanism for negotiation, whereby code-literate users of a DeFi application can submit a proposal to the governance council (usually a group of people elected by the governance token holders) to change an element of the smart contract that results in a better or fairer DeFi offering. If the proposal is voted in by the council, the new smart contract is deployed.

The reality is that when most people speak about a smart contract (particularly in the computer science or coding domains) they are referring to self-executing code on a public blockchain – more often than not, what they are describing does not have all the features of a legally binding agreement, nor is that what they are intending to create. In this instance, the smart contract is more like the automation of an operative clause, rather than a whole contract.

The following examples gives colour to the smart contract versus smart (and legal) contract distinction as it sets out the automated clause (rather than legal contract) method. The scenario in paragraph 3.6 assumes that Bob is code-literate and understands the application of a public blockchain. However, consider the example where Bob is not code-literate. In such a case, Bob needs to interact with Alice's smart contract through a user interface, like a website or an app to do the specified actions (e.g. send ETH, receive X token). In this example, the assumption is also made that Bob would send ETH and receive an ERC-20 standard token in return, unless Alice's smart contract was sophisticated enough to enable cross-chain token swaps. The addition of a user interface in between Alice and Bob may introduce complicating factors in the formation of the agreement.

Some similar real-world "smart clause" as a "smart contract" examples include:

1. Purchasing non-fungible tokens (NFTs) on a virtual marketplace (e.g. OpenSea or SuperRare). Bob identifies a collectible he likes on the marketplace. Bob sends ETH to the site and receives a unique NFT in the same ETH wallet. The NFT represents whatever rights or attributes are associated with the collectible. Sticking to the scenario, let's assume Alice coded the smart contract that facilitates the transfer of NFT tokens to a buyer's ETH address.

2. Alice developed the smart contracts that enable liquidity providers on decentralised exchanges (**DEXs**) to contribute both sides of a pair to an existing or new liquidity pool (e.g. an ETH-YYY pool) and for persons to subsequently interact with the liquidity pool to swap ETH for YYY token, and vice versa. Here, Alice is the equivalent to Hayden Adams of Uniswap. Bob sends a specific amount of ETH and understands that he will receive the equivalent spot value of ETH he sent in YYY token. Bob receives YYY tokens to the same ETH wallet he sent ETH from (same as the NFT example above).

In both of the above scenarios, it cannot be expected that Alice assumes, expects or knows that Bob will buy the NFT or YYY tokens. Alice altogether has a minor role in enabling the transactions to occur on the platforms by virtue of coding the smart contract. It can be argued that Alice had no direct role in any agreement that Bob may have reached with the platform to receive the NFT or the interface to receive YYY tokens. Rather, the smart contracts allow users to "self-deal" by interacting with the smart contract in only the way the smart contract permits.

The NFT marketplace or DEX may be making an offer to treat to the world at large by offering users the opportunity to purchase an NFT or a token listed on a DEX. An argument can be made that when a platform user or website visitor signs the transaction (e.g. 'Confirm' the transaction in Metamask, a browser based wallet), they are accepting the offer.

Consider the scenario where an NFT or a token on a DEX is no longer available. However, the platform or interface shows that the NFT or token is still available, so the user assumes the NFT or token is available. This might be an interface fault, an attempt at fraud by malicious actors, or a lag between updating the interface with information from the underlying distributed ledger. The user proceeds to sign the transaction. If the NFT or DEX token is not available, the transaction will fail and the offer will be rejected. The smart contract can't issue something that doesn't exist. In some cases the ETH required to fund gas that fuels the operation of the smart contract will be expended.

10. Are you aware of programming languages which are specifically designed to enable parties to reach agreement on a distributed ledger? If possible, please give examples of the circumstances in which they could be or have been used (Paragraph 3.14)

The DAML example in paragraph 3.12 just allows for an offer to be made to a specific user. We do not consider that a specific programming language is necessary to reach agreement on a distributed ledger. Rather, for DeFi applications with decentralised models of governance, generally an author of a proposed change or upgrade to a smart contract is responsible for gathering consensus from within the DeFi application's community and collating dissenting opinions before the proposal is put up to be voted by the governance council. Such "soft governance" is human-led, largely through social media channels and video calls with interested parties.

There are programming languages we have seen that are designed to help parties reach an agreement on a distributed ledger. There are some programming languages that can help form and run smart contracts which may be used in conjunction with a distributed ledger. Specific programming languages for smart contracts should not be necessary if drafting contracts on a well-designed smart contract platform that supports natural language and a low code environment.

The Linux Foundation's Accord project has developed the Cicero and Ergo programming languages targeted at legal use cases. To our understanding, these programming languages, despite their being targeted at legal use cases, have not been widely adopted by Australian law firms.

11. Do you consider that offer and acceptance can occur through the operation of autonomous computer programs deployed by the parties on a distributed ledger? If so: (1) in what circumstances? (2) on what legal basis? (Paragraph 3.20)

There is no technical reason that a bespoke and well-designed smart contract platform cannot support offer and acceptance in the same way as an offer is made and accepted now. The ability for truly autonomous computer programs to do this may not be useful, or necessary in most enterprise to enterprise or enterprise to government circumstances. In fact, in these cases the law is probably best served in the conceivable future where offer and acceptance are still human in the loop features –

particularly of an original genesis legal agreement that underpins future contracting cycles (variatinos) and performance of obligations under a legally binding agreement.

It is theoretically possible for the operation of the autonomous program(s) to amount to offer and acceptance, particularly where a human has sanctioned the originating cycle of contract. The parties remain the parties with the autonomous program enacting actions according to the underpinning logic and criteria which the parties have set (or at least agreed to). There may be circumstances where a party argues that the logic of the programs did not operate as intended resulting in a potential issue or mismatch in the offer and/or acceptance. This is particularly a risk where the autonomous computer program is not created, owned or operated by the party, for example where it was programmed by a third party, or a platform provider. It is important to consider – particularly for mistake in formation of contract – which is the relevant state of mind; that of the party, or the programmer? See also the case of *Quoine Pte Ltd v B2C2 Ltd*.[13]

Some further questions to consider include: what the broader policy impact is of differentiating between human actors and autonomous programs? In these types of cases, where an autonomous program is acting on behalf of a human or corporate actor, responsibility can still be traced back to the legal personality. However, there are likely to be cases where parties argue that autonomous programs did not act on their behalf, or where autonomous programs act on their own behalf. In what manner can such actions still be traced to a legal personality or structure?

12. How common is it for parties to enter into smart contracts on a DLT system without knowing each other's real identities and in what circumstances is this likely to arise? Paragraph 3.25

Commercial, traditional contracts

A bespoke and well-designed smart contract platform would have sophisticated permissioning, identification and authorisation of those parties who are users of smart legal contracts. See DIIP 2021 (set out above) that defines this as a critical element of a high integrity platform.

While there may be certain use cases for pseudonymity in smart contracting, either deliberately or because identity is immaterial to the nature of the transaction, for smart contracting to be the evolution of commercial contracting, identity will be a prerequisite for legally enforceable smart contracts absent some other safeguard in terms of remedies in case of breach. Where sophisticated contracting parties are using smart contracts for the benefits of automation, the use of their real identities is not generally raised as a threshold issue.

Ethereum-based smart contracts

Knowledge of identities or at least, blacklisted and whitelisted addresses is a threshold issue for DLT system transactions. It is common for crypto-literate persons to interact

[13] [2020] SGCA(I) 02.

with the smart contracts on a DLT system not knowing who the original programmer was or if the smart contract is subject to a proposal for change. Until recently, a number of decentralised applications (**dApps**) were designed as peer to contract (e.g. MakerDAO) whereas now we are seeing a proliferation of dApps designed as peer to contract to peer (e.g. Aave, Uniswap, Sushiswap). Whilst the P2C2P smart contracts raise concerns about "washing" (i.e. an attempt to clean laundered cryptocurrency) because they are similar in function to mixers and tumblers, crypto-literate persons continue to interact with the smart contracts because of the yield (or return) available from the interaction. No agreement is entered into per se; rather, persons interact with the smart contract because of the actual or perceived clarity and simplicity of the mathematical and financial functions. Identity is not currently a prerequisite for most dApps (although this may change soon based on latest proposed FATF recommendations) but is required at the point of obtaining insurance cover for loss suffered from a dApp through offerings like Nexus Mutual.

In addition, most order-book based digital currency exchanges do not reveal any identifying data, nor the wallet addresses, of the counterparties to a trade.

The following component of our response is a discussion on identity in the absence of a bespoke smart contract platform and using public blockchains e.g. for Bitcoin or Ethereum where identity is generally considered to be pseudonymous and can be a road block to legal dealings.

Current use (cryptocurrency):

The onus on ascertaining the identity of the other contracting party, if necessary to know the identity at all, is generally held by the offeror. For example, if one person wants to send cryptocurrency to a specific person, they should do their due diligence to ascertain the correct address of the recipient person. Similarly, if a person needs to interact with an exchange or a platform, they will obtain the relevant address from the exchange or platform's website. Outside the case of airdrops, it is extremely rare for people to send cryptocurrency to random addresses. Individuals generally do their due diligence and small test transactions to ensure that the address belongs to the intended recipient. And if it is incorrect, the loss is borne by the offeror/sender.

Digital identity initiatives may link DLT addresses to particular individuals in the future. ENS names on the Ethereum blockchain come close to a global digital identity service, but ENS names can be claimed by anyone, so it is not a reliable form of identification.

Key principles and practical concerns for the future

CBDC discussions continue to draw attention to the anonymity of cash and an individual's right to privacy by choosing to use cash rather than other means of payment that involve the capture and sharing of data about transactions. Each country's design of their general use CBDC will have to make a trade-off between appropriate surveillance and anonymity.

The question of pseudonymity and anonymity of commercially transacting parties is somewhat premature, because the use of smart contracts is still at such an early stage in the market and is not often intended to be trying to capture a formal legal commercial agreement. So many commercial agreements currently are formed using an individual's or entities' real identities. To create the ability for individuals or entities to engage in a smart contract transaction anonymously (to replicate cash transactions) would require a philosophical shift from how the parties commence commercial contracting in the first place.

Practically speaking, the extent of knowledge each party to a smart contract has of the other's identity depends on the compliance requirements for the DLT system: for example, with Public Key Infrastructure, as long as a party has established and recorded bono fides status by a given authority, then the requirement of the system is simply to ensure the same party originally identified is the same party as the one transacting. Anonymity or the use of personas are common in the current use of, for example, cryptocurrency-related smart contracts, but for broader usage, the use of identification requirements will likely be stipulated by the requirements of the legal agreements and not by the constraints of the technology itself. For example, the requirement to include a witness for certain types of agreements or deeds may be a limiting factor on maintaining anonymity within a smart contract on a DLT system. Finally it is important to note that total anonymity is considered to not generally be possible due to the systems that can observe other systems and deduce identification details.

13. What evidence might be available to a court to establish the identity of the parties to a smart contract entered into pseudonymously on a DLT system? Paragraph 3.26

In general business contracting, private and permissioned DLT systems are likely to support some form of identity verification to promote more traditional business interactions between known counterparties. This could be achieved using third party KYC providers who verify identity and add data to the DLT system to demonstrate the identity has been verified. This approach is not without issue, however, as the compromise of private keys to a system would allow an actor, other than the person who has been verified, to conduct transactions on the network under the guise of being the verified person. There are various mitigation techniques (such as two factor authentication, key rotation, multisignatory requirements for transactions on behalf of legal entities, etc.) that can be used, however the definitive link is between the account and the private key rather than the individual concerned.

