7CCSMDLC TUTORIAL SOLUTIONS

TOPIC 4: PROTOCOLS

TUTORIALS WEEK 5

Q1. Create a table of the advantages and disadvantages of the major consensus protocols

1. **PoW**
2. **PoS**
3. **PoA**

Protocol	***Positives***	***Negatives***
PoW	▪ Provides a disincentive to Sybil attacks ▪ Due to success of Bitcoin, many people are familiar with it	▪ Complicated to implement ▪ Heavy use of electric power ▪ Incentivizes concentration of mining power
PoS	▪ Aligns incentives of validators with the system as a whole	▪ Still immature, and so may have unintended effects ▪ May be complicated to implement
PoA	▪ Easy to implement. ▪ Efficient use of resources	▪ Requires trusted validators (so therefore only suitable for permissioned blockchains)

Q2. What was the software bug which caused a long internal fork in Bitcoin in March 2013? How was it resolved?

See information here:

https://en.bitcoin.it/wiki/BIP_0050

https://freedom-to-tinker.com/2015/07/28/analyzing-the-2013-bitcoin-fork-centralized-decision-making-saved-the-day/

Q3. Explore the vulnerability of Parity wallets in the Polkadot ICO in 2017. What was the problem? What were the possible solutions?

See information here:

https://techcrunch.com/2017/11/07/a-major-vulnerability-has-frozen-hundreds-of-millions-of-dollars-of-ethereum/

https://fullycrypto.com/polkadot-reruns-ico-18-months-after-parity-disaster

The problem was that the wallets used to collect ETH contributions (ie, contributions in the Ethereum currency Ether) to the Polkadot ICO called another smart contract from a library. This smart contract had a vulnerability which allowed a third party to take control of it and kill it. Someone did this (perhaps accidentally), with the consequence that the wallets holding ETH contributions to Polkadot became frozen. Not all contributions to the Polkadot ICO were in ETH (some were in Bitcoin, and some in US Dollars), so Polkadot was still able to design and build their platform.

Other users also had frozen wallets due to this vulnerability. At the time (November 2017), a proposed solution to these frozen wallets was to hard-fork the Ethereum blockchain on which these wallets sat back to before the vulnerability arose (in a similar way to the hard fork of Ethereum on 20 July 2016 in response to the DAO theft that created Ethereum Classic). The longer this forking does not happen, of course, the harder it is to do, since all the other intervening transactions would be undone by the fork, and so have to be replicated. The affected Polkadot wallets are still frozen.