Blockchain Techniques in Finance:

-Focus on Cryptocurrencies-

Introduction to Blockchain & Cryptocurrencies

1

Blockchain Defined

A decentralized, immutable digital ledger. Ensures transparency and security through cryptographic hashing.

2

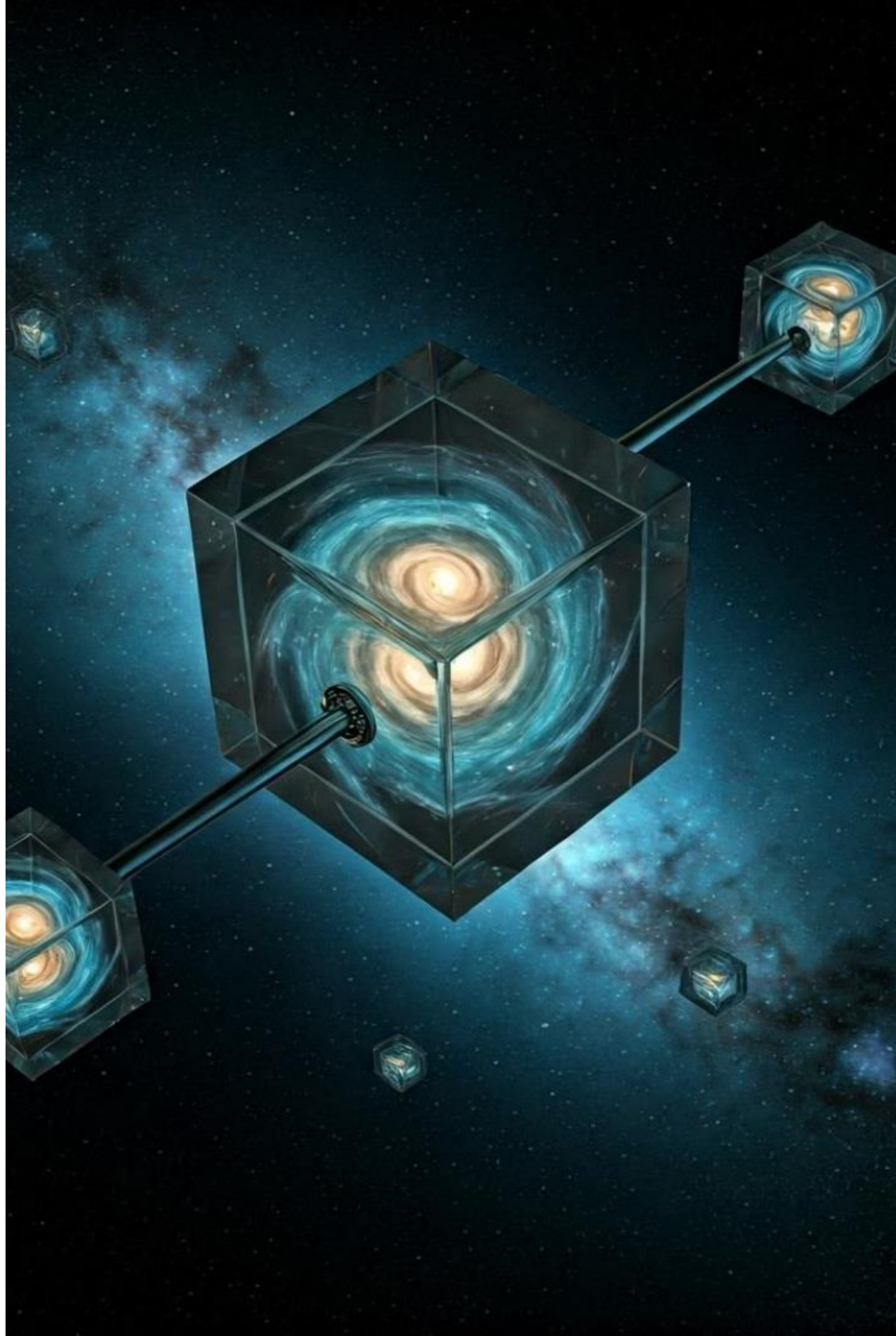
Cryptocurrency Foundation

Digital assets built on blockchain. Utilize cryptography for secure financial transactions and control creation.

