ĐỀ CƯƠNG ÔN TẬP

TIỀN SỐ VÀ CÔNG NGHỆ BLOCKCHAIN

Dành cho sinh viên đại học khối kinh tế, tài chính, công nghệ tài chính

Digital Currency and Blockchain Technology – a bilingual study guide

Hàm băm · Chữ ký số · Đồng thuận · Ví và lưu ký
Hợp đồng thông minh · DeFi · Rủi ro · Pháp luật Việt Nam

Bài tập có lời giải · Tự luận có dàn ý · Trắc nghiệm có đáp án · Mã Python chạy thật

Song ngữ Việt – Anh · Vietnamese – English

Phiên bản 1.0 – Tháng 11 năm 2026
https://tailieuso.vin

MỤC LỤC

CONTENTS

Chương 1. Tiền, tiền số và tài sản mã hóa: tổng quan – *Chapter 1. Money, digital money and crypto-assets: an overview*..... 8

1.1. Tiền là gì và đã đi qua những bước nào – *1.1. What money is and the steps it has taken* 8

1.2. Bốn thứ dễ nhầm với nhau: tiền gửi, ví điện tử, tiền số của ngân hàng trung ương, tiền mã hóa – *1.2. Four things easily confused: deposits, e-wallets, central bank digital currency, cryptocurrency* 11

1.3. Chi tiêu hai lần và những thử nghiệm trước Bitcoin – *1.3. Double spending and the experiments before Bitcoin*.....12

1.4. Sách trắng Bitcoin, khối nguyên thủy và chuỗi khối – *1.4. The Bitcoin white paper, the genesis block and the blockchain* 15

1.5. Phân loại tài sản mã hóa – *1.5. Classifying crypto-assets* 17

1.6. Khái niệm pháp lý ở Việt Nam: tài sản số, tài sản ảo, tài sản mã hóa – *1.6. Vietnamese legal concepts: digital assets, virtual assets, crypto-assets* 19

1.7. Năm đặc điểm của tài sản mã hóa: lợi ích và cái giá – *1.7. Five features of crypto-assets: benefits and costs*.....21

1.8. Đơn vị và quy đổi: satoshi, wei, gwei – *1.8. Units and conversion: satoshi, wei, gwei* 23

1.9. Lợi suất và biến động giá, so với gửi tiết kiệm – *1.9. Returns and price swings, against a savings deposit*.....24

1.10. Vị trí việc làm trong lĩnh vực tiền số và blockchain – *1.10. Jobs in digital money and blockchain* 27

1.11. Tính bằng Python – *1.11. Doing it in Python* 28

1.12. Bài tập vận dụng có lời giải – *Applied exercises with solutions*.....33

1.13. Câu hỏi tự luận và dàn ý trả lời – *Essay questions and answer outlines* 36

1.14. Câu hỏi trắc nghiệm – *Multiple-choice questions*.....37

Chương 2. Mật mã học nền tảng: hàm băm, chữ ký số, khóa và địa chỉ – *Chapter 2. Cryptographic foundations: hashes, signatures, keys and addresses*..... 40

2.1. Hàm băm: dấu vân tay của dữ liệu – *2.1. Hash functions: the fingerprint of data*.....40

2.2. SHA-256 và băm hai lần – *2.2. SHA-256 and double hashing*.....43

2.3. Con trỏ băm và chuỗi khối: sửa khối cũ thì lộ – *2.3. Hash pointers and the chain of blocks: editing an old block shows*.....44

2.4. Cây Merkle và chứng minh thuộc cây – *2.4. The Merkle tree and the proof of membership* 46

2.5. Mật mã khóa công khai và chữ ký số – *2.5. Public key cryptography and digital signatures* 48

2.6. Đường cong elliptic thu nhỏ: cộng điểm và nhân vô hướng – *2.6. A miniature elliptic curve: adding points and scalar multiplication* 50

2.7. ECDSA và Schnorr: ký và kiểm bằng phép tính – *2.7. ECDSA and Schnorr: signing and verifying by calculation* 53
2.8. Từ khóa bí mật đến khóa công khai đến địa chỉ – *2.8. From private key to public key to address* 56
2.9. Sinh khóa bí mật phải ngẫu nhiên: chuyện ví não – *2.9. Private keys must be random: the story of brain wallets* 59
2.10. Khóa công khai làm danh tính, bút danh, máy tính lượng tử và pháp luật Việt Nam – *2.10. Public keys as identities, pseudonyms, quantum computers and Vietnamese law* 60
2.11. Tính bằng Python: sổ Sen Vàng có chuỗi băm và chữ ký – *2.11. Doing it in Python: the Sen Vang ledger with a hash chain and signatures* 62
2.12. Bài tập vận dụng có lời giải – *Applied exercises with solutions* 66
2.13. Câu hỏi tự luận và dàn ý trả lời – *Essay questions and answer outlines* 68
2.14. Câu hỏi trắc nghiệm – *Multiple-choice questions* 70

Chương 3. Giao dịch và sổ cái phân tán – *Chapter 3. Transactions and the distributed ledger* 72
3.1. Sổ cái phân tán và hai cách ghi sổ – *3.1. The distributed ledger and two ways of keeping it* 72
3.2. Cấu trúc một giao dịch Bitcoin – *3.2. The structure of a Bitcoin transaction* 75
3.3. Ngôn ngữ kịch bản (Script): khóa và mở khóa – *3.3. The Script language: locking and unlocking* 78
3.4. Phí giao dịch và hàng chờ (mempool) – *3.4. Transaction fees and the waiting queue (mempool)* 80
3.5. Mạng ngang hàng: nút đầy đủ, nút nhẹ và đường đi của một giao dịch – *3.5. The peer-to-peer network: full nodes, light nodes and the path of a transaction* 84
3.6. Cấu trúc một khối – *3.6. The structure of a block* 86
3.7. Xác nhận: khi nào coi một giao dịch là chắc chắn – *3.7. Confirmations: when a transaction counts as final* 90
3.8. Trình khám phá khối: đọc một giao dịch bằng mắt – *3.8. The block explorer: reading a transaction by eye* 92
3.9. Nâng cấp giao thức: soft fork và hard fork – *3.9. Protocol upgrades: soft fork and hard fork* 93
3.10. Liên hệ Việt Nam: sổ cái và giao dịch trong định nghĩa của luật – *3.10. Vietnam: the ledger and transactions in the law's definitions* 95
3.11. Phần mềm nút, kiểu kịch bản đầu ra và tăng phí cho giao dịch bị kẹt – *3.11. Node software, output script types and raising the fee of a stuck transaction* 96
3.12. Tính bằng Python / Doing it in Python – *3.12. Doing it in Python* 101
3.13. Bài tập vận dụng có lời giải – *Applied exercises with solutions* 106
3.14. Câu hỏi tự luận và dàn ý trả lời – *Essay questions and answer outlines* 108
3.15. Câu hỏi trắc nghiệm – *Multiple-choice questions* 110

Chương 4. Đồng thuận và khai thác – *Chapter 4. Consensus and mining* 112
4.1. Vì sao cần đồng thuận khi không có trọng tài – *4.1. Why agreement is needed when there is no referee* 112

4.2. Đồng thuận Nakamoto: chuỗi nhiều công nhất, khối mồ côi, chia nhánh tạm – *4.2. Nakamoto consensus: the most-work chain, orphan blocks and temporary forks* ... 115
4.3. Bằng chứng công việc: mục tiêu, độ khó và số dùng một lần (nonce) – *4.3. Proof of work: target, difficulty and nonce (number used once)* ... 117
4.4. Điều chỉnh độ khó mỗi 2016 khối – *4.4. Difficulty adjustment every 2,016 blocks* ... 119
4.5. Phần thưởng khối, giảm một nửa và tổng cung – *4.5. Block reward, halving and total supply* ... 121
4.6. Kinh tế đào: sức băm, thu nhập kỳ vọng và điểm hòa vốn – *4.6. Mining economics: hash power, expected income and break-even* ... 123
4.7. Đào chung và phần cứng đào – *4.7. Mining pools and mining hardware* ... 125
4.8. Tấn công 51%, chi tiêu hai lần và đào ích kỷ – *4.8. The 51% attack, double spending and selfish mining* ... 127
4.9. Bằng chứng cổ phần, BFT cấp phép và so sánh các cách đồng thuận – *4.9. Proof of stake, permissioned BFT and a comparison of consensus methods* ... 130
4.10. Liên hệ Việt Nam và vị trí việc làm – *4.10. Links to Viet Nam and job roles* ... 133
4.11. Sybil, che khuất và số dùng một lần mở rộng – *4.11. Sybil, eclipse and the extra nonce* ... 134
4.12. Tính bằng Python – *4.12. Doing it in Python* ... 139
4.13. Bài tập vận dụng có lời giải – *Applied exercises with solutions* ... 146
4.14. Câu hỏi tự luận và dàn ý trả lời – *Essay questions and answer outlines* ... 148
4.15. Câu hỏi trắc nghiệm – *Multiple-choice questions* ... 150

Chương 5. Ví, lưu ký và an toàn tài sản số – *Chapter 5. Wallets, custody and keeping digital assets safe* ... 152
5.1. Ví là gì: ví không chứa tiền, ví giữ khóa – *5.1. What a wallet is: it holds keys, not coins* ... 152
5.2. Ví nóng, ví lạnh, ví phần cứng và ví giấy – *5.2. Hot, cold, hardware and paper wallets* ... 155
5.3. Cụm từ khôi phục và hạt giống – *5.3. The recovery phrase and the seed* ... 157
5.4. Ví phân cấp xác định, đường dẫn dẫn xuất và cách tạo ví – *5.4. Hierarchical deterministic wallets, derivation paths and creating a wallet* ... 160
5.5. Ví đa chữ ký và chia bí mật – *5.5. Multi-signature wallets and secret sharing* ... 163
5.6. Tự lưu ký, lưu ký qua tổ chức và sàn giao dịch tập trung – *5.6. Self-custody, custody through an institution and centralised exchanges* ... 167
5.7. Bằng chứng dự trữ bằng cây Merkle – *5.7. Proof of reserves with a Merkle tree* ... 169
5.8. Các kiểu mất tài sản và cách phòng – *5.8. How assets get lost, and how to prevent it* ... 172
5.9. Ẩn danh và riêng tư: bút danh không phải ẩn danh – *5.9. Anonymity and privacy: a pseudonym is not anonymity* ... 174
5.10. Liên hệ Việt Nam: lưu ký, tài khoản và dịch vụ tài sản mã hóa – *5.10. Vietnam: custody, accounts and crypto-asset services* ... 177
5.11. Ví chỉ xem, giao dịch ký một phần, ví nhẹ và riêng tư nâng cao – *5.11. Watch-only wallets, partially signed transactions, light wallets and advanced privacy* ... 179
5.12. Tính bằng Python / Doing it in Python – *5.12. Doing it in Python* ... 185
5.13. Bài tập vận dụng có lời giải – *Applied exercises with solutions* ... 188

5.14. Câu hỏi tự luận và dàn ý trả lời – *Essay questions and answer outlines* 191
5.15. Câu hỏi trắc nghiệm – *Multiple-choice questions* 192

Chương 6. Ethereum, hợp đồng thông minh và token – *Chapter 6. Ethereum, smart contracts and tokens* 195
6.1. Blockchain như một nền tảng và các đồng tiền mã hóa khác Bitcoin – *6.1. Blockchain as a platform, and crypto coins other than Bitcoin* 195
6.2. Ethereum và mô hình tài khoản – *6.2. Ethereum and the account model* 198
6.3. Hợp đồng thông minh và máy ảo Ethereum – *6.3. Smart contracts and the Ethereum Virtual Machine* 202
6.4. Gas và phí giao dịch – *6.4. Gas and transaction fees* 205
6.5. Token theo chuẩn: ERC-20 và ERC-721 – *6.5. Standard tokens: ERC-20 and ERC-721* 208
6.6. Oracle: đưa dữ liệu ngoài chuỗi vào hợp đồng – *6.6. Oracles: bringing off-chain data into contracts* 211
6.7. Mở rộng quy mô: bộ ba bất khả, kênh thanh toán và rollup – *6.7. Scaling: the trilemma, payment channels and rollups* 213
6.8. Lỗi hợp đồng thông minh, The DAO và lỗ hổng gọi lại – *6.8. Smart contract flaws, The DAO and reentrancy* 216
6.9. Liên hệ Việt Nam: token và hợp đồng thông minh nhìn từ pháp luật – *6.9. The Vietnamese angle: tokens and smart contracts in law* 220
6.10. Bitcoin làm nền tảng, altcoin cụ thể và hợp đồng khóa băm – *6.10. Bitcoin as a platform, specific altcoins and hash time-locked contracts* 222
6.11. Tính bằng Python – *6.11. Doing it in Python* 228
6.12. Bài tập vận dụng có lời giải – *Applied exercises with solutions* 232
6.13. Câu hỏi tự luận và dàn ý trả lời – *Essay questions and answer outlines* 234
6.14. Câu hỏi trắc nghiệm – *Multiple-choice questions* 236

Chương 7. Tài chính phi tập trung, đồng ổn định và token hóa tài sản – *Chapter 7. Decentralised finance, stablecoins and asset tokenisation* 238
7.1. Tài chính phi tập trung là gì – *7.1. What decentralised finance is* 238
7.2. Sàn phi tập trung và nhà tạo lập thị trường tự động – *7.2. Decentralised exchanges and automated market makers* 241
7.3. Nhà cung cấp thanh khoản: phí và tổn thất tạm thời – *7.3. Liquidity providers: fees and impermanent loss* 244
7.4. Cho vay thế chấp phi tập trung – *7.4. Decentralised collateralised lending* 246
7.5. Đồng ổn định và sự sụp đổ của Terra/Luna – *7.5. Stablecoins and the collapse of Terra/Luna* 249
7.6. Lợi suất khai thác thanh khoản: APR và APY – *7.6. Liquidity mining yield: APR and APY* 253
7.7. Token hóa tài sản thực – *7.7. Tokenising real-world assets* 254
7.8. Tổ chức tự trị phi tập trung và NFT – *7.8. Decentralised autonomous organisations and NFTs* 257
7.9. Rủi ro của DeFi và cách tự bảo vệ – *7.9. DeFi risks and how to protect yourself* ... 258

7.10. Liên hệ Việt Nam: quy định về tài sản mã hóa và token hóa – *7.10. Vietnam: rules on crypto-assets and tokenisation* 261
7.11. Tính bằng Python – *7.11. Doing it in Python* 263
7.12. Bài tập vận dụng có lời giải – *Applied exercises with solutions* 269
7.13. Câu hỏi tự luận và dàn ý trả lời – *Essay questions and answer outlines* 271
7.14. Câu hỏi trắc nghiệm – *Multiple-choice questions* 273

Chương 8. Ứng dụng blockchain trong tài chính và kinh tế – *Chapter 8. Blockchain applications in finance and the economy* 275

8.1. Khi nào nên và không nên dùng blockchain – *8.1. When to use a blockchain, and when not to* 275
8.2. Blockchain công khai, riêng và liên minh – *8.2. Public, private and consortium blockchains* 278
8.3. Thanh toán và chuyển tiền xuyên biên giới – *8.3. Payments and cross-border transfers* 281
8.4. Tiền số của ngân hàng trung ương (CBDC) – *8.4. Central bank digital currency (CBDC)* 284
8.5. Truy xuất nguồn gốc chuỗi cung ứng – *8.5. Supply chain traceability* 287
8.6. Tài trợ thương mại và thư tín dụng số – *8.6. Trade finance and digital letters of credit* 290
8.7. Định danh số và chứng chỉ số – *8.7. Digital identity and digital credentials* 292
8.8. Bảo hiểm tham số và thị trường vốn – *8.8. Parametric insurance and capital markets* 294
8.9. Thách thức triển khai và liên hệ Việt Nam – *8.9. Implementation challenges and the Vietnamese context* 296
8.10. Tính bằng Python – *8.10. Doing it in Python* 299
8.11. Bài tập vận dụng có lời giải – *Applied exercises with solutions* 304
8.12. Câu hỏi tự luận và dàn ý trả lời – *Essay questions and answer outlines* 307
8.13. Câu hỏi trắc nghiệm – *Multiple-choice questions* 309

Chương 9. Đầu tư, định giá và rủi ro tài sản mã hóa – *Chapter 9. Investing in crypto-assets: valuation and risk* 311

9.1. Đầu tư, đầu cơ hay đánh bạc: gọi đúng tên việc mình đang làm – *9.1. Investing, speculating or gambling: naming what you are really doing* 311
9.2. Lợi suất, độ biến động, sụt giảm tối đa và tương quan – *9.2. Return, volatility, maximum drawdown and correlation* 314
9.3. Giá trị rủi ro (VaR) lịch sử: một ngày xấu có thể mất bao nhiêu – *9.3. Historical value at risk (VaR): how much a bad day can cost* 317
9.4. Các cách "định giá" tài sản mã hóa và vì sao chúng không dự báo được giá – *9.4. Ways of "valuing" a crypto-asset, and why they cannot forecast price* 320
9.5. Tỷ trọng nhỏ, mua đều định kỳ và tái cân bằng – *9.5. Small weights, regular buying and rebalancing* 323
9.6. Quỹ ETF tài sản mã hóa ở nước ngoài – *9.6. Crypto-asset exchange traded funds abroad* 325

9.7. Sáu loại rủi ro và các sự cố đã xảy ra – *9.7. Six kinds of risk and incidents that have happened* 327
9.8. Lừa đảo: nhận ra và tính được vì sao chúng sụp – *9.8. Scams: how to recognise them and calculate why they collapse* 328
9.9. Tâm lý nhà đầu tư: những thiên lệch làm mình mất tiền – *9.9. Investor psychology: the biases that cost you money* 332
9.10. Quy tắc tự bảo vệ và quy định tại Việt Nam – *9.10. Rules for protecting yourself and the rules in Vietnam* 333
9.11. Tính bằng Python / Doing it in Python – *9.11. Doing it in Python* 336
9.12. Bài tập vận dụng có lời giải – *Applied exercises with solutions* 342
9.13. Câu hỏi tự luận và dàn ý trả lời – *Essay questions and answer outlines* 344
9.14. Câu hỏi trắc nghiệm – *Multiple-choice questions* 346

Chương 10. Pháp luật, quản lý nhà nước và đạo đức nghề nghiệp – *Chapter 10. Law, regulation and professional ethics* 349
10.1. Vì sao nhà nước quản lý tài sản mã hóa – *10.1. Why the State regulates crypto-assets* 349
10.2. Ba cách tiếp cận trên thế giới: cấm, thử nghiệm, cấp phép – *10.2. Three approaches around the world: ban, pilot, licence* 351
10.3. FATF, nơi cung cấp dịch vụ tài sản ảo và quy tắc chuyển thông tin – *10.3. FATF, virtual asset service providers and the travel rule* 353
10.4. Việt Nam: tài sản số, tài sản ảo và tài sản mã hóa trong Luật Công nghiệp công nghệ số – *10.4. Vietnam: digital assets, virtual assets and crypto-assets in the Law on the Digital Technology Industry* 356
10.5. Nghị quyết 05/2025/NQ-CP: thí điểm thị trường tài sản mã hóa – *10.5. Resolution 05/2025/NQ-CP: the crypto-asset market pilot* 357
10.6. Xử phạt vi phạm hành chính theo Nghị định 284/2026/NĐ-CP – *10.6. Administrative penalties under Decree 284/2026/NĐ-CP* 362
10.7. Tài sản mã hóa và phương tiện thanh toán hợp pháp – *10.7. Crypto-assets and lawful means of payment* 364
10.8. Phòng, chống rửa tiền: KYC, giao dịch đáng ngờ và báo cáo – *10.8. Anti-money laundering: KYC, suspicious transactions and reporting* 366
10.9. Thuế, quyền lợi và cách tự bảo vệ của nhà đầu tư – *10.9. Tax, investor rights and self-protection* 369
10.10. Đạo đức nghề nghiệp và lộ trình nghề trong lĩnh vực blockchain – *10.10. Professional ethics and career paths in blockchain* 371
10.11. Tính bằng Python / Doing it in Python – *10.11. Doing it in Python* 374
10.12. Bài tập vận dụng có lời giải – *Applied exercises with solutions* 379
10.13. Câu hỏi tự luận và dàn ý trả lời – *Essay questions and answer outlines* 382
10.14. Câu hỏi trắc nghiệm – *Multiple-choice questions* 383

Phụ lục A. Đáp án câu hỏi trắc nghiệm – *Appendix A. Answer key* 386

Phụ lục B. Công thức – *Appendix B. Formulas* 391

Phụ lục C. Thuật ngữ Việt – Anh – *Appendix C. Vietnamese–English glossary* 398

Phụ lục D. Văn bản pháp luật dùng trong sách – *Appendix D. Legislation used in this book* **406**

Phụ lục E. Tài liệu tham khảo – *Appendix E. References* **408**

Chương 1. Tiền, tiền số và tài sản mã hóa: tổng quan – *Chapter 1. Money, digital money and crypto-assets: an overview*

Mục tiêu chương – *Chapter objectives*

- Nói được tiền là gì, làm ba việc nào, và đã đi qua những dạng nào từ hàng hóa đến thẻ và ví trên điện thoại.
  Say what money is, which three jobs it does, and which forms it has taken from commodities to cards and phone wallets.
- Phân biệt tiền gửi ngân hàng, ví điện tử, tiền số của ngân hàng trung ương và tiền mã hóa theo ba câu hỏi: ai phát hành, ai giữ sổ, có được bảo đảm không.
  Tell bank deposits, e-wallets, central bank digital currency and cryptocurrency apart by three questions: who issues, who keeps the ledger, is it guaranteed.
- Giải thích chi tiêu hai lần, cách ngân hàng chặn nó bằng sổ trung tâm, và vì sao chuỗi khối ra đời; đọc được sơ đồ một giao dịch đi qua mạng.
  Explain double spending, how a bank stops it with a central ledger and why the blockchain appeared; read the diagram of a transaction crossing the network.
- Xếp một token vào đúng loại và nói được khái niệm tài sản số, tài sản ảo, tài sản mã hóa trong pháp luật Việt Nam, kể cả việc chúng không phải phương tiện thanh toán.
  Place a token in the right kind and state the Vietnamese legal concepts of digital, virtual and crypto-assets, including that they are not a means of payment.
- Đổi satoshi, wei, gwei; tính lợi suất, độ biến động và sụt giảm tối đa của một chuỗi giá, so với gửi tiết kiệm; kể tên các vị trí việc làm trong lĩnh vực.
  Convert satoshi, wei and gwei; compute the return, volatility and maximum drawdown of a price series against a savings deposit; name the jobs in the field.

1.1. Tiền là gì và đã đi qua những bước nào – *1.1. What money is and the steps it has taken*

Hãy nhớ lại lần bạn đổi vé xem phim lấy một ly trà sữa với bạn cùng lớp. Muốn được, bạn phải gặp đúng người đang thừa vé và đang thèm trà sữa. Cách đổi hàng lấy hàng như thế hiếm khi trùng nhu cầu. Tiền ra đời để gỡ nút thắt đó: ai cũng nhận nó, nên bạn bán thứ mình có cho người cần, rồi dùng tiền mua thứ mình cần ở người khác.

