When Code Becomes Law

Decentralised Finance and the rise of smart contracts in commerce

Written by **Gabriel Mezhrahid**

coremont

Part 1: Smart Contracts and legal considerations

Preceding Bitcoin and blockchain technology, the idea that computer codes could monitor, execute and enforce legal agreements was theorised in the '90s by a rare species of lawyer able to understand computer science.

Thirty years later, and although this technology is still considered by certain lawyers as sorcery, these modern forms of legal instruments have materialised, developed and prospered in the digital era. But how do they differ from traditional agreements?

The digitalisation of contracts is not a recent phenomenon. The drafting storage and execution of contracts in today's practice has been vastly digitalised. Nevertheless, these dematerialised contracts are in reality the mere digital representation of paper agreements. The process has evolved, but the principles are the same.

In contrast, smart contracts stand out from traditional agreements with unprecedented new features that we will discuss in this article. Hosted on **blockchains**, smart contracts benefit from key features this technology has to offer, such as automatic execution, immutability and transparency of contracts.

These features are made possible thanks to distributed ledger technology, which allow participants of a given network to store and process data on a public ledger to perform transactions. **How does this ledger work in practice?**

A **smart contract** represents a set of pre-defined rules governing a transaction recorded on a public ledger (i.e. a blockchain). All elements of the agreement (e.g., the parties, the object and intended result of the transaction) are collected and shared on a network of computers, where each computer is called a node. Each node will perform an independent review of the transaction, verifying that all the above elements match their version of the public ledger. For example, if A wants to send cryptocurrencies to B, each node will verify that A possesses the said amount of cryptocurrencies on the blockchain. Once these conditions are met, the network will reach a "consensus" on the transaction's validity and will automatically execute the contract. That process leaves an indelible print on the ledger, evidencing that the transaction occurred and shall be considered by the network for future transactions. Note that, aside the initial intention of the parties, no human interaction was needed to operate and execute the transaction in a transparent and decentralised manner. Finally, that transaction was not verified or administered by a central authority like in the case of a bank transfer. Instead, it is processed by a constellation of independent nodes, one ensuring that the other has not deviated from the intention of the parties.

Smart contract is a term used to describe a set of promises specified in digital form, within which the parties performed on these promises (see Szabo 1996)

Blockchain technology can be described as a trustless and fully decentralised peer-to-peer data storage that is spread over all participants that are often referred to as nodes. The blockchain is designed to hold immutable information once data is committed to the chain, and it is therefore a decentralised, distributed, and immutable database in which data is logically structured as a sequence of smaller chunks (blocks).

Key features of smart contracts:

Blockchain or distributed ledger technology enables:

1. Automatic execution
2. Immutability
3. Transparency of contracts
4. No human interaction to monitor or execute
5. Relative anonymity

The evolution of smart contracts to date

1990s
Smart contracts emerge as theoretical possibility

2009
Satoshi Nakamoto releases the Bitcoin whitepaper

2015
The Ethereum blockchain goes live and becomes the first smart contracts decentralised platform

2017
Leveraging smart contract and oracle technology, the first decentralised lending protocols make their appearance (AAVE, REN)

2021
The total value locked in DeFi smart contracts reaches US$110 billion

Paper contracts increasingly become digitalised but principles remain the same

It is important to note that this transparency remains relative, as blockchain technology relies on a dual cryptography system to identify parties using a private key/public key mechanism. Indeed, a smart contract can be carried out between two pseudo-anonymous parties; only identifiable by their public keys (i.e., a set of 42 randomly generated letters/numbers); enough secrecy to grant the confidentiality required by certain contracts.

The most interesting aspect is that, unlike traditional agreements, once a smart contract is deployed, no human intervention (whether operational or judicial) is required for its monitoring or execution. The caveat to that feature is that input parameters are key to a proper automatic execution. Typically, the parameters take the following form: if situation "A" occurs, execute step "B". As a result, they serve two main commercial purposes: (1) ensuring the payment of funds upon certain triggering events and (2) imposing financial penalties if certain objective conditions are not satisfied.

