

Assignment

Summary: The problems bitcoin solves, how blockchain works, why it matters.

Satoshi Nakamoto's Bitcoin whitepaper solved a fundamental problem of the digital age: how to make online payments without a trusted middleman like a bank. The old system was flawed because it allowed transactions to be reversed, incurred high fees, and struggled with "double-spending" the risk that a digital coin could be copied and spent twice. This made small, casual online transactions impractical.

The solution is a revolutionary technology called the blockchain. It acts as a public record book that is duplicated and maintained by a vast network of computers, meaning no single company or government controls it. The process begins when a user announces a transaction. Special network participants, known as miners, then collect these transactions into a block. The core innovation is the proof-of-work system. To add a block to the chain, miners must compete to solve a difficult cryptographic puzzle, which requires significant computational effort and electricity. This process secures the network in two key ways: it makes adding blocks expensive and time-consuming, and it mathematically locks each block to the one before it. Once a block is added, altering it would require redoing its proof-of-work and that of all subsequent blocks, an impossible task against honest network. The system automatically agrees that the longest valid chain is the true history, achieving consensus without a central coordinator.

The importance of this invention goes far beyond creating digital cash. Blockchain provides a new, decentralized model for trust on the internet. It allows us to verify information and transfer assets directly, securely, and transparently. This is enabling a wave of innovation, powering new business models from disintermediated marketplaces to systems that provide unparalleled security for data and supply chains. In essence, blockchain technology is reshaping the digital world by replacing centralized control with a system of mathematical, decentralized trust.