3

FinTech Evolution

Crypto ecosystem growth. Disrupting traditional finance with decentralized solutions and innovative applications.



Blockchain development services are growing in demand all around, but especially in finance. This isn't surprising, considering the benefits they can deliver to financial institutions. Let's take a look at each of them.

Blockchain technology creates a distributed ledger that is shared across all participants in a network. Every transaction is recorded and visible to all stakeholders, which reduces the possibility of manipulation or fraud.

Blockchain uses cryptographic algorithms to secure transactions. Each transaction is linked to the one before it (via hashing)

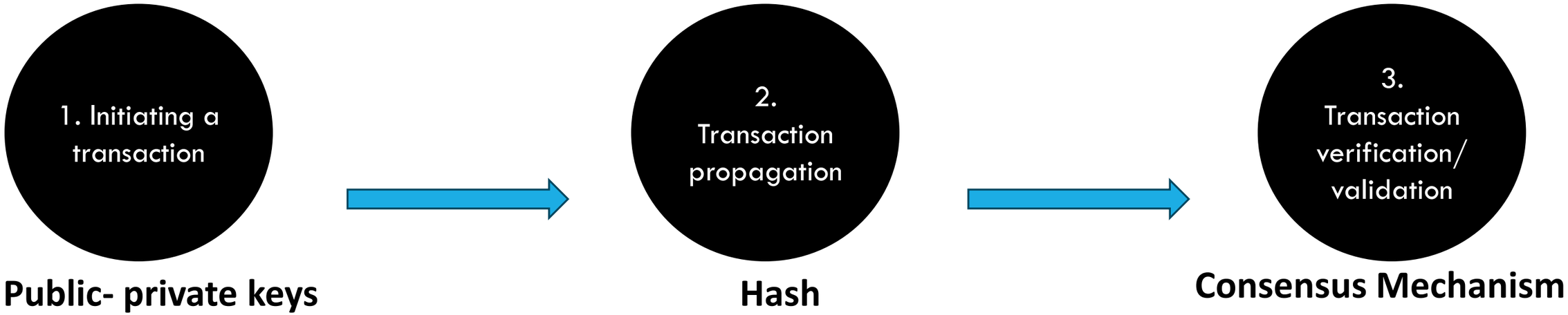
Blockchain eliminates the need for intermediaries, such as banks or brokers, by allowing participants to transact directly with each other which reduces transactions

Blockchain enables faster and more efficient processing by automating processes and reducing manual interventions.

The automation and immutability of blockchain reduce the likelihood of human errors and risks associated with manual processes.

