Artificial Intelligence for Business

Deterministic technologies vs. probabilistic technologies

Lecture 6

Professor: Asror Norov

Preview

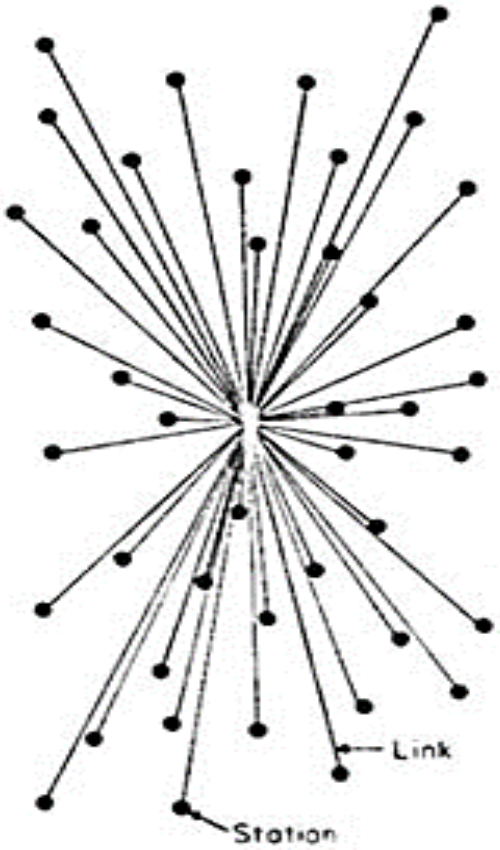
- Blockchains and Distributed Ledgers
- Types of Cryptocurrencies (and uses)
- Current Legal Landscape
- Investment Potential and Concerns
- Smart Contracts

Blockchains and Distributed Ledgers

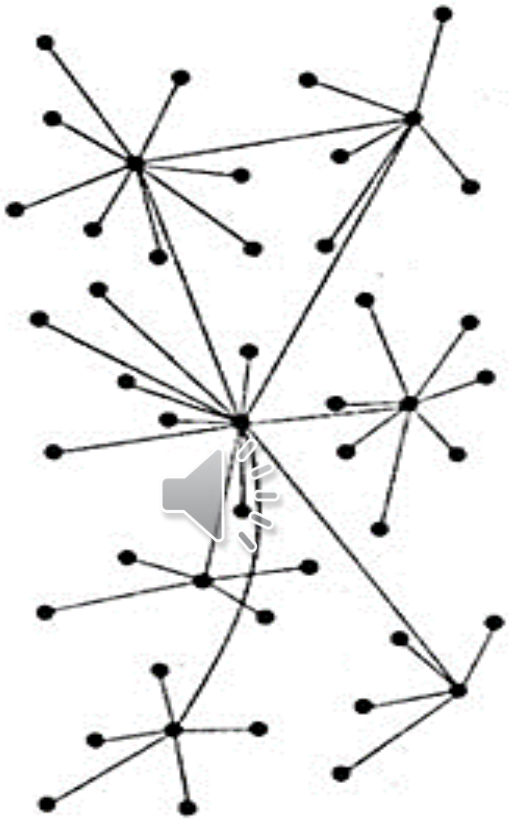
Blockchains and Distributed Ledgers

- Blockchains
  - The technology behind cryptocurrencies.
  - Analogous to the TCP/IP Protocol that is the foundation of the internet

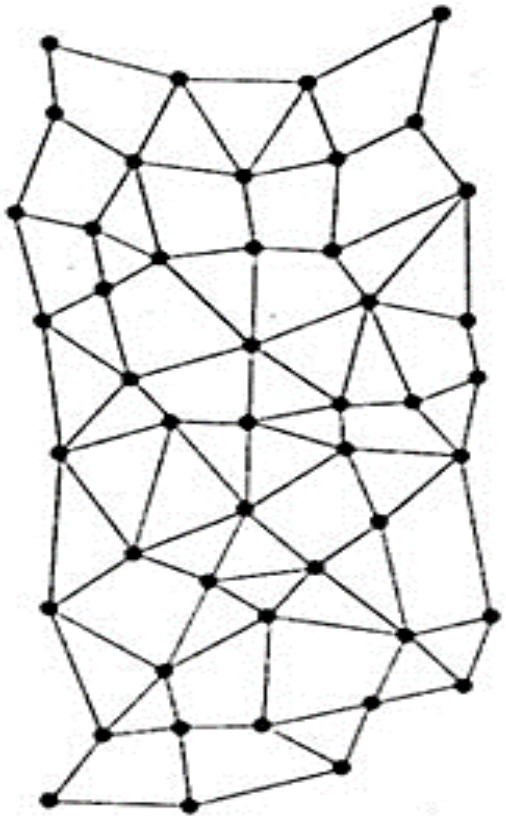
- Blockchains are Distributed Ledgers
  - Ledgers are historically centralized and private
  - Blockchains are Decentralized or Distributed