The compliance requirements set out by a particular generally public DLT system or platform for the establishment of a user account will form the extent of the information available to a court to (seek to) establish the (true) identity of the parties to a smart contract. If the account establishment requirements permit pseudonyms or the hiding of true identities then the court will be limited to being able to identify the details of the pseudonym as verified at the time of establishment of the account.

That being said, numerous companies specialise in chain analysis, and can accurately link addresses to individuals, particularly if the address sent funds to an exchange or platform that performed Know Your Customer (KYC) or other forms of regulatory identity checking. If, however, the tokens belong to a privacy-centric blockchain like

Monero or Oxen, or if the tokens are sent through a mixer or peel chains, it is much more difficult to trace the identity of the owner of an address.

However, we note that it is highly unlikely that an individual will send tokens to a random address. If a platform lists the incorrect address, and the sender sends tokens or interacts with the incorrect address, the next step would be to track down the individual responsible for the platform, or the individual responsible for providing the incorrect address, which may provide the necessary information. In addition, the recipient address could be watched to identify where and when tokens are moved and to which other wallet addresses.

Courts or parties looking to establish the identity of a pseudonymous user can employ tools such as: investigating who registered the website, engaging a chain analysis company to track down where the funds were sent to onward from the incorrect address, and examining the public social media profiles of the platform.

14. Are you aware of, or do you foresee, any difficulties in applying the law on consideration to smart contracts? If possible, please provide examples. Paragraph 3.30

If participants of a smart contract want it to be legally binding in a common law jurisdiction they should endeavour to satisfy the element of consideration. We see no reason why smart contracts should not accommodate this, either through the smart contract code or through natural language.

In the context of smart contracts as used for the purposes of this Call for Evidence, there is no reason why parties to a smart contract cannot establish consideration in the formation of a legally binding agreement, although it will require express agreement by the parties, and most likely best practice will require this to be included in natural language provisions of the smart contract. An appropriate digital platform that supports formation of smart contracts should also provide for payment infrastructure to support payment and evidence of consideration under the smart contract.

However, where automation or code is enacted between two parties and is only one part of a wider business transaction or relationship rather than being documented in a smart contract, it may be difficult to establish that consideration was paid in relation to the automation. In such cases, the arrangement would fall short of the legal requirements for a smart contract due to the failure to establish consideration.

In the context of current DLT users, many if not most do not consider DLT transactions to be legally binding contracts, which is the key difficulty in applying the law on consideration to current uses of those smart contracts. Users are not occupied with satisfying all contractual elements, and ensuring the transaction is legally binding. Rather, users of these system expect the code to execute what it says it will execute when a certain act is performed. In addition, there are not traditional counterparties in a smart contract arrangement – a person interacts with smart contract code that has been deployed to a DLT system secured by a decentralised network of nodes.

15. Are you aware of, or do you foresee, any difficulties in determining whether the parties to a smart contract have reached a certain and complete agreement? If possible, please provide examples. Paragraph 3.35

The complexity of the technological processes and technology stack which support the running, and indeed the existence, of a smart contract are a potential source of uncertainty. Where the contract itself only exists on a digital platform, there becomes a question of what exactly comprises the content of a smart contract: is it just the agreed code and contents of the contract, or the underlying technology stack which hosts and impacts the manner in which the code is both expressed and implemented? Much will depend on the terms of the contract itself and whether it expressly deals with such issues (for example through natural language terms, similar to those which deal with governing law), and on the terms and conditions of the DLT system the contract is on (either express or implied terms and conditions, including through the functional design and capabilities and limitations of the system, and whether the parties are able to be taken to be objectively aware of such capabilities and limitations).

A possible solution to this uncertainty is for the parties to expressly record in the natural language provision of the smart contract their agreement in relation to the code (for example that natural language provisions have priority to the extent coded provisions relate to performance of the same clause).

16. Are you aware of any instances where the parties to a smart contract have expressly agreed that they do not intend to create legal relations? Paragraph 3.46

We are not aware of instances where parties to a smart contract (in the way that term is described for the Call for Evidence) have expressly agreed they do not intend to create legal relations. In DeFI, we do see a number of disclaimers and where incorporated entities exist alongside a decentralised protocol the employees of those entities are extremely careful to ensure they do not act in a way that would look like the protocol is centralised and under the control of that entity.

As noted above in respect of paragraph 3.25, often parties do not intend or indeed care whether a smart non-legal contract (as distinct from a smart contract) also forms a legal contract. Unless smart contracts are considered at law to constitute legal agreements or relations, the general consensus amongst DLT users is that transactions do not automatically constitute legal agreements or relations, they are considered to be merely exchanges. However, this may not necessarily be the case, depending on both the content and context of the smart contract.

Indeed, often smart contracts are run in tandem with broader legal agreements that influence the legal status of those smart contracts and their effects, even where parties do not necessarily intend to create legal relations. It is important to distinguish between instances where parties deliberately intend not to create legal relations, from instances where parties seek to clarify the absence of a legal right within the broader context of potentially binding legal relations. One specific example may be the licence text associated with NFTs. Such licence text expressly provides that the transfer of the NFT does not also transfer copyright or IP rights associated with the creation to the recipient, and that all IP rights are held with the creator. Dapper Labs was among the first to draft such licence terms. Theoretically, these licence terms can be included in the metadata of the NFT transaction itself. For Dapper Labs to be able to enforce the protection offered to the creator by the exclusion, i.e. for the exclusions to be binding, the acceptance of the licence term would need to be within the context of broader legal relations.

17. Do you foresee any difficulties in ascertaining whether parties intend to create legal relations when they transact with one another on a distributed ledger? Paragraph 3.51

Yes, there are potential difficulties in certain use cases for smart contracts. For business contracting we recommend best practice is for the parties to retain natural language provisions with the smart contract that evidence intention to be bound and hence address this issue.

18. Do you consider that source code could meet the definition of "writing" in the Interpretation Act 1978? Paragraph 3.62

Examination of this topic includes the following key points:

- "Writing" as defined by the Interpretation Act 1978 (Interpretation Act) includes 'typing, printing, lithography, photography, and other modes of representation or reproducing words in a visible form'.[14] This is a non-exhaustive definition. Nearly 20 years ago in 2001, the Law Commission (Commission) interpreted the phrase "words in a visible form" as limiting the whole of that definition.[15] The Commission, therefore, concluded that while emails and website trading can fall within the category of other modes of representation or reproducing words in a visible form, the exchange of digital information designed to be acted upon by the software of the recipient system without the need for human intervention (known as EDI) could not. This is because of the impossibility of viewing EDI information in a 'readable' form.[16]

  In reaching this conclusion, the Commission referred to the dual form of electronic information – first, as displayed on a screen and second, its binary machine readable form in which digital information is transmitted or stored. Underlying digital information could not satisfy the requirement of writing but the alternate display of the information on a screen would satisfy the requirements of the Interpretation Act definition.

- Some 20 years later, the UKJT again focused on the possibility of viewing visible form of 'words'. In its view source code is likely to fulfil the requirements of "writing"

[14] Interpretation Act 1978, s 5, Schedule 1

[15] Page 8, 'Electronic Commerce: Formal Requirements in Commercial Transactions'

[16] Page 7, 'Electronic Commerce: Formal Requirements in Commercial Transactions'.

as per the Interpretation Act provided that it can be said to (i) represent or reproduce words and (ii) be made visible on a screen or printout.[17]

In the context of source code, the key area of interrogation, therefore, appears to be whether or not the code can be said to represent words and be represented visually such that a party can understand its meaning.

Source code (as compared to other lower-level languages such as assembly code or binary code) is generally considered the highest-level code for a computer program. It uses a combination of words and symbols and is the most easily human-readable form such that human programmers can read and edit the text. An example of a specific language written for smart contracts includes Solidity. When agreeing on the terms of a smart contract, it would almost certainly be the case that parties agree to the terms as they exist at the level of the "source code".

That code is written through either a lawyer with technical expertise in the relevant programming language or through a combination of lawyers and programmers working together to represent the parties' intentions. Often in DeFi, lawyers are not involved in the design and drafting of smart contracts. However, this is slowly changing and will likely increase in pace as the FATF recommendations are finalised and implemented by various participating countries.

One interpretation is that this process is not so different from the process of taking high-level commercial principles and transposing them into a physical legal contract written in a natural language. Lord Hodge JSC for example noted that 'so long as the operation of the computer program can be explained to a judge who, like me, maybe deficient in our knowledge of computer science, it should be relatively straightforward to conclude that people who agree to use a program with smart contracts in their transactions have objectively agreed to the consequences of the operation of the "if-then" logic of the program'.[18]

There is of course a possibility that where there is an error or a bug in the process of compiling the source code to the machine-readable code such that the behaviour of the code when executed does not reflect the expected behaviour of the source code, as discussed below in respect of paragraphs 4.15 and 4.30.

If the parties are able to open and visibly review the source code (notwithstanding whether they have actually done so) then similar to a contract concluded by email, this could fulfil the current requirement of "in writing" provided that the source code and any other visible content represents the entirety of the contract. Leaving aside issues relating to consumer contracts, the fact that code may not be readily comprehensible to one party is not determinative of whether the code fulfils an "in writing" requirement

[17] Geoffrey Vos, Lawrence Akka, Nicholas Green, Richard Hay, Peter Hunn, Mary Kyle, Christopher Woolard, Antony Zacaroli, 'Legal Statement on Cryptoassets and Smart Contracts' (November 2019) 8. accessed 06 March 2020) at p 38, paragraph 164.

[18] Lord Hodge, "The Potential and Perils of Financial Technology: Can the Law Adapt to Cope?", p. 11, available at: www.supremecourt.uk/docs/speech-190314.pdf, 25.09.2019.

just as a contract written in one natural language may not be able to be read by a given party without an expert translator.

The Digital Law Association also draws the Commission's attention to similar common law requirements of writing where it may be argued that the test of whether an instrument fulfils a "writing" requirement is broader. For example under Australian federal legislation "writing" refers to "any mode of representing or reproducing words, figures, drawings or symbols in a visible form".[19] Australian state-based acts such as the Acts Interpretation Act 1984 (Victoria) feature a similar definition. Arguably this is a broader definition because the requirement that words be represented or reproduced also extends to figures, drawings or symbols in a visible form.

19. Do you consider that parties can "sign" an agreement recorded solely in code? If so: (1) are you aware of technologies that are currently in use or under development to facilitate the signing of agreements recorded solely in code? (2) please provide any examples from your experience of where the parties have signed an agreement recorded solely in code. Paragraph 3.66

Do you consider that parties can "sign" an agreement recorded solely in code?

Under English Law any method of signing (including electronic signature) may be valid so long as its performs the function of a signature i.e. to authenticate the relevant instrument (see Ewan McKendrick, Goode on Commercial Law, 4th edition, 2010, Penguin Books, pages 81 – 82)'

Following the implementation of the Electronics Signatures Directive (Directive 1999/93/EEC) and Electronic Commerce Directive (Directive 2000/31/EC), into English law by the *Electronic Communications Act 2000* and the *Electronic Signatures Regulations 2002,* SI 2002/318, a signature is a method for a person or organisation to identify itself and: (i) to authenticate the electronic data; or (ii) to agree to or approve the contents of electronic data, to which the electronic signature is attached. (see also Law Commission 'Electronic execution of documents' Law Com No 386 3 Sep 2019)

Where a smart contract consists solely of code, parties may sign that contract by applying a digital signature to authenticate code deployed on a DLT system. This would fulfil the requirements of the ECA and eIDAS. Each participant has a unique private key that only they can use to initiate transactions on that DLT system. This key can be considered evidence that someone with access to that private key executed the transaction.

