Smart Contracts under English Law

Just another use case or a legal paradigm shift?

Recent discussion among English lawyers on the subject of smart contracts has raised the question of whether a paradigm shift in private English contract law might be required to deal with disputes arising from their use. This paper discusses three issues:

i. What constitutes a smart contract?
ii. Which types of dispute might arise under a smart contract?
iii. Can the current legal framework respond adequately?

On closer inspection it becomes clear that once the technology and attributes of smart contracts are properly understood, existing contract law and dispute resolution processes are likely to be adequate. However, it is essential for non-specialists to not only be familiar with the underlying technology but also to be closely engaged with developments because, as with most new technologies, things will 'move fast and break often' [1].

1. Useful Terms and Concepts

Most lawyers can interpret what is meant by the legal terms fair, reasonable and even unconscionable. However, the technical language surrounding smart contracts seems to have a 'rabbit caught in the headlights' effect on them. This anxiety can be overcome quite easily, and this paper is intended to assist with just that.

Technical terms used in this paper are *italicised* and defined at the end of this paper where there is also a table of 'Agreed Facts' and 'Guidance Notes'. The aim of this is to show how certain important definitions and technical ideas might be used in a legal setting. A note of caution is needed: many technical terms can have a different meaning to their everyday one (the use of the word '*trustless'* is a case in point) when applied to different flavours of a technology and to differing use cases.

2. Smart Contracts

The term smart contract has recently entered the lexicon to describe agreements between parties with a digital component. There is no agreed definition of the term, but commentators seem to use the following two versions interchangeably:

a) Contracts with terms generated by and embedded in computer code.
b) Contracts generated by codified rules, but which are readable as natural language.

The two raise quite different legal issues from, potentially, a lack of explicit disclosure, transparency or intelligibility of, in a) *meaning to a natural person* and in b) *the rules which generated the natural language* text.

[1] Attributable to Mark Zuckerberg of Facebook according to Google.

However, in both cases the issues of whether there has been proper disclosure in a legal sense is present and, if so, whether there existed a common intention to be bound by the clauses which make up the agreement.

2.1. Neither Smart nor a Contract

To be a smart person is to have the ability to acquire and apply knowledge and skills to solving problems. It usually starts with the creation of novel ideas expressed using words, art, music or even computer code but can also involve creativity only in organising them. On the other hand, a contract, howsoever created [2], is a representation of an agreement where the parties intended to create legal relations. To be properly formed under English law, a contract needs to contain certain elements[3] and most also specify rights and remedies or rely on default rules of law.

The use of the prefix 'smart' in smart contract is ambiguous: it subsumes contracts which are generated using intelligent rules and those which are self-executing. Although in both cases using the descriptor 'smart' signals that there is no direct human involvement, self-executing contracts might be better described as 'dumb'. It is suggested that the degree of smartness of a contract depends on whether the terms it generates come from a linear process, calculation or algorithm (not very smart, almost dumb) or from multi-factorial inputs feeding into rules which evolve over time and improve themselves through finding a better fit with the ever-increasing data set (really smart). These are the extreme ends of the spectrum of 'smartness' in smart contracts as we know them to be today.

2.2. Is Computer Code a Language, an Asset or an Agent?

Smart contracts are associated with computer code which is defined as a set of abstract instructions which when grouped together make a computer program. The code or program is 'executed' by a computer, operating on inputs of data to produce outputs which are displayed, stored or trigger electrical or mechanical events. This gives it the characteristics of a language which allows those that can interpret it to understand each other and for physical devices to be triggered by the electrical signals created. Moreover, the code itself is an intangible asset, the intellectual property of the creator. Finally, it can be used to execute rules in the same way as giving an agent authority to do x if y occurs. Computer code can, therefore, play all three of the roles being discussed depending on the context.

In the context of a self-executing smart contract, the code is written in a non-natural, abstract *language*, has commercial value and is carried in its owners' financial accounts as an *asset* and performs an *agency* function for one or both of the parties.

2.3. Computer Code and Natural Language

A smart contract is frequently defined as "a self-executing contract with the terms of the agreement between buyer and seller being directly derived from

[2] Orally, in writing or by conduct.
[3] Including offer, acceptance, consideration, capacity and consent.

lines of code"[4]. This is not meant to imply that the code simply records (reads and writes to a storage device) a symbolic representation of the words of a contract but rather that the code generates symbols (words, numbers and prose) and initiates actions and events based on electrical inputs, data feeds and people's actions based on a rule set. In other words, it performs the drafting and / or execution of the contract. Code in this sense is more than storage and smart contracts are more than perfectly mapped representations of words and ideas.

Some have suggested that codification of an agreement cannot reflect the nuance and subtlety of prose in natural language. Code can reliably translate prose into a digital record, then store and restore each and every word that man can write. But it is right to say that code cannot currently interpret meaning very well, especially where the idea behind the words is non-binary such as 'reasonable' or 'best efforts' although complex programming rules are being developed to improve that. Experts generally agree that the breakthrough is unlikely to come simply from applying the brute force of computing power and adding ever-increasing complexity.

