803400815101 Blockchain and Smart Contracts

Artificial Intelligence Technologies Program (Graduate)

Graduate School of Natural and Applied Sciences

2023 - 2024 Spring Semester

ANKARA UNIVERSITY

The First University of The Republic of Turkey

Financial Technologies and Crypto Economy

Assist. Prof. Dr. Murat KARAKUS

Email: mrtkarakus@ankara.edu.tr

Faculty of Engineering

Ankara University

Outline

- Topics to cover:
  - Definition, Sense, and History of Money
  - World of Digital Money and Cryptocurrencies
  - Money Politics
  - Financial Blockchain
  - Fundamentals of Peer-to-Peer Cash Payment System
  - General-Purpose Programmable Blockchain Fundamentals

Introduction

- Bitcoin, a cryptocurrency, using blockchain.
- Blockchain networks are not just for crypto currency.
- How digital records with no physical value, like Bitcoin and its derivatives, may become so valuable.
- Concepts of value and money.

Understanding the Definition of Money: Yap Island and Stone Coins (Rai)

Figure 1: Yap Islands money stones

Understanding the Definition of Money: Yap Island and Stone Coins

- Stones are too big for shopping or giving a gift
  - But no one makes it a problem.
- Chief announces new owner
- Everyone learns new owner
- Stone ownership shared among chiefs

Understanding the Definition of Money: Yap Island and Stone Coins

- In the Yap Islands, money as stones
- Value in people's memories.
- Stones' ownership crucial
- System works even without stone location

Understanding the Definition of Money: Yap Island and Stone Coins

- Stone under sea
- Trust in the chief
- Money = consensus tool for a common value judgment
- How or what it will look like next is just a detail.
  - Pieces of stone (as used on Yap island),
  - Coins from the board game Monopoly,
  - Hard-to-copy paper notes,
  - A credit card with a silicon processor, or
  - A unique data records on the Bitcoin blockchain network.

History of Money

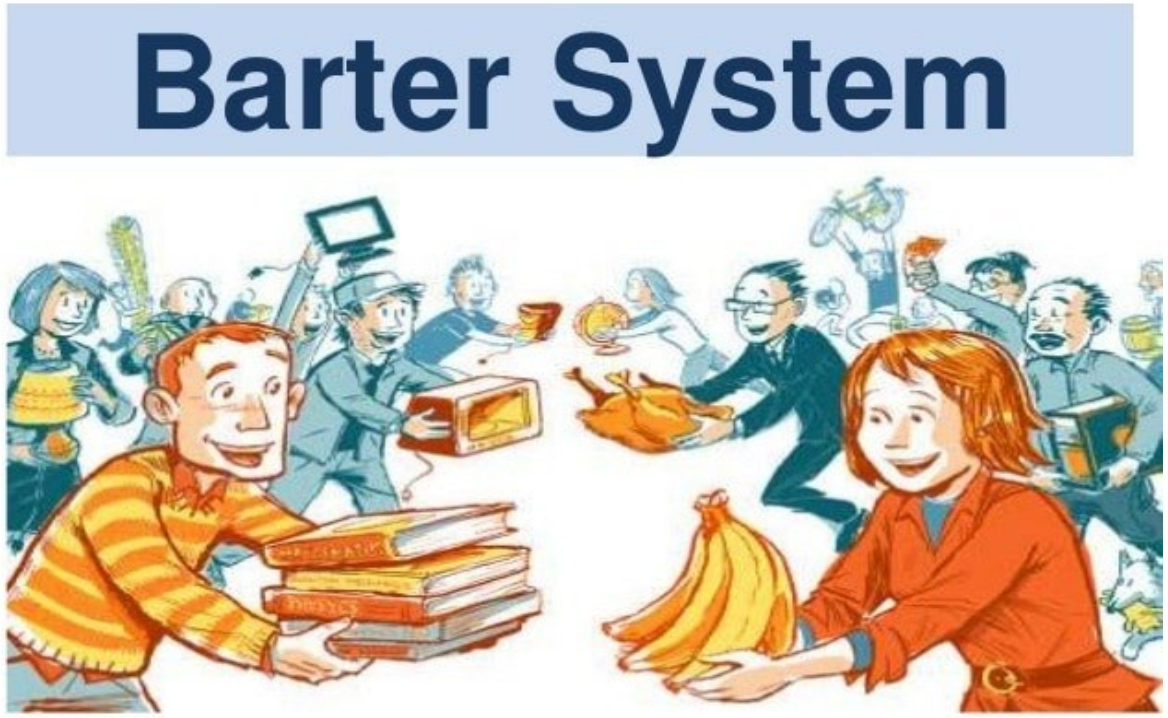


Figure 2: Barter System

History of Money

- Barter system difficulties
- Lack of matching services/goods
- Need for agreed exchange rate
- Transition to price-based barter
- **Price** defined as benefit in barter system