These simple transactions find convenient applications in insurance contracts. Taking AXA's "Fizzy" product as an example: customers agree to pay an insurance premium in exchange for an automatic compensation if their flight is delayed by more than two hours. The parameters are clear and predefined making it possible for instant and transparent compensation when the smart contract conditions are met (i.e., the flight departure delay). No more paperwork, no more negotiations with your insurer, and no burden of proof, therefore reducing the execution and enforcement costs of the contract.

As the adoption of blockchain spreads, and as more and more assets are moving "on-chain" (i.e., being tokenised), correspondingly more smart contracts are developed to handle more sophisticated transactions.

As the technology spreads, the need for hybrid lawyers with computer science skills will grow. Who would have thought that the lawyer of the second half of the 21st century would have to learn how to code? And what should all business people understand in order to stay ahead of this rapidly shifting space?

We are, undeniably, only at the beginning of the possibilities offered by this technology and it is only a matter of time before the infamous indemnification and force majeure clauses make their appearance in smart contracts.

Once the concept of a smart contract is understood, at least three areas of interest arise: (i) the enforceability of a smart contract, (ii) the flexibility of execution, and (iii) the reliance on "off-chain" data.

Judicial enforceability

At first, the question of enforceability may sound irrelevant. As discussed above, the key feature of smart contracts is that, once the code is entered onto the blockchain, it becomes automatic and immutable and so (unless designed otherwise) its performance is inevitable. As a result, it is fair to say that smart contracts are enforceable by nature. The question is whether, even if contractually enforced, a judge will recognise the commercial and legal effects.

The judicial enforceability of smart contracts has been the subject of many debates among legal scholars. Although certain formalities may apply to contracts such as those under the Uniform Commercial Code, under U.S. law, or those associated with contracts or deeds, under English law, nothing under the general principles of common law would prevent a code-only contract to be enforceable, so long as the basic criteria of offer, acceptance, consideration, intention to be legally bound and capacity are met.

In 2019, some legal certainty on this topic was provided by the publication of a statement on the legal status of cryptoassets and smart contracts. This statement followed a public consultation by the UK Jurisdiction Taskforce (UKJT), a task force of the Law Society's LawTech Delivery Panel. In essence, Sir Geoffrey Vos (The Chancellor of the High Court) confirmed that smart contracts are capable of satisfying the requirements of English law contract formation principles. As a consequence, they can be interpreted and enforced using ordinary and well-established legal principles (see Vos 2019 & Bowles 2020).

The judicial enforceability of smart contracts is thus driven by the sole interpretation of the codes that constitute it, effectively declaring the code as law itself (see Fritz & Treichl 2020). Thus, Vos reminded the court that, **"English law does not struggle with the concept of anonymous or pseudo-anonymous parties",** and that the statutory requirement to have the agreement in writing was met, **"in the case of smart contracts whose code element is recorded in a source code"**. He finally concluded that, **"a smart contract is therefore capable of having contractual force".**

Flexibility of execution

Despite the fact that automation of execution presents some serious operational advantages, it also presents challenges in the way businesses currently operate.

If traditional contracts are the safeguard of any commercial relationship, they sometimes act more as commercial guidelines to direct parties' behaviour rather than carved into stone rules. It is not rare that parties enjoy the benefit of not having to execute an agreement, for example to excuse a breach, or accept partial performance to save a long-lasting client relationship.

This flexibility is missing in smart contracts, where the option not to enforce the agreement on an ad hoc basis would not exist unless coded as such in the smart contract itself (see Levi & Lipton 2018).

Traditional contracts are also easily amendable, allowing parties to navigate their contractual relationship in the storm of changing circumstances. The immutable character of the blockchain makes it far more complicated (if not impossible) to amend or stop the execution of a smart contract.

Amending smart contracts may therefore yield higher transaction costs, leaving attorneys with the difficult task of constantly ensuring that their smart contract is rock solid. The spread of smart contracts could change the economic analysis, making the efficient breach doctrine obsolete.

