What is a Smart Contact? (WIP)

What is a smart contract?

The BlockchainHub "A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced. The smart contract code facilitates, verifies, and enforces the negotiation or performance of an agreement or transaction. It is the simplest form of decentralized automation." [1]

Simply put, a smart contract is a distributed trusted program that runs on a blockchain network , it is the business logic of a blockchain application [2]. It is distributed because all the network participants not only have a copy of the smart contract, but they also execute the smart contract. It is trusted because once the participants execute the smart contract, they must have the same outcome and come to consensus. Once the criteria on the blockchain network is met, then its code defined in the smart contract will automatically execute, applying any business logic contained as predifined built-in rules.

There are different names for a smart contract, depending on the blockchain platform. Smart contracts were first proposed by Nick Szabo in "The Idea of Smart Contracts - Nick Szabo - Originally published in 1997"[3], where he coined the term. Ethereum was first to establish the term, "smart contract" for their blockchain platform and due to openness and its explosive popularity that term stuck. However, other blockchain platforms refer to a smart contact differently. For example, Hyperledger Fabric refers to smart contacts as, "Chaincode". Whereas, Hyperledger Sawtooth refers to smart contacts as, "Transaction Families". Yet, "Smart contact" can be used as a general term for code that runs on a blockchain network and that is how we'll use it going forward.

There are various guidelines for how you should implement your smart contract for consistency, privacy, reliability and performance. Each blockchain platform has their own unique features and capabilities for what a smart contact may or may not be able to do. This is mainly due different blockchain platforms catering to their unique features and capabilities. For example, Ethereum forces a limited xxx. However, Fabric allowed xxx. Yet, no matter the blockchain platform, a smart contact is designed to execute - TBD

There are many uses cases for smart contracts. In fact, the word "contract" hints a fundamental use case - to define an agreement or contract between one or more parties. When the terms or criteria of that contract are met, then the code for that contract will execute. The smart contract defines the who, what and how… - TBD

Ref1: https://blockchainhub.net/smart-contracts/

Ref2: https://hyperledger-fabric.readthedocs.io/en/release-1.4/whatis.html

Ref3: https://nakamotoinstitute.org/the-idea-of-smart-contracts/

Architecture of smart contracts

TBD – Discuss types, for example:
• Order-execute
• Execute-order-validate

Ref1: https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf

Differences between a smart contract and a law contract

TBD

Examples of smart contracts

There are many examples of smart contracts. Probably the most popular are in the cryptocurrency space, such as Bitcoin and Ethereum. For example, Bitcoin does have a smart contract, albeit a hard-coded one. In other words, the Bitcoin smart contract defines who, what and how Bitcoin works. Whenever someone initiations a transfer of Bitcoin funds, they are essentially executing a smart contract. You cannot simply modify the Bitcoin smart contract without the majority of the network agreeing your version. The other option would be to fork the network and creating an entirely separate blockchain network. This is similar to how Bitcoin Cash came to be.

Ethereum, on the other hand, allows you to run various smart contracts on the same network. TBD

Example smart contract use case

Ref: Smart Contracts Business and Use Cases

Let's start with an example smart contract for a food supply chain scenario. The food supply chain includes various unique participants, such as the grower or farm, producer, distributor or retailer.

[insert figure 1]

Advanced smart contracts
TBD
• Using analytics
• Rules engine