Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Smart Contracts: coding the fine print

A legal and regulatory guide

Contents

Why do businesses need to understand smart contracts?

Smart contracts are receiving significant attention from businesses across a broad range of industry sectors, and for good reasons. Smart contracts have the potential to:

- Deliver costs savings by streamlining back office processes
- Verify identity and certify transactions
- Provide an indelible record of transacting history
- Enable strangers to trade directly with each other without the need for a trusted third party intermediary
- Automate buy, sell and supply transactions on a B2B and B2C basis, in combination with the Internet of Things

> Smart contracting 'technology could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between $15 – 20 billion per annum by 2022'
>
> *Santander, The Fintech 2.0 Paper: Rebooting Financial Services, 2015*

This briefing considers the potential impact of smart contracts upon various industry sectors, outlines the nature of smart contracts and examines potential obstacles to their uptake. It focusses on whether they have legally binding contractual effect and identifies other contractual risks. Finally it considers how the regulatory and consumer protection landscape will need to be factored into risk assessments for the use of smart contracts by businesses.

Which industry sectors might be affected?

Financial institutions

Banks, financial institutions and insurers are considering use cases for smart contracts and the technology that typically underpins them (so-called 'blockchain' technology) across wide areas of business operations, including in relation to issuing and transferring securities, post-trade processing, syndicated lending, trade finance, swaps, derivatives, foreign exchange and potentially anywhere where counterparty risk arises. Other applications for the technology might include asset, know your client (KYC) and anti-money laundering (AML) registries as well as records of ownership held electronically (including, potentially, securities accounts, investment accounts and cash accounts).

The technology that underpins smart contracts could also be used for intragroup accounts and similar records.

Such applications are not purely hypothetical. The NASDAQ exchange has announced that an issuer (a private company) was able to use NASDAQ's Linq blockchain ledger technology successfully to complete and record the issue of shares to a private investor. The system has potential application in many clearing and settlement contexts.

Insurers are considering the potential use of smart contracting, initially for more simple policies - for example, using smart contracts for flood or crop policies where automated claims payments are linked to a weather data feed or water level monitor. For now, smart contracting is confined to simple insurance risks where pre-contractual disclosures are not required. To the underwriter's advantage, however, automated claims linked to blockchain technology significantly reduce the risk of fraudulent claims, with reduced administrative costs for the insurer. With data fed into such technology, premium levels can be adjusted automatically in response to certain pre-determined events or information received.

Property and real estate

Real estate transfers depend on centralised title registries. Blockchain technology underpinning smart contracts could decentralise them. For example, Factom has been reported as having been in discussions with the government of Honduras to develop a digitised land title registry deploying such technology.

Smart contracts could be used for some real estate transactions (subject to important statutory formalities in relation to certain types of transactions).

Consumer markets

IBM and Samsung have collaborated to develop proof-of-concept use cases in relation to smart contracts.

On a B2C basis, IBM and Samsung have demonstrated the viability of a Samsung washing machine, connected to the Internet of Things, to deploy a smart contract to order and pay for refills of detergent from a retailer, and to detect an impending parts failure, interrogate existing warranty status and order warranty service for the machine (as well as to order and pay for out-of-warranty service thereafter). It could do all this without a centralised controller mediating between the parties.

Energy

On a B2C basis, IBM and Samsung have also demonstrated the viability of using a smart contract associated with a Samsung washing machine, connected to the Internet of Things, to arbitrage energy consumption with other appliances in the home.

The IBM / Samsung proof-of-concept use case also demonstrated that a smart contract was able to reduce household overall consumption at electricity peak cost times.

Infrastructure, mining and commodities

Industrial application of smart contracts may bring efficiencies to infrastructure management.

Operating in conjunction with infrastructure connected via the Internet of Things, smart contracts may provide opportunities to automate processes as diverse as routine and preventative maintenance, subcontractor tendering and call-off, and wider supply chain administration.

The technology underlying smart contracts could be used as an indelible record for ownership of high value commodities. For example, Everledger is developing the technology to track transactions and ownership in relation to diamonds, with potential application for use in verification by insurers, owners, claimants and law enforcement agencies.

Transport

Use of smart contracts in relation to vehicle finance leasing products could include, for example, the ability of a smart contract, working in combination with the Internet of Things, to deploy a 'kill switch' within a leased parked car in order to make it inoperable when repayments have not been maintained.

UATP (a payment network privately owned by many of the world's airlines) has announced a partnership with Bitnet that would enable airlines to accept Bitcoin using the technology that supports smart contracts. However, smart contracts and its supporting technology may have the potential for far wider application in the travel industry (including use for passenger identity verification and ticketing).

Smart contracts could be linked by the Internet of Things to make vehicle road tax payments for on-road vehicles, pay parking charges and book vehicle servicing and, in the rail industry, to make season ticket payments and administer 'Delay Repay' or other passenger compensation schemes using passenger identity verification.

Public authorities may be able to use the technology to maintain vehicle asset registries.

Defect reporting and authorisation of rectification work orders could be streamlined through smart contracts, and better data collection could lead to increased asset availability and reliability.

Technology and innovation

'These technological changes could foretell the biggest revolution since the origin of general purpose computing and transaction processing systems'

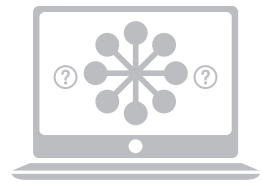
(IBM Institute for Business Value, Empowering the Edge: Practical Insights on a Decentralised Internet of Things, 2015)

Smart contracting and its supporting technology, in combination with the Internet of Things, may lay the foundations for decentralisation of many currently centralised technology processes.