Notwithstanding that for some classes of documents, it is not possible to use an electronic signature (e.g. documents that need filing with the Land Registry), the UKJT noted in its 2019 legal statement that a statutory signature requirement is "highly likely" to be capable of being satisfied by using a private key, because an electronic signature which is intended to authenticate a document will generally satisfy a statutory

[19] Acts Interpretation Act 1901, Part 2 2B.

signature requirement, and a digital signature produced using public-key cryptography is a particular type of electronic signature.

The DLA agrees with the approach of the UKJT.

Some examples from other jurisdictions where digital identity or other methodologies have been adopted to allow for the entirely electronic approval of transactions include the below. While these may not be directly equivalent to 'signing an agreement in code', these examples demonstrate the continuing trend towards acceptance of alternative, non-traditional forms of authority and identity being asserted to that of a signature:

- In Australia it is currently commonplace to establish digital identity, and the Commonwealth Government has mandated standards for that to occur, as can be seen in "The Trusted Digital Identity Framework".[20]

- The Australian "My Health Record Integration" via API (application programming interface) enables business systems to interact with the government's core systems data. For example, the API enables third party applications to obtain the required 'informed' consent to access core data and then attach or link core data points to the third party application's records using machine readable data plus manual data.[21]

- The Australian New South Wales Government has committed to transition entirely to eConveyancing. The *Real Property Amendment (Certificates of Title) Bill 2021* includes a proposal to abolish all real estate certificates of title (CTs). The Bill was introduced into the NSW Parliament on 17 March 2021. If the legislation comes into effect, all existing paper CTs will be cancelled and paper CTs will no longer be issued. Notwithstanding the abolition of paper CTs, the Torrens Title Register will continue to be the single source of truth as to the ownership of real property, as it has always been. However, the abolition of paper based CTs will mean that the manner of establishing what is on the Torrens Title Register will change.[22]

If so: 1) are you aware of technologies that are currently in use or under development to facilitate the signing of agreements recorded solely in code? (2) Please provide any examples from your experience of where the parties have signed an agreement recorded solely in code.

Parties to a smart contract transaction apply their digital signature in order to sign the agreement. Applying a digital signature to a transaction equates to signing an agreement solely in code. Please refer to OpenLaw for recognisable legal contracts

[20] Details of The Trusted Digital Identity Framework are available at https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework.
[21] See more detail, available at: https://developer.digitalhealth.gov.au/resources/faqs/introduction-my-health-record-integration
[22] See more detail, available at: https://www.registrargeneral.nsw.gov.au/property-and-conveyancing/eConveyancing/abolition-of-certificates-of-title

that apply this methodology. Applying a digital signature is no different to electronically signing a document in DocuSign.

The application of a digital signature can be simplified (or complicated) by blockchain wallet user interfaces. In Metamask, the user simply needs to 'Confirm' the transaction in order for Metamask to apply the digital signature. Metamask is a free to download browser based wallet which can be connected to a website in order to initiate the transaction.

20. Do you think that smart contracts using DLT are currently able to utilise eIDAS compliant advanced electronic signatures and qualified electronic signatures? If not, how do you think they could be designed to accommodate these types of signatures? Paragraph 3.73

Yes, smart contracts using DLT can utilise eIDAS compliant advanced electronic signatures and qualified electronic signatures.

In principle, a token-based DLT digital signature is capable of being eIDAS-compliant. The Law Commission highlights the possibility of multiple users bearing rights to digitally signing a blockchain transaction, which can occur by way of a multi-signature wallet.

21. Are you aware of any cases in which parties have arranged for the terms of a deed to be performed by, or recorded in, computer code deployed on a distributed ledger? Paragraph 3.79

We are not aware of any UK-specific projects. Whilst we expect deeds to be capable of being digitally signed and witnessed and either stored or executed on a DLT system, the burden is largely on individuals to engage legal advisors to prepare accompanying legal advice to ensure a natively digital deed is legally valid because the area is so new and untested in courts. This is a costly exercise and a repetitive one for individuals to bear giving rise to the need for government and regulators to issue clear guidance. In the alternative, individuals are deploying smart contracts with the intention that they operate as deeds or wills but which may not stand up as legally valid or pass probate processes.

In Australia, the *Electronic Conveyancing National Law* (ECNL), which has been adopted by all major Australian jurisdictions, allows for land registry instruments such as mortgages (which are deeds in most Australian jurisdictions) to be digitally signed on an approved Electronic Lodgement Network Operator (e.g. PEXA or Sympli).

A template smart contract is available at ethereum.org which is intended to store digital asset wealth until the digital asset owner passes. The temporary COVID measures to allow electronic execution of Wills, some measures of which have been made permanent, have assisted with adding natural language text to the smart contract to ensure it is a legally valid Will or part of a Will. However, the smart contract functions need to be set so as not to transfer digital assets to the specified beneficiaries until after probate is granted notwithstanding that the digital assets could be transferred shortly after a person dies. Due to the novel nature of such an arrangement, it is not clear how quickly a smart contract could be granted probate which veils the arrangement with uncertainty despite it being a clear mechanism for the storage and disposition of digital asset wealth.

22. Do you consider that a deed recorded partly or wholly in code can satisfy the statutory formality requirements applicable to deeds and address the implications of the Mercury decision? Paragraph 3.80

In short, yes. We also note that due to the COVID pandemic, a number of electronic signing and witnessing laws and regulations arose in Australia, including in respect of deeds. It may be worth looking into the guidance issued by Australian Law Societies (e.g. Law Institute of Victoria and the Law Society of New South Wales) on how witnessing and other formalities can be satisfied in a digital environment. At the time of submission, some temporary laws in Australia have lapsed whereas others have been made permanent and it remains to be seen how law makers will address this issue going forward.

In particular, we note that if parties sign digitally an appropriately worded smart contract (i.e. including the words “signed, sealed and delivered”) , the signatures will be date-stamped, which is particularly relevant for highlighting whether the witness signed before or after the other signatories.

In relation to digital signature, and in particular, digital witnessing, it is interesting to consider whether a machine can functionally supply acceptable equivalent of witnessing. Namely, can the objective of witnessing be achieved through digital means by verifying: identity, intention to sign, act showing intention, link between the person and the act, link between the person and the document and that the process has not been tampered with. It is arguable that an appropriate digital platform, software and necessary safeguards and processes in place, digital witnessing may provide a better outcome of the witnessing goals than the current manual, or hybrid virtual/manual processes in place.

INTERPRETATION OF SMART CONTRACTS (CHAPTER 4)

23. Are you aware of, or do you foresee, any difficulties in applying the principles of interpretation to identify whether terms of a particular smart contract are contained in the natural language component or the coded component of the smart contract, or both? Paragraph 4.10

A preferred approach would be that the parties have expressly stated in the contract whether the terms of a contract are to be contained in the natural language or coded component, and made a choice as to which is to be preferred in the case of conflict or overlap.

In particular it is our view that commercial norms are likely to emerge whereby ‘boilerplate’ clauses included in the contract indicate the primacy of the natural language component. This is particularly important in circumstances where an error in the coded component can have immediate unintended impacts to the parties. Current principles of interpretation are such that the courts "do not easily accept that people have made linguistic mistakes, particularly in formal documents".[23] This approach has developed in circumstances where contracts are entirely comprised of natural language, and is not necessarily fit for purpose for coded language which – due to its very precision – can often contain unintended mistakes if only detected upon execution. Testing for bugs and unintended mistakes should become mandatory before a smart contract is deployed and signed.

24. In what circumstances might disputes arise about the proper interpretation of the coded terms of a smart contract? Please provide examples where possible. Paragraph 4.15

The interpretation of what was objectively intended by coded components (where such components are considered to contain a term of a contract) will be a more difficult exercise for the courts, likely requiring expert evidence, given comparative lack of expertise in interpreting coded languages as compared to legal or natural languages. The circumstances could be wide-ranging, particularly when the contract or agreement does not include a list of definitions or agreed natural language terms dealing with the peculiarities introduced by coded components, including for example: how the contract should deal with code, privacy and data related issues, the legal status of the code and hierarchy as between the terms, which may be a mix of code and natural language.

Unlike natural language components, which require humans to interpret and give action to performance, coded components are directly interpreted and performed by machine systems. The nature of disputes which arise from interpretation of coded terms of a smart contract are therefore likely to have to deal with an additional dimension – which is that neither party is necessarily responsible for a flawed

[23] Lord Hoffman in *Investors Compensation Scheme v. West Bromwich Building Society* [1998] 1 WLR 896 (HL) at 913.

interpretation and/or performance of a term in quite the same way as they might be for a natural language term. This is why clear risk allocation terms are advisable, particularly as between the parties and any third parties (particularly those involved in enabling the coded components or digital hosting and actions of the contract).

Key examples of circumstances likely to give rise to disputes include:

- Inconsistencies between natural language and coded components, particularly where both deal with the same, or part of the same, term or contractual process;
- Issues flowing from the limitations of programming languages – including identifying the 'natural meaning' of words expressed in code, as well as discerning the intention of the parties;
- risk of mismatch or mistake in translation between natural language and code;
- risk of incorrect input or output data triggering performance or a change in legal status, for example where a legal right to a transaction is lost due to an automation failing to pick up when an exchange rate has reached a certain limit;
- risk of mistaken execution – an issue for many types of smart contracts will be where the off-ledger status of the agreement does not match or align with the on-ledger status. For example, in relation to insolvency, given the escrow arrangements for payments executed by smart contract. Discrepancies between on-ledger and off-ledger execution status can create insolvency issues. That is, there is a question of whether mistaken payments (due, for example, to an outdated assessment of available funds) constituting an insolvent transaction will have implications for priorities, given the smart contract holds nominal funds (representing a future obligation to pay the final amount) in escrow pending settlement. This will particularly be the case for "physical" agreements where execution relies on physical acts to update the on-ledger status, for example, a supply contract, where the status of delivered goods may not be up to date due to human or technical error, or simply time lapses between updates. In these circumstances, it may be questionable whether the smart contract is the source of truth for execution status in the event of a dispute.

25. Do you consider that the meaning of a coded term of a smart contract would or should be determined by asking what the term would mean to a: (1) reasonable person; (2) reasonable person with knowledge of the relevant code; or (3) functioning computer? Paragraph 4.30

As an overarching principle, the same considerations as those which apply for the interpretation of any part of a legally binding agreement should continue to apply, from a complex commercial transaction to a purchase of real estate through to the simple acceptance of a delivery parcel.

In practice, this is likely to depend on the nature of the particular contract, and in particular the impact of any natural language terms which govern or are intended to give meaning to coded components. A contract where it is found that the objective intention of the parties is that the natural language components are to be given primacy over the coded components will likely rely more heavily on (1) (what the term would mean to a reasonable person), whereas a contract that is wholly in code, or does not expressly or implicitly consider the interactions between code and natural language will likely require a combination approach.

A reasonable person without a coding background should not be relied upon to interpret or understand a coded term without assistance.

So the approach of option (2) (a reasonable person with knowledge of the relevant code) is preferable, though still lacking. If a coded term is considered a contract term, then normal rules of construction should apply – including normal use of allowable evidence. The class of reasonable person should not be restricted as Option 2 presents. It is not required that the reasonable person understand source code, but they must have that code's meaning or explanation conveyed to them. The test could instead provide subjectivity in the form of a reasonable person with the knowledge and expertise to be able to enter into a contract that includes coded terms. The court may be required to translate source code into natural language prior to applying this test. This translation could be completed by an expert or assessor, appointed by the parties jointly or separately or by the court. This reflects the process currently undertaken for foreign language contracts.

