Bitcoin Whitepaper — Executive Summary

Purpose
The paper proposes a decentralized digital currency system that allows online payments to be sent directly from one party to another **without going through a financial institution**.

---

1. The Problem It Solves

Traditional online payments rely on trusted intermediaries (banks, payment processors). This creates:

- Transaction fees
- Fraud risk
- Reversible payments
- Need for trust

The whitepaper's goal: **remove the need for trust** by using cryptography and distributed consensus.

---

2. Core Innovation — Blockchain Ledger

Bitcoin uses a public, distributed ledger called a **blockchain** that:

- Records all transactions
- Is shared across many computers (nodes)
- Cannot easily be altered once confirmed

Transactions are grouped into **blocks**, which are cryptographically linked.

---

3. Proof-of-Work Consensus

To add a block, computers must solve a cryptographic puzzle. This mechanism:

- Secures the network
- Prevents fraud and double-spending
- Determines which participant adds the next block

Participants performing this work are called **miners** and are rewarded with newly created bitcoin.

---

4. Decentralization

No central authority controls the system. Instead:

- Anyone can join the network
- Rules are enforced mathematically
- Trust comes from code and consensus, not institutions

---

5. Limited Supply

The system caps total coins at **21 million**, making it scarce by design. New coins enter circulation as mining rewards, which decrease over time.

---

6. Privacy Model

Bitcoin is **pseudonymous**, not anonymous:

- Transactions are public
- Users are identified by cryptographic addresses, not names

---

7. Security Assumption

The system is secure as long as honest nodes control the majority of computing power. Attackers would need more than 50% of total network power to manipulate it (a “51% attack”).