

Cryptocurrency

By Dr Abdelhak Lefilef

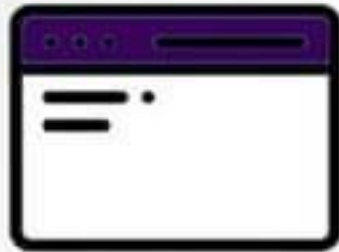




What is Cryptocurrencies?

- ▶ Cryptocurrencies are digital or virtual currencies underpinned by cryptographic systems. They enable secure online payments without the use of third-party intermediaries. "Crypto" refers to encryption algorithms and cryptographic techniques that safeguard these entries, such as elliptical curve encryption, public-private key pairs, and hashing functions.
- ▶ Blockchain technology is central to the appeal and functionality of cryptocurrencies.
- ▶ Cryptocurrency is digital money, like euros or United States dollars, but operates independently from governments and banks, using a decentralized technology (blockchain).

What Is Cryptocurrency?



Cryptocurrency is digital money created from code.



The cryptocurrency economy is monitored by a peer-to-peer internet protocol.



Cryptocurrency is an encrypted string of data or a hash, encoded to signify one unit of currency.

Examples of Cryptocurrency



Bitcoin



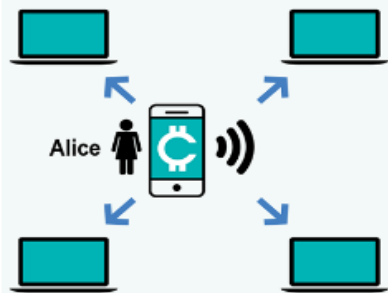
Ethereum



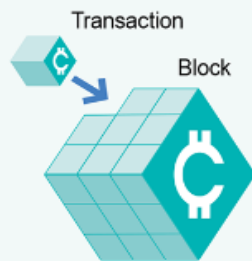
Ripple

How Does a Cryptocurrency Transaction Work?

1 Alice sends **instructions** to **transfer** cryptocurrency to Bob. **Anyone** using the **network** can view the message.



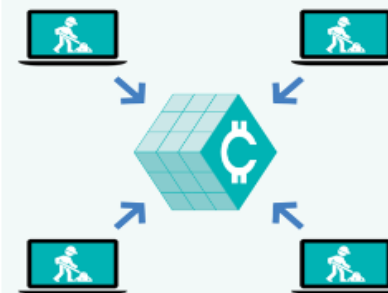
2 **Miners** group the transaction together into a **'block'** with other recently sent transactions.



3 Information from the new **block** is transformed into a **cryptographic code**.



4 Miners compete to find the **code** that will add the new block to the **blockchain**.



5 Once the code is **solved**, the block is added to the **blockchain** and the transaction is **confirmed**.



6 **Bob** receives the **cryptocurrency**.



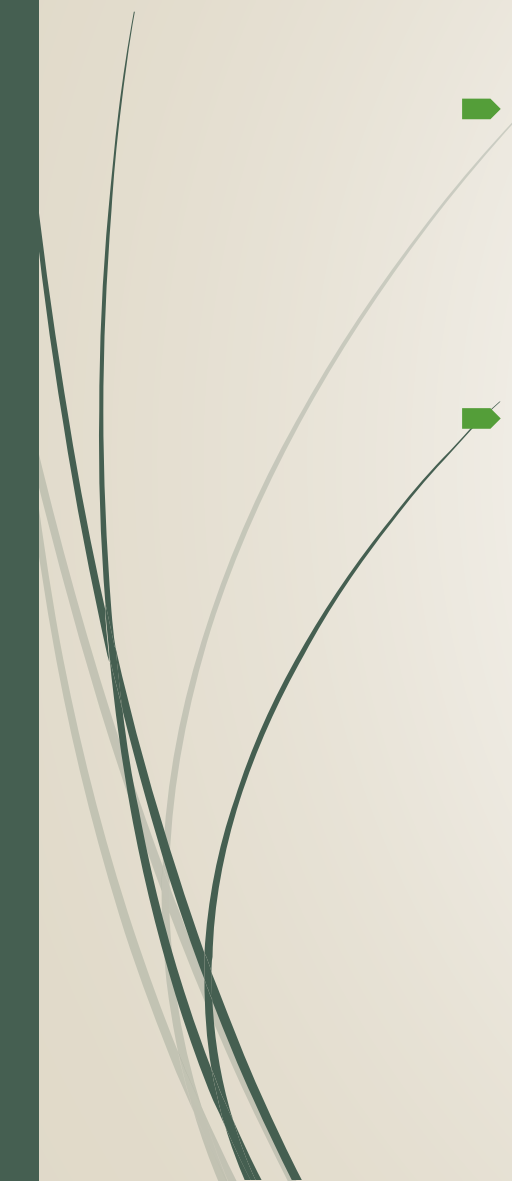


How Does Cryptocurrency Work?

