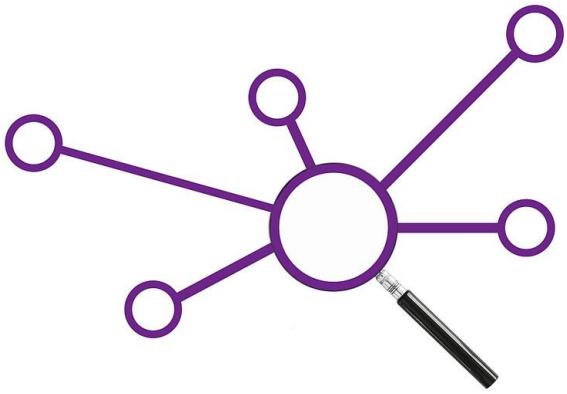
EVERSHEDS SUTHERLAND



How smart is it to use Smart Contracts?

17 October 2019

Lawyers often enjoy making the "joke" that smart contracts are neither smart nor represent legally binding contracts. Simply put a smart contract is a program/tool that can be used to implement a separate normal legal contract, so it seems that the lawyers and technologists will have to find new ways to work together. So the real question seems to be when is it "smart" to use a smart contract?

> **Smart contracts** are self-executing business automation applications that run on a decentralised network such as a blockchain. While the blockchain acts as a database, verifying that transactions have occurred, smart contracts complete pre-determined conditions. Therefore, once specific conditions of a smart contract are fulfilled they can automate the relocation of bitcoin or fiat money etc rooted in a blockchain ledger.

The potential uses of smart contract span across various areas and seem to be only limited by the imagination. For example, smart contracts might:

- be employed to streamline the insurance claims process by automatically activating a claim when specific events occur;
- be a safeguard ensuring royalties go to the correct recipients by documenting ownership rights in a decentralised blockchain system; or
- manage rent and deposits between a landlord and tenant.

Like any evolving technology there are risks that need to be considered and adequately addressed and it is important that these risks and errors in early adoption do not (in my view) overshadow or impede the development of this technology.

For example **smart contracts** seem, at the moment, to be suited to implement simple legal contracts or transactions, that have low value and clear parameters or requirements on the relevant parties/users, and clear termination or exit provisions.

Smart contracts are not currently regulated in Ireland, but that is not to say that they are not being carefully considered. The Law Society of Ireland and the Department of Finance are monitoring developments in this area, as is industry. Kevin O'Brien, head of Consumer Protection – Policy and Authorisations at the Central Bank of Ireland, stated "*If we cannot understand [blockchain], we cannot supervise it, and if we cannot supervise it, we cannot authorise it*". Accordingly we have worked with clients to implement appropriate risk, control and governance frameworks and this requires lawyers to work closely with the relevant stakeholders. To quote Albert Einstein;

> "*If you can't explain it to a six year old, you don't understand it yourself.*"

It is my view that to achieve this level of understanding requires input from all stakeholders hence the early adopters implementing low risk / value smart contracts can lead to substantial benefits to market as this technology develops. Clearly there can be strong business rationales, customer benefits and cost saving to utilising smart contracts in the correct way.

Other EU countries, such as Italy, have recently taken steps to implement a legal framework for smart contracts with Law Decree No. 135/2018. I note that industry in Ireland is considering these issues carefully both at a domestic and international level.

Ireland has a long history of leading developments in technology with talented individuals and, as I write a day after the anniversary of the famous graffiti on Broome Bridge, I am reminded of the wealth of innovation that Ireland is famous for.

> *On October 16th, 1843, Hamilton and his wife Helen were walking along the banks of the Royal Canal from Dunsink Observatory to the Royal Irish Academy where he was president.*
>
> *At Broome Bridge, he had that very rare occurrence in science, a Eureka moment. He suddenly alighted on the solution to a problem he had been working on for a long time and in his excitement, he scratched his formula for Quaternion algebra onto the bridge; $i^2 = j^2 = k^2 = ijk = -1$.*
>
> *Quaternions would later be instrumental in putting the first man on the moon and be used for computer-generated imagery in movies.*

However, I digress, and I agree that it is important to highlight the associated risks of smart contracts in a measured and educated way so that these risks can be best addressed and that Ireland remains a truly innovative centre in Europe.

