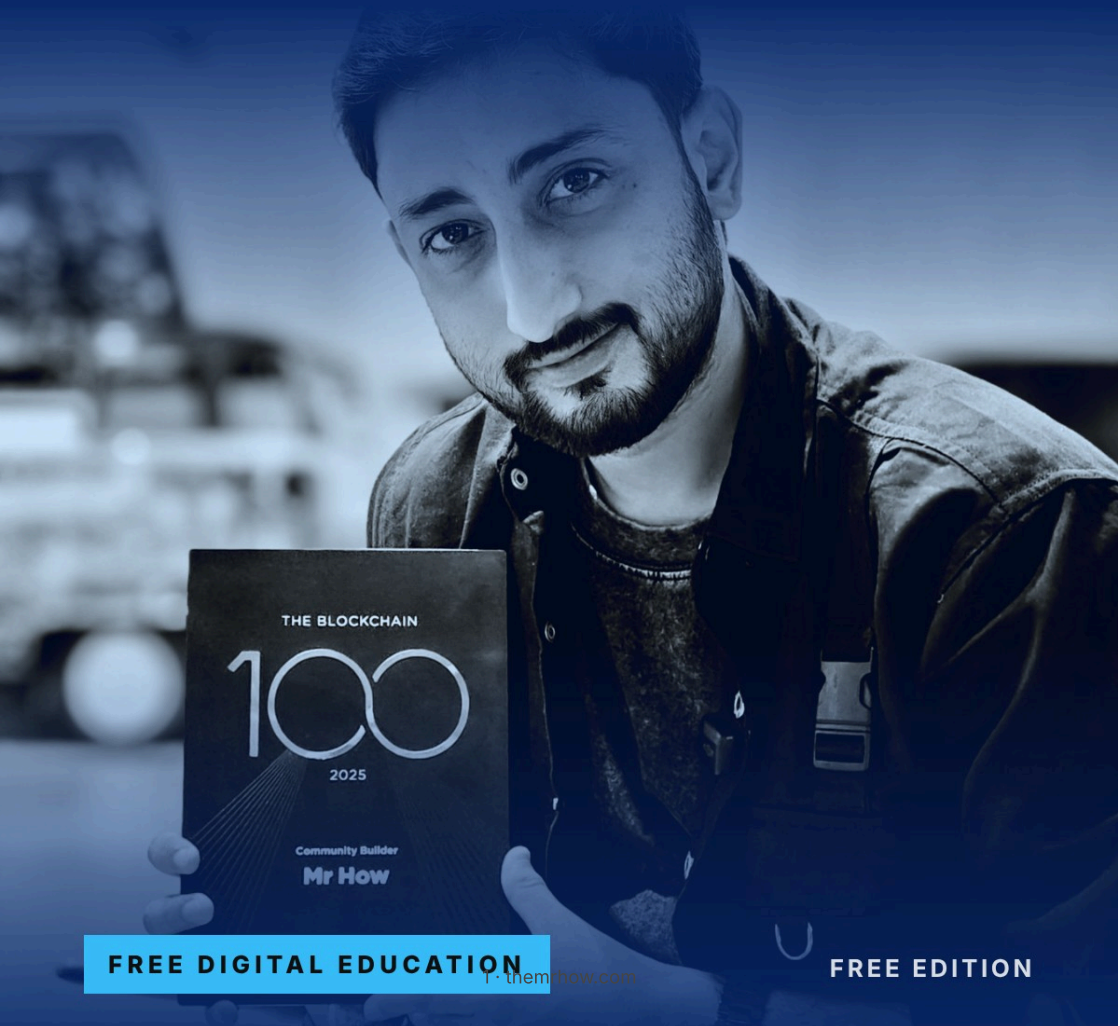
Road to Blockchain

From zero to Web3, one block at a time



FREE DIGITAL EDUCATION

↑ · themrhow.com

FREE EDITION

Road to Blockchain

From zero to Web3, one block at a time

By Mr How

Contents

Who this book is for

Chapter 1. The problem blockchain solves

Chapter 2. Hashes and digital signatures

Chapter 3. Blocks, chains and the ledger

Chapter 4. How everyone agrees: consensus

Chapter 5. Bitcoin: the first blockchain

Chapter 6. Ethereum and smart contracts

Chapter 7. Coins, tokens and stablecoins

Chapter 8. Wallets and keys

Chapter 9. Networks, fees and scaling

Chapter 10. What people build: DeFi, NFTs and beyond

Chapter 11. Blockchain in Pakistan

Chapter 12. Careers on the road to blockchain

Chapter 13. A short history of blockchain, 2008 to 2026

Chapter 14. Hands-on: your first testnet transaction

Chapter 15. Common myths, answered

Glossary

A message from Mr How

Who this book is for

You have heard words like blockchain, Bitcoin, Ethereum, Web3, wallets, gas and stablecoins. Maybe you have used a crypto app. Maybe you have only seen the hype on TikTok. Either way, you want to understand what is actually happening underneath, not just the price charts.

This book starts from zero and builds your understanding the way a blockchain is built: one block at a time, each resting on the one before it. By the end, you will understand how hashes and digital signatures work, why blocks are chained, how thousands of strangers agree on one history, what smart contracts are, how wallets really hold value, and where Pakistan stands. You will also see the careers this technology is creating.

I have been a blockchain educator for six years, and I was named in the Global Blockchain 100 in 2025, one of only 100 people in the whole world honoured for leading the way in blockchain education, research and the wider blockchain

space. This book is the foundation I wish every student had before they ever opened a trading app.

This book is educational. Nothing in it is financial advice. Crypto assets are volatile and can lose most or all of their value.

Chapter 1. The problem blockchain solves

To understand any invention, start with the problem it solves. Blockchain solves a problem that sounds simple but puzzled computer scientists for decades: **how can strangers who do not trust each other agree on a shared record, without a central authority in charge?**

