How Cryptocurrency works?

Presented BY: Dr Abdurashid Turgunov

Course name: Blockchain Technology

Preview

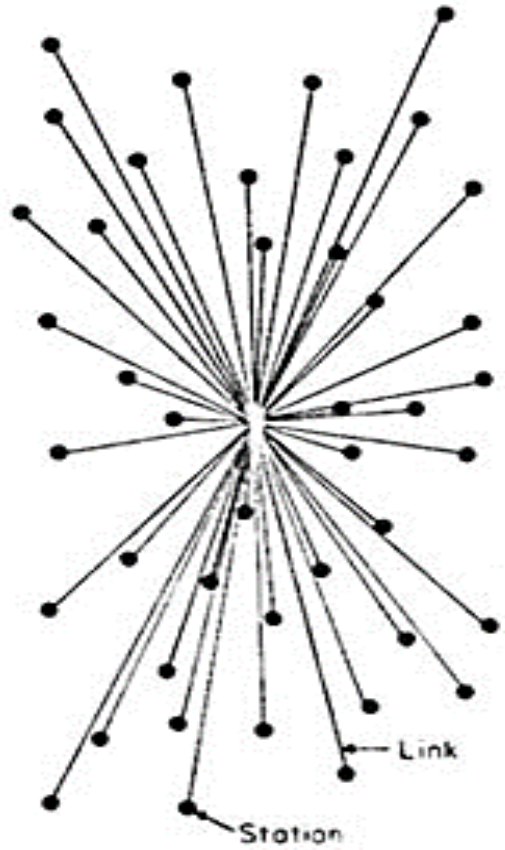
- Blockchains and Distributed Ledgers
- Types of Cryptocurrencies (and uses)
- Current Legal Landscape
- Investment Potential and Concerns
- Smart Contracts
- Other Blockchain Uses

Blockchains and Distributed Ledgers

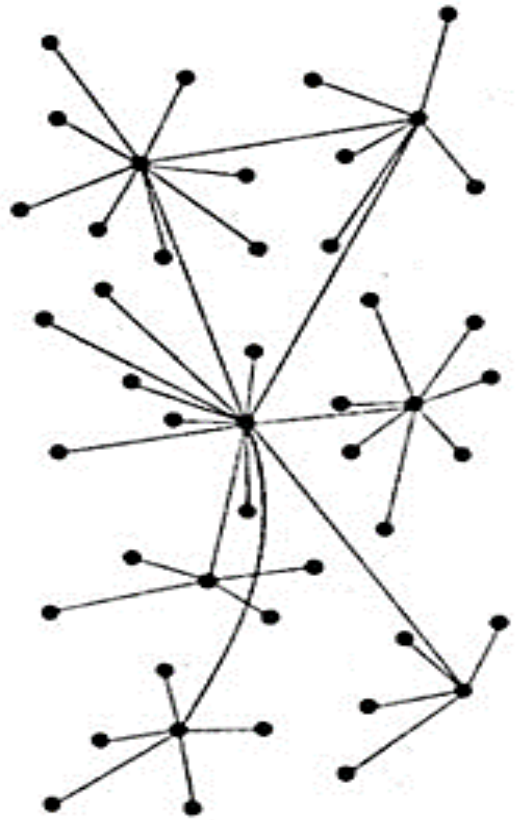
Blockchains and Distributed Ledgers

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

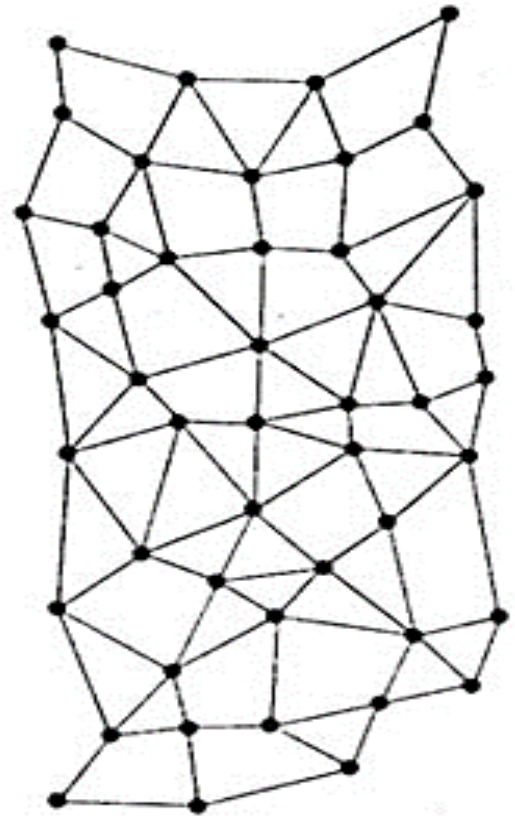
- Blockchains are Distributed Ledgers
  - Ledgers are historically centralized and private
  - Blockchains are Decentralized or Distributed



