Blockchain Wallets and Tokens

Chapter – 5

Fall 2025

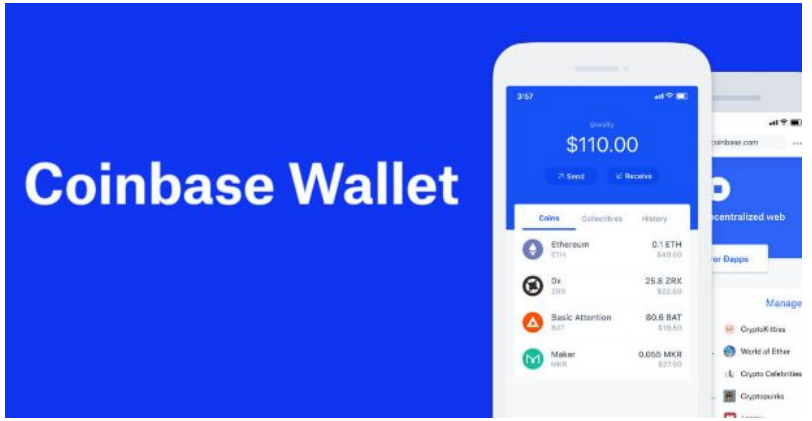
Middle Tennessee State University

Part A – Blockchain Wallets

Blockchain Wallet

EXODUS

METAMASK



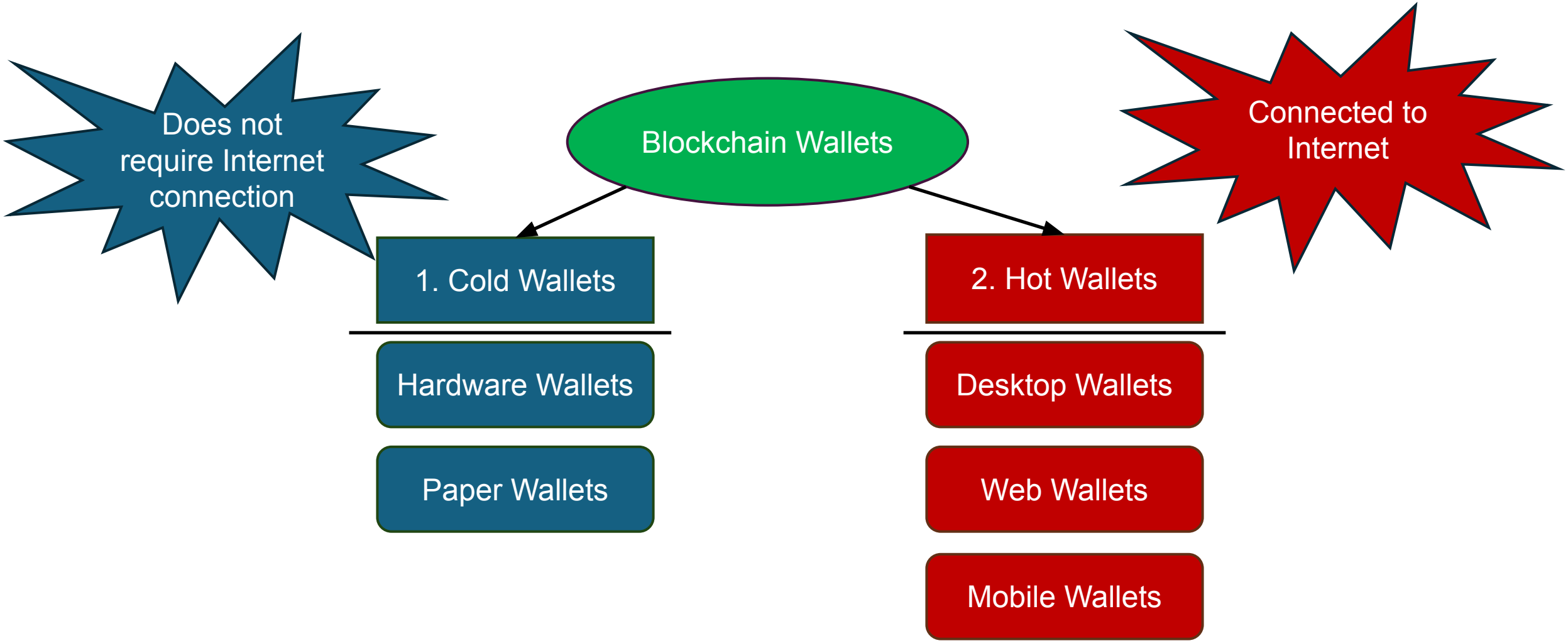
- Tool that enables users to store, manage, and interact with cryptocurrencies on blockchain networks