2.4. Self-Executing & Trustless

Proponents of smart contracts point out that many contain mechanisms which are highly efficient because they are self-executing, self-enforcing and trigger payments. They claim that the benefits include high levels of contract certainty and a reduction in transaction costs.

Another point that is frequently made, particularly where smart contracts exist on *Distributed Ledgers*, is that they are 'trustless'. This adjective is being used in almost the opposite sense to its everyday meaning of being not worthy of trust. In contrast, in the context of, say, Blockchain, it means a system not dependent on trust or without the need for trust of the counterparty. The confusing use of the term as 'a term of art' is revealed when we examine the Land Registry in England and Wales. This is a state run data repository (registry and database) which holds official records of title (deeds) for a property or piece of land. Few would suggest that the Land Registry creates or even holds smart contracts when parties register their sale and purchase on it even though it uses digital technology, has an online presence and uses software protocols[5]. However, all would agree that it is both trustworthy in the traditional sense of the word and also trustless in the distributed ledger sense as it substitutes the need for trust among counterparties with trust in the repository operated by the countries of England & Wales.

2.5. Identity of the Parties

As smart contracts are entered into electronically, establishing the identity[6] of the parties transacting online to a high standard is crucial. Progress in terms of identity security and multi-factor authentication have improved considerably

[4] Another definition from the tech community is "a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract" which is less helpful as it seems to ignore the contract element of the expression.

[5] The most widely used of all is 'http', the Hyper Text Transfer Protocol which defines how messages are formatted, transmitted and what actions Web servers and browsers should make.

6 Identity theft and the ability of a party seeking to release himself from a bad bargain after the event by denying acceptance come to mind.

over the last few years and billions of pounds are now routinely transferred across highly sophisticated payment systems daily making this a well understood technology. The law on this has also evolved and can deal with fraud, deception and liability arising from identity theft reasonably well.

2.6. Distributed Ledger as Repository

A repository or register is a place, physical or virtual, where parties store their agreements and records of ownership and transfer of assets such as money (bank), car (DVLA) and house (Land Registry). The content of a repository is useful as evidence if there is a dispute between parties in situations both where the state requires it and also where they agreed consensually to use one as the source of truth. If the repository is not state operated, such as a privately operated *Distributed Ledger*, the tribunal hearing the dispute will look to the claimant to prove the existence of an agreement to use the ledger. Following that, it will be able to make a judgment as to the quality of the content of the ledger as evidence. If the ledger is deemed secure and robust, the content will be treated as high quality evidence.

3. Artificial Intelligence & Machine Learning

Human intelligence evolved to optimise outcomes using approximations and simple heuristics because that uses fewer (scarce) resources than alternatives[7]. Human behaviour, and the economic activity and choices which flow from it, are also not always utility maximising nor consistent with traditional economic models of equilibrium. In fact, human intelligence is in general poor when it comes to accuracy, reliability and consistency, all things at which machine intelligence excels. Nonetheless, AI professionals often say that their aim is to replicate human (or superhuman) intelligence in machine-led decision making.

Smart contracts are increasingly being created by Artificial Intelligence (AI) and its latest offspring, Machine Learning (ML), a trend which is gathering momentum as it displaces the need for scarce and expensive human coders. It is conceivable that in the near future almost all agreements will involve AI and ML in some way, at some point, in the life cycle[8] of transactions. But what are these technologies and what are their legal implications?

3.1. A Simple Definition

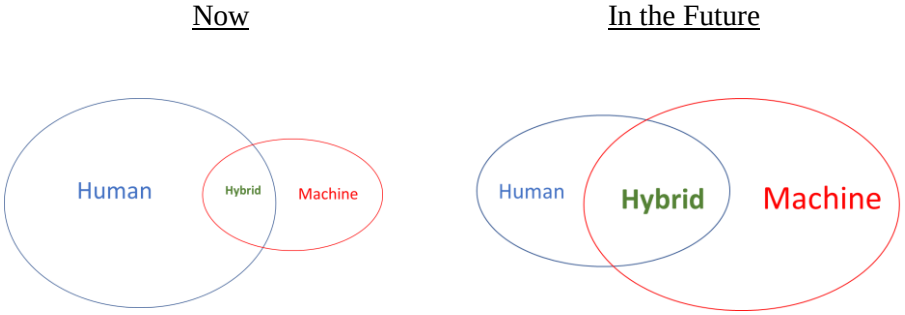
ML is an approach to designing a system whereby the output generating algorithm modifies itself (evolves) over time. The modification is based on back-testing by feeding in as inputs the cumulative data of the past into the current and a challenger model to see which would have performed better. The winner becomes the current model and is used in the hope of improving future outcomes.