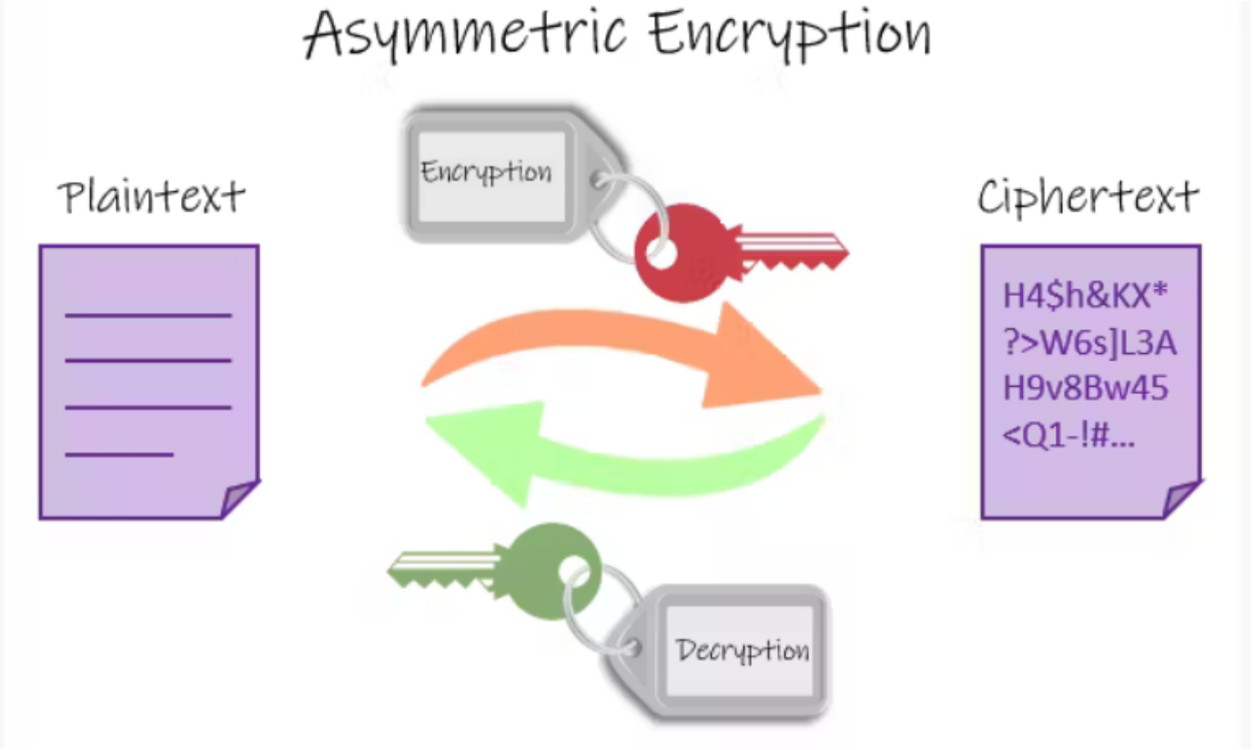
Key Blockchain Techniques in Cryptocurrencies (cryptography)

Definition of Cryptography
Cryptography is the process of developing a set of techniques and protocols to prevent any third party from gaining access to the data during a communication process. The word 'cryptography' is derived from two Greek terms, 'Kryptos' meaning 'hidden' and 'Graphein' meaning 'to write



1. What is public-key cryptography

This method consist of a pair of keys, an **encryption** key and a **decryption** key also named public and private key respectively. Hence, public key is used to encrypt a piece of information while a a private key is used to decrypt the information.