- Serve as a bridge between users and the blockchain

Blockchain Wallet – Contd...

- **Purpose of Blockchain Wallet:**
  - Securely store their cryptocurrency holdings
    - *For e.g.,: Users can securely store Ether (ETH) and other tokens in their MetaMask wallet, protected by their private key*
  - Send and receive cryptocurrencies to and from other users
    - *For e.g.,: Users can send ETH or tokens to other MetaMask users by entering their wallet addresses*
  - Interact with decentralized applications (DApps) and smart contracts
    - *For e.g.,: MetaMask allows users to access and use Ethereum-based DApps and interact with smart contracts for various purposes*
- Examples: Metamask, Exodus, Ledger Nano S, etc.

Types of Blockchain Wallets



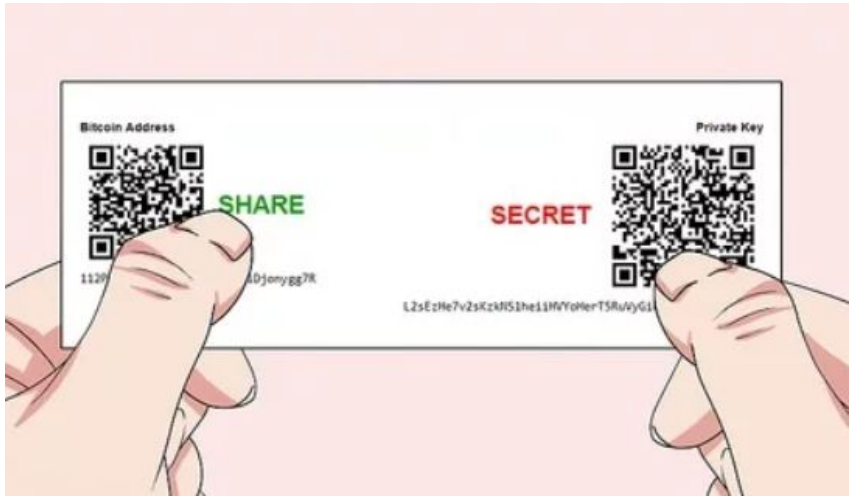
Cold Wallets

- Also known as Cold Storage
- Stored **offline**
- No internet connection required
- Mostly used for long term holdings
- **Strength**:
  - Maximum Security
  - Protection from Online Threats
  - Long-term Storage
- **Weakness**:
  - Inconvenience for daily use
  - Physical possession required

Cold Wallets – Contd...

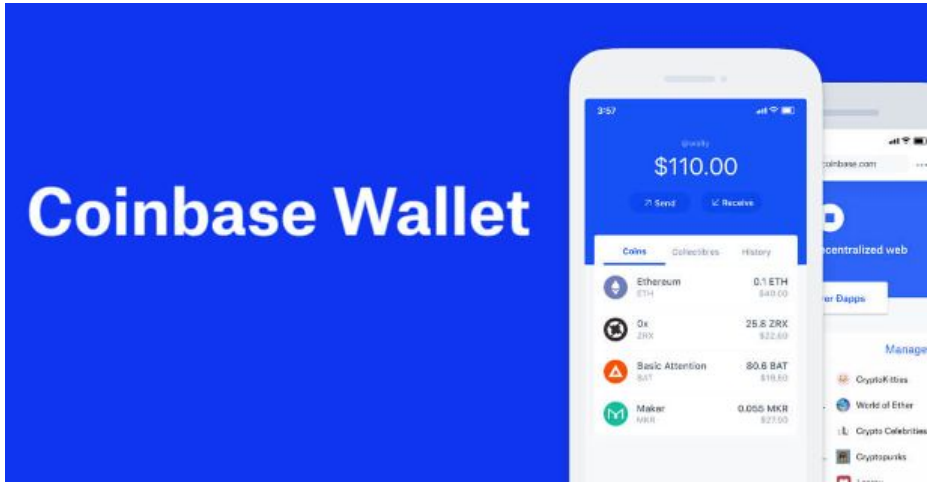
1. **Hardware Wallets**
   - Hardware devices that handles public addresses and cryptographic keys
   - Appears like USB with an OLED screen and side buttons
   - Can be connected to PC and can be accessed by native desktop apps

