Tackle the Smart Contract Vulnerabilities

Parthasarathi R.
Delhi University, India

Puneet Kaushal
Lucideus Technologies, India

INTRODUCTION

The advent of Blockchain technology led the way towards the development of an electronic contract called Smart Contract. Technically, a smart contract is a computer program that is deployed and running on blockchain they are immutable, public and decentralized (Szabo 1997).The decentralized model of immutable contracts denotes that the execution and output of a contract are validated by each participant in the system so that no single party/participant is in control of the money. That is, no one could force the execution of the contract to release the funds, as this would be made invalid by the other participants in the system. Tampering with smart contracts becomes almost impractical.

BACKGROUND

This section briefly features the nature and the need for smart contracts technology along with its basic properties.

What Are Blockchain and the Smart Contract?

A blockchain is a cryptographic database (ledger) maintained by a network of computers, each of which stores a copy of the most up-to-date version. A blockchain protocol is a set of rules that dictate how the computers in the network, called nodes, should verify new transactions and add them to the database.

A smart contract is an electronic form of conventional contract/agreement deployed and running on the blockchain which executes the terms of the contract automatically without any need of trusted third parties (mediator, court, etc) for the effective implementation.

Figure 1 depicts the sample use case of smart contract in the Business (farmer) to customer model.

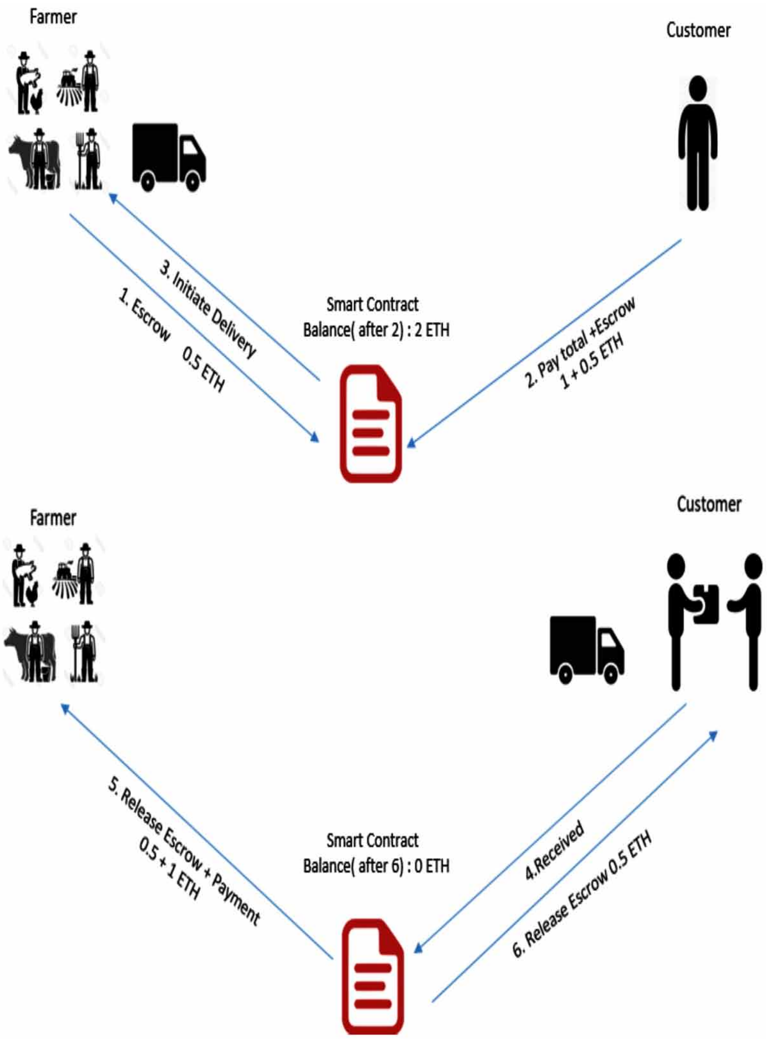
Need for the Smart Contract

Traditional transactions are built on trust and, usually, contracts are considered as a symbol for an existing business deal by the contracting parties. Another major problem with the traditional contracts is that they do not provide enough details about the actual transaction process and as a result. Friction with conflicts between the contracting parties is more frequent (alexbafana 2016).

The above mentioned problems are addressed effectively by the development of a smart contract. In general from the viewpoint of information technology smart contract is viewed as an online program, in reality, it is a multidisciplinary concept that also concerns finance/business and contract law, each with

DOI: 10.4018/978-1-5225-9715-5.ch062

Figure 1. Farmer to customer transction using smart contract



the different perspective (Chapter 9: Building a Secure Future, One blockchain at a time 2018). That is, from the viewpoint of business, a smart contract defines how transactions and payments are executed among different accounts. From the viewpoint of contract law, a contract is an agreement between mutually committed parties (Ustbmde 2018). Because of its interdisciplinary nature, development of smart contract needs collaboration between many experts such as business experts, software and information security engineers, lawyers, and bank managers from different domains (He, et al. 2018).

Properties of Smart Contract

Everything that runs on a blockchain required to be immutable and should have the capability to run through multiple nodes without any compromise on integrity. In order to achieve that, smart contract functionality needs to have three things in common: