Summary

Ethereum is a newer blockchain based application very similar to Bitcoin. The differences that Ethereum offer are tradeoffs that are very useful when comparing the two digital designs. The main layer of benefit that Ethereum offers is the inclusion of a built in Turing Complete programming language where anyone can write smart contracts that create rules for transactions, ownership, and other things. This gives Ethereum a good amount of power and advantage over Bitcoin when it comes to scripting.

Ethereum is made of objects called “accounts” that are identified by 20-byte addresses. These accounts can make transactions with each other and communicate. An account has a nonce (one-time message), a balance, a contract code, and the storage. Transactions between accounts contain the recipient, the amount, the signature, data, STARTGAS (max computational steps), and GASPRICE (fee that sender pays). The last two prevent attackers from running infinite loops. The more steps that someone executes, the higher fee that they must pay.

Ethereum Blockchain is also very similar to Bitcoins. One difference is that Ethereum blocks contain both the transaction list and the most recent state of the ledger. Block number and difficulty are also stored.

Questions

1. How do you get gas and what happens when you run out? What happens when a legitimate sender of ether runs out of gas? Are there cases where a legitimate sender would need heavy computational work?
2. Why does having a Turing complete scripting language built into an application allow for more financial contracts? Why can’t bitcoin have these contracts?