Chương 1
Mật mã và tiền mã hóa

Mục tiêu bài học

- Hiểu được khái niệm cơ bản về mật mã học và vai trò của nó trong việc bảo mật dữ liệu.
- Hiểu được cấu trúc dữ liệu của block trong Blockchain
- Hiểu được hoạt động của các hàm băm (hash function) và cây Merkle (Merkle Tree)
- Tầm quan trọng của con trỏ băm (hash pointer) trong việc tạo tính bất biến và bảo mật dữ liệu
- Vai trò của chữ ký số trong Blockchain

Nội dung bài học

- Giới thiệu về mật mã học và tiền mã hóa
- Cấu trúc của một Block
- Bên trong một Block là gì?
- Hàm băm và Merkle Tree
- Các thuật toán băm
- Con trỏ băm
- Mã hóa khóa công khai, chữ ký số

Mật mã học (Cryptography)

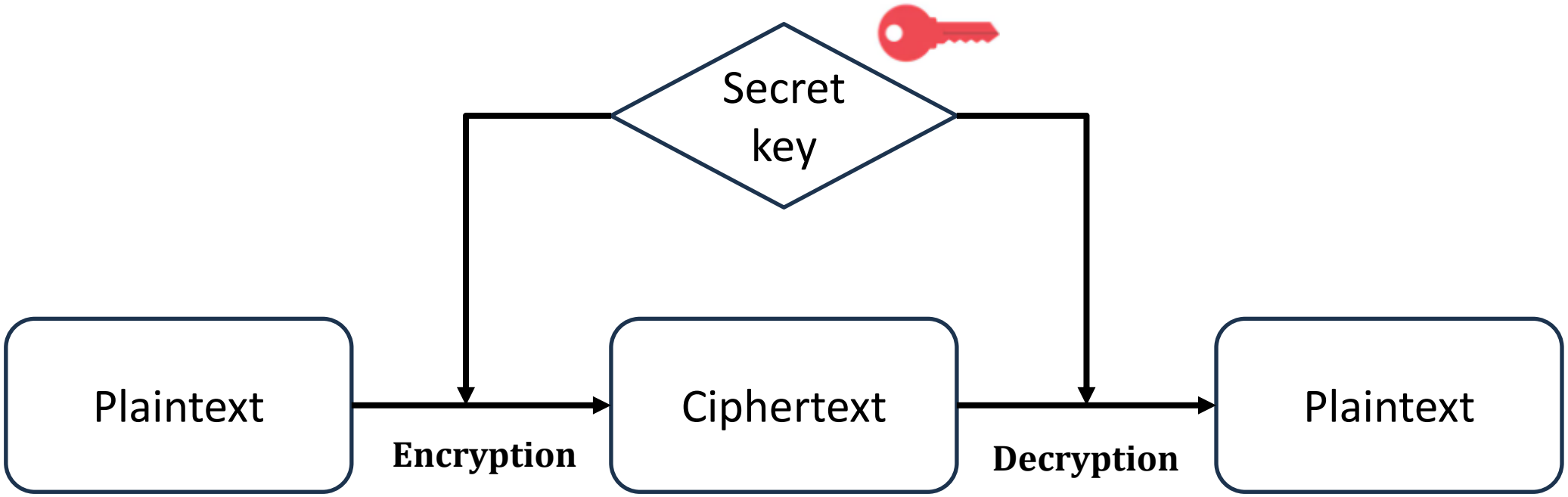
Mật mã học (Cryptography) là giải pháp bảo mật dữ liệu và thông tin giao dịch của người gửi và người nhận, thông qua các kỹ thuật mã hóa và giải mã.

<u>Đảm bảo những tính chất sau cho thông tin:</u>

- **Bảo mật (Confidentiality)**: thông tin chỉ được tiết lộ cho những ai được phép
- **Xác thực (Authentication)**: người gửi (hoặc người nhận) có thể chứng minh đúng là họ
- **Toàn vẹn dữ liệu (Data Integrity)**: thông tin không thể bị thay đổi mà không bị phát hiện
- **Không phủ nhận (Non-repudiation)**: người gửi hoặc nhận sau này không thể chối bỏ việc đã gửi hoặc nhận thông tin.

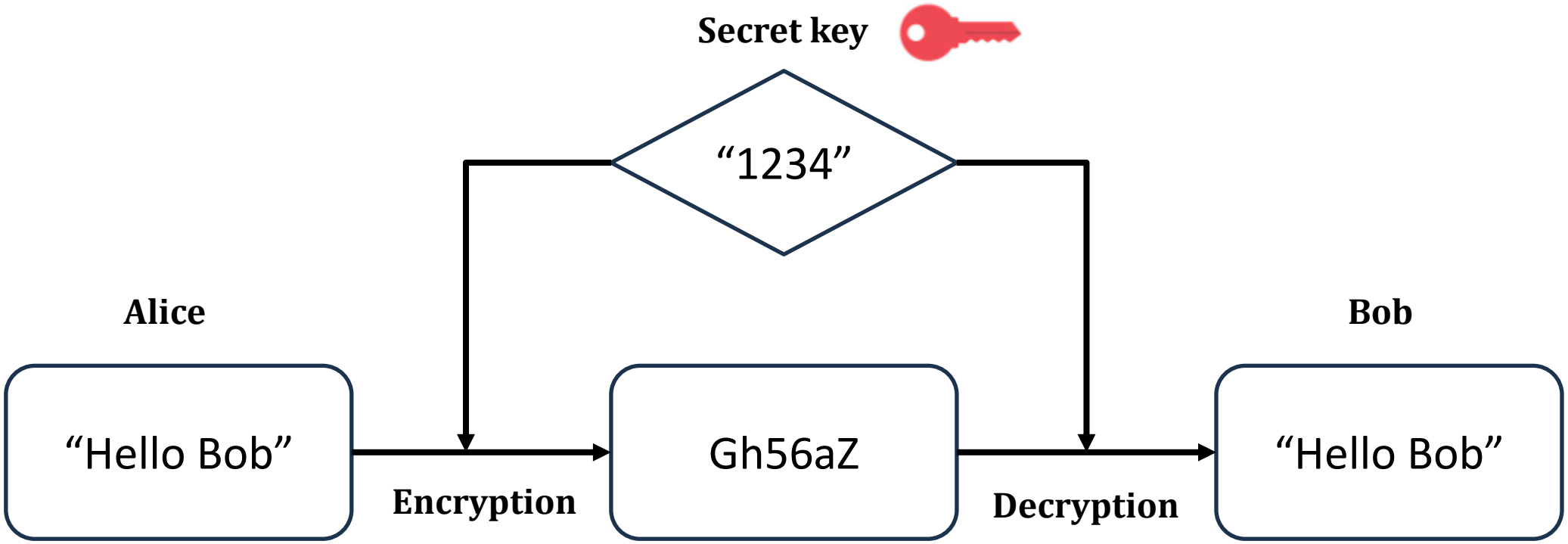
Các loại mã hóa (Encryption)

Mã hóa đối xứng (Symmetric Encryption): Sử dụng một khóa cho cả quá trình mã hóa và giải mã.



Các loại mã hóa (Encryption)