- ▶ cryptocurrency uses cryptography for security purposes, but what does that mean? Cryptocurrencies use advanced mathematical algorithms to secure transactions and protect data from unauthorized access or manipulation. These algorithms serve two primary functions: maintaining user identity privacy and verifying transaction authenticity.
- ▶ Blockchain transactions are public, and addresses (public keys) are pseudonymous, though not wholly anonymous. In other words, while transactions are visible on the blockchain, the users behind them are not easily identifiable. Cryptocurrencies achieve this through cryptographic techniques such as hash functions and digital signatures.



How Does Cryptocurrency Work?

- ▶ Cryptocurrency achieves autonomy through a distributed network of computers collectively known as a blockchain. A blockchain is essentially a decentralized digital ledger that stores transaction data across many specialized computers on the network.
 - ▶ Each of these computers—also called nodes—maintains a copy of the ledger, and a consensus algorithm preserves the blockchain by rejecting fake or inconsistent copies. This distributed architecture increases the network's security because there is no single point of failure, such as a bank vault, for malicious actors to exploit.
- 



How Does Cryptocurrency Work?

- ▶ Cryptocurrencies allow individuals to transfer funds directly to one another. In a typical cryptocurrency transaction, the sender initiates the transfer by creating a digital signature using their private key. The transaction is then sent to the network, where nodes validate it by verifying the digital signature and ensuring the sender has sufficient funds.
- ▶ Once verified, the transaction is added to a new block, which is then added to the existing blockchain. While this may sound complicated, miners take care of these steps so the user doesn't have to worry about them.

Type of crypto



Bitcoin



Altcoins



Stablecoins



Privacy coins



Security tokens



Governance tokens



Memecoins



DeFi tokens



NFT tokens



AI tokens



Gaming tokens



➤ **Bitcoin:**

Founded in 2009, Bitcoin was the first cryptocurrency and is still the most commonly traded. The currency was developed by Satoshi Nakamoto, who is widely believed to be a pseudonym for an individual or group whose precise identity remains unknown.

➤ **Altcoins**

Any cryptocurrency other than Bitcoin, including Ether and Litecoin, is called an altcoin. These alternative coins offer various improvements or different features compared to Bitcoin, ranging from faster transaction times to low transaction fees. **Ethereum:** Developed in 2015, Ethereum is a blockchain platform with its own cryptocurrency, called Ether (ETH) or Ethereum. It is the most popular cryptocurrency after Bitcoin.

Difference between Bitcoin and Ethereum

Features	Ethereum 	Bitcoin 
Inception Year	2015	2009
Founder/Creator	Vitalik Buterin	Satoshi Nakamoto
Primary Use Case	Smart Contracts, DApps, DeFi, NFTs	Store of Value, Peer-to-Peer Transactions
Blockchain Technology	Smart Contracts, Ethereum Virtual Machine (EVM)	Transaction-Based, UTXO Model
Consensus Mechanism	Transitioned from PoW to PoS (Ethereum 2.0)	PoW (Proof of Work)
Maximum Supply	No fixed limit (dynamic Issuance)	21 million BTC
Transaction Speed	Variable up to 15 transitions per seconds.	10 minutes per block (approximate)
Scalability	Layer-two (L2s) scaling like zk rollups, optimistic rollups and state channels; sidechains	Lightning Network, sidechains
Developer Community	Active, focused on DApps, DeFi, and EIPs	Active, with contributions using BIPs
Security Features	Smart contract vulnerabilities, ongoing improvements	Robust security and immutability
Legal Status	Varies by jurisdiction, regulatory challenges	Varies by jurisdiction, regulatory challenges
Historical Performance	Impressive growth with volatility	Pioneering with significant growth and volatility
Real-world Applications	DeFi, NFTs, supply chain, identity verification	Cross-border remittances, hedge against inflation



➤ **Stablecoins**

Stablecoins are cryptocurrencies pegged to stable assets like fiat currencies or commodities to minimize price volatility. They are commonly used for trading or remittances. Examples of stablecoins include Tether, USD Coin, and Dai.