26. Do you consider that performance of the coded terms of a smart contract cannot always be predicted based on a reading of the code? If so, can you provide examples or specific evidence of this occurring? Paragraph 4.31

Much depends on the nature of the coded term; in particular the degree of connectivity, and variability of outcomes accounted for in the code.

How many factors or variables does the code contain, and how many of these are drawn from other coded terms, other contracts, or external systems (for example data inputs or outputs from the code that trigger or otherwise impact or result from performance)? The greater the number of these types of connections and dependencies, the more difficult it is to predict the performance of a coded term. The more complex the coded terms, the more difficult they are to predict. As the smart contracting ecosystem grows in complexity so too will the algorithms and rules used to generate performance, and some are likely to incorporate machine learning and artificial intelligence-based systems. All of these factors contribute to an inability to precisely predict performance. Intersections with real-world events that frustrate, obviate or otherwise impact the intended performance of the code may also create unpredictable situations, for example where human enters data required by a coded term incorrectly, or where manual performance has already taken place, resulting in unintended redundancies.

Whether the code is performing as intended is a legal question, but appropriate boilerplate (for example setting out that natural language terms take primacy) can mitigate this risk, and allow the parties to agree that where the code does not perform as intended, more traditional performance approaches can be used by the parties to ensure proper performance is achieved. However this depends on appropriate legal drafting to achieve this effect, and each contract must be taken on its own terms until or unless principles of construction are developed.

27. What practical or procedural steps could the courts take to resolve disputes about the interpretation of the coded terms of a smart contract? Paragraph 4.32

See our comments regarding expert evidence above in respect of paragraph 4.30.

28. Are parties utilising natural language in smart contracts to make their intentions clear in respect of any coded terms or the contract as a whole? Paragraph 4.37

As detailed in 'Smart Legal Contracts: A Model for the Integration of Machine Capabilities Into Contracts',[24] we consider that commercially, natural language should always be used to capture the contract as a whole, with coded terms sitting 'underneath' agreed terms or processes that are suitable to be automated. This does not mean that the coded components do not form part of the contract – rather, like notice provisions, they provide detailed and/or technical instructions about how performance should be conducted, which can be treated as essential or non-essential depending on the preferences of the parties.

In addition, within the limits of the law, there is much freedom for parties to determine the content and format of a contract. For example, parties may include complicated technical specifications in engineering contracts. Similarly, parties may include explanatory addendums to coded terms such as logic maps or process flowcharts to assist with setting out the agreement for how the code should work.

29. In what (if any) circumstances should courts be able to consider evidence of the parties' pre-contractual negotiations as an aid to interpretation of the coded terms of a smart contract? Paragraph 4.43

This approach should be no different to the current approach as to external evidence. The critical factor is whether the parties expressly address the legal status of the code, including as compared to natural language terms with which it may overlap.

[24] Blycha, Natasha and Garside, Ariane, Smart Legal Contracts: A Model for the Integration of Machine Capabilities Into Contracts (December 7, 2020). Available at SSRN: https://ssrn.com/abstract=3743932 or http://dx.doi.org/10.2139/ssrn.3743932

30. Do you consider that the courts' current approach to contractual interpretation might cause problems in the context of smart contracts? If so: (1) Can you provide examples or specific evidence of this occurring? (2) What could be done to solve these problems? Paragraph 4.45

We have identified above some key issues and considerations to be dealt with, but primarily expect that existing approaches to contractual interpretation are likely to be broadly appropriate, with some adaptations on the practical level, rather than the conceptual.

One final aspect to note is that it is likely that the terms and conditions and technical specifications of any digital platform on which a smart contract is hosted or interacts is likely to impact the interpretation of a smart contract, similar to how governing law or jurisdiction may impact the interpretation of a contract currently.

As mentioned above, we are aware of one matter before an Australian court that is dealing with the issue of "code is law" versus "code of law".

REMEDIES & SMART CONTRACTS (CHAPTER 5)

Dispute resolution and remedies for smart legal contracts

At the outset, it is important to note that there are practical issues which limit the types of contracts which are likely to be subject to disputes. For example, if counterparties are not known to each other (such as token swaps within a decentralised exchange) then there may be a complete inability to contact or locate counterparties in order to engage with a dispute resolution process. In such cases, individuals are contacting various regulators to complain about the dApp and the founding contributors involved in launching the dApp. We understand that recommended regulations covering virtual asset service providers, including dApps, will be finalised by FATF in mid-2021. It is likely that jurisdictional courts and regulators will increasingly become concerned with these types of potential disputes as clearer regulations are introduced and enforced.

This section is confined to smart legal contracts with known counterparties.

Governance of Dispute Resolution

Dispute resolution is fundamentally a question of governance in the formation stage of the contractual arrangements. That is, there is more than one approach to dispute resolution and "contracting parties must choose the most effective institutional governance mechanism to resolve their contractual disputes" that may occur in the future. A recent article published in the *Harvard Negotiation Law Review* proposes that there are four broad institutional possibilities in this regard:

1. Negotiation or mediation;
2. Binding private arbitration;
3. Territorial courts; and
4. Regulatory state.

Adopting this framework, it can be seen that each dispute resolution possibility has different implications for jurisdictional law.

First, there will be a limited role for courts where parties decide to informally resolve disputes and agree on their own remedies. Indeed, parties are required to attempt private dispute resolution options before turning to the courts. As such, we anticipate that minor contractual breaches are likely to be conducted in this way, as is the case currently for traditional legal contracts.

Practically, many contracts provide a safeguard by outlining the intended arrangement, over which parties are then free to adhere to or not as they see fit. For example, supply contracts may provide a deadline by which goods must be delivered. In practice, parties are unlikely to seek damages for minor breaches which do not cause loss (for example, delays of a few minutes). The automatic execution of smart contracts may have significant outcomes for such arrangements. This may also present an issue when determining whether parties have elected to waive a contractual right – in practice, acceptance of practices by conduct would not be able to be inferred where code automatically executes. Parties may be required to specifically elect to accept certain breaches (either by separate negotiation or as built into the smart contract). This may be subject to increased administrative overhead or may involve certain parties having the exposure of having payments withheld or penalties imposed for conduct which would otherwise be accepted. Such issues may need to be considered when drafting smart contracts or when selecting platforms.

Smart contracts may also present an issue of illegality, as it may allow for the enforcement of contracts which would otherwise be void. To a lesser extent, smart contracts may also allow for the continued operation of contracts which are not compliant with their legal obligations to include certain terms (for example, consumer protections, residential tenancy terms and employment protections). This risk is present in natural language contracts – however, parties may have less recourse in circumstances where the contract automatically executes. For example, when a retail client of a bank receives notification that they may be subject to penalty payments for late loan repayments, there is a clear opportunity to challenge the conclusion. This may not be true if the money is automatically deducted via the operation of a smart contract (particularly if it was issued in "standard form" by a party with increased negotiating power, without consequences being properly understood). Restrictions on the use of smart contracts in fields prone to such issues or increased regulatory supervision may assist in mitigating these risks.

Second, there will be an enforcement role for courts where parties have agreed to binding private arbitration. This agreement could be made during the smart legal contract formation or after a dispute has arisen. The form of arbitration could occur on-chain (i.e., through a blockchain-based dispute resolution plugin) or off-chain (i.e. through a commercial arbitrator, ideally with knowledge of smart legal contracts). The role for the courts here is to enforce the decision of the arbitrator.

Third, there will be a significant role for courts if one party commences litigation and a court is given carriage of the matter. A preliminary question here will be how jurisdiction is determined. Parties can provide greater certainty to this question by explicitly stating the governing laws and jurisdiction during the contractual formation stage. However, a court will still require jurisdiction to entertain the case. The common law doctrine of *forum (non) conveniens* may provide some guidance in this regard. Justifiability would be assisted by a clear legislative mandate providing a particular court with jurisdiction over smart legal contract matters.

Fourth, regulation could mandate that an existing administrative body (e.g. an ombudsman) could mandate one type of dispute resolution mechanism. The role of courts here will be to apply existing administrative law principles to reviewing these decisions.

The traditional legal system will need to understand these above dispute resolution possibilities (including blockchain-based dispute resolution systems) and how they interact with the jurisdictional court system.

Enabling Enforcement

There are circumstances where a Court is likely to have to interpret smart contracts, even where dispute resolution clauses may be present – for example, the validity of the dispute resolution clause may be challenged or where the code of a contract is considered to form part of the terms and/or may be a factor in the interpretation of the natural language terms. As such, the Court would need to be able to interpret coded sections of smart contracts and the operation of ADR methods.

In general, experts may be retained by the parties to provide such a background to the Court. While the use of experts has long been effective in allowing Courts to adjudicate complex concepts, smart contracts may be even more complex for the following reasons:

- most judicial officers are unlikely to have an understanding of the concept of smart contracts or their technical operation;
- conflicting experts may be difficult to reconcile in the absence of such knowledge; and
- there is an absence of precedent in the field.

In particular, there may be circumstances where the Court must determine more than what the code actually accomplished (which is a factual inquiry that experts may be able to assist with) but what the parties intended for the code to accomplish. This is a legal conclusion which may require a solid conceptual understanding of the technical operation of the smart contract. This may be achieved through the use of experts who are able to interpret and communicate the conceptual and practical objects of the code, which can then be interpreted by a reasonable person. For the reasons outlined above, parties may consider that judicial interpretation may present the risk of providing an unpredictable outcome as to the operation of the contract. These reasons are also why parties may choose to voluntarily engage an arbitrator with these expert skills and rely on courts to enforce an arbitrator's findings if required.

The likely response of parties may be to prepare either natural language contract terms which are intended to entirely govern any coded components is affected by code, to create an entirely natural language contract, with coded implementation treated as separate to the contract, or to provide a form of explanatory aide in the course of negotiations. Laws governing the use of smart contracts may benefit from specifying what material may be admissible in this interpretation exercise (if any). Training of judicial officers may also be of great assistance in applying these principles.

Where no dispute resolution clause exists, the traditional legal system will need to establish and interpret the terms of smart legal contracts and whether existing legal principles can be imposed on smart contracts. There is a high degree of uncertainty and this may provide grounds for legislative intervention.

Remedies

There are a range of remedies that could be imposed following a dispute resolution process. There is a distinction between remedies “on-chain” (where parties have coded into the smart legal contract ‘remedies’ or specified actions arising in response to specified events or triggers) and “off-chain” (where parties agree, or a binding determination or court order requires, a party to do a particular thing to remedy the breach).

First, at the interlocutory stage, a form of ‘suspension’ or ‘pausing’ of the automatic operation of the contract may assist. For negotiation, mediation and arbitration - parties may agree on this process upfront. Indeed, it is a feature of some blockchain-based dispute resolution mechanisms. For judicial or administrative intervention, this would require that parties are technically able to do this when ordered to do so. Alternatively, courts or regulators would require some ‘gateway’ into the smart legal contracting infrastructure that may not be desirable from a public policy perspective. Such ‘suspension’ or ‘pausing’ orders could be made permanent.

Second, contractual damages could be awarded where loss and damage are appropriately made out. A future issue to consider in this regard is whether courts can award damages denominated in cryptocurrencies or structure remedies around other forms of digital assets. It is likely that there will need to be a legislative basis for doing so.

Third, specific performance could be ordered where damages would not be an adequate remedy and it was determined that the parties intended a particular outcome that the smart legal contract code did not achieve. Again, the availability of this remedy would depend on the technical capabilities of the relevant DLT system or platform, and the ability of Courts to enforce this by locating the relevant parties or platform administrators.