Ví dụ: Alice gởi tin nhắn cho Bob

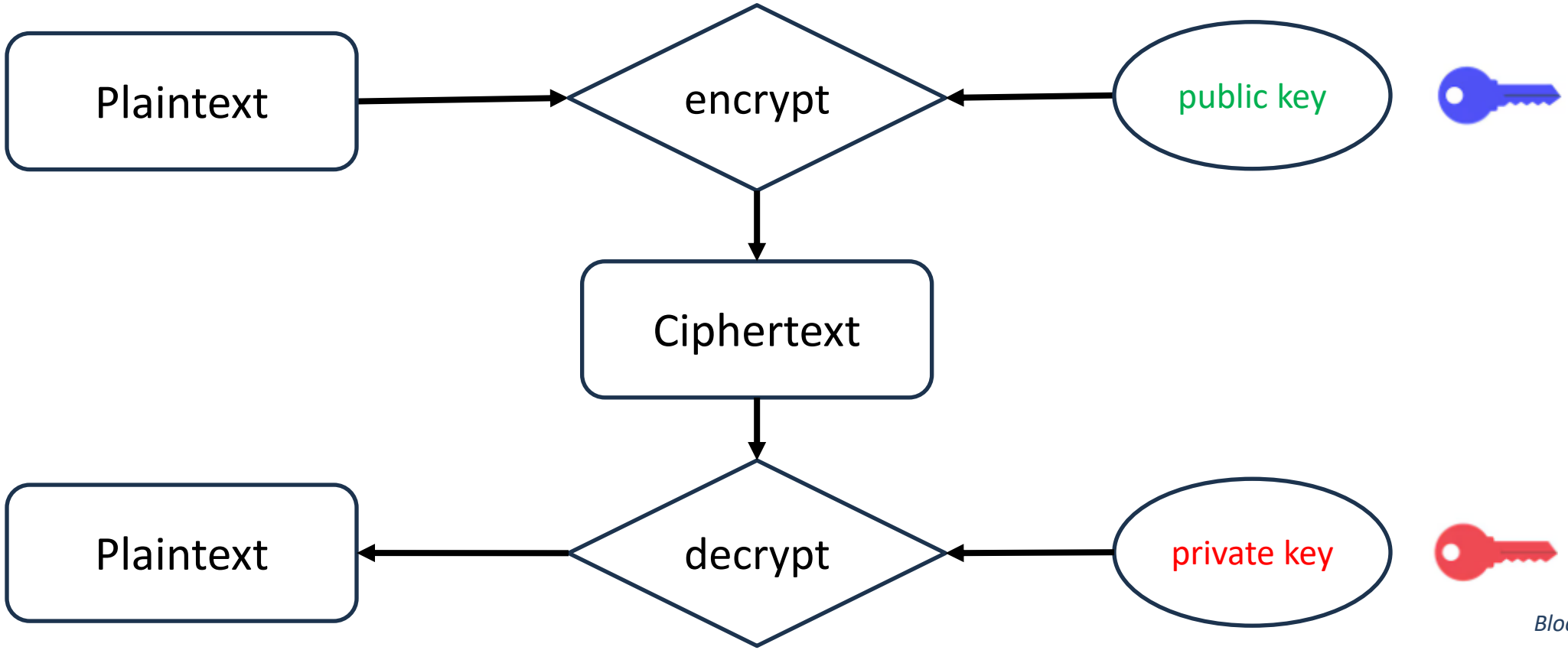


Symmetric Encryption

Các loại mã hóa (Encryption)

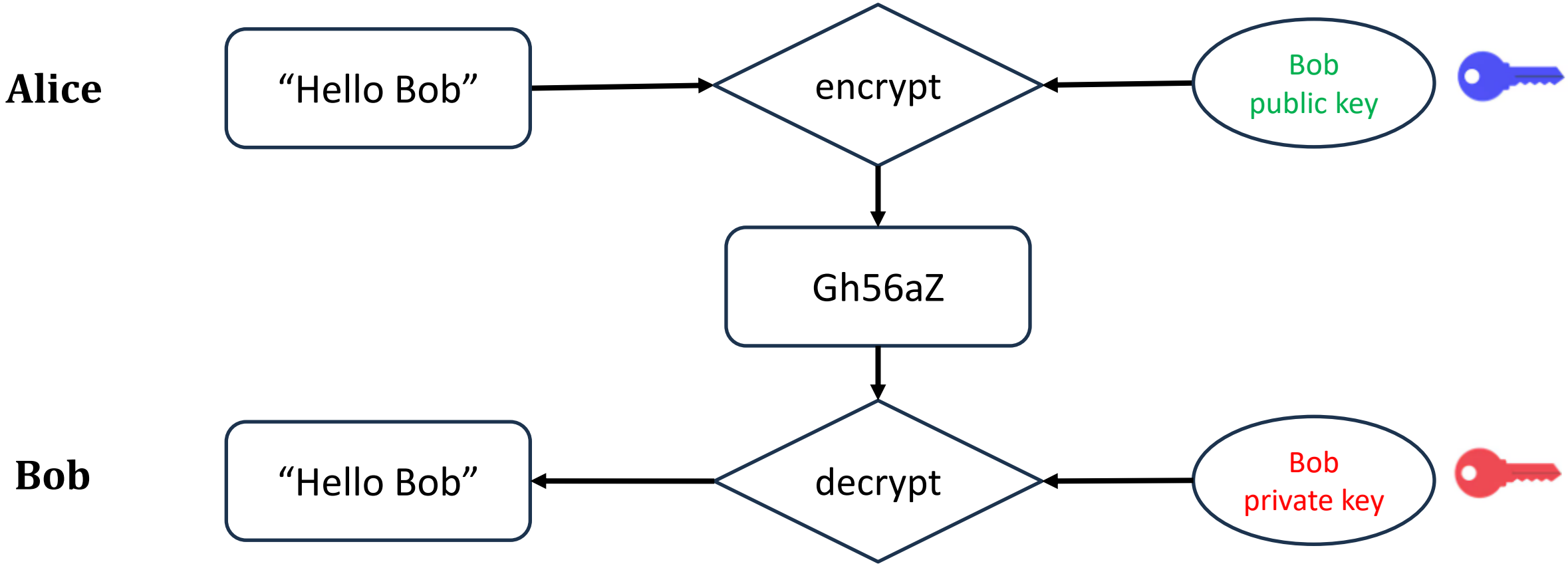
Mã hóa bất đối xứng (Asymmetric Encryption): Sử dụng hai khóa

- **Khóa công khai (Public Key)**: Mã hóa dữ liệu
- **Khóa riêng tư (Private Key)**: Giải mã dữ liệu.



Các loại mã hóa (Encryption)

Ví dụ: Alice gởi tin nhắn cho Bob

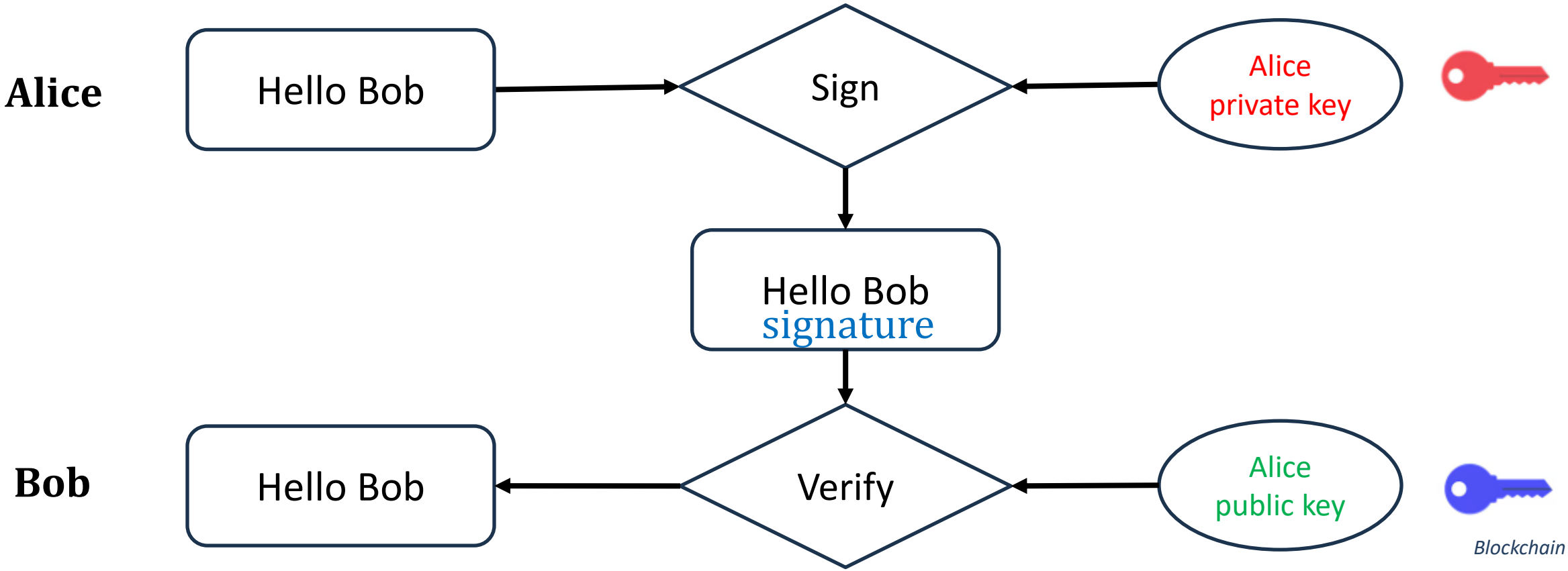


Asymmetric Encryption

Các loại mã hóa (Encryption)

Chữ ký số (Digital Signature): Ngược lại với mã hóa bất đối xứng

- Người gửi sử dụng khóa riêng tư để ký vào thông điệp
- Người nhận xác minh bằng khóa công khai



Tiền mã hóa (Cryptocurrency)

Tiền mã hóa (Cryptocurrency) là một dạng của tiền điện tử hoặc tiền kỹ thuật số là một tài sản kỹ thuật số sử dụng mật mã để bảo mật.

