SECTION 4

SMART CONTRACTS

A **SMART CONTRACT** is a computer protocol which can digitally facilitate, verify, or enforce the negotiation or performance of a contract.

Smart contracts are intended to replace the subjective and fallible human interpretation of complex contracts, and replace it all with computer code, thus allowing the performance of credible transactions without third parties. These transactions are both trackable and irreversible.

They were first described in the mid-1990s, long before the advent of blockchain. The code would assess and execute the terms of the contract, and would be decentralised without any reliance on a central authority to keep things impartial. The problem at the time was that there was no proven distributed database for them to run on.

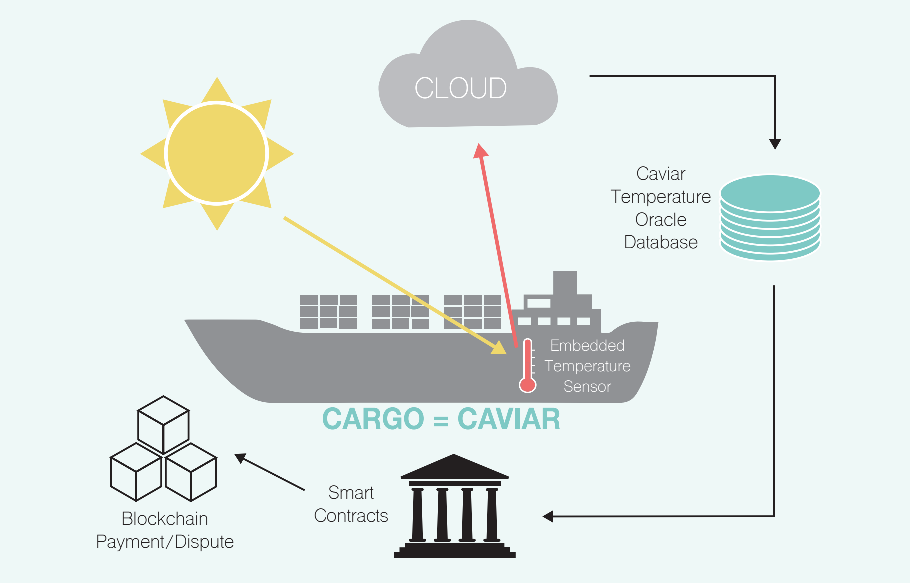
The appearance of Distributed Ledgers made the idea of Smart Contracts a reality, as smart contracts run on a blockchain. The consensus mechanism ensures that decisions are made fairly, and the immutability means that the contract cannot be tampered with. As the smart contract is running on the blockchain it can interact with a cryptocurrency, while also influencing transactions on it.

Promoters of smart contracts claim that many kinds of contractual clauses may be made partially, or fully self-executing and self-enforcing, or both. The aim of smart contracts is to provide security that is superior to traditional contract law, and to reduce the other transaction costs associated with contracting; although their status in the courts has not yet been fully determined. Various cryptocurrencies have implemented types of smart contracts.

SECTION 5

ORACLES

Example to illustrate:
The smart contract pre-conditions of transport state, that at no stage, should the cargo of caviar be at a temperature greater than 2 degrees celsius.


CLOUD
Caviar Temperature Oracle Database
Embedded Temperature Sensor
CARGO = CAVIAR
Blockchain Payment/Dispute
Smart Contracts

The oracle will record the daily temperature readings. These will be retrieved by the smart contract to determine whether contractual conditions have been met.

Blockchain oracles sound like something from ancient mythology, and in a way, they function in a similar role. In ancient stories, people didn't have enough information to make decisions and turned to oracles for information beyond their understanding.

In the same way, blockchains like those of Bitcoin and Ethereum, do not have ready access to information outside of the chain, and so there is no direct way to validate the conditions that smart contracts are based on.

An **oracle** is, simply put, a translator for information provided by an outside platform.

Oracles provide the necessary data to trigger smart contracts to execute when the original terms of the contract are met. These conditions could be anything associated with the smart contract, such as temperature, payment completion or price changes. These oracles are the only way for smart contracts to interact with data outside of the blockchain environment.

Blockchain developers at the cutting edge of new blockchain technology are making constant progress regarding ways to make blockchain better integrated with the outside world. Due to the fact that oracles are themselves smart contracts, designed to interact with the blockchain by providing necessary data, they require developers with expertise in both off-chain and decentralised fields.

The recent and profound need for external data on blockchains has given rise to new and interesting developments in the space. For example, oracles would allow blockchain connection to any existing Application Programming Interface (API), allow payments using traditional payment networks from blockchain, and allow interchain connections between smart contracts and other blockchains.

Oracles are radically important. Smart contracts cannot function without some data source. Without access to these sources of information, use-cases for smart contracts drop to just a tiny fraction of their potential.

However, with these systems, smart contracts have real world applications in virtually every field available. Once data hits the blockchain, the information can be used to execute contracts and provide use-cases, which can disrupt industries across the board.