History of Money

Figure 3: Ancient Greek and Roman coins

History of Money

- Metal coins: Volume and weight issues
- Introduction of paper money
- Chinese invention of paper and printing
- First paper money by the Mongol empire

History of Money

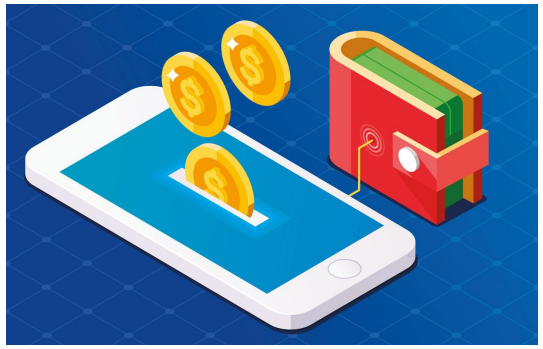
Barter

Gold

Coins (Metal Money)

Banknotes (Paper Money)

Credit Cards (Plastic Cards)



Electronic Money

Cryptocurrencies

Figure 4: Evolution of Money

Features of Money

- The main features of money are as follows:
  - **Mobility**
  - **Durability**
  - **Divisibility**
  - **General Acceptance**

Functions of Money

- The main functions of money are as follows.
  - **A Medium of Exchange (Exchange)**
  - **Common Measure of Value**
  - **A Saving and Borrowing Tool**
  - **An Economic Policy Tool**

Functions of Money

- The history of Money is as old as the history of civilization.
- Money represents the power and freedom of countries
- Para (Turkish word) ← Pare (Persian Word, meaning *small piece*)
- Lira (Turkish Word) ← Libre (Latin Word, meaning *scales*)
- Digital money and cryptocurrency in 21st century

Functions of Money

- Emergence of various 21st-century currencies
- Independent of government support
- Operate in a virtual environment
- Known as cryptocurrencies
- Stored in virtual wallets with passwords

Functions of Money

Figure 5: Token coins of cryptocurrencies

Objectives of Monetary Policy

- Central bank monetary policy
- Money supply and interest rate
- Money supply effects on economy and price level
- Monetary policy based on economic conditions
- Monetary policy goals: price stability and inflation control

Objectives of Monetary Policy

- **Ensuring Price Stability**
  - Reduce the negative impact of the increase in the price level
- **Employment**
  - Prevent and eliminate real unemployment.
- **Economic Growth**
  - Bring total growth in the economy.
- **Interest Stability**
  - Maintain a certain level of stability in interest rates.
- **Stability of Markets:**
  - Prevent the emergence of financial panics
- **Balance of Payments**
  - Maintain the balance of foreign payments

Types of Currency

- Types of coins
  - Fiat money
    - State-controlled
    - Built on trust
  - Digital, virtual, and crypto money
    - Not under state control
    - Have economic value

Types of Currency: Digital Currency

- Digital money → not printed and physically circulated.
- Digital money → stored and transferred electronically.
- Loading money on smart cards and shopping with these.
  - Credit cards

Types of Currency: *Virtual Currency*

- Virtual currencies are a kind of digital money
- A virtual currency is a digital representation of a value
- Not issued by any government or central bank.
- Generally, used as a means of payment in places such as in-app purchases

Types of Currency: Cryptocurrency

- Secure transactions
- Digital and virtual money
- Trust from cryptographic algorithms
- Predetermined production rules

Types of Currency: Cryptocurrency

- Positive and negative features of Cryptocurrencies

Positive Features

- Independent of the central banks
- Includes authentication processes.
- Little or no commission fee for money transfers.
- No time limit for money transfers.

Types of Currency: Cryptocurrency

Negative Features

- No mechanism to oversee cryptocurrencies.
- Limited money supply
  - However, altcoins are produced to overcome this problem.
- High volatility in value.
- Anonimity in transfers.
- More limited use for goods and services
- Nearly impossible tracing in case of theft or loss.

Differences Between Digital Currency and Cryptocurrency

- Issuance
  - Digital currencies → an authority,
  - Cryptocurrencies → no authority.

- Transactions
  - Digital currencies → Real persons,
  - Cryptocurrencies → Confidential.

