Ethereum – Summary

The main purpose of Ethereum is to store several different applications, also called “smart contracts”. Bitcoin has scripts for the purpose, but the bitcoin scripting language is not Turing complete, and therefore cannot offer everything. For example, no loops are allowed in a bitcoin script. Ethereum on the other hand offers a Turing complete language, which means that anything can be programmed, and the program can be stored in the blockchain. However, very computationally expensive programs are not desirable as Ethereum applications require “gas” to run. Each instruction will cost some amount of gas, this is to ensure no infinite loops. Currency is called ether. Unlike bitcoin, Ethereum stores balance for each account, like a traditional bank, also called account-based ledger. Ethereum uses more complicated data structure than bitcoin, something called Patricia trees. To prevent relay attacks, instead of just stating “Alice sends 5 ethers to Bob”, it’s more as “Alice sends her nth transaction 5 ethers to Bob”, once miners verify the 5 ethers transaction, it cannot be replayed as miners will see nth transaction has already been used.