Fourth, smart legal contracts could be ordered to terminate. Here, we consider that parties are likely to consider a method of rescission or termination of code during the formation of the contract. The ease with which a party may terminate code, or the availability of a ‘self-destruct’ function is likely a commercial decision of which party bears the risk of the contract ending or continuing to function. These methods of termination may operate in a manner consistent with established contractual terms, but must also be able to be accommodated by the chosen DLT system or platform.

For example, one such system may be:

- one party may issue a notice of termination due to a breach occurring;
- if the notice is not contested within a reasonable time (as defined by the contract or code), the smart contract may be terminated by mutual consent; and
- if the termination is contested, this may progress to ADR or judicial determination.

However, we note that the structures required in order to enforce such forms of termination would reduce the benefits of smart contracts as an impartial, reliable form of executing contractual operations.

31. Are you aware of, or do you foresee, any practical difficulties in ordering rectification of the coded terms of a smart contract? If so, do you think that parties to a smart contract will, in practice, seek rectification? Paragraph 5.26

On rectification, we do not foresee such difficulties in ordering rectification of terms if parties use a bespoke and well- designed smart contract platform with natural language capability. The parties may then set out how the contract is rectified, within the terms of the contract itself. Natural language capability combined with code would allow the parties to pre-agree how automated systems might respond where acts of reversal are required.

Although the database on which a contact is stored is immutable, it is possible to add new metadata that replaces the old metadata so it is possible to rectify or amend contracts, even those that have been signed. Because all changes are tracked, it is trivial to determine if a contract has been altered after signing and by whom. This leaves open the existing mechanisms for enforcing a bargain – such as litigation, where the court of competent jurisdiction is able to order the legal or natural persons with whom the contract is entered into to abide by the order of the court, with the corresponding sanctions for failure to comply. There are practical difficulties in adopting the same approach in permissionless systems.

We are aware of one matter currently before an Australian court that is dealing with the issue of “code is law” versus “code of law” in relation to the ETH – ETC Hard Fork. In short, the hard fork of the Ethereum blockchain instituted the remedy of rectification (for ETH holders that suffered loss as a result of the DAO attack) but did not need a court to order the remedy of rectification because the act of hard forking achieved this remedy.

32. Are you aware of, or do you foresee, any difficulties in applying the existing law to determine whether the parties have made a common mistake when entering into a smart contract? Paragraph 5.41

See response to Question 31.

33. What steps or precautions (if any) do parties typically take before entering into a smart contract to satisfy themselves that the code will execute as intended? Paragraph 5.42

See response to Question 31.

34. Do you consider that the legal principles concerning unilateral mistake might need to be adapted to accommodate smart contracts concluded by computer programs without human intervention? In particular: (1) is it appropriate to confine a unilateral mistake to a mistake about a term of the contract? (2) what test should the court apply in determining whether the non-mistaken party had knowledge of the mistaken party's mistake? Paragraph 5.56

See response to Question 31.

35. Are you aware of, or do you foresee, any difficulties in applying the existing law to determine whether a smart contract has been entered into as a result of a misrepresentation? Paragraph 5.62

The difficulties will relate to who is making the representations and whether a reasonable person would believe they had sufficient authority to make representations that would be relied upon. Such difficulties will soon be made apparent when enforcement actions are likely commenced against DeFi protocols. Social media posts by founding contributors to a protocol as well as interested community members could constitute representations and misrepresentations that are relied on by retail investors and traders, particularly in relation to the security and resilience of a protocol, and some social media accounts are pseudonymous.

See response to Question 31.

36. Are you aware of, or do you foresee, any difficulties in applying the legal principles concerning rescission to smart contracts which have been vitiated for misrepresentation, duress or undue influence? Paragraph 5.79

At a high level, smart contracts are self-executing and they self-execute quickly. Legal processes are far too slow to keep pace which begs the need for proactive involvement by regulators in releasing smart contract templates (even if this exercise begins with consumer facing standard contracts). If the law were needed to rescind a smart contract, all of the token transactions had and received by the smart contract would increase the difficulty of properly rescinding the smart contract.

See response to Question 31.

37. Are you aware of, or do you foresee, any difficulties in awarding damages for breach of contract where the terms of a natural language contract are performed automatically by computer code? Paragraph 5.91

If breach of contract is reasonably foreseeable, one party could require the counterparty to deposit funds in escrow to automatically meet payment of damages for breach of contract. Where breach of contract is not reasonably foreseeable, the parties should negotiate and agree parameters for the return or splitting of benefits enjoyed as well as the allocation of liability for damages depending on the nature of loss suffered and by whom.

See response to Question 31.

38. Are you aware of, or do you foresee, any difficulties in applying the legal principles concerning termination where the terms of a natural language contract are performed automatically by computer code? Paragraph 5.95

See response to Question 31.

39. Are you aware of, or do you foresee, any difficulties in applying the legal principles concerning breach of contract to contracts recorded wholly or partly in computer code? Paragraph 5.104

See response to Question 31.

40. Are you aware of, or do you foresee, any difficulties in applying the law on frustration to smart contracts? Paragraph 5.112

See response to Question 31.

41. Can you provide examples of terms that parties have included (or might include) in the natural language element of the smart contract to address the risk that subsequent events might affect the performance of the code? Please explain: (1) the drafting of the provision; (2) the subsequent events covered by the provision; (3) the effect, under the provision, of the subsequent event on the contract; and (4) the remedies available to the parties under the provision. Paragraph 5.113

In relation to open source protocols that can be copied and amended (i.e. Hard Forks), public representations and disclaimers are recommended to guide users as to which chain should be considered the original versus the new. This is one of the issues before an Australian court in relation to the ETH – ETC Hard Fork. Absent clear representations, it is left to the court to interpret the facts and circumstances available, which also requires experts, which is a lengthy and expensive process.

See response to Question 31.

42. Are you aware of, or do you foresee, any difficulties in applying the illegality doctrine to claims made in relation to smart contracts? Paragraph 5.117

See response to Question 31.

CONSUMERS & SMART CONTRACTS (CHAPTER 6)

43. Are you aware of any business to consumer smart contracts currently in use or in development? Please give details. Paragraph 6.5

We are aware of a number of pilot programs and proof of concepts for the use of smart contracts in a consumer setting, particularly in the insurance and consumer credit space. However, very few of these pass the initial set-up stage, with one exception NFTs that is looked at last. Please note that some of these use cases (except as where expressly referenced as legally binding) would generally fall into the self-executing code on a blockchain category of smart contract.

(a) Banking and securities

Lygon is a blockchain-based platform for the digitalisation of bank guarantees involving a joint venture between a number of Australian banks along with IBM and retail operator Scentre Group.[25] The platform underwent a live pilot in July/ August 2019 and Lygon as a joint venture was formally announced in February 2021.[26] Lygon enables applicants, issuers and beneficiaries to obtain legally binding guarantees in a single day.

Iberpay, the manager of the Spanish interbank payments infrastructure, is also developing digital bank guarantees.[27] Banco Sabadell, Banco Santander, Bankia, BBVA and CaizaBank completed a proof of concept smart contract for managing bank guarantees in July 2020. The group is focused on broader applications for the automatic execution of payments triggered by smart contracts in blockchain networks.

(b) Insurance-related products

As mentioned in the call for evidence AXA launched its flight delay smart contract platform '**Fizzy'** in September 2017.[28] The product was based on the Ethereum blockchain and allowed customers to receive automatic compensation for flight delays via a self-executing insurance policy. The smart contract integrated with global air traffic databases such that payment would be automatically triggered if a delay of more than 2 hrs occurred. AXA scrapped the product in October 2020 due to a lack of uptake. It cited a lack of distribution channels as one of the contributing factors.

[25] https://www.lygon.io/

[26] AFR 'Scentre, ANZ create first digital bank guarantee with Lygon blockchain' (9 February 2021)

[27] Finextra 'Spanish banks complete tests of programmable payments for smart contracts' (15 July 2020)

[28] Axa 'Axa goes blockchain with fizz' (13 September 2017)

A similar decentralised insurance application **Etherisc Flight Delay** also uses smart contracts to provide consumers with insurance against flight delays and cancellations.[29]

In 2017, B3i (the Blockchain Insurance Industry Initiative) created a proof of concept for a smart contract built and agreed on blockchain technology called **B3i Resinusrance** or B3i Re.[30] This was the first application built on top of the B3i Fluidity platform. By February 2020, nine insurers, four major brokerage firms and eight reinsurers had concluded 30 reinsurance contracts using the product. Future versions are planned for March 2021 and September 2021 to introduce claims management features and extend to additional reinsurance types and lines of business.

(c) Healthcare

In the medical industry, smart contracts are being used by **Encrypgen**[31] to transfer patients' DNA data to researchers for clinical trial purposes.[32] Encrypgen went live in November 2018[33] with 'Gene-Chain', a genomic blockchain marketplace that enables individuals to sell access to their health data and DNA directly to researchers. The blockchain application aims to ensure patients remain in control of their genomic data, while allowing researchers to engage in research to progress treatments and cures for diseases. Researchers that want to use your data have to request, or in some cases even pay for the privilege.

See also the Australian Commonwealth Government's "My Health Record Integration" project.

(d) Residential real estate

Propy is a silicon valley based tech company. Its core product is a residential real estate transaction platform, powered by smart contracts.[34] Once a buyer makes payment to the seller, a smart contract automatically changes ownership of the asset based on the payment information on the blockchain. Propy enabled the word's first property transaction using smart contracts in 2017. While it currently mirrors official land registry records, its mission is to encourage jurisdictions to adopt Propy as their official ledger of record such that a transfer of property over the Propy platform constitutes a legal transfer of the property and the legal registration of that transfer.

Land titles Australia - nearly all examples at present however are pilots. See details at paragraph 3.66 regarding the NSW Government's digital Torrens Title replacing all paper certificates of title.

[29] https://fdd.etherisc.com/#/

[30] B3i media release 'Major reinsurers and brokers complete complex placements on B3is Blockchain Platform' (12 February 2020)

[31] https://encrypgen.com/

[32] Encrypgen blog post 'Mid-year update, June 2020' (June 2020)

[33] The Scientist, 'First Blockchain-based Genomic Data Marketplace Launches' (November 2018)

[34] https://propy.com/

(e) Other products

Other examples include:

- **YouPic**, a decentralised photography platform for photographers.[35] Photographers can securely register and license their images using smart contracts. Photographers received payments through the platform from customers directly, avoiding the need for brokers and their commissions.[36]
- **Drife**, is a ridesharing app operating in Bangalore.[37] It uses a series of personalised smart contracts between drivers and riders, where drivers stake Drife's DRF token to be chosen for rides. Instead of paying a fee for every fare, drivers pay an annual fee to use the app.
- **S7 Airlines**, a Russian-based airline runs a private blockchain to issue and sell tickets using smart contracts.[38] The airline sold the first air ticket in the world that was bought by connecting to a banking system through a blockchain in July 2017.