This is to some extent similar to what humans do when they learn except for the complete absence of using as inputs human qualities[9] like fairness, intuition, empathy and values. Such qualities are not always compatible with the

7 In a sense this an instance of the principle of Occam's Razor.
8 From the point when an offer is made to up to the point when the contract is fully executed and ends, whether by way of fulfilment or breach.
9 Arguably, impossible to codify.

economic aims of commerce. They are also neither sequentially reasoned nor logical so incorporating them in computer algorithms is both difficult and considered to be unlikely to be profit maximising in the near term.

The danger with using AI and ML is that it is easy to apply it at the wrong times and to the wrong problems: for example, when pure human intelligence or automated rules would be optimal. In such situations hybridisation[10] produce the worst of both approaches rather than the best. To visualise, imagine a Venn diagram (comprising concentric ovals below) of the two sorts of intelligence filled with different types of problems. The proposition is that there will be only a tiny subset of problems where a mixing of the two intelligence methodologies adds value although it is conceded that as AI evolves the size of that subset might increase.



4. Self-Executing Contracts

Recording an agreement, whether it is smart or otherwise, is not the same as forming a legal contract or executing it. It is people and their lawyers who form contracts, both smart and stupid, by reflecting the joint intentions of the parties and checking that they satisfy the strict criteria set by contract law. But it is the parties who execute contracts.

4.1. Examples

Imagine the following two scenarios:

1. You enter a self-service car park, read the terms and conditions of use being displayed, accept the offer made by acquiring a ticket to open the barrier, then consume the benefits of the bargain (park your car) and finally settle the monetary compensation due to the operator by paying using your credit card to release the barrier. This exchange follows a computer-led *protocol* and your relationship with the car park operator has been governed by a legal contract. If there is a dispute between you and the operator, such as a third-party causing damage to your car while parked, you will have all legal remedies available subject to countering the usual disclaimer which deftly avoids liability for damage in both contract and negligence.

2. You buy a delayed flight insurance contract from your computer, accepting the terms and conditions of cover which state that upon

10 Put another way, do we really want to create a mule when what we need is a more robust, strong, compact and efficient horse?

> payment of £10 you will receive £200 compensation if BA 101 from London to Edinburgh departing on a certain date is delayed by more than 2 hours. You duly pay the £10 (identifying your credit card) and upload your BA 101 ticket number (identifying you) and receive an email confirmation of the contract generated from a template. Again, this is a perfectly formed and legally valid contract. On the day of the flight, the algorithm checks to see the departure time of BA 101 and finds that the airport published a time stamp for BA 101 which was indeed more than 2 hours after the scheduled time and so your credit card is credited with £200.

Although it is tempting to consider the first scenarion as being under a normal contract and the second a smart contract, they are remarkably similar: both used computer programs consisting of data, instructions, logic, mathematical models, algorithms and electro-mechanical devices to make visual representations and handle physical things (tickets, credit cards and electronic policy documents). Both also self-executed: the car parking transaction by way of gates opening and closing following collecting a ticket with terms and conditions on the back and then payment on departure and the insurance contract by entering credit details, making payment, a look up from a flight data feed and a claims payment.

The illusion of difference arises from the following:

1. The car parking contract is for an 'experienced' service, but an insurance contract is intangible, like a bet.
2. The insurance contract ended (with a claim[11]) without you being engaged whereas the car parking contract ended when you paid the fee to exit.

However, they are both, in legal and commercial terms, self-executing contracts[12], similar to buying a coffee from a vending machine. It is also worth noting that in both cases the transaction protocol was designed to simply replicate what human beings acting lawfully with sentience, planning, foresight and an eye for a legally binding exchange of value would have done, but with an important difference: no element of the sequence of events involved any discretion or judgement. There was simply an algorithmic decision to make an offer which a human accepted, followed by performance (execution). There was also no negotiation between computer and human and no opportunity for adjustment to the protocol, sequence of events and terms. In fact, the transactions (rather than the contracts) could not have been dumber[13] once the parameters were set. Unlike contracts formed between humans, both contracts were also totally inflexible once they reached the point of no return (formation) in that there was no obvious and efficient way to cancel or reverse the transactions, even by offering compensation. Humans will listen to offers for

[11] A human would undoubtedly have authorised the payment of the claim.
[12] The comparison becomes even more entertaining if you had used a self-driving car which decided to use a car park.
[13] The intelligent part was the simplicity based on standardisation designed by rather clever, even smart, humans.

early termination to reflect their opportunity costs and to help each other but most algorithms are deaf and rendered incommunicado by their creators.

4.2. Taxonomy

Given that computer code, algorithms and programs generate smart contracts, it is worth pausing to review the different ways that they can be created. Using a simple, high-level taxonomy, computer algorithms work on the basis of either:

a) Predetermined and fixed rules and data set, or
b) Predetermined and fixed rules applied to an evolving data set, or
c) An evolving rule set and / or data set.