CENTRALIZED
(A)



DECENTRALIZED
(B)



DISTRIBUTED
(C)

How Blockchains Work: Basics

- Chronological Ledger
  - Transactions often “pseudo-anonymous”
  - Transactions are grouped together in “blocks”
  - Transactions are logged and stamped with information about the time, amount, and participants as if a notary is present at every transaction

- Blockchain is not centralized (does not have one owner), therefore there are strict rules about how it must be maintained

How Blockchains Work: Maintenance

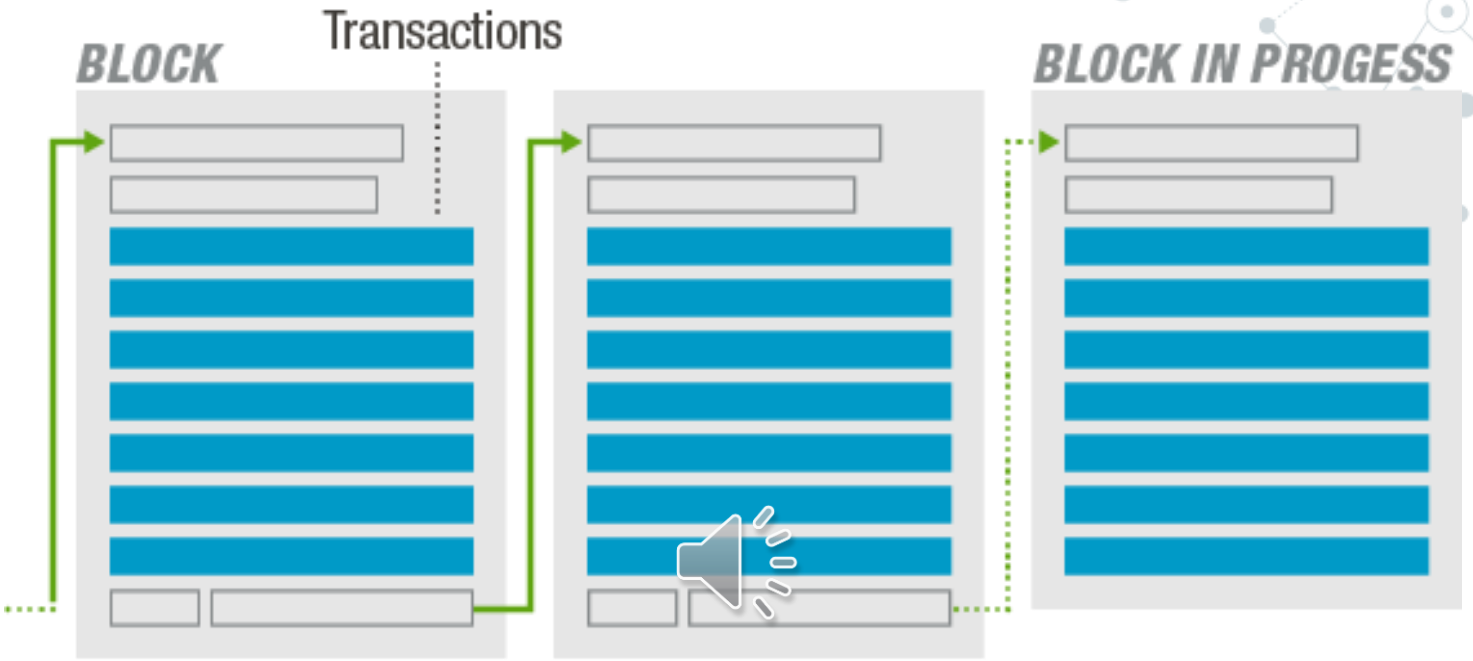
- The individuals who maintain and update the Blockchain are “miners,” and they are paid a reward

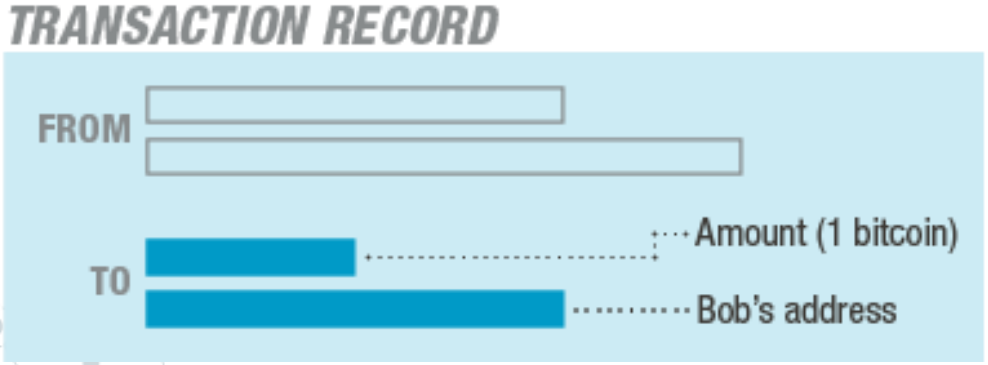
- The Miners process transactions by:
  - Solving a complex mathematical problem
  - Sending transactions to other nodes to be verified.