Think of the time you swapped a cinema ticket for a bubble tea with a classmate. It only worked because you met someone with a spare ticket who also wanted tea. Barter rarely lines up like that. Money exists to untie that knot: everyone accepts it, so you sell what you have to the person who needs it, then spend the money on what you need from somebody else.

Môn Tài chính – Tiền tệ thường nêu từ ba đến bốn chức năng của tiền. Ở đây gom lại ba chức năng, vì chúng đủ để so sánh tiền thật với tiền mã hóa. **Đơn vị tính toán** (unit of account) là thước đo chung: ly cà phê 35.000 đồng, bánh mì 20.000 đồng, ai nhìn cũng so được. **Phương tiện trao đổi** (medium of exchange) là thứ bạn đưa cho người bán để nhận hàng ngay, không cần họ cần đúng thứ bạn có. **Cất trữ giá trị** (store of value) là giữ

được sức mua từ hôm nay sang tháng sau: tiền để trong ví hôm nay vẫn mua được gần như cũ vào tuần tới.

*The Finance and Money course usually lists three or four functions of money. Here they are grouped into three, enough to compare real money with crypto-assets. A **unit of account** is the common yardstick: coffee at 35,000 dong, a bread roll at 20,000 dong, and anyone can compare them. A **medium of exchange** is what you hand to a seller for goods on the spot, with no need for the seller to want what you own. A **store of value** keeps its purchasing power from today into next month: money in your wallet today still buys roughly the same next week.*

Chức năng *Function*	**Câu hỏi để tự kiểm** *Test question*	**Ví dụ** *Example*	**Tiền mã hóa làm được chưa** *How crypto-assets fare*
Đơn vị tính toán *Unit of account*	Mọi giá trong quán có ghi bằng một đơn vị không? *Is every price in the shop quoted in one unit?*	Bảng giá bằng đồng *A price list in dong*	Ít khi: giá hàng vẫn niêm yết bằng đồng *Seldom: shop prices are still posted in dong*
Phương tiện trao đổi *Medium of exchange*	Người bán có nhận không, không cần hỏi thêm? *Will a seller accept it without asking questions?*	Đưa 50.000 đồng mua đồ ăn *Handing over 50,000 dong for a meal*	Tại Việt Nam không phải phương tiện thanh toán hợp pháp (mục 1.6) *In Vietnam not a lawful means of payment (section 1.6)*
Cất trữ giá trị *Store of value*	Sau 3 tháng còn mua được ngần ấy không? *After three months does it still buy as much?*	Tiền gửi tiết kiệm có lãi *An interest-bearing savings deposit*	Giá dao động mạnh nên khó cất trữ ổn định (mục 1.9) *Prices swing widely, so storing value is unsteady (section 1.9)*

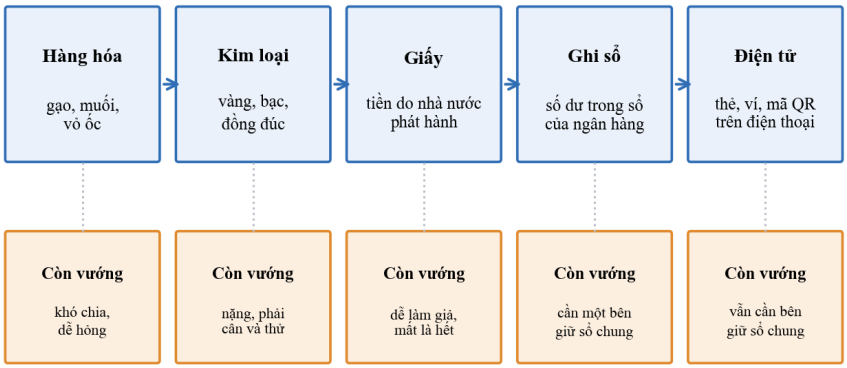
Bảng trên chỉ tóm lại. Điểm cần nhớ: một thứ chỉ được gọi là tiền khi làm được cả ba việc trong đời sống thật, không phải khi có cái tên nghe giống tiền.

The table only summarises. The point to remember: something counts as money when it does all three jobs in real life, not when it merely has a money-like name.

Năm bước tiến của tiền – *Five steps in the history of money*

Tiền đi qua năm dạng. **Hàng hóa**: gạo, muối, vỏ ốc được dùng làm vật trung gian; khó chia nhỏ và dễ hỏng. **Kim loại**: vàng, bạc, đồng đúc thành đồng; bền, chia được, nhưng nặng và phải cân, phải thử thật giả. **Giấy**: nhà nước phát hành giấy nhẹ, dễ mang, nhưng giấy bị làm giả được và mất là mất. **Ghi sổ ngân hàng**: tiền nằm thành số dư trong sổ, chuyển tiền chỉ là sửa hai dòng. **Điện tử**: thẻ, ví, mã QR cho phép sửa hai dòng đó bằng vài chạm trên điện thoại.

*Money has passed through five forms. **Commodities**: rice, salt and shells serve as go-betweens, but they are hard to divide and spoil. **Metal**: gold, silver and copper struck into coins are durable and divisible, yet heavy and must be weighed and tested. **Paper**: the state issues light paper that is easy to carry, but it can be forged and a lost note is gone. **Bank ledger**: money sits as a balance in a book, and a transfer is just editing two lines. **Electronic**: cards, wallets and QR codes let you make that two-line edit with a few taps on a phone.*



Hình 1.1. Hình 1.1. Năm hộp xanh đi từ trái sang phải là năm dạng của tiền; hộp cam bên dưới nói mỗi dạng còn vướng gì. Hai dạng bên phải đều cần một bên giữ sổ chung.

Figure 1.1. *Figure 1.1. The five blue boxes from left to right are the five forms of money; the orange box under each says what still gets in the way. Both right-hand forms need a common ledger keeper.*

Hai dạng cuối giống nhau ở một điểm: tiền thực chất là một dòng số trong sổ của ai đó. Để thấy rõ, hãy theo một lệnh chuyển khoản.

The last two forms share one feature: money is really a line of numbers in somebody's ledger. To see it clearly, follow one bank transfer.

Ví dụ làm mẫu: Hà My chuyển 200.000 đồng cho anh Quân – ***Worked example: Ha My transfers 200,000 dong to Quan***

Dữ kiện: số dư của Hà My là 1.500.000 đồng, của anh Quân là 800.000 đồng, cả hai mở tài khoản ở cùng một ngân hàng.

Data: Ha My's balance is 1,500,000 dong and Quan's is 800,000 dong, both held at the same bank.

1. Hà My mở ứng dụng ngân hàng, nhập số tài khoản của anh Quân và số tiền 200.000 đồng, rồi xác nhận bằng mã một lần.
   Ha My opens the banking app, enters Quan's account number and 200,000 dong, then confirms with a one-time code.
2. Ngân hàng mở sổ, kiểm số dư của Hà My: 1.500.000 ≥ 200.000, đủ tiền.
   The bank opens its ledger and checks Ha My's balance: 1,500,000 ≥ 200,000, enough.
3. Ngân hàng trừ ở dòng của Hà My: 1.500.000 − 200.000 = 1.300.000 đồng.
   The bank deducts on Ha My's line: 1,500,000 − 200,000 = 1,300,000 dong.
4. Ngân hàng cộng ở dòng của anh Quân: 800.000 + 200.000 = 1.000.000 đồng.
   The bank adds on Quan's line: 800,000 + 200,000 = 1,000,000 dong.

Nghĩa là không có tờ tiền nào đi đâu cả: ngân hàng chỉ sửa hai dòng, tổng hai số dư vẫn là 2.300.000 đồng. Cả ngân hàng lẫn hai bạn đều tin vào cuốn sổ đó.

So no banknote went anywhere: the bank simply edited two lines, and the two balances still total 2,300,000 dong. The bank and both friends trust that ledger.

1.2. Bốn thứ dễ nhầm với nhau: tiền gửi, ví điện tử, tiền số của ngân hàng trung ương, tiền mã hóa – *1.2. Four things easily confused: deposits, e-wallets, central bank digital currency, cryptocurrency*

Bạn nghe người ta nói "tiền số" cho cả bốn thứ sau, nhưng chúng khác nhau ở ba câu hỏi: ai phát hành, ai giữ sổ, và nếu có chuyện thì ai đứng ra bảo đảm. Hãy đi lần lượt.

People say "digital money" for all four of the following, yet they differ on three questions: who issues it, who keeps the ledger, and who stands behind it if something goes wrong. Take them one at a time.

Tiền gửi ngân hàng (bank deposit) là số dư trong tài khoản của bạn. Ngân hàng thương mại giữ sổ. Số dư là quyền của bạn đòi tiền ở ngân hàng, tính bằng đồng. **Ví điện tử** (e-wallet) là tài khoản trên ứng dụng của tổ chức cung ứng ví. Họ giữ sổ, đơn vị vẫn là đồng, và việc quản lý theo quy định về dịch vụ thanh toán. **Tiền số của ngân hàng trung ương** (central bank digital currency, CBDC) là tiền pháp định ở dạng số do chính ngân hàng trung ương phát hành, giống như tờ tiền giấy được chuyển sang dạng dữ liệu. **Tiền mã hóa** (cryptocurrency) là đơn vị giá trị chạy trên một mạng máy tính; không có ngân hàng nào giữ sổ, mà nhiều máy cùng giữ và cùng kiểm.

*A **bank deposit** is the balance in your account. A commercial bank keeps the ledger. The balance is your claim on the bank, counted in dong. An **e-wallet** is an account in the app of a wallet provider. The provider keeps the ledger, the unit is still the dong, and the rules on payment services apply. **Central bank digital currency** (CBDC) is legal tender in digital form issued by the central bank itself, like a banknote turned into data. A **cryptocurrency** is a unit of value running on a computer network; no bank keeps the ledger, instead many machines keep it and check it together.*

Loại *Kind*	**Ai phát hành** *Who issues*	**Ai giữ sổ** *Who keeps the ledger*	**Được bảo đảm không** *Is it guaranteed*
Tiền gửi ngân hàng *Bank deposit*	Ngân hàng thương mại tạo ra số dư; đơn vị là đồng *The commercial bank creates the balance; the unit is the dong*	Ngân hàng thương mại *The commercial bank*	Có: ngân hàng có nghĩa vụ trả, chịu giám sát của ngân hàng trung ương *Yes: the bank must repay and is supervised by the central bank*
Ví điện tử *E-wallet*	Tổ chức cung ứng ví; đơn vị là đồng *The wallet provider; the unit is the dong*	Tổ chức cung ứng ví *The wallet provider*	Theo nghĩa vụ hoàn trả của tổ chức cung ứng và quy định quản lý *Through the provider's duty to repay and the rules governing it*

Loại *Kind*	**Ai phát hành** *Who issues*	**Ai giữ sổ** *Who keeps the ledger*	**Được bảo đảm không** *Is it guaranteed*
Tiền số ngân hàng trung ương (CBDC) *Central bank digital currency*	Ngân hàng trung ương *The central bank*	Ngân hàng trung ương, hoặc cùng ngân hàng thương mại (Chương 8) *The central bank, or together with commercial banks (Chapter 8)*	Có: là nghĩa vụ của ngân hàng trung ương *Yes: an obligation of the central bank*
Tiền mã hóa *Cryptocurrency*	Không có bên duy nhất; quy tắc phát hành nằm trong phần mềm của mạng *No single party; the issuance rules sit in the network's software*	Mạng nhiều máy (nút) cùng giữ bản sao *A network of many machines (nodes) each holding a copy*	Không có ai bảo đảm giá trị hay hoàn tiền *Nobody guarantees the value or refunds*

Cột cuối của bảng là chỗ khác nhau lớn nhất cho người dùng. Nếu bạn gõ nhầm số tài khoản ngân hàng, bạn còn có ngân hàng để nhờ truy soát. Với tiền mã hóa, gửi nhầm thường là mất, vì không có bên nào đứng giữa (Chương 5).

The last column is where users feel the biggest difference. If you mistype a bank account number, you still have a bank to ask for a trace. With cryptocurrency a wrong address usually means a lost sum, since no one stands in the middle (Chapter 5).

Một cách nhớ: ví điện tử và CBDC vẫn là "đồng", chỉ khác đường đi; tiền mã hóa là một đơn vị khác hẳn, có sổ riêng và giá riêng. Ví của tiền mã hóa cũng khác tên gọi: nó không chứa tiền, nó giữ chìa khóa mở quyền dùng tài sản trên sổ chung (Chương 5).

A way to remember: e-wallets and CBDC are still "dong", only the route differs; a cryptocurrency is another unit altogether, with its own ledger and its own price. A crypto wallet also differs in name: it holds no coins, it holds the keys to your claim on the shared ledger (Chapter 5).

> **LỖI HAY GẶP / COMMON MISTAKE –** Coi số dư ví điện tử là tiền mã hóa vì cùng "nằm trong điện thoại". Hai thứ khác nhau ở người phát hành và người giữ sổ. Hãy hỏi ba câu: ai phát hành, ai giữ sổ, ai bảo đảm.
> *Treating an e-wallet balance as a cryptocurrency because both "live in the phone". They differ in issuer and ledger keeper. Ask the three questions: who issues, who keeps the ledger, who guarantees.*

1.3. Chi tiêu hai lần và những thử nghiệm trước Bitcoin – *1.3. Double spending and the experiments before Bitcoin*

Một tờ tiền giấy đã đưa cho người này thì không còn trong tay bạn. Nhưng nếu tiền chỉ là dữ liệu, bạn có thể sao chép tệp rồi gửi bản sao cho người khác. Việc dùng cùng một khoản tiền số cho hai giao dịch gọi là **chi tiêu hai lần** (double spending). Nếu không chặn được, tiền số vô giá trị, vì ai cũng tự in thêm bằng cách chép.

A banknote handed to one person is no longer in your hand. But if money is just data, you can copy the file and send the copy to somebody else. Using the same digital money in two transactions is called ***double spending****. If it cannot be stopped, digital money is worthless, since anyone could print more by copying.*

Ngân hàng giải bài toán này bằng một sổ trung tâm. Mọi lệnh chuyển đều đi qua sổ; sổ kiểm số dư rồi trừ ngay trước khi cho lệnh kế tiếp chạy.

Banks solve it with one central ledger. Every transfer passes through that ledger, which checks the balance and deducts at once before the next order runs.

Ví dụ làm mẫu: hai lệnh cùng chi 500.000 đồng – ***Worked example: two orders spending the same 500,000 dong***

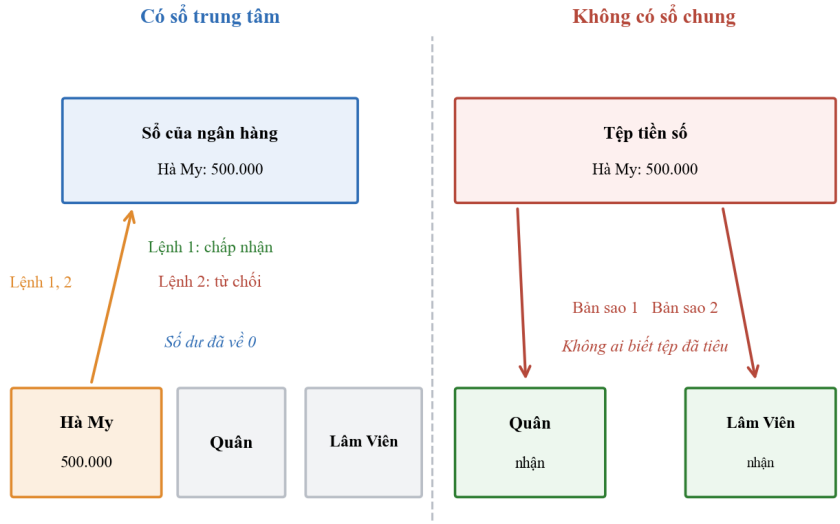
Dữ kiện: Hà My có 500.000 đồng trong sổ. Cùng một phút, cô gửi hai lệnh: lệnh 1 trả anh Quân 500.000 đồng, lệnh 2 trả Công ty Lâm Viên 500.000 đồng.

Data: Ha My has 500,000 dong in the ledger. In the same minute she sends two orders: order 1 pays Quan 500,000 dong, order 2 pays Lam Vien Company 500,000 dong.

1. Sổ nhận hai lệnh và xếp thành hàng, lệnh 1 đứng trước.
   The ledger receives both orders and queues them, order 1 first.
2. Với lệnh 1: số dư 500.000 ≥ 500.000, đủ. Sổ trừ về 0 và cộng 500.000 cho anh Quân.
   For order 1: balance 500,000 ≥ 500,000, enough. The ledger deducts down to 0 and credits Quan 500,000.
3. Với lệnh 2: số dư lúc này là 0 < 500.000, không đủ. Sổ từ chối.
   For order 2: the balance is now 0 < 500,000, not enough. The ledger rejects it.

Nghĩa là Công ty Lâm Viên không nhận được tiền và biết ngay lệnh bị từ chối, vì chỉ có một cuốn sổ quyết định thứ tự.

So Lam Vien Company receives nothing and learns at once that the order failed, because a single ledger settles the order of events.



Hình 1.2. Hình 1.2. Bên trái: một sổ trung tâm nhận hai lệnh, chấp nhận lệnh 1 và từ chối lệnh 2. Bên phải: tiền chỉ là tệp, hai bản sao đều tới tay người nhận vì không có sổ chung.

Figure 1.2. *Figure 1.2. Left: one central ledger takes two orders, accepts order 1 and rejects order 2. Right: money is just a file, and both copies reach their recipients because there is no common ledger.*

Cách này chạy tốt, nhưng cả hệ thống tựa vào một bên. Sổ ngừng chạy thì cả mạng ngừng. Người giữ sổ sửa nhầm, hoặc bị tấn công, thì mọi người cùng chịu. Câu hỏi của Bitcoin (đồng tiền mã hóa đầu tiên, mục 1.4) là: có thể chặn chi tiêu hai lần mà không cần một người giữ sổ chung không?

This works well, but the whole system leans on one party. If the ledger stops, the whole network stops. If the keeper errs or is attacked, everybody suffers. The question behind Bitcoin (the first cryptocurrency, section 1.4) is: can double spending be stopped without a single common ledger keeper?

Các thử nghiệm trước Bitcoin – *Experiments before Bitcoin*

Trước Bitcoin đã có nhiều lần thử. Mỗi lần giải một nửa bài toán và vướng ở nửa còn lại. Bảng sau chỉ nêu ý chính; bạn không cần nhớ ngày tháng.

Many attempts came before Bitcoin. Each solved half the problem and stuck on the other half. The table gives only the main idea; you do not need to remember dates.

Tên *Name*	**Ý chính** *Main idea*	**Còn vướng ở đâu** *Where it stuck*
DigiCash (eCash) của David Chaum *David Chaum's DigiCash (eCash)*	Tiền số giữ riêng tư cho người dùng; công ty giữ sổ để phát hiện chi tiêu hai lần *Digital cash that kept users' privacy; the company kept the ledger to catch double spending*	Khó thuyết phục cửa hàng và ngân hàng chấp nhận; công ty thất bại *Hard to persuade shops and banks to accept it; the company failed*
e-gold *e-gold*	Tiền số có vàng trong kho làm đối ứng, một công ty phát hành và giữ sổ *Digital money backed by gold in a vault, with one firm issuing and keeping the ledger*	Mọi thứ nằm ở một công ty, nên người dùng phải tin công ty *Everything sat with one firm, so users had to trust it*
b-money của Wei Dai *Wei Dai's b-money*	Đề xuất nhiều người cùng giữ sổ *A proposal for many people to keep the ledger together*	Dừng ở ý tưởng, chưa có cách để mọi người cùng đồng ý chạy thật *It stayed an idea, with no working way for everyone to agree*
Bit Gold của Nick Szabo *Nick Szabo's Bit Gold*	Đề xuất dùng bài toán tính toán tốn công để tạo ra "vàng số" *A proposal to use costly computing puzzles to create "digital gold"*	Dừng ở ý tưởng, chưa thành hệ thống hoàn chỉnh *It stayed an idea and never became a full system*
Hashcash của Adam Back *Adam Back's Hashcash*	Người gửi phải giải một bài toán tính toán tốn công, dùng để chống thư rác *Senders must solve a costly computing puzzle, used against spam*	Không phải tiền; ý bài toán tốn công được Bitcoin dùng lại *Not money; Bitcoin reused its costly-puzzle idea*

Điểm chung: hoặc có một bên giữ sổ như ngân hàng, hoặc chưa có cách để người lạ đồng ý với nhau về thứ tự giao dịch. Bitcoin ghép các mảnh có sẵn thành một hệ chạy được: chữ ký điện tử để chứng minh chủ sở hữu, bài toán tốn công kiểu Hashcash, và các trang sổ nối nhau bằng dấu vân tay (mục 1.4).

The common thread: either one party keeps the ledger like a bank, or there is no way for strangers to agree on the order of transactions. Bitcoin assembled existing pieces into a working system: digital signatures to prove ownership, Hashcash-style costly puzzles, and ledger pages linked by fingerprints (section 1.4).

1.4. Sách trắng Bitcoin, khối nguyên thủy và chuỗi khối – *1.4. The Bitcoin white paper, the genesis block and the blockchain*

Tháng 10 năm 2008, một tác giả lấy bút danh Satoshi Nakamoto công bố sách trắng (white paper, tài liệu mô tả thiết kế) về hệ thanh toán điện tử ngang hàng, không cần bên trung gian. Đó là tài liệu Nakamoto 2008. Ngày 3/1/2009, khối đầu tiên của chuỗi, gọi là **khối nguyên thủy** (genesis block), được tạo ra. Giao dịch đầu tiên trong khối ghi kèm dòng chữ "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks", tựa một bài báo cùng ngày.

*In October 2008, an author using the pseudonym Satoshi Nakamoto published a white paper (a document describing a design) for a peer-to-peer electronic payment system with no middleman. That is Nakamoto 2008. On 3 January 2009 the first block of the chain, the **genesis block**, was created. The first transaction in it carries the text "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks", the title of a newspaper article of that day.*

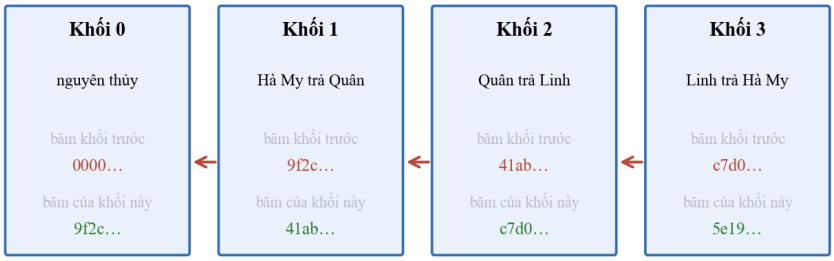
Để hiểu **chuỗi khối** (blockchain), hãy hình dung cuốn sổ ghi nợ chung của cả xóm. Mỗi người trong xóm giữ một bản sao. Cứ một lúc, người ta gom các khoản mới vào một trang, đóng dấu vân tay của trang trước lên trang mới rồi cho cả xóm chép. Muốn sửa một khoản cũ, bạn phải sửa trang chứa nó, mà dấu vân tay của trang đó nằm ở trang kế, trang kế lại nằm ở trang sau nữa, nên cả dãy phía sau lộ ra bị sửa. Và bạn còn phải sửa bản sao của hàng trăm người khác.

