

## **Phụ lục 1:**

### **CÂU HỎI VÀ BÀI TẬP**

**Lưu ý: Chương mở đầu không có câu hỏi và bài tập**

#### **CÂU HỎI VÀ BÀI TẬP CHƯƠNG 1**

1. Sự khác biệt giữa mã hóa đối xứng và mã hóa bất đối xứng là gì?
2. Liệt kê các thuật toán mã hóa đối xứng và giải thích cách chúng hoạt động?
3. Kể tên các thuật toán mã hóa bất đối xứng và giải thích lý do tại sao chúng thường được sử dụng trong bảo mật thông tin?
4. Chế độ hoạt động của mã hóa khối (block cipher mode) là gì?
5. Khái niệm padding trong mã hóa là gì?
6. Vai trò của khóa phiên (session key) trong mã hóa đối xứng là gì?
7. Hàm băm là gì?
8. Tính chất nào của hàm băm là quan trọng nhất?
9. Hàm băm mật mã khác gì so với hàm băm thông thường?
10. Sự khác biệt giữa mã hóa và hàm băm là gì?
11. Tại sao va chạm hàm băm (hash collision) là một vấn đề trong bảo mật?
12. Chữ ký số hoạt động như thế nào?
13. Sự khác biệt giữa chữ ký số và chữ ký điện tử là gì?
14. Vai trò của hàm băm trong chữ ký số là gì?
15. Các thuật toán phổ biến sử dụng trong chữ ký số là gì?
16. Làm thế nào để xác minh tính hợp lệ của chữ ký số?
17. Chữ ký số giúp ngăn chặn các cuộc tấn công như thế nào?

18. Viết một chương trình để mã hóa và giải mã một thông điệp sử dụng thuật toán AES. Thử nghiệm với các chế độ hoạt động khác nhau như ECB, CBC, và GCM.
19. Viết một chương trình để tạo ra một hệ thống mã hóa lai, trong đó sử dụng mã hóa bất đối xứng để mã hóa khóa phiên (session key) và mã hóa đối xứng để mã hóa thông điệp.
20. Sử dụng thuật toán AES trong chế độ ECB để mã hóa một hình ảnh bitmap. Quan sát kết quả và giải thích lý do tại sao chế độ ECB không nên được sử dụng để mã hóa dữ liệu lớn có cấu trúc như hình ảnh.
21. Viết một chương trình đơn giản để tạo ra một hàm băm dựa trên chuỗi ký tự (ví dụ: sử dụng tổng của mã ASCII). Hãy thử nghiệm với một số chuỗi đầu vào khác nhau
22. Cho một chuỗi băm đã được cho trước (ví dụ: d2d2d2...), hãy tìm một chuỗi đầu vào có thể tạo ra băm này. Hãy thử với các hàm băm phổ biến như MD5, SHA-1, SHA-256 và ghi lại thời gian thực hiện.
23. Hãy thử tìm hai chuỗi khác nhau nhưng tạo ra cùng một giá trị băm sử dụng một hàm băm đơn giản tự viết. So sánh kết quả với các hàm băm mật mã phổ biến như MD5 hay SHA-1.
24. Viết một chương trình để kiểm tra tính toàn vẹn của tệp tin sử dụng hàm băm (ví dụ: SHA-256). Hãy thay đổi một số byte trong tệp tin và quan sát sự thay đổi của giá trị băm.
25. Giải thích tấn công Birthday và viết một chương trình mô phỏng nguyên lý tấn công này trên một hàm băm đơn giản, sau đó thực hiện với một hàm băm như MD5 hoặc SHA-1.
26. Viết một chương trình đơn giản sử dụng thuật toán RSA để tạo chữ ký số cho một chuỗi văn bản và sau đó xác minh chữ ký này. Thử nghiệm với các thư viện mật mã phổ biến như PyCryptodome hoặc OpenSSL.
27. Sử dụng thuật toán ECDSA để tạo và xác minh chữ ký số. So sánh hiệu suất của ECDSA với RSA khi ký cùng một thông điệp.
28. Tải về một chứng chỉ số từ một trang web (ví dụ: thông qua HTTPS) và viết một chương trình để trích xuất khóa công khai từ chứng chỉ này. Sử dụng khóa công khai để xác minh một chữ ký số.

29. Nghiên cứu cách chữ ký số được sử dụng trong các hợp đồng thông minh (smart contract) trên nền tảng blockchain. Viết một hợp đồng thông minh đơn giản có sử dụng chữ ký số để xác minh giao dịch.
30. Thực hiện bài tập thực hành để tạo và xác minh chữ ký số bằng cả RSA và ECDSA, sau đó so sánh về kích thước chữ ký, tốc độ ký, và tốc độ xác minh.

