1. Define symmetric encryption. Give two examples.
2. What is the main drawback of symmetric encryption?
3. Explain the concept of a secret key in symmetric cryptography.
4. What is asymmetric encryption? How does it differ from symmetric encryption?
5. Compare AES and DES in terms of key size and security.
6. Explain how RSA encryption works with a simple example.
7. Why is key distribution a challenge in symmetric encryption?
8. How does the Diffie-Hellman key exchange protocol work?
9. What is a man-in-the-middle attack in asymmetric encryption?
10. Explain hybrid encryption and its advantages.
11. What is a cryptographic hash function?
12. Name two widely used hash functions.
13. Why are hash functions considered one-way?
14. What is the avalanche effect in hash functions?
15. How do hash pointers ensure data integrity in blockchain?
16. Explain the difference between SHA-256 and MD5.
17. What is a collision attack in hash functions?
18. How does Bitcoin use hash functions in mining?
19. Can quantum computers break cryptographic hash functions? Justify.
20. What is a Merkle-Damgård construction?
21. What is a digital signature?
22. How does ECDSA differ from RSA signatures?
23. Explain the steps involved in ECDSA signature generation.
24. Why is ECDSA preferred in blockchain over RSA?
25. What is the role of elliptic curves in ECDSA?
26. How can a weak random number generator compromise ECDSA?
27. Explain the significance of the \`r\` and \`s\` values in ECDSA.

28. What is a memory-hard function? Give an example.

29. Why are memory-hard algorithms used in cryptocurrencies?

30. Compare Scrypt and Argon2 in terms of security.

31. Explain the concept of Zero-Knowledge Proof (ZKP).

32. How does zk-SNARK improve blockchain privacy?

33. What is the "Fiat-Shamir heuristic" in ZKP?

34. What is the Byzantine Generals Problem?

35. How does blockchain solve the Byzantine Generals Problem?

36. Explain Practical Byzantine Fault Tolerance (PBFT).

37. Compare PBFT with Nakamoto Consensus.

38. How does quantum computing threaten RSA encryption?

39. What is Shor’s algorithm?

40. Can quantum computers break Bitcoin’s SHA-256? Explain.

41. What is a blockchain?

42. How does mining work in Bitcoin?

43. Explain the role of nonce in mining.

44. What is the 51% attack?

45. What is Proof of Work (PoW)?

46. Compare PoW and Proof of Stake (PoS).

47. What is Proof of Burn?

48. What is a smart contract?

49. Explain Ethereum’s gas mechanism.

50. What was the DAO hack?

51. How can blockchain be used in IoT?

52. Discuss blockchain in medical record management.

53. What are sidechains?

54. What are the legal challenges of cryptocurrency exchanges?

55. How does Bitcoin impact the global economy?

56. What is a Merkle Tree? How does it improve blockchain efficiency?

57. Explain how Bitcoin uses Merkle Trees in block headers.

58. What is a Merkle Patricia Trie (as used in Ethereum)?

59. How are transaction fees determined in Bitcoin?

60. Why do Ethereum transactions require a "gas limit"?

61. How does Bitcoin provide pseudo-anonymity?

62. Compare privacy in Bitcoin vs. Monero/Zcash.

63. What are "coin mixing" services? Are they legal?

64. What is a "chain policy" in blockchain governance?

65. How do forks (e.g., Bitcoin vs. Bitcoin Cash) reflect differing chain policies?

66. Define soft fork and hard fork with examples.

67. Why did Ethereum undergo a hard fork after the DAO hack?

68. Can a soft fork lead to a chain split? Explain.

69. What is a private blockchain? How does it differ from public chains?

70. Why would a company choose a private blockchain over a database?

71. What is Nakamoto Consensus?

72. How does Proof of Work (PoW) prevent Sybil attacks?

73. Explain the "Nothing at Stake" problem in Proof of Stake (PoS).

74. What is a Sybil attack?

75. How does Proof of Stake (PoS) reduce energy consumption compared to PoW?

76. What is Proof of Burn (PoB)?

77. How does Delegated Proof of Stake (DPoS) work?

78. Compare PoW, PoS, and PoB in terms of security and scalability.

79. What is "difficulty adjustment" in Bitcoin mining?

80. Why is energy utilization a criticism of Bitcoin?

81. What programming language is used for Ethereum smart contracts?

82. Explain the "reentrancy attack" in smart contracts.

83. How does the GHOST protocol improve blockchain security?

84. What is a "sidechain"? Give an example.

85. What was Namecoin’s original purpose?

86. What is Go-Ethereum (Geth)?

87. How does a "naive blockchain" differ from production-grade chains?

88. What are the trade-offs in blockchain scalability vs. decentralization?

89. How can blockchain secure IoT devices?

90. Discuss a medical record management system using blockchain.

91. How could blockchain replace traditional Domain Name Service (DNS)?

92. What are "mining puzzles" in Bitcoin?

93. Analyze a real-world case study of a 51% attack (e.g., Ethereum Classic).

94. Who are the key stakeholders in a blockchain ecosystem?

95. How do cryptocurrency exchanges comply with KYC/AML laws?

96. Discuss the impact of Bitcoin on black market economies.

97. What are the tax implications of cryptocurrency trading?

98. How do governments regulate stablecoins?

99. Can blockchain and classical databases coexist? Justify.

100. What is the biggest challenge to mass adoption of blockchain technology?