How Blockchains Work: Hashing

- When all miners agree the problem has been solved correctly, the block is added to the chain and is visible to the entire network

- The unbroken Hash (seal) confirms that the block, and therefore every block before it, is legitimate


BLOCK
Transactions
BLOCK IN PROGESS

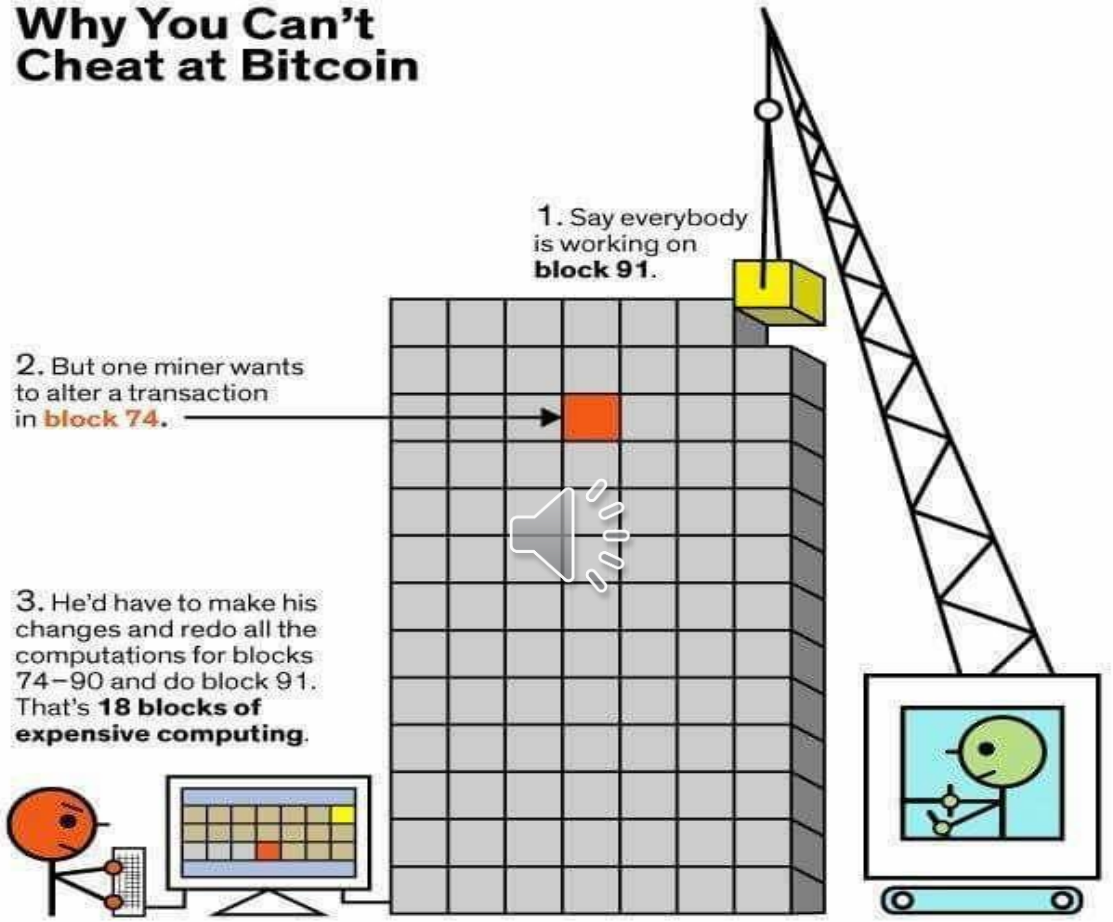

TRANSACTION RECORD
FROM
TO
Amount (1 bitcoin)
Bob's address

How Blockchains Work: Hashing (cont.)

- Recall: Transactions must be validated by other network miners

- Miners incentivized to add “valid” transactions via a reward; invalid transactions are rejected, and thus, no reward is given

Why You Can't Cheat at Bitcoin



4. What's worse, he'd have to do it all **before** everybody else in the Bitcoin network finished **just the one block (number 91)** that they're working on.