Đặc điểm của tiền mã hóa:

- Phi tập trung (Decentralized): Không có cơ quan trung ương kiểm soát, các nút (nodes) xác thực giao dịch
- Bảo mật cao: Giao dịch được bảo vệ bởi thuật toán băm và chữ ký số, dữ liệu không thể thay đổi
- Tính minh bạch: Lịch sử giao dịch được lưu trữ công khai trên Blockchain
- Không thể làm giả: Việc tạo ra tiền mới tuân theo các quy tắc mã hóa nghiêm ngặt

Tiền mã hóa (Cryptocurrency)

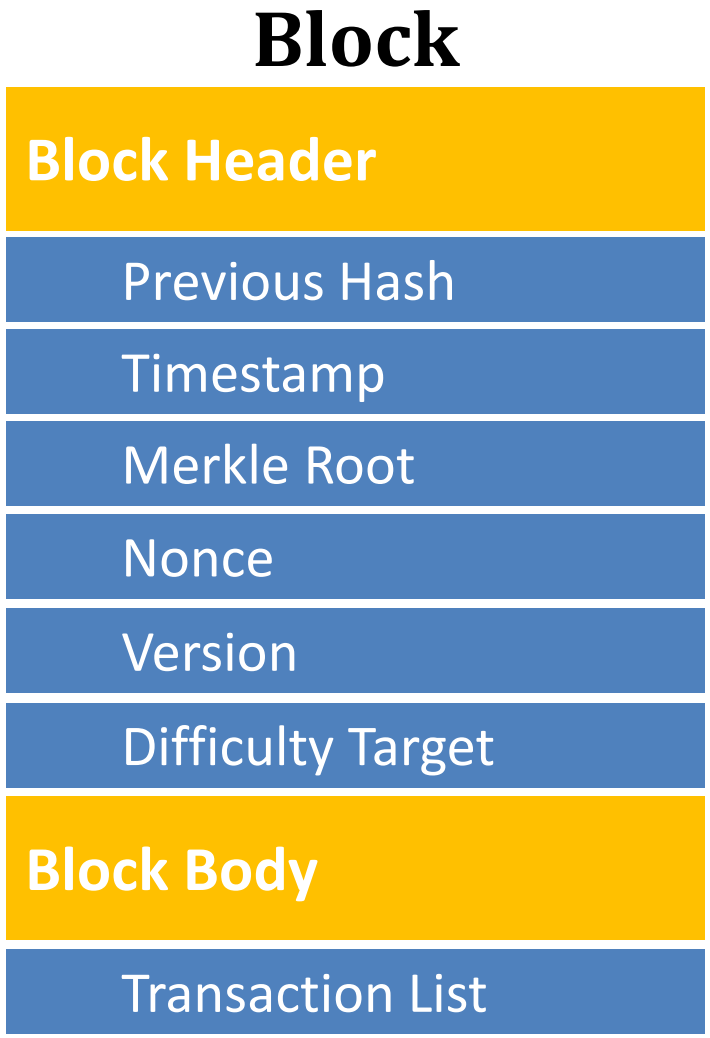
Ví dụ: một số đồng tiền mã hóa nổi bật

- **Bitcoin (BTC):** Đồng tiền mã hóa đầu tiên và có vốn hóa thị trường lớn nhất.

- **Ethereum (ETH):** Nền tảng cho phép triển khai hợp đồng thông minh và ứng dụng phi tập trung.

https://www.binance.com/

Cấu trúc của một Block



Header chứa các thông tin dùng để xác định và liên kết với các khối khác:

- Previous hash: Lưu trữ mã băm của khối trước đó
- Timestamp: Thời điểm khối được tạo ra
- Merkle Root: Là giá trị hash duy nhất đại diện cho toàn bộ transaction List
- Nonce: Sử dụng trong Proof of Work (PoW)
- Version: Phiên bản của giao thức Blockchain
- Difficulty Target: Độ khó giải bài toán

Body chứa dữ liệu chính của khối bao gồm danh sách giao dịch (Transaction List)

Cấu trúc của một Block

Ví dụ:

Block

Block Header

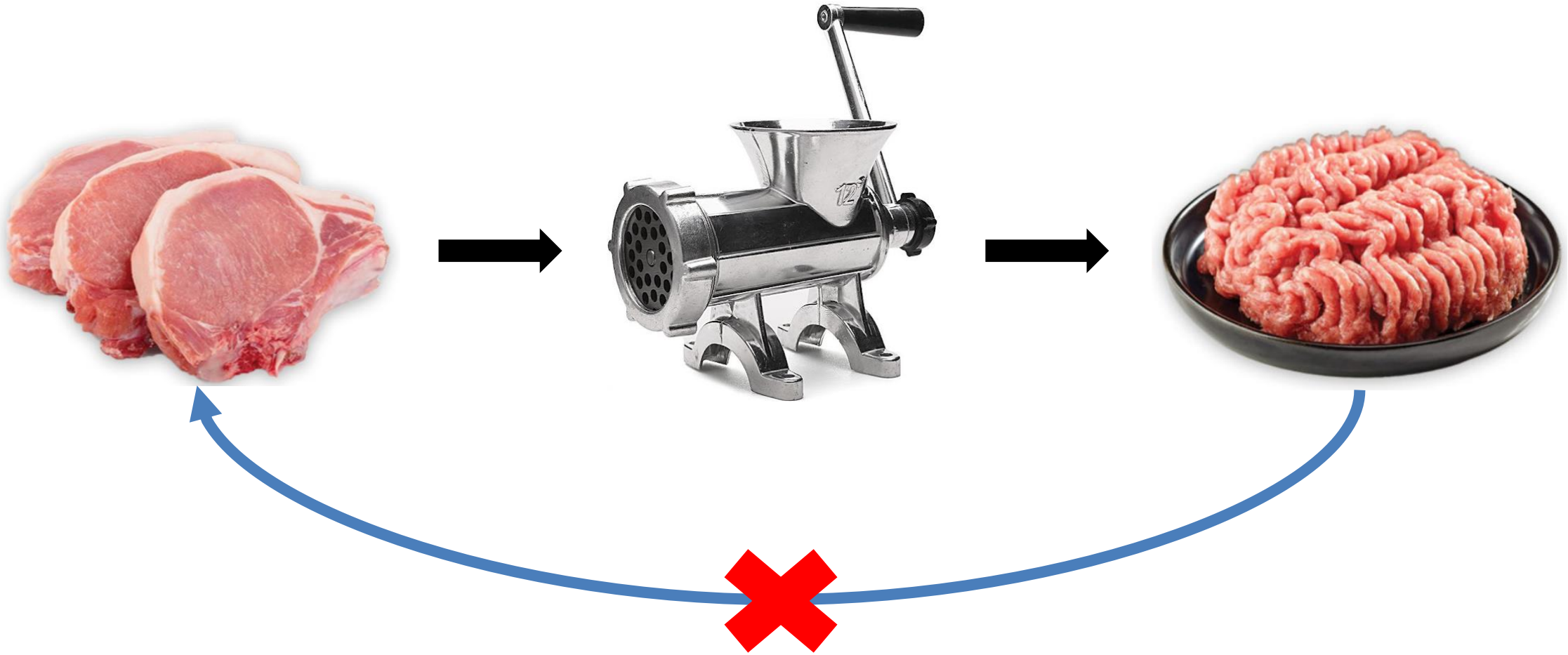
- Previous Hash: abc123...
- Timestamp: 2024-12-01T12:00:00
- Merkle Root: def456...
- Nonce: 789
- Version: 1.0
- Difficulty Target: 0000ffff...

Block Body

- Transaction 1: Alice gửi 10 BTC cho Bob
- Transaction 2: Bob gửi 5 BTC cho Charlie
- Transaction 3: Charlie gửi David 2 USD

Băm (hash)?