The village register

Imagine a village where everyone keeps their savings with one shopkeeper. He writes every deposit, loan and payment in his register. The system works, but it has weaknesses. He can make mistakes. He can change entries. He can refuse service to people he dislikes. If his shop burns down, the records are gone. Everyone must trust one person.

Now imagine a different village. Every family keeps an identical copy of the register. When someone makes a payment, they announce it to the whole village. Everyone checks that the payer actually has the money, and then every family writes the

same entry in their copy. If one family tries to secretly change an old entry, their copy no longer matches everyone else's, and the village ignores it.

That second village is the core idea of a blockchain: a **shared ledger**, copied across many computers, updated by agreed rules, and extremely hard to change once written.

The double-spending problem

Digital information is easy to copy. If I send you a photo, I still have the photo. That is wonderful for photos, but terrible for money. If digital money could be copied, I could pay you and also pay someone else with the same coin. This is called **double spending**.

Banks solve double spending with a central ledger: the bank checks its database and refuses the second payment. Before 2008, every digital money system needed a central party like this. The breakthrough of Bitcoin was to solve double spending without one, using a shared ledger plus a clever way for strangers to agree on the order of transactions.

Why removing the middleman matters

Central systems are not evil. They are efficient and often work well. But they create single points of failure and control. Blockchains offer a different set of trade-offs:

Central ledger	Blockchain ledger
One organisation controls the record	Many independent computers keep the record
Fast and cheap to update	Slower and costlier, because many must agree
Records can be changed by the operator	History is very hard to change
Access can be blocked by the operator	Anyone following the rules can participate
Mistakes can be reversed by support	Mistakes are usually permanent

Notice the last row. The same property that makes a blockchain resistant to tampering also makes it unforgiving. Send money to the wrong address, and there is no customer service to reverse it. Understanding this trade-off is the beginning of blockchain wisdom.

