The Double Spending Problem

Why digital cash needs blockchain consensus

Alice (Attacker)

Has 1 BTC

Transaction 1

Send 1 BTC to Bob

(Buy goods)

Transaction 2

Send 1 BTC to Carol

(Buy services)

PROBLEM: Which transaction is valid?

Without consensus, both recipients think they were paid

SOLUTION: Blockchain consensus determines which Tx is confirmed first

PoW/PoS ensures network agrees on transaction order

Source: Nakamoto, Bitcoin Whitepaper (2008), "Commerce on the Internet"