Decentralisation may provide improved robustness by removing single points of failure that could exist in centralised technology networks, and give impetus for technology and electronics industry suppliers to develop entirely new product and service offerings (such as data storage and management systems and order processing and management functionality).

Smart contracts may enable many machine-human interactions to become machine-to-machine interactions, creating opportunities for device manufacturers.

Devices deploying smart contracts over the Internet of Things are likely to generate vast amounts of data, giving the potential for new storage solutions to be commercialised by technology businesses.



What is a smart contract?

A smart contract is 'a set of promises, specified in digital form, including protocols within which the parties perform on these promises'

(Nick Szabo, Smart Contracts: Building Blocks for Digital Markets, 1996)

Nick Szabo is widely credited for inventing the idea of a smart contract. He gives the example of a drinks vending machine as something embodying its characteristics. When the money is paid, an irrevocable set of actions is put in motion. The money is retained and a drink is supplied. The transaction cannot be stopped in mid flow. The money cannot be returned when the drink is supplied. The transaction's terms are in a sense embedded in the hardware and in the software that runs the machine.

A smart contract is both an instance of coding and a software program that encodes conditions and outcomes. It has these key characteristics:

Digital form: it is in code form

Embedded: contractual clauses (or equivalent functional outcomes) are embedded as code in hardware or software

Performance mediated by technological means: the release of payments and other actions are enabled by technology and rules-based operations

Irrevocable: once initiated, the outcomes for which a smart contract is encoded to perform cannot typically be stopped (unless an outcome depends on an unmet condition). It performs automatically

How do smart contracts work?

The modern conception of a smart contract typically depends on technology similar to that underpinning Bitcoin: a distributed ledger called a 'blockchain'.

A blockchain is a distributed database that records each transaction in a block with the following characteristics:

Hashing: each block contains a hash that is unique to, and references, the previous block in the chain

Transparent: if any data in any block in the chain are later altered, this is immediately apparent to all participants in that system, as that block's hash (and that of any subsequent block) will no longer correspond to the later block's record of that hash

Indelible record: in this way a blockchain provides a complete record of all transactions

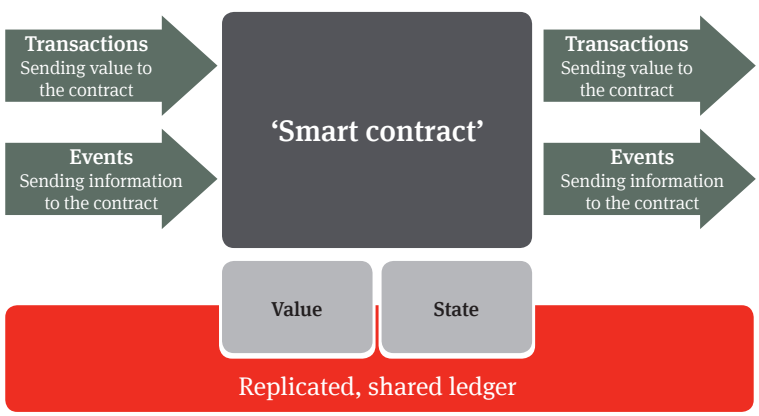
Blockchains are sufficient, but not necessary, for the operation of smart contracts. Other technology can be used. (As many smart contract solutions currently use blockchain technology, this briefing discusses smart contracts in relation to that technology.) They are:

Public or closed: they can be public (open for all to inspect, and controlled by no-one) or they can operate privately within a closed community of participants (for example, within a virtual private network)

Distributed: they operate on a distributed basis – that is, the record or ledger of all transactions is replicated in full on each participant's computer. Accordingly they are highly transparent, because each participant has a complete, traceable record of every transaction recorded on the blockchain. Similarly, smart contracts operating within a blockchain operate on a distributed basis, and both blockchains and smart contracts use cryptography for verification / authentication

Correspondence between the respective copies of the ledger provides the requisite trust between participants, even if they are strangers. It is the system itself, rather than a central authority or third party with whom the parties interact, that is the basis of that trust.

A smart contract within a distributed ledger constituted by a blockchain can be represented to operate like this:



(Richard Gendal Brown, A Simple Model for Smart Contracts, 10 February 2015)

Are there obstacles to widespread adoption?

There are a number of factors that could impede uptake of smart contracting generally, or that need to be taken into account by a business proposing to deploy smart contracts.

The longer the term of a smart contract, the less smart it becomes

Smart contracts may be most effective at delivering their intended value where they are short term or are of instantaneous effect. A distributed ledger recording a smart contract could in theory exist for many years. It is difficult to produce coding intended to have an indefinite duration, as software programmers look to cater for all future eventualities (for example, compatibility with changes in supporting technologies).

Smart contracts may depend on external information sources that inform a smart contract about a particular state of affairs (for example, the satisfaction of a condition), known as 'state' (shown in the diagram above). An example of an external information source is an index of price movements. The longer a smart contract is intended to run for, the greater the risk that such external information sources will cease to exist.

Trade embargos and governmental interventions (such as new legislation) that can make a contract or its performance illegal can supervene after a contract has been entered into and before performance has occurred. This risk becomes greater the longer a smart contract runs for. (There may sometimes be technical solutions to address this risk, such as setting the smart contract to respond to an updating requirement sent by an administrator to reflect, for example, a new regulatory requirement).

