LM07 · INTRODUCTION TO DIGITAL ASSETS · LOS A, B

Digital Assets

CFA Level I · 2025 Curriculum

What Are Digital Assets?

Digital assets are **anything that can be created, stored, and transmitted electronically, with associated ownership or use rights**. They exist on distributed ledger technology (DLT) networks and use cryptography to establish authenticity.

Why they matter for CFA candidates: Expect questions on DLT mechanics, consensus protocols, digital asset types, investment vehicles, and risk/return characteristics.

Key Terminology — Build Your Vocabulary

TERM	DEFINITION
Digital Asset	Any asset existing electronically with ownership/use rights. Includes cryptocurrencies, tokens, NFTs, stablecoins, and CBDCs.
DLT (Distributed Ledger Technology)	A database shared across a network where updates require consensus. The underlying technology for blockchains.
Blockchain	A specific type of DLT where data is stored in blocks linked cryptographically in a sequential chain.
Cryptocurrency	A digital asset using cryptography, typically with its own blockchain, used for peer-to-peer value transfer.
Token	A digital asset built on top of an *existing* blockchain.
Consensus Mechanism	The algorithm the network uses to agree on transaction validity (e.g., Proof of Work, Proof of Stake).
Smart Contract	Self-executing code on a blockchain that enforces agreement terms automatically without intermediaries.
Wallet	Software or hardware that stores the private keys (passkeys) needed to control digital assets.

Hash	A fixed-length cryptographic "fingerprint" of data. Any change to input produces a completely different hash.
Node	A computer participating in the blockchain network, storing a copy of the ledger.

The Three Defining Features

DECENTRALIZATION

No Central Authority

No single entity controls the network. Validation happens through consensus among distributed nodes. Eliminates the need for trusted intermediaries.

CRYPTOGRAPHY

Mathematical Security

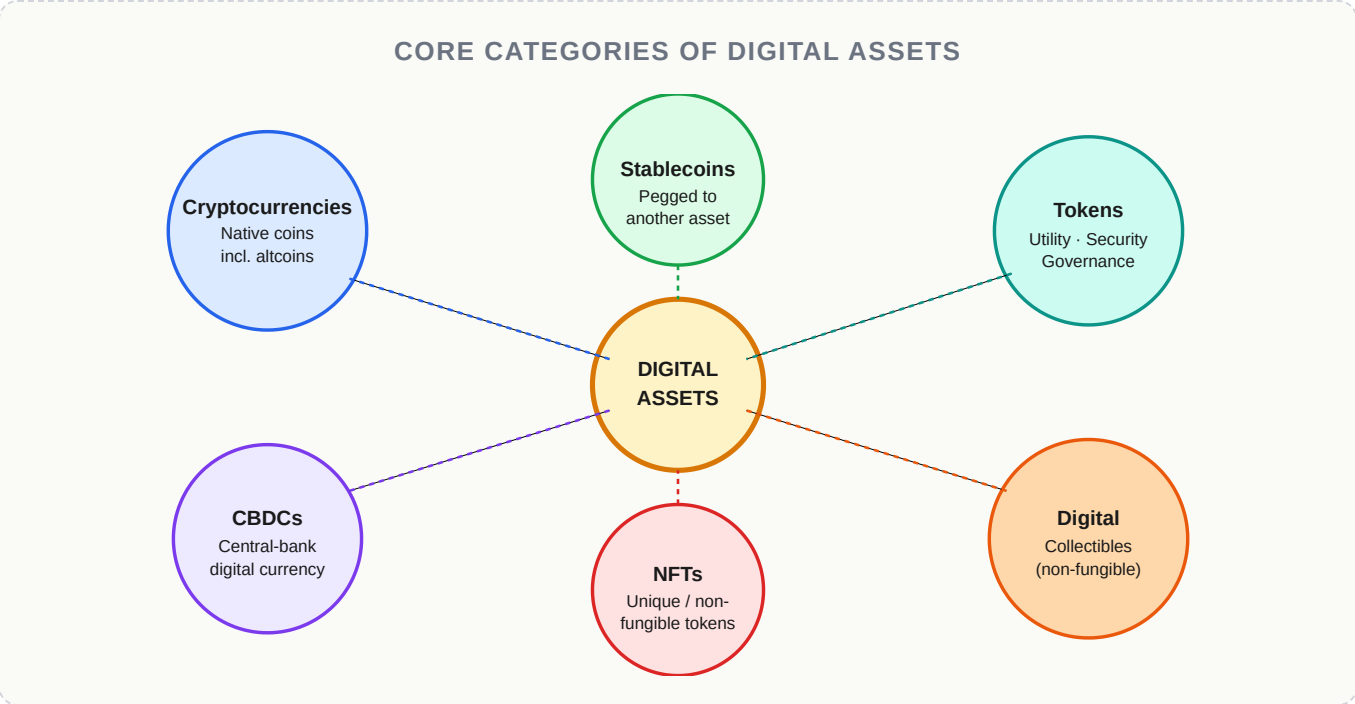
Public/private key pairs for ownership proof. Hash functions for tamper detection. Digital signatures for transaction authorization.

IMMUTABILITY

Tamper-Evident History

Once confirmed, transactions cannot be altered. Each block references the previous block's hash — changing any historical transaction would require rewriting the entire chain.

The Digital Asset Landscape



 Exam Tip: The CFA curriculum groups digital assets by **function**, not by underlying technology. Focus on the source taxonomy: cryptocurrencies (including altcoins and CBDCs), tokens (utility / security / governance / NFTs), stablecoins, and digital collectibles.