(f) NFTs

Businesses are increasingly using NFTs, which use smart contracts, as are artists and celebrities. NFTs are not new, but until recently they were largely confined to crypto enthusiasts. Examples include:

- NBA Top Shot[39] - people are purchasing short videos of digital moments of NBA games through their credit cards, they are a digital equivalent of basketball cards.
- Taco Bell40 has sold NFTs in a promotion.
- Charmin,[41] US based toilet paper manufacturer has sold NFTs

44. When would you estimate that smart contracts might be in common use in business to consumer contracts? Paragraph 6.6

Business to consumer (B2C) contracts are often distinguished from business to business (B2B) contracts on the basis of the different degrees of assumed knowledge that are attributed to contracting parties. Analysis of B2B contracts is typically predicated on the basis that there are at least two equally sophisticated parties with professional knowledge that each understand the terms of the bargain that they have struck while B2C contracts assume an imbalance in bargaining power and knowledge. There is generally no presumption that the lay consumer has read, nor understood the terms of the contract which are assumed to have been set by the company. In most

[35] https://youpic.com/blockchain
[36] YouPic blog post ‘The future of Photography is already here-The YouPic Blockchain’ (25 September 2018)
[37] https://drife.io/#/
[38] S7 Airlines ‘The amount of operations via the S7 Airlines blockchain platform and Alfa-Bank exceeded $1 million in July’ (30 July 2019)
[39] https://www.nbatopshot.com/.
[40] https://www.theverge.com/2021/3/8/22319868/taco-bell-nfts-gif-tacos-sell
[41] https://www.theverge.com/tldr/2021/3/17/22336115/charmin-nft-toilet-paper-cryptoart-marketing

developed legal systems around the world various protections are enshrined into law to seek to address the perceived inequities of B2C contracts, England and Wales being no different. The *Consumer Rights Act 2015* for example seeks to grant consumers certain minimum requirements of transparency and fairness as well as right and remedies which counterparts are unable to contract out of. B2C contracts that do not comply with these obligations can be deemed unenforceable and constitute a breach of consumer protection regulations.

For there to be widespread use of B2C smart contracts certain market conditions must be met, such that the benefits of using smart contracts in the B2C setting outweigh its risks. The DLA proposes the following minimum threshold requirements be satisfied before widespread adoption of smart contracts is likely to take place:

(a) Sufficient time and cost savings

Business stand to benefit from huge efficiencies, both in terms of time and cost, in the adoption of self-enforcing smart contracts in B2C transactions. The greatest efficiencies are likely to apply to large-scale, standard form terms and conditions for which businesses currently spend vast amounts of time and effort in developing, drafting, and enforcing. However, not all provisions of legal contracts are suitable candidates for being expressed in machine-readable form. Current legal parlance relies heavily on ambiguous and abstract concepts such as ‘reasonableness’ and ‘good faith’ which do not find a functional equivalence in code. Over time contracting practices are likely to shift towards more binary yes/no contractual provisions with less reliance on ‘lazy’ or ambiguous legal language. Businesses are likely to see significantly more benefits from using entirely automated end to end smart contracts compared to the automation of one or two provisions, or the value realised from structured data created through smart contracts. While there are still substantial efficiencies to be gained from simple self-executing performance provisions alongside a more traditional legal contract, unless there is a real saving of cost and time then B2C contracts are unlikely to garner the necessary investment that will see them adopted in various sectors.

However, we note that certain of our members are already advising individuals in relation to their interactions with DeFi to use digital assets as collateral to borrow funds to purchase real estate and for small to medium business financing.

(b) Certainty of enforcement

As discussed in Q45 and Q46, there are a number of challenges exemplified in the context of B2C smart legal contracts including obligations of transparency, enforcement of rights e.g. minimum warranty protection. B2C transactions are unlikely to be implemented as smart legal contract until businesses are satisfied that compliance with consumer protections is indeed possible and that there is sufficient consistency in the regulation of smart B2C contracts across multiple jurisdictions. We know that globalisation is a continuing trend and many businesses prefer to adopt standard terms with minimal variation between jurisdictions. Smart contracts also rely on distributed ledger technology that may not reside in a single jurisdiction, rather to exist across multiple locations.

Different regulatory bodies in different jurisdictions are currently at various points in their lifecycle of research, interpretation and support of smart contracts. The Law Commission is certainly at the forefront of such research and is to be commended for this. However, it is surely the case that widespread adoption of smart contracts will be supressed until businesses can be reassured that their business terms for particular consumer products do not require vastly different approaches, systems, coding rules and other features in order for such contracts to be enforced in each of their core markets.

(c) Access to reliable data

Smart contracts rely on a variety of data feeds to trigger certain events or transactions.[42] Traditional contracts by contrast rely on the sharing of information as between parties or perhaps interconnected systems. Typically a human is required to ensure that information is shared with another party, an assessment is required to validate the information and ensure it complies with the terms of the contract, before the relevant action can be progressed. Smart contracts for B2C transactions are therefore likely to grow in popularity alongside the growing banks of trusted data relating to the relevant action. Access to such data is more widespread in some sectors than others e.g. financial markets have seen significant progress in the adoption of public data sets through initiatives such as open banking. Another challenge mentioned by commentators is the challenge of time in the context of changing data sources.[43] Simple point in time B2C transactions such as making a food purchase are less likely to need to deal with this additional layer of complexity, but for more complex B2B and B2C arrangements close monitoring of the data source, its validation and mechanisms for making suitable adjustments will be required to be developed. Until such a time, it is likely that the adoption of smart contracts in B2C transactions will be limited to simple, standardised use cases involving point in time purchases.

(d) Improved co-operation and standardisation of smart contract development

At present, smart contracts tend to be carefully created to address single, bespoke use-cases. While there are a smattering of proof of concepts for B2C smart contracts, it is clear that there is currently no general consensus or standard that can be shared. Although the DLA is aware of organisations such as the Accord Project who are focused on developing an ecosystem and open source tools to develop smart legal contracts. Given developers are generally tasked with creating smart contracts from scratch, presumably based on existing legal contracts, it is likely that there is substantial duplication of effort, not insignificant mistakes and a great deal of testing before running in a live application. Until standards are developed and businesses do not need to re-

[42] Unsworth R. (2019) Smart Contract This! An Assessment of the Contractual Landscape and the Herculean Challenges it Currently Presents for "Self-executing" Contracts. In: Corrales M., Fenwick M., Haapio H. (eds) Legal Tech, smart contracts and Blockchain. Perspectives in Law, Business and Innovation. Springer, Singapore. https://doi.org/10.1007/978-981-13-6086-2_2

[43] Ibid

solve similar problems every time it seeks to prepare a new smart contract it is likely that take up of B2C, and in fact all smart contracts will be limited.

A significant limiting actor on B2C smart contracts is the fact that it is difficult to achieve scalability of the technology and energy production with current market solutions.

45. What challenges do you foresee in applying consumer protection laws to consumer contracts entered into wholly or partly in code? Are there any additional existing protections, beyond those we have discussed, which you think are or will be particularly important in the smart contract context? Paragraph 6.39

The DLA's discussion for question 44 applies to this question.

The following expands on the discussion of standards in question 44 (improved co-operation and standardisation of smart contract development), and businesses should not be required to resolve similar problems every time it seeks to prepare a new smart contract. There is an opportunity for smart contracts (and thus contractual terms) to be valid and not breach the law, which is not always the case with wet contracts. For example, in the New Zealand context, two studies have shown the high prevalence of unfair contract terms in New Zealand online contracts. Every contract analysed in two studies contained unfair contract terms.[44] Legislation banning unfair contract terms in consumer contracts, however, is relatively new in New Zealand and the rate in which such terms occur in contracts are likely to be lower than in the UK. By "approved for use", a body such as the Competition and Markets Authority (CMA) could take the responsibility of vetting smart contracts. While this would add to the CMA's workload initially, after a library of smart contracts had been created the work would reduce and would greatly increase consumer protection in the UK. One limitation is that consumers purchasing goods or services from organisations based outside the UK would not be as well protected; however, those consumers are not well protected in the UK with wet contracts.

46. What, if any, additional protections do you think are required for consumers entering into smart contracts? In particular, do you consider that there is a case for an explicit legal requirement that terms of a consumer contract which are fully or partly in code must be explained in natural language before the conclusion of the contract? Paragraph 6.40

Yes, there should be an explicit legal requirement that terms of a consumer contract which are fully or partly in code must be explained in natural language to the

[44] Alexandra Sims and Louise Mara, 'Unfair Online Contract Terms in New Zealand: Evaluating the Effect of Regulatory Change' (2016) 24 Competition & Consumer Law Journal 128 and Victoria Stace, Victoria, Emily Chan and Alexandra Sims, 'New Zealand's Unfair Contract Terms Law Fails to Incentivise Businesses to Remove Potentially Unfair Terms from Standard Form Contracts' (2020) 27(3) Competition and Consumer Law Journal 235.

consumer. That explanation must be given early in the process. It is too late for someone to be given the opportunity to view (and save/print) after a person has begun entering in their details. For example, the explanation could be made available alongside an image or description of the service or good.

Intellectual Property – Royalty Distribution

This is not a specific question, but the DLA has some additional information to add about the use of smart contracts in royalty distribution in addition to Ujo music.

The use of blockchain, and therefore smart contracts, to assist musicians including with recovering royalty payments, has been discussed for a number of years, with a number of projects trialling blockchain.[45] More recent blockchain projects for royalty distribution include:

- Blokur[46] uses a blockchain to streamline the collection of royalties. Blokur has recently been announced as an approved partner of the Mechanical Licencing Collective (MLC)'s Data Quality Initiative.[47] The MLC is responsible for administering the compulsory licences for the use of musical works on streaming services in the United States. Blokur also allows users to request a license directly from publishers. Blokur first began on the Ethereum blockchain, but it is not clear if it is still using Ethereum.
- Smart contracts for Creative Interactions[48] – a project funded by Innovate UK under the Collaborative Research & Development programme, aims to facilitate low friction interactions between creators of music and their customers to unlock new value in the creative ecosystem by using blockchain.

[45] See, for example, Marcus O'Dair, 'How Blockchain Could Help Musicians Make a Living from Music' 7 July 2016, The Conversation, https://theconversation.com/how-blockchain-could-help-musicians-make-a-living-from-music-52125

[46] https://blokur.com/

[47] Silva Montello, The Mechanical Licensing Collective + Blokur = More $$$ for Music Publishers' 10 December 2020 https://medium.com/blokur/blokur-has-been-announced-as-an-approved-partner-of-the-mechanical-licensing-collective-mlc-s-89c066c43c86.

[48] https://www.digicatapult.org.uk/for-large-businesses/collaborative-research-and-development/smart-contracts-for-creative-ip-distribution

JURISDICTION & SMART CONTRACTS (CHAPTER 7)

47. Are you aware of, or do you foresee, any difficulties in identifying the place of formation of a smart contract? Paragraph 7.27

We do not foresee difficulties beyond those identified in the Call for Evidence for the reasons set out below.

In relation to determining jurisdiction of smart contracts, the location of formation of a contract provides a way to determine applicable law. However, consideration should be given to connecting factors affecting the contract in deciding jurisdiction.[49]

When it comes to smart contracts, the question of where the smart contract was made is complicated by possibility of cross-border parties (particularly digital nomads) initiating smart contracts entirely online and hence, no obvious state or country of contracting. This is further complicated by the distributed nature of the underlying technology.

The place of formation of a contract is important as it is one of the key factors to consider when determining of relevant jurisdiction.[50] Marshall in reconsidering the principles of contract law refers to this as the 'country' formulation of a contract.[51] In this case he considers that the place of contracting and place of performance carry a great weight in determining applicability of jurisdiction and hence the law.[52]

Traditionally, various courts have considered the place of contracting by its physical attributes. For example, McCafferty gives insight to how the Federal Circuit Courts determine enforceability in cases of contracts. One of the factors the courts look at is the place of contracting, especially with regards to a physical location.[53] In the case of *James Miller & Partners Ltd v Whitworth Street Estates (Manchester) Ltd*, the court considered the place of contracting as the physical location of where the contract was made. In that case it was Scotland.[54]

This idea of place of contract as a physical space raises difficulties in nominating the internet as a place of contracting for smart contracts. Similar challenges arise with smart contracts being created by distributed ledger systems, as all information is decentralised across multiple nodes which may or may not reside in a given jurisdiction. The nodes control information flow and therefore pinpointing a "server" location is difficult. The other option then is to ask whether the platform of agreement can be deemed a place of contracting. This can be a website hosting the transaction or

[49] Anne McCafferty (n1) 95.