## **CÂU HỎI VÀ BÀI TẬP CHƯƠNG 2**

1. Blockchain là gì? Hãy giải thích ngắn gọn khái niệm này.
2. Nêu các đặc điểm quan trọng của blockchain và giải thích tại sao tính bất biến là yếu tố quan trọng nhất.
3. Thuật toán đồng thuận là gì? So sánh PoW và PoS.
4. Hợp đồng thông minh là gì? Cho một ví dụ về ứng dụng của nó.
5. Mô tả cách các khối (blocks) liên kết với nhau trong blockchain.
6. Ai là người đã phát triển giao thức Paxos, đặt nền móng cho các cơ chế đồng thuận trong mạng máy tính?
  - a. Satoshi Nakamoto
  - b. Leslie Lamport
  - c. Stuart Haber
  - d. David Chaum
7. Năm nào bài báo "Bitcoin: A Peer-to-Peer Electronic Cash System" được xuất bản?
  - a. 1991
  - b. 2008
  - c. 2009
  - d. 2016
8. Đặc điểm nào dưới đây không thuộc tính chất của công nghệ blockchain?
  - a. Sổ cái chỉ cho phép ghi thêm (Ledger)
  - b. Bảo mật bằng mật mã (Secure)
  - c. Tập trung hóa quản lý
  - d. Phân tán và chia sẻ thông tin
9. Ứng dụng blockchain đầu tiên là gì?
  - a. Ethereum
  - b. Bitcoin
  - c. NFT
  - d. Hashcash
10. Blockchain chính thức được giới thiệu với công chúng vào năm nào?
  - a. 1989

- b. 1991
- c. 2009
- d. 2016

11. So sánh sự khác biệt cơ bản giữa blockchain công khai và blockchain riêng tư.
12. Blockchain lai có thể được ứng dụng vào lĩnh vực bất động sản như thế nào? Đưa ra một ví dụ minh họa.
13. Vì sao blockchain liên minh được xem là một giải pháp kết hợp giữa blockchain công khai và riêng tư?
14. Hãy giải thích tại sao việc một tổ chức khởi tạo blockchain công khai ngừng hoạt động không làm ảnh hưởng đến sự vận hành của mạng.
15. Theo bạn, nhược điểm "kém minh bạch" của blockchain liên minh có ảnh hưởng như thế nào đến các ứng dụng trong thực tế?
16. Tiền mã hóa là gì?
17. Tiền mã hóa hoạt động như thế nào?
18. Kể tên một số loại tiền mã hóa phổ biến.
19. Phân biệt tiền mã hóa và tiền fiat.  
Hãy trình bày sự khác biệt giữa tiền mã hóa và tiền fiat, đặc biệt là trong các yếu tố như cơ chế phát hành, kiểm soát và tính thanh khoản.
20. Phân tích cách mà công nghệ blockchain đảm bảo tính bảo mật cho giao dịch tiền mã hóa.  
Hãy giải thích các cơ chế bảo mật mà blockchain sử dụng để bảo vệ các giao dịch tiền mã hóa, bao gồm vai trò của mật mã học, cơ chế đồng thuận, và cấu trúc phân tán.
21. Nghiên cứu các ứng dụng của tiền mã hóa trong các ngành khác nhau.  
Chọn một ứng dụng cụ thể của tiền mã hóa (ví dụ: tài chính phi tập trung - DeFi) và nghiên cứu cách nó ảnh hưởng đến ngành đó. Trình bày một ví dụ thực tế về việc sử dụng tiền mã hóa trong ứng dụng này.
22. Tokenomics là gì?  
Giải thích một cách đơn giản về tokenomics và tầm quan trọng của nó trong hệ sinh thái blockchain.
23. So sánh sự khác biệt giữa kinh tế token (tokenomics) và kinh tế truyền thống?  
Hãy giải thích những điểm khác biệt chính giữa việc sử dụng tiền tệ trong nền kinh tế truyền thống và sử dụng token trong blockchain.
24. Bitcoin có một số đặc điểm quan trọng trong tokenomics. Bạn có thể liệt kê và giải thích các đặc điểm này không?  
Đưa ra các yếu tố chính trong tokenomics của Bitcoin và cách chúng ảnh hưởng đến giá trị của Bitcoin.