Chapter 2. Hashes and digital signatures

Two pieces of cryptography make blockchains possible: **hash functions** and **digital signatures**. You do not need advanced maths to understand what they do.

Hash functions: digital fingerprints

A hash function takes any input, a word, a book or a whole movie, and produces a fixed-length output called a **hash**. Bitcoin uses a function called SHA-256, which always produces 256 bits, usually written as 64 hexadecimal characters.

Good cryptographic hash functions have four key properties:

1. **Deterministic.** The same input always gives the same hash.
2. **Fast to compute.** Any computer can calculate a hash quickly.
3. **Avalanche effect.** Change one letter of the input and the hash changes completely and unpredictably. "Pakistan" and

"pakistan" produce totally unrelated hashes.

4. **One-way and collision-resistant.** You cannot work backwards from a hash to the input, and it is practically impossible to find two different inputs with the same hash.

Because of these properties, a hash works like a fingerprint for data. If someone gives you a file and its hash, you can hash the file yourself and compare. If the hashes match, the file has not been changed by even one character.

Public and private keys

Blockchains use **public-key cryptography**. You generate a pair of mathematically linked keys:

- A **private key**: a secret number that only you should ever know.
- A **public key**: derived from the private key, safe to share. Your blockchain **address** is usually derived from your public key.

The magic is that it is easy to calculate the public key from the private key, but practically impossible to go the other way. Your address can be public, while your private key stays secret.

Digital signatures

When you send a transaction, your wallet uses your private key to create a **digital signature** for that specific transaction.

Anyone can use your public key to check that the signature is valid, proving that the owner of the private key approved the transaction, without ever seeing the private key itself. Change even one detail of the transaction, such as the amount, and the signature no longer matches.

> **Why this matters for you**
>
> On a blockchain, whoever controls the private key controls the funds. There is no "forgot password" button. This is why Chapter 8 on wallets, and the three crypto commandments from Book 2, are so important.

Chapter 3. Blocks, chains and the ledger

Now we can build the chain itself.

Transactions

A transaction is a signed message that says, in effect, "move this value from my address to that address". Users broadcast transactions to the network, where they wait in a pool until they are included in a block.

Blocks

A block is a batch of transactions plus a **header**. In Bitcoin, the header includes:

- The hash of the **previous block's header**
- A **Merkle root**: a single hash that summarises all transactions in the block
- A **timestamp**
- A difficulty target and a **nonce**, used in mining (Chapter 4)

The chain

Because every block contains the hash of the block before it, the blocks form a chain stretching back to the very first block, called the **genesis block**. Now imagine someone tries to change a transaction in an old block. The block's contents change, so its hash changes. The next block contained the old hash, so the link breaks. To hide the change, the attacker would have to recalculate that block and every block after it, faster than the rest of the network keeps adding new ones. On a large network, that is practically impossible. This is what people mean when they say a blockchain is **immutable**.

Merkle trees, briefly

A Merkle tree hashes transactions in pairs, then hashes those hashes in pairs, and so on until one hash remains: the Merkle root. This lets a light wallet prove that a specific transaction is in a block by checking a small number of hashes, without downloading every transaction. It is one of the quiet engineering ideas that makes blockchains practical on phones.

Nodes

A **node** is a computer that runs the blockchain's software, keeps a copy of the ledger and checks every new transaction and block against the rules. Full nodes verify everything

independently. This is why the rules are hard to change secretly: thousands of nodes would reject invalid blocks.

Two ways to track balances

UTXO model (Bitcoin)	Account model (Ethereum)
Your "balance" is a set of unspent outputs from past transactions, like notes in a wallet	Each address has a balance, like a bank account
Spending consumes whole outputs and creates change	Spending subtracts from the balance
Simple and good for privacy patterns	Convenient for smart contracts

Chapter 4. How everyone agrees: consensus

Thousands of nodes, spread across the world, with no boss. Who decides which block comes next? The answer is a **consensus mechanism**: a set of rules that makes honest behaviour profitable and cheating expensive.