LOS A · DISTRIBUTED LEDGER TECHNOLOGY

Distributed Ledger Technology — The Foundation

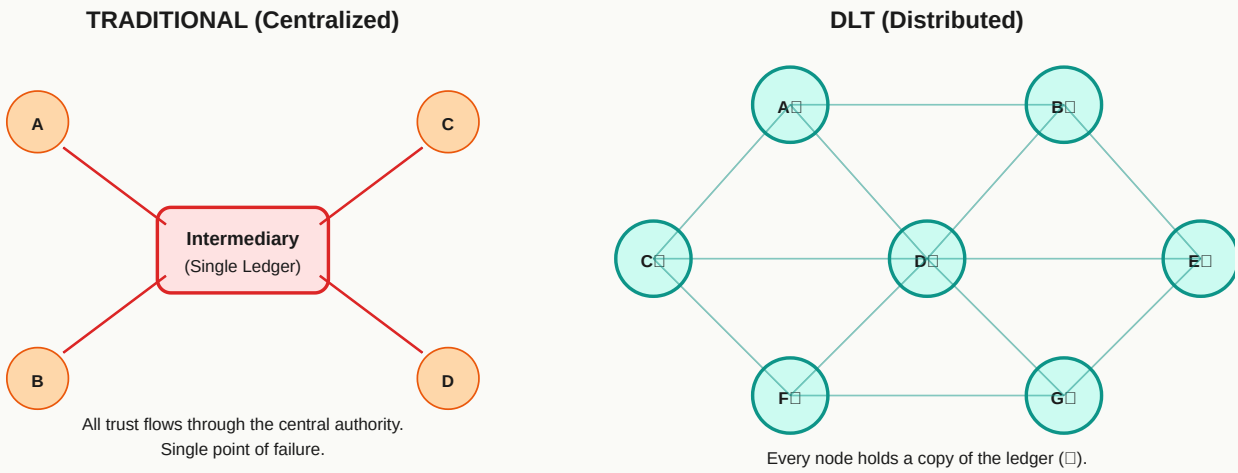
To understand any digital asset, you must first understand DLT. It is the underlying technology that makes digital assets possible — not just cryptocurrencies, but also tokenized securities, smart contracts, and decentralized finance.

Core Elements of DLT

- **Digital ledger** — a record of transactions shared across the network
- **Consensus mechanism** — the protocol by which participants agree on the ledger's state
- **Participant network** — the set of nodes maintaining and validating the ledger
- **Cryptography** — secures transactions, authenticates participants, and prevents tampering
- **Smart contracts** — self-executing programs that can automate contingent claims

Traditional Ledgers vs. Distributed Ledgers

THE KEY ARCHITECTURAL DIFFERENCE



How DLT Works — At a Glance

1. **Transaction initiated.** A user signs a transaction with their private key and broadcasts it to the network.
2. **Network receives the transaction.** Nodes across the network see the pending transaction.
3. **Consensus process.** Validators (miners under PoW, stakers under PoS) bundle pending transactions into a proposed block.
4. **Verification.** Other nodes independently verify signatures and balances.

5 **Block added.** Once consensus is reached, the block is appended and all nodes update their ledger copies.

DLT Benefits and Drawbacks

✓ Benefits

- **No intermediary** — eliminates banks, clearinghouses, registrars
- **Transparency** — transactions visible to participants (on public chains)
- **Immutable** — cannot be altered retroactively
- **Continuous availability** — no market hours
- **Programmability** — smart contracts enable contingent logic

✗ Drawbacks

- **Scalability** — throughput limitations relative to centralized systems
- **Energy consumption** — PoW chains consume significant electricity
- **Regulatory uncertainty** — unclear legal status in many jurisdictions
- **No recourse** — lost private keys = permanent loss of access
- **Complexity** — technical barriers for retail participants
- **Volatility** — most digital assets have large price swings

 Exam Tip: When the exam asks about DLT *advantages*, think: elimination of intermediaries, transparency, immutability. For *drawbacks*, think: scalability limits, energy use (PoW), regulatory ambiguity, and irreversibility of errors.

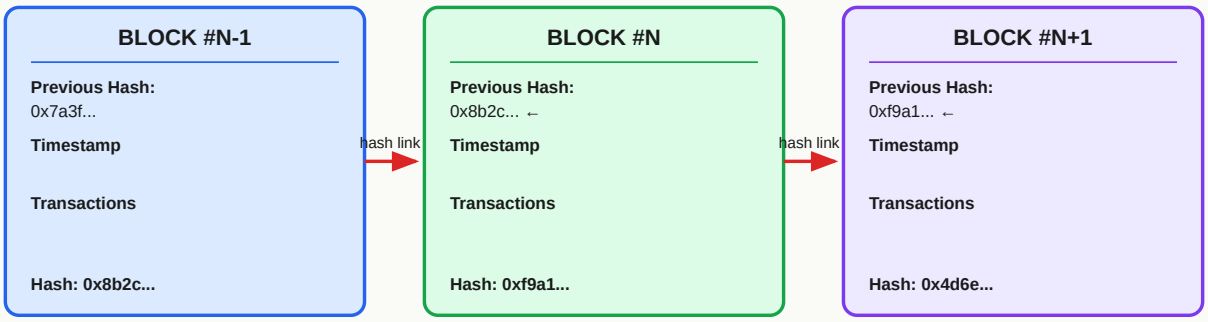
LOS A · BLOCKCHAIN STRUCTURE

Blockchain — How Blocks Are Linked

A **blockchain** is a specific type of DLT. The word is literal: data is stored in *blocks* that are cryptographically linked into a *chain*. Understanding this architecture explains why blockchains are tamper-evident.