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

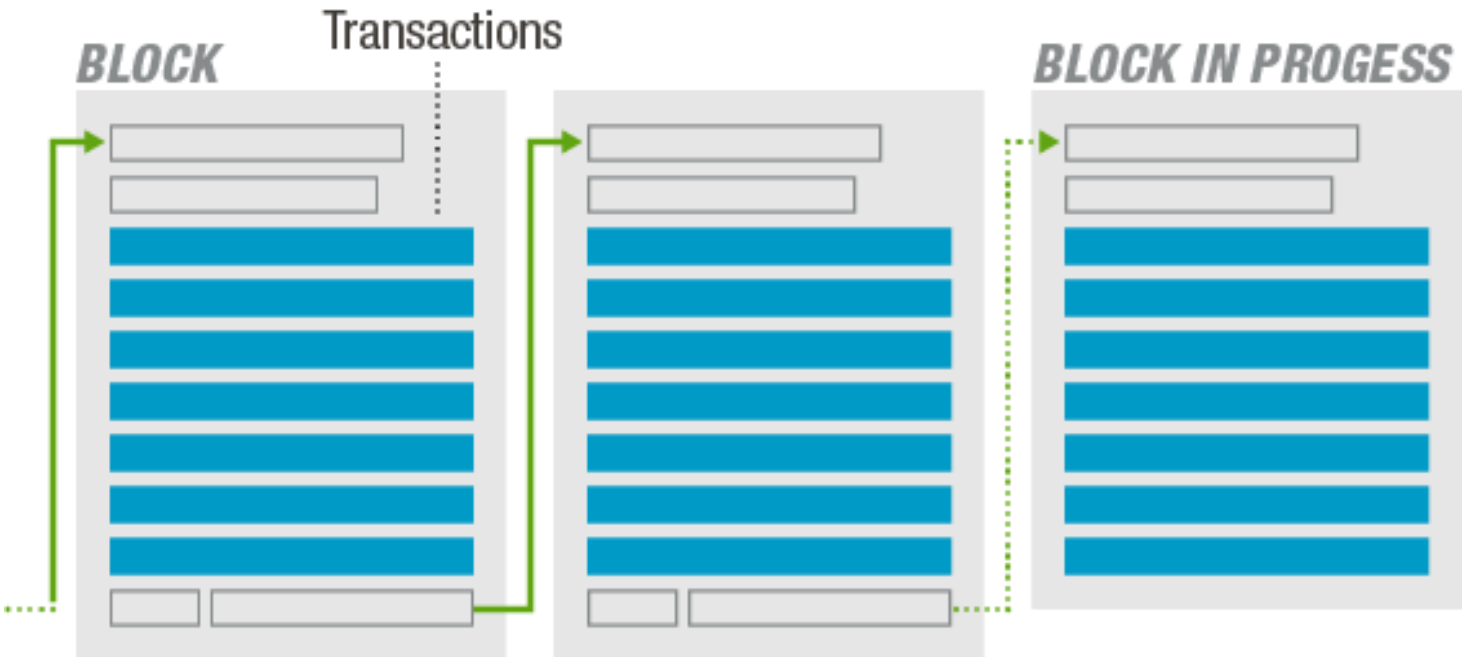
- The individuals who maintain and update the Blockchain are “miners,” and they are paid a reward