[50] Anne McCafferty, "*Internet Contracting And E-Commerce Disputes: International And Internet Contracting And E-Commerce Disputes: International And U. S. Personal Jurisdiction U. S. Personal Jurisdiction*" (2011) 2 The Global Business Law Review The Global Business Law Review, 95.

[51] Brooke Marshall, "Reconsidering The Proper Law Of The Contract" (2021) 13(1) Melbourne Journal of International Law 31.

[52] Ibid.

[53] Ibid 96.

[54] *James Miller & Partners Ltd v Whitworth Street Estates (Manchester) Ltd* (1969) 1 WLR 377 CA.

even a signature verification app. As a platform, the eco-system exists within its terms and condition and arguably the law of its relevant jurisdiction (if and only if one is readily and exclusively identifiable).

Despite these challenges both courts and economists[55] have noted that the place of contracting is not a definitive approach to jurisdiction. There are other factors that must be taken into consideration. McCafferty identifies the place of contracting as part of a larger group of considerations in determining choice of law. Article 3 of the Rome Convention and the question of place of contracting, scholars such as Brigg have shown that the country formulation is not preferred when compared to the use of the system of law formulation.[56] The latter formulation considers connecting factors rather than intention of parties in contracting when looking at the application of law. The distinction was brought out in the case of *Rossano v Manufacturers' Life Insurance Company*, where the court upheld that the connecting factors to Ontario law provided for choice of law to be asserted there rather than in Egypt, where the parties contracted.[57]

48. In what circumstances do you think that jurisdiction to hear a dispute in relation to a smart contract could be based on the actions and location of an agent? Paragraph 7.30

We do not consider that computer programs that have reached agreement autonomously should be considered 'agents' of the parties for the purposes of the rules on jurisdiction. We agree with the view expressed in the call for evidence.

49. Do you think that a rejection of state law in favour of the rules contained in the platform's protocol is or should be a choice that can be given effect to under article 3(1) of the Rome I Regulation? Paragraph 7.42

Parties' freedom to contract should provide the opportunity to adopt a platform's rules and protocol that can be incorporated into the terms of the contract to govern the agreement between the parties, but as a matter of public policy, platforms should be governed by state law.

We agree with the view expressed in the Call for Evidence that a choice of platform rules would not be a choice of law that could be given effect to under article 3(1) of the Rome I Regulation (in its current form). We do not see merit in legislative proposal to allow a choice of a non-national system of law due to broader public policy implications.

[55] Dieter Schmidtchen, Roland Kirstein and Alexander Neunzig, *Conflict Of Law Rules And International Trade A Transaction Costs Approach* (Centre for the Study of Law and Economics, 2004), 23.

[56] Adrian Briggs, Agreements on Jurisdiction and Choice of Law (Oxford University Press, 2008) 435.

[57] *Rossano v Manufacturers Life Insurance Co* (1963) [1963] 2 QB 352.

Parties have freedom to contract and choose the terms of their contract. The *locus classicus* is the case of *Printing and Numerical Registering company v Sampson*.[58] In the case, George Jessel MR set out the principles of freedom to contract. He stated that as a matter of public policy, a person of full age and competent understanding shall have the utmost liberty of contract. He stated that this agreement to contract under their own terms must be held sacred and shall be enforced by the courts of Justice. This doctrine has been debated in courts over various contractual terms. For example, the concept of caveat emptor exhibits the range of freedom parties have to contract in a given matter in terms of risks taken to contract between parties

This doctrine permeates into the question of choice of law. The Rome I Regulation allows for parties to determine what law would apply. Under Article 3(1), parties must expressly demonstrate the choice of law. The parties can agree to a choice of law being applicable partly or wholly. We note that the Rome I Regulation does not state what type or which law is applicable. A literal meaning afforded to the convention would point us to consider all types of laws. Taken from this standpoint, the law as per Black's Law Dictionary, means a rule or method according to which actions coexist or follow each other. This could place sharia law, community-based law and in this case, computer code protocols under the definition of valid law.

However, the purposive approach to the Rome I Regulation extends to looking at the applicable law as state law. Martina Mantovani, in her presentation on conflict of laws in contractual and non-contractual matters recognizes that the law chosen by the parties to a contract must be state law.[59] She notes that the Regulation itself can not recognize anything else as formal law. Turning to recital 13 of the Regulation, we note the Regulation implies that parties cannot rely on non-state laws to govern, but rather they can incorporate them as terms of a contract. This means that the non-state laws can be relied on in the contract but do not govern the contract. The result is that parties cannot rely on computer code as a basis of governing law.

We can also draw comparison to common law principles such as from the guiding notes to the submission provided for the case of *Shamil Bank of Bahrain V Beximco*.[60] The question was whether the court could consider Sharia law as a permissible law in the law of contracts. The appeal was dismissed on the basis that sharia law was not a state-based law. It was not a law that was recognised in the United Kingdom. Therefore, U.K contracts law would apply in the matter. Sharia law is a non-state law that the courts could not apply. This is an important case since it provides a possible line of comparison when it comes to smart contract protocols as law.

From the case, we see Morison J firmly present a case in which non-state laws can exist in the same forum as state laws. In paragraph 54 of the decision his honour notes that the use if Sharia law was used as a tool to trump English law and exclude the courts.[61] The law, based on not state action, was not in any way capable of being

[58] *Printing and Numerical Registering Co v Sampson* (1875) (1875) LR 19 Eq 462.

[59] Martina Mantovani, "Freedom Of Choice And Applicable Law In The Absence Of Choice In Matters Relating To A Contract (Rome I Regulation)" in Conflict Of Laws In Contractual And Non Contractual Matters (2020).

[60] Shamil Bank of Bahrain v Beximco Pharmaceuticals Ltd [2004] 1 W.L.R. 1784.

[61] Ibid[54].

enforced despite connection to England and performance carried out in England. His honour pointed out that common law has provided a stable form of law under which contractual liability can be resolved. Under the scope of the decision and ratio, smart contract protocols can also be subject to subjective change at any point. Smart contract code and protocols may not set out in a formal document, differ from one transaction to another and cannot be pinpointed to a specific source of enforceability. This renders the code ineffective to be relied on as law or a source of law.

50. Can an express choice of applicable law be embodied in computer code? If possible, please provide any practical examples of a coded clause expressing a choice of applicable law. Paragraph 7.45

We assume it is technically possible but the real question is what would the purpose and value be of embodying express choice of applicable law in code. In a future state where laws of an applicable jurisdiction are also expressed as code, there would be obvious benefits to having the contract digitally connected to applicable laws of the jurisdiction.

It may also be beneficial for commercial businesses with significant number of contracts in multiple jurisdictions to be able to interrogate their portfolio of contracts to identify choice of law elections under their contracts. In this instance the code may not need to be shared operative code between counterparties to the smart contract, but rather code attached to the contract for contract management purposes.

For legal certainty however, we recommend that natural language provisions be included to make this express election, for certainty and to avoid any possible error or malfunction in the coded nomination.

51. What factors are capable of connecting a smart contract to a particular jurisdiction, for the purposes of article 4(3) and 4(4) of the Rome I Regulation? Paragraph 7.59

Despite the additional issues with selection of jurisdiction for smart contracts discussed in question 41, in many respects the identifying factors that are capable of connecting smart contracts to particular jurisdictions will be similar in principle to traditional contracts.

The jurisdiction of the smart contracting platform may be a relevant factor in the connection of smart contracts, and in particular where parties chose to run a smart contract on a platform and the platform rules influence the parties' express election of governing law of the jurisdiction of the platform.

52. Are you aware of, or do you foresee, any difficulties in the context of smart contracts in applying the choice of law rules that apply under the Rome I Regulation to contracts of carriage (article 5), consumer contracts (article 6), insurance contracts (article 7) and individual employment contracts (article 8)? Paragraph 7.61

Contracts of carriage (article 5)

The conceptual issue brought about by discrepancies between off-ledger ("physical") and on-ledger status of the contract provides difficulty in application of this provision. This causes difficulties in reconciling concepts such as the "habitual residence of the carrier" for the purposes of determining applicable law. However the concept of "place of delivery" should not prove difficult, given the reliance on off-ledger performance for contracts of carriage (e.g. supply contracts)

It must be noted that freedom of choice under article 3 is retained, for the parties to nominate the law of the country where:

a) the passenger has his habitual residence; or

b) the carrier has his habitual residence; or

c) the carrier has his place of central administration; or

d) the place of departure is situated; or

e) the place of destination is situated.

This remains consistent with current thoughts on best-practice for smart contracts, which would be to include a natural language governing law clause (as a boilerplate or non-functional note, for example).

Consumer contracts (article 6)

The same conceptual issue regarding "habitual residence" of the consumer will apply as that in contracts of carriage of goods. The question then is whether the self-executing nature of smart contracts create counterparty risk, given consumer contracts may be standard-form. Given Article 3 provides for freedom of choice of law, in some cases a seller may want discretion over whether or not to sell into a particular jurisdictions due to unfavourable governing law in the jurisdiction of the consumer. This may need to be built into the agreement through form of logic statement excluding sale to consumers from certain jurisdictions.

53. Do you think that a rule of jurisdiction based on the place of contractual performance can be applied where the performance takes place on a distributed ledger? Paragraph 7.72

We agree with the Call for Evidence in that place of performance can be determined traditionally were automation under a smart contact results in real world events.

For example, if a smart contract is meant to carry out the fulfilment of delivery of commodities, the place of performance doctrine would be effectively used based on the physical place of performance, namely the consignee's address. However, in cases where the results of the smart contract are within the distributed ledger system, then there is difficulty in placing jurisdiction by place of performance. This is more so with regards to services rendered totally on DLT. For example, purchase of crypto art or NFTs. The ownership of crypto art exists in the DLT together with the art itself. The art is not physically delivered to the buyer, only access to view the art digitally (unless delivery is construed as the delivery of data that can be visually interpreted).

Jurisdiction based on place of performance is a test used under the Brussels 1 Regulation to provide a context on how choice of law and conflict of law questions can be resolved. Article 5(1)(b) of the Brussels Regulation states that in the absence of an agreement to the contrary, the place of performance is the place where, under the contract, the goods or services were delivered or should have been delivered. This approach is what could be termed as a “cause-and-effect” mechanism in contracting. Jurisdiction by place of performance looks at where the effect of the contract took place. Therefore, when we turn to issues such as smart contracts, if we want to apply the same standard, we should ask whether the effects are ones that provide for delivery of goods or services in a physical place other than the distributed ledger system.

Faye Fangei, looks at this question in depth where she considers how courts should determine jurisdiction based on place of performance. She states that when it comes to digital contracts, especially concerning goods, the place of performance is where delivery of the products takes place, and the same with services.[62] The difficulty comes in where there are many places where performance takes place. She takes the view held in *Drack GmBh V Lex International Veriend GmBh*, where the court stated that when looking into provision of goods over the internet, in particular contracts performed in various places, the defendant must be ready to be sued in any place that has the closest connection with performance of the contract. Therefore, when applying this to the situation of smart contracts the question becomes, where are the resultant goods delivered or services performed. If there are multiple places of performance then the precedent above would satisfy the question of jurisdiction.