The trend, however, is towards AI led smart contracts based on category c) and that is where cutting edge software developments driven by ML are taking place; where *algorithms* themselves change over time from an initial rule and data set in ways which are not predetermined. Such algorithms can be said to acquire a will of their own and 'evolve' to produce a better fit or outcome so as to maximise the creator's goal(s) such as profit or fewer complaints. They produce outputs which depend on the way that they are programmed. Their outputs then feed into contract terms (price, availability, service level etc.) and each time a new smart contract is formed, the terms can be different in the same way that a shop offers discounts at certain times or petrol retailers change fuel prices as part of a business strategy.

Our self-service car park and insurance examples above fall into category a). They could also fall into category b) where, say, the parking fee calculated is a function of occupancy (similar to Uber surge pricing) or the insurance premium adjusts as BA's record of delays deteriorates over time. Neither would fall into category c) unless the terms offered to customers changed over time by virtue of the algorithm making changes to itself.

5. Smart Contracts and the Law

5.1. Key Legal Issues

What legal issues do smart contracts raise and are any truly *sui generis* such that disputes arising need special rules and laws? Concerns about smart contracts seem to be focused on their legal status and uncertainty about how to apply existing law to them. Lawyers are asking the following questions in deciding whether there is a need for clarificatory steps[14] to be taken:

i. Whether smart contracts need a legal framework for their existence so that the parties may exercise rights. How they need to be formed to be legally valid. Whether they are binding in law once formed.
ii. Are any issues raised by identity, anonymity, the use of encryption or attempts to avoid state involvement.
iii. What rights do they create and are these different from traditional rights. What remedies are appropriate and are they different from traditional remedies.

[14] As at May 2019, The LawTech Delivery Panel was conducting a consultation primarily focused on Cryptoassets, but which also invited commentary on smart contract validity and enforceability.

iv. What rules of contractual interpretation apply.

5.2. Legal Framework and Validity

Private contracts, and so smart contracts, do not need a legal framework to exist and bind the parties, *per se*, although they can possess characteristics which can deem them void or voidable under law. In the context of smart contracts, this raises the question of whether they possess any particular characteristics which might make them fall into either of these categories.

In order to exercise rights under a smart contract, one needs to know the identity of the counterparty and this would not be known *prima facie* if a party (or parties) chose by agreement to act anonymously. Anonymity can also be used to hide a party's lack of capacity or illegality and that would make the contract void *ab initio* if discovered. It is increasingly common in digital transactions to, for example, map a real identity to an identifier (e.g. username) held by the system to avoid signalling which might affect the price in a traded market [15].

Validity, illegality and even the engagement of the legal system is not in play if the parties agree to, and do, perform their obligations. Validity requires formality (some form of writing) with email and digital signatures now being accepted by the English courts and that the agreement is not illegal as to its subject matter under a public policy test. Although English law will generally uphold any contract which is not illegal, public policy considerations can cause a contract to be void.

Once valid, the smart contract is binding if there is agreement of the terms after offer and acceptance has occurred and something of value has been exchanged. With smart contracts, these conditions can be easily met by requiring the offeror and offeree to use a digital protocol to communicate this. In practice this means designing the software and algorithms, process (including establishing identity), and email and other messaging as well as graphical interfaces to display and record what has been agreed, all of which is done routinely in e-commerce.

In the case of self-executing smart contracts which proceed irreversibly, calls for a legal decision are likely to occur after the event as they are usually instantly executed after formation. It therefore makes sense for the parties to a smart contract to ensure its validity from the beginning, before a dispute arises. Because of this, there are arguably good reasons for the state to insist that the parties make these as representations or even warranties in certain situations, such as where consumers are involved.

5.3. Identity

A smart contract where a payment is required to initiate it carries almost no identity risk where the parties 'piggyback' the sophisticated technologies employed by the payment service providers (banks and other authorised firms such as PayPal). The standard of proof of counterparty identity applied to remote (electronic) transactions depends on their value. For low value

[15] Such a veil should be possible to pierce in litigation with the cooperation of the operator of the system if such a right to disclosure is contained in the rules.

transactions, computers routinely check the identity of an online presence through asking the following three questions using electronic communications:

Question[16]	**Answer**
Who do you say you are?	(I am) John Smith.
What do you know about John Smith?	(My mother's maiden name was) Susan Jones.
Do you possess John Smith's smartphone?	Yes (If you send a code to the mobile phone registered to John Smith, you will receive it back)

This digital question and answer exchange is usually enough to prove identity for low value transactions but not for property or long term arrangements. This is consistent with the principles of English law which requires a higher standard of proof of acceptance (in which identity is subsumed) for high value or long-term transactions, usually by way of a physical signature or document exchange using known IP [17] addresses and end-to-end encryption.

5.4. Anonymity and Encryption

With smart contracts, anonymity usually means that a party to a contract is identified by an alias. Therefore, it is not possible to identify that party without reference to a key which can map the alias to a legally recognisable identity.

