**7CCSMDLC TUTORIAL QUESTIONS and SOLUTIONS**
**TOPIC 7: ICOs**
**TUTORIALS WEEK 8**

**Q1: Have a look at the Polkadot White Paper (also known as the "Pink Paper"), written by Gavin Wood, which presents the proposed technical vision of the Polkadot network:**

https://polkadot.com/papers/Polkadot-whitepaper.pdf

(a) What is the purpose of the network?
(b) What are the roles in the network?
(c) What responsibilities does each role have?
(d) What is the consensus protocol?

Answers:

(a) What is the purpose of the network? See Section 3.
(b) What are the roles in the network? See Section 4.
(c) What responsibilities does each role have? See Section 4.
(d) What is the consensus protocol?
Proof-of-Stake. See Section 5.5.1:
"Through the choice of a BFT [Byzantine Fault-Tolerant] consensus mechanism with validators formed from a set of stakeholders determined through an approval voting mechanism, we are able to get a secure consensus with an infrequently changing and modest number of validators."

**Q2. What is Delegated Proof-of-Stake (DPoS) protocol? Give an example of major blockchain using it.**

DPoS is a form of PoS where nodes with stakes do not **all** validate (and upload) blocks. Instead the nodes with stakes vote for representative nodes to undertake the validation duties. Voting is usually in proportion to stakes (ie, in proportion to the numbers of tokens that each voting node has staked). For example, 1000 nodes with stakes may vote for just 20 nodes to be validators. If one of the 1000 nodes has staked 30% of the total number of tokens staked, then that node will have 30% of the votes. Usually the role of validator is not permanent, but only for a pre-defined period (say 1 month), and there is a new election at the end of each period.

A major blockchain which uses DPoS is EOSIO:

https://developers.eos.io/welcome/latest/protocol-guides/consensus_protocol

Some information here:

www.geeksforgeeks.org/delegated-proof-of-stake/

**Q3. What was the vulnerability in the DAO exploitation in 2016? How did a recursive call exploit this vulnerability?**

There is a summary here:

https:\\blog.b9lab.com/the-dao-hack-in-eight-minutes-94919018692d

For further reading, the article and paper by Mack, Zamfir and Sirer is interesting:

https://blog.bitmex.com/wp-content/uploads/2017/11/A-Call-for-a-Temporary-Moratorium-on-The-DAO.pdf

==========