Will it be possible to demonstrate that the coding performs as the parties intended?

How will it be possible (without actually instigating the operation of the smart contract) to prove to the satisfaction of both parties that the coding of a smart contract can and will do what they intend it to do?

Some form of acceptance testing may be required. This may only be realistically viable for high volume, repeat transactions using the same form of smart contract coding.

Confidentiality

All transactions, including the flow of money and pricing, are exposed in the public blockchain of a smart contract for inspection by anyone, yet most contracting parties wish to keep their terms and conditions and pricing information private.

For this reason, the parties may prefer to use a private blockchain as the basis of their smart contract. Exceptions to this might be public procurement or an open tender situation, and there may also be technical solutions to control read access to information that a participant wishes to hold back from general viewing.

Identifiable community

Blockchain transactions can be pseudonymous. While the system itself is intended to create the requisite trust between the participants, in a contracting context the identity of the counterparty may be of fundamental importance to the other party.

For this reason a business may prefer to operate within a closed community of participants, where an administrator can control membership.

Persistence of the community

Confidence in the long term nature of a distributed ledger depends upon confidence in the fact that the participants who host it (and who therefore ensure its survival) will themselves persist as a community.

In the smart contracting context, that means having confidence that those who maintain the blockchain will continue to do so. If they do not, the record of the smart contract itself may be put at risk. For example, proponents of blockchain technology acknowledge that there is a theoretical risk that the technology supporting smart contracts could be 'overwhelmed' by an attacker with control of 51% or more of the network's total hashing power (at least in the context of Bitcoin's deployment of blockchain). That risk is particular to blockchains and might increase if the community begins to ebb away.

To deal with that concern, the participants may look to a third party who is willing to host the blockchain as a document of record for as long as it is needed. There is already a model for this type of arrangement in the e-mortgages industry in the US, where Bank of New York Mellon is used for certification and custody of eNotes.

Storage constraints

The number of devices connected to the Internet of Things 'is forecasted to surpass 25 billion in 2020, up from 10 billion today'

(Gartner, Gartner Says the Internet of Things Installed Base will Grow to 26 Billion Units by 2020, 2013)

Large-scale storage capacity may be needed to store the blockchains that devices connected to the Internet of Things generate in relation to smart contracts. It may be impractical for, say, consumers to store blockchains on domestic computers, and technology architecture may need to be developed separately to store identity blockchains, content blockchains and transactional data blockchains relating to a smart contract (perhaps with a trusted third party storage provider).

However, there are already technical solutions that may address the problem of storage capacity. Storage of large amounts of data can be dealt with by deploying a pointer hash in the blockchain which directs the user to access the stored data from an 'off-chain' database. In this way the blockchain simply controls the logic of the smart contract, but does not attempt to store all the data relating to it. Nevertheless, some businesses may still wish to store their own complete copy for added reassurance.

Compatibility

The use of compatible data fields is the traditional way in which data is matched up from different sources. Currently there is no commonly accepted standard for data fields used by competing smart contract solutions providers.

Despite advances in contextual data matching techniques, in something as fundamental as contract data this could limit uptake where two parties use different smart contract solutions.

In due course it can be expected that a particular solution's data fields will become the default standard by reason of ubiquity, and in the meantime it may be necessary for a party to insist that its counterparty uses the same smart contract solution.

Are smart contracts legally binding?

Many laws that the courts might need to consider in analysing the legal status of smart contracts were developed in an analogue context, and may not be well adapted to cater for the digital environment within which smart contracts operate.

For example, it is tempting to conclude that, just because the moniker *smart contract* includes the word contract, it is a *legally binding contract* as a matter of law. This is not necessarily correct.

To be a contract in the legal sense, the following four essential elements must be present under most common law legal systems (civil law jurisdictions may prescribe other requirements):

- offer and acceptance;
- consideration;
- intention to create legal relations; and
- certainty of terms.

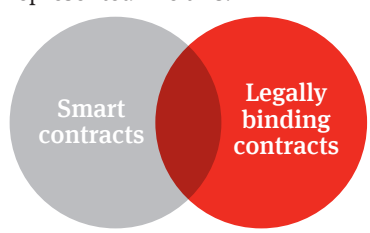
Some of these four essential elements may be absent in the coding of a smart contract. For example:

- smart contracts that are designated to the blockchain at the instance of one party raise issues about whether there has been an offer and an acceptance (requiring bilateral conduct). It may be possible to address this uncertainty by prescribing what constitutes the offer and what constitutes acceptance in the smart contract itself (in the same way that online purchasing terms and conditions often prescribe when an offer is made and the methods by which it can be accepted online). Although such provisions might be helpful, they are unlikely to be conclusive of the issue before a court charged with deciding the issue in the context of the facts as a whole; and
- is there certainty of all the essential terms? Smart contracts are typically short – 500 lines of code would not be unusual. This brevity adds to the risk that there may not be sufficient certainty for there to be a contract in the legal sense.

The courts are used to finding the existence of a contract in the absence of incomplete (or no) documentation. Under most common law legal systems, provided the four essential elements are present, a contract can be made orally, or partly orally and in writing; it can be implied from the conduct of the parties; and it can be made via email or by clicking a button on a website.