A smart contract in this context relies upon rules which it follows exactly, and as such can lead to unsuitable results. As any lawyer or reasonable person is aware **"the exception proves the rule"** and it is hard to envisage all variants that can arise in a contract or the implementation of a contract. For example, it is often argued that in its current state smart contracts cannot react to secondary considerations in the off-chain world. Smart contracts cannot currently respond to external events or address nuanced concepts of "reasonableness". They require detailed considerations of all applicable variables in execution and this can be daunting from a legal and programming perspective. Viewed through this prism, smart contracts are not actually smart, they are deterministic. However, we are in the early days of adoption and the pace of development is rapid. It is entirely conceivable that these risks and limitations will be appropriately addressed.

The accuracy of data entered into a smart contract is essential as once smart contract rules are in place they are unalterable. Neither the user nor programmer can amend a contract once it has been written. This gives rise to the question, what legal recourse is available where a smart contract cannot be accessed or modified in line with changes in the law or business environment? I have worked with clients to carefully consider termination triggers and other mitigants.

The data inputted originates from external sources as a blockchain cannot directly gather data. It is generally sourced from data feeds and Application Program Interfaces. The real-time data feeds for blockchains are called "oracles". They are the middleware between the data and the contract. The blockchain servers have no visibility into how a particular smart contract works. The participating companies in the blockchain network must rely on one oracle for the information being entered into the smart contract.

A potential problem with smart contract data is that there is no completely trustworthy data, according to Sergey Nazarov, CEO of Chainlink. Nazarov, in a white paper, wrote that data may be "*benignly or maliciously corrupted due to faulty web sites, cheating service providers, or honest mistakes*".

On the face of things it may appear that smart contracts are revolutionary, however they face many difficulties including security. Whilst in theory the ledger is secure, it is still subject to the risk of cyber-attacks, particularly those of a public nature. The operation of the platform can cause security risks, and bugs or defects may not be promptly highlighted and resolved by the users or developers.

There are also potentially high implementation costs and the general risk of human error could result in heavy financial losses. In June 2016, a hacker exploited a weakness in the code of the Decentralised Autonomous Organization obtaining $50 million of digital money. The incident conveys how coding can be just as vulnerable to human mistakes. Rather than penetrating the smart contract's security procedures, the hacker detected a loophole within the code. Similarly, some traditional contracts can be manipulated with their own loopholes. Even with this new technology it appears that human error will remain a risk.

I note that Tokyo-based company Fujitsu has claimed to have designed an algorithm that detects risks within Ethereum smart contracts created on blockchain technology. The algorithm is intended

to identify vulnerabilities and errors within smart contracts that are coded in GO language, which is often used in blockchain contract construction. The detection technology analyses 13 risks vectors Fujitsu has identified. Again such algorithms are still being developed and tested.

If smart contracts are to fulfil their potential, it is essential that we mitigate the highlighted risks. There is a need for working groups to address such risks and join with developers. Claire Fitzpatrick, Strategic Operations Director at ConsenSys, stated at the Law Society of Ireland FinTech Symposium; "*Legal firms have a great appetite to understand the technology, and are crying out for regulation and guidance on regulation as a starting point*".

It is my view that any regulation and guidance will need significant input from industry.

I do not wish to overshadow the potential of smart contracts but it is vital to address the risks involved. To conclude, utilisation of smart contracts is an area which is evolving rapidly. If the market intends to fully exploit their potential it is necessary to take appropriate steps in mitigating their associated risks.

Deborah Hutton
Partner and Head of Asset Management & Regulation

+353 1 6644 273
+353 86 184 9114
DeborahHutton@eversheds-sutherland.ie