Why is Bitcoin So Valuable?

- Bitcoin's price rised to $60,000 since 2008
- Trust in Bitcoin technology
- Acceptance by large communities
- Attention from tech enthusiasts and programmers
- Bitfinex hack in 2016
- Suspension of US dollar transfers
- Bitcoin price increase in other exchanges

Why is Bitcoin So Valuable?

- NSA data breach by hackers
- WannaCry virus attacks for Bitcoin ransom
- Bitcoin price exceeding $1,200 in February 2017
- Worldwide Bitcoin demand due to news and media
- Bitcoin's rapid price fluctuations from January 2018

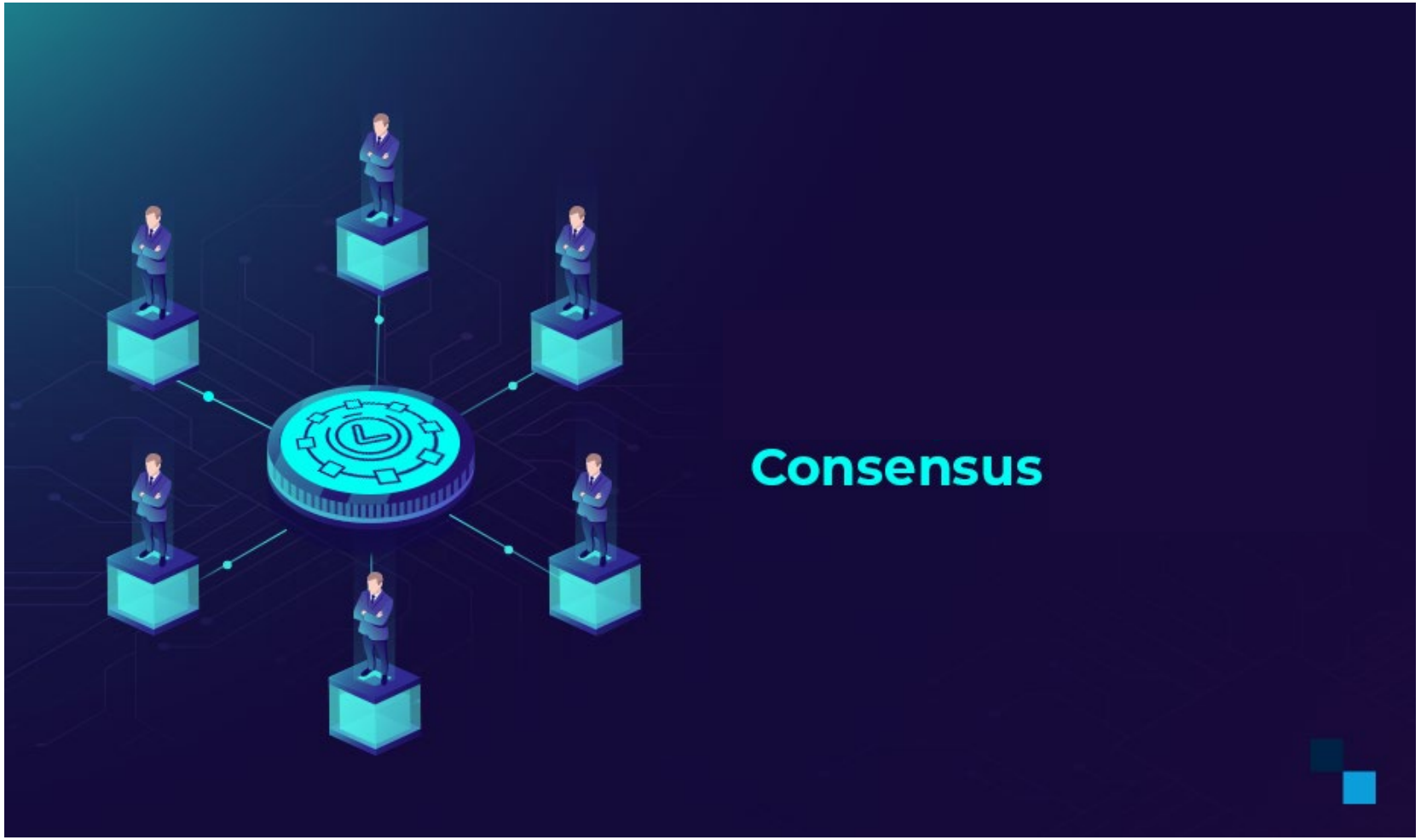
World of Digital Money and Cryptocurrencies

Figure 6: According to the data of coindesk.com, which gives the market value of Dollar/Bitcoin, the market value of 1 BTC on March 18, 2024 was stated as $67,500.31.