When faced with a smart contract, a court could come to one of a number of potential conclusions:
There is no legally binding contract
There is a legally binding contract, and it is constituted by the smart contract
There is a legally binding contract, and it is constituted partly by the smart contract and partly by other terms and conditions (some of which may be implied or construed from the conduct of the parties)
There is a legally binding contract, and it is constituted entirely from matters extraneous to the smart contract, such as implied terms. The smart contract simply performs certain outcomes of the contract when conditions are satisfied

The legal status of smart contracts can accordingly be represented like this:



There is a clear risk exposure for businesses where commercial arrangements are not backed up by the reassurance of legally binding contractual relations. Some smart contract solution providers propose bridging this 'contracting gap' with hybrid contracting models (see *Are There Technical Solutions?*).

Can complex contracts be encoded?

Natural language contracts often provide for complex commercial arrangements between the parties. Would a smart contract be able to encode such arrangements? Or are there limits to what a smart contract might be able to achieve?

A complex or sophisticated contract usually contains a number of legal phrases, the meaning of which may not be settled at law, and which may only be determined by legal analysis (applying principles of contractual interpretation).

For example, each of the following may have a number different meanings (or their meanings may change over time as case law evolves):

- 'material adverse change';
- 'best endeavours';
- 'reasonable endeavours';
- 'reasonable notice'; or
- 'reasonable steps'.

These formulations involve judgement and are a question of degree. They do not lend themselves well to encoding within smart contracts.

Similarly, take a smart contract that provides for the delivery of goods or services. If it is encoded to release payment automatically if the goods comply with a specification or the services comply with a services description:

- how would the automatic protocol be able to verify that the goods actually comply with the specification?
- would a smart contract be able to operate where a subjective evaluation of the quality of the services as against a services description is required in order to verify compliance?

The problem these examples highlight is that, as the technology stands, smart contracts may not be able to encode the subtlety and richness of contracts written in natural language or to cater for the exercise of discretion given to one party.

There may already be technical solutions to work around this problem. For example, where the exercise of discretion (or a decision of some kind) is required of one of the participants to a smart contract, it could be accommodated by building in a mechanism to halt performance of the smart contract temporarily while input from the participant (or a third party empowered to verify a state of affairs) is sought.

To build in such a dependency:

- runs the risk of undermining a key virtue of a smart contract: lack of dependency on a participant / third party agency; and
- means that the parties can no longer be certain that an event (for example, the release of payment) will happen on an irrevocable basis once the smart contract is put in place.

Even with such a dependency, a smart contract could still deliver value to businesses by co-ordinating the various stages of the transaction by process automation.

Are there other technical solutions?

The participants to a smart contract may not always intend that it has legally binding contractual effect. For example, in some smart contract deployments the smart 'contract' may simply be an automated process (so that, if 'X' occurs, then 'Y' happens).

However, in other deployments the participants may well want a smart contract to have contractual effect. Here, to deal with the problems raised by complex contracts, as well as the more fundamental issue of ensuring that what is put in place has legally binding contractual effect, some smart contract solution providers propose deploying a so-called 'split' contracting model.

With some variation, the split contracting model broadly reflects aspects of the functionality advocated for what are known as 'Ricardian contracts'. These use an identifier (a hash) to link a natural language contract to some form of automated activity, such as payment.

According to its proponents, split contracting seeks to adopt the best that long form, natural language contracting and smart contracting can offer. A split contracting model uses technology indelibly to link a natural language contract to smart contract architecture. The smart contract architecture administers the data-driven performance components of the arrangement.

Other models may also be possible. For example, the parties could put in place a master supply contract under which each smart contract entered into under it incorporates its terms by reference, and triggers supply.

These kinds of smart contracting models have the disadvantage that not all the contractual terms are stored in one place. An analogy can be drawn here with website terms and conditions regulating the ordering and supply of online goods and services (often found by clicking on a link). If the buyer is not made aware of the terms and conditions, they may 'come too late' to be incorporated into its contract with the seller. Smart contracting solutions will wish to avoid such an outcome.

On the other hand, assuming that natural language terms and conditions have been successfully incorporated into a smart contract, such smart contracting models may have the advantage that they help to address the uncertainties associated with the legal status of a smart contract and to accommodate the complexity inherent in natural language contracts.

What are the other contractual issues?

There are a number of other contractual issues that arise in relation to the deployment of smart contracts. (Some of these may not be a problem in the case of a split contracting or master contracting model, where there may be requisite contractual certainty if the parties are identified.)

Despite some suggestions to the contrary in media coverage on smart contracts, it is reasonable to suppose that the courts probably will not take a fundamentally different approach to contract law in relation to a smart contract from that routinely applied by them in relation to any other document (electronic or otherwise) or set of circumstances that is claimed to have legally binding contractual effect.

Legal formalities for form of documentation

Statute or regulation in many jurisdictions requires that certain types of contracts (or other documents or conveyances) must be in writing and / or signed by one or more parties in order to be legally valid. For example:

- assignments of certain types of intellectual property rights;
- guarantees;
- contracts for the sale of land, or a charge or mortgage over land; and
- transfers of certificated shares.

Some transactions may also be required to take the form of deeds (such as land transfers, certain property leases, powers of attorney and trustee appointments), and in many common law jurisdictions the courts have laid down requirements relating to the form and method for signing deeds (these must be adhered to in order for a document to take effect as a deed).

> These various requirements could hinder the use of smart contracts in certain contexts. For example, is an encoded smart contract (say, one not capable of being rendered in natural language) ever in 'writing' for the purposes of the relevant legislative or regulatory requirement?
>
> Much will depend on the particular statutory or regulatory wording and interpretative aids. Businesses will require legal advice in relation to the relevant jurisdictions to determine whether smart contracting complies with the local law requirements.