➤ **Privacy coins**

Users who respect privacy are drawn to privacy coins like Monero and Zcash, which aim to hide transaction details, including who sent or received the money.

➤ **Token**

A token is a digital unit of value or utility that exists on a particular blockchain. Tokens represent assets or functionalities and are often built on top of existing blockchain platforms like Ethereum, Binance Smart Chain, or Solana.



Token

- In general, a crypto token is another way to say “cryptocurrency,” “digital asset,” or “crypto asset.” More specifically, a crypto token is an asset that represents ownership or value in a decentralized system.
- They are created on blockchain platforms and are used for various purposes, such as granting access to specific goods or services, representing shares in a project, or as an incentive for users to participate in a particular ecosystem.

Tokens

- All coins may be considered tokens, but not all tokens are considered coins.
- Coins have their own blockchains, whereas tokens are built on an existing blockchain.



What is a token?

- ▶ People new to crypto may find it unclear to understand what a token is. This is because the word has roughly three overlapping meanings.
- ▶ In a technical sense, a token is an asset that represents ownership or value in a decentralized system. In this sense, it's no different from "cryptocurrency," "digital asset," or "crypto asset."
- ▶ A token can mean any crypto asset other than Bitcoin and, to a lesser extent, Ethereum. It has a similar meaning to "altcoin" (alternative coin).
- ▶ Perhaps the most commonly used meaning of token within the crypto industry is as a crypto asset that is a non-native blockchain token. For example, ETH is the native token of the Ethereum blockchain. Any other crypto assets that exist on the Ethereum blockchain are tokens

What is the difference between cryptocurrency and token?

Coins

- Built into a blockchain (native to its own blockchain technology)
- Requires significant resources and skills to create
- Mostly distributed through mining
- Used to store or transfer money
- Valid with any merchant who uses the currency

VS.

Tokens

- Built on top of an existing blockchain
- Relatively easy to create
- Mostly distributed through ICOs (Initial Coin Offerings)
- Valid with one merchant
- Variety of uses (e.g., security, asset representation)



Is Bitcoin a token?

- ▶ Yes and no!!!!.
- ▶ Technically, a bitcoin (1 BTC) is a token—a digital asset that represents ownership of value in a decentralized system. However, within the crypto industry, tokens often refer to any crypto asset besides Bitcoin and, to a lesser extent, Ethereum. Tokens also usually have uses aside from money-like properties.



Types of tokens

- The additional functionality of tokens is limited only by the imagination. So far, tokens can be classified into several broad categories of use. As crypto evolves, it's safe to say that there will be innovative uses no one has considered. Here are some common uses of tokens currently:
- Utility Tokens
- Security Tokens
- Stablecoins
- Governance tokens
- Non-Fungible Tokens (NFTs)



Utility Tokens

- These tokens provide access to products or services within a specific blockchain platform or decentralized application (DApp).
- For example, users may need to acquire utility tokens to access storage space on a decentralized cloud storage platform or to participate in decentralized finance (DeFi) services.




Security Tokens

- These represent ownership in an underlying asset, such as shares in a company, real estate, or other forms of investments.
- Security tokens are subject to regulatory requirements and can give investors rights to dividends, voting, or profit-sharing.




Stablecoins

- Stablecoins are tokens pegged to the value of a fiat currency, most often the US dollar.
 - They are built to allow users to trade and invest in cryptocurrency without the price volatility associated with many other coins and tokens.
 - Some famous examples of stablecoins include USDT, USDC, and DAI.
- 




Governance tokens

- Governance tokens allow holders to participate in decision-making processes for a particular project or platform. They can propose, discuss, and vote on various aspects of the project, such as protocol upgrades or changes to the platform's fee structure.
- 



Non-Fungible Tokens

- Non-Fungible Tokens (NFTs): Unlike other tokens, NFTs are unique and indivisible.
 - Each NFT represents a unique digital asset, such as artwork, collectibles, or virtual real estate.
 - NFTs have gained popularity due to their ability to provide proof of ownership and provenance for digital assets.
- 

Initial Coin Offering (ICO); What is an ICO?

- An Initial Coin Offering (or ICO) is a method for teams to raise funds for a project in the cryptocurrency space. In an ICO, teams generate blockchain-based tokens to sell to early supporters. This serves as a crowdfunding phase – users receive tokens that they can use (either immediately or in the future), and the project receives money to fund development.
- The practice was popularized in 2014 when it was used to fund the development of Ethereum. Since then, hundreds of ventures have adopted it, with varying degrees of success (particularly during the 2017 boom).