Proof of Work

Bitcoin uses Proof of Work. Miners collect transactions into a candidate block and repeatedly change the nonce, hashing the header each time, looking for a hash below a target number. Because hashes are unpredictable, the only way is trial and error, billions of attempts per second. The first miner to find a valid hash broadcasts the block; others verify it instantly (checking one hash is easy) and build on top of it. The winner receives the **block reward** plus transaction fees.

Bitcoin adjusts the difficulty roughly every two weeks so that blocks arrive about every ten minutes on average, no matter how much mining power joins or leaves.

Why does this stop cheating? Rewriting history would require redoing the work of the blocks being replaced and outpacing the honest network. An attacker would need more than half of the network's total mining power. This is called a **51% attack**, and on a large network the cost of the hardware and electricity is enormous, while success would destroy trust in the very coin the attacker is trying to steal.

Proof of Stake

Ethereum switched from Proof of Work to Proof of Stake in September 2022, in an upgrade called the Merge. In Proof of Stake, **validators** lock up (stake) coins as collateral. The protocol selects validators to propose and attest to blocks. Honest work earns rewards. Provably dishonest behaviour, such as signing two conflicting blocks, can be punished by **slashing**: destroying part of the validator's stake. Proof of Stake uses a tiny fraction of the energy of Proof of Work, because security comes from capital at risk rather than electricity burned.

Finality

In Proof of Work, a transaction becomes safer with every block added after it; many services wait for several confirmations. Many Proof of Stake systems add explicit **finality**, after which reversing a block would require destroying a large amount of staked value.

	Proof of Work	Proof of Stake
Security comes from	Computing power and energy	Staked coins at risk
Block producers	Miners	Validators
Punishment for cheating	Wasted energy and missed rewards	Slashing of stake
Energy use	Very high	Very low
Main example	Bitcoin	Ethereum

Chapter 5. Bitcoin: the first blockchain

In October 2008, during a global financial crisis, a person or group using the name **Satoshi Nakamoto** published a nine-page paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System". In January 2009, the Bitcoin network started with the genesis block. Satoshi's real identity is still unknown.

The monetary rules

- **Fixed supply:** there will never be more than 21 million bitcoin.
- **Halving:** the block reward started at 50 BTC and halves every 210,000 blocks, roughly every four years. After the April 2024 halving, it is 3.125 BTC per block.
- **Divisibility:** one bitcoin is divisible into 100 million units called satoshis, so you never need to buy a whole coin.

Why people value it

Supporters see Bitcoin as digital scarcity: a money that no government or company can print more of, that anyone can hold with just a private key, and that can move across borders. Critics point to its price volatility, energy use, use in some crimes, and the fact that it produces no income. Both views have serious arguments behind them. Your job as a learner is to understand both, not to pick a team because of a video.

What Bitcoin is not

Bitcoin is not anonymous. Its ledger is public, and every transaction can be seen forever. Addresses are pseudonymous, but analysis firms and authorities can often link them to real identities, especially through exchanges that verify customers. It is also not a guaranteed investment. Its price has fallen by more than 70% several times in its history.

Chapter 6. Ethereum and smart contracts

If Bitcoin is a shared ledger for one currency, Ethereum, launched in 2015, is a shared computer. Its key idea is the **smart contract**.

What a smart contract is

A smart contract is a program stored on the blockchain that runs exactly as written when someone sends it a transaction. Think of a vending machine: put in the right coins, press a button, and the machine gives you the item, with no shopkeeper needed. A smart contract can hold funds, follow rules and interact with other contracts, and everyone can see and verify its code.

The Ethereum Virtual Machine

Every Ethereum node runs the same computation, in an environment called the Ethereum Virtual Machine (EVM), and must arrive at the same result. Smart contracts are often written in a language called Solidity and compiled into

instructions the EVM understands. Many other blockchains are "EVM-compatible", which means the same contracts and tools work on them too.