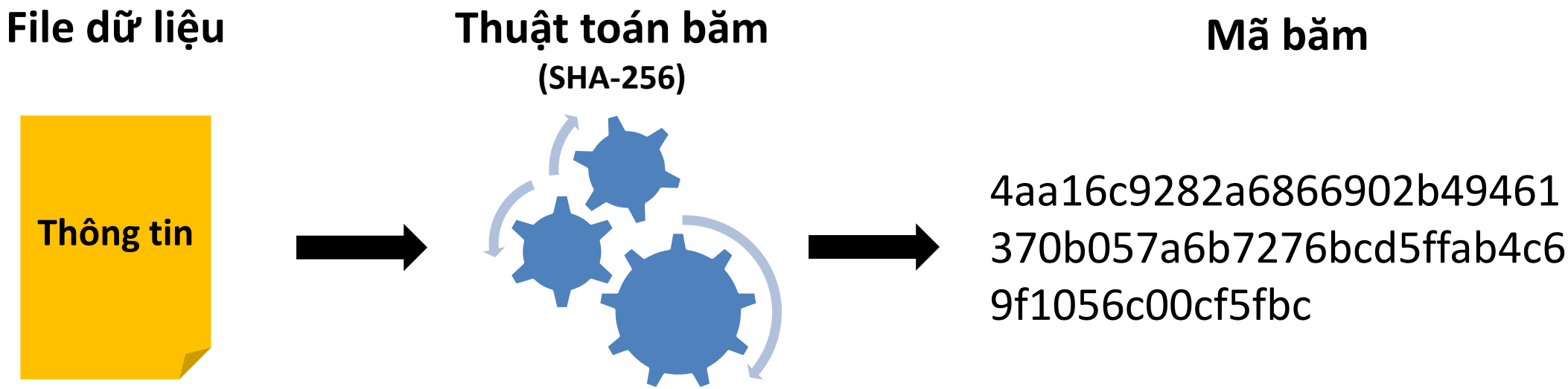
Băm là kết quả đầu ra của một quá trình chuyển đổi dữ liệu đầu vào (input) thành một chuỗi ký tự cố định (hash value) thông qua **hàm băm**.



Hàm băm (Function hash)?

Hàm băm là một thuật toán toán học, nhận dữ liệu đầu vào có kích thước bất kỳ và tạo ra một mã băm đầu ra cố định.

- **Một chiều**: Không thể giải ngược từ mã băm để tìm lại dữ liệu gốc.
- **Đầu ra cố định**: Bất kể kích thước đầu vào, mã băm đầu ra luôn có độ dài cố định.
- **Kháng xung đột**: Hai dữ liệu khác nhau gần như không bao giờ tạo ra cùng một mã băm.



Hàm băm (Function hash)?

Ví dụ: Hàm băm (SHA-256)

"Xin chào" → 117ae605a3a02bf47978fba60ef2bf4a08a73eb34b0124d9a1a088c8cab6d9de

"Xin,chào" → aa84ec72aaff7a7d2606c697f2800292234da529f1621c38be90af63201bfc26

Các thuật toán băm

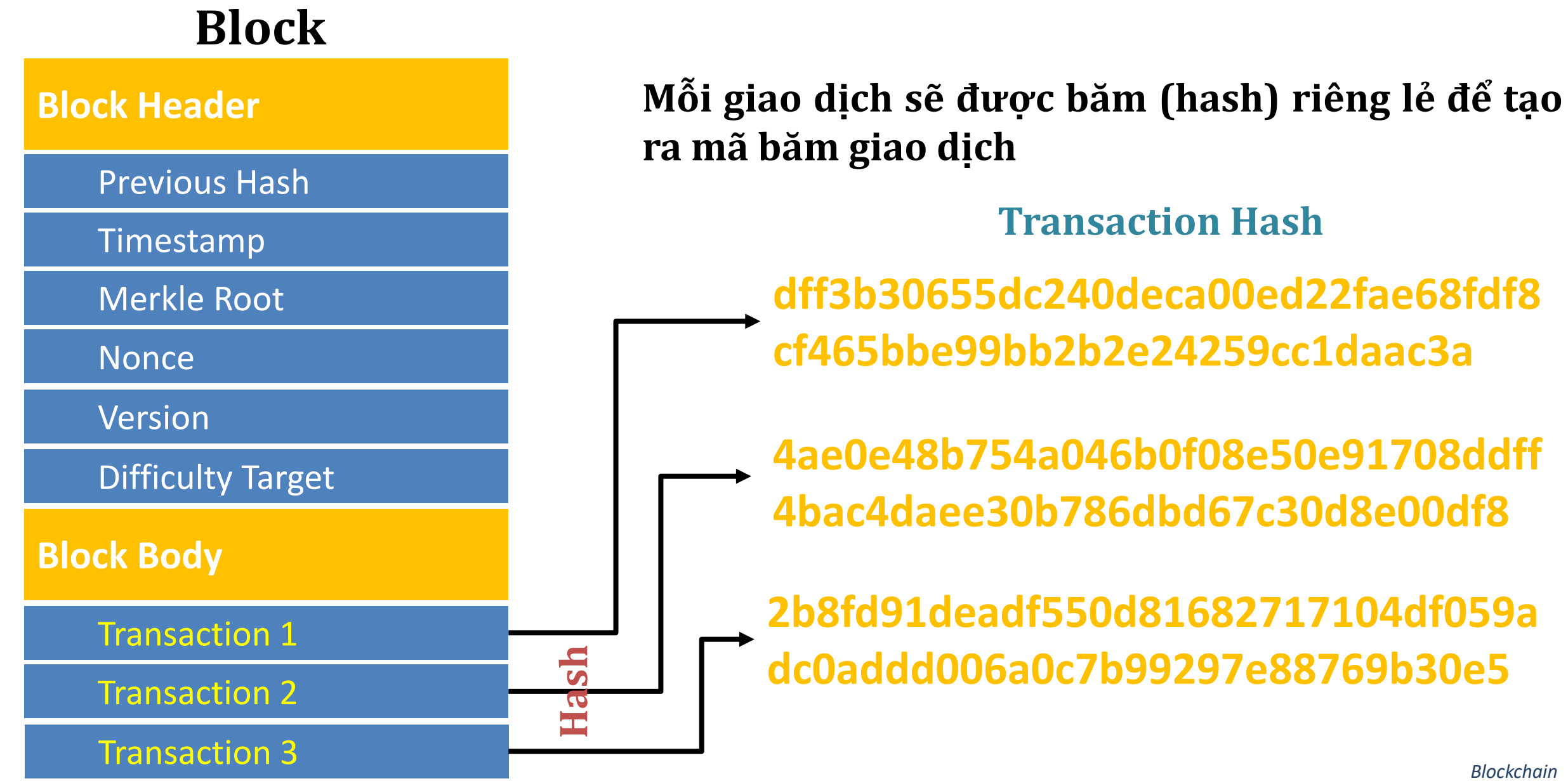
MD5
128 bit
Độ dài chuỗi: 32
Kém an toàn

Dễ xung đột

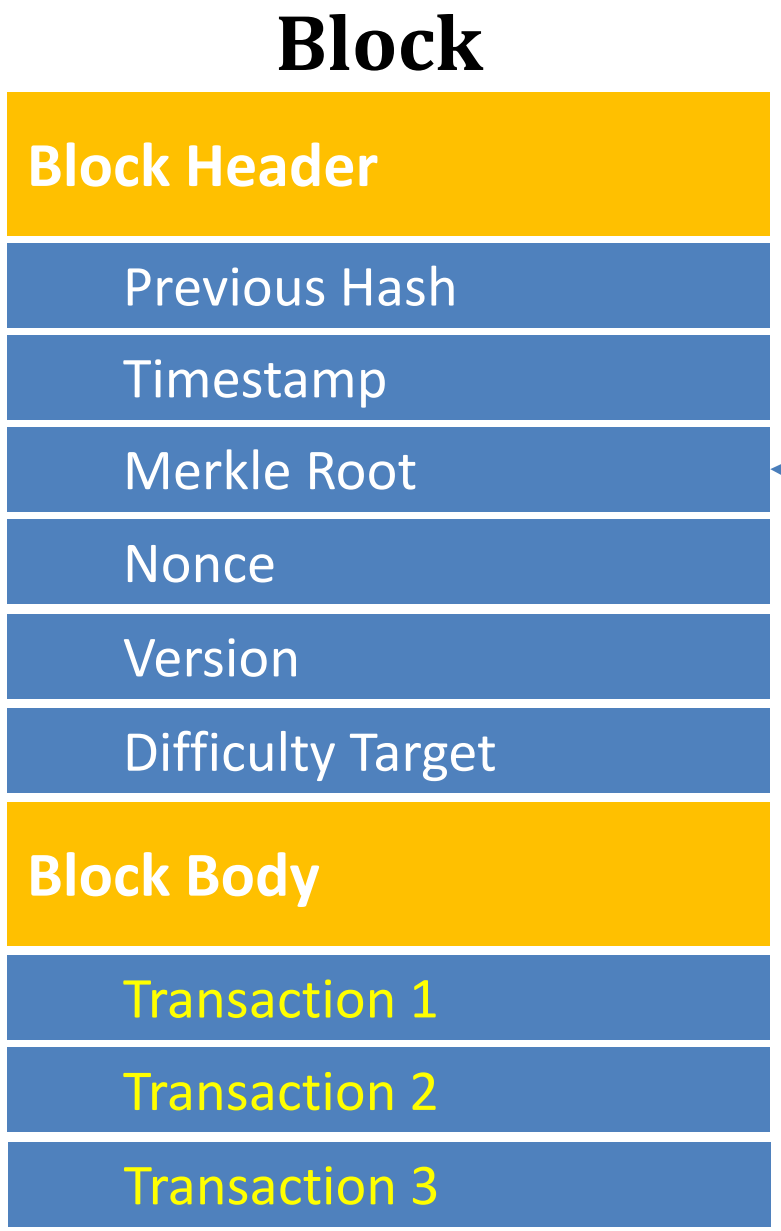
SHA-256
256 bit
Độ dài chuỗi: 64
An toàn cao

