Module 7: Wallets, Faucets and Keccak-256

Crypto Faucet

- an online platform (usually a website or mobile app) that distributes tiny amounts of cryptocurrency for free.
- It is a drip of small fractions of digital coins to users who complete simple tasks.
- designed to be a low-risk way for people to get started with crypto.

Two Main Types of Faucets:

Mainnet:

- is the live, production version of a network (where real value is exchanged).
- A website or app that gives away tiny fractions of real digital assets (like Bitcoin or Solana)
- These tokens have market value and can be traded or spent.
- To introduce beginners to a new coin or to provide just enough "dust" to pay for a single transaction fee on a new network

Testnet:

- is a simulation used for practice and development.
- A service that provides "fake" tokens for use on a test network (e.g., Sepolia for Ethereum, Amoy for Polygon).
- developers and students pay for Gas Fees when deploying smart contracts or testing transactions without spending actual cash.
- Relatively large amounts (e.g., 0.1 to 0.5 ETH per day) because the coins are free to create.

Difference between Mainnet and Testnet:

Feature	Mainnet Faucets	Testnet Faucets
Token Value	Real. Can be sold or traded for cash.	Zero. Only for practice/development.
Payout Size	Extremely tiny (e.g., $0.01 worth of BTC).	Large enough to test a system.
Primary Goal	Marketing and onboarding new users.	Helping developers test smart contracts.
Withdrawal	High minimum threshold (takes a long time).	Usually instant but capped per 24 hours.

Comparison of Mainnet and Testnet

Feature	Mainnet Faucet	Testnet Faucet
Monetary Value	Yes (Real Money)	No (Play Money)
Risk level	High (Irreversible real loss)	Low (Safe to make mistakes)
Best For	Onboarding & Marketing	Testing & Learning
Example Network	Ethereum Mainnet, Bitcoin	Sepolia, Holesky, Amoy
Difficulty to Get	Hard (Lots of ads/tasks)	Easier (Verification/Social login)

Testnet Faucets (For Learning & Development)

Network	Faucet Provider	Daily Drip Amount	Requirements
Ethereum (Sepolia)	Google Cloud Faucet	0.05 ETH	Google Account
Ethereum (Sepolia)	Alchemy Faucet	0.1 ETH	Alchemy Account
Solana (Devnet)	Solana Official Faucet	1.0 SOL	Wallet Address
Polygon (Amoy)	Polygon Faucet	0.5 MATIC	Discord/Social Login
Multi-Chain	QuickNode Faucet	Varies	Wallet Connection

Best Mainnet Faucets (For Real Crypto)

- FreeBitco.in, is one of the oldest and most trusted Bitcoin faucets. You can "roll" for free BTC every hour.
- Cointiply, a multi-task faucet where you earn by watching videos, playing games, or taking surveys. It pays out in BTC, LTC, and DOGE.
- Fire Faucet, is the popular for its Auto-Faucet, you claim multiple different coins automatically once you earn Activity Points.
- RollerCoin, ia a Game-Based faucet. You play 8-bit style mini-games to simulate mining power and earn real Bitcoin, Ethereum, and Dogecoin.
- FaucetPay, is a micro-wallet that connects to hundreds of other small faucets, making it a central hub to collect tiny rewards

Rules to protect your wallet:

1. A legitimate faucet will only ever ask for your public address (starts with 0x... or similar).
2. It is a scam if a site asks for your 12 or 24 words to "verify" your wallet.
3. Some high-end faucets (like Alchemy) require your wallet to have a tiny amount of real crypto (e.g., 0.001 ETH) to prove you are a real person and not a robot script.
4. Real faucets give you fractions of a cent and not 1 full Bitcoin ($100,000+) for clicking an ad.

Other Browser Wallets:

1. Rabby Wallet, is often preferred by power users and developers over MetaMask because it is designed specifically for DeFi and dApp interaction.

Advantage:

- It automatically switches networks based on the dApp you are using
- It has a pre-transaction simulation for security protection that shows you exactly what your smart contract will do (and if it will fail) before you spend any gas.

2. Coinbase Wallet, is a browser Extension and is a very stable alternative that works seamlessly with the "Injected Provider" option.