Proof of signature

Public/private key cryptographic technology is typically used as the basis for initiating a smart contract, and it can also show the chronology (known as 'timing stamping') for doing that. Would public/private key initiation satisfy the requirements (laid down in statutes or regulations in force in many jurisdictions) for certain types of document to be *signed* by the parties?

Some legal systems have the benefit of legislation that may assist in answering this question. For example:

- **the United States of America** has the federal Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 7001; Pub. Law 106-229 (June 30, 2000), and the Uniform Electronic Transactions Act of 1999, which was adopted in most states except for Illinois, New York and Washington, along with various state electronic signature laws that purport to govern the use of electronic records and signatures to some extent (for example, the New York Electronic Signatures and Records Act, N.Y. State Tech. Law §§ 301-309 and N.Y. Comp. Codes R. & Regs. Tit. 9, Part 540);
- **member states of the European Union** benefit from the Electronic Signatures Directive (1999/93/EC). From 1 July 2016 the Electronic Identification Regulation (EU/910/2014) will apply to govern the position;
- **Australia** has the Electronic Transactions Act 1999 (Cth) along with various state electronic signature laws (for example, the Electronic Transactions Act 2000 (NSW));

- **Canada** has the Personal Information Protection and Electronic Documents Act and various provincial statutes that purport to govern the use of electronic signatures in documents that are legally required. Most provincial statutes, such as the Electronic Commerce Act of Ontario, also address the use of an electronic signature as a means of expressing offer and acceptance for the purposes of the formation of a contract; and

- **Singapore** has the Electronic Transactions Act (ETA) (Cap 88), which governs the use of electronic signatures and the validity of electronic records.

Legal analysis that takes into account the particular facts and the particular technology that supports the entering into of a smart contract may be required in order to determine whether the stipulated means of signifying an electronic signature under such legislation would be satisfied.

The law of different jurisdictions in this regard is not consistent. Where legislation applies only to contracts, it will be necessary to determine if the smart contract at issue actually has contractual status (or would do so, with a valid signature) in order to benefit from the legislation.

In some jurisdictions (for example, under the UK's Electronic Communications Act 2000, which implements the Electronic Signatures Directive) the legislation may be of assistance where the requirement for there to be a signature is not laid down by statute or regulation (by according evidential value to certain electronically 'signed' documents). However, it does not solve the problem where there is a *statutory or regulatory requirement* for a signature.

The UK's Electronic Communications Act 2000 envisages that the UK Parliament could pass regulations to give electronic signatures evidential effect where there is a statutory or regulatory requirement for a signature. There still exists a vast number of enactments for which no such facilitative provision has been enacted. Accordingly legal analysis will still be required to determine whether the requirement for a signature can be satisfied by an electronic signature under many statutes and regulations in the UK.

Identity of parties

In order to be legally valid, the common law of many jurisdictions provides that a contract must be entered into by a legal person (a human or other legal entity) having legal capacity to do so. There is also common law authority (for example, in English law) to the effect that, for a contract to arise, there needs to be sufficient certainty over who the other contracting party actually is. Civil law jurisdictions may lay down other requirements.

Transactions using blockchain technology can be conducted pseudonymously. Would a court regard a smart contract as having legally binding effect if it is simply not possible to identify who the other contracting party is?

Moreover, if a dispute arose regarding a smart contract, how would an aggrieved party identify the other party in order to bring legal proceedings against it?

These are significant concerns. They might be able to be addressed by the use of closed community blockchains where the members are all identified.

Evidence of contract

A paper version of a contract is evidence of the existence of a contract, but it is not itself the contract. Ultimately a contract is whatever a court finally determines it is.

For example, a court may take evidence that a natural language contract has been subsequently amended, that it ought to include certain implied terms (perhaps required by legislation), or that its provisions contain an error on its face that ought to be rectified

by the court. A court might approach a smart contract in a similar way.

However, what would be the position if:

- a smart contract does not specify, or the parties have not agreed as part of the contract between them, a natural language rendering of the code that will have conclusive effect between them in the case of a dispute?
- the meaning of a smart contract's code is different from the natural language rendering of that code? How would a court determine what the real contract constitutes?

The courts have experience in evaluating expert evidence as to the meaning of code. However, one way to avoid such a dispute would be for the parties to agree (perhaps in the smart contract or in terms imported into it by reference) that a particular rendering of the code into natural language (perhaps a rendering verified by an independent third party) constitutes the contract between them for all purposes in the case of a dispute.

Jurisdiction and governing law

Take the situation of, say, a global hedge fund, using a smart contracting platform based in Switzerland, which enters into smart contracts with investors in China and US. Which country's regulators would have jurisdiction over such arrangements? Which courts would have jurisdiction to determine any disputes between them, and what law would they apply?

Natural language contracts often include alternative dispute resolution mechanisms (such as arbitration) so that the parties can avoid court proceedings if dispute resolution is required. Within the EU, for example, Regulation 524/2013 provides for the establishment of an EU-level online dispute resolution platform for B2C disputes about contractual obligations arising from online sales and service contracts.

For some technical questions, natural language contracts sometimes also include an 'expert determination' procedure by which a technical matter in dispute can be finally determined by recourse to an expert without having to take the additional step of going to court.

Because a smart contract automatically performs across distributed computing systems, it may be difficult for a court to determine the place of that performance when attempting to decide what governing law ought to apply to the smart contract.

