Response to the UKJT's Public Consultation on crypotoassets, DLT and Smart contracts under English private law[1]

I am not a lawyer, nor formally trained in the legal tradition. I have however done some of the early work in this space by designing the Ricardian Contract [2], a method by which ordinary contracts can be digitised and made available to computer programs without losing their primary audience, the human parties. I have also worked in areas that are integral to contracts, such as governance, information security and identity. I entered the space currently known as blockchain or distributed ledger technologies (DLT) in 1995, when it was more broadly known as financial cryptography.

I am encouraged by the UKJT's caution in proposing any new prescriptions to deal with the emergence of smart contracts. In my view, little or no new change is required of jurists in the English or common law tradition at least, beyond some familiarisation and the application of already well established principles. In contrast, I see a grave danger unfolding as countries rush in new and custom legislation to regularise the space. These countries will have to suffer inapplicable frameworks for a decade or more before they can ease them away.

I would like to respond to section 2 on Enforceability of smart contracts, but *in reverse order* as the story unfolds better in this way. With this approach, we might divide and conquer the complexities, and the finale of 2.1's Principle Question is dealt with more easily.

This response benefited from incisive commentary from Judge Enrique Agudo Fernandez (Court of First Instance and Instruction, Province of Madrid, Spain). The many errors in law and logic will be all mine.

Ian Grigg
May-June 2019
iang@iang.org

[1] UK Jurisdiction Taskforce Consultation:
https://www.lawsociety.org.uk/news/stories/cryptoassets-dlt-and-smart-contracts-ukjt-consultation/
[2] Ian Grigg, "The Ricardian Contract," First IEEE International Workshop on Electronic Contracting, (WEC) 2004, http://iang.org/papers/ricardian_contract.html

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 [12] 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?

2.2 Ancillary questions

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?

Smart Contracts of wholly computer code

It is unlikely that computer code could be considered "writing" in routine circumstances. Writing code is generally a specialist task for programmers who can be highly paid because the deployment of robust and secure code is a hard job. And even as there are millions of developers around the world, the languages used for smart contract code are highly specialised, cutting down the experts who know these languages to the thousands.

Further, even these experts will not wish to utter an opinion lightly; the trend today is to have smart contracts written by one programmer and audited by another, further stressing that this is not for the ordinary reader. The audit cost can range from £5,000 to £20,000.

> *The code of a smart contract is even opaque to the average coder under average circumstances.*

Work has been under way to develop new languages that would ease the reading test. But non-programmer languages have been a research topic for at least 4 decades, and in the opinion of this author, no substantial breakthrough in non-expert readability is expected in less than another decade.

Therefore, it is extremely unlikely that a 'smart contract' consisting only of computer code could be considered to be *in writing* as the normal person of reasonable capabilities would expect it.

> *It will be a high bar for a court to accept the code as "in writing."*

It also seems highly unlikely that a contract is found at all. It is an assumption at law that an adequate representation of reality and/or the real substance of the deal is understood by the parties before they should come to the conclusion of a contract. In addition, issues related to the information requirements on consumer contracts, use of standard terms or the simple opportunity to read a contract all play a part in achieving knowledge and then understanding of the obligational content and intent [3].

> *"So long as the operation of the computer program can be explained to judges who, like me, may be 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."*

Therein lies an assumption: if it can be explained to the reasonable judge, then it can (likely) be explained to the reasonable person. If not, then what? In our belief, an explanation of a contract for the reasonable judge and the reasonable person can only be found in prose that is related to the contract. A topic to which we turn in the next section.

A statutory exception could be carved out to deal with these difficulties, but we do not recommend this. By way of example, statutory exceptions were carved in several jurisdictions for digital signatures including the UK. But they would not likely make it easier for non-programmers to understand computer code, and thus will not make it easier to identify and

---

[3] Lord Hodge, Justice of the Supreme Court, "The Potential and Perils of Financial Technology: Can the Law adapt to cope?" The First Edinburgh FinTech Law Lecture, University of Edinburgh - 14 March 2019

close the contract. Providing such a subsidy as a statutory exception then risks a blowback from participants who realise, in albeit vague form, that the law forces them to accept something that is fundamentally opaque, and therefore dangerous to their wellbeing. As happened with digital signature designs, consumers will likely not adopt the system.

