A10: Blockchain Identity Lab

Put Your Name & Photo on the Blockchain

Prof. Joerg Osterrieder

Spring 2026

Key Terms Glossary

Cryptography & Keys

- **ECDSA** — Elliptic Curve Digital Signature Algorithm; creates key pairs and signs transactions
- **Keccak-256** — Ethereum's hash function (SHA-3 family); derives addresses from public keys
- **Private Key** — 256-bit secret; proves ownership, signs transactions — never share!
- **Public Key** — Derived from private key via ECDSA; shared openly
- **Hex (0x)** — Base-16 encoding; all Ethereum data uses hex with 0x prefix

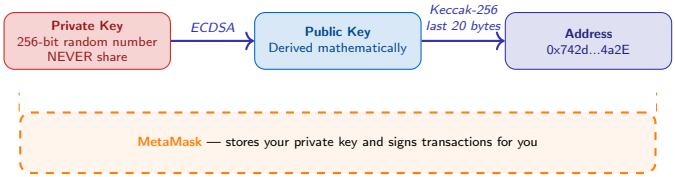
Blockchain Tools & Concepts

- **Gas** — Transaction fee paid to validators; measured in gwei (10^{-9} ETH)
- **IPFS** — InterPlanetary File System; decentralized storage using content hashes
- **CID** — Content Identifier; unique hash IPFS assigns to each file
- **MetaMask** — Browser wallet; stores your keys and signs transactions
- **Etherscan** — Block explorer; inspect transactions, addresses, and contracts on-chain
- **Sepolia** — Ethereum test network; free test ETH, no real monetary value

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

Concept 1: What is a Blockchain Wallet?



Key Points

- A wallet is a **key pair**, not an account at a bank
- The address is public (like an email address)
- The private key is secret (like a password — but **unrecoverable**)
- MetaMask is a browser extension that manages keys

Security Rule #1

Never share your private key or seed phrase with anyone — not MetaMask support, not your professor, not this lab.

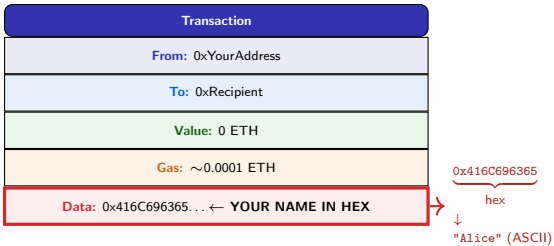
Why Ethereum Addresses?

- 20-byte hash of public key
- Starts with 0x
- 42 hex characters total
- Case-insensitive (EIP-55 adds checksum)

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

Concept 2: Anatomy of an Ethereum Transaction



Key Points

- Transactions carry **arbitrary data** in the "data" field
- We send 0 ETH to ourselves — the value is the **data**, not the transfer
- Anyone can read this data forever via a block explorer (Etherscan)
- Cost: only the gas fee (∼$0.01 on testnet)

Immutability Warning

Once confirmed, your name is on-chain **permanently**. There is no delete, no edit, no undo.

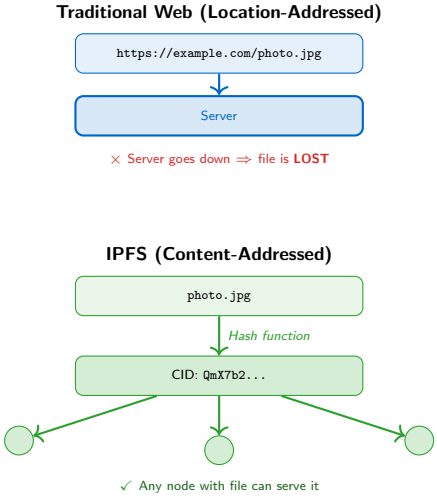
Hex Encoding

- `A` = 41, `l` = 6C, `i` = 69, ...
- Prepend `0x` to signal hexadecimal

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

Concept 3: IPFS — Content-Addressed Storage



Key Points

- IPFS identifies files by their **content hash** (CID), not by location
- Same file always produces the same CID (**deterministic**)
- Change one pixel ⇒ completely different CID
- We store the tiny CID on-chain, not the 5 MB image (cost!)