Advantage:

- It has excellent integration with Base and other EVM chains.
- It's a great choice if you want a cleaner, more modern user interface than MetaMask.

3. Brave Wallet, is a Native Browser Wallet but don't even need an extension. Brave has a wallet built directly into the browser's core code.

Advantage:

- it is often faster and less prone to extension lag or crashes.

4. OKX Web3 Wallet, developed one of the most powerful multi-chain wallets.

Advantage:

- If you are testing smart contracts that might eventually bridge to other ecosystems, OKX provides a very robust testing environment.

5. Phantom (Multi-Chain Mode), Originally a Solana-only wallet, Phantom now fully supports Ethereum and Polygon.

Advantage:

- If you are a developer who works on both Solana (Rust) and Ethereum (Solidity), you can use one single wallet for both.

Lifecycle of a User

Wallet as Identity - This is your Wallet Address

Remember: A wallet isn't just a container for money; it's a pair of cryptographic keys

Faucet as Fuel - is a smart contract that sends tokens to your Wallet Address upon request.

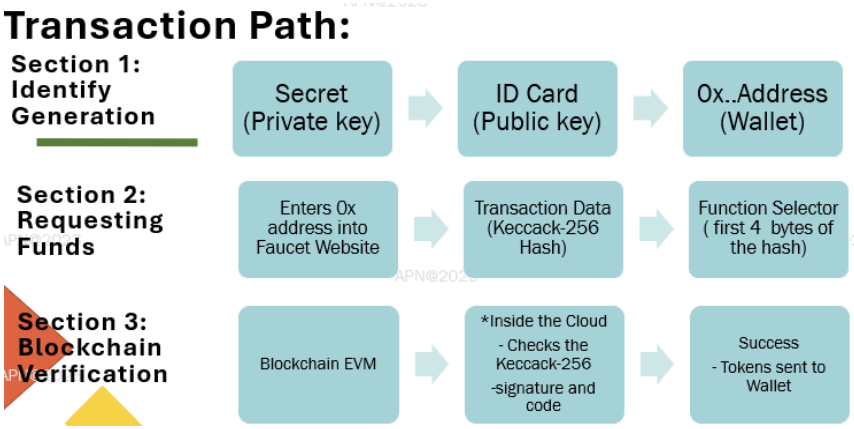
Remember: You provide your address to the faucet, and it triggers a "Write" function on the blockchain to send you test ETH, to pay the gas fee.

Keccak -256 as Engine - is the cryptographic hash function that powers everything

Remember: Your Wallet Address is actually the last 20 bytes of a Keccak-256 hash of your public key

Keccak-256

- (pronounced *ket-chak*) is the cryptographic hash function that serves as the DNA generator for the Ethereum ecosystem.
- it is the specific math that creates your wallet address and makes your smart contracts work.
- **it** remains the undisputed standard for EVM (Ethereum Virtual Machine) blockchains.
- Its dominance isn't just about technical specs; it's a mix of **historical timing**, **unique security architecture**, and **network effects**.



The Computation of Wallet Address:

1.**Private Key,** start with a random 256-bit number.

2.**Public Key,** use Elliptic Curve math (secp256k1), a public key is derived.

3.**Keccak Hashing,** The system takes that public key and runs it through the Keccak-256 algorithm.

Trimming, It takes **the last 20 bytes** of that hash, adds 0x to the front and that is your Wallet Address.

Exmaple:

Step 1: Binary Conversion (ASACII value =1 byte = 8 bits)

C = 67 = 01000011

H = 72 = 01001000

A = 65 = 01000001

I = 73 = 01001001

N =78 = 01001110

Step 2:The 10*1 Rule (complete the 1088 bits)

CHAIN = 40 bits

1.Add Domain bits : 01 (standard for Ethereum's Keccak)

2. **Add Pad start: add 1**
3. **Add Pad Gap: Add nth zeroes to fill the space**
4. **Add pad end: Add a final 1**

Message + Domain + Pad Start + nth zeroes + pad end = 1088

Step 3:XOR State = start with 1600 bit of all zeroes

Step 4: Permutation = 24 rounds

Step 5: The final Hash

- **the first 256 bits of the final 1600 and convert then to Hexadecimal**

Example Wallet Address:

Raw hash:

Address: 32 bytes = 64 Hex

Note: 1 byte = 2 Hex = 1 hex = 15 = 1111 1111

Trimming: 20 byte rule

-64 characters down to 12 bytes

-Rule: Take only the last 20 bytes of the Keccack 256 hash

-Hexadecimal= 20 * 2 = 40 characters

0c2be79367ba0c0b59460475 b90d65a624909bc36eee6bffdecf3c5acd7774c0

0c2be79367ba0c0b59460475 b90d65a624909bc36eee6bffdecf3c5acd7774c0

b90d65a624909bc36eee6bffdecf3c5acd7774c0

0xb90d65a624909bc36eee6bffdecf3c5acd7774c0

Wallet address

Module 8 :Token and ERC in Blockchain Technology

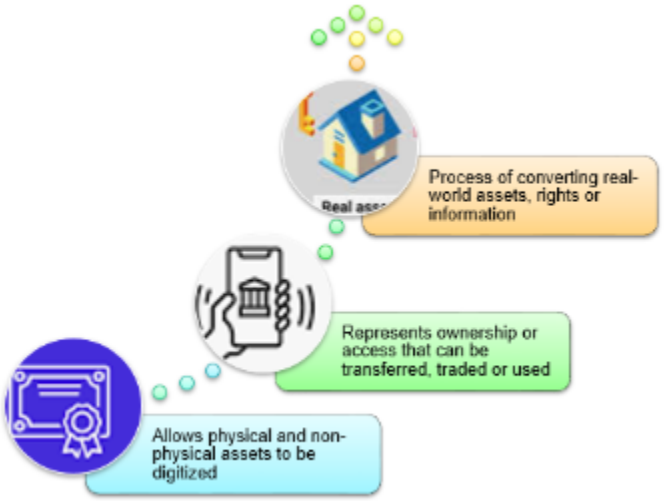
TOKEN

- in the context of blockchain refers to a digital representation of value or rights that exist on a blockchain.
- can serve various purposes, including representing assets, enabling transactions, or providing access to specific applications or services.
- They are created using smart contracts and operate on blockchain platforms like Ethereum, Binance Smart Chain etc.
- In the Blockchain ecosystem, any asset that is digitally transferable between two people is called a token.

- Depending on the properties assigned to them, they have different classification and uses.

TOKENIZATION

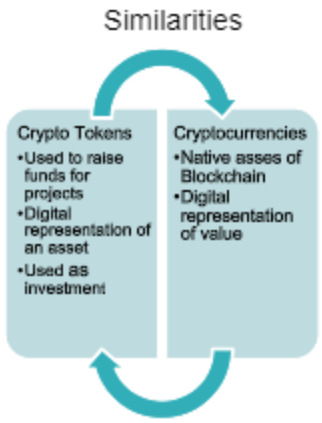
- refers to the process of converting real-world assets, rights, or information into digital tokens on a blockchain.
- represent ownership or access to these assets and can be transferred, traded, or used within a decentralized system. T
- allows physical and non-physical assets to be digitized, increasing liquidity, transparency, and accessibility for investors and participants in a blockchain ecosystem.



Key Aspects of Tokenization

Representation of Assets	Physical Assets: Real estate, gold, art, or commodities can be tokenized and represented as digital tokens on a blockchain. Digital Assets: Intellectual property, music rights, or digital artwork can also be tokenized. Non-fungible tokens (NFTs) are an example

	where each token represents a unique digital item.
Fractional Ownership	Tokenization enables the division of large assets into smaller, tradeable tokens, allowing investors to buy and sell fractions of high-value assets, such as real estate or fine art. This opens up investment opportunities to a broader range of people by lowering entry barriers.
Increased Liquidity	By converting traditionally illiquid assets (like real estate) into tokens, tokenization enhances liquidity. These tokenized assets can be easily bought, sold, or traded on secondary markets, offering more flexibility for investors
Transparency and Security	Tokenization leverages blockchain's transparency and immutability. Every token transaction is recorded on the blockchain, creating a permanent, auditable history of ownership and transfers. This increases trust and reduces fraud
Programmability	Tokens can be programmed with specific rules and conditions, such as smart contracts. This allows for automated actions, such as distributing dividends to token holders, enforcing voting rights, or automatically executing contractual terms



Crypto or cryptography

- refers to the various encryption algorithmsand cryptographic techniques that safeguard crypto tokens and currencies, such as elliptical curve encryption, public-private key pairs, and hashing functions.