Anatomy of a Block

THREE BLOCKS LINKED IN A CHAIN



Each block contains the previous block's hash — changing any historical block breaks the chain.

Why Immutability Works — The Domino Effect

Suppose an attacker wanted to change a transaction in **Block #N-1**. Here's what happens:

1. Changing the transaction changes the block's **data**
2. This changes Block #N-1's **hash**
3. Block #N's "Previous Hash" field no longer matches → invalidates Block #N
4. That changes Block #N's own hash
5. Block #N+1 is now invalid too... **and so on through the entire chain**
6. The attacker would need to outpace the rest of the network combined (the "51% attack")

For large permissionless chains, this is computationally and economically infeasible.

Common Blockchain Misconceptions

MISCONCEPTION	REALITY
"Blockchain and DLT are the same thing"	Blockchain is one specific *type* of DLT.
"Blockchain is anonymous"	It is **pseudonymous**. Wallets aren't directly tied to identity, but transactions are permanently public and can often be linked to real identities.

"Transactions are instant"	Block times and finality rules vary by chain. Confirmation is typically slower than centralized systems in some respects.
"Blockchain is free"	Every transaction pays a network fee to validators.
"It can never be hacked"	Protocols are highly secure, but *surrounding infrastructure* (exchanges, wallets, applications) has been exploited.

 Exam Tip: For the exam, key blockchain properties are: **sequential** (blocks in order), **immutable** (tamper-evident through hash linking), **distributed** (all nodes hold copies), and **consensus-validated** (not one central authority).

LOS A · CONSENSUS PROTOCOLS

Proof of Work vs. Proof of Stake

Without a central authority, how does a distributed network agree on which transactions are valid? The answer is a **consensus mechanism**. The CFA curriculum focuses on the two dominant approaches: Proof of Work (PoW) and Proof of Stake (PoS).

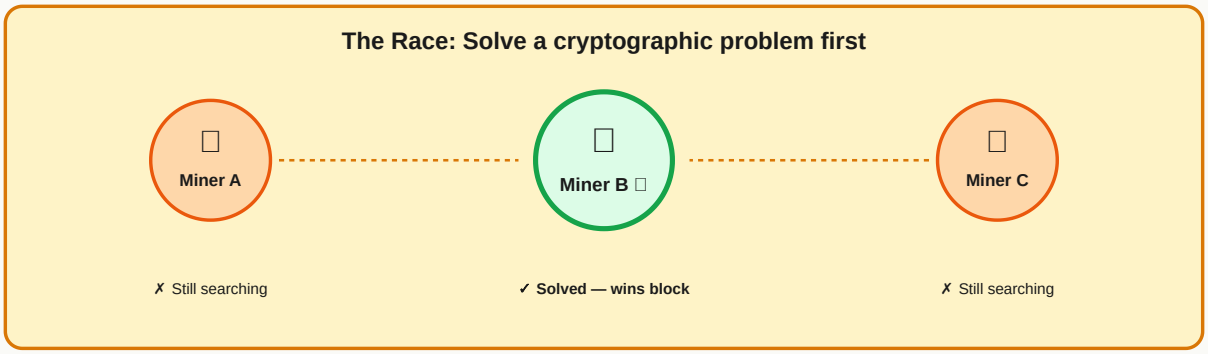
The Core Question: Who Writes the Next Block?

Every consensus mechanism answers this question differently. Two key dimensions to compare:

- **Security** — how hard is it to attack the network?
- **Resource used** — computation versus staked capital

Proof of Work (PoW) — How Bitcoin Works

PROOF OF WORK — THE MINER'S RACE

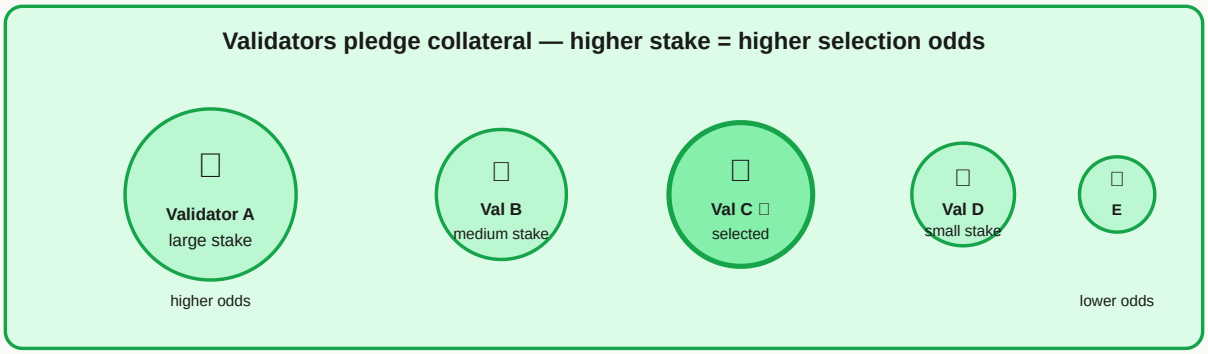


How PoW Works:

1. **Miners compete** to solve a cryptographic problem using computational power.
2. The first miner to find a valid solution broadcasts the new block to the network.
3. Other nodes **verify** the solution quickly (checking is fast even though solving is slow).
4. The winning miner receives a **block reward** plus transaction fees.

Proof of Stake (PoS) — Validator Selection by Stake

PROOF OF STAKE — VALIDATORS PLEDGE COLLATERAL



How PoS Works:

1. Validators **pledge collateral** (stake their tokens) to participate.
2. The protocol selects a validator, with selection weighted toward larger stakes, to propose the next block.
3. Other validators attest to the block's validity.
4. Honest validators earn rewards; a validator acting against protocol rules risks losing part of their pledged stake.

