Mohammad H. Tabatabaei

Ethereum

Many altcoins were introduced after Bitcoin for providing application-specific functionality in addition to cryptocurrencies. However, Ethereum tried to create a general-purpose platform by the help of blockchain and smart contracts. Thus, Ethereum can be used to implement any application-specific altcoin's functionality.

In Ethereum, anyone can spend some fee to add a contract into a special transaction, and then the contract will be kept on the blockchain. The contract is a program which is written in bytecode and executed by Ethereum-specific virtual machine (EVM). There are many applications that can be implemented by Ethereum including prediction markets, smart property, escrowed payments, auctions and ordering books.

In contrary to Bitcoin, Ethereum supports loops, thus, in order to prevent running contracts forever, Ehereum utilizes gas. Gas is the amount of money which is spent for executing each virtual machine instruction. As different operations cost different amounts, very expensive computations are not appropriate for Ethereum. At the beginning of every program call, the user must specify the amount of gas that is needed to spent. If the gas is finished in the middle of the program execution, all changes to the program's state are reverted and the miner caches the gas. Hence, Ethereum is much more suitable for applications that require security protocol logic because it can provide anonymous parties a condition to trust each other.

Another difference between Bitcoin and Ethereum is about the data structure. Although, Bitcoin blockchain stores only transactions, Ethereum uses an account-based model which means that Ethereum just stores a balance for each address. Every block contains a digest of the current state of every address in addition to the state of every contract. In order to have fast lookups and the ability of updating an address's value Ethereum uses a Patricia tree instead of Merkel tree which is used in Bitcoin.

Finally, in addition to EVM, a new programming model, and Patricia tree data structure, Ethereum is different from Bitcoin in terms of consensus protocol. Ethereum needs just 12 seconds for creating a block instead of 10 minutes which is needed for Bitcoin. Furthermore, proof-of-work is also different in Ethereum. Currently, it is a mix of hash functions in order to be memory hard, though Ethereum tends to change this method to a proof-of-stake system.