The Consensus Triggering the Value

- The journey towards a cashless society
- Trust element in debit and credit card transactions
- Role of banking infrastructure and government oversight in cashless transactions

The Consensus Triggering the Value



The Consensus Triggering the Value

World of Digital Money and Cryptocurrencies

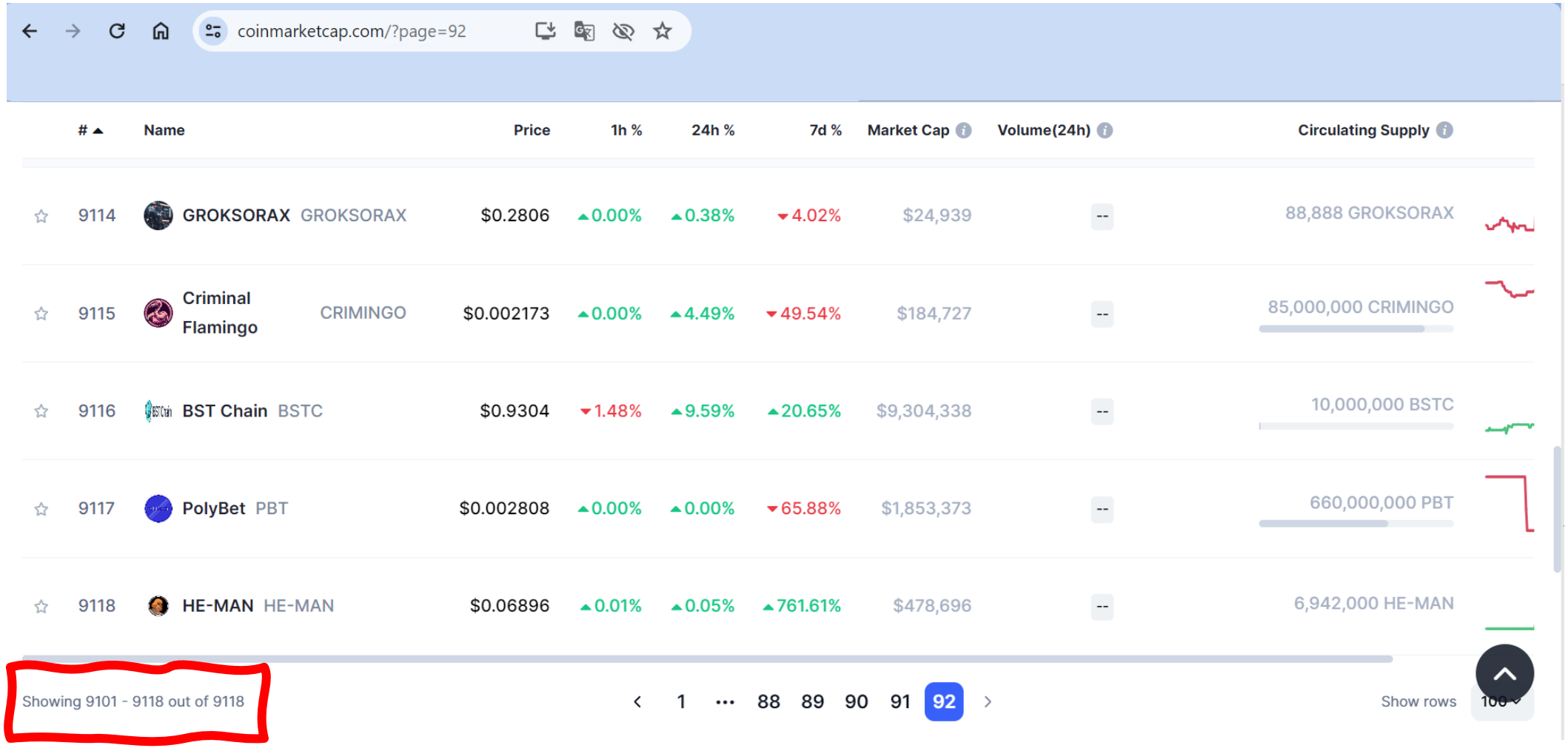
- Digital money is not new, not limited to Bitcoin
- 1983: David Chaum's scholarly article[1] introduced cryptology for digital money
- 1990: David Chaum launched DigiCash
- DigiCash allowed users to save money as "eCash" on computers
- Privacy and security not prioritized in early online behavior

