KONSTANTINOS CHRISTIDIS, MICHAEL DEVETSIKIOTIS, K.CHRISTIDIS(North Carolina State University, Raleigh, NC 27606, USA )

“Blockchains and Smart Contracts for the Internet of Things “

Blockchains allow us to have a distributed peer-to-peer network where non-trusting members can interact with each other without a trusted intermediary, blockchain-iot combination facilitates the sharing of services and resources which forms a connection between different devices, we can verify using different cryptography technique.

As the blockchain enables trustless network ie. the parties can transit even though they don’t trust each other, as there is no trust issue between the parties which means that the interaction between the two parties will be much faster.

These functionality of blockchain is very useful for researchers and developers who are working in hot domain as it is secure and fast to obtain data.

All the IoT devices of a manufacturer operate on the same blockchain network. The manufacturer deploys a smart contract that allows them to store the hash of the latest firmware update on the network .The devices either ship with the smart contract’s address baked into their blockchain client, or they find out about it via a discovery service. They can then query the contract, find out about the new firmware, and request it by its hash via a distributed peer-to-peer filesystem.

Tien Tuan Anh Dinh , Rui Liu, Meihui Zhang , Gang Chen, Beng Chin Ooi, and Ji Wang ”Untangling Blockchain: A Data Processing View of Blockchain Systems”

In the original design, Bitcoin’s blockchain stores coins as the system states. For this application, Bitcoin nodes implement a simple replicated state machine model which moves coins from one address to another. Since then, block-chain has grown beyond crypto-currencies to support user-defined states and Turing complete state machine models.For example, Ethereum enables any decentralized, replicated applications known as smart contracts.

The blockchain can be classified as public blockchain and private blockchain.

Public blockchain:

Bitcoin is the most well known example of public block-chains. In Bitcoin the states are digital coins (crypto-currencies), and a transaction moves coins from one set of addresses to another. Each node broadcasts a set of transactions it wants to perform. Special nodes called miners collect transactions into blocks, check for their validity, and start a consensus protocol to append the blocks onto the blockchain. Bitcoin uses proof-of-work (PoW) for consensus, only a miner which has successfully solved a computationally hard function can append to the blockchain. Bitcoin transaction speed remains very low as it takes high computation to validate the block it is nearly 7 transactions per second.

Private blockchain:

Hyperledger is among the most popular private blockchains.Three phase protocol is used in this blockchain to validate the transaction.In the pre-prepare phase, a leader broadcast a value to be commit by other nodes. Next, in the prepare phase, the nodes broadcast the values they are about to commit. Finally, the commit phase confirms the committed value when more than two third of the nodes agree in the previous phase.