*To grasp a **blockchain**, picture a village's shared debt book. Everyone in the village holds a copy. Every so often, people gather the new entries onto one page, stamp the fingerprint of the previous page on the new one, and the whole village copies it. To change an old entry you must change the page holding it, but that page's fingerprint sits on the next page, and the next on the one after, so the whole run behind it shows signs of tampering. And you would have to alter hundreds of other people's copies too.*

Ba từ cần giải thích. **Khối** (block) là một trang của sổ, chứa nhóm giao dịch. **Hàm băm** (hash function) là phép biến mọi dữ liệu thành một dãy ký tự độ dài cố định, như dấu vân tay: đổi một chữ trong dữ liệu thì dấu vân tay khác hẳn (Chương 2). **Sổ cái phân tán** (distributed ledger technology, DLT) là sổ mà nhiều bên cùng giữ bản sao và cùng kiểm. Chuỗi khối là một kiểu sổ cái phân tán, trong đó các khối nối nhau bằng mã băm.

*Three words need explaining. A **block** is one page of the ledger, holding a group of transactions. A **hash function** turns any data into a string of fixed length, like a fingerprint: change one letter of the data and the fingerprint becomes entirely different (Chapter 2). A **distributed ledger***

(distributed ledger technology, DLT) is a ledger that many parties hold copies of and check together. A blockchain is one kind of distributed ledger, in which blocks are linked by hashes.



Hình 1.3. Hình 1.3. Mỗi hộp là một khối: dòng đỏ là dấu vân tay của khối trước, dòng xanh lá là dấu vân tay của chính nó. Mũi tên đỏ chỉ ngược về khối trước; sửa khối 1 thì dòng xanh của khối 1 đổi, khớp với dòng đỏ của khối 2 bị vỡ.

Figure 1.3. *Figure 1.3. Each box is a block: the red line is the previous block's fingerprint, the green line its own. Red arrows point back to the previous block; edit block 1 and its green line changes, so the match with block 2's red line breaks.*

Một giao dịch mã hóa đi qua những đâu – *Where a crypto transaction travels*

Dữ kiện: Hà My chuyển 0,001 BTC (BTC là ký hiệu đơn vị bitcoin) từ ví này sang ví khác của chính cô, chỉ để làm quen. Các bước dưới là bức tranh tổng; từng bước được mổ xẻ ở Chương 3.

Data: Ha My moves 0.001 BTC (BTC is the symbol for the bitcoin unit) from one of her wallets to another of her own, just to get used to it. The steps are the overall picture; Chapter 3 dissects each.

1. Hà My nhập địa chỉ nhận (một dãy ký tự đóng vai số tài khoản) và số tiền. Ứng dụng ví dùng khóa bí mật của cô, một mật khẩu dài chỉ cô giữ, để ký lệnh. Chữ ký chứng minh cô là chủ mà không lộ khóa.
   Ha My enters the receiving address (a string of characters acting as an account number) and the amount. The wallet app uses her secret key, a long password only she holds, to sign the order. The signature proves she is the owner without revealing the key.
2. Lệnh đã ký được phát tới các máy trong mạng. Mỗi máy kiểm chữ ký và kiểm số tiền này chưa tiêu trước đó.
   The signed order is broadcast to machines on the network. Each checks the signature and that this money has not been spent before.
3. Một máy gom lệnh hợp lệ vào khối mới, đính dấu vân tay của khối trước và thêm khối vào chuỗi theo quy tắc của mạng.
   One machine collects valid orders into a new block, attaches the previous block's fingerprint and adds the block to the chain under the network's rules.

4. Các máy khác kiểm khối rồi chép về sổ của mình. Khi đó giao dịch có 1 xác nhận.
   Other machines check the block and copy it to their ledgers. The transaction then has 1 confirmation.
5. Mỗi khối mới nối sau đó thêm một xác nhận. Với Bitcoin, mục tiêu là một khối khoảng 10 phút; người nhận thường chờ khoảng 6 xác nhận, tức chừng một giờ, mới coi là chắc.
   Each later block adds one confirmation. In Bitcoin the target is one block about every 10 minutes; recipients usually wait for about 6 confirmations, roughly an hour, before treating it as final.

Chuỗi khối không phải là Bitcoin. Bitcoin là một hệ cụ thể dùng chuỗi khối; còn chuỗi khối là kỹ thuật ghi sổ mà nhiều hệ dùng, kể cả những hệ không phát hành đồng tiền nào (Chương 8).

A blockchain is not Bitcoin. Bitcoin is one particular system built on a blockchain; the blockchain is a record-keeping technique many systems use, including some that issue no coin at all (Chapter 8).

1.5. Phân loại tài sản mã hóa – *1.5. Classifying crypto-assets*

Khi nghe "tiền mã hóa", nhiều bạn nghĩ chỉ có Bitcoin. Thực tế có nhiều loại với mục đích khác nhau. Phân loại quan trọng vì mỗi loại chịu quy định khác nhau, và vì nhìn nhầm loại là nhìn nhầm rủi ro.

When you hear "cryptocurrency", you may think only of Bitcoin. In fact there are several kinds with different purposes. Classifying matters because each kind falls under different rules, and mistaking the kind means mistaking the risk.

Đồng tiền mã hóa gốc (native coin) là đơn vị của chính một chuỗi khối, dùng để trả phí và thưởng cho máy giữ sổ. **Token tiện ích** (utility token) cho quyền dùng một dịch vụ, như phiếu đổi 10 kg cà phê. **Token chứng khoán** (security token) đại diện quyền kiểu cổ phần, trái phiếu. **Đồng ổn định** (stablecoin) cố giữ giá gần một tài sản tham chiếu như đồng đô la. **NFT** (non-fungible token, token không thay thế được) là token độc nhất, như giấy chứng nhận cho một tác phẩm. **CBDC** là dạng số của tiền pháp định (mục 1.2).

*A **native coin** is the unit of a blockchain itself, used to pay fees and reward the machines that keep the ledger. A **utility token** gives the right to use a service, like a voucher for 10 kg of coffee. A **security token** represents rights like a share or a bond. A **stablecoin** tries to hold its price near a reference asset such as a dollar. An **NFT** (non-fungible token) is a one-of-a-kind token, like a certificate for a single artwork. A **CBDC** is a digital form of legal tender (section 1.2).*

Loại *Kind*	**Dùng để làm gì** *Used for*	**Ví dụ trong sách** *Example in this book*	**Có phải tài sản mã hóa theo Luật 71 không** *Is it a crypto-asset under Law 71*
Đồng gốc *Native coin*	Trả phí mạng, thưởng cho máy giữ sổ *Paying network fees and rewarding ledger keepers*	Chuỗi "Sen Vàng" có đồng gốc SVG *The "Sen Vang" chain has the native coin SVG*	Thường có, nếu không rơi vào phần loại trừ *Usually yes, unless caught by the exclusions*
Token tiện ích *Utility token*	Đổi lấy hàng hóa hoặc dịch vụ *Redeemable for goods or services*	Token LVC của Lâm Viên: 1 LVC đổi 1 kg cà phê *Lam Vien's LVC token: 1 LVC for 1 kg of coffee*	Thường có *Usually yes*
Token chứng khoán *Security token*	Đại diện cổ phần, trái phiếu *Representing shares or bonds*	Token đại diện cổ phần Lâm Viên *A token representing Lam Vien shares*	Không: Điều 47 loại trừ chứng khoán *No: Article 47 excludes securities*
Đồng ổn định *Stablecoin*	Giữ giá gần tài sản tham chiếu để thanh toán, giao dịch *Holding a price near a reference asset for payments and trading*	VNDx, đồng tự đặt gắn với đồng Việt Nam *VNDx, an invented coin pegged to the dong*	Xét từng trường hợp theo định nghĩa chung *Judged case by case under the general definition*
NFT *NFT*	Chứng nhận quyền với một vật độc nhất *Certifying rights over a unique item*	Chứng nhận số cho một bức ảnh vườn cà phê *A digital certificate for a coffee-farm photo*	Xét từng trường hợp theo định nghĩa chung *Judged case by case under the general definition*
CBDC *CBDC*	Tiền pháp định ở dạng số *Legal tender in digital form*	Dạng số của đồng, do ngân hàng trung ương phát hành *The digital form of the dong, issued by the central bank*	Không: dạng số của tiền pháp định bị loại trừ *No: digital forms of legal tender are excluded*

Cột cuối cho thấy một điều bất ngờ: tên "token" hay "tiền mã hóa" không quyết định gì. Điều quyết định là thứ đó thực chất đại diện cho cái gì. Một token đại diện cổ phần vẫn là chứng khoán, dù nó chạy trên chuỗi khối.

The last column shows something surprising: the label "token" or "cryptocurrency" settles nothing. What counts is what the thing actually represents. A token that represents shares is still a security, even though it runs on a blockchain.

Ví dụ làm mẫu: Lâm Viên xếp loại bốn thứ – ***Worked example: Lam Vien classifies four items***

Dữ kiện: Công ty Cà phê Lâm Viên đang xem bốn món. (a) Phiếu LVC, mỗi phiếu đổi 1 kg cà phê. (b) Token đại diện 1% cổ phần công ty. (c) VNDx, mỗi VNDx do công ty phát hành đổi 1 đồng. (d) Chứng nhận số độc nhất cho lô cà phê đặc biệt.

Data: Lam Vien Coffee Company is looking at four items. (a) The LVC voucher, each redeemable for 1 kg of coffee. (b) A token representing 1% of the company's shares. (c) VNDx, each unit issued by the company redeemable for 1 dong. (d) A one-of-a-kind digital certificate for a special coffee lot.

1. Hỏi mỗi món đại diện cho cái gì. (a) quyền nhận hàng. (b) cổ phần. (c) một đồng. (d) một vật độc nhất.
   Ask what each item stands for. (a) a right to goods. (b) shares. (c) one dong. (d) a unique item.
2. Gọi tên loại. (a) token tiện ích. (b) token chứng khoán. (c) đồng ổn định. (d) NFT.
   Name the kind. (a) a utility token. (b) a security token. (c) a stablecoin. (d) an NFT.
3. Đối chiếu Điều 47 khoản 2: (b) đại diện cổ phần là chứng khoán nên không thuộc tài sản mã hóa. Ba món còn lại xét theo định nghĩa chung.
   Check Article 47, clause 2: (b) represents shares, a security, so it is not a crypto-asset. The other three are judged under the general definition.

Nghĩa là món (b) sẽ đi theo luật chứng khoán chứ không theo khuôn tài sản mã hóa, dù nó ra đời trên chuỗi khối.

So item (b) follows securities law rather than the crypto-asset framework, though it was born on a blockchain.

> **PHẢI THUỘC / MEMORISE –** Phân loại theo thứ được đại diện, không theo cái tên. Token đại diện chứng khoán không phải tài sản mã hóa theo Luật 71 Điều 47; dạng số của tiền pháp định (CBDC) cũng bị loại trừ.
> *Classify by what is represented, not by the name. A token representing a security is not a crypto-asset under Law 71, Article 47; digital forms of legal tender (CBDC) are excluded too.*

1.6. Khái niệm pháp lý ở Việt Nam: tài sản số, tài sản ảo, tài sản mã hóa – *1.6. Vietnamese legal concepts: digital assets, virtual assets, crypto-assets*

Bạn sẽ gặp ba cụm từ gần nhau trong luật: tài sản số, tài sản ảo, tài sản mã hóa. Chúng lồng nhau như ba vòng tròn, từ rộng đến hẹp. Đi từ ngoài vào trong sẽ dễ nhất.

You will meet three close phrases in the law: digital assets, virtual assets and crypto-assets. They nest like three circles, from wide to narrow. Moving from the outside in is the easiest route.

Vòng ngoài là **tài sản** theo Bộ luật Dân sự năm 2015, Điều 105 khoản 1: "Tài sản là vật, tiền, giấy tờ có giá và quyền tài sản." Vòng giữa là **tài sản số**, Luật Công nghiệp công nghệ số số 71/2025/QH15, Điều 46: tài sản theo Bộ luật Dân sự, "được thể hiện dưới dạng dữ liệu số, được tạo lập, phát hành, lưu trữ, chuyển giao và xác thực bởi công nghệ số trên môi trường điện tử". Vòng trong là hai loại ở Điều 47 khoản 2: **tài sản ảo** (dùng để trao đổi hoặc đầu tư) và **tài sản mã hóa**, là loại tài sản số "sử dụng công nghệ mã hóa

hoặc công nghệ số có chức năng tương tự để xác thực" trong lúc tạo lập, phát hành, lưu trữ, chuyển giao.

*The outer ring is **property** under the 2015 Civil Code, Article 105, clause 1: "Property comprises objects, money, valuable papers and property rights." The middle ring is a **digital asset**, Law on the Digital Technology Industry No. 71/2025/QH15, Article 46: property under the Civil Code "expressed as digital data, created, issued, stored, transferred and authenticated by digital technology in an electronic environment". The inner ring is the two kinds in Article 47, clause 2: **virtual assets** (used for exchange or investment) and **crypto-assets**, a kind of digital asset "using cryptography or similar digital technology to authenticate" during creation, issuance, storage and transfer.*

Cả hai loại ở vòng trong đều "không bao gồm chứng khoán, các dạng số của tiền pháp định và tài sản tài chính khác". Vì thế token đại diện cổ phần hay CBDC không phải tài sản mã hóa theo luật này (mục 1.5). Luật có hiệu lực từ 1/1/2026 (Điều 50 khoản 1). Điều 48 khoản 1 điểm đ giao Chính phủ quy định điều kiện kinh doanh dịch vụ tài sản mã hóa.

Both inner kinds "exclude securities, digital forms of legal tender and other financial assets". So a token representing shares, or a CBDC, is not a crypto-asset under this law (section 1.5). The law took effect on 1 January 2026 (Article 50, clause 1). Article 48, clause 1, point đ leaves the conditions for doing business in crypto-asset services to the Government.

Bậc *Level*	**Văn bản** *Source*	**Nói gì** *What it says*
1. Tài sản *1. Property*	Bộ luật Dân sự 2015, Điều 105 *Civil Code 2015, Article 105*	Vật, tiền, giấy tờ có giá, quyền tài sản *Objects, money, valuable papers, property rights*
2. Tài sản số *2. Digital asset*	Luật 71/2025/QH15, Điều 46 *Law 71/2025/QH15, Article 46*	Tài sản dạng dữ liệu số, xác thực bằng công nghệ số *Property as digital data, authenticated by digital technology*
3a. Tài sản ảo *3a. Virtual asset*	Luật 71, Điều 47 khoản 2 điểm a *Law 71, Article 47(2)(a)*	Dùng để trao đổi hoặc đầu tư; loại trừ chứng khoán, dạng số của tiền pháp định *For exchange or investment; excludes securities and digital forms of legal tender*
3b. Tài sản mã hóa *3b. Crypto-asset*	Luật 71, Điều 47 khoản 2 điểm b *Law 71, Article 47(2)(b)*	Xác thực bằng công nghệ mã hóa hoặc tương tự; loại trừ như trên *Authenticated with cryptography or similar; same exclusions*
4. Dịch vụ *4. Services*	Luật 71, Điều 48; Nghị quyết 05/2025/NQ-CP, Điều 3 *Law 71, Article 48; Resolution 05/2025/NQ-CP, Article 3*	Chính phủ quy định điều kiện; Nghị quyết 05 thí điểm thị trường *The Government sets conditions; Resolution 05 pilots a market*

Nghị quyết 05/2025/NQ-CP (hiệu lực 9/9/2025, thí điểm 5 năm) nhắc lại hai định nghĩa trên ở Điều 3 và đặt khung thí điểm: tổ chức phát hành là doanh nghiệp Việt Nam, tài sản cơ sở là tài sản thực (Điều 5). Việc chào bán, phát hành chỉ dành cho nhà đầu tư nước

ngoài (Điều 6 khoản 1). Điều 7 khoản 2 nói nhà đầu tư trong nước giao dịch ngoài tổ chức được cấp phép sẽ bị xử lý, từ 6 tháng sau khi tổ chức đầu tiên được cấp phép. Chương 10 đi sâu từng điều kiện.

Resolution 05/2025/NQ-CP (in force from 9 September 2025, a five-year pilot) repeats the two definitions in Article 3 and sets the pilot frame: issuers are Vietnamese enterprises and underlying assets are real assets (Article 5). Offers and issuance are open only to foreign investors (Article 6, clause 1). Article 7, clause 2 says domestic investors trading outside licensed firms will be dealt with, starting 6 months after the first firm is licensed. Chapter 10 goes through each condition.

Tài sản mã hóa không phải phương tiện thanh toán – ***Crypto-assets are not a means of payment***

Được công nhận là tài sản không có nghĩa là được dùng để trả tiền. Luật Ngân hàng Nhà nước (văn bản hợp nhất 141/2026), Điều 17 khoản 2, viết: "Tiền giấy, tiền kim loại do Ngân hàng Nhà nước phát hành là phương tiện thanh toán hợp pháp". Tài sản mã hóa không nằm trong danh sách đó. Dùng tài sản mã hóa để trả tiền hàng hóa, dịch vụ có thể bị xử lý theo quy định về phương tiện thanh toán không hợp pháp (Nghị định 340/2025/NĐ-CP, Điều 30 khoản 6 điểm d). Nên khi Công ty Lâm Viên nhận đơn hàng, tiền hàng phải đi bằng đồng qua ngân hàng.

Being recognised as property does not mean it may be used to pay. The Law on the State Bank (consolidated text 141/2026), Article 17, clause 2, reads: "Banknotes and coins issued by the State Bank are lawful means of payment". Crypto-assets are not on that list. Using crypto-assets to pay for goods or services can be dealt with under the rules on unlawful means of payment (Decree 340/2025/ND-CP, Article 30, clause 6, point d). So when Lam Vien Company takes an order, payment must travel in dong through a bank.

> **LẬP LUẬN ỦNG HỘ – PHẢN ĐỐI / FOR AND AGAINST** – **Ủng hộ** việc công nhận tài sản nhưng không cho thanh toán: người dân có quyền sở hữu rõ, còn đồng tiền quốc gia vẫn là phương tiện duy nhất, giữ ổn định tiền tệ. **Phản đối**: người đã nắm tài sản mã hóa phải đổi sang đồng mới tiêu được, và giá dao động trong lúc chờ đổi gây thiệt hại. Hai phía đều có lý; bạn cần biết cả hai để trình bày được quy định.
>
> ***For** recognising property but not payment: people get a clear ownership right, while the national currency stays the only means of payment, protecting monetary stability. **Against**: holders must convert to dong before spending, and price swings while waiting can cause losses. Both sides have a point; you need both to explain the rule.*

1.7. Năm đặc điểm của tài sản mã hóa: lợi ích và cái giá – *1.7. Five features of crypto-assets: benefits and costs*

Mỗi đặc điểm sau có hai mặt. Đọc kỹ mặt thứ hai, vì đó là nơi người mới thường vấp.

Each feature has two faces. Read the second face carefully, since that is where beginners stumble.

Phi tập trung (decentralisation): không một bên nào nắm quyền ghi sổ. Lợi: không có một điểm hỏng duy nhất. Giá: không có ai để gọi khi có sự cố. **Minh bạch**: mọi giao dịch trên chuỗi công khai ai cũng đọc được, nên kiểm tra không cần xin phép ai. Giá: lịch sử

chi tiêu của một địa chỉ cũng ai cũng xem được. **Bút danh** (pseudonymity): bạn dùng mã riêng thay vì tên thật. Lợi: không phải đưa tên khi tạo ví. Giá: bút danh không phải ẩn danh, vì phân tích dữ liệu có thể nối mã với người thật (Chương 5). **Khó sửa**: giao dịch đã ghi vào nhiều khối thì khó đảo. Lợi: không ai lén sửa lịch sử. Giá: chuyển nhầm là không đòi lại được. **Toàn cầu**: mạng không có biên giới, chuyển cho người ở nước khác nhanh. Giá: pháp luật mỗi nước một khác, nên vừa tiện vừa rủi ro về tuân thủ.

***Decentralisation**: no single party controls writing to the ledger. Benefit: no single point of failure. Cost: nobody to phone when something breaks. **Transparency**: every on-chain transaction is public and anyone can read it, so checking needs nobody's permission. Cost: an address's spending history is visible to all. **Pseudonymity**: you use a private code instead of your real name. Benefit: no name needed to make a wallet. Cost: a pseudonym is not anonymity, since data analysis can link a code to a real person (Chapter 5). **Hard to alter**: once a transaction sits under many blocks it is very hard to reverse. Benefit: nobody quietly rewrites history. Cost: a wrong transfer cannot be recovered. **Global reach**: the network has no borders, so sending to someone abroad is fast. Cost: laws differ by country, so it is convenient and also a compliance risk.*

Đặc điểm *Feature*	**Ưu** *Advantage*	**Nhược** *Disadvantage*	**Hà My gặp ở đâu** *Where Ha My meets it*
Phi tập trung *Decentralised*	Không có điểm hỏng duy nhất *No single point of failure*	Không có nơi khiếu nại *Nowhere to complain*	Gửi nhầm địa chỉ, không ai hoàn lại *A wrong address, and nobody refunds*
Minh bạch *Transparent*	Ai cũng kiểm được sổ *Anyone can audit the ledger*	Lịch sử chi tiêu bị xem được *Spending history can be viewed*	Bạn bè tra được số dư địa chỉ cô cho họ *Friends can look up the balance of an address she shared*
Bút danh *Pseudonymous*	Không cần tên khi tạo ví *No name needed to open a wallet*	Có thể bị nối với người thật *Can be linked to a real person*	Địa chỉ cô dùng ở sàn gắn với tên của cô *An address she uses on an exchange ties to her name*
Khó sửa *Hard to alter*	Lịch sử đáng tin *A trustworthy history*	Không đảo ngược được giao dịch sai *Wrong transactions cannot be undone*	Chuyển sai số tiền là mất *A wrong amount is lost*
Toàn cầu *Global*	Chuyển nhanh qua biên giới *Fast cross-border transfers*	Mỗi nước một luật *A different law in each country*	Một dịch vụ ở nước ngoài có thể không hợp pháp tại Việt Nam *A service abroad may be unlawful in Vietnam*

LỖI HAY GẶP / COMMON MISTAKE – Cho rằng "khó sửa" nghĩa là "không bao giờ sai". Chuỗi khối chỉ làm khó sửa lịch sử; dữ liệu nhập vào sai từ đầu thì vẫn nằm đó mãi.