[1] *Chaum, David (1983). "Blind signatures for untraceable payments" (PDF). Advances in Cryptology Proceedings. 82 (3): 199–203.*

World of Digital Money and Cryptocurrencies

World of Digital Money and Cryptocurrencies

- Success of Bitcoin led to emergence of altcoins
- Thousands of altcoin attempts
- Reasons for interest: income potential, easy earnings


coinmarketcap.com/?page=92
Name Price 1h % 24h % 7d % Market Cap Volume(24h) Circulating Supply
9114 GROKSORAX GROKSORAX $0.2806 0.00% 0.38% 4.02% $24,939 -- 88,888 GROKSORAX
9115 Criminal Flamingo CRIMINGO $0.002173 0.00% 4.49% 49.54% $184,727 -- 85,000,000 CRIMINGO
9116 BST Chain BSTC $0.9304 1.48% 9.59% 20.65% $9,304,338 -- 10,000,000 BSTC
9117 PolyBet PBT $0.002808 0.00% 0.00% 65.88% $1,853,373 -- 660,000,000 PBT
9118 HE-MAN HE-MAN $0.06896 0.01% 0.05% 761.61% $478,696 -- 6,942,000 HE-MAN
Showing 9101 - 9118 out of 9118
1 ... 88 89 90 91 92
Show rows 100

Is Cryptocurrency Threatening the World of Finance and Banking?

- 2008 global financial crisis eroded consumer trust in banking
- Anarchists see Bitcoin as a threat to global money markets
- Bitcoin's decentralization, resistance to inflation, and post-crisis popularity

Is Cryptocurrency Threatening the World of Finance and Banking?

- Bitcoin's value is still measured in dollars
- Bitcoin is not a true alternative to the global financial system
- Bitcoin's volatility raises concerns about everyday transactions
- Media attention and publicity are driving Bitcoin trading

Is Cryptocurrency Threatening the World of Finance and Banking?

- Uncertainty regarding Bitcoin's future as a currency
- Concerns about Bitcoin's security and vulnerability
- The transparency of Bitcoin network nodes
- Questions about the ability of states to control or stop Bitcoin
- Potential risks related to hacking and government surveillance
- Impact on trust in Bitcoin
- The transformative potential of blockchain technology

What is the Difference Between Cryptocurrencies and Each Other?

- Cryptocurrencies serve different purposes and offer different features.
- Main features of cryptocurrencies as follows:
  - Consensus Approach/Process
  - The problem used in the cryptocurrency production process
  - The hashing algorithm used
  - Developing other service capabilities within the platform
  - Average time (frequency) required to generate each new block
  - Block size (the block size is determined as 1MB in the Bitcoin structure.)
  - Amount of cryptocurrencies that can be created (volume of emissions)

What is the Difference Between Cryptocurrencies and Each Other?

- Litecoin (LTC) has a 2.5-minute block frequency
- Bitcoin has an average block time of 10 minutes
- Litecoin's consensus mechanism discourages dedicated hardware mining
- Maximum Supply:
  - Litecoin - 84 million coins
  - Bitcoin - 21 million coins

What is the Difference Between Cryptocurrencies and Each Other?

- Zcash encrypts sender, receiver, and amount in transactions
- Altcoins employ diverse approaches to address technical challenges
- Dogecoin introduced a random incentive payout for block generation
- This feature was canceled due to a system error

Financial Blockchain

- Blockchain 1.0: DLT - Initially focused on financial transactions
- The foundation of cryptocurrency production
- Concept introduced by Hal Finney in 2005
- Satoshi Nakamoto's white paper in 2009
- Commencement of the blockchain 1.0 era

Financial Blockchain

- Blockchain 1.0 → Application for the creation of a network-managed reliable cryptocurrency

- Basic components of Blockchain 1.0 technology;
  - Cryptocurrency
  - Wallet
  - Cryptocurrency mining rigs
  - Crypto mining software

Financial Blockchain

- **Cryptocurrency:** Digital or virtual forms of currency
- **Crypto Wallets and Software:** Programs for storing cryptocurrencies
- **Private Key:** Essential for storing and securing cryptocurrencies
- Sending and Receiving Cryptocurrencies
- **Types of Crypto Wallets:** Hot wallets and Cold wallets

