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

Paper Subject: Handbook on the Philosophy of Information, 2008
Paper link: https://ir.cwi.nl/pub/13851/13851B.pdf
Key Contributions/Findings/Conclusions

1. Interdisciplinary themes defining the transmission of information are presented with precise mathematical descriptions.
2. Information is analyzed and concepts like quantum information theory are defined among 29 different sub topics that are mentioned in the flow of the paper.
3. Shannon and his successors have provided a Quantitive basis to analyzing information in terms of Bit, Entropy and through other aspects of physics like thermodynamics
4. Information is not just words, letters or signals but acutally bits, electrical currents, and essentially electrons moving through space.

Key Technology Insights

1. Entropy, Error Correcting Codes are defined which open up the domain of Markov chains, decision trees, and generally analyzing the transmission of information as dictated by Shannon.
2. Quantum analysis of information is done, and qubits are mentioned. Qubits are electrons that have a superimposition and can exist in two states. Quantum mechanics works on amplitudes, and this domain opens up the quantum computing aspect.
3. Quantum computers are much like GPUs. They'll be slower to perform regular tasks using the classical theory of information, but the tasks which will require parallelizing using quantum states, will be run much faster.
4. Channel coding and noise in channel help analyze the flow of information over a noisy domain, and how algorithms and theorems in mathematics can help us still recover information from such domains.

Key Insights relevant to Scalable Computing

1. Quantum computers are not scalable and will be slower than usual
2. Cryptography would be required in IoT in a post-quantum world
3. Shannon's law apply to all IoT devices
4. Data reduction explored in the 20th century, has yielded high grade importance in the flow of information and helps low powered devices work more efficiently as they have to deliver lesser information.

Paper Subject: Demystifying Cryptography behind Blockchains and a Vision for Post-Quantum Blockchains Managed by Blockchain
Paper Link: https://ieeexplore-ieee-org.elib.tcd.ie/document/9298215
Key Contributions/Findings/Conclusions

1. Cryptographic primitives are discussed and background is laid for cryptography in blockchain systems.
2. Bitcoin and Ethereum account addresses using the above cryptographic premitives are explored in detail
3. Future works for developing ligh and scalable protocol for Post Quantum Blockchains
4. NIST standardization for post quantum cryptography is discussed.

Key Technology Insights

1. Based on the number of keys, cryptosystems are classified as Symmetric and Asymmetric/Public key cryptosystems. In symmetric system both encryt/decryt algo use the same key. In Asymmetric private key – public key pair is used.
2. Elliptic Curve Cryptography.
3. Bitcoin addresses are hashed public keys and the elliptic curve with secp256k1 constansts as public key cryptosystem for generating addresses.
4. Ethereum uses Keccack-256 cryptographic hash function which was developed in 2007 in a competion conducted by NIST

Key Insights relevant to Scalable Computing

1. Cryptography is a major part of Blockchain systems that empower the IoT communication and exchange of information
2. Cracking cryptographic hashes and number theoretic problems like discrete logarithm problem would be easier to solve and crack in a post-quantum world.
3. Grover's Algorithms and Shor's Algorithm are forcing a redesign of the blockchains using cryptosystems resistant to quantum attacks.
4. NIST is standardizing post-quantum cryptosystems striving for a lightweight and efficient ecosystems.