- 25.** Lý do tại sao việc dự đoán số lượng token đang lưu hành là quan trọng trong các dự án blockchain?  
Phân tích tầm quan trọng của việc kiểm soát số lượng token và kế hoạch phân phối token trong các dự án tiền mã hóa.
- 26.** NFT là gì?  
Giải thích khái niệm NFT và sự khác biệt giữa NFT và các tài sản có thể thay thế như tiền điện tử.
- 27.** Tại sao NFT lại quan trọng đối với nghệ sĩ và người sáng tạo nội dung?  
Hãy giải thích tầm quan trọng của NFT đối với nghệ sĩ và người sáng tạo nội dung trong việc xác thực quyền sở hữu và tạo ra giá trị cho các tác phẩm kỹ thuật số.
- 28.** NFT không thể chia nhỏ, tại sao lại có một số nền tảng giới thiệu quyền sở hữu một phần?  
Phân tích lý do tại sao việc chia nhỏ NFT thành các phần nhỏ hơn lại trở thành xu hướng mới, và nền tảng Fractional đã giúp gì cho thị trường NFT.
- 29.** Hãy nêu ví dụ về một dự án NFT trên nền tảng Cardano và cách nó đã phát triển hệ sinh thái NFT trên Cardano.  
Giới thiệu về dự án NFT đầu tiên trên nền tảng Cardano và những tác động của nó đối với sự phát triển của hệ sinh thái NFT trên Cardano.
- 30.** NFT phụ thuộc vào yếu tố nào để giá trị của chúng tăng theo thời gian?  
Phân tích yếu tố cung và cầu ảnh hưởng như thế nào đến giá trị của NFT trong thị trường đầu tư.
- 31.** NFT là gì?  
Giải thích khái niệm NFT và sự khác biệt giữa NFT và các tài sản có thể thay thế như tiền điện tử.
- 32.** Tại sao NFT lại quan trọng đối với nghệ sĩ và người sáng tạo nội dung?  
Hãy giải thích tầm quan trọng của NFT đối với nghệ sĩ và người sáng tạo nội dung trong việc xác thực quyền sở hữu và tạo ra giá trị cho các tác phẩm kỹ thuật số.
- 33.** NFT không thể chia nhỏ, tại sao lại có một số nền tảng giới thiệu quyền sở hữu một phần?  
Phân tích lý do tại sao việc chia nhỏ NFT thành các phần nhỏ hơn lại trở thành xu hướng mới, và nền tảng Fractional đã giúp gì cho thị trường NFT.
- 34.** Hãy nêu ví dụ về một dự án NFT trên nền tảng Cardano và cách nó đã phát triển hệ sinh thái NFT trên Cardano.  
Giới thiệu về dự án NFT đầu tiên trên nền tảng Cardano và những tác động của nó đối với sự phát triển của hệ sinh thái NFT trên Cardano.
- 35.** NFT phụ thuộc vào yếu tố nào để giá trị của chúng tăng theo thời gian?  
Phân tích yếu tố cung và cầu ảnh hưởng như thế nào đến giá trị của NFT trong thị trường đầu tư.

36. Thách thức lớn nhất của NFT trong thị trường hiện tại là gì? a) Tính bất ổn của thị trường  
b) Tính bảo mật của blockchain  
c) Giá trị nghệ thuật của NFT  
d) Khả năng xác thực danh tính
37. Tại sao phí giao dịch cao lại là một thách thức lớn đối với người dùng NFT? a) Phí giao dịch cao chỉ ảnh hưởng đến người bán  
b) Phí giao dịch làm giảm lợi nhuận từ việc đầu tư vào NFT  
c) Phí giao dịch làm giảm sự tham gia của người tiêu dùng và tạo ra rào cản đầu vào  
d) Phí giao dịch không ảnh hưởng đến sự phát triển của NFT
38. NFT có thể giúp nghệ sĩ trong việc bảo vệ bản quyền của tác phẩm như thế nào? a) Bằng cách cho phép nghệ sĩ sao chép tác phẩm của mình dưới dạng NFT  
b) Bằng cách giúp nghệ sĩ nhận doanh thu trực tiếp từ việc bán NFT  
c) Bằng cách cho phép nghệ sĩ bán tác phẩm qua các công ty lớn  
d) Bằng cách giảm giá trị tác phẩm nghệ thuật gốc
39. Ví trong blockchain là gì? Giải thích tầm quan trọng của ví đối với người dùng tiền mã hóa.
40. Phân biệt các loại ví phần mềm, ví cứng, ví trực tuyến và ví giấy. Nêu ưu nhược điểm của từng loại ví.
41. Khóa công khai và khóa riêng trong ví có vai trò như thế nào trong việc bảo mật tài sản kỹ thuật số?
42. Ví tiền mã hóa có ảnh hưởng gì đến việc giao dịch và quản lý tài sản số như tiền mã hóa hoặc NFT?
43. Hãy giải thích nguyên lý hoạt động của ví trong thế giới blockchain, đặc biệt trong việc ký giao dịch và bảo mật tài sản.
44. Liệt kê các biện pháp bảo mật mà ví sử dụng để bảo vệ tài sản của người dùng.
45. Những vấn đề bảo mật và rủi ro phổ biến mà người dùng ví cần lưu ý khi sử dụng ví kỹ thuật số?
46. Tại sao địa chỉ trên blockchain lại quan trọng đối với giao dịch tiền mã hóa?
47. Hợp đồng thông minh có thể sử dụng địa chỉ ví blockchain như thế nào để tự động thực hiện các hành động?
48. Trong hệ sinh thái NFT, địa chỉ ví có vai trò gì trong việc chuyển nhượng tài sản?
49. Làm thế nào blockchain có thể giúp quản lý và lưu trữ các tài sản kỹ thuật số ngoài tiền mã hóa?