Cost Intuition

Storing 5 MB on Ethereum mainnet ≈ $10,000+ in gas.
Storing a 46-byte CID ≈ $0.01.

CID Formats

- CIDv0: starts with `Qm...` (base58, 46 chars)
- CIDv1: starts with `bafy...` (base32)
- Both are hashes — both work with Pinata

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10-blockchain-identity/instructions.html

Lab Overview

Learning Objectives

- Store arbitrary data on a public blockchain
- Send transactions with custom data payloads (MetaMask)
- Experience content-addressed storage (IPFS)
- Verify on-chain data via block explorer (Etherscan)
- (Bonus) Mint an NFT as on-chain media reference

Lab Details

- Time: 90 minutes
- Individual work
- Sepolia testnet (no real money)
- Scoring: 85 core + 15 bonus = 100 max

Safety Note

This lab uses the Sepolia TESTNET. Testnet ETH has zero monetary value. All transactions are public and permanent.

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

Tools You Will Need

Wallet & Blockchain

- **MetaMask** — browser wallet
- Sepolia faucets:
  - Google Cloud (primary)
  - Chainlink
  - QuickNode
  - Alchemy
  - Chainstack
- **Etherscan Sepolia** — block explorer

Data & Storage

- **ASCII-to-Hex Converter** — text to hex
- **Pinata** — IPFS pinning (free tier)
- **thirdweb** — no-code NFT deploy
- **OpenSea Testnet** — view NFTs

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

Phase 1: Wallet Setup & Testnet ETH

15 min — 10 pts

Steps

1. Install MetaMask from metamask.io/download
2. Create wallet, **save recovery phrase**
3. Enable Sepolia: Settings > Advanced > "Show test networks" ON
4. Select **"Sepolia test network"**
5. Visit a faucet, paste your address, request ETH
6. Confirm balance appears in MetaMask (∼30–60 sec)

MetaMask v11+ Note

The hex data toggle may have moved in newer versions. If not under Settings > Advanced, look for a "Hex" tab in the Send screen. See MetaMask docs.

Deliverable

- Screenshot of MetaMask showing Sepolia ETH balance

Faucet Tip

If one faucet is down, try another. Google Cloud and Chainstack do not require mainnet ETH.

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

Phase 2: Your Name on the Blockchain

20 min — 25 pts

Steps

1. Go to rapidtables.com ASCII-to-Hex converter
2. Type your full name (e.g., `Alice Johnson - Cryptoeconomics 2026`)
3. Copy hex output, prepend `0x` (e.g., `0x416C696365...`)
4. In MetaMask: Send > Recipient = **your own address**
5. Amount: **0 ETH**, paste hex into "Hex Data" field
6. Confirm transaction (gas ~0.0001 ETH)
7. Click "View on block explorer" or search on sepolia.etherscan.io
8. Input Data > "View Input As" > UTF-8 — your name appears!

Discussion

"You just wrote data to a public, immutable ledger. Anyone with the tx hash can read your name — forever. How does this differ from posting on social media?"

Deliverable

- Etherscan link showing your name in transaction input data

Common Pitfall

Hex string must have no spaces and start with exactly `0x`

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

Phase 3a: Upload Photo to IPFS

30 min total — 40 pts

Steps

1. Go to app.pinata.cloud and create a free account
2. Click "Add Files" > "File", upload your photo (< 5 MB)
3. Copy the **CID** (Content Identifier) — looks like `QmX...` or `bafy...`
4. Go to "Gateways" in Pinata dashboard
5. Note your dedicated gateway: `your-gateway.mypinata.cloud`
6. Test: `https://your-gateway.mypinata.cloud/ipfs/YOUR_CID`

Pinata Gateway Warning

The old public gateway (`gateway.pinata.cloud`) no longer works. You **must** use your account-specific dedicated gateway URL.