Gas

Running code on thousands of computers is expensive, so every operation costs **gas**, paid in the network's native coin (ETH on Ethereum). Gas prevents infinite loops and spam, and rewards validators. When the network is busy, gas prices rise.

Token standards

- **ERC-20:** the standard for fungible tokens, where each unit is identical, like a currency. Most stablecoins on Ethereum are ERC-20 tokens.
- **ERC-721:** the standard for non-fungible tokens (NFTs), where each token is unique.

Code is law, and code has bugs

Because smart contracts run automatically and are hard to change, a bug can be catastrophic. Over the years, attackers have exploited contract bugs to steal very large sums. This is why smart contract **auditing** and security research are among the most important and best-paid skills in the industry.

Chapter 7. Coins, tokens and stablecoins

Coins and tokens

A **coin** is the native asset of a blockchain: BTC on Bitcoin, ETH on Ethereum. It pays fees and secures the network. A **token** is an asset created by a smart contract on an existing blockchain. Creating a token is easy, which is why there are hundreds of thousands of them, and why most have little or no real value.

Stablecoins

A **stablecoin** is a token designed to keep a stable value, usually one US dollar. They have become one of the most-used products in crypto, especially for cross-border payments and for people in countries with weak currencies.

Type	How it stays stable	Main risk
Fiat-backed (e.g. USDT, USDC)	Issuer holds cash and short-term government debt as reserves	Trust in the issuer, its reserves and regulators
Crypto-backed	Over-collateralised with other crypto in smart contracts	Sharp crashes in the collateral
Algorithmic	Code adjusts supply to hold the peg	Collapse if confidence breaks, as seen in past failures

A stablecoin can lose its peg, briefly or permanently. "Stable" describes the goal, not a guarantee.

Tokenisation

Tokenisation means representing a real-world asset, such as a government bond, a property share or a commodity, as a token on a blockchain. Banks and governments are experimenting with this because it can make settlement faster and ownership easier to track. Pakistan's new crypto law includes licence categories for issuing tokens tied to currencies and other assets.

CBDCs are different

A central bank digital currency (CBDC) is digital money issued by a central bank. It may use some ideas from blockchains, but it is centrally controlled, the opposite of Bitcoin's design. Many central banks, including the State Bank of Pakistan, have studied digital currency projects.

Chapter 8. Wallets and keys

This is the most practically important chapter in the book, because it is where most people lose money.

What a wallet really is

A crypto wallet does not store coins. Coins live on the blockchain. A wallet stores your **keys**, shows your balances by reading the blockchain, and signs transactions for you.

Custodial and self-custody

Custodial (exchange account)	Self-custody wallet
The company holds the keys	You hold the keys
Password recovery possible	Lose the seed phrase, lose the funds
Risk: exchange hack, freeze or collapse	Risk: your own mistakes, phishing, malware
Convenient for trading	Better for long-term ownership, if you are careful

The crypto saying "not your keys, not your coins" points to real history: several major exchanges have collapsed or frozen customer funds. But self-custody is not automatically safer for beginners, because many lose funds through their own mistakes. Learn both, and choose deliberately.

The seed phrase

Most self-custody wallets generate a **seed phrase** of 12 or 24 words from a standard word list. These words can regenerate all your private keys. Write them on paper (or engrave them on metal), store them somewhere safe and private, and never photograph them, type them into websites, or share them with anyone, including "support". If anyone else gets your seed phrase, they own everything in that wallet.

Hot and cold wallets

- **Hot wallets** are apps or browser extensions connected to the internet. Convenient, but exposed to malware and phishing.
- **Cold wallets**, often hardware devices, keep keys offline and sign transactions inside the device. Safer for larger amounts.

Approvals: the hidden risk

When you use a decentralised app, you may give a smart contract permission to spend your tokens. Unlimited approvals

to malicious or hacked contracts are a common way wallets get drained. Only connect to apps you trust, read what you sign, and periodically review and revoke old approvals using reputable tools.