PoW vs. PoS — Side-by-Side

FEATURE	PROOF OF WORK (POW)	PROOF OF STAKE (POS)
Resource Required	Computational power	Pledged collateral (staked tokens)
Validator Selection	First to solve the cryptographic problem	Weighted by stake
Energy Consumption	High	Much lower
Security Model	Cost of computational power and energy	Economic cost of forfeited stake
Example	Bitcoin	Ethereum

The 51% Attack

In PoW, an attacker controlling more than half of the network's computational power could in principle rewrite recent blocks. For large, well-established chains this is considered infeasible because of the resource cost required.

 Exam Tip: Focus on: **PoW = miners solve a cryptographic problem using computational power. PoS = validators pledge collateral.** Bitcoin = PoW. Ethereum = PoS.

LOS A · NETWORK ACCESS CONTROL

Permissioned vs. Permissionless Networks

Beyond the consensus mechanism, blockchains differ in **who can participate**. This matters for use case, regulatory treatment, and investment relevance.

Side-by-Side Comparison

PERMISSIONLESS

Open to Anyone (Public)

- No central authority controls access
- Anyone can read, write, and validate
- Fully decentralized by design
- Transactions publicly visible
- Censorship-resistant
- **Example: Bitcoin**

Best for: open peer-to-peer networks and applications where anyone should be able to transact.

PERMISSIONED

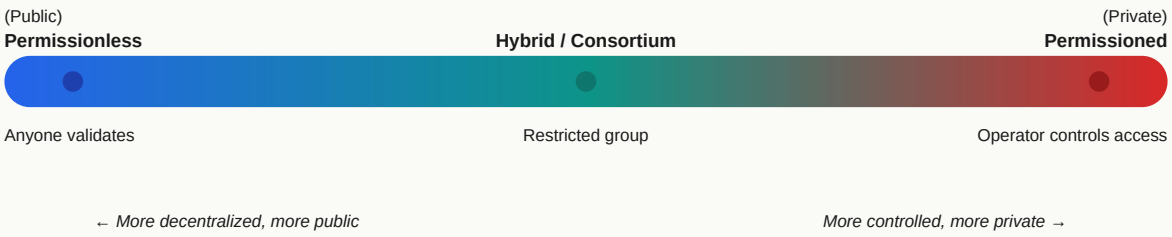
Access-Controlled (Private)

- An administrator controls who participates
- Often restricted to known entities
- More privacy controls
- Easier to fit existing regulatory frameworks
- **Used for enterprise / consortium applications**

Best for: settings where participants must be identified and vetted.

The Spectrum

FROM FULLY DECENTRALIZED TO FULLY CENTRALIZED



Exam Tip: On the exam, **"decentralization"** is associated with permissionless networks. **"Controlled access"** or **"enterprise use"** implies permissioned. Most investment-grade digital assets (like Bitcoin) live on permissionless blockchains.

QUIZ 1 · DLT FUNDAMENTALS

Test Your Understanding: DLT, Blockchain & Consensus

Q1. Which of the following is a *key advantage* of distributed ledger technology over traditional centralized databases?

Q2. In a Proof of Work consensus mechanism, validators (miners) are primarily selected based on:

Q3. A consortium of regulated institutions wants to use a blockchain for internal settlement among known counterparties. Which type of network is *most* appropriate?

Q4. A "51% attack" on a Proof of Stake network is economically discouraged because:

LOS B · DIGITAL ASSET TAXONOMY

Types of Digital Assets

The CFA curriculum divides digital assets into several categories: cryptocurrencies (including altcoins and central bank digital currencies), tokens (utility, security, governance, and NFTs), stablecoins, and digital collectibles.

① Cryptocurrencies — Native Coins

Cryptocurrencies have their **own dedicated blockchains**. They are typically used as a means of value transfer on their networks.

₿ Bitcoin (BTC)

Uses Proof of Work. **Supply capped at 21 million BTC**. Often framed as "digital gold" — a store-of-value narrative driven by scarcity.

Ξ Ether (ETH)

The native coin of the Ethereum smart-contract platform. Used to pay transaction fees on the network.

Altcoins are other cryptocurrencies built on or derived from Bitcoin-style technology.

② Tokens — Built on Existing Blockchains

Unlike cryptocurrencies, **tokens do not have their own blockchain**. They are built on top of an existing blockchain.

TOKEN TYPE	PURPOSE
Utility Tokens	Grant access to a specific service or product on a platform.
Security Tokens	Digital representation of traditional securities (equity or debt). Typically issued through initial coin offerings (ICOs) and subject to securities regulation.
Governance Tokens	Confer voting rights in decentralized protocols.
Non-Fungible Tokens (NFTs)	Unique, indivisible tokens representing ownership of a specific item; each is linked to a certificate of authenticity.

Asset-backed tokens represent fractional ownership of physical or financial assets and are classified as securities.

③ Stablecoins — Pegged-Value Digital Assets

A **stablecoin** is a digital asset whose value is pegged to another asset, most commonly a fiat currency such as the U.S. dollar. Stablecoins may be **collateralized by a basket of assets** (such as fiat currency reserves or other assets) or maintained by **smart-contract / algorithmic** mechanisms.

> **⚠ Algorithmic Stablecoin Risk**
> Algorithmic stablecoins rely on protocol rules rather than reserves to hold their peg. **TerraUSD** is the canonical example of an algorithmic stablecoin that collapsed when it lost its peg — illustrating the fragility of purely algorithmic designs.

④ Central Bank Digital Currencies (CBDCs)

A **CBDC is a digital version of a sovereign banknote** issued directly by a central bank. CBDCs differ from decentralized cryptocurrencies in that they are centralized, issued and controlled by the central bank, and function as a direct claim on the issuing authority — similar to physical cash.

⑤ Non-Fungible Tokens (NFTs)

NFTs represent unique, indivisible digital assets, each linked to a certificate of authenticity. Unlike fungible assets (where every unit is interchangeable), each NFT is distinct.

Fungible vs. Non-Fungible:

> **Fungible**
> Every unit is interchangeable — like 1 BTC being equivalent to any other BTC, or one dollar bill being equivalent to another.

> **Non-Fungible**
> Each token is unique. Two NFTs on the same contract are not interchangeable — like individual artworks or deeds.

 Exam Tip: Remember: **cryptocurrency** has its own chain; a **token** lives on another chain. **Fungible** = interchangeable; **non-fungible** = unique. A **stablecoin** is pegged to another asset. A **CBDC** is a central-bank-issued digital currency (centralized, not decentralized).

LOS C · DECENTRALIZED FINANCE

Smart Contracts & Decentralized Finance (DeFi)

Smart contracts let blockchains do more than transfer currency — they enable programmable financial infrastructure. The collection of financial applications built on smart contracts is called DeFi.

What Is a Smart Contract?

A **smart contract** is a self-executing program stored on a blockchain that runs automatically when predetermined conditions are met. One common use case is the **automatic execution of contingent claims** — payments that trigger when the specified conditions are satisfied.

Key properties:

- **Deterministic** — same inputs produce the same outputs
- **Automatic** — no human required to trigger execution
- **Transparent** — code is publicly visible on public chains
- **Permissionless** — anyone can interact with it on public chains

What Is DeFi?

Decentralized Finance (DeFi) refers to a **marketplace of decentralized applications (dApps)** that deliver financial services — such as lending, trading, and derivatives — using smart contracts on public blockchains, without traditional intermediaries.

DeFi applications disintermediate many of the functions that banks, brokerages, and exchanges traditionally provide, replacing them with smart-contract logic that anyone with a wallet can access.

How DeFi Lending Works

 WORKED EXAMPLE

Scenario: A user wants to borrow a stablecoin using a volatile cryptocurrency they hold as collateral — without selling it.

✓ SOLUTION

1. The user **deposits** the crypto collateral into a DeFi lending smart contract.
2. The contract allows the user to **borrow** a fraction of the collateral's value — the protocol requires **over-collateralization** (the collateral is worth more than the loan).
3. Borrowed tokens are sent to the user's wallet — no credit check or approval process.
4. If the collateral's value falls below a threshold, the smart contract **automatically liquidates** part of it to repay the loan.

Key differences from traditional lending:

- **No credit check** — over-collateralization replaces creditworthiness
- **Continuously available** — not limited to business hours
- **Automated liquidation** — no negotiation or delay

DeFi Risks — Major Categories

□ Smart Contract Risk

Code bugs or exploits can drain funds from a DeFi protocol.

□ Liquidity Risk

DeFi liquidity can evaporate quickly if collateral values crash or users withdraw en masse.

□ Custody Risk

Losing your private keys (passkeys) makes holdings inaccessible. No recovery mechanism exists.

⚖ Regulatory Risk

DeFi operates in a rapidly evolving and often unclear regulatory environment.

□ **Exam Tip:** On the exam, DeFi advantages: **disintermediation, continuous access, transparency**. Disadvantages: **smart-contract bugs, regulatory uncertainty, custody risk, and over-collateralization requirements**.

LOS B, C · COMPARATIVE ANALYSIS

Digital Assets vs. Traditional Financial Assets

A frequent exam question asks you to compare digital assets with traditional financial assets. The CFA curriculum emphasizes four specific dimensions.

The Four-Dimension Comparison

DIMENSION	DIGITAL ASSETS	TRADITIONAL FINANCIAL ASSETS
Inherent Value	Typically lack fundamental cash flows. Value derived from network effects, scarcity, and utility on the network.	Determined primarily by expected future cash flows (dividends, coupons, rents).
Transaction Validation	Decentralized ledger secured by cryptography and consensus.	Private ledgers maintained by central intermediaries.
Medium of Exchange	Limited direct use in commerce; typically converted to fiat for purchases.	Rarely used as a direct medium; convertible to fiat.
Legal / Regulatory Protection	Limited and still evolving; jurisdiction-specific.	Well-established, mature regulatory frameworks.

Valuation Challenge

Core valuation problem: Traditional assets have cash flows that can be discounted (DCF, DDM). Most cryptocurrencies do not generate cash flows, so their value has to be framed in terms of **scarcity, network adoption, and utility demand** rather than discounted cash flow. This is a fundamental difference from equities, bonds, and real estate — and a key reason valuations can be volatile.

Store of Value — Bitcoin vs. Gold

BITCOIN VS. GOLD — STORE-OF-VALUE PROPERTIES

GOLD

- ✓ Scarce (limited supply)
- ✓ Durable
- ✓ Divisible
- ✓ Fungible
- ✓ Long monetary history
- ✗ Costly to store and transport
- ✗ Purity must be verified
- ✗ Not programmable

BITCOIN

- ✓ Capped supply (21M)
- ✓ Digitally durable
- ✓ Highly divisible
- ✓ Fungible
- ✓ Globally portable
- ✓ Verifiable cryptographically
- ✗ Short monetary history
- ✗ High price volatility
- ✗ Requires technical literacy

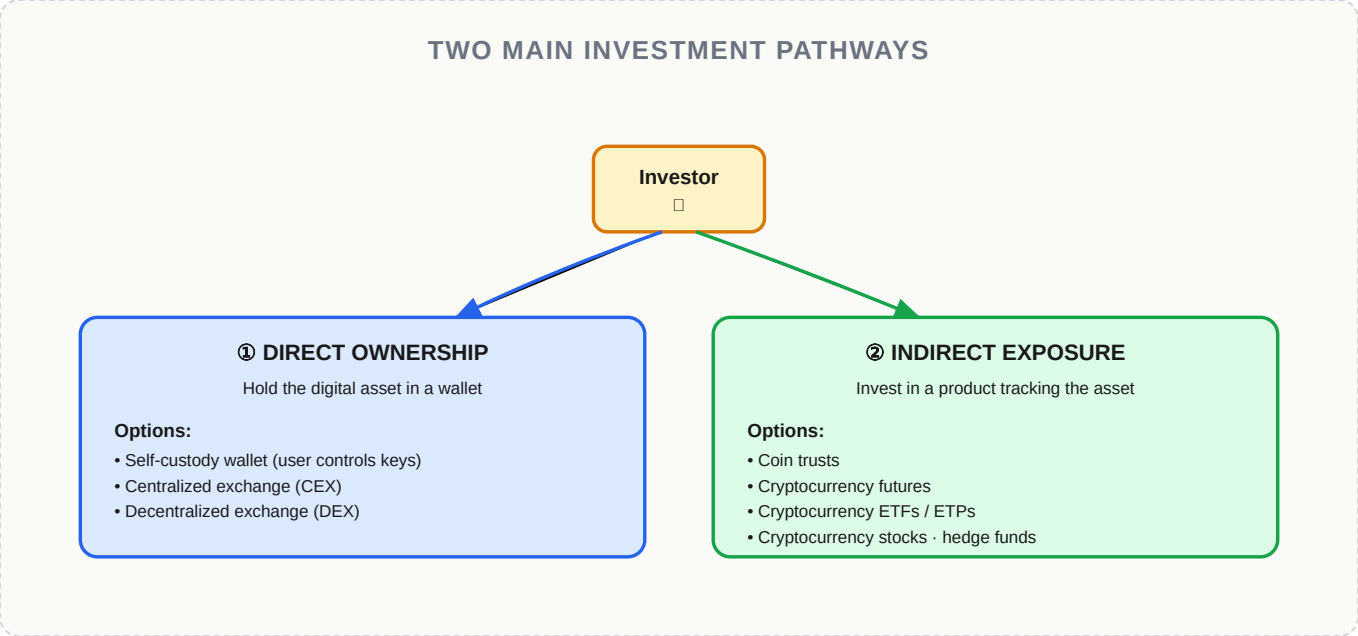
Exam Tip: The exam often tests whether you understand digital assets **lack cash-flow-based intrinsic value**. Their prices are driven by network effects, scarcity, and utility demand — not by DCF.

LOS C · INVESTMENT FORMS & VEHICLES

How Investors Access Digital Assets

Investors can hold digital assets **directly** through a wallet or **indirectly** through investment vehicles that track them.

Direct vs. Indirect Investment



Direct Ownership — Centralized vs. Decentralized Exchanges

CENTRALIZED EXCHANGES (CEX)

- Operated by a company; the exchange holds user assets in custody
- Easier onboarding and high liquidity
- Typically regulated in their jurisdictions
- **Risk: exchange hacks, insolvency, or account freezes**

DECENTRALIZED EXCHANGES (DEX)

- Peer-to-peer trading via smart contracts
- Users retain custody throughout the trade
- No central operator; no onboarding/KYC required
- **Risk: smart-contract bugs and price slippage**

Custody — Keys and Passkeys

Direct ownership means controlling the **private keys (passkeys)** that authorize transactions. If those keys are lost, the underlying cryptocurrency is effectively worthless to the holder — there is no central authority to recover them. An estimated **20% of Bitcoin** is believed to sit in lost or abandoned wallets.

Indirect Investment Vehicles

Indirect vehicles provide exposure to digital assets without holding them directly:

- **Coin trusts** — pooled vehicles that hold crypto on behalf of investors
- **Cryptocurrency futures** — regulated derivatives referencing a cryptocurrency's price
- **Cryptocurrency ETFs / exchange-traded products** — exchange-traded vehicles offering exposure to digital assets
- **Cryptocurrency stocks** — equities of publicly traded companies whose business is tied to crypto (exchanges, miners, etc.)
- **Cryptocurrency hedge funds** — actively managed private funds focused on digital assets

Asset-backed tokens, which represent fractional ownership of physical or financial assets, are classified as securities.

 Exam Tip: Direct investment = you hold the asset (and the keys). Indirect = you own a product that tracks the asset. Know the main indirect vehicles: **coin trusts, futures, ETFs/ETPs, cryptocurrency stocks, and hedge funds**.

LOS C · INVESTMENT CHARACTERISTICS

Digital Assets — Risk & Return Characteristics

Historically, Bitcoin — the most studied digital asset — has exhibited **high returns, high volatility, and low (but rising) correlations with traditional asset classes**. These properties drive both its appeal as a potential diversifier and its significant risk profile.

Qualitative Profile

DIMENSION	BITCOIN (ILLUSTRATIVE)	TRADITIONAL ASSET CLASSES
Return	High but highly variable across periods	Moderate; dependent on asset class
Volatility	Substantially higher than equities or bonds	Lower and more stable
Drawdowns	Very deep drawdowns (peak-to-trough)	Smaller on average
Correlation with equities	Historically low, but has risen in recent years	Generally interrelated (stock/bond dynamics)

Key Risk Characteristics

HIGH VOLATILITY

Large price swings

Bitcoin's volatility has been materially higher than that of traditional asset classes, with wide daily and weekly ranges.

DEEP DRAWDOWNS

Peak-to-trough losses

Bitcoin has experienced multiple severe drawdowns, with losses exceeding those of major equity indices in typical downturns.

NON-NORMAL RETURNS

Fat tails

Return distributions are skewed with frequent extreme observations — standard deviation understates tail risk.

CORRELATION INSTABILITY

Regime-dependent

Correlations with equities have been low historically but tend to *rise during periods of market stress*, reducing diversification benefit when it is most needed.

The Correlation Paradox

Because Bitcoin has historically shown low-to-moderate correlation with traditional asset classes, it can offer a **diversification benefit** within a diversified portfolio. However, correlations tend to **rise during market stress** — so the expected diversification benefit may attenuate precisely when it would be most valuable.

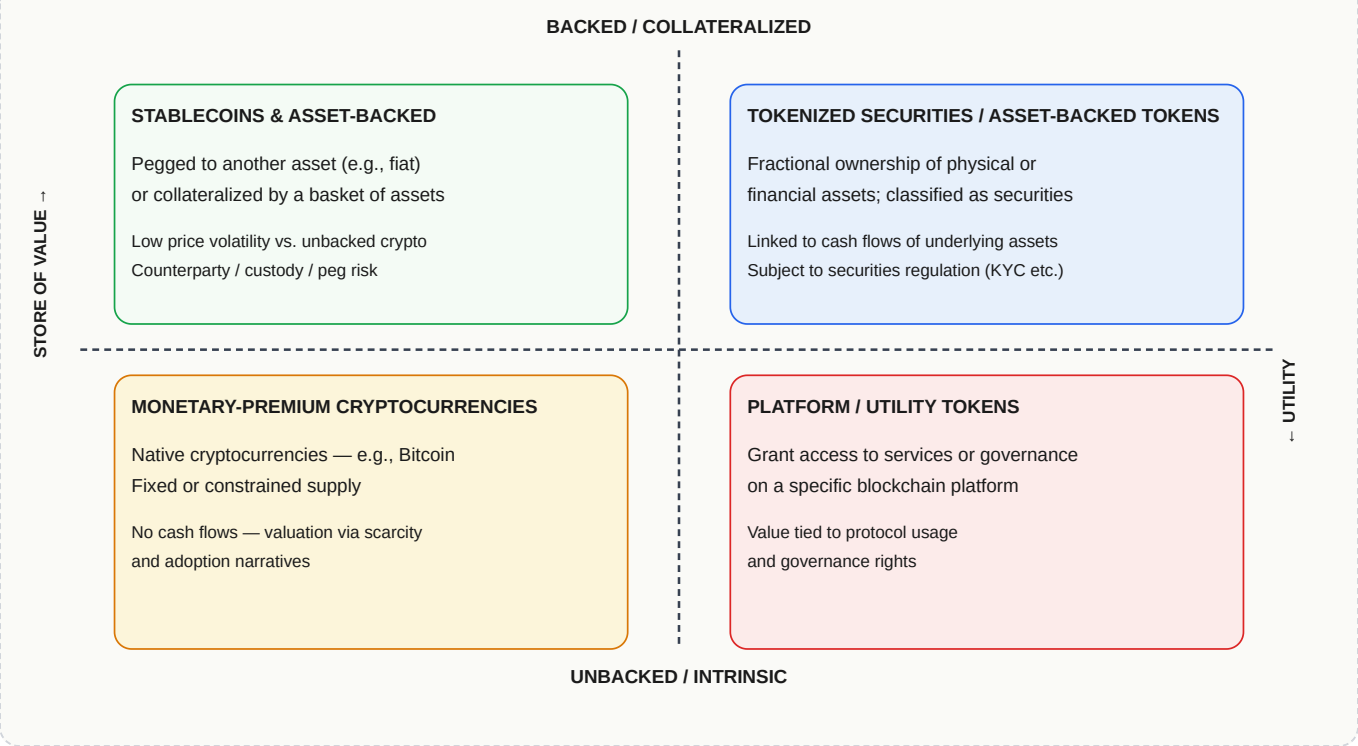
Sources of Risk Specific to Digital Assets

RISK SOURCE	DESCRIPTION
Scam ICOs and fraud	Fraudulent token offerings, including rug-pulls.
Market manipulation	Pump-and-dump schemes, and the influence of large holders (sometimes called "whales") on thinly traded tokens.
Theft / hacking	Exchange, wallet, and protocol exploits can result in irretrievable loss.
Lost credentials	Losing the private keys (passkeys) that control a wallet makes the holdings inaccessible.
Regulatory uncertainty	Rules vary by jurisdiction and continue to evolve.

 Exam Tip: Exam focus: digital assets can offer a **potential diversification benefit** due to low-but-rising correlations — balanced against **high volatility, deep drawdowns, and multiple tail risks** (fraud, theft, lost keys, and regulatory risk).

Digital Asset Taxonomy Map

MAPPING DIGITAL ASSETS BY BACKING AND USE CASE



QUIZ 2 · DIGITAL ASSETS & INVESTMENT

Test Your Understanding

Q5. Which of the following is a *fungible* digital asset?

Q6. Compared to traditional financial assets, digital assets are *most* distinctively characterized by:

Q7. A DeFi lending protocol *primarily* manages credit risk through:

Q8. An investor buys shares of a cryptocurrency ETF rather than holding the underlying cryptocurrency directly. Which statement *best* describes the trade-off?

INTERACTIVE TOOL

Digital Asset Portfolio Allocation Calculator

Experiment with how adding a Bitcoin allocation to a traditional stock/bond portfolio affects expected return, volatility, and Sharpe ratio. The inputs are user-defined assumptions — try a range of values to see how sensitive the result is.

Choose a Preset Scenario

ASSET ALLOCATION (MUST SUM TO 100%)

Stocks		59%
Bonds		40%
Bitcoin		1%

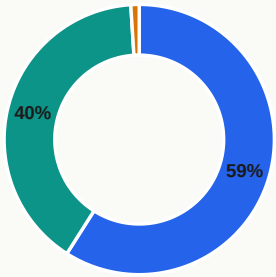
Total: 100% ✓

ASSET ASSUMPTIONS (EDITABLE)

BTC Expected Return		15%
BTC Volatility		70%
BTC-Stocks Correlation		0.30

EXPECTED RETURN	PORTFOLIO VOLATILITY	SHARPE RATIO
7.65%	10.06%	0.263
Annualized	Standard deviation	Assuming 5% risk-free

Portfolio Allocation — Live Visualization



Portfolio Allocation

- Stocks: 59%
- Bonds: 40%
- Bitcoin: 1%

vs. Stock/Bond Baseline

Your Portfolio:
Return: 7.65%
Vol: 10.06% | Sharpe: 0.263

Analysis vs. Stock/Bond Baseline

✓ **Marginal improvement.** Return +0.05pp, Vol +0.06pp, Sharpe +0.003.

 Exam Tip: Try a small BTC allocation first — when correlations stay moderate, a small allocation can modestly improve a portfolio's Sharpe ratio due to imperfect correlation. Large BTC weights generally raise volatility more than they raise expected return. The practical takeaway: diversification benefit depends critically on correlation — and correlations tend to rise in stress.

FINAL COMPREHENSIVE QUIZ

Final Assessment — Integrating Digital Asset Concepts

Q9. The main value proposition of using blockchain for cross-border payments is:

Q10. Which statement about stablecoins is *most accurate*?

Q11. An investor wants exposure to Bitcoin without managing a wallet or private keys. The *best* option is:

Q12. Which of the following is *least* likely to be a fundamental driver of cryptocurrency value?

MODULE COMPLETE

Your Scorecard

0 / 12

LM07 Key Takeaways — Exam-Ready Cheat Sheet

Foundation — DLT & Blockchain

1. **DLT** = Distributed Ledger Technology: a shared database updated via consensus. **Blockchain** = a specific type of DLT where data is stored in cryptographically linked blocks.
2. Three defining features: **Decentralization** · **Cryptography** · **Immutability**. Each block's hash references the previous — tampering requires rewriting the whole chain.

Consensus Mechanisms

3. **Proof of Work (PoW)**: used by Bitcoin. Miners solve a cryptographic problem using computational power. Energy-intensive.
4. **Proof of Stake (PoS)**: used by Ethereum. Validators pledge collateral and are selected to propose blocks in proportion to their stake.

Network Types

5. **Permissionless**: open to anyone (Bitcoin). **Permissioned**: access-controlled, used in enterprise / consortium settings.

Digital Asset Types

6. **Cryptocurrencies** have their own blockchain (Bitcoin, Ether). **Tokens** are built on top of an existing blockchain.

7. Token subtypes: **Utility** (service access), **Security** (regulated equity/debt-like), **Governance** (voting), and **NFTs** (unique, linked to a certificate of authenticity).
8. **Stablecoins** are pegged to another asset and may be collateralized by a basket of assets or maintained algorithmically. **CBDCs** are digital banknotes issued by central banks — centralized, not decentralized.

Smart Contracts & DeFi

9. **Smart contracts**: self-executing programs (e.g., automatic execution of contingent claims).
10. **DeFi**: a marketplace of decentralized applications (dApps) delivering financial services via smart contracts. Uses over-collateralization and automated liquidation instead of credit checks.

Digital vs. Traditional Assets

11. Key distinction: digital assets typically **lack cash-flow-based fundamental value**. Traditional assets are valued via DCF/DDM on cash flows.
12. Digital assets: decentralized validation, limited regulatory protection, and only limited direct use as a medium of exchange.

Investment Characteristics

13. **Direct** (wallet-based, via centralized or decentralized exchanges) vs. **Indirect** (coin trusts, futures, ETFs / ETPs, cryptocurrency stocks, hedge funds).
14. **Bitcoin risk profile**: high return, high volatility, low (but rising) correlation with traditional asset classes; diversification benefit attenuates in market stress.
15. Losing private keys (passkeys) renders a cryptocurrency holding inaccessible — an estimated **20% of Bitcoin** is in lost or abandoned wallets.

⚡ Exam-Trap Reminders

- **Blockchain ≠ DLT** — blockchain is one TYPE of DLT
- **Pseudonymous ≠ anonymous** — transactions are permanently public
- **PoW uses more energy than PoS**
- **Cryptocurrency (own chain) ≠ Token (on existing chain)**

- **CBDC = centralized** — not decentralized crypto
- **Cryptocurrencies typically lack cash flows** — can't be valued via DCF
- **DeFi uses over-collateralization**, not credit checks
- **Correlations rise in crises** — diversification benefit can be limited when most needed

⚡ Quick Recall

DLT = Distributed Ledger Technology

Bitcoin = PoW, capped at 21 million, framed as "digital gold"

Ethereum = PoS, smart-contract platform

DeFi = marketplace of decentralized applications providing financial services

Digital asset categories: cryptocurrencies (incl. altcoins and CBDCs), tokens (utility / security / governance / NFTs), stablecoins, and digital collectibles

Indirect vehicles: coin trusts, futures, ETFs / ETPs, cryptocurrency stocks, hedge funds

Step 1 of 15