CS5363 Blockchain Technologies and Applications: Hw5
Merkle Patricia Tree

1. Task

- Implement a Simplified World State Trie [as Diagram-1] based on Merkle Patricia Tree [Merkle Patricia Tree]
  - (Keys = Some Account Addresses, Values = Account Balances)
  - Implement "Branch Node", "Extension Node", & "Leaf Node"
  - Support basic "Trie operations": Construct a Trie, display a Trie, search nodes, insert nodes, update nodes...
  - Calculate the State Root based on RLP Encoding & Keccak256(SHA3) Hashing [RLP, Keccak256]
- Simulate Transaction Scenario & store the balance records in your World State Trie
  - Scenario 1: Initially, there are 5 users (A, B, C, D, E) in your Blockchain network. Therefore, your Trie should record these 5 users' account balances. Your Trie should be recorded as a unique State Root [as Table-2].
  - Scenario 2: After User-A transfers 2 Ether to User-D, and User-C transfers 6 Ether to a new User (User-F). Now, there are 6 users (A, B, C, D, E, F) in your Blockchain network. Therefore, your Trie should update original 5 users' account balances, and insert new nodes which record User-F's account balance. Similarly, your Trie will be recorded as a new State Root [as Table-3].

2. Submission

Compressed in zip file:

- Your Program (in any programming language)
- Readme file (which explains how to run your program)
- Test_paper.pdf, including:
  - The Trie Diagram & the State Root in Scenario 1
  - The Trie Diagram & the State Root in Scenario 2

Diagram-1

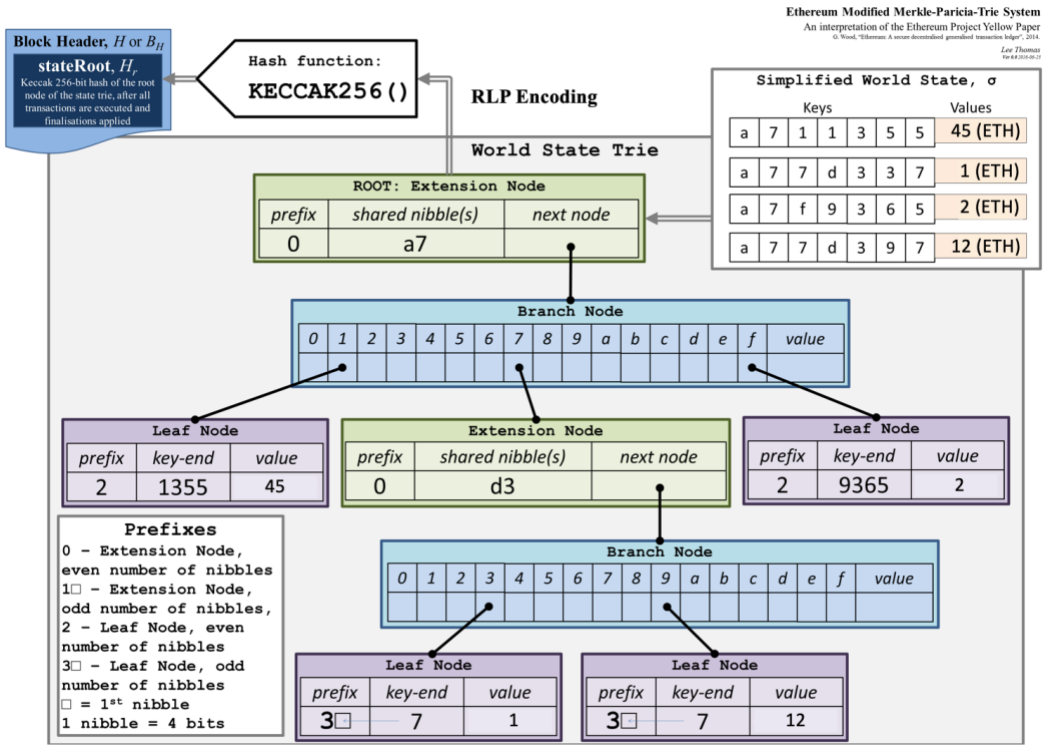

Table-1: Simple test case, as example in Diagram 1

User (not)	Account Address (key)	Balance (value)
A	a711355	45
B	a77d337	1
C	a7f9365	2
D	a77d397	12
State Root		
5838ad5578f346f40d3e6b71f9a82ae6e5198dd39c52e18deec63734da512055		

<Remark>

- As Diagram-1, store the address & balance in your Trie.
- (A, B, C, D) are just accounts' nicknames, no need to be stored in your Trie.

Table-2: Initially, there are 5 users stored in your State Trie.

User	Account Address (key)	Balance (value)
A	7c3002ad756d76a643cb09cd45409608abb642d9	10
B	7c303333756d555643cb09cd45409608abb642d9	20
C	7c303333756d777643cb09c999409608abb642d9	30
D	7c303333756d777643cb09caaa409608abb642d9	40
E	111102ad756d76a643cb09cd45409608abb642d9	50
State Root		
???		

Table-3: After some transactions, your State Trie is updated.

User	Account Address (key)	Balance (value)
A	7c3002ad756d76a643cb09cd45409608abb642d9	10 - 2
B	7c303333756d555643cb09cd45409608abb642d9	20
C	7c303333756d777643cb09c999409608abb642d9	30 - 6
D	7c303333756d777643cb09caaa409608abb642d9	40 + 2
E	111102ad756d76a643cb09cd45409608abb642d9	50
F	11113333756d76a643cb09cd45409608abb642d9	+ 6
State Root		
???		

<Remark>

- Similarly, (A, B, C, D, E, F) are just accounts' nicknames, no need to be stored in your Trie.
- Simply, we suppose no reward and other information generated in this transaction