Financial Blockchain

- Hot Wallet
- Uses Online Software
- Protects Private Keys

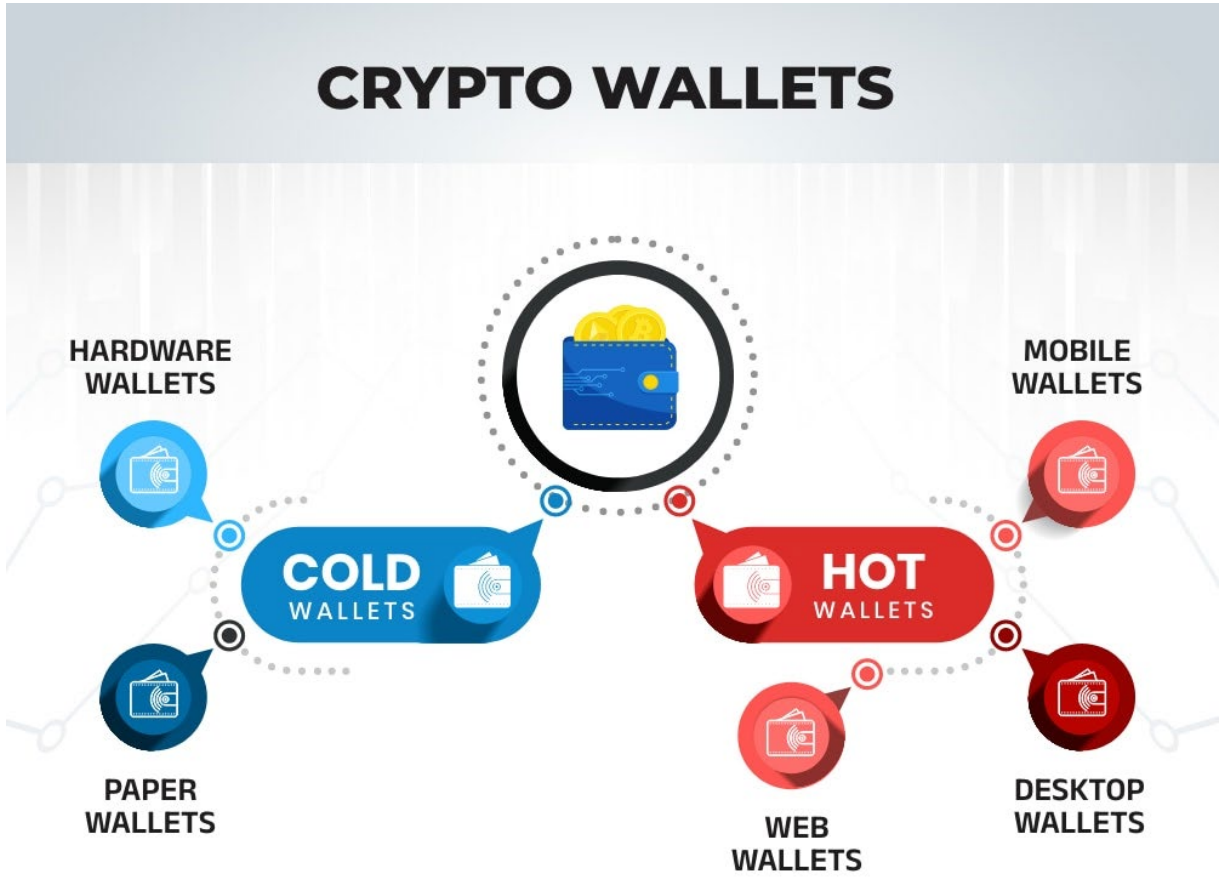


Figure 8: Crypto hot and cold wallets

Financial Blockchain

- Cold Wallets (Hardware Wallets)
- Offline Electronic Devices (e.g., Flash Memory)
- Secure Storage of Private Keys

Figure 9: Trezor and Ledger (crypto hardware wallets)

Financial Blockchain

- **Crypto Mining Software**: Solves complex math problems for coin generation
- **Blockchain Core**: Connects to blockchain network, runs a node
- Generally open source
- **Cryptocurrencies**: First implementation of Blockchain 1.0
- Medium of exchange
- Created and stored electronically
- Uses cryptographic techniques
- Allows money transfer verification

Bitcoin Peer-to-Peer Electronic Cash System (Bitcoin P2P-ECS)

- Peer-to-Peer Electronic Cash System (P2P-ECS)
  - Bitcoin network
- The P2P-ECS forms the basis of the open chain type
- P2P-ECS is essentially digital data
  - Enables two parties to create a payment system based on trust without the need for an intermediary institution.