Interventions in law will likely create barriers that will reduce adoption.

Contracts consisting of partly computer code and partly prose

Let us now assume that the contract in question purports to consist in part of prose in plain English [4], in the normal contract tradition, and in other part of computer code. Let us also assume that the prose is divided into two parts, that part that relates in some way to the computer code, and that part that has little or nothing to do with the computer code (which latter part we ignore for this discussion).

Then, the question arises how the code relates to the (relevant) prose, and *vice versa*.

Within the computing world, when we do not or cannot practically understand the code, we almost always mitigate this lack with documentation of some form [5]. Practically all equipment - hard & soft - comes with instruction manuals, so it is no difficult step to realise that all usable smart contracts will come with some explanatory text of some form.

The smart contract will be described in explanatory text.

Then, it is only one more small step to place that explanatory step into the prose part of the contract [6]. Indeed, if not placed within the contract in express form, a court would tend to refer primarily to the explanatory text for that precise goal: explanation. And would therefore be minded to treat the explanatory text as implied terms, or in other laymen words, absorb the external explanatory text into the contract. It therefore makes more sense for authors of the contract to be express in their explanatory terms than implied.

The prose will describe the code.

Divergence between the code and the prose

Now that we have both an explanation in prose and a performance in code, the obvious question occurs: what if they diverge?

---

[4] Or any other relevant language to the parties.

[5] Not being able to understand the code is more routine than not, for the economic reasons of not wanting to spend the time unless absolutely necessary.

[6] Indeed, as an aside, the documentation that explicitly describes the interface for a piece of code is often called ‘the contract,’ a term of art in computer science.

Divergences can and will occur between the description in the prose and the computer code. The parties then will need to know which one dominates in the event of divergence and especially conflict.

I shall show by a logical argument that it is the prose that should dominate: A contract in words can express the dominance, so if a code-over-prose outcome is required it is a simple matter to write in exactly that clause:

> "in the event of conflict between this prose explanation and the code, the code shall dominate."

Likewise, the reverse can as easily be stated.

But code cannot state that, either way. Code itself doesn't admit the concepts of prose or dominance or any other legal concept, and indeed it only has the barest notion of code itself. So by elimination, any statement of dominance must be in prose.

Therefore any statement in the prose will dominate, because it is the one that can state it so, either way.

> *A clause in prose dominates the actions of the code.*

We can also look at the case of if the prose is silent on the issue of domination, that is, it does not include rules of conflict as above.

As we have noted, the parties, unless they are expert programmers, will have little chance of understanding the code. Then, to understand the code and audit it for conformance, they necessarily need to hire expert practitioners for that role - thus creating barriers and costs, and ultimately creating more prose on which the parties rely. And the court would likely find itself in the same position, having to rely on expert witnesses to interpret the code, and incurring the concomitant costs and risks.

As it happens, the computer science world is well used to handling this interchange between parties (or owners) and developers: developers are routinely employed to turn prose (documentation) into code, and are routinely and professionally held to the prose over the code. This is only economic - developers can understand prose, and IT purchasers rarely can understand code. The lingua franca for IT development is therefore prose documentation known more typically as *requirements*, and the delivered code is tested by the purchaser against that documentation.

Occam's razor suggests the prose should dominate, even when silent on conflict, as to do otherwise would go against computer science tradition.

> *The prose will always dominate the code, except or including where it explicitly passes domination to the code.*

It is of course better for the prose to explicitly state its dominance, as this reduces the chance that an alternate logic is sought and perhaps found in dispute.

Could a contract composed partly of computer code and partly of prose be found to be “in writing ?”