> *Assuming "hard to alter" means "never wrong". A blockchain only makes history hard to rewrite; data entered wrongly from the start stays there for good.*

1.8. Đơn vị và quy đổi: satoshi, wei, gwei – *1.8. Units and conversion: satoshi, wei, gwei*

Bạn có thể mua một ly cà phê bằng một phần nhỏ của bitcoin. Để ghi những phần nhỏ đó mà không phải viết nhiều chữ số 0, người ta đặt đơn vị nhỏ riêng, như đồng và xu nhưng sâu hơn. **Satoshi** là đơn vị nhỏ nhất của bitcoin: 1 BTC = 100.000.000 satoshi. **Wei** là đơn vị nhỏ nhất của ether (ETH), đồng gốc của mạng Ethereum, một chuỗi khối khác ngoài Bitcoin (Chương 6): 1 ETH = 10^{18} wei. **Gwei** là một tỷ wei, dùng để ghi phí: 1 ETH = 10^{9} gwei. **Gas** là đơn vị đo công sức tính toán mà mạng Ethereum tính cho mỗi giao dịch; mỗi gas có một giá tính bằng gwei, phí = số gas dùng ∗ giá gas.

*You may pay for a coffee with a small slice of a bitcoin. To write such slices without a string of zeros, people define small units, like dong and cents but finer. The **satoshi** is the smallest unit of bitcoin: 1 BTC = 100,000,000 satoshi. The **wei** is the smallest unit of ether (ETH), the native coin of the Ethereum network, a blockchain separate from Bitcoin (Chapter 6): 1 ETH = 10^{18} wei. The **gwei** is a billion wei, used for quoting fees: 1 ETH = 10^{9} gwei. **Gas** measures the computing effort the Ethereum network charges for each transaction; each unit of gas has a price quoted in gwei, and the fee = gas used ∗ gas price.*

Đơn vị *Unit*	**Bằng bao nhiêu** *Equals*	**Dùng để** *Used for*
1 BTC *1 BTC*	100.000.000 satoshi *100,000,000 satoshi*	Ghi số bitcoin lớn *Large bitcoin amounts*
1 satoshi *1 satoshi*	0,00000001 BTC *0.00000001 BTC*	Ghi số nhỏ và phí *Small amounts and fees*
1 ETH *1 ETH*	10^{9} gwei = 10^{18} wei *10^{9} gwei = 10^{18} wei*	Ghi số ether lớn *Large ether amounts*
1 gwei *1 gwei*	10^{-9} ETH = 10^{9} wei *10^{-9} ETH = 10^{9} wei*	Ghi phí gas *Quoting gas fees*

Tổng cung bitcoin được thiết kế tối đa khoảng 21 triệu BTC (Chương 4). Chia 21 triệu cho 100.000.000 phần mỗi đồng cho thấy số satoshi cả hệ thống là lớn, nên việc ghi bằng satoshi là hợp lý.

The bitcoin supply is designed to reach a maximum of about 21 million BTC (Chapter 4). With 100,000,000 satoshi in each coin, the system holds a very large count of satoshi, so quoting in satoshi is sensible.

Ví dụ làm mẫu: Hà My nhận 2.350.000 satoshi – *Worked example: Ha My receives 2,350,000 satoshi*

Dữ kiện: tỷ giá đề bài đặt là 1 BTC = 1.250.000.000 đồng. Hà My nhận 2.350.000 satoshi. Ở một mạng khác, giao dịch tiêu 21.000 gas, giá gas 25 gwei mỗi gas. Hãy đổi các số ra BTC, đồng, gwei, wei, ETH.

Data: the exercise sets the rate at 1 BTC = 1,250,000,000 dong. Ha My receives 2,350,000 satoshi. On another network a transaction uses 21,000 gas at 25 gwei per gas. Convert the figures into BTC, dong, gwei, wei and ETH.

1. Satoshi ra BTC: chia cho 100.000.000. 2.350.000 / 100.000.000 = 0,0235 BTC.
   Satoshi to BTC: divide by 100,000,000. 2,350,000 / 100,000,000 = 0.0235 BTC.
2. BTC ra đồng: nhân tỷ giá. 0,0235 ∗ 1.250.000.000 = 29.375.000 đồng.
   BTC to dong: multiply by the rate. 0.0235 ∗ 1,250,000,000 = 29,375,000 dong.
3. Phí gas ra gwei: nhân gas với giá gas. 21.000 ∗ 25 = 525.000 gwei.
   Gas fee in gwei: multiply gas by the gas price. 21,000 ∗ 25 = 525,000 gwei.
4. Gwei ra wei: nhân 10^9. 525.000 ∗ 10^9 = 525.000.000.000.000 wei.
   Gwei to wei: multiply by 10^9. 525,000 ∗ 10^9 = 525,000,000,000,000 wei.
5. Gwei ra ETH: chia 10^9. 525.000 / 10^9 = 0,000525 ETH.
   Gwei to ETH: divide by 10^9. 525,000 / 10^9 = 0.000525 ETH.

Nghĩa là Hà My nhận 0,0235 BTC, tương đương 29.375.000 đồng theo tỷ giá đề bài, và giao dịch bên mạng kia tốn 0,000525 ETH tiền phí.

So Ha My receives 0.0235 BTC, equal to 29,375,000 dong at the exercise's rate, and the transaction on the other network costs 0.000525 ETH in fees.

> **LỖI HAY GẶP / COMMON MISTAKE –** Đọc 1.000.000 satoshi thành 1 BTC, sai gấp 100 lần: 1.000.000 satoshi chỉ bằng 0,01 BTC. Nhớ mốc 100.000.000 và đếm đủ số chữ số 0 trước khi chuyển.
> *Reading 1,000,000 satoshi as 1 BTC, wrong by a factor of 100: 1,000,000 satoshi is only 0.01 BTC. Remember 100,000,000 and count every zero before sending.*

$$\text{BTC} = \text{satoshi} \,/\, 100.000.000 \tag{1.1}$$

$$\text{wei} = \text{gwei} * 10^9, \quad \text{ETH} = \text{gwei} \,/\, 10^9 \tag{1.2}$$

1.9. Lợi suất và biến động giá, so với gửi tiết kiệm – *1.9. Returns and price swings, against a savings deposit*

Giá tài sản mã hóa thay đổi từng phút. Để nói về chuyện đó bằng con số, ta cần ba thước đo đơn giản. **Lợi suất** (return) là phần trăm thay đổi giá trong một kỳ. **Độ biến động** (volatility) cho biết lợi suất dao động mạnh hay nhẹ quanh mức trung bình; đo bằng độ lệch chuẩn. **Sụt giảm tối đa** (maximum drawdown) là mức giảm sâu nhất từ một đỉnh xuống đáy sau đó, thứ mà người cầm giữ thấy rõ nhất trên đường đi.

*Crypto-asset prices change by the minute. To talk about it in numbers we need three simple yardsticks. **Return** is the percentage change in price over a period. **Volatility** tells whether returns swing hard or gently around their average, measured by standard deviation. **Maximum drawdown** is the deepest fall from a peak to a later low, the thing holders feel most along the way.*

Ví dụ làm mẫu: token LVC trong 12 tháng – ***Worked example: the LVC token over 12 months***

Dữ kiện (do đề bài đặt, không phải giá thật): giá cuối tháng của token LVC, tháng 0 đến tháng 12, và tiền gửi tiết kiệm lãi 6%/năm gửi 12 tháng. Bảng sau cho giá và lợi suất từng tháng.

Data (set by the exercise, not real prices): LVC's month-end prices from month 0 to month 12, and a savings deposit at 6% a year for 12 months. The table gives the price and each month's return.

Tháng *Month*	**Giá (đồng)** *Price (dong)*	**Lợi suất tháng** *Monthly return*
0	10.000 *10,000*	–
1	11.200 *11,200*	12,0% *12.0%*
2	9.800 *9,800*	-12,5% *-12.5%*
3	10.500 *10,500*	7,1% *7.1%*
4	12.600 *12,600*	20,0% *20.0%*
5	11.900 *11,900*	-5,6% *-5.6%*
6	8.900 *8,900*	-25,2% *-25.2%*
7	9.500 *9,500*	6,7% *6.7%*
8	10.800 *10,800*	13,7% *13.7%*
9	13.200 *13,200*	22,2% *22.2%*
10	12.100 *12,100*	-8,3% *-8.3%*
11	11.400 *11,400*	-5,8% *-5.8%*
12	12.000 *12,000*	5,3% *5.3%*

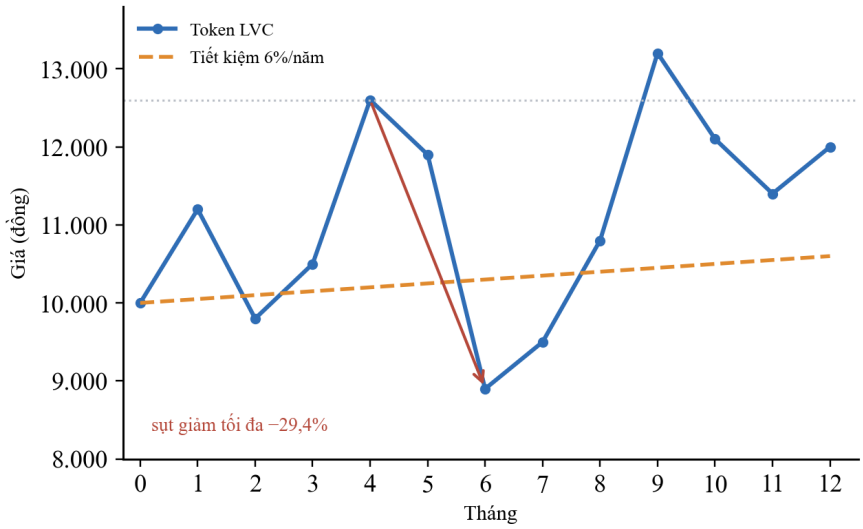
Đọc bảng: tháng 6 là tháng tệ nhất (-25,2%), tháng 9 là tháng tốt nhất (22,2%). Giá nhảy lên xuống mạnh dù cuối năm vẫn cao hơn đầu năm.

Reading the table: month 6 is the worst month (-25.2%) and month 9 the best (22.2%). The price jumps up and down hard even though the year ends higher than it began.

1. Lợi suất tổng = giá cuối / giá đầu − 1 = 12.000 / 10.000 − 1 = 20,0%.
   Total return = last price / first price − 1 = 12,000 / 10,000 − 1 = 20.0%.
2. Độ biến động: lấy trung bình lợi suất tháng (2,47%), tính độ lệch chuẩn mẫu của 12 lợi suất: 14,1% mỗi tháng.
   Volatility: take the mean monthly return (2.47%) and the sample standard deviation of the 12 returns: 14.1% a month.
3. Sụt giảm tối đa: đỉnh chạy 12.600 (tháng 4), đáy 8.900 (tháng 6). 8.900 / 12.600 − 1 = -29,4%.
   Maximum drawdown: running peak 12,600 (month 4), low 8,900 (month 6). 8,900 / 12,600 − 1 = -29.4%.
4. Tiết kiệm: 10.000 ∗ (1 + 6%) = 10.600 đồng, lợi suất 6,0%.
   Savings: 10,000 ∗ (1 + 6%) = 10,600 dong, a return of 6.0%.

Theo chuỗi này, LVC hơn tiết kiệm 14,0 điểm phần trăm sau 12 tháng, nhưng có lúc mất 29,4% so với đỉnh, và mỗi tháng dao động chừng 14,1%. Tiền gửi tiết kiệm biết trước kết quả; token thì không. Chuỗi 12 điểm là quá ngắn để nói gì về tương lai.

On this series, LVC beats the deposit by 14.0 percentage points after 12 months, but at one point lost 29.4% from its peak, and swings about 14.1% a month. A savings deposit has a known outcome; the token does not. A 12-point series is too short to say anything about the future.



Hình 1.4. Hình 1.4. Đường xanh là giá LVC lên xuống mạnh; đường cam đứt là tiền gửi tiết kiệm tăng đều. Mũi tên đỏ chỉ đoạn sụt từ đỉnh tháng 4 xuống đáy tháng 6.

Figure 1.4. *Figure 1.4. The blue line is LVC's price, swinging hard; the dashed orange line is the savings deposit growing steadily. The red arrow marks the fall from the month 4 peak to the month 6 low.*

LỖI HAY GẶP / COMMON MISTAKE – Lấy trung bình cộng lợi suất tháng (2,47%) nhân 12 rồi tưởng là lợi suất cả năm: ra 29,7%, trong khi thực tế là 20,0%. Lợi suất nhiều kỳ phải nhân dồn (1 + r) lên, không cộng.

> *Multiplying the mean monthly return (2.47%) by 12 and calling it the annual return: that gives 29.7%, while the actual is 20.0%. Multi-period returns compound by multiplying (1 + r), not by adding.*

$$r = (P_1 - P_0) / P_0 \quad (1.3)$$

$$\sigma = \sqrt{(\Sigma (r_i - \bar{r})^2 / (n - 1))} \quad (1.4)$$

$$MDD = \min (P_t / \text{đỉnh chạy đến } t - 1) \quad (1.5)$$

1.10. Vị trí việc làm trong lĩnh vực tiền số và blockchain – *1.10. Jobs in digital money and blockchain*

Anh Quân kể: ở công ty công nghệ tài chính nơi anh làm, ít ai chỉ "mua bán coin". Phần lớn việc là giữ cho hệ thống chạy đúng, an toàn và hợp pháp. Bảng sau cho bạn bức tranh sáu vị trí và kỹ năng cần có; mỗi kỹ năng sẽ xuất hiện ở những chương sau.

Quan explains: at the fintech firm where he works, few people just "trade coins". Most of the work is keeping systems correct, secure and lawful. The table gives you a picture of six roles and the skills they need; each skill shows up in a later chapter.

Vị trí *Role*	**Việc hằng ngày** *Daily work*	**Kỹ năng** *Skills*	**Học ở** *Where you learn it*
Lập trình viên blockchain *Blockchain developer*	Viết và thử phần mềm chạy trên chuỗi khối, ví và hợp đồng thông minh *Writes and tests software running on a blockchain, wallets and smart contracts*	Python hoặc ngôn ngữ khác, cấu trúc dữ liệu, mật mã cơ bản *Python or another language, data structures, basic cryptography*	Chương 2, 3, 6 *Chapters 2, 3, 6*
Kỹ sư bảo mật *Security engineer*	Bảo vệ khóa, kiểm tra máy chủ lưu ký, ứng phó khi bị tấn công *Protects keys, checks custody servers, responds to attacks*	Mật mã, quản lý khóa, an toàn hệ thống *Cryptography, key management, system security*	Chương 2, 5 *Chapters 2, 5*
Kiểm toán hợp đồng thông minh *Smart contract auditor*	Đọc mã của hợp đồng thông minh (chương trình tự chạy trên chuỗi) để tìm lỗi trước khi triển khai *Reads smart contract code (a program that runs itself on the chain) to find faults before launch*	Đọc mã, tư duy tấn công, viết báo cáo trung thực *Reading code, an attacker's mindset, honest reporting*	Chương 6, 7 *Chapters 6, 7*

Vị trí *Role*	**Việc hằng ngày** *Daily work*	**Kỹ năng** *Skills*	**Học ở** *Where you learn it*
Chuyên viên tuân thủ AML/KYC *AML/KYC compliance officer*	Nhận biết khách hàng (KYC), phát hiện giao dịch đáng ngờ, báo cáo theo luật phòng, chống rửa tiền (AML) *Identifies customers (KYC), spots suspicious transactions and reports under the anti-money laundering (AML) law*	Pháp luật, phân tích dòng tiền, cẩn trọng *Law, cash-flow analysis, care*	Chương 5, 10 *Chapters 5, 10*
Phân tích dữ liệu chuỗi *On-chain data analyst*	Đọc dữ liệu giao dịch công khai để thống kê, truy vết dòng tiền *Reads public transaction data for statistics and tracing flows*	Thống kê, Python, đọc trình khám phá khối *Statistics, Python, reading block explorers*	Chương 3, 5, 9 *Chapters 3, 5, 9*
Quản lý sản phẩm *Product manager*	Quyết định tính năng ví, thanh toán, truy xuất nguồn gốc cho người dùng và doanh nghiệp *Decides wallet, payment and traceability features for users and firms*	Hiểu người dùng, pháp lý, tài chính, giao tiếp *Understanding users, law, finance, communication*	Chương 8, 10 *Chapters 8, 10*

Đạo đức nghề nghiệp đi cùng mọi vị trí: giữ kín dữ liệu khách hàng, không quảng cáo lợi nhuận, công bố xung đột lợi ích (Chương 10).

Professional ethics go with every role: keep customer data confidential, do not advertise profits, disclose conflicts of interest (Chapter 10).

1.11. Tính bằng Python – *1.11. Doing it in Python*

Bốn đoạn mã sau chạy thật trên máy, chỉ dùng thư viện chuẩn của Python. Kết quả in bên dưới mỗi đoạn là kết quả chạy; số trong các mục trên khớp với chúng. Dữ liệu là số tự đặt.

The four code blocks that follow really run, using only Python's standard library. The output under each block is what it printed; figures in earlier sections match them. All data is invented.

Đoạn 1. Đổi satoshi, wei, gwei – *Block 1. Converting satoshi, wei and gwei*

```
SAT_MOI_BTC = 100_000_000
WEI_MOI_GWEI = 10**9
GWEI_MOI_ETH = 10**9
TY_GIA = 1_250_000_000   # đồng cho 1 BTC (dữ kiện đề bài)

sat = 2_350_000
btc = sat / SAT_MOI_BTC
dong = sat * TY_GIA // SAT_MOI_BTC
print(f"{sat:,} satoshi = {btc} BTC = {dong:,} dong")
```

```
gas, gia_gas = 21_000, 25     # gia_gas tính bằng gwei
phi_gwei = gas * gia_gas
phi_wei = phi_gwei * WEI_MOI_GWEI
phi_eth = phi_gwei / GWEI_MOI_ETH
print(f"Phí: {phi_gwei:,} gwei = {phi_wei:,} wei")
print(f"Phí bằng ETH: {phi_eth}")
```

Kết quả chạy / *Output*

```
2,350,000 satoshi = 0.0235 BTC = 29,375,000 dong
Phí: 525,000 gwei = 525,000,000,000,000 wei
Phí bằng ETH: 0.000525
```

Số nguyên của Python không tràn, nên 525.000.000.000.000 wei vẫn chính xác. Với số lớn như vậy, dùng số nguyên đáng tin hơn số thập phân.

Python integers do not overflow, so 525,000,000,000,000 wei stays exact. With figures this large, integers are safer than decimals.

Đoạn 2. Lợi suất, độ biến động, sụt giảm tối đa – *Block 2. Return, volatility and maximum drawdown*

```
gia = [10000, 11200, 9800, 10500, 12600, 11900, 8900,
       9500, 10800, 13200, 12100, 11400, 12000]
r = [gia[i] / gia[i - 1] - 1 for i in range(1, len(gia))]
tong = gia[-1] / gia[0] - 1
tb = sum(r) / len(r)
sd = (sum((x - tb) ** 2 for x in r) / (len(r) - 1)) ** 0.5

dinh, sut = gia[0], 0.0
for g in gia:
    dinh = max(dinh, g)
    sut = min(sut, g / dinh - 1)

tiet_kiem = 0.06
print(f"Lợi suất 12 tháng : {tong:.1%}")
print(f"Trung bình tháng  : {tb:.2%}")
print(f"Độ biến động tháng: {sd:.1%}")
print(f"Sụt giảm tối đa   : {sut:.1%}")
print(f"Tiết kiệm 6%/năm  : {tiet_kiem:.1%}")
```

Kết quả chạy / *Output*

```
Lợi suất 12 tháng : 20.0%
Trung bình tháng  : 2.47%
Độ biến động tháng: 14.1%
Sụt giảm tối đa   : -29.4%
Tiết kiệm 6%/năm  : 6.0%
```

Kết quả khớp mục 1.9: 20,0% trong 12 tháng, độ biến động 14,1% mỗi tháng, sụt giảm tối đa -29,4%. Mã dùng độ lệch chuẩn mẫu, chia cho n − 1.

The results match section 1.9: 20.0% over 12 months, volatility of 14.1% a month, a maximum drawdown of -29.4%. The code uses the sample standard deviation, dividing by n − 1.

Đoạn 3. Sổ trung tâm chặn chi tiêu hai lần – *Block 3. A central ledger blocks double spending*

```
so_du = {"Hà My": 500_000, "Quân": 0, "Lâm Viên": 0}
lenh = [("Hà My", "Quân", 500_000),
        ("Hà My", "Lâm Viên", 500_000)]


for i, (a, b, tien) in enumerate(lenh, 1):
```

```
    if so_du[a] >= tien:
        so_du[a] -= tien
        so_du[b] += tien
        print(f"Lệnh {i}: chấp nhận")
    else:
        print(f"Lệnh {i}: từ chối, {a} còn {so_du[a]:,}")

for ten, tien in so_du.items():
    print(f"{ten}: {tien:,}")
print("Tổng :", sum(so_du.values()))
```

Kết quả chạy / *Output*

```
Lệnh 1: chấp nhận
Lệnh 2: từ chối, Hà My còn 0
Hà My: 0
Quân: 500,000
Lâm Viên: 0
Tổng : 500000
```

Điều làm nên sự khác biệt là dòng if: sổ kiểm số dư rồi trừ ngay trước khi nhận lệnh sau. Tổng số tiền không đổi, chỉ chuyển chỗ.

What makes the difference is the if line: the ledger checks the balance and deducts at once before accepting the next order. The total never changes, it only moves.

Đoạn 4. Chuỗi khối thu nhỏ và việc sửa khối cũ – *Block 4. A tiny blockchain and editing an old block*

```
import hashlib

def bam(chu):
    return hashlib.sha256(chu.encode()).hexdigest()

def xay(giao_dich):
    truoc, chuoi = "0" * 64, []
    for gd in giao_dich:
        h = bam(truoc + gd)
        chuoi.append((gd, truoc, h))
        truoc = h
    return chuoi

gd = ["Hà My trả Quân 200", "Quân trả Linh 50",
      "Linh trả Hà My 20"]
goc = xay(gd)
for i, (g, t, h) in enumerate(goc, 1):
    print(f"Khối {i}: băm {h[:12]}… trỏ về {t[:12]}…")

gd[0] = "Hà My trả Quân 20"
moi = xay(gd)
for i in range(3):
    kq = "giữ nguyên" if moi[i][2] == goc[i][2] else "ĐỔI"
    print(f"Sau khi sửa khối 1, khối {i + 1}: {kq}")
```

Kết quả chạy / *Output*

```
Khối 1: băm 71a354d0dc57… trỏ về 000000000000…
Khối 2: băm 24837d3d1ef1… trỏ về 71a354d0dc57…
Khối 3: băm 0f0496e56f1d… trỏ về 24837d3d1ef1…
Sau khi sửa khối 1, khối 1: ĐỔI
Sau khi sửa khối 1, khối 2: ĐỔI
Sau khi sửa khối 1, khối 3: ĐỔI
```

Sửa một chữ ở khối 1 làm băm của cả ba khối đổi, vì mỗi khối băm cùng dấu vân tay của khối trước. Đó là lý do một lịch sử đã ghi khó sửa lén. Chương 2 làm kỹ hơn với cây Merkle và bằng chứng công việc.