Addresses and networks

The same token can exist on several blockchains. USDT, for example, exists on multiple networks. If you send a token on the wrong network, or to an address that does not support it, funds can be lost. Always check the network as well as the address, and send a small test amount first for large transfers.

Chapter 9. Networks, fees and scaling

Blockchains face a famous challenge: the **trilemma**. It is hard to be highly decentralised, highly secure and highly scalable all at once. Different projects choose different trade-offs.

Layer 1 and Layer 2

A **Layer 1** is a base blockchain such as Bitcoin, Ethereum or Solana. A **Layer 2** is a system built on top of a Layer 1 to process transactions more cheaply and quickly, while relying on the Layer 1 for security.

- **Rollups** bundle many transactions off-chain and post compressed data or proofs to Ethereum. Optimistic rollups assume transactions are valid unless challenged; zero-knowledge rollups post cryptographic proofs that the transactions are valid.
- **The Lightning Network** lets Bitcoin users open payment channels and send many small payments off-chain, settling to the main chain later.

Bridges

Bridges move assets between blockchains, usually by locking tokens on one chain and issuing a representation on another. Bridges hold large amounts of value and have been among the most frequently hacked parts of the ecosystem. Use them carefully, and prefer well-established ones.

Why fees differ

Fees depend on demand for block space, how much computation a transaction needs and the design of the network. A simple transfer on a busy Layer 1 can cost far more than the same transfer on a Layer 2 or a cheaper chain. For users in Pakistan, low-fee networks are a big reason stablecoins are popular for small transfers, but cheaper networks may come with different security trade-offs.

Chapter 10. What people build: DeFi, NFTs and beyond

Decentralised finance (DeFi)

DeFi rebuilds financial services with smart contracts instead of institutions:

- **Decentralised exchanges** let users swap tokens using liquidity pools. Automated market makers set prices using formulas based on the pool's balances.
- **Lending protocols** let users deposit assets to earn interest or borrow against collateral. If collateral value falls too far, positions are automatically liquidated.
- **Oracles** bring outside data, such as asset prices, onto the blockchain. If an oracle is manipulated, protocols that rely on it can be exploited.

DeFi is open and innovative, but risky: smart contract bugs, oracle attacks, sudden liquidations and confusing interfaces. High advertised yields usually mean high hidden risk.

NFTs

Non-fungible tokens represent unique items: digital art, collectibles, tickets, memberships or in-game items. The 2021 NFT boom was followed by a sharp crash, and many collections lost most of their value. The underlying idea, provable digital ownership, continues to find uses in ticketing, gaming and identity.

DAOs

A decentralised autonomous organisation is a group that coordinates using smart contracts and token-based voting. DAOs manage treasuries and protocol decisions, though in practice voting power is often concentrated among large holders.

Real-world uses beyond finance

Supply chain tracking, digital certificates and credentials, land and property records, and cross-border settlement are all areas where organisations experiment with blockchains. Not every problem needs a blockchain. A good engineer asks: do multiple parties who do not fully trust each other need to share a record without one controlling it? If not, an ordinary database is usually better.

Chapter 11. Blockchain in Pakistan

Pakistan is one of the world's most active countries in crypto adoption, driven by a large young population, remittances and freelancers paid in foreign currency. Regulation has moved quickly since 2025.

- **2018:** the State Bank of Pakistan told banks and payment companies not to deal in virtual currencies.
- **July 2025:** the Virtual Assets Ordinance created the Pakistan Virtual Assets Regulatory Authority (PVARA).
- **August 2025:** NCCIA declared 46 betting, forex and binary trading apps illegal.
- **December 2025:** PVARA granted No Objection Certificates to Binance and HTX, a first step towards licensing, not a licence to operate.
- **2026:** Parliament passed the Virtual Assets Act, 2026, making PVARA a permanent regulator. The State Bank allowed banks to serve PVARA-licensed firms. PVARA opened licensing with eleven categories, from exchanges and custody to token issuance and mining services.