2. **Paper Wallets**
   - Physically printed QR coded form wallet
   - Can be generated using paper wallet generator like bitaddress.org
   - Once the key pair is generated, you have the **option to print it**
   - Should be stored in secured and dry location
   - Less popular after the invention of hardware wallets



Hot Wallets

- Cryptocurrency wallets that are **connected to the internet**
- Suitable for daily transactions, trading, and interacting with decentralized applications
- **Strength**:
  - Convenience
  - Real-time access
  - Integrated exchange services
  - Increased participation in **Decentralized Exchanges (DEXs)** and **Decentralized Finance (DeFi)**
- **Weakness**:
  - Security Risks (susceptible to hacking, phishing, malware attacks, etc.)
  - Limited Long-Term Security
  - Balancing Security and Convenience

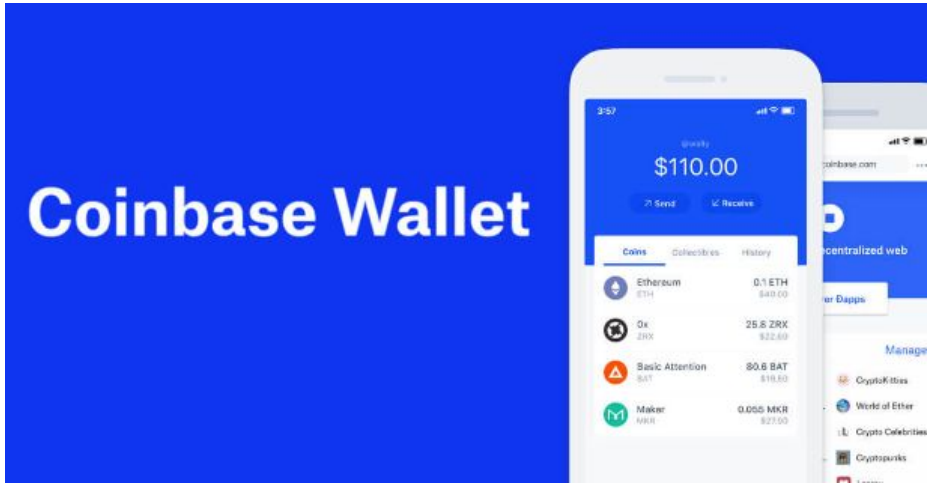


EXODUS

METAMASK

Hot Wallets – Contd...

1. **Desktop Wallets**
   - Installable software packs available for operating systems
   - Applications for cryptocurrency management on devices
   - Convenient for daily transactions
   - User-friendly interfaces
   - E.g., Exodus, Atomic Wallet, etc.
2. **Web Wallets**
   - Online services accessible through web browsers
   - Accessible from any device with an internet connection
   - Susceptible to phishing attacks
   - E.g., MetaMask, MyCrypto, Binance Web Wallet, etc.
3. **Mobile Wallets**
   - Just like desktop wallets made for smartphones
   - Highly portable, allowing transactions on the go
   - E.g., Coinbase, Coinomi, Mycelium, etc.