Changing one character in block 1 changes the hash of all three blocks, since each block hashes together the previous block's fingerprint. That is why a recorded history is hard to alter quietly. Chapter 2 goes further with Merkle trees and proof of work.

> **PHẢI THUỘC / MEMORISE –** Lợi suất tổng nhân dồn các kỳ; độ biến động là độ lệch chuẩn của lợi suất; sụt giảm tối đa đo từ đỉnh chạy. Tiền gửi tiết kiệm biết trước kết quả, token thì không.
> *Total return compounds the periods; volatility is the standard deviation of returns; maximum drawdown is measured from the running peak. A savings deposit has a known outcome, a token does not.*

Bảng thuật ngữ – *Glossary*

Thuật ngữ *Term (Vietnamese)*	**Tiếng Anh** *English*	**Giải thích ngắn** *Short definition*
tiền	money	thứ mọi người chấp nhận để đo giá, trao đổi và cất giữ giá trị *what people accept to measure prices, to exchange goods and to store value*
đơn vị tính toán	unit of account	đơn vị chung để ghi giá, ví dụ đồng *the common unit for quoting prices, such as the dong*
phương tiện trao đổi	medium of exchange	thứ đưa cho người bán để lấy hàng, không cần trùng nhu cầu *what you hand to a seller for goods, with no need for matching wants*
cất trữ giá trị	store of value	giữ sức mua từ hôm nay sang mai *keeping purchasing power from today to tomorrow*
tiền số của ngân hàng trung ương (CBDC)	central bank digital currency (CBDC)	tiền pháp định ở dạng số do ngân hàng trung ương phát hành *legal tender in digital form issued by the central bank*
tiền mã hóa	cryptocurrency	đơn vị giá trị chạy trên mạng sổ cái phân tán, dùng mật mã để xác thực *a unit of value on a distributed ledger network, authenticated with cryptography*
tài sản mã hóa	crypto-asset	loại tài sản số dùng công nghệ mã hóa để xác thực (Luật 71, Điều 47) *a digital asset authenticated with cryptography (Law 71, Article 47)*

Thuật ngữ *Term (Vietnamese)*	**Tiếng Anh** *English*	**Giải thích ngắn** *Short definition*
tài sản số	digital asset	tài sản thể hiện bằng dữ liệu số (Luật 71, Điều 46) *property expressed as digital data (Law 71, Article 46)*
chi tiêu hai lần	double spending	dùng cùng một khoản tiền số cho hai giao dịch *using the same digital money in two transactions*
sổ cái	ledger	cuốn sổ ghi ai có bao nhiêu và ai chuyển cho ai *the book recording who holds what and who paid whom*
sổ cái phân tán (DLT)	distributed ledger technology (DLT)	sổ cái mà nhiều bên cùng giữ bản sao và cùng kiểm *a ledger of which many parties hold copies and check together*
chuỗi khối (blockchain)	blockchain	sổ cái gồm các khối nối nhau bằng mã băm *a ledger of blocks chained together by hashes*
hàm băm	hash function	phép biến dữ liệu thành dấu vân tay có độ dài cố định *a function turning data into a fixed-length fingerprint*
khối nguyên thủy	genesis block	khối đầu tiên của một chuỗi khối *the first block of a blockchain*
đồng ổn định	stablecoin	token cố gắng giữ giá gần một tài sản tham chiếu *a token that tries to hold its price near a reference asset*
NFT	non-fungible token (NFT)	token độc nhất, không thay thế lẫn nhau *a one-of-a-kind token that cannot be swapped for another*
satoshi	satoshi	đơn vị nhỏ nhất của bitcoin, bằng một phần trăm triệu BTC *the smallest unit of bitcoin, one hundred-millionth of a BTC*
gwei và wei	gwei and wei	đơn vị nhỏ của ether: 1 ETH = 10^9 gwei = 10^{18} wei *small units of ether: 1 ETH = 10^9 gwei = 10^{18} wei*

Thuật ngữ *Term (Vietnamese)*	**Tiếng Anh** *English*	**Giải thích ngắn** *Short definition*
bút danh	pseudonymity	dùng mã riêng thay tên thật; ai cũng thấy mã nhưng không thấy tên *using a code instead of a real name; everyone sees the code but not the name*
phi tập trung	decentralisation	không một bên nào nắm quyền ghi sổ và quyết định *no single party controls writing to the ledger or decides*
lợi suất	return	phần trăm thay đổi giá trị của khoản đầu tư trong một kỳ *the percentage change in an investment's value over a period*
độ biến động	volatility	mức dao động của lợi suất quanh mức trung bình, đo bằng độ lệch chuẩn *how far returns swing around their mean, measured by standard deviation*
sụt giảm tối đa	maximum drawdown	mức giảm sâu nhất từ một đỉnh xuống đáy sau đó *the deepest fall from a peak to a later low*
KYC	know your customer (KYC)	quy trình nhận biết khách hàng của tổ chức tài chính *a financial firm's process for identifying its customers*
AML	anti-money laundering (AML)	phòng, chống rửa tiền *preventing the laundering of criminal proceeds*

1.12. Bài tập vận dụng có lời giải – *Applied exercises with solutions*

Bài 1. Đổi đơn vị và tính phí mạng – *Exercise 1. Converting units and network fees*

Anh Quân chuyển cho Hà My 3.750.000 satoshi và tự trả thêm phí mạng 1.600 satoshi. Tỷ giá đề bài đặt là 1 BTC = 900.000.000 đồng. Hãy đổi số tiền Hà My nhận ra BTC và ra đồng, tính tổng số satoshi rời ví anh Quân và phí mạng ra đồng. Ngoài ra, anh chuyển 0,8 ETH sang một ví khác với 21.000 gas ở giá 30 gwei mỗi gas: hãy đổi 0,8 ETH ra gwei và wei, rồi tính phí theo gwei và theo ETH.

Quan sends Ha My 3,750,000 satoshi and pays a network fee of 1,600 satoshi on top. The exercise sets the rate at 1 BTC = 900,000,000 dong. Convert what Ha My receives into BTC and dong, find the total satoshi leaving Quan's wallet, and the fee in dong. He also moves 0.8 ETH to another wallet using 21,000 gas at 30 gwei per gas: convert 0.8 ETH into gwei and wei, then find the fee in gwei and in ETH.

1. Đổi satoshi ra BTC: 3.750.000 / 100.000.000 = 0,0375 BTC.
   Satoshi to BTC: 3,750,000 / 100,000,000 = 0.0375 BTC.
2. Ra đồng: 0,0375 ∗ 900.000.000 = 33.750.000 đồng. Hà My nhận số tiền tương đương 33.750.000 đồng.
   In dong: 0.0375 ∗ 900,000,000 = 33,750,000 dong. Ha My receives the equivalent of 33,750,000 dong.
3. Tổng rời ví anh Quân: 3.750.000 + 1.600 = 3.751.600 satoshi, tức 0,037516 BTC.
   Total leaving Quan's wallet: 3,750,000 + 1,600 = 3,751,600 satoshi, or 0.037516 BTC.
4. Phí ra đồng: 1.600 ∗ 900.000.000 / 100.000.000 = 14.400 đồng.
   Fee in dong: 1,600 ∗ 900,000,000 / 100,000,000 = 14,400 dong.
5. 0,8 ETH = 0,8 ∗ 10^9 = 800.000.000 gwei = 8 ∗ 10^{17} wei (800.000.000.000.000.000 wei).
   0.8 ETH = 0.8 ∗ 10^9 = 800,000,000 gwei = 8 ∗ 10^{17} wei (800,000,000,000,000,000 wei).
6. Phí gas: 21.000 ∗ 30 = 630.000 gwei = 0,00063 ETH.
   Gas fee: 21,000 ∗ 30 = 630,000 gwei = 0.00063 ETH.

Bài 2. Lợi suất token SVG so với tiết kiệm – ***Exercise 2. Return on the SVG token against a savings deposit***

Token SVG có giá cuối 9 tuần liên tiếp (đồng): 20.000, 21.400, 19.800, 18.600, 20.500, 22.100, 19.900, 21.000, 21.800. Tiền gửi tiết kiệm có lãi 4,8%/năm, tính lãi đơn theo 8 tuần trên 52 tuần của năm. Hãy tính lợi suất tổng của SVG, lợi suất tuần tệ nhất và tốt nhất, sụt giảm tối đa, rồi so với tiết kiệm.

The SVG token closes at these prices (dong) over nine consecutive weeks: 20,000, 21,400, 19,800, 18,600, 20,500, 22,100, 19,900, 21,000, 21,800. A savings deposit pays 4.8% a year, simple interest for 8 weeks out of 52. Find SVG's total return, its worst and best weekly return and its maximum drawdown, then compare with the deposit.

1. Lợi suất tổng = 21.800 / 20.000 − 1 = 9,0%.
   Total return = 21,800 / 20,000 − 1 = 9.0%.
2. Lợi suất từng tuần = giá tuần sau / giá tuần trước − 1. Tệ nhất -10,0% (tuần 6), tốt nhất 10,2% (tuần 4).
   Weekly return = this week's price / last week's price − 1. Worst -10.0% (week 6), best 10.2% (week 4).
3. Đỉnh chạy tới tuần 1 là 21.400, đáy sau đó là 18.600: sụt giảm tối đa = 18.600 / 21.400 − 1 = -13,08%.
   The running peak of week 1 is 21,400 and the later low is 18,600: maximum drawdown = 18,600 / 21,400 − 1 = -13.08%.
4. Tiết kiệm 8 tuần: 4,8% ∗ 8 / 52 = 0,74%.
   Deposit for 8 weeks: 4.8% ∗ 8 / 52 = 0.74%.
5. SVG hơn tiết kiệm 8,26 điểm phần trăm, nhưng trên đường đi có lúc giá thấp hơn đỉnh trước đó 13,1%. Chuỗi giá là dữ kiện đề bài, không dự báo gì.
   SVG beats the deposit by 8.26 percentage points, but along the way it was 13.1% down from an earlier peak. The price series is an exercise input and predicts nothing.

Bài 3. Lời mời lãi 3% mỗi tuần và khách muốn trả bằng tài sản mã hóa – ***Exercise 3. A 3%-a-week offer and a customer who wants to pay in crypto-assets***

Một nhóm trên mạng mời Công ty Cà phê Lâm Viên góp 100.000.000 đồng mua đồng LVX, cam kết lãi cố định 3% mỗi tuần, có thể rút bất kỳ lúc nào, "không rủi ro". Cùng lúc, một khách nước ngoài đề nghị trả tiền lô cà phê tại Việt Nam bằng tài sản mã hóa. Hãy tính số tiền sau 52 tuần nếu lãi gộp đúng cam kết, nêu ít nhất ba dấu hiệu đáng ngờ, và nói căn cứ pháp luật để từ chối khoản trả bằng tài sản mã hóa.

An online group invites Lam Vien Coffee to put in 100,000,000 dong to buy LVX coins, promising a fixed 3% a week, withdrawable at any time, "risk free". At the same moment a foreign customer offers to pay for a coffee shipment in Vietnam with crypto-assets. Compute the sum after 52 weeks if the promised interest compounds, give at least three warning signs, and state the legal basis for declining the crypto payment.

1. Hệ số 52 tuần = $1{,}03^{52} = 4{,}6509$; số tiền = $100.000.000 * 4{,}6509 = 465.088.590$ đồng (lãi 365,1% một năm).
   52-week factor = $1.03^{52} = 4.6509$; sum = $100{,}000{,}000 * 4.6509 = 465{,}088{,}590$ dong (a gain of 365.1% in a year).
2. Dấu hiệu 1: lãi cố định cao gấp nhiều lần lãi tiết kiệm, không gắn với hoạt động tạo ra thu nhập nào. Dấu hiệu 2: lời hứa "không rủi ro". Dấu hiệu 3: rút lúc nào cũng được mà không nói tiền lãi lấy từ đâu.
   Sign 1: a fixed return many times a savings rate, tied to no income-producing activity. Sign 2: the promise of "no risk". Sign 3: withdrawal at any time with no word on where the interest comes from.
3. Hệ quả: lãi chỉ trả được nếu người mới liên tục nộp tiền; khi dòng tiền mới chậm lại, nhóm không trả nổi. Công ty nên từ chối và không chuyển tiền (Chương 9 phân tích sâu).
   Consequence: interest can be paid only while newcomers keep paying in; once new money slows, the group cannot pay. The company should decline and send nothing (Chapter 9 analyses this in depth).
4. Khoản trả bằng tài sản mã hóa: tài sản mã hóa không phải phương tiện thanh toán hợp pháp; tiền giấy, tiền kim loại do Ngân hàng Nhà nước phát hành mới là phương tiện thanh toán hợp pháp (Luật Ngân hàng Nhà nước VBHN 141/2026, Điều 17 khoản 2).
   Payment in crypto-assets: a crypto-asset is not a lawful means of payment; only banknotes and coins issued by the State Bank are (Law on the State Bank, consolidated text 141/2026, Article 17, clause 2).
5. Dùng tài sản mã hóa để trả tiền hàng hóa, dịch vụ có thể bị xử lý theo quy định về phương tiện thanh toán không hợp pháp (Nghị định 340/2025/NĐ-CP, Điều 30 khoản 6 điểm d). Công ty yêu cầu khách chuyển khoản bằng đồng qua ngân hàng.
   Using crypto-assets to pay for goods or services can be dealt with under the rules on unlawful means of payment (Decree 340/2025/ND-CP, Article 30, clause 6, point d). The company asks the customer to pay in dong through a bank.

1.13. Câu hỏi tự luận và dàn ý trả lời – *Essay questions and answer outlines*

Câu 1. Phân biệt tiền gửi ngân hàng, ví điện tử, tiền số của ngân hàng trung ương và tiền mã hóa theo ba câu hỏi: ai phát hành, ai giữ sổ, có được bảo đảm không.
Question 1. *Distinguish bank deposits, e-wallets, central bank digital currency and cryptocurrency by three questions: who issues, who keeps the ledger, and is it guaranteed.*

- Tiền gửi ngân hàng: ngân hàng thương mại giữ sổ, số dư là quyền đòi tiền ở ngân hàng.
  Bank deposits: the commercial bank keeps the ledger and the balance is a claim on the bank.
- Ví điện tử: tổ chức cung ứng ví giữ sổ, đơn vị vẫn là đồng.
  E-wallets: the wallet provider keeps the ledger and the unit is still the dong.
- Tiền số của ngân hàng trung ương: ngân hàng trung ương phát hành, là dạng số của tiền pháp định.
  Central bank digital currency: issued by the central bank, a digital form of legal tender.
- Tiền mã hóa: không có người phát hành duy nhất, mạng nút giữ sổ, không có ai bảo đảm giá trị.
  Cryptocurrency: no single issuer, a network of nodes keeps the ledger, and nobody guarantees its value.
- Kết luận bằng bảng: ai chịu rủi ro khi mất dữ liệu hoặc khi bên giữ sổ sai sót.
  Conclude with a table: who bears the risk when data is lost or the ledger keeper errs.

Câu 2. Chi tiêu hai lần là gì? Ngân hàng giải bài toán này thế nào và vì sao cách đó chưa dùng được khi không có bên giữ sổ chung?
Question 2. *What is double spending? How does a bank solve it, and why does that solution fail when nobody holds a common ledger?*

- Tiền là dữ liệu thì sao chép được; tờ tiền giấy thì không.
  Money that is data can be copied; a banknote cannot.
- Cách ngân hàng: sổ trung tâm, kiểm số dư, trừ ngay, từ chối lệnh sau.
  The bank's way: a central ledger, check the balance, deduct at once, reject the later order.
- Điều kiện để cách đó chạy: mọi người tin vào bên giữ sổ.
  The condition for it to work: everyone trusts the ledger keeper.
- Hướng của sổ cái phân tán: nhiều bên cùng giữ bản sổ và cùng kiểm.
  The distributed ledger's direction: many parties hold copies of the ledger and check together.
- Các thử nghiệm trước Bitcoin gặp khó ở đâu (DigiCash, e-gold).
  Where the pre-Bitcoin attempts ran into trouble (DigiCash, e-gold).

Câu 3. Phân tích tài sản mã hóa trong pháp luật Việt Nam: thuộc khái niệm nào, gồm gì và không gồm gì, và vì sao không phải phương tiện thanh toán. Nêu một lập luận ủng hộ và một lập luận phản đối cách quy định này.

Question 3. *Analyse crypto-assets in Vietnamese law: which concept they fall under, what they include and exclude, and why they are not a means of payment. Give one argument for and one against this approach.*

- Tài sản theo Bộ luật Dân sự Điều 105; tài sản số theo Luật 71 Điều 46.
  Property under Civil Code Article 105; digital assets under Law 71, Article 46.
- Điều 47 khoản 2: tài sản ảo, tài sản mã hóa, tài sản số khác.
  Article 47, clause 2: virtual assets, crypto-assets, other digital assets.
- Loại trừ: chứng khoán, dạng số của tiền pháp định, tài sản tài chính khác.
  Exclusions: securities, digital forms of legal tender, other financial assets.
- Phương tiện thanh toán hợp pháp: Luật Ngân hàng Nhà nước Điều 17 khoản 2.
  Lawful means of payment: Law on the State Bank, Article 17, clause 2.
- Lập luận ủng hộ: giữ ổn định tiền tệ, bảo vệ người dân. Lập luận phản đối: khó dùng trong giao dịch giữa các bên thỏa thuận.
  For: protects monetary stability and the public. Against: harder to use between parties who agree to it.

1.14. Câu hỏi trắc nghiệm – *Multiple-choice questions*

1. Bảng giá của quán ghi ly cà phê 35.000 đồng và bánh mì 20.000 đồng. Tiền đang làm chức năng nào?
A cafe menu lists coffee at 35,000 dong and a bread roll at 20,000 dong. Which function is money performing?

A. Cất trữ giá trị qua nhiều năm / *Storing value over many years*
B. Đơn vị tính toán, đo giá trị mọi hàng / *Unit of account measuring every good*
C. Điều tiết lãi suất thị trường / *Steering market interest rates*
D. Phát hành thêm tiền cho nền kinh tế / *Issuing more money for the economy*

2. Số dư tài khoản ngân hàng của Hà My được ghi ở đâu?
Where is the balance of Ha My's bank account recorded?

A. Trong chip của thẻ nhựa / *In the chip of her plastic card*
B. Trên máy tính của mọi người dùng / *On every user's computer*
C. Ở ngân hàng trung ương, mỗi người một dòng / *At the central bank, one line per person*
D. Trong sổ của ngân hàng thương mại nơi mở tài khoản / *In the ledger of the commercial bank where she opened it*

3. Hà My nhận 2.500.000 satoshi. Số đó bằng bao nhiêu BTC?
Ha My receives 2,500,000 satoshi. How many BTC is that?

A. 0,025 BTC / *0.025 BTC*
B. 0,25 BTC / *0.25 BTC*
C. 0,0025 BTC / *0.0025 BTC*
D. 25 BTC

4. Loại nào là tiền pháp định ở dạng số do ngân hàng trung ương phát hành?
Which is legal tender in digital form issued by a central bank?

A. Đồng ổn định do công ty tư nhân phát hành / *A stablecoin issued by a private company*
B. Số dư trong ví điện tử của một ứng dụng / *A balance in an app's e-wallet*
C. Tiền số của ngân hàng trung ương (CBDC) / *Central bank digital currency (CBDC)*
D. Token tiện ích đổi lấy dịch vụ / *A utility token redeemable for a service*

5. Giá một token đi từ 10.000 đồng xuống 8.000 đồng rồi lên 9.200 đồng. Lợi suất tổng của cả hai bước là bao nhiêu?
A token's price falls from 10,000 dong to 8,000 dong then rises to 9,200 dong. What is the total return over both steps?

A. +8%
B. −20%
C. +15%
D. −8%

6. Theo Luật Công nghiệp công nghệ số Điều 47 khoản 2 điểm b, điều nào nằm NGOÀI khái niệm tài sản mã hóa?
Under Article 47, clause 2, point b of the Law on the Digital Technology Industry, which falls OUTSIDE the concept of a crypto-asset?

A. Tài sản số dùng công nghệ mã hóa để xác thực khi chuyển giao / *A digital asset using cryptography to authenticate transfers*
B. Chứng khoán / *Securities*
C. Tài sản số dùng công nghệ tương tự để xác thực khi phát hành / *A digital asset using similar technology to authenticate issuance*
D. Tài sản số được lưu trữ bằng công nghệ mã hóa / *A digital asset stored using cryptography*

7. Giá token là 100 đồng, tăng 20% rồi giảm 20%. Giá cuối là bao nhiêu?
A token costs 100 dong, rises 20% then falls 20%. What is the final price?

A. 100 đồng / *100 dong*
B. 104 đồng / *104 dong*
C. 96 đồng / *96 dong*
D. 80 đồng / *80 dong*

8. Vì sao ngân hàng chặn được chi tiêu hai lần cùng một số dư?
Why can a bank stop the same balance being spent twice?

A. Sổ trung tâm trừ số dư ngay ở lệnh đầu rồi từ chối lệnh sau / *A central ledger deducts at the first order and rejects the next*

B. Mỗi đồng tiền có mã riêng không thể sao chép / *Each coin carries a code that cannot be copied*

C. Khách hàng cam kết không chi hai lần / *Customers promise not to spend twice*

D. Mọi cửa hàng cùng giữ một bản sổ / *Every shop keeps a copy of the ledger*

Chương 2. Mật mã học nền tảng: hàm băm, chữ ký số, khóa và địa chỉ – *Chapter 2. Cryptographic foundations: hashes, signatures, keys and addresses*

Mục tiêu chương – *Chapter objectives*

- Giải thích hàm băm là gì, ba tính chất của nó, và tự băm một câu bằng SHA-256 để thấy đổi một ký tự thì giá trị băm đổi hẳn.
  Explain what a hash function is, its three properties, and hash a sentence yourself with SHA-256 to see that changing one character changes the hash completely.
- Dựng được chuỗi khối bằng con trỏ băm và cây Merkle, rồi nói vì sao sửa một khối cũ thì lộ và chứng minh một giao dịch thuộc khối chỉ bằng vài giá trị băm.
  Build a chain of blocks from hash pointers and a Merkle tree, then say why editing an old block shows and prove a transaction belongs to a block with only a few hashes.
- Nêu ba thao tác của chữ ký số (tạo khóa, ký, kiểm), cộng điểm và nhân vô hướng trên đường cong elliptic thu nhỏ, và ký rồi kiểm một tin nhắn bằng ECDSA.
  State the three operations of a digital signature (generate keys, sign, verify), add points and multiply by a scalar on a miniature elliptic curve, and sign then verify a message with ECDSA.
- Đi từ khóa bí mật qua khóa công khai đến địa chỉ Base58Check, giải thích mã kiểm tra, và nhận ra vì sao khóa phải sinh ngẫu nhiên (chuyện ví não).
  Go from a private key through a public key to a Base58Check address, explain the checksum, and see why keys must be random (the brain wallet story).
- Biết bút danh khác ẩn danh, nói được ý chính về máy tính lượng tử, và nối các khái niệm với Điều 46, 47 Luật Công nghiệp công nghệ số.
  Know that a pseudonym differs from anonymity, give the main idea on quantum computers, and link the concepts to Articles 46 and 47 of the Law on the Digital Technology Industry.