As of November 2026, no crypto platform has been publicly announced as holding a full PVARA licence. For the latest status and a platform checker, see the Crypto Rules page on themrhow.com. Book 5, *Crypto for Beginners*, explains what these rules mean for ordinary users.

Opportunities for Pakistan

- Cheaper, faster remittances and freelancer payments
- Tokenisation of government securities and real assets, under regulation
- A large pool of young developers who can build for global Web3 companies
- Blockchain-based records for land, education credentials and supply chains

Chapter 12. Careers on the road to blockchain

The most reliable way to benefit from blockchain is not speculation. It is skills. The industry hires globally and remotely, and it values proof of work more than degrees.

Role	What they do	Skills to learn
Smart contract developer	Writes and tests on-chain programs	Solidity or Rust, testing frameworks, security basics
Security auditor	Finds vulnerabilities before attackers do	Deep Solidity, common attack patterns, audit contests
Front-end Web3 developer	Builds apps that connect to wallets and contracts	JavaScript, React, Web3 libraries
Researcher and analyst	Studies protocols, data and markets	On-chain data tools, writing, economics
Community and education	Builds and supports user communities	Communication, content, moderation, technical understanding
Compliance and risk	Helps firms meet regulations	AML/CFT, regulation, blockchain analytics

A learning path

1. Understand the fundamentals in this book thoroughly.
2. Use a test network (testnet) and a self-custody wallet with test coins, which have no real value, to practise sending transactions safely.
3. Learn one programming language well; JavaScript or Python are friendly starting points.

4. For development, learn Solidity using free official documentation and open-source tutorials, and build small contracts on a testnet.
5. Publish your work on GitHub, write about what you learn, and join hackathons and open-source projects.

> **Beware "blockchain jobs" that ask for money**
>
> Real Web3 companies do not ask candidates to deposit crypto, buy tokens or pay for "onboarding". If a job requires you to send funds, it is a scam.

Chapter 13. A short history of blockchain, 2008 to 2026

Understanding where the technology came from helps you judge where it is going, and spot the patterns of hype and crash that repeat every few years.

Year	Milestone
2008	Satoshi Nakamoto publishes the Bitcoin white paper during the global financial crisis.
2009	The Bitcoin network launches with the genesis block.
2010	An early user famously pays 10,000 BTC for two pizzas, one of the first real-world purchases.
2014	Mt. Gox, then the largest Bitcoin exchange, collapses after losing a huge amount of customer bitcoin, an early lesson in custodial risk.
2015	Ethereum launches, bringing smart contracts to a public blockchain.
2016	The DAO hack on Ethereum leads to a controversial network split into Ethereum and Ethereum Classic.
2017	The ICO boom: thousands of projects raise money by selling tokens; most later fail.
2020 to 2021	DeFi and NFTs explode in popularity; major companies and investors enter the market.
2022	A brutal year: the TerraUSD algorithmic stablecoin collapses, several lenders fail, and the FTX exchange collapses. Ethereum completes the Merge to Proof of Stake.
2024	The US approves spot Bitcoin exchange-traded funds; the fourth Bitcoin halving reduces the block reward to 3.125 BTC.

2025	Pakistan creates PVARA; NCCIA bans 46 betting and binary apps; the first PVARA NOCs are granted.
2026	Pakistan passes the Virtual Assets Act and opens licensing; tokenisation and stablecoin regulation advance in many countries.

The pattern

Look at the table again. Every few years, a wave of excitement brings in new users and money, often around a new idea: ICOs, DeFi, NFTs, memecoins. Then failures, frauds and price crashes follow. Each time, the technology itself keeps developing underneath, and some genuinely useful things survive. The lesson for you: excitement is not evidence. Ask what survives the crash.

Chapter 14. Hands-on: your first testnet transaction

Reading about blockchains is useful. Using one is unforgettable. A **testnet** is a copy of a blockchain used for testing, where coins have no real value. You can practise everything without risking a single rupee.

