NOTES FOR TEACHERS

Keys and Wallets

Students learn what a bitcoin wallet really holds: not coins, but a secret private key. The coins stay on the shared record at an address anyone can see and pay into, only the private key can sign them away, and no one can reset a key that is lost or copied.

Grades 9–12 | **1:29 video** | **Managing Risk 12-11b** | **Free to use, no sign-up**

STEP 1

Before watching

> If someone asked where the money in a banking app actually is, what would you say? Is it inside the phone?

STEP 2

Watch the episode

Bitcoin Basics, 1:29: thesteadyblock.com/episodes/keys-and-wallets/ (also on YouTube, @TheSteadyBlock)

STEP 3

Discussion questions

1. The episode compares a bitcoin address to a mailbox that anyone can look into and drop payments in. What about an address is public, and what has to stay secret?
2. To spend, Max's wallet uses his key to sign the payment, and everyone can check the signature without ever seeing the key. Why does it matter that the key itself is never handed over? What could happen if it were?
3. Supporters say that when you hold your own key, the coins are yours alone, with no company in charge of them; critics point out that it also means no company can help if the key is lost or copied, and that many people find keys hard to manage. Would you rather be the only one responsible for a key, or have someone who could help? What would you give up either way?

STEP 4

Exit quiz

1. What does a bitcoin wallet actually hold?

A. The coins themselves, like cash in a purse
B. Keys that can sign the coins away
C. A list of everyone's passwords
D. A bank account number

2. In the episode, what is the mailbox with Max's address on it?

A. Max's wallet app
B. Max's private key
C. A box at a real post office
D. A spot on the shared record that anyone can see and pay into

3. How does Max spend from his address without giving away his key?

A. His wallet uses the key to sign the payment, and anyone can check the signature
B. He sends the key to the person he is paying
C. A bank approves the payment for him
D. He types the key into the receiver's app

4. Why is guessing someone's private key hopeless?

A. It changes every second
B. A bank guards it
C. It is a number picked at random, about 78 digits long
D. It is written in a secret language

5. What happens if you lose your private key and have no backup?

A. The wallet company sends you a new one
B. The coins are locked away for good
C. The coins go back to whoever sent them
D. You can reset it with your email address

Key terms

Private key	A secret number, picked at random, that signs payments; whoever holds it controls the coins.

Address	Where coins on the shared record are sent, like a mailbox number; anyone can see what it holds.
Signature	Proof made with a private key that the owner approved a payment; anyone can check it without seeing the key.
Wallet	An app or device that keeps your keys and does the signing; the coins themselves stay on the shared record.

National standard

MAIN STANDARD · MANAGING RISK 12-11B

Describe conditions under which individuals should and should not disclose their Social Security numbers, account numbers, or other sensitive information.

Part of standard Managing Risk 12-11: “Online transactions and failure to safeguard personal documents can make consumers vulnerable to privacy infringement, identity theft, and fraud.”

MANAGING RISK 8-7C

Describe steps people can take to safely manage their finances using mobile technology.

SAVING 12-3B

Compare and contrast the features of mobile payment accounts, cryptocurrency accounts, and checking/savings accounts.

A private key is the most sensitive information a bitcoin owner has: spending never requires sharing it, anyone who copies it can take the coins, and no one can reset it. That makes it a clear case for Managing Risk 12-11b (when never to disclose sensitive information) and for using a wallet app safely (8-7c).

From the National Standards for Personal Financial Education (Council for Economic Education and Jump$tart Coalition, 2021), Managing Risk grade 12, p. 40; Managing Risk grade 8, p. 38; Saving grade 12, p. 23.

Numbers in this episode

As of October 2026

- 78 digits: A private key is a number picked at random below about 1.16 × 10^77 (just under 2^256), so it can be about 78 digits long. Guessing one by chance is hopeless.
- 1 key: Spending a coin needs a signature that only its private key can make. Anyone can check the signature with the matching public key, and the private key is never revealed (Bitcoin whitepaper §2; BIP340).
- 0 coins: What a wallet holds: keys, not coins. The coins are entries on the shared record, and the wallet keeps the keys that can sign them away.

- No reset: There is no company or help desk that can recover a lost key. Wallets give you a backup (a list of 12 or 24 words), which is the next episode.

Where each number comes from is listed on the episode page.

Further reading

For students or teachers who want to go deeper.

FOR STUDENTS **Crypto Asset Custody Basics for Retail Investors – Investor Bulletin** (https://investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins/crypto-asset-custody-basics-retail-investors-investor-bulletin-0)

U.S. Securities and Exchange Commission, Office of Investor Education and Assistance (Investor.gov), December 2025

A plain-language government bulletin: wallets store private keys, not the assets; a lost private key means permanent loss; and how holding your own keys compares with letting a company hold them.

FOR TEACHERS **Public Key Encryption ("Kid Krypto")** (https://classic.csunplugged.org/activities/public-key-encryption/)

CS Unplugged, University of Canterbury

A free, no-computer class activity in which students try to intercept a message, showing how a public part everyone can use and a private part only one person holds work together. It uses encryption rather than signatures, but the idea is the same.

FOR TEACHERS **Bitcoin: A Peer-to-Peer Electronic Cash System** (https://nakamotoinstitute.org/library/bitcoin/)

Satoshi Nakamoto (2008), Satoshi Nakamoto Institute copy

Section 2 defines a coin as a chain of digital signatures: each owner signs it over to the next owner's public key, and anyone can check the chain.

Links checked October 2026.

Free to use in class. Educational content only, not financial or investment advice.
Episode narration uses a synthetic voice. Answer keys and teacher sheets: email hello@thesteadyblock.com.