An English law contract can only be valid if it is entered into by a natural or legal person[18] with legal capacity to do so. If there is anonymity at the outset which is agreed as between the parties, this rule does not necessarily mean that the contract is invalid should that issue be raised subsequently. There is nothing in law *prima facie* preventing the parties from choosing to remain anonymous at the outset. This might at first blush be argued to be allowed under the doctrine of freedom of contract but that is not logical: the freedom of contract doctrine relates to the right of eligible parties to form contracts and bind each other (subject to the exceptions of illegality and public policy) but not parties who can never be identified as being a known natural or legal person. This is because, under English law, that freedom exists only where it does not violate contract law which requires proper and unambiguous identification of the parties. Failing to do that at the outset does not mean all is necessarily lost and a rescue is possible by establishing true, real-world identity later. This needs to be addressed by scholars or tested in court.

In any event, as between parties to a contract (whether smart or not), anonymity cannot exist where money is involved and traditional payment service providers are used. This is because compliance regulations[19] require providers to carry out identity checks under compliance regulations. This is not always the case where

[16] Phrased usually as Name, Mother's Maiden Name with a mobile device used for 'two-factor authentication'.
[17] A numerical label assigned to the device connected to a computer network which identifies and locates it.
[18] Human or entity with legal persona such as a company.
[19] Anti Money Laundering, Sanctions and Politically Exposed persons.

Cryptoassets and Cryptocurrencies are used as payment as they operate across private networks[20] which have no state regulator as yet. In these networks, the decision to require disclosure and verification of identity is made by the network operator. As a result, such networks (e.g. *distributed ledgers*) have the potential to host anonymous exchange and, as a consequence, hide illegal activity and convert the monetary proceeds of crime into Cryptoassets.

5.5. Human Rights and Equality Acts

Smart contracts which require a party to identify itself and which then perform profiling checks algorithmically can easily breach the Human Rights Act and Equality Act 2010 through illegal discrimination. Imagine an algorithm created to identify a person belonging to a religion or having a sexual identity so as to deny access to forming a smart contract. This situation could go undetected for a long time with no one the wiser as there would be no way of knowing the cause of the inability of a party to progress to contract formation. A pattern of such failure could highlight the potential breach, but it would then need to be prosecuted [21] and disclosure sought to establish whether there was discriminatory bias built into the algorithm's rules[22].

5.6. Contractual Interpretation, Rights and Remedies

English contract law has for centuries developed through case law and occasional statutory reform. In addition, there are doctrines and principles which are routinely applied to standard and novel issues of law and fact. As a system based on common law, it is widely accepted to be world-class in almost all respects and used throughout the world. The question here is whether it is fit for purpose to govern smart contracts as we currently have them and how we foresee they might develop.

A canter through the traditional categories of contractual interpretation issues might include reliance on negotiations prior to the formation of the agreement, whether to apply an objective test, and whether to apply a contextual and purposive approach. There seems to be nothing in this list to be particularly troublesome in the smart contract context. The issues which seem to be more difficult include how one might deal with mistake, rectification and the contra proferentem rule.

With smart contracts, it is highly likely that there will be one party in control of the technology (algorithms and processes) as well as initiating things by making offers. There is, as a result, scope for great asymmetry in the degree of control and bargaining power and this might lead to a large number of (allegedly) harmed counterparties arguing that there was mistake on their part as they were not given information as to the basis on which the offer they accepted was made. Also, parties would find it easy to purse compensation under the contra

[20] Frequently using Distributed Ledger to keep records.

[21] That decision usually requires an estimated better than 50% chance to proceed.

[22] Twitter and Facebook have faced accusations of using just such algorithms to create 'echo chambers' and deny access to parties not having a history of using the appropriate liberal voice on their sites.

proferentem rule based on the fact that the smart contract was both ambiguous as to its effect and 'drafted' by the counterpart's algorithms and computers.

Secondly, rectification of self-executing contracts handled by computers will present parties with an opportunity to bring lengthy delay as they scramble amongst complex data repositories to provide evidence in disclosure, notwithstanding the opacity and unintelligibility of evolving algorithms (see the Black Box problem below).

6. Disputes

Contract disputes turn on the application of law to facts and so any review of disputes arising under smart contracts must differentiate between the types of factual evidence which could be presented in context and the hard law which might apply to that. Having said that, it is impossible to accurately predict the types of dispute that will arise in the future in the domains we are discussing. However, a cursory review of the technologies and the way that they are currently being used suggests that the following issues have potential to be relevant.

6.1. The Black Box Problem

Many commercial applications of AI start with algorithms which are simply a 'black box' [23] to non-technical people. Their aim is to end up with a discrimination strategy based on an evolving model[24] which generates ever-changing contract terms. If the algorithm's rules are generated by ML, the 'black box' problem can be exacerbated to the point where even the coder who created the ML algorithmic processes cannot easily retrace or explain the rationale and steps in the evolution of the algorithm. The rules in such situations are possibly unknowable and even if they were knowable could be subject to commercial secrecy or privilege which creates a potentially insoluble problem. This would mean that any legal issue which turned on it would have to be based on empirical, outcome based evidence and judgment rather than proof of how (and why) the algorithm evolved from its initial conditions.