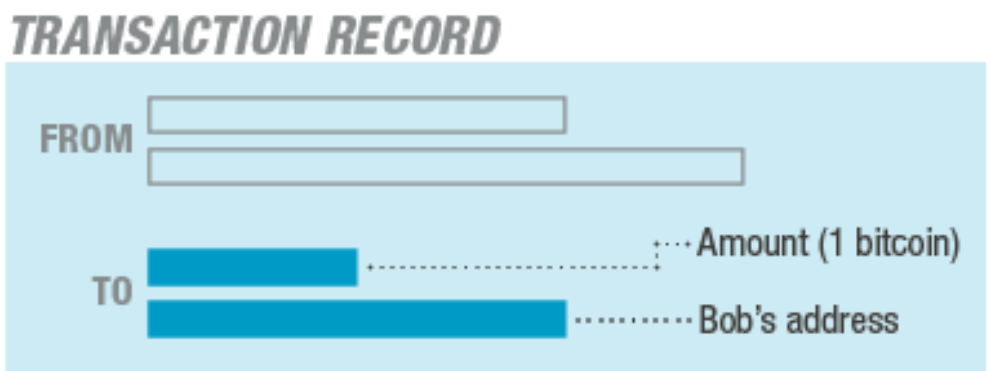
- The Miners process transactions by:
  - Solving a complex mathematical problem
  - Sending transactions to other nodes to be verified.

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

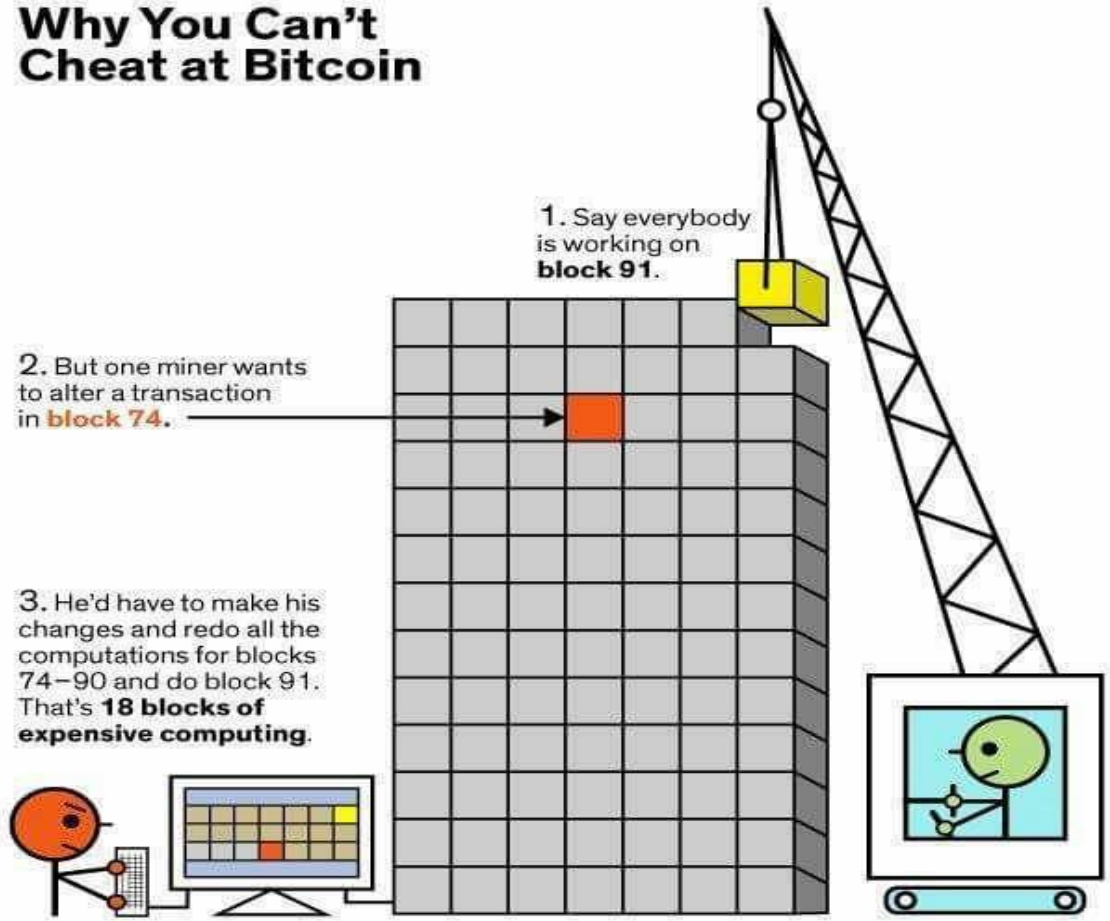

Transactions
BLOCK
BLOCK IN PROGESS


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.

