Deep Tech Dispute Resolution Lab

Submission to the UK Jurisdiction Taskforce consultation on the status of cryptoassets, distributed ledger technology and smart contracts under English private law

I. Introduction

The Deep Tech Dispute Resolution Lab ('Lab'), based at Oxford Law Faculty, welcomes the opportunity to contribute to the UKJT's consultation on the legal status of cryptoassets, DLT, smart contracts and associated technologies in the UK ('Consultation'). Our Lab aims to create an internationally leading hub of interdisciplinary and multi-stakeholder research cooperation that advances the study of deep technologies in dispute resolution. We provide a forum of discussion and knowledge sharing among a global network of researchers, the legal profession, dispute resolution institutions, companies, and the deep tech sector. In fostering close collaboration among Lab members and stakeholders, we produce high-quality research analysing this exciting, fast-moving field as well as incubate high potential start-ups working on deep technologies that could transform the landscape of dispute resolution.

We share the UKJT's view that English private law and the jurisdiction of England and Wales are well placed to provide the necessary infrastructure for addressing complex legal and regulatory issues arising from the rapid development and increasing use of new and deep technologies and the subsequent changes in the commercial landscape. We believe that this important foundation can be built by clarifying the current state of English law on the critical questions raised in this Consultation. In our submission, we wish to focus on the questions relating to the 'Enforceability of smart contracts' in paragraph 2 of Annex 1 (*Questions to be addressed in the Legal Statement*).

> **2 Enforceability of smart contracts**
>
> **2.1 Principal question:**
>
> ***In what circumstances is a smart contract capable of giving rise to binding legal obligations, enforceable in accordance with its terms (a "smart legal contract")?***
>
> **2.2 Ancillary questions**
>
> 2.2.1 How would an English court apply general principles of contractual interpretation to a smart contract written wholly or in part in computer code?
>
> 2.2.2 Under what circumstances would an English court look beyond the mere outcome of the running of any computer code that is or is part of a smart contract in determining the agreement between the parties?
>
> 2.2.3 Is a smart contract between anonymous or pseudo-anonymous parties capable of giving rise to binding legal obligations?
>
> 2.2.4 Could a statutory signature requirement be met by using a private key?
>
> 2.2.5 Could a statutory "in writing" requirement be met in the case of a smart contract composed partly or wholly of computer code?

II. Preliminary observation

There is potentially a conceptual issue arising from the Consultation in relation to the definition of a "smart legal contract". Annex 4, paragraph 5 characterises a "smart legal contract" as a contract that "either is, or is part of, a binding legal contract". A "smart contract", on the other hand, is defined as "merely" computer code that may or may not have legal ramifications. a smart contract may or may not be, or be part of, a smart legal contract.

In our experience, most people in the coder and programmer community view smart contracts as nothing more than autonomous software agents capable of self-execution. Vitalik Buterin's conceptualisation of "persistent scripts" or "stored procedures" may be a more accurate depiction. From this perspective, there is little point in drawing a line between a "smart legal contract" and a "smart contract" and any attempts at developing a test for deciding whether a smart contract is legally binding would be futile. Nevertheless, we agree with Sir Geoffrey Vos' remarks in the Consultation about the need for legal certainty and the protection of legal rights when market participants and investors enter into transactions involving cryptoassets and smart contracts. As such, the concept of a "smart legal contract" with binding legal obligations is a necessary development for the mainstream utilisation of these technologies.

III. Contract formation

The conventional elements of contract formation in English private law can be applied to smart legal contracts. The underlying process of formation remains generally unchanged when parties enter into a smart legal contract. There may be potential complications arising from the computer language used, depending on the form or model of the smart legal contract (such as the different models outlined in section 4 of Annex 4) and the interaction of code with natural language. However, in our view, such technical obstacles can generally be resolved by programmers and lawyers. The substance of formation rules in English contract law, such as offer and acceptance, intention to create legal relations, and consideration, are still applicable to smart legal contracts.

Some difficulties may arise where the smart legal contract is between anonymous or pseudo-anonymous parties (question 2.2.3 of Annex 1). We recognise that in most business transactions, knowing and verifying the identity of the counterparty is fundamental. A digital identity system that enables the verification of the counterparty's characteristics without revealing the underlying data related to the counterparty's actual identity could facilitate such anonymous or semi-anonymous contracting. However, it is still unclear how parties' contractual obligations and rights may be enforced against a counterparty in breach where the counterparty's real-world identity remains unknown. In designing digital identity systems, the current limits to enforcement by courts should be recognised. For example, how would a monetary damage award be enforced against an anonymous party in breach?