50. Ứng dụng của địa chỉ trên blockchain trong các DApp là gì và nó mang lại lợi ích gì cho người dùng?
51. Những ứng dụng nào có thể sử dụng blockchain để quản lý danh tính cá nhân và bảo vệ quyền riêng tư?
52. Microtransactions trên blockchain được thực hiện như thế nào và tại sao chúng lại có chi phí thấp?
53. Chức năng của địa chỉ ví blockchain trong việc tạo và quản lý thẻ quà tặng là gì?
54. Sổ cái trong blockchain khác với sổ cái truyền thống như thế nào?
55. Tại sao blockchain không cần một tổ chức trung gian để duy trì sổ cái?
56. Giải thích khái niệm "immutability" trong blockchain và tại sao nó quan trọng đối với tính bảo mật của giao dịch?
57. Những đặc điểm nào của sổ cái blockchain giúp tăng cường tính minh bạch và bảo mật?
58. Cơ chế đồng thuận như Proof of Work (PoW) hoặc Proof of Stake (PoS) hoạt động như thế nào trong việc xác nhận các giao dịch trên blockchain?
59. Mô tả quy trình ghi nhận và xác thực giao dịch trong blockchain.
60. Blockchain sử dụng mã hóa bất đối xứng để bảo vệ giao dịch như thế nào?
61. Tại sao việc không thể thay đổi dữ liệu trong blockchain lại giúp bảo vệ khỏi gian lận?
62. Giải thích các lợi ích mà sổ cái blockchain mang lại cho các ứng dụng tài chính và phi tài chính.

### **CÂU HỎI VÀ BÀI TẬP CHƯƠNG 3**

1. Bitcoin được tạo ra bởi ai, và mục tiêu ban đầu của nó là gì?
2. Giao dịch Bitcoin được xác thực và thêm vào blockchain như thế nào?
3. Điều gì trong bảo mật giao dịch Bitcoin?
4. Địa chỉ Bitcoin được tạo ra như thế nào từ khóa công khai?
5. Ví Bitcoin là gì, và có những loại ví nào? Ưu và nhược điểm của từng loại?
6. Vai trò của các node và thợ đào trong mạng lưới Bitcoin là gì? gì đảm bảo rằng giao dịch Bitcoin là không thể thay đổi và minh bạch?
7. Sự khác biệt giữa khóa công khai và khóa bí mật là gì? Vai trò của chúng

8. Bitcoin đã thay đổi cách chúng ta nhìn nhận tiền tệ và giao dịch tài chính như thế nào?
9. Những thách thức chính mà Bitcoin phải đối mặt là gì? (ví dụ: tiêu thụ năng lượng, khả năng mở rộng)
10. Bitcoin khác biệt như thế nào so với các hệ thống tài chính truyền thống về tính minh bạch, bảo mật, và phân quyền?
11. Cardano ra đời trong bối cảnh nào, và những vấn đề nào của blockchain thế hệ trước mà nó muốn giải quyết?
12. Giai đoạn khởi động (2015-2017) của Cardano đã đạt được những cột mốc quan trọng nào?
13. Lộ trình phát triển của Cardano được chia thành những giai đoạn nào, và mục tiêu chính của mỗi giai đoạn là gì?
14. Tầm nhìn tương lai của Cardano là gì, và nó có tác động như thế nào đến hệ sinh thái blockchain?
15. Kiến trúc của Blockchain Cardano được chia thành những lớp nào, và vai trò của từng lớp là gì?
16. Cơ chế đồng thuận Ouroboros của Cardano hoạt động như thế nào để đảm bảo tính bảo mật và phân quyền?
17. Mô hình UTxO khác biệt như thế nào so với mô hình dựa trên tài khoản?
18. Lợi ích chính của mô hình EUTxO của Cardano là gì, và tại sao nó phù hợp cho hợp đồng thông minh?
19. Các thành phần cơ bản của EUTxO bao gồm những gì, và vai trò của chúng trong giao dịch?
20. Khóa trong Cardano được sử dụng như thế nào để đảm bảo tính bảo mật và xác thực giao dịch?
21. Địa chỉ thanh toán và địa chỉ stake khác nhau như thế nào, và vai trò của chúng trong hệ sinh thái Cardano?
22. Hợp đồng thông minh trên Cardano hoạt động như thế nào trong mô hình EUTxO?