2.1. Hàm băm: dấu vân tay của dữ liệu – *2.1. Hash functions: the fingerprint of data*

Mỗi người có một dấu vân tay. Nhìn dấu vân tay, bạn không đoán được chiều cao hay tính cách của chủ nhân, nhưng hai người khác nhau gần như chắc chắn có hai dấu khác nhau. Hàm băm (hash function) làm việc tương tự với dữ liệu. Bạn đưa vào một tệp, một câu hay một giao dịch bất kỳ, hàm băm trả về một chuỗi ký tự có độ dài cố định, gọi là giá trị băm (hash value).

Everyone has a fingerprint. A fingerprint tells you nothing about the owner's height or character, yet two different people almost surely have different prints. A hash function does the same job for data. You feed in any file, sentence or transaction, and it returns a string of fixed length, called the hash value.

Ba điều cần nhớ ngay. Một: cùng đầu vào luôn ra cùng giá trị băm, nên hai máy tính ở hai đầu thế giới băm cùng một tệp sẽ thấy cùng một dấu vân tay. Hai: đầu vào dài hay ngắn thì giá trị băm vẫn dài bằng nhau. Ba: từ giá trị băm bạn không thể suy ngược ra đầu vào, giống như từ dấu vân tay bạn không dựng lại được cả con người.

Three things to remember at once. One: the same input always gives the same hash value, so two computers at opposite ends of the world hashing one file see one fingerprint. Two: whether the input is long or short, the hash value has the same length. Three: from the hash value you cannot work back to the input, just as a fingerprint cannot rebuild a whole person.

Hàm băm không phải là mã hóa. Mã hóa (encryption) là khóa dữ liệu lại để người có chìa mở ra đọc được. Băm thì không có chìa: dữ liệu gốc không quay lại được. Bạn dùng băm để kiểm tra dữ liệu có bị sửa không, không dùng để giấu rồi đọc lại.

A hash is not encryption. Encryption locks data so that someone with the key can open and read it. A hash has no key: the original cannot be recovered. You use a hash to check whether data has been altered, not to hide data and read it back later.

Một hàm băm dùng cho tiền số cần ba tính chất. Bảng sau nói mỗi tính chất bằng lời thường, kèm chỗ nó được dùng.

A hash function used for digital money needs three properties. The table puts each in plain words and shows where it is used.

Tính chất *Property*	**Nói bằng lời thường** *In plain words*	**Ví dụ đời thường** *Everyday picture*	**Dùng ở đâu** *Where it is used*
Kháng va chạm *Collision resistance*	Không ai tìm được hai đầu vào khác nhau mà ra cùng một giá trị băm. *Nobody can find two different inputs with the same hash value.*	Hai người khác nhau không thể có chung dấu vân tay. *Two different people cannot share a fingerprint.*	Dùng giá trị băm đại diện cho một giao dịch hay một khối. *A hash stands for a transaction or a block.*
Che giấu *Hiding*	Biết giá trị băm thì không đoán được đầu vào, nếu đầu vào đã trộn thêm một số ngẫu nhiên đủ lớn. *Knowing the hash tells you nothing about the input, if a large random number was mixed in.*	Phong bì dán kín: ai cũng thấy phong bì, không ai thấy thư. *A sealed envelope: all see it, nobody sees the letter.*	Cam kết một giá trị rồi mở ra sau. *Committing to a value and revealing it later.*
Thân thiện câu đố *Puzzle friendliness*	Muốn ra một giá trị băm có dạng cho trước thì chỉ còn cách thử đi thử lại, không có đường tắt. *To reach a hash of a set shape you can only try again and again; there is no shortcut.*	Xổ số đoán số: chỉ có cách mua nhiều vé. *A number lottery: the only way is to buy many tickets.*	Là nền của việc "đào" khối ở Chương 4: thợ đào thử đi thử lại để tìm một giá trị băm có dạng cho trước. *The base of "mining" in Chapter 4: miners try again and again to find a hash of a set shape.*

Bạn thử ngay. Đoạn mã sau băm hai câu giống nhau, chỉ khác một chữ số. Python tính thật bằng thư viện hashlib có sẵn.

Try it. The code below hashes two sentences that differ by a single digit. Python computes it for real with the built-in hashlib library.

```
import hashlib


def bam(s):
    return hashlib.sha256(s.encode()).hexdigest()


a = "HaMy gui Quan 5 Sen Vang"
b = "HaMy gui Quan 6 Sen Vang"
ha, hb = bam(a), bam(b)
print("Dau vao A:", a)
print("Dau vao B:", b)
print("Bam A:", ha[:32] + "...")
print("Bam B:", hb[:32] + "...")
khac = bin(int(ha, 16) ^ int(hb, 16)).count("1")
print("So bit khac nhau:", khac, "tren 256")
```

Kết quả chạy / *Output*

```
Dau vao A: HaMy gui Quan 5 Sen Vang
Dau vao B: HaMy gui Quan 6 Sen Vang
Bam A: 9053b8e31f23e85fcce5832dd379b241...
Bam B: a0fe4d37390e7e08f60fc6aec6b330ec...
So bit khac nhau: 137 tren 256
```

Hai câu chỉ khác chữ số 5 và 6, nhưng hai giá trị băm không có nét nào giống nhau. Trong 256 bit đầu ra, có 137 bit khác nhau, gần một nửa. Đó là hiệu ứng thác đổ (avalanche effect): đổi một ký tự đầu vào, cả giá trị băm đổi theo. Nhờ tính này, ai sửa dù một dấu phẩy trong một giao dịch thì dấu vân tay của giao dịch lộ ra là đã khác.

The two sentences differ only in the digits 5 and 6, yet the hashes share no visible pattern. Of the 256 output bits, 137 differ, nearly half. This is the avalanche effect: change one input character and the whole hash changes. So even a changed comma in a transaction shows up as a different fingerprint.

Ứng dụng cho Hà My. Hà My gửi Quan 5 đồng Sen Vàng và lưu giá trị băm của lệnh chuyển. Sau đó, nếu ai đổi số 5 thành 6 trong bản lưu, Hà My băm lại và thấy hai chuỗi khác hẳn. Cô không cần đọc lại từng chữ để biết bản lưu đã bị đụng vào.

Applied to Ha My. Ha My sends Quan 5 Sen Vang coins and stores the hash of the transfer. If someone later changes 5 to 6 in the stored copy, Ha My hashes it again and sees two entirely different strings. She does not need to reread every word to know the copy was touched.

PHẢI THUỘC / MEMORISE – Hàm băm biến dữ liệu bất kỳ thành một chuỗi dài cố định, theo một chiều. Ba tính chất: kháng va chạm, che giấu, thân thiện câu đố. Đổi một ký tự đầu vào thì khoảng một nửa số bit đầu ra đổi (hiệu ứng thác đổ).

A hash function turns any data into a string of fixed length, in one direction. Three properties: collision resistance, hiding and puzzle friendliness. Change one input character and about half the output bits change (avalanche effect).

LỖI HAY GẶP / COMMON MISTAKE – Nghĩ rằng băm là mã hóa và có thể giải ngược để lấy lại dữ liệu. Băm không có chìa khóa và không có phép giải ngược. Muốn đoán đầu vào, kẻ xấu chỉ có cách thử từng khả năng.

Thinking a hash is encryption that can be reversed to recover the data. A hash has no key and no reverse step. To guess the input, an attacker can only try each possibility.

2.2. SHA-256 và băm hai lần – *2.2. SHA-256 and double hashing*

Bitcoin dùng hàm băm tên SHA-256 (Secure Hash Algorithm, 256 bit). Đầu vào là chuỗi byte dài tùy ý. Đầu ra luôn là 256 bit, tức 32 byte. Khi viết ra giấy, người ta đổi 256 bit đó sang hệ thập lục phân (hexadecimal, hệ 16 dùng 16 ký hiệu 0 đến 9 và a đến f). Mỗi ký tự hex thay cho 4 bit, nên giá trị băm có 256 / 4 = 64 ký tự.

Bitcoin uses a hash function called SHA-256 (Secure Hash Algorithm, 256 bit). The input is a string of bytes of any length. The output is always 256 bits, which is 32 bytes. When written on paper, those 256 bits are shown in hexadecimal (base 16, using the 16 symbols 0 to 9 and a to f). Each hex character stands for 4 bits, so a hash has 256 / 4 = 64 characters.

Bạn đọc đoạn mã sau theo từng bước. Bước 1: lấy câu lệnh chuyển tiền làm đầu vào. Bước 2: băm một lần ra 32 byte. Bước 3: lấy 32 byte đó băm thêm một lần nữa. Bước 4: đếm độ dài và so sánh với trường hợp đầu vào dài gấp 1.000 lần.

Read the next piece of code step by step. Step 1: take the transfer instruction as input. Step 2: hash it once to get 32 bytes. Step 3: hash those 32 bytes once more. Step 4: count the lengths and compare with an input 1,000 times longer.

```
import hashlib


x = b"HaMy gui Quan 5 Sen Vang"
mot = hashlib.sha256(x).digest()
hai = hashlib.sha256(mot).digest()
print("Do dai dau ra:", len(mot), "byte =", len(mot) * 8, "bit")
print("Do dai chuoi hex:", len(mot.hex()), "ky tu")
print("Bam 1 lan:", mot.hex()[:16] + "...")
print("Bam 2 lan:", hai.hex()[:16] + "...")
dai = hashlib.sha256(x * 1000).hexdigest()
print("Dau vao dai gap 1000 lan, hex:", len(dai), "ky tu")
print("So dau ra co the co:", f"{2**256:.4e}")
```

Kết quả chạy / *Output*

```
Do dai dau ra: 32 byte = 256 bit
Do dai chuoi hex: 64 ky tu
Bam 1 lan: 9053b8e31f23e85f...
Bam 2 lan: 010422477ce6ddea...
Dau vao dai gap 1000 lan, hex: 64 ky tu
So dau ra co the co: 1.1579e+77
```

Kết quả cho thấy đầu ra luôn có 256 bit, tức 64 ký tự hex, dù đầu vào dài gấp 1.000 lần. Số đầu ra có thể có là 2^{256}, khoảng $1{,}1579 * 10^{77}$. Con số này lớn hơn nhiều so với số hạt cát trên Trái Đất, nên hai đầu vào khác nhau gần như không bao giờ trùng giá trị băm.

The result shows the output is always 256 bits, 64 hex characters, even when the input is 1,000 times longer. The number of possible outputs is 2^{256}, about $1.1579 * 10^{77}$. That is far more than the grains of sand on Earth, so two different inputs almost never share a hash value.

$$\text{Số giá trị băm có thể có} = 2^{256} \approx 1{,}1579 * 10^{77} \tag{2.1}$$

Vì sao Bitcoin băm hai lần? Băm hai lần là lấy giá trị băm của giá trị băm: H(H(x)). Cách này che thêm một lớp, vì một số cách tấn công vào hàm băm đơn không còn dùng được trên kết quả băm lần hai. Bạn gặp băm hai lần khi tính mã giao dịch, khi nối các nhánh cây Merkle ở mục 2.4 và khi tính mã kiểm tra của địa chỉ ở mục 2.8.

Why does Bitcoin hash twice? Double hashing means taking the hash of the hash, H(H(x)). It adds a layer, because some attacks on a single hash no longer work on the second round. You meet it when computing transaction identifiers, when joining branches of the Merkle tree in section 2.4, and when computing the checksum of an address in section 2.8.

SHA-256 thuộc họ SHA-2. Thư viện chuẩn Python còn có hàm SHA3-256, thuộc họ SHA-3, cho kết quả khác SHA-256 và khác cả hàm keccak-256 mà Ethereum dùng. Vì vậy các đoạn mã trong sách không tạo ra địa chỉ Ethereum thật.

SHA-256 belongs to the SHA-2 family. The Python standard library also has the SHA3-256 function, from the SHA-3 family, which gives results different from SHA-256 and from the keccak-256 function Ethereum uses. So the code in this book does not produce real Ethereum addresses.

> **LỖI HAY GẶP / COMMON MISTAKE –** Đếm độ dài giá trị băm bằng số ký tự hex rồi nhầm với số bit. 64 ký tự hex là 256 bit, không phải 64 bit. Mỗi ký tự hex chỉ mang 4 bit.
> *Counting the hash length in hex characters and mistaking it for bits. 64 hex characters are 256 bits, not 64 bits. Each hex character carries only 4 bits.*

2.3. Con trỏ băm và chuỗi khối: sửa khối cũ thì lộ – *2.3. Hash pointers and the chain of blocks: editing an old block shows*

Con trỏ thường chỉ vị trí của một dữ liệu. Con trỏ băm (hash pointer) làm hai việc cùng lúc: chỉ vị trí của dữ liệu và kèm giá trị băm của chính dữ liệu đó. Giống như bạn ghi số trang của một tờ hóa đơn trong tập hồ sơ, và dán thêm một con dấu niêm phong ghi dấu vân tay của tờ đó. Mở tờ ra, bạn đối chiếu con dấu để biết tờ hóa đơn còn nguyên.

An ordinary pointer only says where some data sits. A hash pointer does two jobs at once: it says where the data sits and it carries the hash of that data. Think of writing the page number of an invoice in a file and adding a seal that records the fingerprint of that page. When you open the page, you check the seal to know the invoice is untouched.

Nối các con trỏ băm lại, bạn có chuỗi khối (blockchain). Mỗi khối chứa dữ liệu của nó và giá trị băm của khối đứng ngay trước. Giá trị băm của khối sau được tính từ cả dữ liệu mới lẫn giá trị băm trước đó, nên nó mang theo cả lịch sử phía sau lưng.

Link hash pointers together and you have a blockchain. Each block holds its own data and the hash of the block just before it. The hash of a later block is computed from both its new data and the earlier hash, so it carries the whole history behind it.

Các bước kiểm một chuỗi khối, bạn làm như sau. Bước 1: bắt đầu từ khối đầu, lấy giá trị băm của nó. Bước 2: ghép giá trị đó với dữ liệu khối kế tiếp rồi băm ra giá trị mới. Bước 3: so giá trị mới với giá trị đã ghi trên khối kế tiếp. Bước 4: khớp thì đi tiếp, lệch thì dừng và báo chỗ lệch.

To verify a chain, you do this. Step 1: start at the first block and take its hash. Step 2: join that value to the data of the next block and hash to get a new value. Step 3: compare the new value with the one recorded on the next block. Step 4: if they match, move on; if not, stop and report the break.

```
import hashlib

def bam(s):
    return hashlib.sha256(s.encode()).hexdigest()

def chuoi(du_lieu):
    truoc, ra = "0" * 64, []
    for x in du_lieu:
        truoc = bam(truoc + x)
        ra.append(truoc)
    return ra

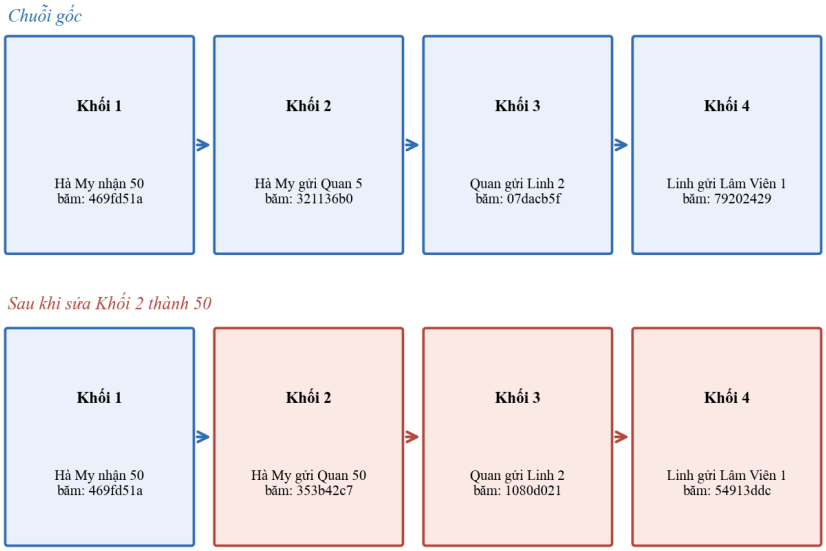
goc = ["Khoi 1: Ha My nhan 50 Sen Vang", "Khoi 2: Ha My gui Quan 5",
       "Khoi 3: Quan gui Linh 2", "Khoi 4: Linh gui Lam Vien 1"]
sua = list(goc)
sua[1] = "Khoi 2: Ha My gui Quan 50"
for i, (a, b) in enumerate(zip(chuoi(goc), chuoi(sua)), 1):
    print("Khoi", i, a[:8], b[:8], "giong" if a == b else "LECH")
```

Kết quả chạy / *Output*

```
Khoi 1 469fd51a 469fd51a giong
Khoi 2 321136b0 353b42c7 LECH
Khoi 3 07dacb5f 1080d021 LECH
Khoi 4 79202429 54913ddc LECH
```

Bài mẫu: chuỗi bốn khối ghi các lệnh chuyển Sen Vàng của Hà My, Quan và Linh. Kẻ gian sửa Khối 2 từ "gửi Quan 5" thành "gửi Quan 50". Kết quả: Khối 1 vẫn khớp (469fd51a), còn Khối 2, 3 và 4 đều lệch. Khối 2 lệch vì dữ liệu đổi. Khối 3 lệch vì nó chứa băm cũ của Khối 2. Khối 4 lệch theo cùng cách. Cả 3 khối sau chỗ sửa đều lộ.

Worked example: a chain of four blocks records Sen Vang transfers by Ha My, Quan and Linh. A cheat edits Block 2 from "to Quan 5" to "to Quan 50". Result: Block 1 still matches (469fd51a), while Blocks 2, 3 and 4 all differ. Block 2 differs because its data changed. Block 3 differs because it holds the old hash of Block 2. Block 4 differs in the same way. All 3 blocks after the edit give it away.



Hình 2.1. Hàng trên là chuỗi bốn khối gốc, hàng dưới là chuỗi sau khi sửa Khối 2. Chỉ Khối 1 còn xanh; từ Khối 2 trở đi các giá trị băm đổi hết và hiện màu đỏ.

Figure 2.1. *The top row is the original chain of four blocks; the bottom row is the chain after editing Block 2. Only Block 1 stays blue; from Block 2 on, every hash changes and turns red.*

Muốn che dấu vết, kẻ gian phải tính lại giá trị băm của mọi khối sau chỗ sửa và thuyết phục cả mạng chấp nhận chuỗi mới. Việc tính lại tự nó không khó. Cái khó là Bitcoin bắt mỗi khối phải kèm một bằng chứng công việc (proof of work: máy phải thử hàng triệu lần mới tìm ra), tốn điện, như Chương 4 sẽ nói. Con trỏ băm làm việc sửa lộ ra, còn bằng chứng công việc làm việc sửa trở nên đắt.

To hide the trace, the cheat must recompute the hash of every block after the edit and persuade the whole network to accept the new chain. Recomputing is not hard in itself. The hard part is that Bitcoin makes every block carry a costly proof of work (a proof that machines had to try millions of times to find), as Chapter 4 explains. Hash pointers make an edit visible; proof of work makes it expensive.

> **LỖI HAY GẶP / COMMON MISTAKE –** Cho rằng chuỗi khối "không thể sửa". Chính xác hơn: sửa được nhưng để lại dấu vết lộ ngay, và muốn che dấu vết phải làm lại công việc của mọi khối sau đó.
> *Believing a blockchain "cannot be edited". More exactly: it can be edited, but the edit shows at once, and hiding it means redoing the work of every later block.*

2.4. Cây Merkle và chứng minh thuộc cây – *2.4. The Merkle tree and the proof of membership*

Một khối có thể chứa hàng nghìn giao dịch. Nếu muốn nói "khối này có giao dịch của Hà My", bạn không muốn gửi cả khối. Cây Merkle (Merkle tree, do Ralph Merkle đề xuất năm 1979) giải bài toán này. Nó gom hàng nghìn giao dịch vào một giá trị băm duy nhất gọi là gốc Merkle (Merkle root), và cho phép chứng minh một giao dịch thuộc khối chỉ với vài giá trị băm.

A block may hold thousands of transactions. To say "this block contains Ha My's transaction", you do not want to send the whole block. The Merkle tree (proposed by Ralph Merkle in 1979) solves this. It gathers thousands of transactions into a single hash called the Merkle root, and lets you prove that one transaction belongs to the block with only a few hashes.

Cách dựng, bạn làm từ dưới lên. Bước 1: băm từng giao dịch, ta có tầng lá. Bước 2: ghép hai giá trị băm kề nhau thành một cặp rồi băm cặp đó, ta có tầng trên. Bước 3: lặp lại cho đến khi chỉ còn một giá trị, đó là gốc Merkle. Bước 4: nếu một tầng có số lẻ giá trị, nhân đôi giá trị cuối để đủ cặp (cách Bitcoin dùng).

You build it from the bottom up. Step 1: hash each transaction to get the leaf layer. Step 2: join two neighbouring hashes into a pair and hash the pair to get the layer above. Step 3: repeat until one value remains; that is the Merkle root. Step 4: if a layer has an odd number of values, duplicate the last one to complete the pair (the way Bitcoin does it).

$$\text{Gốc} = H(\, H(\, H(T1) \,\|\, H(T2)\,) \,\|\, H(\, H(T3) \,\|\, H(T4)\,)\,) \qquad (2.2)$$

Chứng minh thuộc cây (Merkle proof) làm như sau, lấy ví dụ chứng minh T3 thuộc khối. Bước 1: người chứng minh gửi giá trị băm của T4, là "người anh em" cùng cặp với T3. Bước 2: người kiểm tra tự băm T3, ghép với giá trị của T4 rồi băm, được nhánh bên phải.

Bước 3: người chứng minh gửi thêm giá trị nhánh bên trái (ghép T1 và T2). Bước 4: người kiểm tra ghép hai nhánh, băm, rồi so kết quả với gốc Merkle đã công bố trong đầu khối (phần mở đầu của khối, nơi ghi gốc Merkle).

