L01 — Introduction to Cryptoeconomics

Cheatsheet

What is Cryptoeconomics?

Core Definition

Cryptoeconomics = **Cryptography** + **Economics**.
Design of decentralised systems where *economic incentives* enforce desired behaviour, removing the need for a trusted central authority.

Key insight: participants are assumed rational and self-interested; the protocol must make honest behaviour the dominant strategy.

Not a sub-field of cryptography alone; equally draws on game theory, mechanism design, and network economics.

Core Concepts

Trustless — Parties need not trust each other or any intermediary; trust is placed in the *protocol* and *mathematics*.

Permissionless — Anyone can participate without prior approval. No gatekeepers.

Decentralised — Control is distributed across many nodes; no single point of failure or control.

Double-spending — The attempt to spend the same digital coin twice. Bitcoin's core innovation is preventing this *without* a bank.

Consensus — Agreement among distributed nodes on the canonical state of the ledger.

Immutability — Once confirmed and buried under subsequent blocks, a transaction is computationally infeasible to alter.

Bitcoin Timeline

Date	Event
1997	Adam Back proposes **Hashcash** (PoW for email)
1998	Wei Dai proposes **b-money**
Oct 2008	Satoshi Nakamoto publishes **Bitcoin whitepaper**
3 Jan 2009	**Genesis block** mined (Block 0); coinbase: "Chancellor on brink..."
12 Jan 2009	First Bitcoin transaction (Satoshi → Hal Finney)
22 May 2010	**Bitcoin Pizza Day** — 10,000 BTC for two pizzas
2010	Satoshi disappears from public forums
Feb 2011	Bitcoin reaches $1 USD parity
Nov 2012	**1st Halving**: reward 50 → 25 BTC
2013	Mt. Gox at peak; Bitcoin reaches $1,000
Jul 2016	**2nd Halving**: reward 25 → 12.5 BTC
Jul 2017	SegWit activated; BCH fork
Dec 2017	ATH ≈$20,000
Jul 2020	**3rd Halving**: reward 12.5 → 6.25 BTC
Nov 2021	New ATH ≈$69,000
Apr 2024	**4th Halving**: reward 6.25 → 3.125 BTC

Bitcoin Key Facts

Property	Value
Max supply	21,000,000 BTC (hard cap)
Block time	≈10 minutes
Halving interval	Every 210,000 blocks (≈4 years)
Genesis block	3 January 2009
Initial reward	50 BTC per block
Current reward	3.125 BTC (post-4th halving)
Last BTC mined	≈ year 2140
Consensus	Proof of Work (SHA-256)
Script	Bitcoin Script (not Turing-complete)

Blockchain Trilemma (Buterin)

Any blockchain can fully achieve **at most two** of the three:

Property	Meaning
Scalability	High throughput; many transactions per second
Decentralisation	Many independent validators; no single point of control
Security	Resistant to attack; costly to corrupt 51%+ of nodes

Examples:

- Bitcoin — Security + Decentralisation (sacrifices throughput)
- Visa — Scalability + Security (centralised)
- Early ETH 2.0 sharding — attempts all three with trade-offs

Byzantine Generals Problem

Setup: n generals must agree on a battle plan over unreliable messengers; up to f generals may be traitors sending conflicting messages.

Result (Lamport et al. 1982): Consensus is achievable if and only if $n \geq 3f + 1$ (i.e., honest nodes $> \frac{2}{3}$ of total).

Relevance: Bitcoin solves BGP in an open, permissionless setting using Proof of Work — economic cost replaces known-identity assumptions.

BFT (Byzantine Fault Tolerant) — property of a system that can reach consensus despite Byzantine failures.

Terminology Quick Reference

Term	One-Line Definition
Block	Container of ordered transactions + header hash
Chain	Ordered sequence of blocks linked by prev. hash
Node	Network participant storing full or partial chain
Miner	Node competing via PoW to append next block
Hash	Fixed-length deterministic fingerprint of data
Nonce	Number miners vary to find valid block hash
Difficulty target	Threshold hash must be below to be valid
Merkle tree	Binary hash tree over transactions in a block
UTXO	Unspent Transaction Output — Bitcoin's account model
Fork (soft)	Backward-compatible protocol upgrade
Fork (hard)	Non-backward-compatible split; creates new chain
Whitepaper	Nakamoto (2008) 9-page founding document
Satoshi	Smallest BTC unit: 10^{-8} BTC