This poses several novel issues when viewed through the lenses of contract law, consumer protection regulations[25] and even public policy. For example, even if the final algorithm used to generate the contract was decipherable (known outputs for known inputs), could a disputant argue that the price generated in the smart contract was either not based on its reasonable expectations or was erroneous? If so, how could either party produce reliable evidence as to the workings of the model that led to the generation of the price charged? And would that not be an intractable problem if the evolution of the model itself was not knowable?

[23] In science, a black box is something which can be viewed in terms of its inputs and outputs without any knowledge of its internal workings.
[24] For if the evolved optimal model which produced the smart contract was predictable, that specific model would have been the starting point.
[25] e.g. UCTA 1977 where there was an attempt to limit liability.

6.2. Discriminatory Pricing

Discrimination which benefits only some customers is not a problem in and of itself in a generally competitive market; prices charged by an algorithm could just as well be lower as the system learns that such a strategy increases profits. However, a problem can arise when the strategy which generated discriminatory terms is either opaque or undiscoverable. The scope for intentional breaches of human rights and equality legislation driven by discriminatory algorithms has already been discussed above.

AI and ML technologies have already produced far-reaching changes to the marketplace dynamic as we can see from the arrival of multi-sided platforms such as Google and Facebook in, respectively, search and social media. These platforms offer a so-called 'free' service in return for the user agreeing to provide personal data and be exposed to digital advertising. However, the self-generated data of the user (U) has value, which is monetized by exposing U to targeted, paid-for advertisements. Each time a search is done or a post created by U, algorithms receive that data and use it to predict what U is likely to want to buy based on both U's prior behaviour (such as past searches and posts) and that of people similar to U. This predictive model then places the paid-for ad in front of U in return for income from the advertiser[26] who hopes to conclude a sale.

The legal question is whether the advertiser (with or without the platform's assistance) was within its rights to generate a (sale and purchase) agreement containing a price which discriminated against U because it was using data on U's history and propensity without disclosing that to U openly. And that this led U to pay more than he would have done if he had been 'anonymous'[27].

6.3. Disclaimers

Both the Black Box problem and discriminatory pricing point to a need to revisit legal orthodoxies when dealing with disputes which could arise under smart contracts. Where a 'black box' algorithm generates a smart contract, it can have legal implications in terms of validity, rights, duties and claims. If, say, a seller offers a 'personalized' smart (auto generated) contract to a retail customer[28] with a price computed by an intelligent (AI or ML driven) algorithm which incorporates that consumer's prior behaviour and other characteristics, and each customer is offered a different price, there would clearly be discrimination[29]

[26] The number, size and variety of competition law cases and successful prosecutions by state regulators which so often involve intelligent algorithm driven activity (pricing and ads) has shown the potential for abuse of a dominant position from deploying these technologies when trading with buyers and sellers. Amazon too has faced scrutiny around algorithmic pricing which favoured the prioritisation of its own products when selling from its website through what are for all intents and purposes smart contracts.

[27] Browsers now allow users to surf the web 'incognito' which can make their IP address unknowable, but this may not necessarily make them anonymous to a sophisticated algorithm.

[28] In contrast, the same practice would probably be fine in an unregulated business to business contract (unless public policy and other restrictions as to commercial practice and honesty were to bite) under the doctrine of caveat emptor.

[29] It is well known that airlines and hotels discriminate by altering their offers and discounts for each visitor to their websites based on algorithms which analyse their behaviour and propensity, aiming to maximise profit without losing the customer.

between customers. Although not all discrimination is illegal as car insurance pricing based on no-claims history confirms, there is a big difference between rational, justifiable and transparent differentiation of terms offered to customers and a smart contract generated by a Black Box type of algorithm. Lawyers advising companies using smart contracts will be aware of this or, if not, should be. And if they seek to protect their clients, they might well put into smart contract a legally robust disclaimer along the lines of:

"You accept that the price in your contract is determined by an algorithm and that this can lead to very different prices and terms being offered to different customers and even to the same customer at different times. You further accept that the methodology and rules used to generate prices and terms cannot be predicted or even known, and you agree that, to the extent this is the case, we cannot be required by you to produce them in the event of a dispute, except as required by law."

Some important legal questions might arise:

1. Would the disclaimer clauses survive a challenge under UCTA by a consumer?
2. Could the consumer (as claimant) not successfully assert that there was discrimination or unfairness (or another basis) for his claim that he was knowingly charged more than others through analysis of his vulnerability and access to his personal data and history?