The courts are used to dealing with difficult jurisdictional issues in, for example, contracts formed over the Internet (say, for website sales of goods and services). Jurisdictional problems in the case of smart contracts might be ameliorated (to some degree) by the use of appropriate 'choice of law', 'jurisdiction', 'alternative dispute resolution' and 'expert determination' clauses in the smart contract itself (or in terms imported into it by reference).

Bugs in coding

Almost all commercially produced software contains bugs or coding errors of some kind. Bugs or errors in relation to smart contracts may be of a number of different types. They could include:

Internal logic errors: for example, errors in coding of a smart contract

Platform logic errors: for example, processing errors in the system hosting the smart contract solution, preventing a smart contract from automatically performing

External integration errors: for example, where a smart contract refers the verification

of the satisfaction of a condition out to an external information source that has ceased to exist *(see External Information Sources Ceasing to Exist, below)*

External state at odds with internal assumptions: preventing automatic performance. For example, a smart contract may provide that, on a certain date, shares will transfer from the share account of party A to party B's share account, but on that date party A's share account no longer contains those shares.

What is the legal position if a bug or error in relation to a smart contract results in an error or mistake in what the parties thought they had agreed or in an outcome that was not intended?

The law in many common law jurisdictions permits the courts to correct an error in a written contract in some circumstances. They can generally:

- do so for misnomer if there is manifestly an error in the naming of a party;
- use contractual construction to resolve ambiguities; or
- deploy the doctrine of rectification to correct a contract in limited circumstances.

(Civil law jurisdictions may have other mechanisms available.)

In approaching the issue, the courts may need to decide whether or not a smart contract has an existence that is separate from its code. If a court were to take the view that the code is the contract, and not separate from it, they might be willing to treat a bug in that code in the same way as they do a manifest clerical error (or a missing word or sentence) on the face of a contract, and provide a 'legal fix' for the coding error.

The courts might be more willing to provide a remedy for the consequences of a coding error where the parties have agreed that a particular rendering of code into natural language constitutes the contract in the case of a dispute.

Where a contract results in an unexpected outcome (that is, one not provided for in the contract), the courts of common law jurisdictions may sometimes imply terms into the contract in order to 'plug the gap'. Where automatic performance of a smart contract results in an unexpected outcome, the courts may decide to approach the problem in the same way.

In addition to bugs and errors that are an issue for any software, proponents of blockchain technology acknowledge that there is a theoretical risk of a '51% control' attack in the case of that particular technology (at least in the context of Bitcoin's deployment of blockchain).

Such an attack:

- allows the attacker to 'censor' real-time transactions and to create invalid transactions in real time; and
- does not alter the past (for example, past transaction history that occurred before the attacker obtained control).

A 51% control attack on a network running smart contracts is at least conceivable where blockchain technology is relied on, and could allow the attacker to give the impression that it has fulfilled the conditions of a smart contract. However, it might become obvious that such conditions have not been fulfilled, because the attacker would not be able to change the past history, nor the original content supporting the smart contract.

Other lines of attack in relation to a smart contract may also be possible, such as:

'Sybil' attacks: here an attacker creates numerous identities, and uses them to 'surround' a computer or node. In such a case, a simulated (false) network would appear as authentic, and a would-be smart contract participant may wrongly assume it is transacting within a genuine smart contracting environment

'Denial of service' attacks: these could hinder a smart contract's participants from transacting or otherwise interacting.

It is unclear whether the courts would treat a party otherwise in breach of contract as a result of these various attacks as being in some way exonerated in that situation (it may depend on the facts and the relevant law applicable).

Coding errors in smart contracts and attacks give rise to other legal uncertainties. If a smart contract malfunctions in some way (perhaps because of a bug), causing loss to a party (perhaps by wrongly refusing payment or some other form of settlement), how would the courts allocate liability?

With some exceptions cross-jurisdictionally, the courts generally allocate liability in a contracting context on the basis of fault: breach in the case of contract, or negligence in the case of tort. If a smart contract auto-performs in a way that was not anticipated (and in a way that could not be attributed to a breach of contract by one of the parties), the party otherwise bearing the loss may face difficulties in establishing liability on the part of the other party or a third party.

On the other hand, it is an established principle of the common law in many jurisdictions that a contractual breach is still a breach even if it is not deliberate. Civil law jurisdictions may approach the issue differently. Much may therefore depend on the facts, how a court characterises the auto-performance failure (for example, whether it is a breach or simply an intervening act breaking the chain of causation), and the applicable law.

These uncertainties underscore the need for a smart contract to limit or exclude liability. A party to a smart contract that is silent on such issues runs the risk that it could be liable for the failure of a smart contract to perform (for example, to release payment), even if that breach was not the result of its own act or omission.

Similarly, a smart contract should include (perhaps by importing them by reference) provisions that exonerate breach where the breach arises as a result of a force majeure event (such as unavailability of the Internet, corruption of data during carriage or hosting, cyber intrusion, or a 51% control attack).

Users of smart contract solutions should review the liability position under their subscriber contracts with the smart contract solution provider to establish to what extent the solution provider is itself liable (if at all) if it causes the party to be in breach of a smart contract. The finally negotiated position in that regard should be reflected on a back-to-back basis with the liability position provided for in the smart contract itself.

Cyber security and intrusion

A private blockchain hosted on, say, a public cloud could be vulnerable to cyber intrusion, data loss or corruption. A private cryptographic key could be maliciously acquired, and transactions entered into fraudulently. In such cases, would a party who is denied the benefit of a smart contract have any remedy?