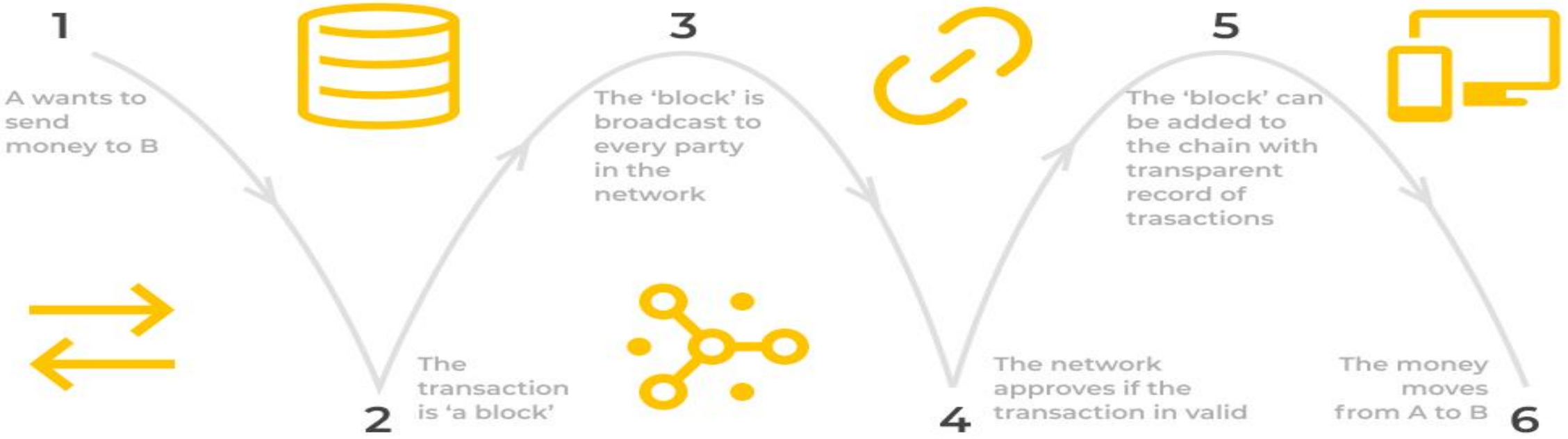


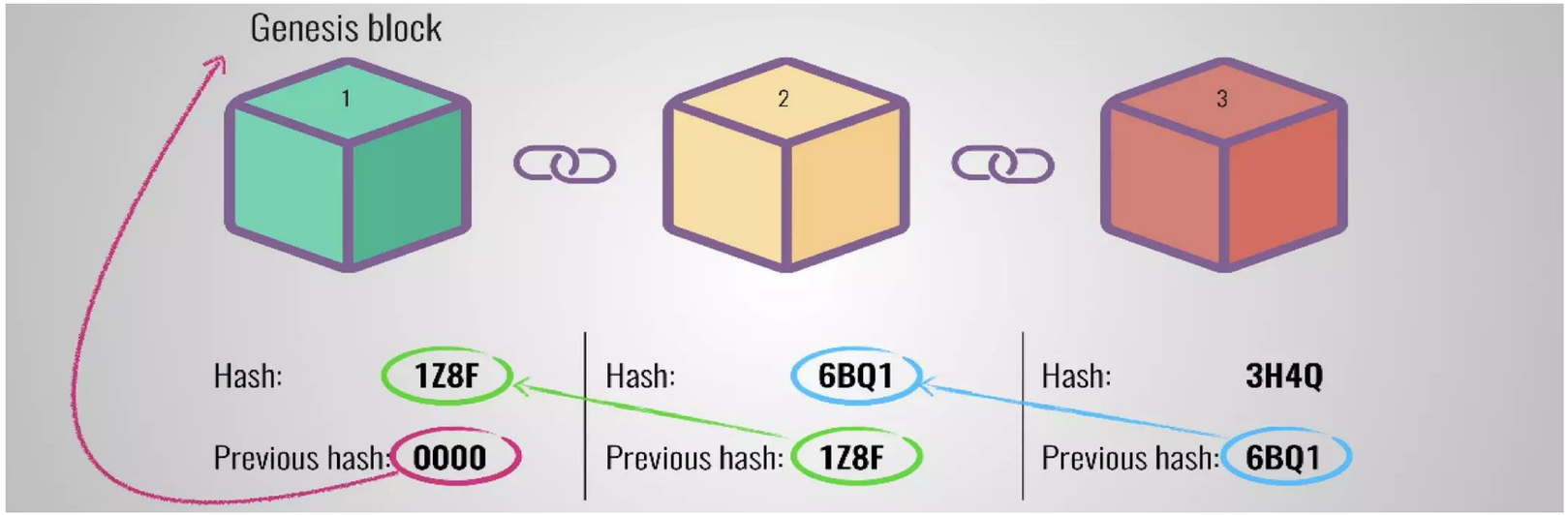
HASHING CRYPTOGRAPHY

2. Hash function - Hash functions generates a unique identifier for any set of inputs. Basically, it is a process that takes plain text data of any size and converts it into a unique ciphertext of a specific length. Hence, no two pieces of content will have the same hash digest, and in case if the content changes even slightly the hash digest changes as well.