Key Concepts

- **IPFS** = decentralized storage
- **CID** = cryptographic hash of file content
- Same file always produces same CID (deterministic)
- Image is on IPFS, **not yet on the blockchain**

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

Steps

1. Convert CID to hex (same rapidtables tool)
2. Optionally prepend label: `IPFS_CID:QmX...` before converting
3. Send **0 ETH** to yourself with hex CID in data field
4. Verify on Etherscan: Input Data > UTF-8 shows the CID
5. Take CID from Etherscan, open via your Pinata gateway
6. The chain now **proves** you uploaded this image at this time

Discussion

"Why store the CID on-chain instead of the image itself? A 5 MB image on Ethereum would cost thousands of dollars in gas. The CID is a tiny pointer to off-chain storage."

Deliverables

- Pinata screenshot with CID
- Etherscan link with CID in input data
- Working IPFS gateway link to your image

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

Phase 4 (Bonus): Mint Your Photo as an NFT

25 min — 15 pts

Steps

1. Go to thirdweb.com/dashboard, connect MetaMask (**Sepolia!**)
2. Deploy > browse > "NFT Collection" (ERC-721)
3. Name: `YourName Identity NFT`, Symbol: `IDNFT`, Network: Sepolia
4. Click "Deploy Now", confirm in MetaMask
5. Go to "NFTs" tab > "+ Mint"
6. Name: `My Blockchain Identity - YourName`
7. Description: `My photo permanently linked to the blockchain`
8. Upload your photo, click "Mint NFT", confirm
9. Copy contract address, search on testnets.opensea.io

What is an NFT, Really?

- An NFT is a smart contract that maps token IDs to metadata URIs
- The image is stored off-chain (IPFS); the token is on-chain
- "Owning" an NFT = the contract says your address owns token #N

Deliverables

- thirdweb screenshot of minted NFT
- OpenSea testnet link

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

Key Concepts

On-Chain vs Off-Chain

- On-chain: transaction data, smart contract state — immutable, expensive
- Off-chain: IPFS files, web content — mutable (can be unpinned), cheap
- Best practice: store **pointer** on-chain, **data** off-chain

Content Addressing (IPFS)

- Files identified by hash of content, not by location
- Change one pixel $\Rightarrow$ completely different CID
- Anyone with CID can retrieve the file (if pinned)
- If Pinata goes offline, other IPFS nodes with the file still serve it

Immutability

- Once confirmed, blockchain data cannot be edited or deleted
- Your name and CID are on Sepolia permanently
- Privacy implication: public blockchains are forever

NFTs as Metadata Pointers

- ERC-721 contract stores: owner address + token URI
- Token URI points to JSON metadata (often on IPFS)
- The "image" is a URL inside that metadata

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

Reflection Questions

10 pts

Discuss with Your Neighbor, Then Write Your Answers

1. Your name is now permanently on a public blockchain. What are the privacy implications? How does this differ from posting on social media?
2. Why did we store the image CID on-chain instead of the image itself? What would happen if we tried to store a 5 MB image directly on Ethereum?
3. The IPFS CID is a hash of your image. If you modified one pixel, would the CID change? Why?
4. How does this lab demonstrate the concept of "immutability" in blockchain?
5. (Bonus) If Pinata goes offline, can your image still be retrieved from IPFS? What about from the blockchain?

A10

Lab: digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

Get Started

Assignment Page

digital-ai-finance.github.io/crypto-economics/assignments/A10_blockchain_identity/instructions.html

All Assignments

digital-ai-finance.github.io/crypto-economics/assignments/index.html

Open your browser and get started!

All four phases can be completed in 90 minutes using only a web browser and MetaMask.