Mạng blockchain Bitcoin

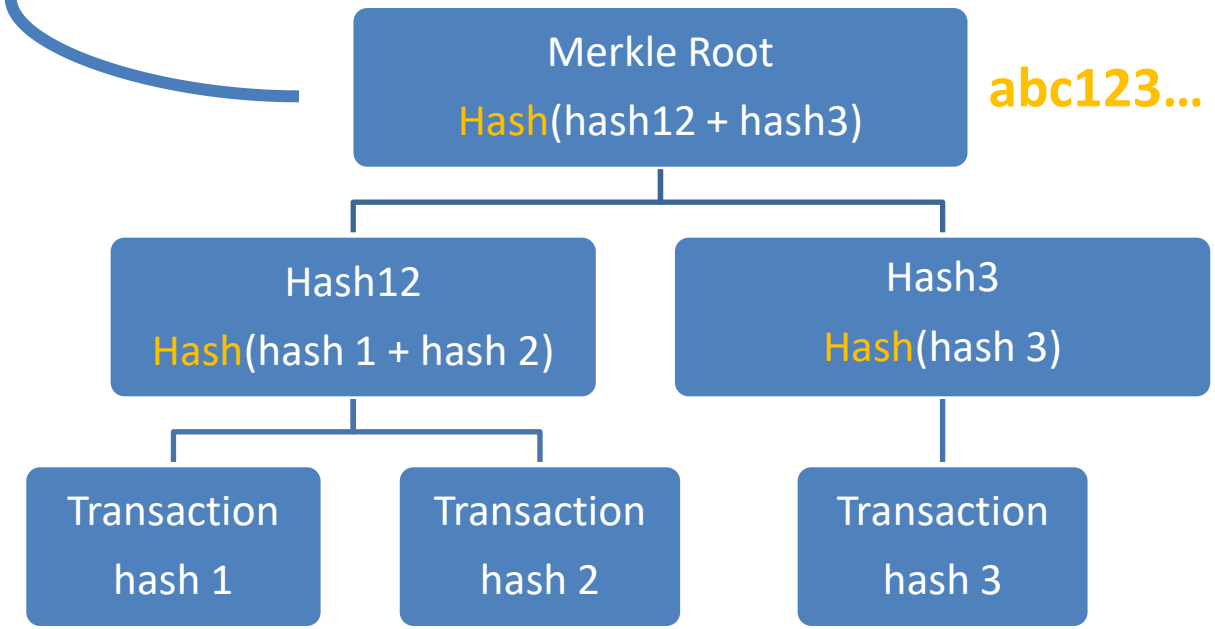
Bên trong một Block được mã hóa như thế nào?



Bên trong một Block được mã hóa như thế nào?



- Mã băm của từng giao dịch trong Body được tổ chức thành một cấu trúc cây nhị phân gọi là **Merkle Tree**
- **Merkle Root** được lưu trong Header, là mã băm cuối cùng đại diện cho toàn bộ giao dịch trong khối.



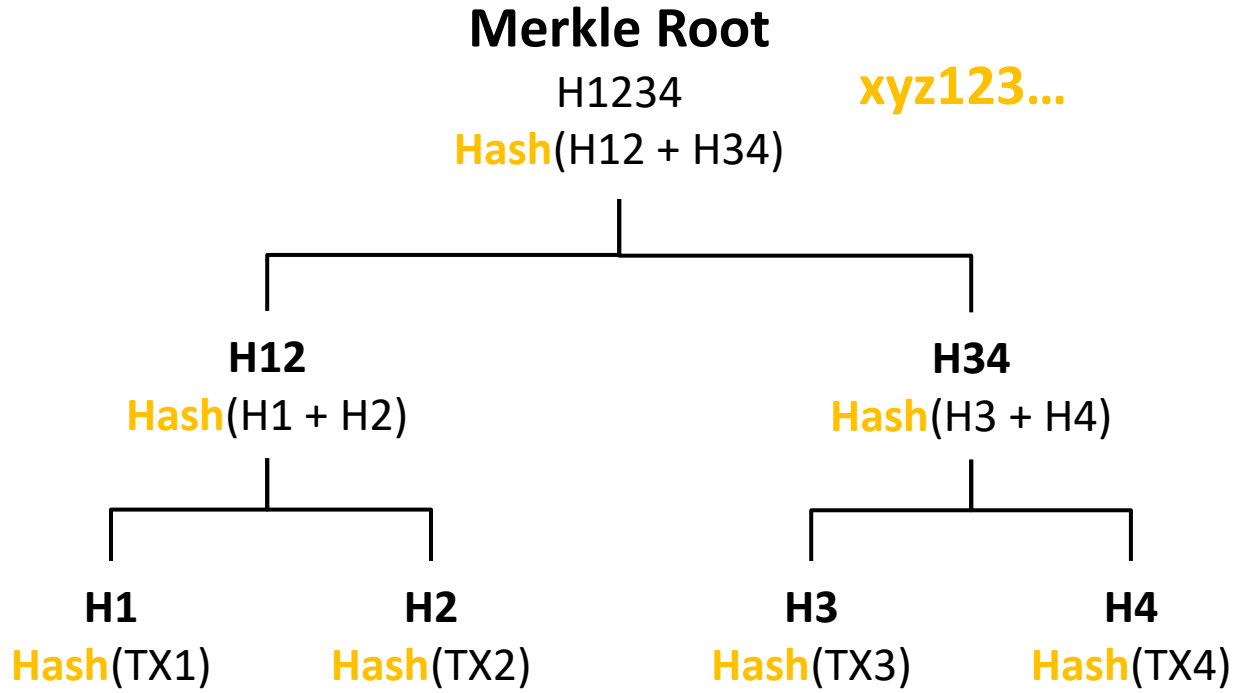
Cách tổ chức cây Merkle Tree

Cấu trúc cây Merkle:

- Mỗi giao dịch trong Block Body được băm thành một **mã băm giao dịch** (Transaction Hash).
- Các mã băm giao dịch này được kết hợp theo cặp, sau đó băm lại để tạo **nút cha**.
- Quá trình này tiếp tục đến khi chỉ còn một giá trị duy nhất ở gốc cây (Merkle Root).

Ví dụ: Giả sử Block Body có 4 giao dịch

ID Giao dịch	Transaction Hash
101	Hash(TX1) = abc123
102	Hash(TX2) = def456
103	Hash(TX3) = ghi789
104	Hash(TX4) = jkl012



Bên trong một Block được mã hóa như thế nào?

Mã hóa của cả khối (Block Hash) được tạo ra như thế nào?

Bên trong một Block được mã hóa như thế nào?

Block

- **Block Header**
  - Previous Hash
  - Timestamp
  - Merkle Root
  - Nonce
  - Version
  - Difficulty Target
- **Block Body**
  - Transaction 1
  - Transaction 2
  - Transaction 3

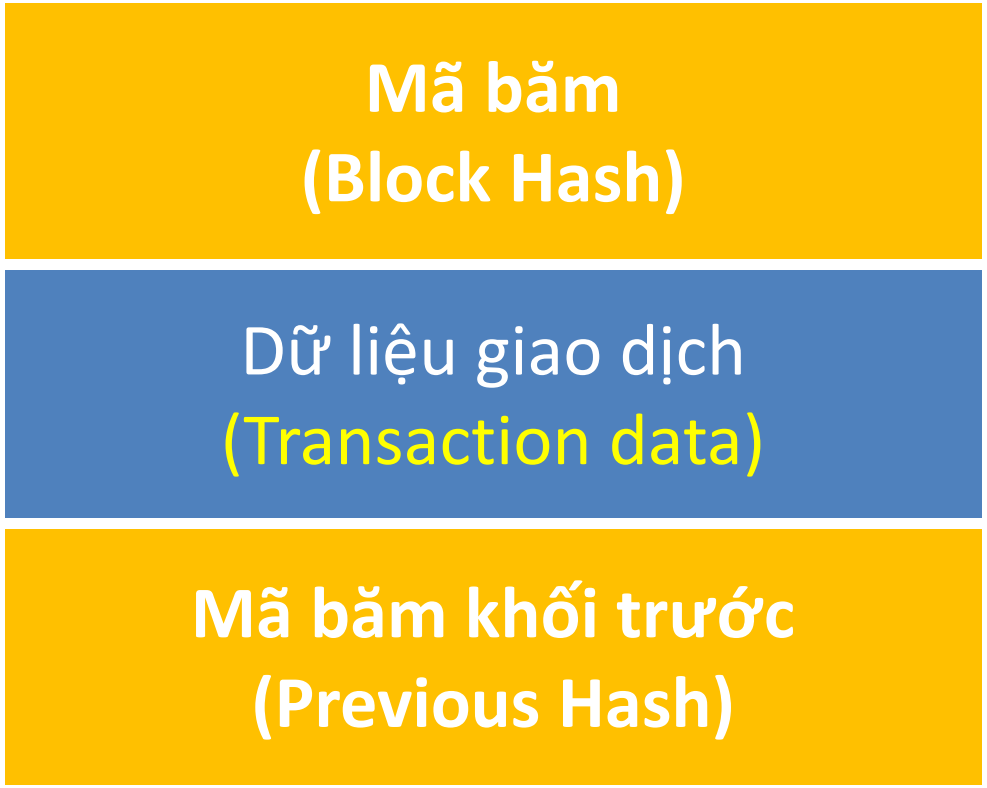
Block Hash là mã băm duy nhất đại diện cho toàn bộ khối, được tính toán từ dữ liệu trong Header

