Market Talks
EDUCATION CENTER

BLOCKCHAIN · BEGINNER · LESSON 13 OF 13

Myths and Realities

Six things people often get wrong about blockchains, in both directions, and what the evidence actually shows

5 min read 6 quiz questions with answer key

BLOCKCHAIN · BEGINNER · LESSON 13 OF 13

Myths and Realities

IN ONE SENTENCE

Blockchains are neither magic nor a scam. They are very good at a few specific things, such as settling value without a middleman and keeping a shared record that is hard to change, and weak at others. Knowing which is which protects you from both hype and dismissal.

Myth 1: "Bitcoin is anonymous"

Reality: it is pseudonymous, as Lesson 5 explained. Addresses carry no names, but every payment between them is public forever. Once one address is linked to a person, for example through an exchange that checked their identity, much of their history can be traced.

A clear case came in June 2021. After the Colonial Pipeline ransomware attack, which disrupted fuel supplies on the US East Coast, the US Justice Department followed the ransom on the blockchain and recovered 63.7 of the 75 bitcoins paid. A public ledger turned out to be a poor hiding place.



Figure 1. Blockchains are strong at a few specific jobs and weak at others. Most myths come from forgetting one side of the balance.

ANALOGY: A PEN NAME IN A GLASS HOUSE

Imagine writing every letter under a pen name, but all your letters are pinned to the wall of a glass building on a busy street. Nobody knows your real name at first. But the moment someone sees you post one letter, they can read every other letter signed with the same pen name.

Myth 2: "Crypto is mostly used for crime"

Reality: crime is real, but it is a small share of the activity. The analytics firm Chainalysis estimated that illicit addresses received at least $154 billion in 2025, a very large number, yet still less than 1% of all crypto transaction volume it tracked. Much of that total came from sanctions evasion and theft by state-backed groups.

Both halves matter. The share is small, but the amounts are large enough that regulators, exchanges and banks treat crypto crime seriously, which is why exchanges ask for identity checks.

Myth 3: "Blockchains can't be hacked"

Reality: the Bitcoin ledger itself has never been rewritten, but almost everything around it can be attacked. The biggest losses come from the edges: exchanges, wallets, smart contracts and **bridges**, which move tokens between chains. In March 2022, attackers took about $625 million from the Ronin bridge used by the game Axie Infinity after gaining control of most of the keys that approved its withdrawals. The US Treasury later linked the theft to the North Korean Lazarus Group.

Small chains are a second weak spot. If a network has little mining power or stake behind it, rewriting recent blocks can be affordable, a so-called 51% attack. Security depends on how much it would cost to cheat, and that cost is very different from one chain to another.

Myth 4: "If it's on a blockchain, it's true"

Reality: a blockchain proves that a record has not been changed since it was written. It does not prove the record was right in the first place. If a supplier types "organic" next to a box of ordinary vegetables, the chain will faithfully keep that false claim forever.

This is sometimes called the **oracle problem**: whenever real-world facts such as prices, deliveries or ownership enter a blockchain, someone has to report them, and that someone must be trusted. The chain is strongest when the asset lives entirely on it, like bitcoin itself.

Myths 5 and 6: "Bitcoin wastes energy" and "Blockchains are fast and free"

Reality on energy: Bitcoin mining does use a lot of electricity, about 138 terawatt-hours a year according to a 2025 Cambridge study, or roughly 0.5% of global electricity use. The same study found that 52.4% came from sustainable sources, mainly hydropower, wind and nuclear. Proof-of-stake networks like Ethereum use only a tiny fraction of that. Whether the energy is worth it remains a real debate.

Reality on speed: public blockchains are slow by design, because thousands of computers must agree. Bitcoin handles only a handful of transactions per second on its main chain, and fees rise

when demand spikes, as Lesson 11 showed. Faster systems are being built on top, but each makes trade-offs.

Where blockchains are strong	Where they are weak
Moving value without a middleman	Speed and cost at large scale
Records that are very hard to change	Checking that real-world data is true
Open to anyone, hard to censor	Mistakes and thefts cannot be undone
Everyone can verify the rules	Privacy, since everything is public

Why this matters for traders

- **Myths move prices.** On 12 May 2021, Tesla stopped accepting bitcoin for cars, citing the energy used by mining, and bitcoin fell about 12% that day. Stories about energy, crime and hacks come back again and again, and markets often react before the facts are checked.
- **Hacks hit tokens, not always the chain.** When a bridge or exchange is drained, the tokens involved can collapse while the underlying network carries on normally. Ask what exactly was attacked before deciding what it means for the coin you hold.
- **Hype cuts both ways.** "Blockchain will fix everything" and "blockchain is useless" are both easy headlines. The useful question is always narrower: does this project need an open, shared record, and does it actually use one?

Key terms

Pseudonymous	Using addresses instead of names. Activity is public, and identity stays hidden only until an address is linked to a person.
Bridge	A service that moves tokens between two blockchains, often holding large amounts in one place, which makes it a frequent target.
51% attack	An attack where someone controls most of a chain's mining power or stake and uses it to rewrite recent blocks.
Oracle problem	The difficulty of getting real-world information onto a blockchain without having to trust whoever reports it.