A Merkle proof works as follows, taking the proof that T3 belongs to the block. Step 1: the prover sends the hash of T4, the sibling paired with T3. Step 2: the verifier hashes T3 itself, joins it to the value of T4 and hashes, getting the right-hand branch. Step 3: the prover also sends the value of the left-hand branch (T1 joined with T2). Step 4: the verifier joins the two branches, hashes, and compares the result with the Merkle root published in the block header (the opening part of a block, where the Merkle root is written).

```
import hashlib

def sha(b):
    return hashlib.sha256(b).digest()

def cay(giao_dich):
    tang = [sha(x.encode()) for x in giao_dich]
    tat_ca = [tang]
    while len(tang) > 1:
        if len(tang) % 2:
            tang = tang + [tang[-1]]
        tang = [sha(tang[i] + tang[i + 1])
                for i in range(0, len(tang), 2)]
        tat_ca.append(tang)
    return tat_ca

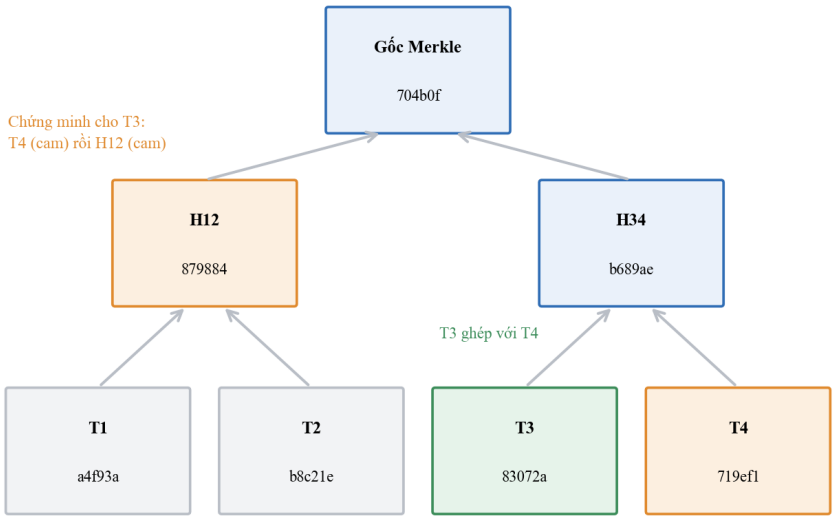
gd = ["T1: HaMy gui Quan 5", "T2: Quan gui Linh 2",
      "T3: Linh gui LamVien 1", "T4: LamVien gui HaMy 3"]
c = cay(gd)
print("Goc Merkle:", c[-1][0].hex()[:16] + "...")
x = sha(gd[2].encode())
x = sha(x + c[0][3])       # T3 ben trai, T4 (anh em) ben phai
x = sha(c[1][0] + x)       # nhanh T1+T2 ben trai, nhanh vua tinh ben phai
print("Tinh lai tu T3:", x.hex()[:16] + "...")
print("Khop goc:", x == c[-1][0])
gd[2] = "T3: Linh gui LamVien 9"
print("Sua T3, goc moi:", cay(gd)[-1][0].hex()[:16] + "...")
```

Kết quả chạy / *Output*

```
Goc Merkle: 704b0f3797e6b427...
Tinh lai tu T3: 704b0f3797e6b427...
Khop goc: True
Sua T3, goc moi: d609a1b8000b09c8...
```

Bài mẫu với bốn giao dịch của Hà My, Quan, Linh và công ty Lâm Viên. Gốc Merkle bắt đầu bằng 704b0f3797e6b427. Để chứng minh T3, người kiểm tra nhận hai giá trị băm (của T4 và của nhánh T1 ghép T2), tự tính lại và ra đúng gốc đó. Khi đổi T3 từ "1" thành "9", gốc mới là d609a1b8000b09c8, khác hẳn.

Worked example with four transactions by Ha My, Quan, Linh and Lam Vien company. The Merkle root begins 704b0f3797e6b427. To prove T3, the verifier receives two hashes (of T4 and of the branch T1 joined to T2), recomputes and reaches that same root. When T3 changes from "1" to "9", the new root is d609a1b8000b09c8, entirely different.



Hình 2.2. Bốn giao dịch T1 đến T4 ở hàng dưới, hai nhánh H12 và H34 ở giữa, gốc Merkle ở trên cùng. Muốn chứng minh T3 (màu xanh lá), chỉ cần hai giá trị màu cam: T4 và H12.

Figure 2.2. *Four transactions T1 to T4 on the bottom row, two branches H12 and H34 in the middle, the Merkle root at the top. To prove T3 (green) you need only the two orange values: T4 and H12.*

Vì sao cách này tiết kiệm? Với n giao dịch, độ dài chứng minh chỉ bằng số tầng của cây, tức $\lceil \log_2 n \rceil$ giá trị băm. Với 1.000 giao dịch, đó là 10 giá trị băm, tức 320 byte, trong khi cả danh sách giá trị băm của 1.000 giao dịch nặng 32.000 byte. Nút nhẹ (light node, chỉ giữ phần đầu khối) nhờ cách này mà kiểm được giao dịch của mình mà không tải cả khối.

Why is this thrifty? With n transactions, the proof is as long as the number of tree levels, $\lceil \log_2 n \rceil$ hashes. For 1,000 transactions that is 10 hashes, or 320 bytes, while the full list of hashes for 1,000 transactions weighs 32,000 bytes. A light node (which keeps only block headers) can check its own transaction this way without downloading the whole block.

$$\text{Độ dài chứng minh Merkle} = \lceil \log_2 n \rceil \text{ giá trị băm} \tag{2.3}$$

> **LỖI HAY GẶP / COMMON MISTAKE –** Quên ghép đúng thứ tự trái – phải khi tính lại gốc. H(A ‖ B) khác H(B ‖ A), nên người kiểm tra phải biết giá trị anh em nằm bên trái hay bên phải.
>
> *Forgetting the left and right order when recomputing the root. H(A ‖ B) differs from H(B ‖ A), so the verifier must know whether the sibling sits on the left or the right.*

2.5. Mật mã khóa công khai và chữ ký số – *2.5. Public key cryptography and digital signatures*

Hãy nghĩ đến hòm thư công cộng đặt trước cổng. Ai đi qua cũng bỏ thư vào được qua cái khe, nhưng chỉ chủ nhà có chìa mở nắp lấy thư. Mật mã khóa công khai (public key cryptography) tạo ra một cặp khóa như vậy. Khóa công khai (public key) giống cái khe: bạn đưa cho mọi người. Khóa bí mật (private key) giống chìa: chỉ mình bạn giữ.

Picture a public postbox at your gate. Anyone passing can drop a letter through the slot, but only the owner has the key to open the lid and take the letters out. Public key cryptography builds

such a pair. The public key is like the slot: you hand it to everyone. The private key is like the key to the lid: only you keep it.

Trong tiền số, cặp khóa này dùng theo chiều ngược lại để ký. Chữ ký số (digital signature) là bằng chứng rằng chủ của khóa bí mật đã đồng ý với một tin nhắn cụ thể, mà không cần lộ khóa bí mật. Cũng như chữ ký tay trên giấy, nhưng chữ ký số gắn chặt với nội dung: đổi một chữ trong tin nhắn thì chữ ký cũ không còn đúng.

In digital money the pair is used the other way round, to sign. A digital signature is proof that the owner of the private key agreed to one specific message, without revealing the private key. It is like a handwritten signature on paper, but it is tied to the content: change one word in the message and the old signature no longer fits.

Ba thao tác tạo nên một hệ chữ ký số, mỗi thao tác ai làm và làm gì như sau.

Three operations make up a digital signature scheme. Who does what is set out as follows.

1. Tạo khóa. Hà My mở ví (wallet, ứng dụng giữ khóa) của mình. Ví lấy một số ngẫu nhiên làm khóa bí mật, rồi tính từ đó ra khóa công khai. Hà My công bố khóa công khai, cất kỹ khóa bí mật.
   Generate keys. Ha My opens her wallet (an app that holds keys). The wallet draws a random number as the private key, then computes the public key from it. Ha My publishes the public key and keeps the private key safe.
2. Ký. Muốn gửi Quan 5 đồng Sen Vàng, ví băm nội dung lệnh rồi dùng khóa bí mật tính ra chữ ký, thường gồm hai số. Lệnh và chữ ký được gửi lên mạng cùng nhau.
   Sign. To send Quan 5 Sen Vang coins, the wallet hashes the content of the order and uses the private key to compute the signature, usually two numbers. The order and signature go to the network together.
3. Kiểm. Một nút mạng (node, máy tính tham gia mạng) nhận lệnh. Nó băm lại nội dung, rồi dùng khóa công khai của Hà My kiểm chữ ký có khớp không. Khớp thì nhận lệnh, lệch thì bỏ. Nút mạng không cần biết khóa bí mật.
   Verify. A network node (a computer taking part in the network) receives the order. It hashes the content again and uses Ha My's public key to check whether the signature fits. If it fits, the order is accepted; if not, it is dropped. The node never needs the private key.

Chữ ký số phải thỏa ba điều. Chỉ chủ khóa bí mật ký được. Ai cũng kiểm được bằng khóa công khai. Chữ ký gắn với đúng một tin nhắn, nên không thể cắt chữ ký của lệnh này dán sang lệnh khác. Đó là tính chất không giả mạo được (unforgeability). Mục 2.6 và 2.7 cho thấy phép tính cụ thể đứng sau.

A digital signature must meet three conditions. Only the owner of the private key can sign. Anyone can verify with the public key. The signature is tied to exactly one message, so it cannot be cut from one order and pasted onto another. This is called unforgeability. Sections 2.6 and 2.7 show the actual computation behind it.

Ba khái niệm hay bị nhầm với nhau là hàm băm, mã hóa và chữ ký số. Bảng sau đặt chúng cạnh nhau.

Three concepts are often confused: hash, encryption and digital signature. The table sets them side by side.

Khái niệm *Concept*	**Mục đích** *Purpose*	**Cần khóa không** *Needs a key?*	**Quay lại dữ liệu gốc được không** *Can it be reversed?*
Hàm băm *Hash function*	Tạo dấu vân tay để kiểm dữ liệu có bị sửa. *Makes a fingerprint to check whether data was altered.*	Không *No*	Không *No*
Mã hóa *Encryption*	Giữ bí mật nội dung, chỉ người có chìa đọc được. *Keeps content secret; only the key holder can read it.*	Có *Yes*	Có, bằng khóa giải mã *Yes, with the decryption key*
Chữ ký số *Digital signature*	Chứng minh chủ khóa bí mật đồng ý với đúng tin nhắn này. *Proves the private key owner agreed to exactly this message.*	Có, một cặp khóa *Yes, a key pair*	Không có gì để quay lại, chỉ kiểm đúng hay sai *Nothing to reverse; it only checks true or false*

Ứng dụng cho Quan và Linh. Anh Quân vận hành hệ thống lưu ký (giữ hộ khóa cho khách hàng) của công ty. Khi chị Linh yêu cầu chuyển một khoản, hệ thống chỉ thực hiện nếu chữ ký khớp khóa công khai đã đăng ký của chị. Ai làm giả lệnh mà không có khóa bí mật của chị Linh thì bước kiểm của Quân loại ngay.

Applied to Quan and Linh. Quan runs the company's custody system (which keeps keys on behalf of clients). When Linh asks for a transfer, the system carries it out only if the signature fits her registered public key. Anyone forging the order without Linh's private key is rejected at Quan's verification step.

> **PHẢI THUỘC / MEMORISE –** Khóa công khai đưa cho mọi người, khóa bí mật chỉ chủ giữ. Ký dùng khóa bí mật, kiểm dùng khóa công khai. Chữ ký gắn với đúng một tin nhắn: đổi nội dung thì chữ ký cũ vô hiệu.
> *The public key is given to everyone; the private key only the owner keeps. Signing uses the private key, verifying uses the public key. A signature is tied to exactly one message: change the content and the old signature is void.*

> **LỖI HAY GẶP / COMMON MISTAKE –** Nghĩ rằng "khóa công khai dùng để ký, khóa bí mật dùng để kiểm". Ngược lại: ký bằng khóa bí mật, kiểm bằng khóa công khai. Ai nhìn thấy khóa công khai cũng kiểm được, nhưng không ai ký thay được.
> *Thinking "the public key signs and the private key verifies". It is the other way round: sign with the private key, verify with the public key. Anyone who sees the public key can verify, but nobody can sign in your place.*

2.6. Đường cong elliptic thu nhỏ: cộng điểm và nhân vô hướng – *2.6. A miniature elliptic curve: adding points and scalar multiplication*

Muốn có cặp khóa công khai – bí mật, cần một phép tính đi xuôi dễ nhưng đi ngược gần như không thể. Bitcoin chọn phép tính trên đường cong elliptic (elliptic curve). Đừng lo

về tên gọi: với bài này, đó chỉ là một tập hợp điểm (x, y) thỏa một phương trình, kèm quy tắc "cộng" hai điểm ra điểm thứ ba.

To get a public and private key pair you need a calculation that is easy forwards and almost impossible backwards. Bitcoin chose a calculation on an elliptic curve. Do not worry about the name: for this section it is just a set of points (x, y) that satisfy an equation, plus a rule for "adding" two points to get a third.

Bitcoin dùng phương trình $y^2 = x^3 + 7$, tính theo số học đồng hồ. Số học đồng hồ (modular arithmetic) giống như kim giờ: sau 12 giờ quay về 0. Ở đây "đồng hồ" có p số, và mọi kết quả đều lấy phần dư khi chia cho p. Bitcoin dùng một số nguyên tố p cỡ 2^{256}. Để bạn tính tay được, sách dùng p = 43.

Bitcoin uses the equation $y^2 = x^3 + 7$, computed with clock arithmetic. Clock arithmetic (modular arithmetic) works like the hour hand: after 12 o'clock it goes back to 0. Here the "clock" has p numbers, and every result is the remainder after dividing by p. Bitcoin uses a prime p around 2^{256}. So that you can compute by hand, this book uses p = 43.

Với p = 43, có 30 điểm (x, y) thỏa phương trình, cộng thêm một điểm đặc biệt gọi là điểm vô cực (point at infinity), đóng vai số 0 của phép cộng. Chọn điểm xuất phát G = (2, 12), gọi là điểm gốc (generator). Hình 2.3 vẽ 30 điểm đó và sáu bội đầu tiên của G.

With p = 43 there are 30 points (x, y) that satisfy the equation, plus one special point called the point at infinity, which plays the role of zero for addition. Take the starting point G = (2, 12), called the generator. Figure 2.3 draws those 30 points and the first six multiples of G.

Quy tắc cộng hai điểm $A = (x_1, y_1)$ và $B = (x_2, y_2)$ làm theo từng bước. Bước 1: tính độ dốc λ. Nếu A khác B, $\lambda = (y_2 - y_1) / (x_2 - x_1)$; nếu A trùng B (nhân đôi), $\lambda = 3x_1^2 / (2y_1)$. Phép chia ở đây là nhân với số nghịch đảo theo mod 43. Bước 2: tính $x_3 = \lambda^2 - x_1 - x_2$. Bước 3: tính $y_3 = \lambda(x_1 - x_3) - y_1$. Bước 4: lấy phần dư mod 43 cho cả hai số, ta có A + B = (x_3, y_3).

The rule for adding two points $A = (x_1, y_1)$ and $B = (x_2, y_2)$ goes step by step. Step 1: compute the slope λ. If A differs from B, $\lambda = (y_2 - y_1) / (x_2 - x_1)$; if A equals B (doubling), $\lambda = 3x_1^2 / (2y_1)$. Division here means multiplying by the inverse under mod 43. Step 2: compute $x_3 = \lambda^2 - x_1 - x_2$. Step 3: compute $y_3 = \lambda(x_1 - x_3) - y_1$. Step 4: take both numbers mod 43; then A + B = (x_3, y_3).

$$\lambda = (y_2 - y_1)/(x_2 - x_1);\ x_3 = \lambda^2 - x_1 - x_2;\ y_3 = \lambda(x_1 - x_3) - y_1 \pmod p \quad (2.4)$$

Bài mẫu 1: tính 2G và 3G. Nhân đôi G = (2, 12): $\lambda = 3 * 2^2 / (2 * 12) = 12 / 24 = 1/2$. Trong mod 43, nghịch đảo của 2 là 22, vì $2 * 22 = 44$, dư 1. Vậy λ = 22. $x_3 = 22^2 - 2 * 2 = 480$, dư 7. $y_3 = 22 * (2 - 7) - 12 = -122$, dư 7. Vậy 2G = (7, 7). Tiếp theo 3G = G + 2G: $\lambda = (7 - 12) / (7 - 2) = -5 / 5 = -1$, dư 42. $x_3 = 42^2 - 2 - 7 = 1.755$, dư 35. $y_3 = 42 * (2 - 35) - 12$, dư 21. Vậy 3G = (35, 21).

Worked example 1: compute 2G and 3G. Doubling G = (2, 12): $\lambda = 3 * 2^2 / (2 * 12) = 12 / 24 = 1/2$. In mod 43 the inverse of 2 is 22, because $2 * 22 = 44$, remainder 1. So λ = 22. $x_3 = 22^2 - 2 * 2 = 480$, remainder 7. $y_3 = 22 * (2 - 7) - 12 = -122$, remainder 7. So 2G = (7, 7). Next 3G = G + 2G: $\lambda = (7 - 12) / (7 - 2) = -5 / 5 = -1$, remainder 42. $x_3 = 42^2 - 2 - 7 = 1,755$, remainder 35. $y_3 = 42 * (2 - 35) - 12$, remainder 21. So 3G = (35, 21).

Cộng G với chính nó k lần ta được k ∗ G, gọi là nhân vô hướng (scalar multiplication). Đoạn mã sau làm đúng phép cộng điểm vừa tính tay, rồi nhân G lên nhiều lần cho đến khi quay về điểm vô cực.

Adding G to itself k times gives k ∗ G, called scalar multiplication. The code below performs the point addition you just did by hand, then multiplies G up until it returns to the point at infinity.

```
p, G = 43, (2, 12)          # duong cong y^2 = x^3 + 7 (mod 43)

def cong(P, Q):
    if P is None or Q is None:
        return P or Q
    (x1, y1), (x2, y2) = P, Q
    if x1 == x2 and (y1 + y2) % p == 0:
        return None
    if P == Q:
        m = 3 * x1 * x1 * pow(2 * y1, -1, p) % p
    else:
        m = (y2 - y1) * pow(x2 - x1, -1, p) % p
    x3 = (m * m - x1 - x2) % p
    return (x3, (m * (x1 - x3) - y1) % p)

def nhan(k, P):
    R = None
    for _ in range(k):
        R = cong(R, P)
    return R

print("G nam tren duong cong:", (G[1]**2 - G[0]**3 - 7) % p == 0)
for k in range(1, 7):
    print(k, "* G =", nhan(k, G))
print("31 * G =", nhan(31, G), "(None la diem vo cuc)")
```

Kết quả chạy / *Output*

```
G nam tren duong cong: True
1 * G = (2, 12)
2 * G = (7, 7)
3 * G = (35, 21)
4 * G = (21, 18)
5 * G = (12, 12)
6 * G = (29, 31)
31 * G = None (None la diem vo cuc)
```

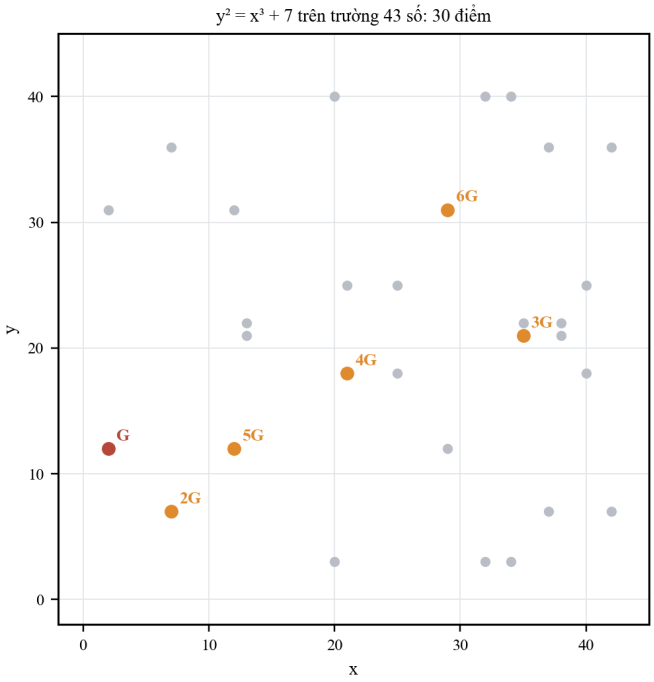
Các bội của G lặp lại sau 31 bước: 31 ∗ G là điểm vô cực. Số 31 gọi là bậc (order) của G, ký hiệu n. Bội của G chỉ có 31 giá trị, nên với đường cong thu nhỏ này kẻ gian thử tối đa 30 lần là tìm ra k. Với đường cong thật của Bitcoin (tên secp256k1, cùng dạng $y^2 = x^3 + 7$), p và n đều cỡ 2^{256}, nên cách thử này vô vọng.

The multiples of G repeat after 31 steps: 31 ∗ G is the point at infinity. The number 31 is called the order of G, written n. Multiples of G take only 31 values, so on this miniature curve a cheat needs at most 30 tries to find k. On Bitcoin's real curve (named secp256k1, of the same form $y^2 = x^3 + 7$), p and n are both around 2^{256}, so that approach is hopeless.

Đây chính là cặp khóa. Hà My chọn khóa bí mật k = 13. Khóa công khai là Q = 13 ∗ G = (13, 21). Đi xuôi (biết k, tính Q) chỉ cần vài phép cộng. Đi ngược (biết Q và G, tìm k) gọi là bài toán logarit rời rạc trên đường cong elliptic. Với số lớn, chưa ai biết cách giải nhanh.

This is exactly the key pair. Ha My picks the private key k = 13. The public key is Q = 13 ∗ G = (13, 21). Going forwards (know k, compute Q) takes a few additions. Going backwards (know Q and G, find k) is called the elliptic curve discrete logarithm problem. For large numbers no fast way to solve it is known.

$$\text{Khóa công khai } Q = k * G \text{ (k là khóa bí mật, G là điểm gốc)} \qquad (2.5)$$



Hình 2.3. Ba mươi chấm xám là các điểm của đường cong thu nhỏ $y^2 = x^3 + 7$ trên 43 số. Chấm đỏ là G, các chấm cam là 2G đến 6G; các bội của G nhảy khắp nơi, không theo đường nào có thể đoán.

Figure 2.3. *The thirty grey dots are the points of the miniature curve $y^2 = x^3 + 7$ over 43 numbers. The red dot is G and the orange dots are 2G to 6G; the multiples of G jump around with no guessable path.*

> **LỖI HAY GẶP / COMMON MISTAKE –** Vẽ đường cong elliptic của Bitcoin như một đường trơn liên tục. Trên trường hữu hạn nó chỉ là một đám điểm rời rạc, như Hình 2.3. Đường trơn chỉ là hình minh họa trên số thực.
> *Drawing Bitcoin's elliptic curve as a smooth continuous line. Over a finite field it is only a cloud of separate points, as in Figure 2.3. The smooth line is only an illustration over real numbers.*

2.7. ECDSA và Schnorr: ký và kiểm bằng phép tính – *2.7. ECDSA and Schnorr: signing and verifying by calculation*

Bây giờ ghép đường cong với hàm băm để làm chữ ký. Thuật toán chữ ký số trên đường cong elliptic (ECDSA, Elliptic Curve Digital Signature Algorithm) là loại chữ ký Bitcoin dùng từ đầu. Để dễ tính, sách chuyển sang đường cong $y^2 = x^3 + 7$ trên p = 163, điểm gốc G = (2, 34), bậc n = 139 (đã kiểm: 139 ∗ G là điểm vô cực). Khóa bí mật của Hà My là d = 57, khóa công khai Q = d ∗ G.