Although the burden of proof would naturally fall on the claimant, it would have no way of establishing what had happened by way of asking for disclosure on the rules of the Black Box as *neither* party would be able to look inside the 'black box' to support its case. Ironically, even the algorithm-using respondent acting honestly would not be able to show conclusively how the smart contract terms were arrived at if required by law. The claimant's case would likely collapse for lack of evidence and it would be arguable that there exists a lacuna in the judicial system which prevents justice for the claimant even though the smart contract was entered into consensually.

Other legal issues a claim like this might raise includes the applicability of caveat emptor, freedom of contract, public policy, etc. and resolving such arguments would inevitably involve weighing up various competing doctrines. It is foreseeable that commentators would point to a lacuna in the law and injustice. Which so often results in a call for a hurried legislative fix and often bad law being legislated. With the potential for a deluge of claimants to suddenly appear, the legislature (and judiciary) would be nervous and inclined to pass protective legislation (and judgements) and one can see the floodgates argument also being made.

7. Benefits of Smart Contracts

Weighing in against the potential for rather awkward (and hard) cases to be brought to the courts are the significant benefits of smart contracts. *Algorithms* and *distributed ledgers* used, respectively, to generate and manage smart

contracts, can provide enormous efficiency benefits to the parties to a contract[30]. *Algorithms* provide speed and accuracy of information exchange to achieve offer and acceptance of key terms. D*istributed ledgers* receive, amend and hold contracts with a high degree of certainty that the content of the agreement has not been tampered with[31] and so eliminate tampering which maintains an irrefutable (based on probability theory) trail and quality of evidence going well beyond the civil threshold of proof.

Moreover, a transaction recorded under an agreed *protocol* with *encryption* and promulgated and stored (even amended) using *distributed ledger* is safer, cheaper and easier to evidence when things go wrong. And there can never be more than one version of the contract or its history to argue over.

8. The Future

Disputes under smart contracts might bring some novel issues into play but the issues, while being different in some respects, are not going to be dealt effectively with anticipatory legislation because the subject matter and issues on which decisions will depend are simply impossible to foresee. It is also difficult to predict whether the majority of disputes will involve consumers and businesses or be between businesses or even technology firms. In view of this, a good approach is for firms, their lawyers and judges to be armed with knowledge and insights so as to present and resolve the issues clearly and intelligently in order that current law can develop incrementally.

To do this, legislators, judges and lawyers will need to understand and interpret claims and responses in unusual scenarios of which they (and even the parties) will have had little experience. For example, where one of the parties argues that the contract was not properly formed, the tribunal will need to be persuaded that the use of a specific technology and process included offer, acceptance, consideration and formality. In cases where the existence of the agreement itself was not in question, the dispute would likely be about performance, breach and remedy. Possibly requiring a decision on whether the parties explicitly agreed to use an algorithm which generated (wrote) the contract terms on behalf of one of them [32] or whether statutory protection against disclaiming liability applies.

It is considered likely that these and other similar or derivative legal issues will represent the bulk of cases brought to courts with the occasional high-level technical dispute on whether, say, a *distributed ledger* system can be relied on to produce evidence which passes the civil threshold of proof. And even in such cases if the key issue turned on the computer code's embedded, abstract rules or mathematical probabilities, expert witnesses could be used to assist the

[30] Another beneficial use case for AI is when lawyers use it to generate draft contracts (templates) which are then used as a starting point by human lawyers. Such programs extract relevant data from prior communications and high-level, non-binding, agreements such as emails, Letters of Intent or Heads of Agreement and populate relevant standard contract clauses with facts.

[31] This is because the latest version of a contract and the history of how it came about is secured using decentralisation and consensus based rules built into the technology.

[32] Possibly invoking the contra proferentem rule.

lawyers and tribunal on what would likely be narrow, technical points of evidence.

Much has been written over the centuries about the ability of the English legal system to deal effectively and fairly with private contractual disputes. Most would agree that its strength[33] lies in the inherent flexibility of its common law tradition and light touch legislation. The legal profession is currently reviewing the law applicable to technology-led transactions involving *Distributed Ledger* technology, *Cryptoassets* and *Tokens* and appears cautious in claiming that it is fully equipped to regulate the needs of parties contracting in the digital age.

Rightly driven by a desire to be a world class jurisdiction for hearing technology disputes, English law practitioners should not be afraid that an uncertain future lies ahead for the English legal system in that domain. And if there is any such anxiety, it can easily be rectified through consultation[34], scholarly research and familiarisation and training.

The legal profession does, however, need to understand the basics of smart contracts to make correct judicial decisions and that is certainly manageable even though technical issues at the extreme might be beyond their ken. Novel technology disputes are routinely heard by the Technology and Intellectual Property courts and tribunals and, whether or not experts are used, appropriately trained judicial decision makers seem to be perfectly capable of delivering justice in dealing with them. In the end, smart contracts and related technologies are really not very different in the challenges they pose. To quote Marie Antoinette: "There is nothing new except what has been forgotten."