Bitcoin uses **SHA-256**
Ethereum uses **Keccak-256**

HOW A BLOCKCHAIN WORKS





3. CONSENSUS MECHANIMS

Proof of Work (PoW): is a consensus mechanism used by blockchain networks (like Bitcoin) to validate transactions and secure the network.
In PoW, participants (miners) compete to solve complex mathematical puzzles, and the first one to solve it gets the right to add a new block to the blockchain and receive a reward.
This process requires significant computational power and energy, making it resource-intensive.

Proof of Stake (PoS): an alternative consensus mechanism where validators are selected to create new blocks based on the number of coins they hold and are willing to "stake" or lock up as collateral. Instead of solving puzzles, the validators are chosen randomly to validate transactions, making the process more energy-efficient compared to PoW.

	Proof-of-Work	Proof-of-Stake
Block creators	Miners	Validators
Resource required to win blocks	Energy	Coins or tokens
Cost of participation	Cost of equipment and the energy to run it	Cost of coins or tokens
Strength	Cost of equipment and energy provide robust security	Energy efficiency allows more scalability
Weakness	Enormous expenditure of energy	Network control can be purchased

THE USE OF BLOCKCHAIN IN FINANCE

Decentralized Finance (DeFi)
DeFi platforms enable peer-to-peer financial services—like lending, borrowing, and trading—without relying on traditional intermediaries like banks. This decentralized approach increases accessibility and transparency while reducing transaction costs

Cross-Border Transactions: Blockchain allows for faster, low-cost international transactions by eliminating intermediaries, enabling real-time fund transfers

Trade Finance Platforms: Blockchain streamlines trade processes by digitizing paper-based transactions and enhancing transparency, reducing delays and risks in global trade

Tokenization of Real Assets
Blockchain enables the digitization of real-world assets (like real estate or artwork) into tokens. These tokens represent ownership and can be traded easily, offering increased liquidity.

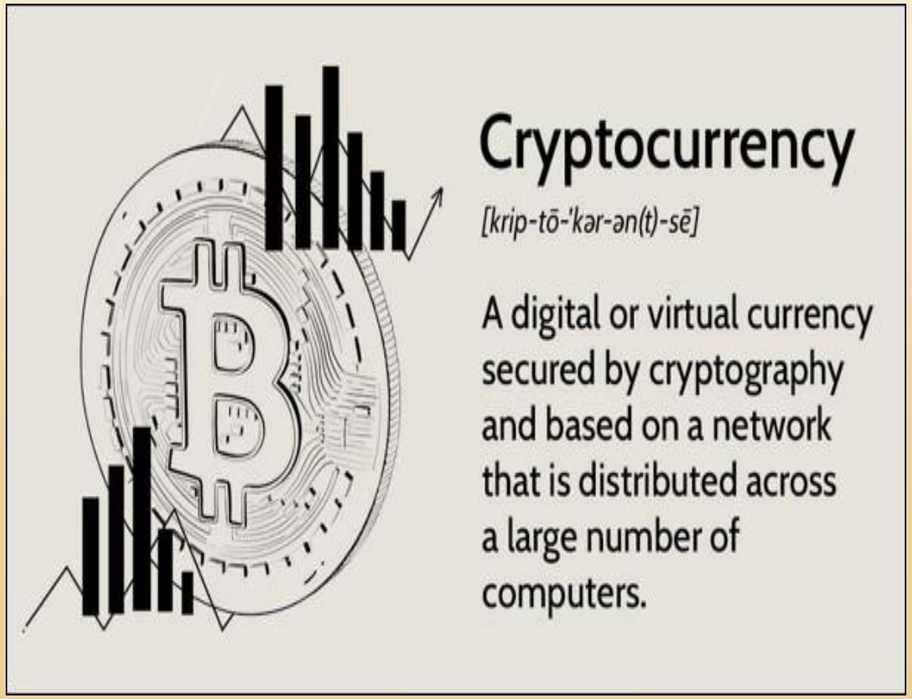
Smart Contracts and Automation
Smart contracts are self-executing agreements with terms directly written in code. These contracts automate transactions and reduce the need for intermediaries, enhancing the speed and security of financial operations like loan disbursement or insurance claims processing