What you need

- A reputable self-custody wallet app or browser extension, downloaded from its official source
- Access to a testnet supported by that wallet, such as an Ethereum test network
- Test coins from an official "faucet", a website that gives out free test coins

Step by step

1. **Create a new wallet.** Write the seed phrase on paper. Even though this is a test wallet, practise the habit of protecting it properly.

2. **Switch to the testnet** in your wallet's network settings. Check that the network name clearly says test.
3. **Copy your address** and request test coins from the faucet. Wait for them to arrive.
4. **Create a second account** in the same wallet, and copy its address.
5. **Send a small amount** of test coins from the first account to the second. Notice the gas fee estimate before you confirm.
6. **Find your transaction** on the testnet's block explorer by pasting the transaction hash.

Reading a block explorer

A block explorer is a website that shows everything on a blockchain. For your transaction, you will see:

- **Transaction hash:** the unique ID of your transaction.
- **Status:** pending, successful or failed.
- **Block number:** which block included it.
- **From and To:** the sending and receiving addresses.
- **Value:** how much was sent.
- **Gas used and gas price:** what the transaction cost and why.

Click on the block number, and you will see every other transaction in the same block. Click on your address, and you will see its full history. This is the transparency of public

blockchains: anyone can audit anything. It is also why privacy on a blockchain is limited.

What you just learned

You generated keys, received funds, signed a transaction, paid gas, and verified the result independently. That is the full lifecycle of a blockchain transaction, the same process that moves billions of dollars every day.

Testnet safety

Never enter a real seed phrase into a site that asks you to "connect for test coins". Use a fresh wallet for experiments, and never mix it with real funds.

Chapter 15. Common myths, answered

"Blockchain is just Bitcoin." Bitcoin is the first and largest blockchain, but the underlying ideas, shared ledgers, cryptographic signatures and consensus, are used in many other systems.

"Crypto is completely anonymous." Most public blockchains are transparent. Addresses do not show names, but transactions are visible forever and can often be linked to real identities through exchanges and analysis.

"Blockchains cannot be hacked." Large, well-established blockchains have proven very resistant to attacks on their core rules. But exchanges, bridges, smart contracts, wallets and people are hacked regularly. Most losses happen at the edges, not in the chain itself.

"Everything should be on a blockchain." No. Blockchains are slower and more expensive than ordinary databases. They

make sense when many parties who do not fully trust each other need a shared record that no single party controls.

"Crypto is only for criminals." Some criminals use crypto, as they use cash and bank transfers. Most activity is ordinary trading, payments and experimentation, and public ledgers often help investigators trace funds.

"It's too late to learn." The technology, the laws and the industry in Pakistan are still being built. Understanding them now puts you early, not late.

Glossary

- **Address:** a public identifier where crypto can be sent.
- **Block:** a batch of transactions with a header linking it to the previous block.
- **Consensus:** the rules by which network participants agree on the ledger.
- **Gas:** the fee for computation on Ethereum and similar networks.
- **Hash:** a fixed-length fingerprint of data.
- **Layer 2:** a scaling system that relies on a base blockchain for security.
- **Node:** a computer that keeps and verifies a copy of the blockchain.
- **Private key:** the secret that controls funds at an address.
- **Seed phrase:** words that can regenerate a wallet's private keys.
- **Smart contract:** a program that runs on a blockchain.
- **Stablecoin:** a token designed to hold a steady value.

- **Validator:** a participant who stakes coins to help produce and verify blocks.

A message from Mr How

When I started teaching blockchain, most people in Pakistan only heard about it through scams and price hype. Today we have a regulator, a law and a generation of young people who can build for the whole world. That is a huge change, and it is only the beginning.

Do not let anyone reduce this technology to "which coin will pump". Learn how it works. Build with it. Protect yourself and your family. The road to blockchain is long, but every block you add to your knowledge makes the chain stronger.

See you on the chain. Mr How