Manu Duggal

28 May 2019

Manu Duggal is an arbitrator, consultant and expert witness. He specialises in the functional areas of technology and finance in the context of disputes, competition and insurance under English law. He has been a founder and investor in technology businesses and in particular marketplace platforms for many years. He is a Member of the Chartered Institute of Arbitrators and sits on appeals as a Member of the Charity Tribunal. He holds an LLM, an MBA and degrees in Physics and Law.

www.manuduggal.com

[33] English private law is of course not unique in this and there are many common law jurisdictions which are formidable competitors.

[34] The UK Jurisdiction Taskforce of the LawTech Delivery Panel is aiming to do just this.

Key Definitions

The aim of this section is to provide a simplified, jargon-free perspective on key concepts and terms frequently used in discussion about smart contracts. Together, they provide a framework for understanding the core technologies used to create, hold and make smart contracts. A note of caution is needed: as with most new technologies, a technical term can have a different meaning when applied to different flavours of the technology and to differing use cases.

Algorithm: A procedure coded in a programming language which defines instructions to be executed in order to get a desired result.

Artificial Intelligence: Computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

Bitcoin: A monetization of *Blockchain* technology through the creation, transfer and tracking of a notional 'cryptocurrency' exchangeable into traditional currency.

Blockchain: A specific deployment or use case of a *distributed ledger*.

Code: A set of abstract instructions which when part of a bigger library makes a computer program. This is 'executed' by a computer, operating on inputs of data to produce outputs which are displayed, stored or trigger electrical or mechanical events.

Distributed Ledger: A network of computers which operate across national boundaries and compete to store the encrypted content of the latest version of an entry of numbers, letters and pictures in a ledger.

Encryption: Encoding information using a cipher so that only authorized parties possessing the decoding cipher can access it. The original message or data is transformed (encrypted [35]) using an algorithm and that has to be reversed by another algorithm possessed by the intended recipient(s) to restore the original. Encryption does not itself prevent interference and capture of the data but makes the content unintelligible to an interceptor.

Machine Learning: An application of Artificial Intelligence which can automatically create and evolve rules and models to achieve a target outcome and improve them using data but without explicit programming. The system learns and improves often using rival models and back testing.

Miner: Digital actor on a *distributed ledger* using computers to add a marker to the last version of the ledger entry (preserving the original) and hold it in return for a small fee. When users of a *distributed ledger* (qua contracting parties) create an entry on the ledger (say a trade or a contract), a new competition is triggered among *Miners* with the winner

35 Encryption is not new – the German Enigma code was deciphered at Bletchley Park during World War II.

authorised to hold the latest version of the ledger entry after it has marked it up with an extending tag while retaining the history of past holders and their mark ups.[36]

Protocol: In order for two computers to talk to each other, they must be speaking the same language. A protocol is a set of rules that define the meaning of what is sent and received between computers. To work, there must be a pre-existing agreement as to how the information will be structured and how each side will send and receive it.

Token: Similar to a betting 'chip 'in a casino, a token is a digital asset which can be created, exchanged with others for non-monetary assets or rights and for real assets (money) and intangible assets (services or points). The value of a token is a function of the trust the holder has that it will be honoured by others when an exchange is sought.

36 Each time the ledger entry is changed, the content grows in the same way as a physical land title Deed grows with the addition of each new owner. The key difference here is that each Miner holds all the complete history (distributed consensus) but only one current version of the ledger entry exists. The ledger entry can be checked by retracing the mark ups (extending tags) made by all Miners who marked it up without the need for a central or state sponsored repository. Which means that collusion and tampering is said to be near-impossible.

Guidance Notes

The following table presents in the artificial form of 'Agreed Fact' and 'Guidance Note' how some of these definitions and technical ideas might be used in a legal setting:

Agreed Fact	**Guidance Note**
An *algorithm* was used by A to generate the smart contract with B using pre-defined inputs and rules programmed by Party A.	Even though the *algorithm* operated without reference to A, it reflects the means and medium by which A made the offer which B accepted in forming the contract. A is responsible for the result of the operation of the *algorithm*, including the terms of the contract. B is a party to the contract on those terms to the extent that acceptance can be shown.
A d*istributed ledger* was used by A and B to hold a record of their original smart contract, subsequent amendments and assignment or sale of that.	Challenges to the existence of a contract or, on the other hand, validity are clearly not the same thing. *Distributed ledgers* run by established operators with published *protocols* can be presumed to be secure and a source of truth as to the record they hold and its history. As such, the existence of the contract can start with that presumption. It is a matter of legal interpretation whether it is illegal or fails for validity.
Encryption was used by A when it sent the smart contract to B for acceptance to maintain confidentiality. A key was provided to B so that it could read the contract and it was agreed that communications and amendments to it would be encrypted with the same key.	The revocation or substitution of the *encryption* key by A was not permitted. Thus, it cannot now claim that any changes made to the contract after that are valid and binding on B because B's ability to read those has been removed by A's actions. As such, the changes made by A were not communicated to B.