There is common law authority in some jurisdictions under which the courts can regard as void contracts that have been entered into by a rogue who has passed itself off as a party (civil law jurisdictions may approach the matter differently). It is not clear whether the courts would treat a smart contract in the same way.

Irrevocability and amendments

It is a typical design feature of smart contracting solutions that, once a smart contract is initiated, automatic performance cannot be stopped. If there are prescribed conditions for auto-performance, a smart contract will automatically perform on their satisfaction.

Proponents of blockchain technology and smart contracting see the irrevocable nature of a smart contract as a desirable design feature. However, from a legal perspective, irrevocability can give rise to a number of issues.

Natural language contracts often need to be brought to an end, changed or amended, perhaps to reflect changes to the underlying commercial arrangement, to correct errors, or to reflect changes in law.

While amendments to contractual terms incorporated by reference into a smart contract might be possible (if they contemplate that changes to them will amend the contract as a whole), any desired changes cannot change the encoded aspects of the smart contract on the blockchain. As performance is encoded as part of the functionality of the program, there is no ability to change or replace a block transaction once it has been set in motion.

> There is 'no mechanism for dealing with this scenario, no mechanism for bringing ledger state and legal state back into alignment'
>
> *(Robert Sams, No, Bitcoin is not the future of securities settlement, 18 May 2015, www.clearmatics.com).*

Technical solutions might be possible in some instances (such as setting the smart contract to respond to an updating requirement sent by an administrator to reflect, for example, a new regulatory requirement, mentioned earlier).

Similarly, contractual terms incorporated by reference into a smart contract could potentially address the irrevocable nature of a smart contract by, for example, requiring a party contractually to:

- transfer back what has been transferred (via the smart contract) to it if certain specified events occur after the contract has been initiated (these could approximate to certain termination rights typically found in natural language contracts); or
- to place what has been transferred to it into an escrow arrangement pending resolution of a contractual dispute.

Such provisions may not always be effective (for example, on insolvency or in a trade embargo scenario). Appropriate legal advice will required before seeking to implement such provisions.

Is automatic contracting by self-execution binding?

Implicit in the IBM and Samsung proof-of-concept use cases for smart contracts operating over the Internet of Things (see *Which Industry Sectors Might be Affected?*, above) is that it could well be devices connected to the Internet of Things that will be entering into smart contracts, rather than humans. Smart contracts would therefore be entered into on a machine-to-machine basis.

Similarly smart contracts can themselves be coded automatically to enter into other contracts when certain conditions are satisfied.

The law in most jurisdictions requires that an arrangement must be entered into by a legal person with legal capacity in order for that arrangement to constitute a legally binding contract.

The courts may need to decide whether or not machine-to-machine and automatic smart contracting constitute an exercise of agency powers on behalf of the original contracting party, causing it to be legally bound.

The answer will depend on a factual and legal analysis, and is likely to vary cross-jurisdictionally.

Vitiating elements

Because a smart contract is, by design, typically irrevocable in nature once initiated (in terms of automatic performance that cannot be stopped), discussion about smart contracts often assumes that they are irrevocable for all purposes, including in a legal sense.

However, the common law in many jurisdictions (as augmented by statute in some cases) provides that a contract can be discharged (or brought to an end) in certain circumstances (civil law jurisdictions may include alternative ways of dealing with some of these situations).

For example, a contract can be:

- discharged by frustration, impossibility, operation of law, illegality, or mistake; or
- brought to an end by rescission, which undoes a contract as if it had never existed (that is, *ab initio*) and restores the parties to their pre-contract positions. Here a party or the court rescinds the contract as a remedy for some wrong. (This is the main remedy for misrepresentation under, for example, English law, although damages are usually paid instead.)

How can the irrevocable and irreversible nature of a smart contract (from an operating perspective) be reconciled with the existence of legal principles that entitle a party to terminate a contract (from the time of termination) or to completely unwind a contract in some cases (as if it had never entered into it)?

In common law jurisdictions, a court would probably be reluctant to come to a view that the parties had in some way given up their rights to bring a contract to an end by virtue of having entered into a smart contract in the absence of express wording to that effect.

‘The more valuable the right, the clearer the language [surrendering it] will need to be’

Stocznia Gdynia SA v Gearbulk Holdings Ltd [2009] EWCA Civ 75, Moore-Bick LJ at paragraph 23

However, where a remedy is at a court's discretion, a court might exercise that discretion in a way that recognises the practicalities of the irreversible nature of a smart contract.

External information sources ceasing to exist

What is the legal position if a smart contract refers the verification of the satisfaction of a condition out to an external information source (for example, movement in a pricing index published by an electronic feed) where that information source ceases to exist (sometimes known as 'link rot') before the satisfaction of the condition?

If the information source such as a pricing index ceases to exist, the satisfaction of the condition cannot be verified and auto-performance based on satisfaction of the condition will not occur.

In natural language contracts the courts in most common law jurisdictions would need to determine whether the contract could be interpreted so as to refer to, say, a replacement pricing index or whether a term could be implied to that effect.

Parties proposing to enter into a smart contract will wish to avoid such uncertainties. However, it may be extremely difficult to put in code form instructions to use a 'replacement index'. What constitutes a replacement index may be a question of judgement or degree. While it would be easier to identify and code for the use of a specific, alternative index, in longer term smart contracts there is a risk that it, too, may cease to exist.

How will smart contracts operate within a regulated environment?