Types of Cryptocurrencies and Uses

Types of Cryptocurrencies and Uses

- Bitcoin origins: Peer-to-Peer “cash-like” transactions
- Limited Quantity (21 million coins)
- No need for third-party intermediary
- Double-spend problem

Types of Cryptocurrencies and Uses (cont.)

- Protocol Tokens and Uses:
  - Store Value
  - Acts more like cash
  - Usually considered a security

Types of Cryptocurrencies and Uses (cont.)

- Protocol Tokens

Types of Cryptocurrencies and Uses (cont.)

- Utility/Application Tokens and Uses:
  - May store value, but usually has a function
  - Acts similar to an arcade token
  - Sometimes considered a security, sometimes not

Current Regulatory Landscape

Current Regulatory Landscape

- SEC
- U.S. Treasury/FinCEN
- IRS
- State Regulators/Lawsuits

Investment Potential and Concerns

Investment Potential and Concerns

- How and Where to Invest
  - Exchanges
  - Crypto ATMs
  - Peer-to-Peer

Investment Potential and Concerns

- How and Where to Invest
  - ETFs
  - Futures
  - Hedge Funds
  - Initial Coin Offerings (ICOs)

Tax Concerns

- As Income
  - Market Value of:
    - Currency
    - Good or Service Provided
- As Property
  - Cost Basis
  - Capital Gains

Smart Contracts

Smart Contracts

- Self-automated computer programs that can carry out the terms of any contract

- Mostly based on objective conditions precedent
  - “If, then” criteria

Smart Contracts (cont.)

- Variables: Readily Verifiable Data
- Oracles

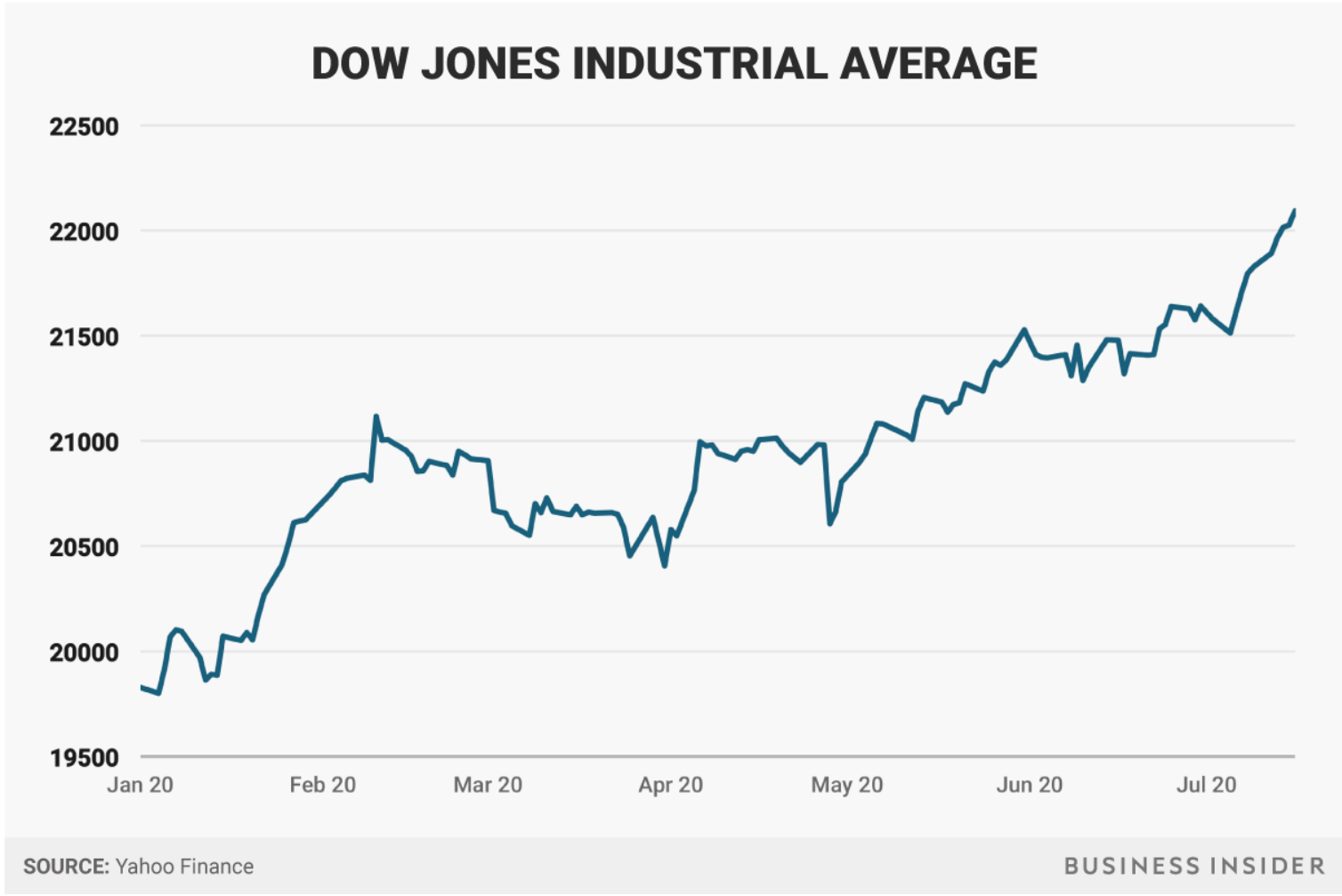
Smart Contracts (cont.)