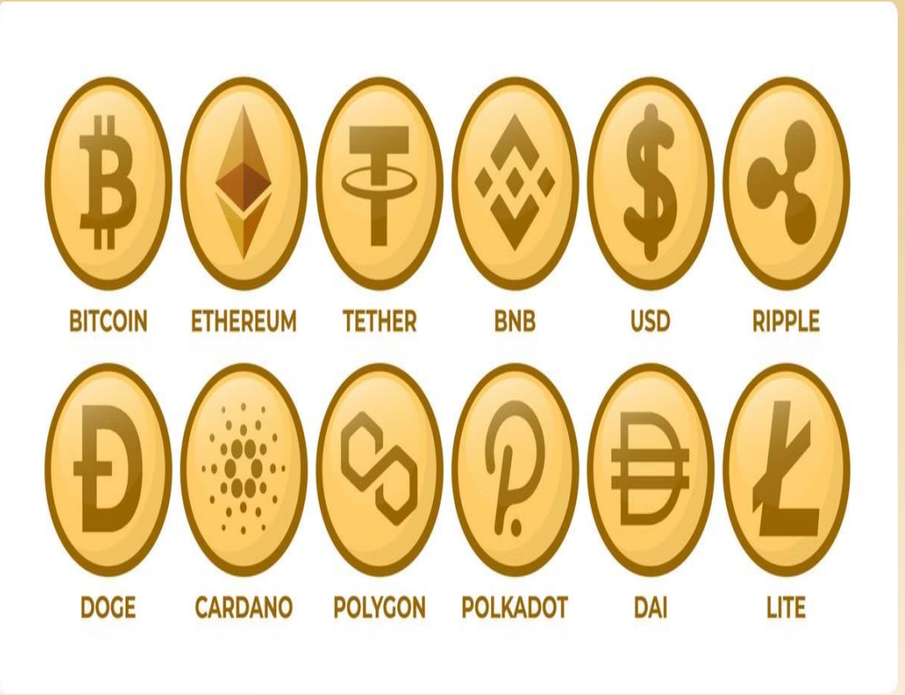
Cryptocurrencies

Bitcoin (2009) is a decentralized digital currency that operates on a peer-to-peer network, allowing users to send and receive payments without relying on intermediaries like banks or governments, Bitcoin is often considered both a store of value and a medium of exchange

Ethereum is a decentralized, open-source blockchain platform that allows developers to create and deploy **smart contracts** and decentralized applications (DApps). It was proposed by **Vitalik Buterin** in 2013 and officially launched on **July 30, 2015**. Ethereum's blockchain provides a flexible platform for creating programmable contracts and financial services through **Ether (ETH)**, its native cryptocurrency

Cryptocurrency	Primary Use Case	Key Feature
Bitcoin (BTC)	Store of Value	Limited Supply (21 million)
Ethereum (ETH)	Smart Contracts / dApps	Programmable Blockchain
Tether (USDT)	Stablecoin	Pegged to US Dollar





Cryptocurrency Wallets & Exchanges

Hot Wallets

Online storage for active trading. Convenient but more vulnerable to cyber attacks.

Cold Wallets

Offline storage for long-term holdings. Highly secure but less convenient for transactions.

Exchanges

Platforms for buying, selling, and trading cryptocurrencies. Vary in fees, security, and available assets.

Security Measures

Private keys, multi-factor authentication, and hardware security modules protect digital assets.

Risks and Challenges of Cryptocurrencies

1

Regulatory Uncertainty

Inconsistent global policies create compliance challenges. Legal status varies widely between jurisdictions.

2

Security Risks

Hacks and scams pose constant threats. Proper security measures are crucial for protection.

3

Volatility

Extreme price fluctuations impact value. Market sentiment and news can cause rapid changes.