Consumer protection measures

Legislatures in many countries acted to regulate in favour of consumer protection when it became clear that B2C contracting (and other commercial interactions with consumers) would become a significant feature of the Internet. Prescribed requirements for website terms and conditions for online sales, online privacy policies, cookie use transparency, and distance selling consumer cancellation rights are all examples of legislative initiatives implemented in a number of jurisdictions to protect consumers.

If, therefore, smart contracts are likely to become ubiquitous on a B2C basis, it would not be surprising if legislatures were similarly to act to implement or extend specific consumer protection measures in relation to them.

The legal systems of many developed economies already include laws providing for a range of consumer protection measures that give consumers enhanced redress in relation to the provision of goods and services. Depending on the jurisdiction, and what is being supplied, these might include one or more of the following:

- rights in respect of the provision of pre-contractual information;
- cooling off periods (that is, the right of a consumer to get out of a contract for a short period after having entered into it);
- standards of performance, such as warranties; and
- other rights that must be included in the terms and conditions of a consumer contract (for example, rights to require re-supply or repair of defective content and refund rights).

In addition, in many jurisdictions the regulatory or licensing requirements applicable to specific industries (such as banks, insurers, telecommunications and other public utilities) often prescribe contractual provisions that must be included by the business in its contracts with consumers.

It may be difficult for regulated businesses to demonstrate that an encoded smart contract includes such information, and encoding such information may not satisfy applicable transparency obligations.

Moreover, regulated businesses will need to consider whether using a smart contracting form could, in and of itself, prevent a consumer from being able to exercise consumer rights.

Accordingly it will be necessary for regulated businesses to take appropriate legal advice on a jurisdiction-by-jurisdiction basis before deploying smart contracts.

Financial services

Some financial services regulators are already alive to the disruptive possibilities of blockchain technology and smart contracting.

The UK's Financial Conduct Authority, for example, has expressed a desire to explore the technology's use in financial services beyond the domain of virtual currencies such as Bitcoin. Similarly the Bank of England has said that the application of distributed ledger technology could have 'far-reaching implications' for the financial services industry.

There are, however, certain regulatory challenges in the use of the technology within financial services. For example:

- there are a number of key questions that law- and policy-makers need to consider in developing their regulatory responses to blockchain

technology. These include (but there are many more): (1) what exactly is it that should be regulated?; (2) which activities related to the operation of blockchain technology should be regulated?; (3) should they be regulated only where they relate to the delivery of financial services in respect of regulated instruments or products (like shares, for example)?; (4) should the category of 'regulated instruments' be extended, to include digital currencies (for instance)?; (5) where regulation is applied, who is it that should be subject to and responsible for compliance with the relevant obligations?; and (6) how should regulatory responses be pitched so as to avoid stifling innovation?;

- to date, the responses of regulators globally to blockchain technology have been somewhat fragmented, and are (generally speaking) at quite an early stage. The financial services industry may therefore continue for some time to face a lack of certainty and consistency in terms of the regulatory treatment of smart contracts and other applications of blockchain technology;

- it remains unclear how AML and KYC regulatory obligations may be credibly performed in the context of a pseudonymised blockchain transaction, where the ability to identify the other participants can be obscured. Regulatory advice on a jurisdiction-by-jurisdiction basis will be required to ascertain: (1) whether private blockchains (within closed communities of identified counterparties) might deliver sufficient information to enable a regulated bank or financial institution to discharge its AML and KYC obligations; and (2) how such obligations could be performed in the context of smart contracting more generally;

- compliance with anti-bribery and corruption legislation generally requires a business to have an understanding of (and an ability to control) its supply chain participants (such requirements are not limited to the financial services sector). That may be impossible if the counterparty is not identifiable. Legal advice will be necessary to determine whether private blockchains within closed communities of identified counterparties might enable a business to assert control over, and have sufficient transparency in respect of, its supply chain; and

- financial services firms are commonly subject to governance, systems and controls obligations (for example, securing systems, managing risks, reducing the risk of financial crime). Firms' directors and senior managers should be aware that, while it may be attractive to develop new business models, improperly delegating tasks to a smart contract without adequate risk management systems in place may carry significant risks of poor customer outcomes. It is critical that existing, new and emerging risks associated with innovative financial technology are identified and managed effectively to achieve resilience, security and reliability (for example, through robust design and testing procedures).

Any regulated business contemplating using smart contracts will need to take appropriate regulatory advice before doing so.

What are the implications for business?

The legal status of smart contracts as legally binding contracts will need to be analysed before deployment.

An obvious use for smart contracts is to reduce execution risk (by making transfer of the relevant asset or instrument in question near to inevitable by virtue of automatic performance). However, that may only achieve factual (that is, *de facto*) transfer. It may still be necessary, therefore, to apply established legal concepts and principles in order to determine whether transfer has been achieved *de jure* (at law).

In such circumstances, in the short term, as a risk mitigation strategy, smart contracts may need to be of short duration and low in value - the longer the term of a smart contract, the less smart it may become.

Businesses proposing to use smart contracts would be well advised to obtain a regulatory and legal assessment for any deployment that is likely to pass the proof-of-concept phase.

'One strategy that does offer certainty, however, is not advisable: sitting on the sidelines and waiting for others to pioneer this technology. Choosing that seemingly safer option merely raises the likelihood that when today's risks have been resolved, it will be difficult to catch up with market leaders.'

(IBM Institute for Business Value, Empowering the Edge: Practical Insights on a Decentralised Internet of Things, 2015)

Contact

Nick Abrahams
nick.abrahams@nortonrosefulbright.com
Tel +61 2 9330 8312