- Variables: Readily Verifiable Data
- Oracles: Reliable sources
  - Social Security DMF
  - FAA Records
  - National Weather Service
- Crowdsourcing
  - Voting

Smart Contracts (cont.)

- Think: Escrow Agreements
  - Money held in escrow until performance is met
  - Once performance is validated, money released
  - Regulated by an unbiased party, which only seeks the objectively “right” answer, devoid of outside influence

Smart Contracts: Ethereum


DOW JONES INDUSTRIAL AVERAGE
22500
22000
21500
21000
20500
20000
19500
Jan 20
Feb 20
Mar 20
Apr 20
May 20
Jun 20
Jul 20
SOURCE: Yahoo Finance
BUSINESS INSIDER

DAO: Distributed Autonomous Organization

- DAO: the most popular Smart Contracts platform

- A DAO is “a tightly packed collection of smart contracts written on the Ethereum blockchain”

- A DAO’s smart contracts amount to a series of by-laws that determine how its constituency — anyone around the world who has bought DAO tokens with ethers — votes on decisions.

DAO: Distributed Autonomous Organization (cont.)

- Ether: Entry Token used to:
  - Record transactions
  - Vote on outcomes
  - Purchase other tokens within the ecosystem

- Transactional process (sharding)
  - Top level retains “master ledger”
  - Lower level nodes run Proof of Stake
  - Much more efficient from a scaling perspective (compared to Bitcoin simple Proof of Work)

Other Blockchain Applications

Other Blockchain Applications

- Issuing Stocks and Bonds
- Insurance
- Land Registries
- Supply Chain Integrity

Reference and source

- 1. Bitcoin & Cryptocurrency Technologies: Bitcoin Mining, Blockchain Basics And Cryptocurrency Trading & Investing For Beginners | 7 Books In 1 by Boris Weiser (Author)
- 2. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Crypto Trading, Derivatives, Digital Assets) – Illustrated, September 15, 2018 by Antony Lewis (Author)
- 3. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World – June 12, 2018 by Don Tapscott (Author), Alex Tapscott (Author)
- 4. Blockchain Technology for IoT Applications (Blockchain Technologies) 1st ed. 2021 Edition
- by Seok-Won Lee (Editor), Irish Singh (Editor), Masoud Mohammadian (Editor)
- 5. Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher (Author) Format
- 6. Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond – October 19, 2017 by Chris Burniske (Author), Jack Tatar (Author)