Assignment – 3
Information and Capacity - Philosophical and Technical Considerations
TCDID: 22333721, Name: Pallavit Aggarwal

Paper 1

Paper Subject: Handbook on the Philosophy of Information, 2008

- Information can be analysed in multiple ways depending on the context and the nature of problem
- Shannon paved the way to quantifying information using methods like Entropy.
- Quantum computers come with a lot of hope, but would be like GPUs
- Cryptographic systems would be at the most risk in a post quantum world.

Paper 2

Paper Subject: Demystifying Cryptography behind Blockchains and a Vision for Post-Quantum Blockchains

- NIST is developing standards for post quantum cryptographic world!
- Blockchains would need to be redefined once quantum computers start breaking hashes
- Ethereum uses Keccack -256 developed in a competition conducted by NIST. While Bitcoin uses secp256k1
- Breaking cryptographic hashes currently is computationally infeasible.