EXODUS

METAMASK

Part B – Tokenization in Blockchain

Tokenization in Blockchain

- **Tokenization** -> Process of converting real-world assets into digital tokens
- **Token** -> digital representation of an asset, right, or unit of value
- Tokens exist as digital assets or smart contracts in blockchain
- E.g., cryptocurrencies, utility tokens, security tokens, non-fungible tokens, governance tokens, stable coins, etc. can be different forms of tokens
- **E.g. of Tokenization:**
  - Real Estate: Tokenizing a property to allow fractional ownership and trading
  - Art and Collectibles: NFTs represent ownership of digital and physical art
- **Strength of Tokenization:**
  - Liquidity: Tokens can be traded easily on exchanges.
  - Fractional Ownership: High-value assets become accessible to a wider audience (***depending upon the type of token***)
- **Weaknesses of Tokenization:**
  - Regulatory Challenges: Compliance with varying regulations can be complex
  - Security: Tokens are susceptible to scams and fraud

Use Cases of Tokens

- **Cryptocurrencies**
  - Digital currencies such as Ethereum, Bitcoin, etc.
- **Utility Tokens**
  - purchase specific services or products within a particular blockchain application or platform
  - E.g., the Binance Coin (BNB) is used to pay for fees on the Binance exchange
- **Security Tokens**
  - represent ownership in an asset, company, or fund
  - used for various forms of investments, like real estate, stocks, and venture capital
- **Non-Fungible Tokens (NFTs)**
  - unique tokens that represent ownership of a specific item, piece of content, or digital asset
  - gained popularity in art, collectibles, and gaming
- **Governance Tokens**
  - grant holders voting rights or decision-making power within a decentralized organization or platform

An Example: Real Estate: Tokenizing a Property

- Tokenizing a property means representing ownership and the value of a real estate asset as digital tokens on a blockchain

- Fractional Ownership:
  - Division into numerous digital tokens
  - For instance, a high-value property can be divided into thousands or even millions of tokens, allowing multiple investors to own a share
- Trading:
  - Can be bought and sold on blockchain-based platforms
  - Provides liquidity to real estate assets that are traditionally illiquid
  - Investors can easily buy or sell their share of a property at any time, rather than waiting for a property sale
- Ownership Rights:
  - Token holders have ownership rights to the real estate asset in proportion to the number of tokens they hold
  - These rights may include a share of rental income, voting rights on property management decisions, or a percentage of any profits when the property is sold
- E.g.,:
  - A luxury apartment building valued at $10 million
  - Divided in one million tokens, each representing a $10 ownership share
  - Own 100,000 tokens, have a 10% ownership stake in the property
  - Receive 10% of rental income, have a say in property management decisions, and can sell their tokens at any time

Benefits of Tokenization

- **Liquidity Enhancement**
  - increases the liquidity of traditionally illiquid assets like real estate, art, and collectibles
  - allows investors to buy and sell their holdings more easily
  - especially noticeable in the real estate market
- **Fractional Ownership**
  - enables fractional ownership
  - making high-value assets accessible to a broader range of investors
- **Accessibility and Inclusivity**
  - lowers the barrier to entry for various asset classes
  - a wider range of investors, including those with limited capital, to participate in investments
  - diversification of investment portfolios
- **Transparency**
  - transparency reduces the potential for fraudulent activities
- **Cost Efficiency**
  - Reduction of administrative costs due to the automation through smart contracts
  - Elimination of intermediaries, paperwork, and administrative overhead
- **24/7 Trading**
  - assets can be traded around the clock, seven days a week, on global exchanges and platforms
  - greater flexibility and responsiveness

Different types of Token Standards

What is a Token Standard?

- Set of rules and specifications
- defines how a specific type of digital token should be created, managed, and function within a blockchain ecosystem
- provides a common framework for developers to create tokens with consistent behavior
- Token standards serve several essential purposes:
  - **Interoperability**
    - different blockchain applications
    - exchanged on various decentralized exchanges
    - stored in compatible cryptocurrency wallets
    - across the blockchain ecosystem without compatibility issues
  - **Uniformity**
    - uniform structure
    - easier for developers to understand
    - provides a consistent user experience
  - **Security**
    - thoroughly reviewed, tested, and audited
    - reducing the risk of vulnerabilities and security issues
  - **Ecosystem Growth**
    - development of a broader ecosystem
    - creation of decentralized applications, marketplaces, and services

What is ERC (Ethereum Request for Comments) Token?