Công thức chung:

Block Hash = Hash(
Previous Hash
+ Merkle Root
+ Timestamp
+ Nonce
+ Difficulty
+ Version)

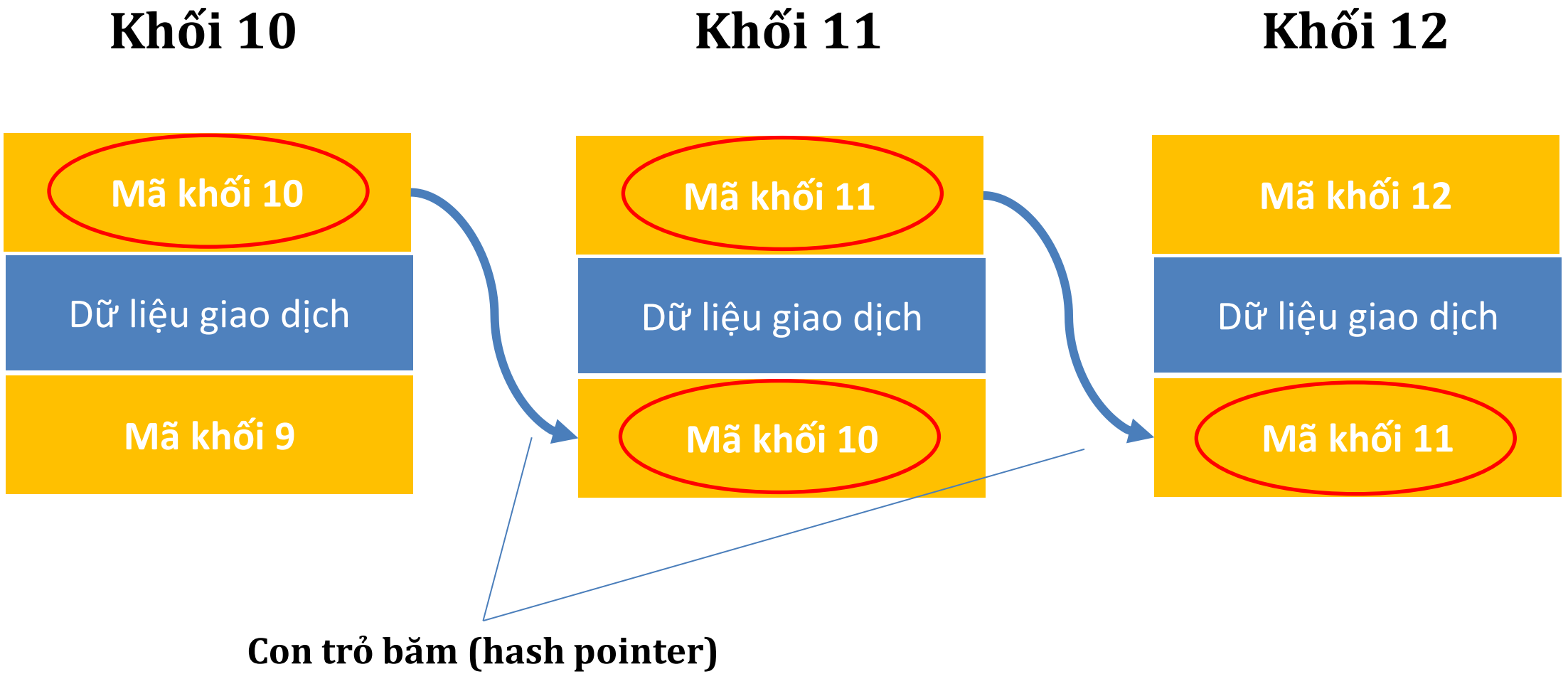
Bên trong một Block được mã hóa như thế nào?

Một Block điển hình



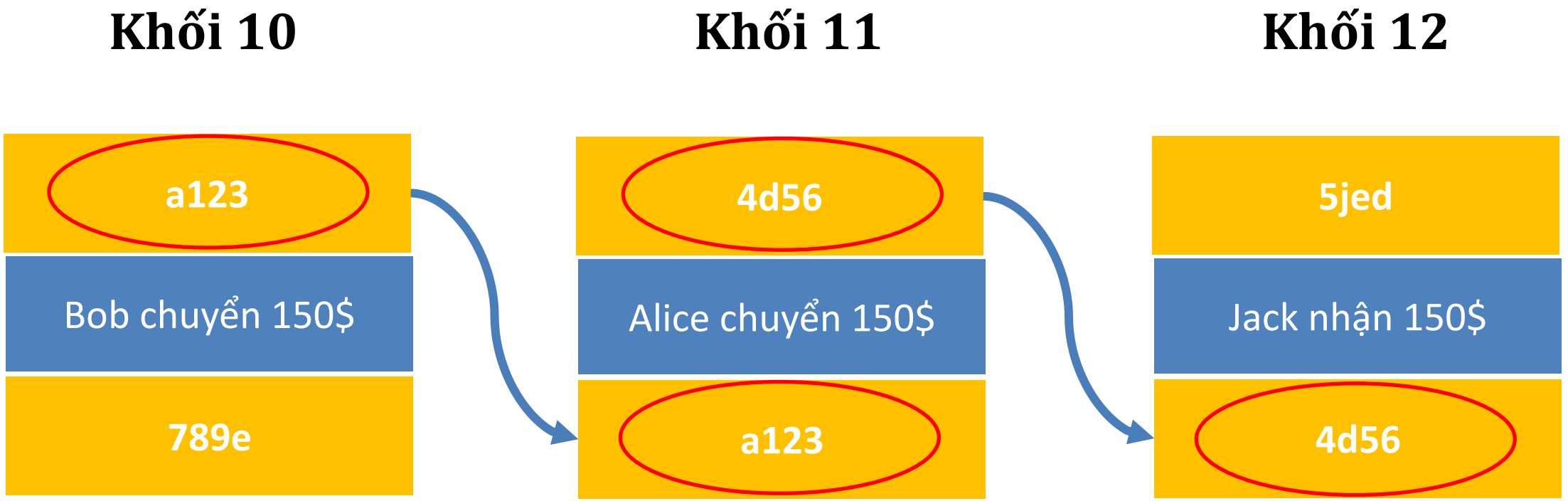
- **Mã băm (Block Hash)** đại diện duy nhất cho dữ liệu (chẳng hạn như nội dung khối hoặc giao dịch) và đảm bảo tính toàn vẹn của dữ liệu.
- Không thể giải ngược