The Consultation asks two specific questions regarding formal requirements. Question 2.2.4 concerns whether private keys can be considered signatures to a binding legal contract. Private keys are commonly used (with corresponding public keys) in DLT-based smart contracts to verify the parties' identities. In our view, signing a smart legal contract with a private key can be deemed the legal signature of the party possessing the private key. However, an important caveat should be raised regarding the security of private keys. Currently, there are mechanisms available to protect private keys and their storage in smart cards or physical storerooms. The use of protected hardware and special edge services are highly encouraged but may not be enough to prevent private keys from being stolen.

If the broader aim of the Consultation and Legal Statement is to develop a legal foundation capable of supporting the mainstream utilisation of smart contracts, we believe that a smart contract composed partly or wholly in code should be covered under certain statutory "in writing" requirements (Question 2.2.5). Such requirements will have to adapted to recognise smart legal contracts as complying with the relevant formalities of "in writing".

IV. Interpretation of smart contracts

We believe the general principles of interpretation in English law can accommodate smart contracts written wholly or partly in code (question 2.2.1). With some adaptions to the courts' approach, it is possible to ascertain the intention of the parties or the specific meaning of a contractual term written in computer code (sometimes referred to as "dry code" as opposed to natural language that is described as "wet code"). While computer code appears precise (and seemingly does not leave room for different interpretations), there are still various potential problems. If the developer failed to see nuances in the code or there is a bug in the code, the "dry code" in the smart contract can bring about consequences that one or more parties did not foresee.

If there is an incompatibility or substantial difference between computer code and corresponding natural language in a smart legal contract, the courts will need the assistance of developers to explain the "natural meaning" of the terms forming a coding line. However, such assistance may not be enough given the differences in the logical architecture of computer code and natural language. Professor Sarah Green has argued that courts should apply a "reasonable coder" test for interpreting smart contracts. The test first applies the orthodox reasonable observer test to the last stage of the "human-to-human discussion" to asertain what the parties wanted the code to do. Second, the test turns to what a reasonable coder would understand the code to mean according to the interpretation of the agreement between the parties. However, we recognise that it may not be feasible for courts to readily introduce such a test (or any other proposals that significantly amend the orthodox test). As such, legislative guidelines on the interpretation of smart contracts would be useful.

V. Other issues to consider

We understand that the scope of the Consultation and Legal Statement is limited to private law and does not address other areas of law where smart contracts may also create legal uncertainty. Nevertheless, we believe there are still a range of private law issues relating to smart contracts that should be considered. We discuss three examples below.

First, there is the question of how oracles in smart contracts should be treated by existing principles and rules of English private law. Oracles bridge the real and virtual worlds in smart contracts where the network requires outside information (external data) to determine an outcome. Some oracles may be human-based, capable of incorporating their views on real-world events or verifying whether performance of a contractual term has taken place. The legal status and liability of oracles (in the case of flaws and errors) would need to be clarified.

Second, the Consultation does not examine the issue of remedies. We appreciate that it is difficult to discuss the availability of and access to appropriate remedial actions without first establishing the legal status of smart contracts and if they give rise to binding legal obligations and rights. However, we believe this is too important an issue to be left unaddressed.

Finally, there should be future opportunities for the LawTech Delivery Panel to explore and debate issues concerning risk allocation among different market participants (including developers) as well as the adoption of alternative dispute resolution mechanisms within smart contracts.

VI. Conclusion

We are very hopeful that the Legal Statement will provide further clarity on the circumstances in which smart contracts can create binding legal obligations. The issues raised in the Consultation, although not comprehensive, are important foundational questions regarding the enforceability of smart contracts. In our submission, we have also raised several alternative questions regarding smart contracts under the current framework of English private law.

Our general view is that the English legal framework—with the advantage of common law's flexibility, can be adapted to deal with many of the issues raised in the Consultation, without substantial legislative intervention. Should any new legislation be enacted to deal with cryptoassets, DLT, and smart contracts, we believe that the selected direction of travel that regulators adopt must be able engender trust among stakeholders and foster innovation in this space.