Primitive	Strengths	Weaknesses
Conventional public-key cryptography (RSA/ECC)	• Widely used and tested. • No known classical attacks.	• Vulnerable to quantum attack via Shor's algorithm. • Vulnerable to store-now-decrypt-later quantum attacks. • Should not be used for information with significant forward value. • Memory overheads: ciphertext longer than plaintext. • Computationally relatively slow.
Conventional private-key cryptography (e.g AES)	• Widely used and tested. • No known efficient classical or quantum attacks. • Computationally efficient. • No memory overheads: plaintext and ciphertext are of equal length. • Hardware optimisation: many modern processors contain dedicated AES co-processors and instructions.	• Absence of security proofs. • Quantum attacks offer quadratic enhancement of brute-force attacks (can be offset by doubling key lengths).
Hash functions (e.g SHA)	• Widely used and tested. • No known efficient classical or quantum attacks. • Computationally efficient. • Hardware optimisation: many modern processors contain dedicated SHA co-processors and instructions.	• Quantum attacks offer quadratic enhancement in finding pre-images (can be offset by doubling hash lengths).
Post-quantum cryptography (lattice-based methods)	• Promises robustness against both classical and quantum attacks. • Compatible with existing classical hardware. • Adoption is straightforward.	• New and inadequately tested. • Not yet standardised.
Post-quantum cryptography (hash-based digital signatures)	• Security inherited only from pre-image resistance of hash functions, considered very strong.	• Large memory overheads.
Quantum cryptography	• Theoretically offers perfect information-theoretic security.	• Only facilitates private-key cryptography. • Not applicable to public-key cryptography. • Channel authentication relies on classical techniques. • Highly limited utility. • Not suitable for roaming devices. • Restricted to point-to-point communication. • No broadcasting. • Requires new and expensive infrastructure. • Heightened risk of denial-of-service attacks. • Heightened risk of side-channel attacks. • Real-world implementations largely untested.
Secure quantum computation (homomorphic encryption & blind quantum computing)	• Theoretically offers perfect information-theoretic security.	• Not presently available. • Requires quantum communication infrastructure between client and server.
Blockchains	• Can adopt post-quantum cryptography upon availability.	• Security inherited from underlying choice of public-key cryptography and hash functions. • Current implementations largely rely on RSA/ECC and vulnerable to future quantum attacks.
Hybrid cryptography	• Multiple encryption ensures security unless all layers of encryption are compromised.	• Increased computational, memory and communications overheads.