Bitcoin Peer-to-Peer Electronic Cash System (Bitcoin P2P-ECS)

- Unique equipment needed for mining
- Users paid in coins or cryptocurrency
- Block length increases as new blocks are added
- Halving: Reduced payout as maximum bitcoins mined is being approached

Main Features of P2P-ECS

- Bitcoin limited to 21 million coins
- Mining reward halves every four years
- Digital wallets have public and private keys
- Private key for wallet access
- Public key for cryptocurrency transfers on the blockchain

Main Features of P2P - ECS

- Bitcoin P2P - ECS's features compared to other currencies :
  - Not dependent on a central authority
  - Production and use of a digital technology
  - Inability to imitate and reproduce
  - Transaction confirmation time is approximately 10 minutes
  - Transactions with P2P technology

Bitcoin P2P - ECS Block Structure

- Blocks use cryptography to encrypt data
- Bitcoin P2P - ECS is a cryptocurrency
- 1 MB blocks previously (~2000 transactions)
- SegWit activation increased block size to 4 MB, boosting transactions per second

Working Principle of Bitcoin P2P – ECS

- Each node accesses an open ledger
- Network nodes validate new transactions
- New data enters the memory pool
- Verified as blocks before being added to the network
- Block generation time: 10 minutes

Working Principle of Bitcoin P2P - ECS

- Senders sign transactions with private keys
- Transaction data is stored in the register
- Verification by other nodes
- Transaction inclusion in a block
- Requirement for a bitcoin wallet
- Generation of public and private keys for the wallet
- Public key as an account number

Working Principle of Bitcoin P2P – ECS

- Ahmet uses Berna's public key to transmit crypto money.
- The public key does not reveal the person's identify.
- Berna receives the crypto once the block transaction is authorized.
- Berna's private key unlocks this cryptocurrency.
- Cryptocurrencies require a private key that is blockchain credentials.

Working Principle of Bitcoin P2P – ECS

- Avoid double transactions with blockchain
- Accurate real-time transaction data
- Blockchain timestamping
- Blocks recorded chronologically
- Timestamps prevent reuse or copying

About Blockchain 2.0

- Blockchain 1.0 is stable but has performance issues, cloud integration issues, and deployment issues.
- **Blockchain 2.0, a peer-to-peer value exchange system**, solves these issues and advances blockchain technology.
- The first general-purpose **programmable blockchain** enabled Blockchain 2.0.
- **Blockchain 2.0** technology helps markets, **not a focus crypto money**.
- **Smart contracts** and certificates facilitate asset exchange.