ICO VS IPO

- While the name sounds similar to an Initial Public Offering (IPO), the two are fundamentally very different methods of acquiring funding.
- IPOs usually apply to established businesses that sell partial ownership shares in their company to raise funds.
- In contrast, ICOs are a fundraising mechanism that allows companies to raise funds for their projects in very early stages.
- When ICO investors purchase tokens, they do not buy any ownership in the company.



How does an ICO work?

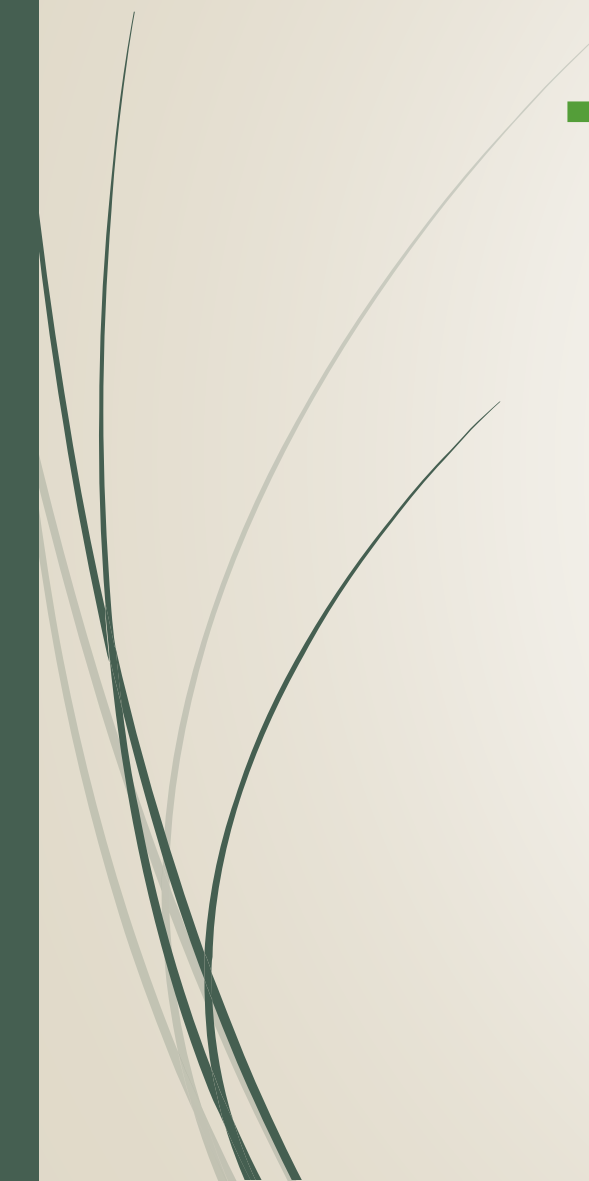
- An ICO can take many forms. Sometimes, the team hosting it will have a functional blockchain that they'll continue to develop in the coming months and years. In this case, users can buy tokens sent to their addresses on the chain.
- Alternatively, the blockchain might not have launched so that the tokens will be issued on an established one (such as Ethereum). Once the new chain is live, holders can swap their tokens for fresh ones issued on top of it.
- The most common practice, however, is to issue tokens on a smart-contract-capable chain. Again, this is done predominantly on Ethereum; many applications use the ERC-20 token standard. Though not all originate from ICOs, it's estimated that there are upwards of 200,000 different Ethereum tokens today.


The role of crypto and digital assets in financial institution

- Here are key points explaining the role of crypto and digital assets in financial institutions:
- **1. Diversification of Investment Portfolios**
- **2. Innovation in Payments and Settlements**
- **3. Access to New Revenue Streams**
- **4. Decentralized Finance (DeFi) Integration**
- **5. Improved Transparency and Security**
- **6. Regulatory Challenges and Compliance**
- **7. Expansion of Financial Inclusion**
- **8. Hedge Against Inflation and Economic Instability**
- **9. Tokenization of Traditional Assets**



Diversification of Investment Portfolios

- ▶ Crypto and digital assets provide financial institutions with a new asset class that offers unique risk-return characteristics. Unlike conventional investments like stocks, bonds, or commodities, cryptocurrencies frequently behave independently and are subject to market dynamics unrelated to more significant financial markets. By incorporating digital assets into their portfolios, financial institutions can reduce overall risk through diversification. This is particularly attractive in financial market volatility, where crypto assets may serve as a hedge or alternative investment, enhancing institutional resilience and expanding investment opportunities within the financial sector.
- 