Faye also considers the question on fully digitized products that have no tangibility.[63] This presents a more difficult question to answer. In her reasoning, she raises this aspect as a non-conclusive argument, where there is no definite answer on performance. She states that the place of download cannot be fully considered the place of performance. The location of the receiving server could be a possibility of place of performance. Nonetheless, the reasoning brings about a more complicated scenario when we consider distributed ledger systems and the general effect of the architecture of a decentralized ledger system. The challenge is that fragments of a digital product within the distributed ledger cannot definitively identify the place of performance. Similar reasoning could be applied to smart contracts.

Therefore using place of performance in respect of fully digital products of smart contracts is problematic. The best alternative is to consider jurisdiction based on more connecting factors other than place of performance.

[62] Faye Fangfei, "Obstacles And Solutions To Internet Jurisdiction A Comparative Analysis Of The EU And US Laws" (2008) 3(4) Journal of International Commercial Law and Technology, 235.
[63] Ibid.

54. What factors do you think are capable of connecting a claim in relation to a smart contract to a particular jurisdiction? Para 7.85

In the recent UK case *Ion Science Ltd v Persons Unknown*, the High Court decided that the *lex situs* of a token is the place where the person or company who owned the coin or token is domiciled. This approach disregards the distributed nature of DLT, and imposes a legal reality to resolve a dispute in the UK jurisdiction. This may be problematic for contracts between multi-signatories, autonomous or anonymous parties to a contract.

As with many of our answers, if parties are able to use a properly developed smart contract platform with a well thought through set of features, such as those outlined in DIIP 2021, this will override any particular jurisdictional issues as it will allow – belt and brace style for the familiar set of boilerplate clauses that normally handle these things, to continue to do so, for example, to make adjudications about jurisdiction, by the natural language inclusion of a jurisdiction clause, where this will work together (rather than detract) with the platform to also enact any attached automations.

55. Which, if any, rules for establishing jurisdiction do you consider will be most problematic in the smart contracts context? Do you agree with our analysis of the issues as described in this call for evidence? Paragraph 7.86

We agree with the analysis of the issues as described in the Call for Evidence.

FINAL QUESTIONS (CHAPTER 8)

56. Are there any issues we should be considering on smart contracts beyond those we discuss and ask about in this call for evidence? Paragraph 8.3

Utility of smart contracts in facilitating IP transactions

The following response is a good example of a problem, a new type of transaction attempting to solve it, but the solution falling short when using a public, permissionless DLT solution that fails to allow for good natural language drafting to solve for the complexity that a logic based approach alone will not currently solve. A properly developed smart contract platform should be able to help get the benefit of the automation as well as the natural language. In its absence, relying on public platforms, we are unable to facilitate certain IP transactions and end up with some of the concerns set out below.

One of the most frequently cited concerns in the music industry is the vast sums of revenue that never reach the artist. Such complaints have become even more widespread with the growth of music streaming services. There are a number of factors contributing to this problem – the divisibility of copyright such that rights holders can transfer one or more of the exclusive rights in a copyright work to different persons, the lack of centrally available databases of ownership information, and the proliferation of intermediaries including publishers, record companies, content distribution platforms and financial payment processors who all take a clip of royalty payments that may be due to the artist.[64] All of this culminates in a complex and opaque web of licensing agreements that neither benefits rights holders nor users.

Smart contracts represent a promising tool for facilitating the transfer of rights in copyright protected works such as music, video, software, photos directly between IP right holders and users.[65]

Rights holders may be able to publish IP assets on a DLT, thus creating a quasi-immutable record of ownership. Smart contracts can be used to automate who has access to the relevant assets, and self-enforce any limitations of use built into the code by the rights holder.[66]

- Royalty payments can be coded in based on various algorithms e.g. adjustments to suit current market demand (demanding a higher price and thus maximising

[64] B Bodo et al., 'Blockchain and smart contracts: the missing link in copyright licensing?' (2018) 26(4) *International Journal of Law and Information Technology* 311-336, 333.

[65] Milan Sallaba et al., Blockchain @ Media - A new Game Changer for the Media Industry?, *Deloitte* 13 (2017), https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-mediatelecommunications/deloitte-PoV-blockchain-media.pdf.

[66] B Bodo et al., 'Blockchain and smart contracts: the missing link in copyright licensing?' (2018) 26(4) *International Journal of Law and Information Technology* 311-336, 333.

revenues) or lower prices when demand drops. Fees may also be differentiated based on commercial and non-commercial use.[67]

- Smart contracts running on DLT can provide additional transparency across which various stakeholders in a transaction can agree on, and automatically provide for, the transfer of funds to authorised parties in return for the granted rights in the relevant asset. This ensures a quick and direct payment of the relevant royalty to the person or persons who are entitled to receive royalty payments.
- Reliance on intermediaries is reduced such that payment times are significantly decreased and sent directly to the intended recipient.

Organisations such as Ujo music[68] and (although no longer operational useful as an illustrative example, JAAK[69]) were developing decentralised databases which rely on smart contracts to automate royalty payments. Although JAAK's 'KORD' blockchain network was initially piloted as a music-as-a-platform marketplace to buy and sell rights in music, its hope was to create a single database of royalty and IPR ownership information across a range of intellectual property rights and industries.[70] The promise of smart contract based management of copyright and other IP assets may further be bolstered by the use of non-fungible tokens (NFTs) that can act as unique certificates of ownership for any assigned digital assets. NFTs can be resold, distributed and licensed in accordance with the built-in restrictions coded into the NFT by the owner.

However, there are a significant number of unresolved issues which limit the applicability of smart contracts to IP transactions. Bodo, Gervais and Quintais for example have identified difficulties in mapping smart contracts to specific, individual uses of IP assets.[71]

- The regulation and enforcement of licensed use of on-chain vs off-chain IP assets is fraught with difficulty e.g. copyright is subject to a range of important exceptions which seek to appropriately balance the rights of authors and those of users. Smart contracts, which operate on 'if-then' rules are likely to face difficulties in assessing whether various off-chain uses are covered by exceptions or limitations. Pech has identified the potential for rights holders to 'over licence' where users may be required to enter into licences, when in fact no licence is required for a certain use at law.[72]
- Another crucial issue to resolve is how to address jurisdictional conflicts as between the copyright laws that exists in different territories, in particular different

[67] S Pech 'Copyright Unchained: How Blockchain Technology can Change the Administration and Distribution of Copyright Protected Works' (2020) 18(1) *Northwestern Journal of Technology and Intellectual Property* 1-50, 38 citing D Tapscott and A Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money Business, and the World* (Penguin Random House, 2nd ed, 2018, 234.

[68] https://ujomusic.com/

[69] https://jaak.io/

[70] https://theiabm.org/wp-content/uploads/2018/12/The-Blockchain-Pioneers-vaugn.pdf

[71] B Bodo et al., 'Blockchain and smart contracts: the missing link in copyright licensing?' (2018) 26(4) *International Journal of Law and Information Technology* 311-336, 333.

[72] S Pech 'Copyright Unchained: How Blockchain Technology can Change the Administration and Distribution of Copyright Protected Works' (2020) 18(1) *Northwestern Journal of Technology and Intellectual Property* 1-50, 45.

> rules around exhaustion of rights. While copyright is one of the more standardised areas of intellectual property protection and several international treaties on copyright and related rights exist – it is still the case that there is considerable variation in exceptions to copyright, terms and in fact the exclusive rights that attach to copyright works, particularly in the digital arena.[73] '

The fact that cryptocurrencies are considered necessary for payments to occur via smart contracts is also a limiting factor in the adoption of smart contracts for royalty payments. The purchase of cryptocurrencies remains relatively complex – whether artists seek to create their own or use existing currencies such as Bitcoin or Ether, the process for purchasing cryptocurrency is not well known and can take considerable time and effort (one of the very reasons that platforms such as Spotify were set up for music distribution).[74]

There are many open questions and challenges to the adoption of smart contracts in the field of IP licensing, notwithstanding general challenges of smart contracts particularly around technical restrictions and scalability. However, if industry and legislators can work together to overcome these problems, smart contracts could conceivably help to alleviate some of the challenges to traditional models of content distribution that exist in the digital sphere.

Assumptions underpinning the Call for Evidence

At the Hult International Business School students are taught to embrace traditional technology architecture including standards (as discussed in this document) but to see this as a commodity within the overall business ontology of the given solution. This ontology includes financial and other value based currencies and capital (financial, natural, human etc) that can be captured, tokenised and utilised. Top down legal (law) and bottom-up grass roots informal garments (lore) as well as expertise in relationship (interconnectedness between people, things, systems and AI) need to be considered.

57. Which other jurisdictions should we look to for their approach to smart contracts, and why? Paragraph 8.4

There may be merit in the Commission considering the following jurisdictions to the extent the Commission hasn't done so already:

[73] E.g. In New Zealand copyright generally lasts for the life of the author plus fifty years, whereas in many other jurisdictions including Australian and the United States the general position in life of the author plus seventy years.

[74] S Pech 'Copyright Unchained: How Blockchain Technology can Change the Administration and Distribution of Copyright Protected Works' (2020) 18(1) *Northwestern Journal of Technology and Intellectual Property* 1-50, 38 citing D Tapscott and A Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money Business, and the World* (Penguin Random House, 2nd ed, 2018, 233; Rachael O'Dwyer 'Does Digital Culture Want to be Free? How Blockchains Are Transforming the Economy of Cultural Goods' in Ruth Catlow et al. (eds) Artists Re:Thinking the Blockchain (2017), 301; Milan Sallaba et al., Blockchain @ Media - A new Game Changer for the Media Industry?, Deloitte 13 (2017), https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-mediatelecommunications/deloitte-PoV-blockchain-media.pdf, 11.

a) Australia in relation to the Australian Governments projects including Health Records (see Para 3.66) and Digital Law Technologies prototype.

b) The USA in relation to eChecks (see para 3.66).

c) Singapore generally in relation to a progressive jurisdiction that has actively taken steps to encourage digital transformation across key industries.

d) New Zealand in relation to progressive approach to rules as code for legislation.

58. Are there any legal reforms that you consider immediately necessary to remove uncertainty and unlock some of the potential benefits and cost savings of smart contracts? Paragraph 8.5

Yes. Support for a well-designed smart contract platform that is DIIP 2021 compliant (including support for the protocol, or something similar) will remove considerable barriers (risks) to the profession and business in adopting digital contracting with efficiency gaining automations and new structured data sets with less uncertainty. The average analogue contract has a nine per cent leakage of value, as a whole of UK economy consideration, this is substantial. This is before we even consider how we can use legal instruments and digital policy documents to better support compliance. We as a profession should lead the charge on making what we do more efficient – our legal duties in fact require it.

Legal reforms may also be required to encourage government funding to ensure platforms/infrastructure and applications developed to support any aspect of the law (disputes, legislation, contracting) take a long view to the future of the profession. This includes the impact of data collection and AI on citizen’s privacy, certainty and access when approaching the law. These are core legal ideals that must be safely transported to the digital domain. There is some evidence that relying solely on commercial motivations to drive digital infrastructure and applications will not be sufficient to ensure a safe and easy transition to digital smart legal contracts. There is also some evidence that relying on the current solutions developed in pursuit of solely commercial or crypto/commercial drivers will not lead to the low energy platforms required to help combat climate change.

The Digital Law Association commends the Law Commission on its work in relation to smart contracts and would welcome the opportunity to discuss any of these matters further.

FIND US AT

in @digitallawassociation

f @DigitalLawAssoc

@digitallawassociation

@DigitalLawAssoc

CONTACT US

✉ info@digitallawassociation.com