Then, finally we can attempt to address the original question (2.2.5).

A smart contract could be considered to be in writing, if at a minimum, any significant or disputed part of the code were described in the prose in such a fashion as to pass a reasonable person test or similar.

2.2.4 Could a statutory signature requirement[7] be met by using a private key?

The short answer is no, and to reach a level suitable for a statutory requirement a lot of support would be required.

Private keys are just numbers that can through mathematics produce other numbers. These latter produced or derivative numbers are public keys and digital signatures, which last can be verified the public key.

This reliance on numbers and mathematics presents a flaw - alone, observers would have no way of knowing who has used the private key to produce these verifiable numbers. When maths is done over numbers in high school, the presence in the student’s notebook is sufficient, but when numbers are sent over the Internet to support contracts, it is a whole other matter.

To support the interpretation of the produced numbers as signatures, statutory or otherwise, an *infrastructure* would typically be required to ensure that only a given person had access to that private key, and that the person understood that the use of the private key was equivalent to making a statutorily significant signature.

> *Only in the context of an infrastructure can signatures made by a private key be held equivalent to signing.*

---

[7] This is UKJT’s Consultation’s footnote 12: *For example, in the context of a disposition of an equitable interest (under s53(1)(c) Law of Property Act 1925 (LPA)) or of a legal assignment (under s136(1) LPA)?*

No such infrastructure is imposed in typical open blockchains. Such an infrastructure could be created, for example as has been envisaged under the EU's electronic signature directives [8].

A private law scenario is examined in "The Governed Blockchain" which envisages a blockchain community formed under a Constitution [9]. This legally significant document suggests basic rules and norms for the community, and refers resolution of disputes to its own forum of dispute resolution using Arbitration. The persons within the community, and especially the chosen forum, can more readily find that the digital signatures formed by the tools within its chosen blockchain technology are acceptable for a signing requirement, because its community is formed and is holistic, and its own forum of dispute resolution will likely align with the Community's intent.

Yet, even this mechanism is not without difficulties. In "Legal analysis of the governed blockchain" it was pointed out that the acceptance of the founding Constitution by each member suffered from the same difficulty - without a clear context, any digital signature collected over the Constitution does not clearly evidence anything of the signer [10]. The signature of the entering member over the Constitution may find itself challenged at law and may not meet a statutory or other requirement, thus throwing legal doubt on all following signatures with the blockchain.

This criticism could be overcome with a ceremony. For example already accepted members could endorse and witness the new member's acceptance, in person, a ceremony conducted successfully by CAcert [11]. But to date no blockchain known to the author has attempted that. Likewise, a contract signing ceremony can be made by placing the signing keys onto a hardware device and have it display the contract to be signed. Devices such as smartphones can be programmed to walk the user through the ceremony.

Therefore, in sum, a blockchain signature is a long way short of achieving legal recognition, because it is at heart just a number derived from another number, and labelling it as a signature means little. A court hearing such a case, and faced with a repudiation of entry into the contract by one or other party, would likely have to fall back to the normal process of identifying the

---

[8] Electronic Signatures Directive 1999/93/EC now replaced by eIDAS 910/2014

[9] Ian Grigg, "The Governed Blockchain," in relation to the EOS blockchain, 2018 http://iang.org/papers/the_governed_blockchain.html

[10] Adam Sanitt and Ian Grigg, "Legal analysis of the governed blockchain," a collaboration between Norton Rose Fulbright and block.one, 2018. https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/imported/emea_4957_online-publication-and-pdf__legal-analysis-of-the-governed-blockchain_v4.pdf?la=en&revision=c15aa8eb-48d5-4d06-8851-8226bdb1145f or https://www.nortonrosefulbright.com/en/knowledge/publications/0d56a3a5/legal-analysis-of-the-governed-blockchain

[11] CAcert uses a worldwide network of 'Assurers' to verify identity in person, and as an additional task, check the member's understanding and acceptance of the CAcert Community Agreement.

acceptance of the contract by other means: where is the offer and acceptance, was intent expressed, was understanding achieved, etc.

