Bird & Bird & Smart Contracts

Introduction

The first generation of blockchain technology was used to process and record Bitcoin transactions. The second generation of blockchain technology, coded to enable a wider functionality, heralded more diverse uses beyond just operating a ledger of cryptocurrency transactions. Perhaps the best known use of this second generation blockchain technology is the public Ethereum blockchain, based on smart contract technologies.

This briefing note is intended to be a high-level overview of smart contracts, covering what they are, how they function, and their interface with contract law.

For more in-depth content on a variety of blockchain topics, please visit our Blockchain in Focus webpage.

What is a smart contract?

A smart contract is an agreement between parties in the form of a computer code on how a set of procedures or processes will operate. The concept of smart contracts is not new but it has received renewed focus given the deployment of smart contracts on a blockchain which means that they are immutable once the code has been uploaded (unless a "kill switch" has been included in the code). Smart contracts automatically execute when the conditions in the coded agreement are met, removing the need for a trusty third party, such as a bank, to execute the transaction or agreement.

A commonly cited analogy is that of a jukebox, where the software in the machine enables the transfer of an output (e.g. the music) on the occurrence of an input (e.g. correct payment).

Process for establishing a smart contract, on a blockchain

Typically, the process for establishing and executing a smart contract will follow the below framework (this is based on deployment on the public Ethereum blockchain):

1. The relevant parties negotiate terms and create the smart contract code based on agreed terms.
2. One party creates a "contract transaction" which includes the compiled smart contract code and signs the contract transaction to create a digital signature.
3. The contract transaction and digital signature are sent to the blockchain network for validation and recorded on the blockchain database.
4. The smart contract is included in a block and has its own address so account holders or trusted third parties know where to find it and send transactions to it.
5. The smart contract is triggered in response to valid inputs: transactions sent from the relevant account holders or from trusted third party systems.

Bird & Bird & Smart Contracts

Smart contracts and contract law

Smart contracts, under English law, may constitute a legal contract (provided the key elements of a contract are met: offer, acceptance, intention to create legal relations and consideration).

It remains to be seen however if they are capable of acting as a complete substitute for natural language contracts, for the following reasons:

- Contractual nuance: it is not currently possible to create a code that captures all of the subtle nuances and complexities of commercial agreements. Computer code is not able to capture non-exhaustive lists of circumstances (like force majeure events) or replace centuries of common law and statute relied upon to deal with issues such as fraud, misrepresentation or mistake.

- Flexibility: once a smart contract is deployed and immutably recorded on a blockchain, little can be done to change its logic, unless the deploying party has introduced a "kill" mechanism to stop the code executing. Without a kill mechanism, if a person sends a transaction to the smart contract by accident the code will automatically self-execute and it cannot be reversed unless the parties independently agree to reverse it through a separate transaction.

In light of the above, we recommend that agreements between parties relating to smart contracts are based on a natural language contract which then incorporates by reference the relevant, agreed smart contract code. To the extent that there is a conflict between the two, the parties to the natural language contract can agree which component (i.e. either the natural language contract or the smart contract) will prevail.

Smart contract use case

A very simple example of how a smart contract could be used in the real world is that of flight delay insurance:

1. A customer purchases a flight delay insurance package to receive compensation for a flight delay over a specified time.
2. The terms of this agreement are coded and stored in a smart contract which is recorded on a blockchain and consults an air-traffic database to determine the flight's status (third party databases relied upon by the smart contract are referred to as "oracles").
3. If the flight is delayed by the specified amount of time the smart contract automatically executes and triggers the agreed output (e.g. confirming the customer is due compensation)
4. The insurance company (via an API) would need to consult the blockchain and be alerted to this output. On receipt of the output it would then execute a payment transfer from its bank to the customer's bank.

Here the terms of the smart contract are very simple, a specified input (the flight's delay time) results in a specified output (the customer's compensation). However, there would still need to be a natural language contract in place (for the reasons previously mentioned). Also, automatic execution of the payment (on receipt of the output) is not currently possible. Hence the reason why the insurance company would need to consult the blockchain and then notify its bank of the payment transfer on receipt of a valid output.

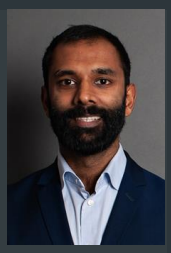
Bird & Bird & Smart Contracts

For more information or a free initial meeting, please contact:

Key contacts

Jonathan Emmanuel
Partner

Tel: +442074156052
jonathan.emmanuel@twobirds.com

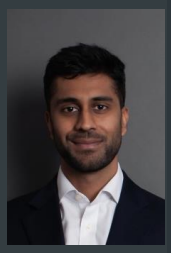


Gavin Punia
Senior Associate

Tel: +442030176884
gavin.punia@twobirds.com

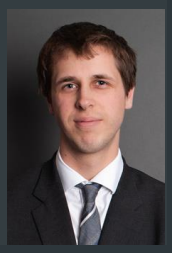
Ash Shah
Associate

Tel: +442074156606
ash.shah@twobirds.com



Thomas Hepplewhite
Associate

Tel: +442074156777
tom.hepplewhite@twobirds.com



Charles Hill
Trainee Solicitor

Tel: +442074156745
charles.hill@twobirds.com

"The firm is at the forefront of some of the most cutting-edge mandates in the area, advising on innovative matters in payments, crowdfunding, open banking and blockchain."

Chambers FinTech UK, 2020

twobirds.com

Abu Dhabi & Amsterdam & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw