CHARTA LEARNING · LESSON NOTES

Digital assets and distributed ledger technology

CFA Level I · Alternative Investments

You will learn: Tell the kinds of digital asset apart, explain why they are hard to value and risky, describe how a distributed ledger works and where finance uses it, and compare the vehicles for holding digital assets.

Running example: Examples follow the Meridian Foundation, a made-up $200m endowment considering a small slice of digital assets. All figures are round numbers made up for teaching.

1. Kinds of digital asset, and why they resist valuation

- A digital asset is a claim or unit of value recorded only in digital form, usually on a shared ledger. A cryptocurrency is meant to be a medium of exchange or store of value, and is a claim on no one.
- A token represents a claim or right on a project or service. A stablecoin is a token designed to hold a fixed value, usually by holding reserves.
- An ordinary share is valued by discounting its cash flows. A coin has none, so discounted cash flow valuation does not apply. Its price rests on adoption, scarcity (rules limiting supply) and sentiment.

Value of a level payer = D ÷ r

A SHARE AGAINST A COIN

Share pays D = $4; value at r = 8%	4 ÷ 0.08	**$50**
Value at r = 10%	4 ÷ 0.10	**$40 (−20%)**
A coin with no cash flows	0 ÷ r	**nothing to value**

Watch out: Trying to value a coin by discounting cash flows.

2. The risks: volatility, recovery, correlation, stablecoins

- Volatility is how widely returns swing around their average, measured by the standard deviation; multiply a monthly figure by √12 to annualise. Digital assets are far more volatile than a broad share index.
- A big fall needs a larger gain to recover, because the gain is measured on a smaller base. Early supporters argued coins would be unrelated to shares and cushion a sell-off, but in stress coins have tended to fall with shares, and the price history is short.
- A stablecoin is only as safe as its reserves. The peg can hold until the cash runs out and then break, and holders who wait lose most. Custody (who holds the key) and regulation, which differs by country and keeps changing, are extra risks that past data cannot price.

Gain to recover = fall ÷ (1 − fall)

MADE-UP FIGURES

Coin vs index monthly st. dev. (six months)	sample, n − 1	**21.2% vs 1.9%**
Annualised	monthly × √12	**73.3% vs 6.4%**
Falls of 20% / 50% / 75% need gains of	20 ÷ 80 / 50 ÷ 50 / 75 ÷ 25	**25% / 100% / 300%**
$190m in shares falls 30%; $10m coin falls 60%	(57 + 6) ÷ 200	**31.5% loss (28.5% if the coin stays flat)**
Stablecoin: reserves 90 cash + 10 paper sold at 70%	90 + 7; 7 ÷ 10	**late tokens get $0.70**

Watch out: Treating a stablecoin as risk free, or expecting a coin to diversify shares.

3. How a distributed ledger works

- A ledger is a record of who owns what. A distributed ledger is a shared record kept by many participants with no central authority; an entry counts only when most agree. The price is effort and speed: many people must do the same work.
- Entries are grouped in blocks. Each block carries a hash (a short digital fingerprint of data) of the block before it, forming a blockchain. Altering an old entry changes its fingerprint and breaks the link in every later block, so tampering is plain to see.
- Consensus is the rule that decides which version is authoritative. Proof of work: participants compete with computing power, so cheating costs real resources. Proof of stake: participants lock up coins and are chosen in proportion; cheaters can be slashed. Permissioned: known, accountable members validate.
- A permissionless ledger is open to anyone (most public cryptocurrencies). A permissioned ledger is limited to approved, known members (most financial institutions, who must know counterparties and meet anti money laundering duties).

COST OF CHEATING (MADE-UP NETWORKS)

Proof of work: redo blocks 2 to 5	4 blocks; 10 min ÷ 10% = 100 min each	**400 min**
Honest blocks added meanwhile	400 ÷ 10	**40**
Proof of stake: stake 1,000 of 100,000; 1,000 blocks; reward 0.5	1% × 1,000 = 10 blocks; × 0.5	**5 coins**
Slashed 10% of stake if caught	10% × 1,000	**100 coins**

Watch out: A ledger shows a record has not been altered, not that the entry was true when written.

4. Where finance uses the technology

- Settlement is the final swap of cash and asset after a trade. A shared ledger can record it almost at once instead of days later, cutting the cost of waiting and the counterparty exposure.
- Tokenisation turns ownership of an asset into digital tokens, giving divisible ownership and a transferable record. It does not guarantee a market: the asset is as risky as before and tokens may trade thinly.
- A smart contract is a program on the ledger that carries out an agreement automatically when set conditions are met. It guarantees the coded terms execute, not that they are the terms the parties meant, that the counterparty is solvent, or that a court will enforce it.

SETTLEMENT, TOKENISATION AND A SMART CONTRACT

$10m trade, 2 days at 4% a year	10m × 4% × 2/365	**$2,192**
Building $50m into 50,000 tokens	50m ÷ 50,000	**$1,000 a token**
Your 20 tokens	20 ÷ 50,000	**0.04% of the building**
Net rent $2.5m: rent per token	2.5m ÷ 50,000	**$50 (5%)**
$1,000 bond, coupon 4% coded as 40%	400 − 40	**$360 paid too much**

5. Vehicles for holding digital assets

- The private key proves ownership and the wallet holds it; whoever controls the key controls the asset. A lost key is a permanent loss. Each vehicle swaps one risk for another.
- Direct: your own wallet (you carry the custody burden) or leaving it on a centralised exchange (the exchange can fail, be hacked or misbehave: counterparty risk, separate from price volatility).
- Indirect: a futures based fund (roll costs, as futures expire), a trust or fund holding the asset (price can differ from net asset value, a premium or discount), or shares of a company such as a miner (business risk and amplified exposure).
- Moving from own wallet toward miner shares, you gain convenience and lose a clean link to the asset. Risks common to every vehicle are extreme volatility, uncertain regulation and no cash flows.

> **Premium or discount = market price ÷ NAV − 1**

VEHICLE RISKS

$100,000 on a failed exchange, 40 cents recovered	100,000 × 40%	**lose $60,000 (60%)**
Futures fund: spot flat, next month 102 vs 100	$100 \times (100 \div 102)^{12}$	**78.8 after 12 rolls (−21%)**
Trust: NAV 60, price 66; NAV 75, price at 10% discount	75 × 0.90 = 67.50; 67.50 ÷ 66 − 1	**return 2.27% vs asset +25%**
Miner: 3 coins a day at $50,000, costs $120,000	150,000 − 120,000	**profit $30,000 a day**
Coin falls 20%	120,000 − 120,000	**profit $0**

Watch out: Assuming a vehicle removes the underlying risks.

Key takeaways

- Digital assets come as cryptocurrencies, tokens and stablecoins; most have no cash flows, so discounted cash flow does not apply.
- Gain to recover = fall ÷ (1 − fall); a 40% fall needs about 66.7%.
- Correlation with shares rose in stress and the history is short; a stablecoin is only as safe as its reserves.
- A distributed ledger is a shared record linked by hashes and kept honest by consensus; institutions mostly use permissioned ledgers.
- Uses in finance: settlement, tokenisation and smart contracts, which execute as coded, not as meant.
- Every holding vehicle adds its own risk: custody, exchange failure, roll cost, premium or discount, or business risk.

Quick check

1. A coin falls 40%. What gain gets it back to the start?
   Answer: 40 ÷ 60 = 66.7%, not 40%.
2. Trust NAV $80, price $72. Premium or discount?
   Answer: 72 ÷ 80 − 1 = −10%, a 10% discount.
3. What does a smart contract guarantee?
   Answer: That the coded terms execute as written.