Cơ chế liên kết các Block



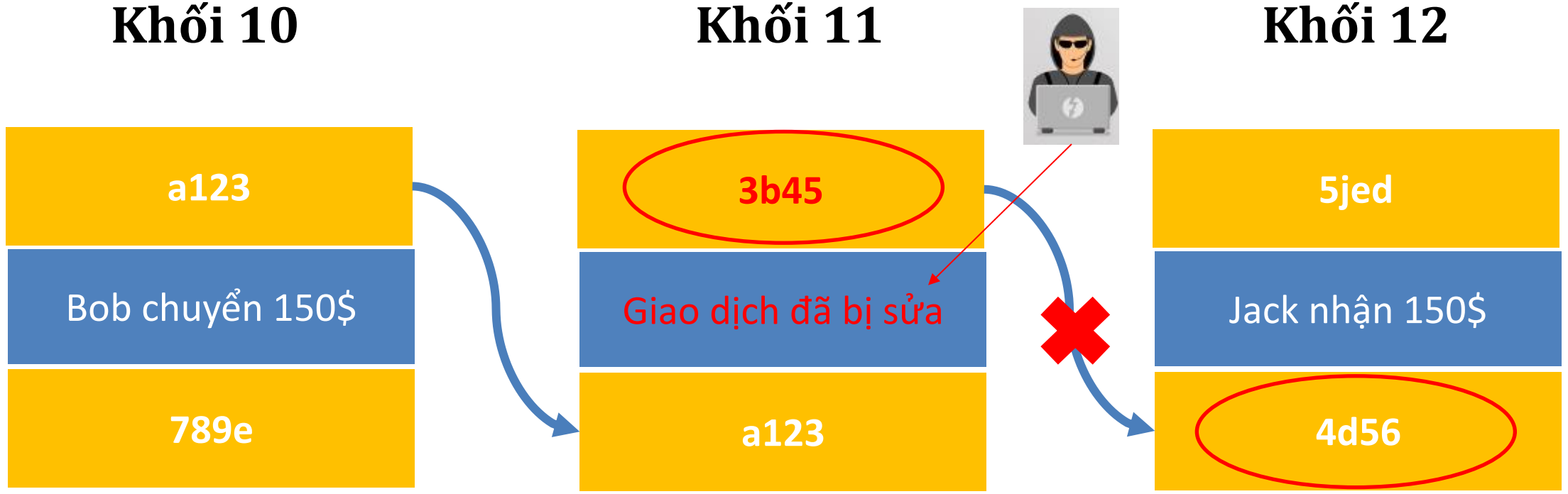
Cơ chế liên kết các Block

Ví dụ: Mạng blockchain như sau



Cơ chế liên kết các Block

Ví dụ: Giải sử khối 11 giao dịch đã bị chỉnh sửa



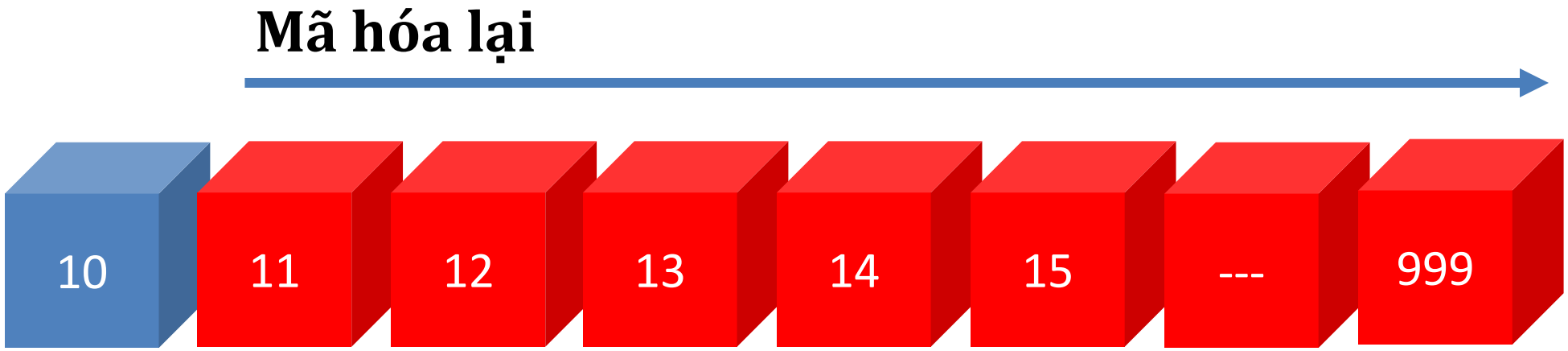
- Mã của khối 11 đã bị thay đổi
- Chuỗi sẻ bị đứt tại khối 11
- Khối 11 bất hợp lệ

Cơ chế liên kết các Block

Làm thế nào để Khối 11 hợp lệ trở lại?

Cơ chế liên kết các Block

- Đưa mã mới của khối 11 vào khối 12
- Tiếp tục mã hóa khối 12, nhưng điều này dẫn đến việc mã liên kết với khối 13 lại bị sai
- Và cứ như thế cần phải sửa lại khối cuối cùng của chuỗi



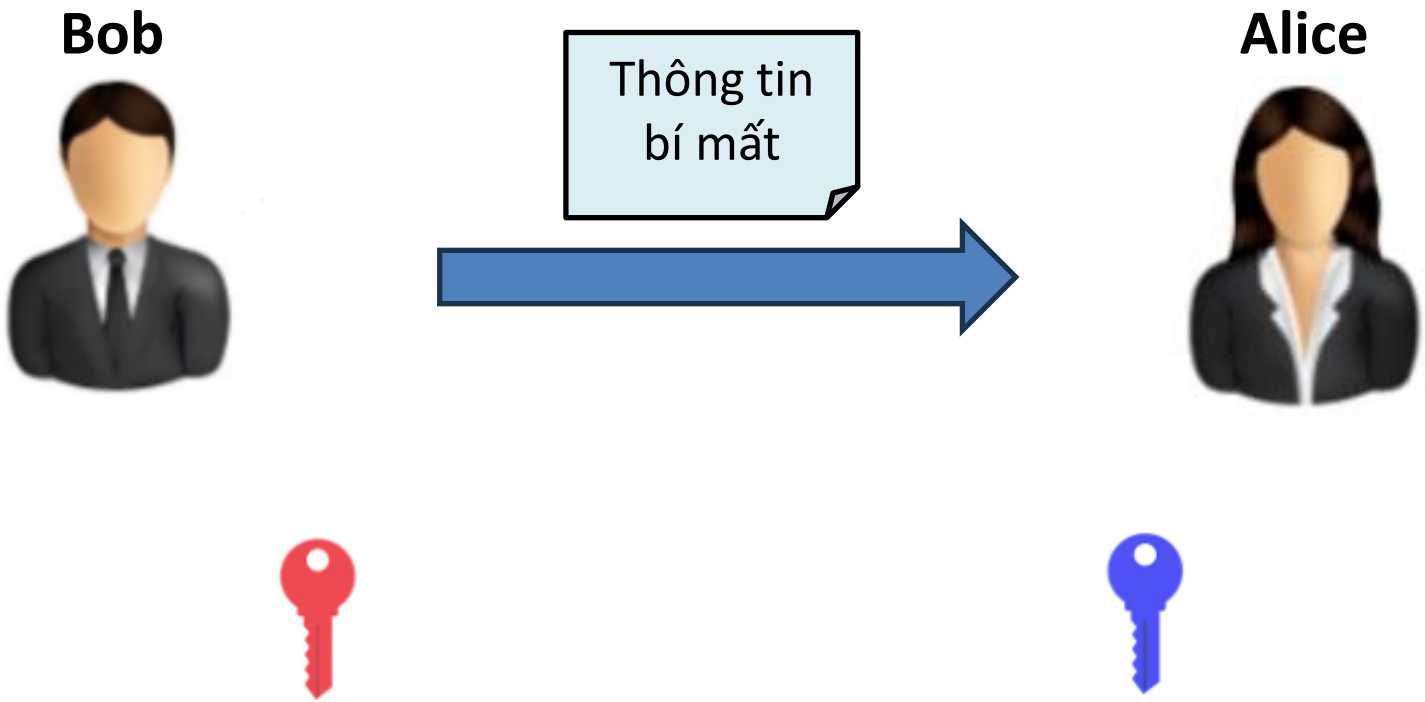
Kết luận: Sửa đổi 1 khối thì cần tính toán lại toàn bộ các khối đứng sau nó.

Mã hóa khóa công khai (RSA)

"Thuật toán được Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại Học viện Công nghệ Massachusetts (MIT). Tên của thuật toán lấy từ 3 chữ cái đầu của tên 3 tác giả."