Oracle and off-chain sources

Regardless of the layer one blockchain they are built on (e.g. Ethereum, Binance or Solana…), smart contracts are closed-circuit protocols that cannot access information outside their own realm. This limitation appears to greatly limit the applications of smart contracts. For example, the insurance smart contract discussed above can operate solely on the basis that it receives flight departure times.

Omniscient of their network but blind to the outside world, smart contracts need to rely on data and parameters from the real world – also called "off chain resources" - to survive. This presents two issues: first, smart contracts do not have the ability to pull data from off-chain resources; instead, that information needs to be incorporated in the smart contract. Second, if the data at issue is in constant flux, and since the code is replicated across multiple nodes across the network, different nodes may be receiving different information, even just a few seconds apart.

For these reasons, so-called "oracles" have been developed. Oracles are specific protocols that feed smart contracts with external information necessary to trigger the predetermined actions defined in their codes. They act as on-chain APIs providing information into smart contracts **(see ethereum.org/oracles)**. Working as a bridge between the blockchain and the real world, they typically feed blockchain with instant and real time price fluctuation of one or several assets or the occurrence of a particular event, but can virtually share any data available online.

In a data-driven economy like ours, the introduction of oracles has shifted the perception of smart contracts from abstract tools to ground-breaking technology. Leveraging this new instrument, developers have created sophisticated smart contracts capable of performing complex financial functions, such as decentralised lending or synthetic options.

In the second article of this series on smart contracts, we will explore more in detail the existing and future applications of this technology in finance. Although smart contract oracles are unable to utter prophecies like the Pythia, they foretell that the financial revolution (if any) will not be televised, it will be decentralised.

Written by
Gabriel Mezhrahid

About Coremont

Coremont provides market-leading portfolio management technology and outsourced services across all investment management and trading functions, including risk and quantitative analysis, operations, treasury, accounting and regulatory reporting.

Clients include hedge fund managers and institutional asset managers, spanning four continents.

The cornerstone of Coremont's offering is Clarion, cloud-based portfolio management technology, which is powered by Coremont's proprietary pricing models and analytics. Clarion helps clients navigate the daily demands of trading and risk management, with advanced capabilities in derivatives.

Coremont LLP is an FCA-regulated financial services firm which was spun out from Brevan Howard in early 2018. With offices in London, New York and Hong Kong, Coremont employs over 350 people.

For more information, visit coremont.com

Important Information - CONFIDENTIAL – DO NOT COPY OR DISTRIBUTE

This document, the information contained herein and any attached materials (collectively the "document") have been provided specifically for the use of the intended recipient only and must be treated as proprietary and confidential. If you have received this document in error please delete it and notify the sender immediately. This document remains the property of Coremont, which reserves the right to require its return (together with any copies or extracts thereof) at any time upon request. It may not be passed on, nor reproduced in any form, in whole or in part, under any circumstances without express prior written consent from Coremont. Any unauthorised review, retransmission, dissemination, forwarding, printing, copying or other use of this document is prohibited. Coremont may be legally required to produce the document to regulatory authorities and others with legal rights to the information. Internet communications cannot be guaranteed to be secure or error free as information could be intercepted, changed corrupted, lost, arrive late or contain viruses.

Any information in this document should be regarded strictly as guidance and for informational purposes only. Coremont does not provide investment, legal, accounting or tax advice. Coremont and the sender make no warranties regarding the accuracy or completeness of the information in this document and it should not be relied upon for any purpose and is subject to change without notice. Information contained in this document is unaudited and Coremont accepts no liability for any errors or omissions in this document. Coremont and its representatives, members, officers and employees accept no responsibility for any losses suffered as a result of reliance on the information in this document or the reliability, accuracy, or completeness thereof. Coremont assumes no obligation to update any information contained in this document.

In this document, "Coremont" means Coremont LLP and its affiliates. Coremont LLP is a limited liability partnership authorised and regulated by the Financial Conduct Authority of the United Kingdom and registered in England & Wales (reg. no. OC420985).