What is **Request for Comments** (**RFC**)?

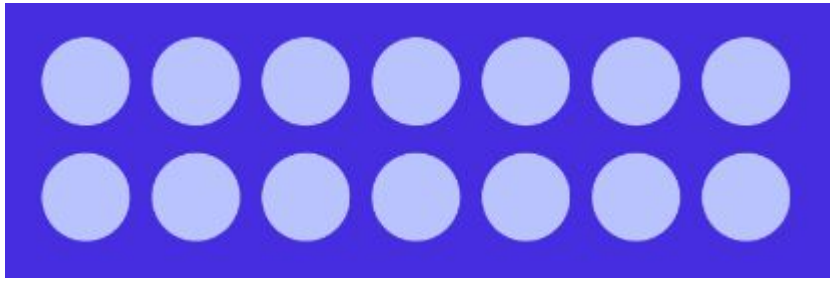
- Documents that contain technical specifications and organizational notes for the **Internet and Computer Networks**
- Produced by *Internet Engineering Task Force (IETF)*
- Topics related to routing, addressing, transport, security, and other protocols
- E.g., HTTP, TCP/IP, DNS, TLS, SSL, SMTP, etc.
- Facilitates proposals, open discussion, collaboration, and peer review of proposed standards and protocols

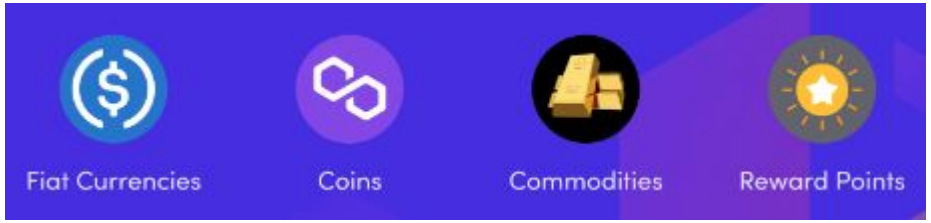
What is **Ethereum Request for Comments** (**ERC**)?

- Ethereum's version of RFC
- Document that programmers use to write smart contracts on **Ethereum Blockchain**
- Topics related to Ethereum-related proposals (such as token standards and smart contract interfaces)
- E.g., ERC-20, ERC-721, ERC-1155, etc.
- Establish standard rules and specifications for creating, managing, and interacting with digital assets and smart contracts on the Ethereum blockchain

ERC-20 Tokens

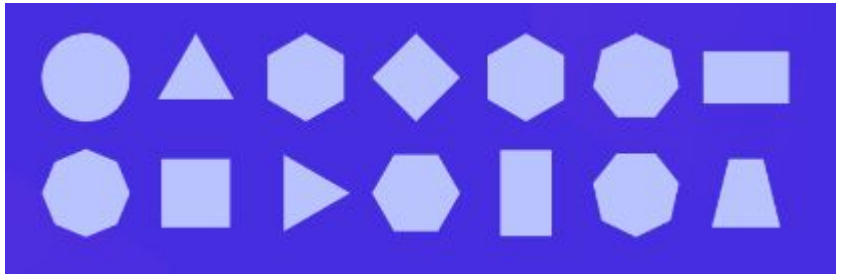
- Ethereum Request for Comment 20
- Most widely adopted token standard on Ethereum
- ERC-20 tokens are **fungible (interchangeable/tradeable)** and **divisible**
- Each token is **identical** and **interchangeable** with any other token of the same type
- *E.g., Comparison with the **Lego blocks***
- Use cases:
  - Fiat currencies (government-controlled money such as the U.S. dollar)
  - Commodities
  - Reward Points
  - Financial assets
- Also, often used to fundraise through **ICOs** (initial coin offerings)
- ICOs are similar to IPOs (Initial Public Offerings)
- **Strengths**:
  - Interoperability
  - Liquidity
- **Weakness**:
  - Not suitable for representing unique, non-fungible assets like art or real estate
- Example: DAI (a stablecoin), Chainlink (a utility token), and Tether (a stablecoin) are all based on the ERC-20 standard





