The following are my takeaways from the mandatory paper and the topic that I selected from it.

In the first paper we look at different techniques and optimizations for transmission of information. To illustrate this with an example,

Let's say Alice wants to send bob 1 letter in the English alphabet and he can ask yes and no to identify this. If we apply linear search to this, then he will ask yes no 26 times in worst case, but if apply binary search, that is we eliminate half of the search space every time we get log(26) to the base 2.

And information transmission is predictable and can be refined using probabilities.

Claude Shannon quantifies this as Entropy and he uses the letter H to represent it. So now the number of searches can be multiplied by the probabilities and a weighted summation can be taken.

Predictability can also be used to do compression on the message in a noiseless channel.

In a noisy channel, where you have interference in the voltages, we have to do error correction.

Now, The Classical model can be extended to the Quantum model. A qubit, like a bit is the building block of quantum information. It can be anything between 0-1 and this middle state is called a superposition. When we use the fact that a qubit can exist in a superposition, we can form an entanglement with more than one qubit.

This entangled state can be used by computers and shared among them as a protocol for communication. Quantum computers are only fast, when we make use the fact that all these superpositions are available to us at the same time.

Much like GPU, if the algorithm doesn't take advantage of the superposition and interference then Quantum computer might even be slower

Now moving to the next part,
So quantum computers picture in the topic of scalability as both public-key cryptosystems and hash functions are threatened by the evolution of quantum computers.

The three papers I selected evaluate and review the post-quantum world of blockchains and cryptography.

public-key or asymmetric cryptography is essential for authenticating transactions and Hash functions are important for generating digital signatures and for linking the blocks of a blockchain

In particular Grover's algorithm poses threat to hash functions, while Shor's algorithm threatens public-key cryptography thereby forcing researchers to think about redesigning Blockchains by making use of cryptosystems that are resistant to quantum attacks, thus creating post-quantum cryptosystems.

The first larger figure shows time to break a symmetric key. and the smaller image right to it, shows the asymmetric key – factorization algorithm times. The time is mentioned in seconds, and Tq shows quantum times. 3.1 x 10^8 is 10 years.

As of now, Researchers have determined that 160-bit elliptic curves can be broken with a 1000-qubit quantum computer, while 1024-bit RSA would need roughly 2,000 qubits. The most powerful quantum computer IonQ, has only 79 qubits. But in the next 5 to 10 years such kinds of computers will be functional enough.

There are research projects like zk-STARK, PQCrypto, SAFECrypto and Prometheus that are working on making cryptosystems resistant to such attacks and they're introducing multiple new techniques in the algorithms and the way system is designed.

National Institute of Standards and Technology is in the process of standardizing the post-quantum cryptosystems and currently has reached to round 3. This is the same institute which conducted a competition in 2007 and Keccak-256 hash function used by Ethereum was the winning algorithm.

Nowadays, there are no post-quantum blockchain algorithms that provide, at the same time, small key size, short signature/hash sizes, fast execution, low computational complexity and low energy consumption. Such factors are especially critical for resource-constrained embedded devices like the ones used in the Internet of Things.

Thank you.