Assignment 6

Blockchain & smart contracts using Ethereum

Blockchain

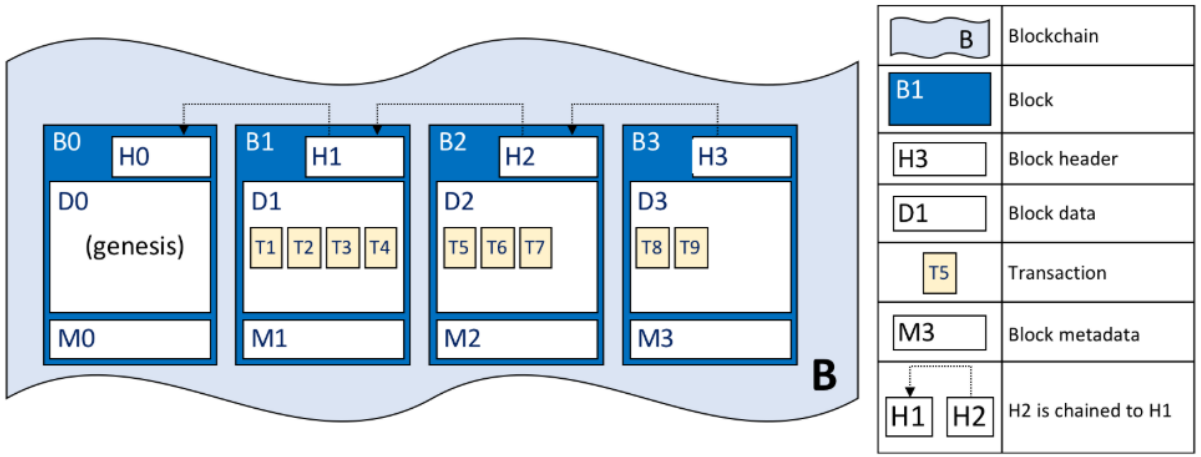
Date	Detail	Debit	Credit	Balance
22.04.16	Invoice 10575	245.00		245.00
26.04.16	Invoice 10583	385.00		630.00
8.05.16	Invoice 10590	260.00		1,135.00
30.05.16	Payment received		1,135.00	0.00
10.06.16	Credit 025 for returns		80.00	-80.00
21.06.16	Invoice 10623	540.00		460.00

- Essentially a **decentralized, distributed ledger**
- Continues to be available even if a server or a group of servers on a network are not available
- Any server or node on a network is connected to every other node on the network directly or indirectly
- A special database that **do not allow modification of existing data**
- Newer transaction to be stored in append only pattern without any scope to modify past transaction
- Ethereum is an implementation of Blockchain

Ethereum

- Main objective of Ethereum is to accept transactions from accounts, update their state and maintain this state as current state till another transaction updates it again
- Decoupling between when a transaction is accepted by Ethereum and when the transaction is executed and written to the ledger
- Decoupling is quite important for decentralization and distributed architecture to work as expected

Blockchain

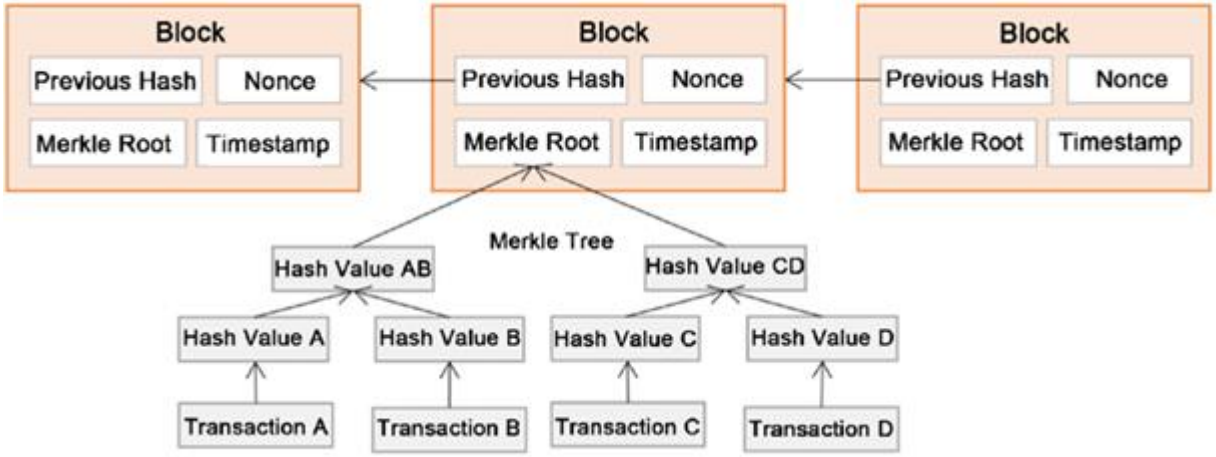


- Asymmetric cryptography refers to process of using two separate keys for encryption and decryption
- Encrypt with public key, Sign with private key
- Hashing transforms any length data into a fixed length data and it is not possible to re-generate or identify the original data from resultant string data
- Ethereum hashes all the transaction data, hashes multiple transaction hashes to generate single root transaction hash and in fact the blocks in Ethereum are also represented as hash

Ether

- Ether is the currency of Ethereum
- Every activity on Ethereum that modifies its state costs Ether as fee
- Miners who are successful in generating and writing a block in chain are also rewards Ether
- Base unit is called ‘wei’ – 1e18 wei = 1 ether
- Changing cost of Ether makes the cost of using the same service very high on certain days and low on other days
- Gas, the internal currency of Ethereum, helps to alleviate this problem
- Cost is predetermined in Ethereum not in Ether but in Gas units
- Gas price will then be adjusted to lower price when price of Ether increases and higher price when price of Ether decreases

Mining



- For each block of transactions, miners use computers to repeatedly and very quickly guess answers to a puzzle until one of them wins
- Miners will run the block's unique header metadata through a hash function only changing the 'nonce value' to match the target hash (which contains a number of leading zeros)
- **0000000000001x2xhf2sdkfhsdfh2ksdfhksdfhsdf**
- If the miner finds a hash that matches the current target, he'll be awarded ether and broadcast the block across the network for each node to validate and add to their own copy of the ledger

Smart Contracts

- Nodes belonging to miners and each miner maintains an instance of ledger, which contains all blocks in the chain
- Nodes that help with smart contracts called EVM, which deploys, stores and executes code written in them
- Smart contracts removes intermediaries & ‘middlemen’, aka self executing contracts
- Smart contracts are very similar to Object oriented classes. A smart contract can call another smart contract just like an Object-oriented object to create and use objects of another class
- Solidity is an object-oriented programming language for writing smart contracts (*.sol)
- Use local IDE or online IDE like Remix (https://remix.ethereum.org/)

Transactions & Blocks

- Transactions
  - **From** Account property denotes the account that is originating the transaction
  - **To** account property refers to an account that is receiving ethers or benefits
  - **Value** refers to the amount of ether that is transferred
  - **Input** refers to the compiled contract bytecode and is used during contract deployment in EVM
- Blocks
  - are containers for transaction
  - contains multiple transactions

  based on Gas limit

Truffle

- Blockchain smart contract suite
- Development environment and testing framework
- Compile & test contracts
- Makes life easier for Ethereum developers, as well as for those who seek to gain a deeper understanding of how this technology works