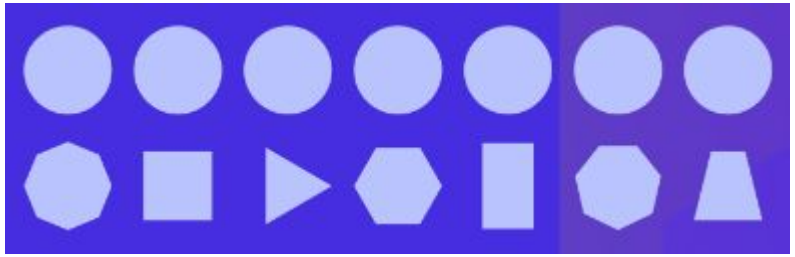
ERC-721 Tokens

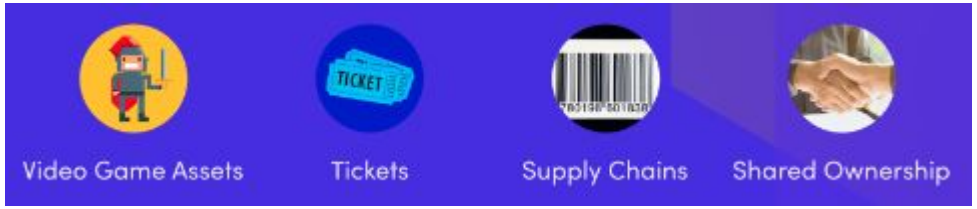
- Ethereum Request for Comment 721
- Commonly referred to as **NFTs** (Non-Fungible Tokens)
- Represents **one of a kind, unique, non-interchangeable, non-divisible asset**
- E.g., the Mona Lisa painting **cannot** be exchanged for a replica
- *E.g., Comparison with the **unique puzzle pieces***
- ERC-721 tokens represents **ownership** of **unique** digital and physical items
- Use cases:
  - Digital Art
  - Collectibles
  - Authenticity
  - Real Estate
- **Strength**:
  - Uniqueness, ensures digital ownership and scarcity
  - Ownership provenance and tracing
- **Weakness**:
  - not suitable for representing divisible or fungible assets like cryptocurrencies or shares
- Example: CryptoKitties (collectible cats), CryptoPunks (unique avatars), and NBA Top Shot (digital collectible basketball cards) are built on the ERC-721 standard



ERC-1155 Tokens

- Ethereum Request for Comment 1155
- **Multi-token** standard
- **Versatile** token standard that supports both **fungible** and **non-fungible** tokens within a single contract
- **Divisible** for fungible tokens and **non-divisible** for non-fungible tokens
- Use Cases:
  - Video Game Assets
  - Tickets
  - Supply Chains
  - Shared Ownership
- **Strength**:
  - Flexibility, *allows developers to create multiple types of tokens within a single smart contract*
  - Efficiency, *reduced gas costs*
- **Weakness**:
  - Complexity
  - Lack of standardization, unlike ERC-20 and ERC-721
- Example: Enjin Coin (ENJ) and associated gaming assets are often implemented using ERC-1155





Soulbound Tokens (SBT)

- The name ‘Soulbound’, coined from World of Warcraft game
- A kind of **non-fungible** token (non-interchangeable)
- NFTs are transferrable but SBTs are not
- Similar to ERC-721, but ***transfer*** function is banned
- After acquiring one, it is always in user’s personal wallet and identity
- **cannot** be bought, sold or given to another person
- non-transferable NFTs held by a **private crypto wallet** known as **Souls**
- E.g., certificates of competence, reputation, education, medical records, work history
- Use Cases:
  - Schools,
  - Recruiting companies,
  - Hospitals
  - Event organizers
  - Research organizations
- No formal Soulbound token specifications exist so far
- First time mentioned in whitepaper published by Vitalik Buterin in May 2022

End of Chapter-5