This leaves a problem for the court to solve, which might be expensive, and we might have been able to avoid it with better practices. Yet this author for one does not see this as more than any other difficult day in the courts. Firstly, courts are well equipped to dealing with this issue; to find the contract is the court's meat & drink. Secondly, relatively few contracts will end up in dispute, and in the case of a governed blockchain, even fewer would be expected to reach the courts, assuming the internal forum did a passable job.

2.2.3 Is a smart contract between anonymous or pseudo-anonymous parties capable of giving rise to binding legal obligations?

An anonymous person, say Alice [12], that files a dispute would typically have to show who she is in order to, at a minimum, gain standing. If Alice prefers not to show herself, many challenges would be placed before the court:

- ★ Is Alice the same person as the one who entered into and benefits from the contract?
- ★ Has Alice legal capacity to enter into a contract?
- ★ Is Alice within territorial jurisdiction? What rights apply?
- ★ How does anonymous Alice prepare her case? Is she the same person throughout?
- ★ How does the court enforce against Alice?
- ★ And, if the court rules for Alice, she would still have enjoyed the benefit of having less risk of enforcement on her. Is this just?

Therefore, I believe true anonymity to be incompatible to contracting.

> *Anonymous persons cannot sustain their place as parties to effectively sustain contractual obligations and benefits.*

On the other hand, a case filed against an anonymous person would likewise raise some questions - capacity of the party, an effective defence and a risk of unenforceability. Many courts happily hear cases against John Does and there is an unfortunate trend to litigate against inanimate objects such as seized monies, thus depriving their owners of a defence. The court could find merit in a case against an anonymous person for other purposes: insurance, unknown heirs or squatters, etc.

[12] In this document we use the normal cryptographic convention of Alice & Bob, and therefore the first party is female, the second male, the third (Carol) female, and so forth.

In the cryptographic tradition, we rely heavily on *pseudonymity*. A pseudonymous person is one that uses a cryptographic proof of existence and authority, but provides no other information customarily expected such as name and address. In technical terms, the *pseudonym* can sign with her key to enter into a contract, and sign again to show she is the same party when filing suit, thus establishing standing. Alice's key may also control an account with value, and thus both receive value due to the contract, and provide some remedy in enforcement. The court could also ask Alice as psuedonym for a bond of performance.

Pseudonymous parties may enter into contracts, and may be held to consequences.

Pseudonymity is distinct from anonymity, and is sometimes seen as a basis for identity. Blockchains work customarily with pseudonyms, a well-proven cryptographic security technique dating back to the 1990s.

The experience of the blockchain community EOS may be instructive here. In the case of 'ha4tamjtguge,' [13] claimant filed suit that he had been tricked by the respondent to place value into an account by name of 'ha4tamjtguge' now controlled by respondent, an unknown person. This case raised many novel questions: jurisdiction, crime, non-appearance of the respondent, pseudonymity.

The Arbitrator held that jurisdiction under the Constitution's article IX [14] for dispute resolution was established:

> "The person who initiated the registration, unstaking and/or otherwise attempted to remove the value was not clearly identified as a Member, nor was clearly tagged as using the chain. Yet, the Constitution is written both broadly and exclusively: in order to use the chain in any way, the Constitution probably applies automatically in much the same way that the notice posted at a railway station informs the users of their rights & obligations. The respondent undertook more than one action that would fall within this class, and could not be said to be an accidental trespasser."

The arbitrator further held that the pseudonym had adequate chance to respond by means of sending a Memo to the psuedonym, and publishing a general notice. The ruling was issued and enforced, the account was returned to the claimant.