23. Những điểm khác biệt chính giữa hợp đồng thông minh trên Cardano và các blockchain khác là gì?
24. Các vai trò chính trong quản trị On-Chain của Cardano là gì, và mỗi vai trò có trách nhiệm gì?
25. Quy trình ra quyết định trong quản trị On-Chain của Cardano diễn ra như thế nào?
26. Các loại hành động quản trị trên Cardano bao gồm những gì, và mỗi loại có mục đích gì?

#### **CÂU HỎI VÀ BÀI TẬP CHƯƠNG 4**

- 1 Thuật toán đồng thuận blockchain là gì, và vai trò của nó trong việc duy trì tính an toàn và ổn định của hệ thống phân tán?
- 2 Nêu các bước chính trong cơ chế hoạt động của một thuật toán đồng thuận blockchain.
- 3 Tại sao tính phi tập trung (decentralization) lại là yêu cầu quan trọng đối với một thuật toán đồng thuận?
- 4 Mô tả bài toán các vị tướng Byzantine và sự liên quan của nó đến hệ thống chịu lỗi Byzantine (BFT).
- 5 So sánh các ưu, nhược điểm của thuật toán Proof of Work (PoW) và Proof of Stake (PoS).
- 6 Giải thích cách hoạt động của thuật toán Proof of History (PoH) trong mạng Solana và vai trò của nó trong việc tăng tốc độ xử lý giao dịch.
- 7 Thuật toán Proof of Authority (PoA) hoạt động như thế nào, và tại sao nó phù hợp với các mạng blockchain riêng tư (private blockchain)?
- 8 Mô tả cơ chế chọn Slot Leader trong thuật toán Ouroboros của Cardano.
- 9 Thuật toán Proof of Capacity (PoC) giúp giảm tiêu thụ năng lượng như thế nào, và nó khác gì so với PoW?
- 10 Bằng chứng ủy quyền cổ phần (DPoS) giải quyết vấn đề tập trung hóa như thế nào so với PoS?

- 11 Hãy giải thích cách hệ thống chịu lỗi Byzantine (BFT) đảm bảo tính ổn định của mạng lưới blockchain ngay cả khi một số nút không trung thực.
- 12 Một thợ đào sử dụng thuật toán PoC có 5 TB dung lượng lưu trữ, trong khi người khác có 10 TB. Tính xác suất tương đối của mỗi người trong việc tạo khối mới.
- 13 Lập bảng so sánh ưu, nhược điểm của PoW, PoS và PoC. Đề xuất tình huống ứng dụng phù hợp cho từng thuật toán.
- 14 Mô phỏng cách tạo và xác thực khối bằng thuật toán PoW. Mô tả các bước từ tạo khối ứng viên đến xác nhận khối hợp lệ.
- 15 Nếu bạn phải xây dựng một blockchain cho một ứng dụng tài chính với yêu cầu cao về tốc độ và bảo mật, bạn sẽ chọn thuật toán nào trong số PoW, PoS, PoH hoặc PoA? Giải thích lý do.

### **CÂU HỎI VÀ BÀI TẬP CHƯƠNG 5**

1. Phân tích các thách thức chính về khả năng mở rộng của blockchain và đề xuất giải pháp khắc phục.
2. Tại sao vấn đề tiêu thụ năng lượng lại là một thách thức lớn đối với blockchain? Các giải pháp nào đang được phát triển để giải quyết vấn đề này?
3. So sánh các thách thức về mặt kỹ thuật và thách thức về mặt quản trị trong việc triển khai blockchain.
4. Thảo luận về vai trò của khung pháp lý trong việc phát triển và ứng dụng công nghệ blockchain.
5. Đánh giá tác động của các thách thức xã hội đối với việc chấp nhận và áp dụng rộng rãi công nghệ blockchain.