Now combine the curve with the hash function to make a signature. The Elliptic Curve Digital Signature Algorithm (ECDSA) is the kind of signature Bitcoin has used from the start. To keep

the sums easy, the book moves to the curve $y^2 = x^3 + 7$ with $p = 163$, generator $G = (2, 34)$ and order $n = 139$ (checked: $139 * G$ is the point at infinity). Ha My's private key is $d = 57$ and her public key is $Q = d * G$.

Ký làm theo bốn bước. Bước 1: băm tin nhắn, lấy phần dư khi chia cho n, ta có z. Bước 2: chọn một số dùng một lần k (nonce, "number used once"), tính điểm $k * G$ và lấy hoành độ của nó mod n, gọi là r. Bước 3: tính $s = k^{-1} (z + r * d) \bmod n$. Bước 4: chữ ký là cặp (r, s).

Signing takes four steps. Step 1: hash the message and take the remainder on division by n; call it z. Step 2: choose a number used once, k (a nonce), compute the point $k * G$ and take its x coordinate mod n; call it r. Step 3: compute $s = k^{-1} (z + r * d) \bmod n$. Step 4: the signature is the pair (r, s).

Kiểm cũng bốn bước và chỉ cần khóa công khai Q. Bước 1: tính z từ tin nhắn nhận được. Bước 2: tính $w = s^{-1} \bmod n$. Bước 3: tính $u_1 = z * w$ và $u_2 = r * w$. Bước 4: tính điểm $u_1 * G + u_2 * Q$; chữ ký đúng khi hoành độ của điểm đó mod n bằng r.

Verifying is also four steps and needs only the public key Q. Step 1: compute z from the received message. Step 2: compute $w = s^{-1} \bmod n$. Step 3: compute $u_1 = z * w$ and $u_2 = r * w$. Step 4: compute the point $u_1 * G + u_2 * Q$; the signature is valid when its x coordinate mod n equals r.

$$s = k^{-1} (z + r * d) \bmod n; \quad \text{kiểm: } u_1 = z * s^{-1},\ u_2 = r * s^{-1},\ x(u_1 * G + u_2 * Q) \equiv r \pmod n \qquad (2.6)$$

```
import hashlib
p, n, G = 163, 139, (2, 34)      # y^2 = x^3 + 7 (mod 163)

def cong(P, Q):
    if P is None or Q is None:
        return P or Q
    (x1, y1), (x2, y2) = P, Q
    if x1 == x2 and (y1 + y2) % p == 0:
        return None
    if P == Q:
        m = 3 * x1 * x1 * pow(2 * y1, -1, p) % p
    else:
        m = (y2 - y1) * pow(x2 - x1, -1, p) % p
    x3 = (m * m - x1 - x2) % p
    return (x3, (m * (x1 - x3) - y1) % p)

def nhan(k, P):
    R = None
    for _ in range(k):
        R = cong(R, P)
    return R

def bam(tin):
    h = hashlib.sha256(tin.encode()).hexdigest()
    return int(h, 16) % n

d, k = 57, 41        # khoa bi mat va so dung mot lan (do de bai dat)
Q = nhan(d, G)
tin = "HaMy gui Quan 5 Sen Vang"
r = nhan(k, G)[0] % n
s = pow(k, -1, n) * (bam(tin) + r * d) % n
print("Q =", Q, "| z =", bam(tin), "| (r, s) =", (r, s))

def kiem(tin, r, s):
```

```
    w = pow(s, -1, n)
    P = cong(nhan(bam(tin) * w % n, G), nhan(r * w % n, Q))
    return P is not None and P[0] % n == r
print("Tin that:", kiem(tin, r, s))
print("Tin sua :", kiem("HaMy gui Quan 50 Sen Vang", r, s))
```

Kết quả chạy / *Output*

```
Q = (11, 69) | z = 117 | (r, s) = (13, 65)
Tin that: True
Tin sua : False
```

Bài mẫu 2 đọc theo kết quả. Tin nhắn "HaMy gui Quan 5 Sen Vang" băm ra z = 117. Với k = 41, điểm k ∗ G có hoành độ mod 139 là r = 13. $s = 41^{-1} * (117 + 13 * 57) \bmod 139 = 65$. Khóa công khai Q = 57 ∗ G = (11, 69). Khi kiểm, $w = 65^{-1} = 77$, $u_1 = 113$, $u_2 = 28$, điểm tính ra là (152, 119), hoành độ 152 mod 139 = 13, đúng bằng r. Khi đổi 5 thành 50 trong tin nhắn, z đổi nên phép kiểm trả "False": chữ ký cũ không dùng được cho lệnh mới.

Worked example 2, read from the result. The message "HaMy gui Quan 5 Sen Vang" hashes to z = 117. With k = 41, the point k ∗ G has x coordinate mod 139 equal to r = 13. $s = 41^{-1} * (117 + 13 * 57) \bmod 139 = 65$. The public key is Q = 57 ∗ G = (11, 69). To verify, $w = 65^{-1} = 77$, $u_1 = 113$, $u_2 = 28$, the computed point is (152, 119), and 152 mod 139 = 13, exactly r. When 5 becomes 50 in the message, z changes and the check returns "False": the old signature cannot serve the new order.

Một điểm cần nhớ kỹ về số dùng một lần k. Nếu ký hai tin khác nhau mà dùng lại cùng k, kẻ nhìn thấy hai chữ ký giải được hệ phương trình và tìm ra khóa bí mật d. Vì vậy ví tốt tạo k theo cách không lặp lại, không bao giờ do người dùng tự đặt. Anh Quân kiểm điều này khi đánh giá phần mềm ví cho công ty.

One point to remember well about the number used once, k. If two different messages are signed with the same k, anyone who sees both signatures can solve the equations and find the private key d. So a good wallet creates k in a way that never repeats and is never chosen by the user. Quan checks this when assessing wallet software for the company.

Chữ ký Schnorr là một cách ký khác, đơn giản hơn. Người ký chọn k, tính R = k ∗ G, tính e bằng cách băm R cùng tin nhắn, rồi gửi (R, s) với s = k + e ∗ d mod n. Người kiểm thử s ∗ G có bằng R + e ∗ Q không. Phép kiểm này "tuyến tính": chữ ký của nhiều người cộng lại được thành một chữ ký, điều ECDSA khó làm. Bảng sau so hai loại.

The Schnorr signature is another, simpler way to sign. The signer picks k, computes R = k ∗ G, computes e by hashing R together with the message, and sends (R, s) with s = k + e ∗ d mod n. The verifier tests whether s ∗ G equals R + e ∗ Q. This check is "linear": signatures from several people can be added into one, which ECDSA finds hard. The table compares the two.

Tiêu chí *Criterion*	**ECDSA**	**Schnorr**
Công thức chữ ký *Signature formula*	$s = k^{-1} (z + r * d)$, cần phép chia (nghịch đảo) *$s = k^{-1} (z + r * d)$, needs a division (inverse)*	$s = k + e * d$, chỉ cần cộng và nhân *$s = k + e * d$, only addition and multiplication*
Gộp nhiều chữ ký *Combining signatures*	Khó, phải làm nhiều vòng trao đổi *Hard; needs several rounds of exchange*	Dễ, vì phép kiểm tuyến tính *Easy, because the check is linear*
Dùng trong Bitcoin *Use in Bitcoin*	Loại chữ ký có từ đầu *The signature type from the start*	Được thêm vào sau qua nâng cấp Taproot *Added later through the Taproot upgrade*

PHẢI THUỘC / MEMORISE – Ký ECDSA: z = băm tin nhắn, r = hoành độ của $k * G$, $s = k^{-1} (z + r * d) \bmod n$. Kiểm: điểm $u_1 * G + u_2 * Q$ phải có hoành độ bằng r. Không bao giờ dùng lại số k cho hai tin khác nhau.
ECDSA signing: z = hash of the message, r = x coordinate of $k * G$, $s = k^{-1} (z + r * d) \bmod n$. Verifying: the point $u_1 * G + u_2 * Q$ must have x coordinate equal to r. Never reuse k for two different messages.

LỖI HAY GẶP / COMMON MISTAKE – Ký xong rồi gửi cả khóa bí mật d kèm chữ ký "để người nhận kiểm". Người kiểm chỉ cần khóa công khai Q. Hễ khóa bí mật rời máy của chủ thì coi như đã mất.
Sending the private key d along with the signature "so the receiver can check". The verifier needs only the public key Q. Once the private key leaves its owner's device, treat it as lost.

2.8. Từ khóa bí mật đến khóa công khai đến địa chỉ – *2.8. From private key to public key to address*

Địa chỉ là chuỗi bạn đưa cho người khác để họ gửi tiền số vào. Nó giống số tài khoản ngân hàng, nhưng không do ngân hàng cấp: ví của bạn tự tính ra từ khóa công khai. Có hai lý do không dùng thẳng khóa công khai. Địa chỉ ngắn hơn, và băm thêm một lớp che khóa công khai cho đến khi bạn tiêu tiền.
An address is the string you give others so they can send digital money to you. It resembles a bank account number, but no bank issues it: your wallet computes it from your public key. There are two reasons not to use the public key directly. The address is shorter, and an extra hash hides the public key until you actually spend.

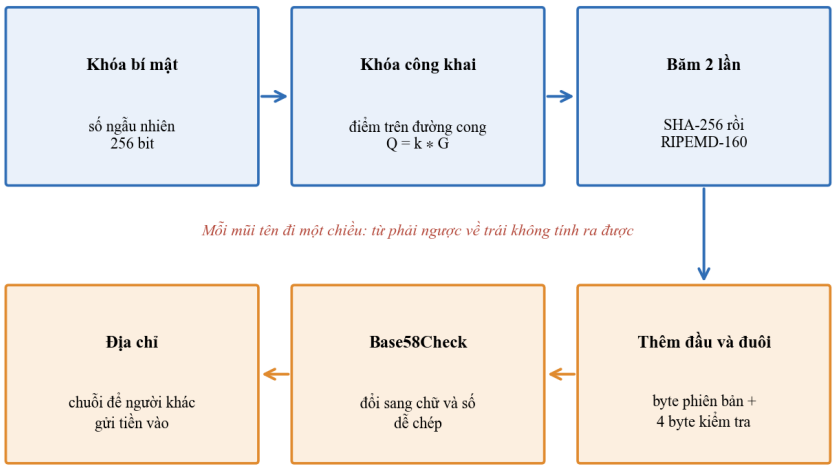
Ví tính địa chỉ kiểu Base58Check theo sáu bước. Bước 1: lấy khóa công khai. Bước 2: băm bằng SHA-256. Bước 3: băm kết quả bằng RIPEMD-160, ra 160 bit (20 byte). Bước 4: gắn một byte phiên bản ở đầu (00 cho địa chỉ kiểu cũ, làm địa chỉ bắt đầu bằng chữ số 1). Bước 5: băm hai lần SHA-256 chuỗi 21 byte đó, lấy 4 byte đầu làm mã kiểm tra và gắn vào cuối. Bước 6: đổi cả 25 byte sang chữ và số theo hệ Base58.

The wallet computes a Base58Check address in six steps. Step 1: take the public key. Step 2: hash it with SHA-256. Step 3: hash the result with RIPEMD-160, giving 160 bits (20 bytes). Step 4: attach a version byte at the front (00 for the old-style address, which makes the address begin with the digit 1). Step 5: double hash that 21-byte string with SHA-256, take the first 4 bytes as the checksum and attach them at the end. Step 6: convert all 25 bytes into letters and digits in base 58.

Base58 dùng 58 ký tự: chữ số và chữ cái, bỏ bốn ký tự dễ nhìn nhầm là số 0, chữ O hoa, chữ I hoa và chữ l thường. Nhờ vậy người chép địa chỉ bằng tay ít nhầm hơn.

Base58 uses 58 characters: digits and letters, leaving out the four that are easily mistaken: the digit 0, capital O, capital I and lowercase l. People copying an address by hand then make fewer mistakes.

$$\text{Địa chỉ} = \text{Base58}(\, v \,\|\, \text{RIPEMD160}(\text{SHA256}(Q)) \,\|\, KT\,),\ KT = 4 \text{ byte đầu của } \text{SHA256}(\text{SHA256}(v \,\|\, \text{RIPEMD160}(\text{SHA256}(Q)))) \qquad (2.7)$$



Hình 2.4. Dòng trên đi từ khóa bí mật đến băm hai lần, dòng dưới gắn đầu, đuôi và đổi sang Base58Check ra địa chỉ. Mọi mũi tên đi một chiều, nên người ngoài nhìn địa chỉ không suy ngược ra khóa bí mật.

Figure 2.4. *The top row runs from the private key to the double hash, and the bottom row adds the front and tail and converts to Base58Check to give the address. Every arrow goes one way, so an outsider cannot work back from the address to the private key.*

Đoạn mã sau tạo địa chỉ minh họa từ một chuỗi byte tự đặt đóng vai khóa công khai nén. Chuỗi này không thuộc khóa nào, nên địa chỉ chỉ để xem cách làm, không dùng để nhận tiền.

The code below builds an illustrative address from a self-chosen byte string standing in for a compressed public key. That string belongs to no real key, so the address is only to show the method and cannot receive money.

```
import hashlib
B58 = "123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz"


def sha(b):
```

```
    return hashlib.sha256(b).digest()


def base58(b):
    n = int.from_bytes(b, "big")
    s = ""
    while n:
        n, r = divmod(n, 58)
        s = B58[r] + s
    dau = len(b) - len(b.lstrip(b"\0"))
    return "1" * dau + s


khoa_ck = b"\x02" + sha(b"khoa cong khai cua Ha My (minh hoa)")
h160 = hashlib.new("ripemd160", sha(khoa_ck)).digest()
tai_trong = b"\x00" + h160
kiem = sha(sha(tai_trong))[:4]
dia_chi = base58(tai_trong + kiem)
print("Dia chi minh hoa:", dia_chi)
print("Ma kiem tra (4 byte):", kiem.hex())
print("Do dai:", len(dia_chi), "ky tu")
```

Kết quả chạy / *Output*

```
Dia chi minh hoa: 13ng4YMHPTHTBkK5tSZbV8t6bsnuS6e8yR
Ma kiem tra (4 byte): 1d052dfc
Do dai: 34 ky tu
```

Địa chỉ minh họa là 13ng4YMHPTHTBkK5tSZbV8t6bsnuS6e8yR, dài 34 ký tự và bắt đầu bằng 1 vì byte phiên bản là 00. Mã kiểm tra 4 byte là 1d052dfc. Mã kiểm tra có tác dụng gì? Đoạn mã sau giải ngược địa chỉ, tính lại 4 byte và so. Rồi nó đổi đúng một ký tự để xem điều gì xảy ra.

The illustrative address is 13ng4YMHPTHTBkK5tSZbV8t6bsnuS6e8yR, 34 characters long, and begins with 1 because the version byte is 00. The 4-byte checksum is 1d052dfc. What does the checksum do? The next code decodes the address, recomputes the 4 bytes and compares. Then it changes exactly one character to see what happens.

```
import hashlib
B58 = "123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz"


def sha(b):
    return hashlib.sha256(b).digest()


def hop_le(dia_chi):
    n = 0
    for ch in dia_chi:
        n = n * 58 + B58.index(ch)
    b = n.to_bytes(25, "big")
    return sha(sha(b[:21]))[:4] == b[21:]


dc = "13ng4YMHPTHTBkK5tSZbV8t6bsnuS6e8yR"
i = 10
sai = dc[:i] + ("a" if dc[i] != "a" else "b") + dc[i + 1:]
print("Dia chi goc :", dc, hop_le(dc))
print("Go sai 1 chu:", sai, hop_le(sai))
```

Kết quả chạy / *Output*

```
Dia chi goc : 13ng4YMHPTHTBkK5tSZbV8t6bsnuS6e8yR True
Go sai 1 chu: 13ng4YMHPTaTBkK5tSZbV8t6bsnuS6e8yR False
```

Địa chỉ gốc qua phép kiểm, địa chỉ gõ sai một ký tự bị loại. Ví của bạn vì thế báo "địa chỉ không hợp lệ" thay vì gửi tiền vào một nơi không ai giữ. Mã kiểm tra chỉ bắt lỗi gõ nhầm,

không chứng minh địa chỉ có chủ. Bạn vẫn có thể gõ đúng một địa chỉ hợp lệ của người lạ.

The original address passes the check and the mistyped one is rejected. Your wallet therefore says "invalid address" instead of sending money to a place nobody holds. The checksum only catches typing slips; it does not prove the address has an owner. You can still type a perfectly valid address that belongs to a stranger.

Địa chỉ Bech32 (bắt đầu bằng bc1) là kiểu mới hơn. Nó chỉ dùng chữ thường nên không lẫn hoa thường, dùng bảng 32 ký tự, và mã kiểm tra mạnh hơn, phát hiện lỗi tốt hơn và giúp chỉ ra vị trí gõ sai. Cách tính vẫn đi từ khóa công khai qua băm; khác ở bảng ký tự và mã kiểm tra. Sách chỉ cần bạn nhận ra bc1 là một kiểu địa chỉ hợp lệ.

A Bech32 address (starting with bc1) is the newer kind. It uses lowercase only so case cannot be confused, uses a 32-character table, and has a stronger checksum that detects errors better and helps locate the typo. The computation still goes from the public key through hashes; the differences are the character table and the checksum. You only need to recognise bc1 as a valid address style.

> **LỖI HAY GẶP / COMMON MISTAKE –** Nghĩ địa chỉ là "tài khoản chứa tiền" và chỉ ví ban đầu mới dùng được nó. Địa chỉ chỉ là dấu vân tay của khóa công khai. Ai giữ khóa bí mật khớp với nó thì ký chuyển được số tiền đã gửi về đó.
> *Thinking an address is an "account holding money" that only the original wallet can use. An address is just a fingerprint of a public key. Whoever holds the matching private key can sign to move the money sent to it.*

2.9. Sinh khóa bí mật phải ngẫu nhiên: chuyện ví não – *2.9. Private keys must be random: the story of brain wallets*

Toàn bộ sức mạnh của chữ ký số nằm ở chỗ không ai đoán ra khóa bí mật. Khóa bí mật là một số cỡ 2^{256}, tức có khoảng $1{,}16 * 10^{77}$ khả năng. Điều đó chỉ đúng nếu số được chọn ngẫu nhiên. Một số do con người nghĩ ra, dù trông dài và phức tạp, thuộc về một tập nhỏ hơn nhiều những số người ta hay nghĩ tới.

All the strength of a digital signature rests on nobody being able to guess the private key. A private key is a number around 2^{256}, about $1.16 * 10^{77}$ possibilities. That holds only if the number is chosen at random. A number a person thinks up, however long and complicated it looks, belongs to a much smaller set of numbers people tend to think of.

Ví não (brain wallet) là kiểu lấy một câu mình nhớ trong đầu, băm bằng SHA-256, rồi dùng kết quả làm khóa bí mật. Thuận tiện vì không phải chép khóa ra giấy. Nguy hiểm vì kẻ xấu lập sẵn một danh sách câu hay gặp (câu hát, thành ngữ, mật khẩu phổ biến), băm từng câu rồi dò xem khóa nào có tiền. Máy tính làm việc đó hàng triệu lần mỗi giây.

A brain wallet takes a phrase you remember, hashes it with SHA-256 and uses the result as the private key. It is convenient because nothing needs to be written down. It is dangerous because a bad actor prepares a list of common phrases (song lines, proverbs, popular passwords), hashes each one and checks which key holds money. A computer does this millions of times a second.

```
import hashlib, secrets

def khoa_tu_cau(cau):
    return hashlib.sha256(cau.encode()).hexdigest()

tu_dien = ["matkhau123", "toiyeuvietnam", "hamy2005", "bitcoin",
           "123456789", "iloveyou", "quan1234", "caphe"]
khoa_nan_nhan = khoa_tu_cau("hamy2005")   # cau Ha My tu nghi ra
for lan, cau in enumerate(tu_dien, 1):
    if khoa_tu_cau(cau) == khoa_nan_nhan:
        print("Tim ra sau", lan, "lan thu, cau la:", cau)
        break

ngau_nhien = secrets.token_hex(32)
print("Khoa ngau nhien dai", len(ngau_nhien), "ky tu hex")
print("Hai lan sinh giong nhau:", ngau_nhien == secrets.token_hex(32))
```

Kết quả chạy / *Output*

```
Tim ra sau 3 lan thu, cau la: hamy2005
Khoa ngau nhien dai 64 ky tu hex
Hai lan sinh giong nhau: False
```

Kết quả: danh sách chỉ có 8 câu, kẻ xấu tìm ra cụm "hamy2005" sau 3 lần thử. Khóa sinh ngẫu nhiên bằng thư viện secrets (lấy ngẫu nhiên từ hệ điều hành) thì dài 64 ký tự hex và hai lần sinh không bao giờ trùng nhau. Hãy so thang đo. Dù kẻ xấu có một nghìn triệu triệu (10^{15}) phép thử mỗi giây, thử hết 2^{256} khả năng cũng cần khoảng $3{,}67 * 10^{54}$ năm.

Result: the list has only 8 phrases, and the bad actor finds "hamy2005" on the third try. A key made at random with the secrets library (which draws randomness from the operating system) is 64 hex characters long and two draws never match. Now the scale. Even if the bad actor made a thousand million million (10^{15}) tries a second, going through all 2^{256} possibilities would take about $3.67 * 10^{54}$ years.

Quy tắc cho người dùng: để ví tự sinh khóa, không bao giờ tự nghĩ câu để làm khóa. Với lập trình viên: dùng nguồn ngẫu nhiên của hệ điều hành (như secrets), không dùng hàm random thông thường, vì hàm đó đoán trước được nếu biết hạt giống.

Rule for users: let the wallet generate the key, and never invent a phrase to serve as a key. For programmers: use the operating system's randomness (such as secrets), not the ordinary random function, because that one is predictable if its seed is known.

> **LỖI HAY GẶP / COMMON MISTAKE –** Nghĩ rằng một câu dài và có số, ký hiệu là đủ làm khóa bí mật. Độ dài của câu không bằng độ ngẫu nhiên. Câu do người nghĩ ra vẫn nằm trong tập các câu người khác dò được.
> *Believing a long phrase with digits and symbols is enough to serve as a private key. The length of a phrase is not its randomness. A phrase a person invents still lies in the set others can search.*

2.10. Khóa công khai làm danh tính, bút danh, máy tính lượng tử và pháp luật Việt Nam – *2.10. Public keys as identities, pseudonyms, quantum computers and Vietnamese law*

Trong mạng tiền số không có tổ chức nào cấp chứng minh thư. Danh tính của bạn chính là khóa công khai (hoặc địa chỉ suy ra từ nó). Ai ký được bằng khóa bí mật khớp là "chủ"