About Blockchain 2.0

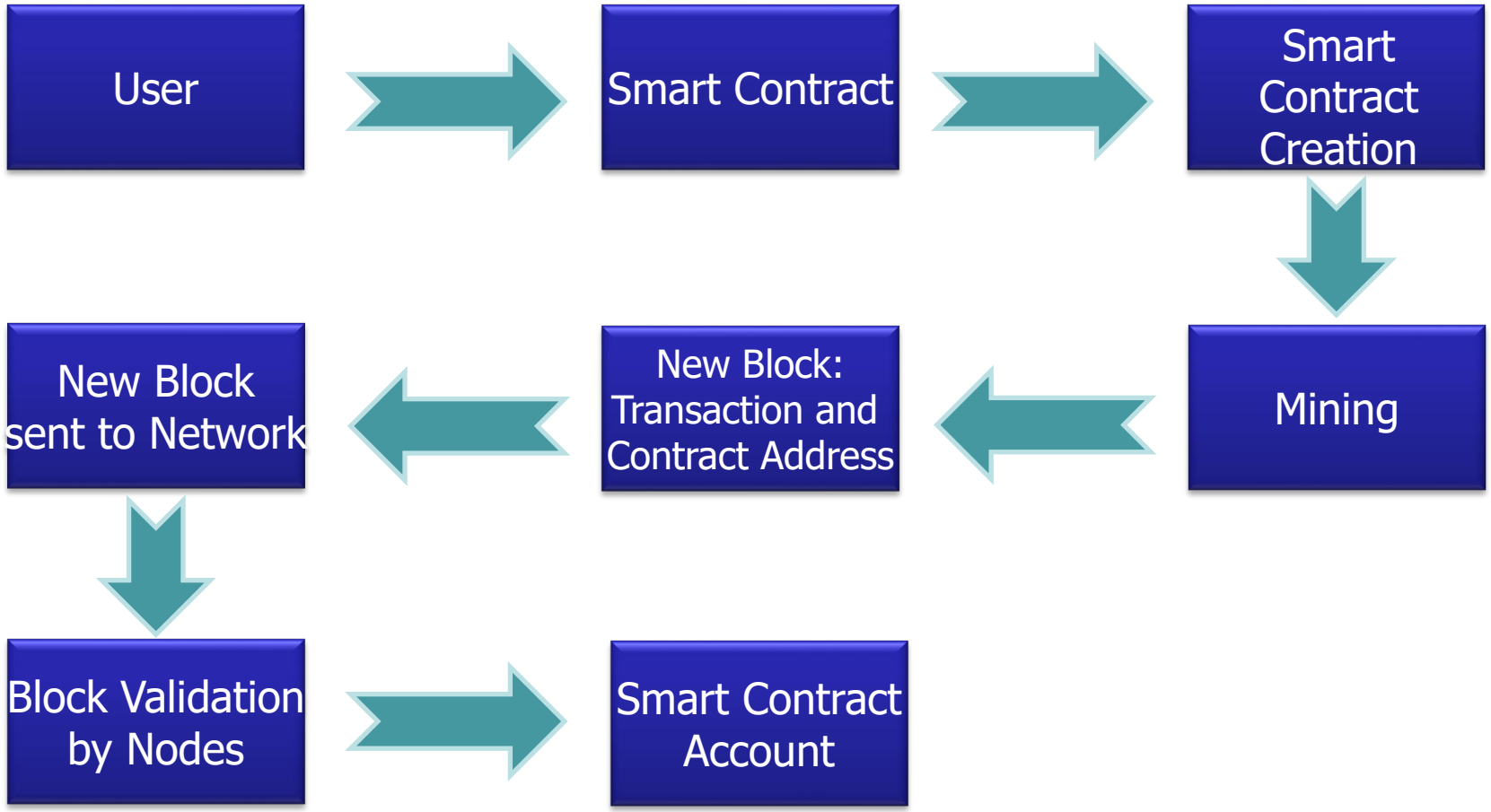


Figure 10: Preparation and operation flow of smart contract

First General-Purpose Programmable Blockchain: Ethereum

- P2P – ECS: Basis for the first general-purpose blockchain (Ethereum)
- Independent of central authority
- Used for cryptocurrency and digital assets
- Utilized in financial services, games, smart contracts, and apps
- Powers immutable, accessible programs
- Low-cost cryptocurrency transactions

First General-Purpose Programmable Blockchain: Ethereum

1. First general-purpose programmable blockchain: Resource for all actors

- Blockchain's public transaction database: Single truth in the ecosystem
- Public and shared database: Stores user-application transactions
- Transactions validated by thousands of computers
- Transactions are final and tamper-proof
- Protects blockchain integrity

First General-Purpose Programmable Blockchain: Ethereum

2. Platform for smart contracts

- Critical application infrastructure
- Acts as the "World Computer"
- Applications and transaction data distributed over thousands of nodes
- Ability to store and strengthen applications
- Key feature distinguishing blockchain from P2P - ECS

First General-Purpose Programmable Blockchain: Ethereum

- Some of the features of the first general purpose programmable blockchain:
  - Banking for everyone
  - A more private internet
  - Peer-to-peer network
  - Censorship resistance

Working Principle of First General Purpose Programmable Blockchain

- Millions of simultaneous transactions
- Similar to P2P - ECS
- Transactional state machine
- Valid transactions enable state changes
- Mining utilizes computational resources for valid block construction

Working Principle of First General Purpose Programmable Blockchain

- A node that advertises as a miner can produce blocks or verify them.
- Miners must give proof when adding a block to the network.
- The block is legitimate if there is proof.
- The network pays miners for validating new blocks.
-
- Every block mined earns **Ether**.

Blockchain Applications used in Financial Technologies

- Programmable blockchain technology:
  - payment systems,
  - financial research,
  - insurance,
  - loan and debt transactions, etc.
- Some of the blockchain applications used in the financial field:
  1. Commercial Finance Platforms
  2. Exchange Transactions
  3. Cross-Border Transactions
  4. Credit Reporting Processes
  5. Digital Authentication

Q/A


WHEN?
HOW?
WHERE?
WHO?
WHAT?
WHEN?
WHAT?
WHERE?
WHAT?
WHERE?
When?
HOW?
WHEN?
What?
Where?
When?
WHERE?
ANY
WHERE?
QUESTIONS?
What?
When?
When?
Why?
WHEN?
When?
WHAT?
When?
Why?
HOW?
WHAT?
Where?
When?
What?
WHEN?
Why?
WHERE?
When?
HOW?
Why?