---

[13] EOS Core Arbitration Case #ECAF00000023, "VH *versus* unidentified person(s) in possession of the private keys to EOS account ha4tamjtguge." Ruling issued 2018-11-08
https://www.eoscorearbitration.io/wp-content/uploads/2018/11/ECAF-Ruling-Case-0023-2018-11-08-AR-001.pdf

[14] *"All disputes arising out of or in connection with this Constitution shall be finally settled under the Rules of Dispute Resolution of the EOS Core Arbitration Forum by one or more arbitrators appointed in accordance with the said Rules."*

In principle, the presence of pseudonymity is not a barrier to binding legal obligations in the blockchain world. But a certain amount of support appears necessary. In “ha4tamjtguge” a Constitution referring to a community forum of dispute resolution was key to resolution, as was a strongly organised pseudonym system and persistent value at risk. Where the line is drawn would have to be found on a case by case basis, and therefore this question should be dealt with by courts and forums of arbitration rather than be predicted in legislation.

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?

As the running of computer code is opaque to all but a small group of expert, related programmers, and as these programmers are not typically the users of their code, we believe that an English court will almost always look beyond the computer code. In fact, we expect it to be the reverse - the court will only rarely look into the computer code when there is a precise question related to how the explanation and prose related. And even then, because of the opacity of computer code, the court will look for expert guidance.

In the alternate, a plastic example could be constructed: Two expert smart contract authors could agree on the running of a smart contract between themselves, perhaps in the context of a bet. Typically, even in unexpected circumstances, these two programmers would accept the result of the code. And a court would if faced with this rare circumstance simply agree: the code did what the code did.

In contrast, smart contracts today are almost always run between a business of some description and a consumer of likewise broad description. The business has chosen the smart contract, presumably by contracting experts. The consumer in contrast has for example only the website to go upon. In such a circumstance, a court would look broadly at what could be seen as the contract, including websites, videos, social media activities.

This would be a taxing investigation. A business could easily reduce the court’s time by declaring a Ricardian contract [15]. This mechanism ties the source code with prose such that it is

[15] Op cit. Ricardian Contracts are used in R3’s Corda and block.one’s EOSIO. See:
Richard Gendal Brown et al, “Corda: An Introduction,” 2016
https://docs.corda.net/_static/corda-introductory-whitepaper.pdf ;
Block.one, “EOSIO Software Release: Ricardian Contract Specifications and the Ricardian Template” Toolkit
https://medium.com/eosio/eosio-software-release-ricardian-contract-specifications-and-the-ricardian-template-toolkit-a0db787429d1

clear (by means of cryptographic hashes) what the description of the contract is. Tools, to the extent that they exist, could make it more obvious to the consumer what is included in the contract by following the trail of hashes and presenting the prose. At the least, that which was directly intended by the business to be part of the contract would then be clear.

A well-formed Ricardian contract that adequately represented the agreement would bring the court to a similar position as with contracts recorded on paper: it would set 'the four corners of the page.'

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?

I believe it would be a similar process to that with contracts recorded in paper.

1. Identify the prose, and any other elements such as code or documentation.
2. Establish that the parties had entered into an agreement.
3. Determine what that agreement was, taking into consideration the prose, the claims and actions of the parties and any customary or legal norms.
4. Apply the law.

If the prose clearly identifies computer code in some form, that can be considered. If there is no prose, and if there is no surrounding infrastructure to make code into a contract, the court will be tempted to find that there is no contract was formed, at least that could be enforced under the normal principles.

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”)?

Given all of the above, I believe that an English law court would find a good contract if some or all of these elements were found:

- The contract was primarily and usefully explained in prose,
  - the code and prose were tightly linked, and
  - the code followed the prose.
- An infrastructure exists that includes, *inter alia*,
  - founding documents,
  - membership ceremonies,
  - Minimum identity such as pseudonyms,
  - contract signing ceremonies, and
  - clear sign posts for dispute resolution.

Many issues such as enforcement remain, and where the line is drawn is hard to predict. I believe that the experience of cases is needed to find those answers, and any prescriptive approach will likely just hamper the development of experience and case law.