Innovation in Payment Systems and Settlements

- ▶ Cryptocurrencies and blockchain technology have revolutionized payment systems by enabling faster, more efficient, and cheaper transactions—especially in cross-border payments. Traditional financial systems often rely on multiple intermediaries, increasing costs and time delays. Digital assets such as stablecoins and cryptocurrencies enable real-time, low-cost settlements, bypassing the need for intermediaries. This not only enhances the operational efficiency of financial institutions but also reshapes the broader financial sector by setting new standards for international payments, remittances, and financial services infrastructure.



Creation of New Revenue Streams

- ▶ Financial institutions are generating new revenue opportunities by offering services related to crypto and digital assets. These include crypto trading platforms, custodial services for securely storing digital assets, and investment products like crypto-based ETFs (exchange-traded funds). As the demand for digital assets grows among retail and institutional investors, financial institutions are expanding their product offerings to capture market share, supporting profitability. This integration also stimulates competition and innovation in the financial sector as banks, asset managers, and fintech companies explore ways to capitalize on the booming digital asset market.



Decentralized Finance (DeFi) and Its Disruption of Traditional Models

- ▶ Decentralized Finance (DeFi) is an emerging sector built on blockchain technology that offers financial services without traditional intermediaries such as banks or brokers. Through DeFi platforms, users can lend, borrow, trade, and earn interest on their digital assets. Financial institutions are now exploring ways to participate in or integrate with DeFi protocols to access decentralized liquidity and offer innovative financial products. This is leading to a transformation in the financial sector as decentralized solutions challenge traditional banking models, increase transparency, and reduce costs associated with financial intermediation.




Enhanced Security and Transparency through Blockchain Technology

- ▶ Blockchain, the underlying technology for most cryptocurrencies, provides a transparent, secure, and immutable record of transactions. Financial institutions can leverage blockchain to enhance security, reduce fraud, and ensure the integrity of transaction records. This heightened level of transparency is precious in meeting compliance and regulatory requirements. By adopting blockchain solutions, institutions in the financial sector can improve auditability and reporting processes while building greater trust with clients. This integration strengthens the overall security framework within the financial ecosystem.





Regulatory Compliance and Challenges

- ▶ The rise of digital assets brings significant regulatory challenges. Financial institutions must navigate complex and evolving regulations related to anti-money laundering (AML), know-your-customer (KYC), and consumer protection. As regulators worldwide work to establish more precise guidelines for crypto assets, financial institutions play a crucial role in shaping compliance frameworks within the sector. Meeting these regulatory standards is essential for integrating digital assets into mainstream finance, ensuring the stability and legitimacy of the broader financial market. The success of crypto adoption in financial institutions will largely depend on establishing a regulatory framework that balances innovation with financial stability and consumer protection.
- 



Expanding Financial Inclusion

- ▶ Cryptocurrencies and digital assets have the potential to increase financial inclusion by providing access to banking services for underbanked and unbanked populations. Through digital wallets and decentralized networks, financial institutions can offer low-cost financial services in regions with limited traditional banking infrastructure. This expands the customer base for financial institutions and enhances global financial inclusion. Moreover, digital assets enable micropayments and peer-to-peer transactions, often impractical using traditional banking systems. By promoting inclusion, the financial sector can tap into new markets, fostering growth and development on a global scale.
- 



Hedge Against Economic Instability and Inflation

- ▶ In countries experiencing economic instability or high inflation, digital assets like Bitcoin are increasingly seen as an alternative store of value. Financial institutions can provide their clients access to crypto assets as part of a broader portfolio management strategy to mitigate the risks associated with inflation and currency devaluation. This role as an inflation hedge connects crypto to the broader financial sector, where traditional assets may be losing value. Financial institutions enhance their service offerings by offering alternative investments and providing more comprehensive risk management solutions.



Tokenization of Traditional Assets

- ▶ Tokenization refers to converting physical or traditional financial assets, such as real estate, equities, or commodities, into digital tokens on a blockchain. Financial institutions are beginning to use tokenization to fractionalize ownership of these assets, making them more accessible and tradable. Tokenization increases liquidity, enables 24/7 trading, and democratizes access to previously illiquid markets. This development represents a significant shift in how assets are managed and traded within the financial sector, providing more flexibility and accessibility for investors while creating new products for financial institutions.
- 