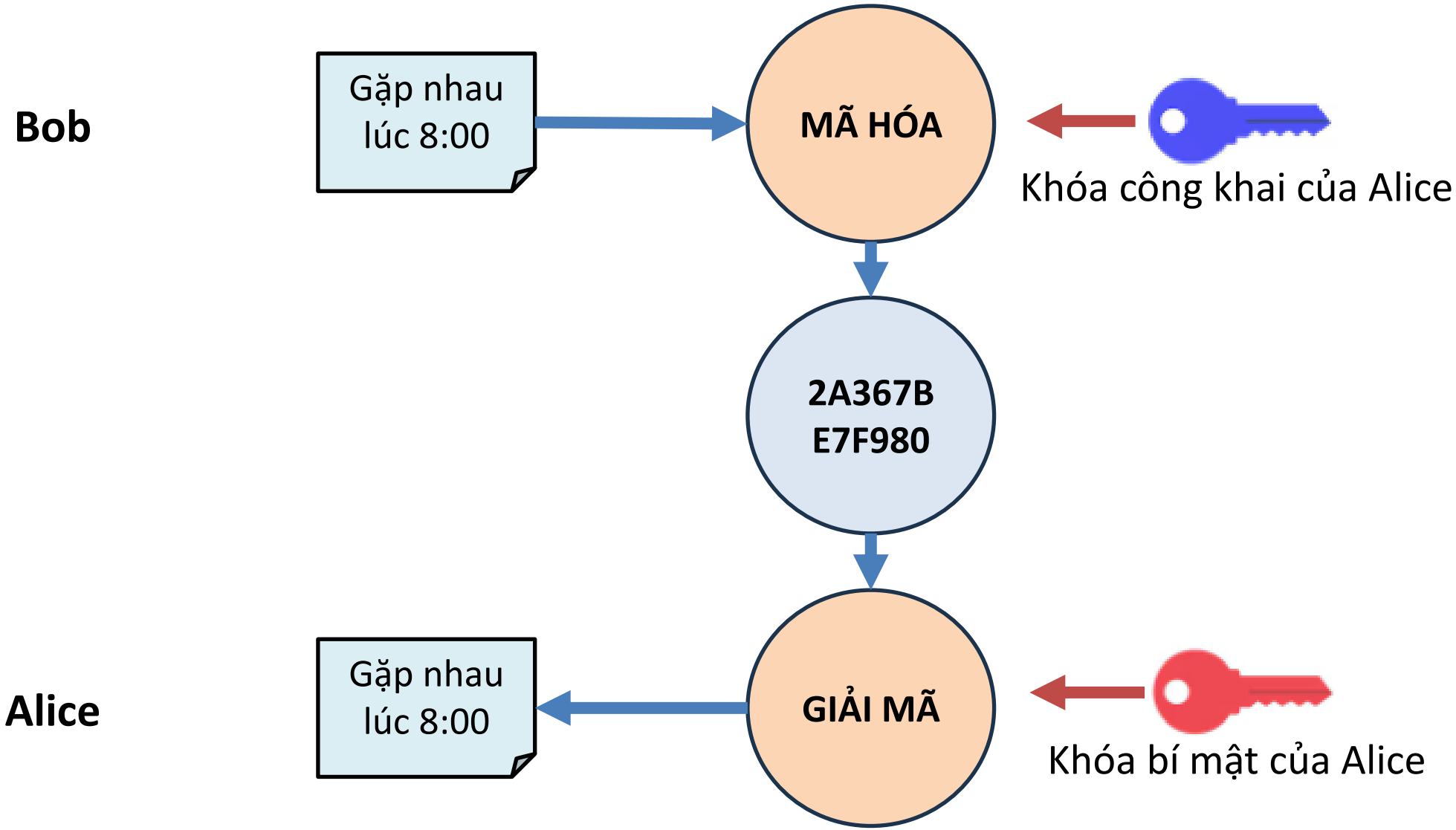
Theo wikipedia

Mã hóa khóa công khai (RSA)



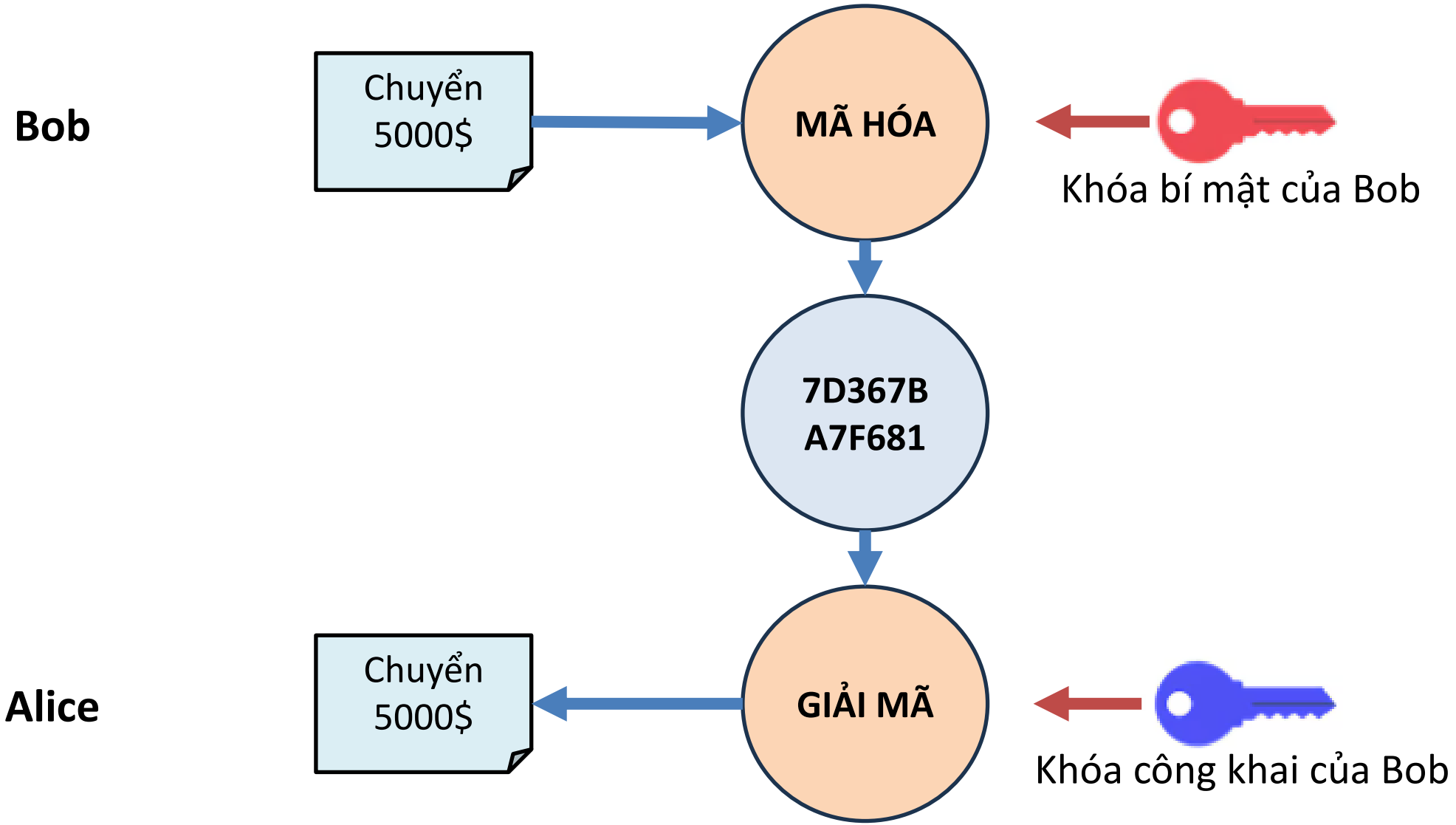
Mã hóa khóa công khai (RSA)

Ví dụ: Bảo mật nội dung giao dịch



Mã hóa khóa công khai (RSA)

Ví dụ: Chữ ký số xác minh giao dịch



Tự học

Source code: *#Tạo hàm băm SHA-256 và mã hóa khóa công khai RSA*

Course: 010100087602 - Công nghệ chuỗi khối
(HK2 năm 2024 - 2025)

1. Mã băm: sha-256.py
2. Tạo cặp khóa công khai: generateKeyRSA.py

   Mã hóa: encryptRSA.py

   Mã hóa: decryptRSA.py
3. Tạo chữ ký số và xác nhận: sign_verifyRSA.py

Triển khai hoạt động của một Blockchain cơ bản

Ví dụ: Quản lý điểm sinh viên

Thực hành

Các thành phần chính của một chuỗi khối cơ bản

- **Giao dịch (Transaction):** Mỗi giao dịch chứa **mã sinh viên**, **môn học** và **điểm số**
- **Khối (Block):** Mỗi khối chứa danh sách giao dịch, mã băm của khối trước và mã băm của khối, timestamp (dấu thời gian)
- **Chuỗi khối (Blockchain):** Các khối được liên kết với nhau thông qua hash
- **Cơ chế đồng thuận:** Xử lý các giao dịch chờ xử lý để tạo ra một khối mới

Công cụ cần thiết

- **Ngôn ngữ lập trình:** Python
- **Thư viện hỗ trợ:** hashlib (tạo hash), datetime (xử lý thời gian)

Thực hành

Source code: *#Triển khai hoạt động của một Blockchain cơ bản*

Course: 010100087602 - Công nghệ chuỗi khối
(HK2 năm 2024 - 2025)


Thank you