Illicit volume	The value of crypto received by addresses linked to crime, such as scams, theft, ransomware and sanctions evasion.
Proof of stake	A way of securing a blockchain by locking up coins instead of using mining, which needs far less electricity.

Key takeaways

1. Bitcoin is pseudonymous, not anonymous, and payments can be traced, as the Colonial Pipeline recovery showed.
2. Illicit activity is large in dollars but has stayed under 1% of tracked crypto volume.
3. The Bitcoin ledger has never been rewritten, but exchanges, bridges, smart contracts and small chains are attacked regularly.
4. A blockchain keeps records unchanged, but it cannot check whether real-world data was true when it was entered.
5. Bitcoin uses a lot of energy and public chains are slow by design. Knowing the real strengths and limits protects you from hype in both directions.

Test yourself

Circle one answer for each question. The answer key with explanations is on the next page. You can also take this quiz online at markettalks.info and see your score instantly.

1. Why is Bitcoin described as pseudonymous rather than anonymous?

- A Transactions are hidden from everyone except miners
- B Addresses have no names, but every transaction is public and can be traced
- C Only exchanges can see the blockchain
- D Users must register their names on the blockchain

2. What did Chainalysis find about illicit crypto activity in 2025?

- A It made up most of all crypto volume
- B It was zero after new regulations
- C It was at least $154 billion but still under 1% of tracked volume
- D It was only found on Bitcoin

3. In the Ronin hack of March 2022, what was attacked?

A. The Bitcoin blockchain itself
B. A bridge, by taking control of most of the keys that approved withdrawals
C. Every Ethereum wallet at once
D. A miner's hardware

4. A supplier records false information on a blockchain. What does the blockchain guarantee?

A. The information will be corrected automatically
B. The information is true because it is on a blockchain
C. The record will not be changed later, even though it was false
D. Miners will reject the false data

5. According to the 2025 Cambridge study, roughly what share of global electricity does Bitcoin mining use?

A. About 0.5%
B. About 5%
C. About 25%
D. More than half

6. A bridge holding a popular token is hacked. What is the most sensible first question for a trader?

A. Has the whole blockchain stopped working?
B. Should I sell every coin I own immediately?
C. Is it true that all blockchains are now unsafe?
D. What exactly was attacked, and which tokens does it affect?

Answer key

1 B

Addresses have no names, but every transaction is public and can be traced

The ledger is fully public. Once an address is tied to a person, their past payments can be followed, as investigators did with the Colonial Pipeline ransom.

2 C

It was at least $154 billion but still under 1% of tracked volume

The dollar amount was large, but compared with all tracked activity the share stayed below 1%.

3 B

A bridge, by taking control of most of the keys that approved withdrawals

The attackers took over the keys that approved bridge withdrawals. The underlying blockchains kept working normally.

4 C

The record will not be changed later, even though it was false

A blockchain protects records from later changes. It cannot know whether a real-world claim was true when it was entered. This is the oracle problem.

5 A

About 0.5%

The study estimated about 138 terawatt-hours a year, roughly 0.5% of global electricity use, with just over half from sustainable sources.

6 D

What exactly was attacked, and which tokens does it affect?

Most hacks hit services built around a chain, not the chain itself. Knowing what was attacked tells you which assets are really at risk.

SOURCES

- NPR, US recovers millions in ransom paid to Colonial Pipeline hackers (June 2021): https://www.kunc.org/npr-news/2021-06-07/u-s-has-recovered-some-of-the-millions-paid-in-ransom-to-colonial-pipeline-hackers
- The Block, crypto crime topped $150 billion in 2025 (Chainalysis): https://www.theblock.co/post/384753/crypto-crime-150-billion-usd-2025-state-actors-scale-onchain-chainalysis
- TechCrunch, US officials link North Korean Lazarus hackers to $625M Ronin theft: https://techcrunch.com/2022/04/15/us-officials-link-north-korean-lazarus-hackers-to-625m-axie-infinity-crypto-theft
- Cambridge Judge Business School, sustainable energy rising in bitcoin mining (April 2025): https://jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/
- SiliconANGLE, Bitcoin price plunges after Tesla drops bitcoin payments (May 2021): https://siliconangle.com/2021/05/12/bitcoin-price-plunges-elon-musk-pulls-support-citing-environmental-concerns/

Market Talks

CONTINUE LEARNING

This lesson is part of the free Blockchain track at the MARKET TALKS Education Center: Beginner, Intermediate and Advanced lessons, each with a quiz and a downloadable PDF.

Education Center
Lessons from first principles to advanced topics

Markets Analysis
Technical and fundamental analysis on major markets

Reports
Bitcoin, Gold, Silver, SPX and more

markettalks.info

Telegram @MARKET_TALKS

For education only. Nothing in this document is financial advice. © 2026 MARKET TALKS. You are welcome to share this PDF unchanged.