Cryptocurrencies

- on the other hand, are virtual currencies on a blockchain. These systems that allow for secure online payments and the storing of value.

Crypto tokens

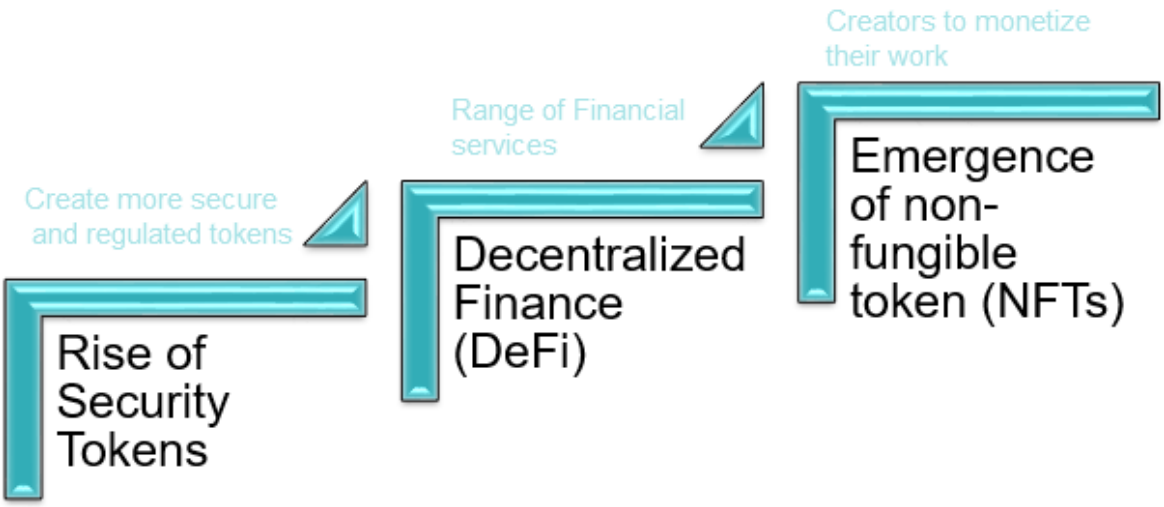
- are transactional units created on top of existing blockchains by blockchain companies or projects.
- They are created using standard templates like that of the Ethereum network.
- Such blockchains work on the concept of smart contract or decentralized applications wherein the programmable, self-executing code is used to process and manage the various transactions that occur.

Different forms of tokens:

ERC20: the “fungible” tokens	• First token standard to have established itself in the Ethereum ecosystem, the ERC20 token is managed by a smart contract that presents a list of minimal functions: how to create new units divided into fractions, destroy them and transfer them to another portfolio. • Most of these tokens come from an ICO (Initial Coin Offering) and are linked to a specific project, with its own value proposition. Some ERC20 are interesting and part of our list of cryptocurrencies that stand out in 2019. • The use of ERC20s is extremely varied: exchange or value assets within the ecosystem of a project, representation of an asset that is the underlying whose value remains fixed against a state currency.
ERC721 : the “non-fungible” tokens	• Popularised by CryptoKitties, built on the basis of ERC20 and take all its technical characteristics, with one fundamental difference: they are non-fungible tokens that represent a digital object with unique characteristics: a serial number, a name, character characteristics or game objects. • The term “crypto-collectible” is also used, very popular in the field of video games or property. • are always unique and cannot be replicated or subdivided into token fractions.

ERC1411 : the “Security tokens”	• Based once again on the ERC20, security tokens include assets that require compliance with financial law. • They represent financial products in the traditional sense, such as shares, bonds, debts or property titles. • Subject to the same rules as traditional products, investment or trading in these assets is limited to the so-called “qualified” investors. • The particularity of ERC1411 tokens is that they cannot be freely transferred like traditional ERC20 tokens: a third party is responsible for authorizing or not the transfer of these digital objects in order to comply with the laws and state regulations managing the underlying assets they represent.

Future of of Crypto Tokens:



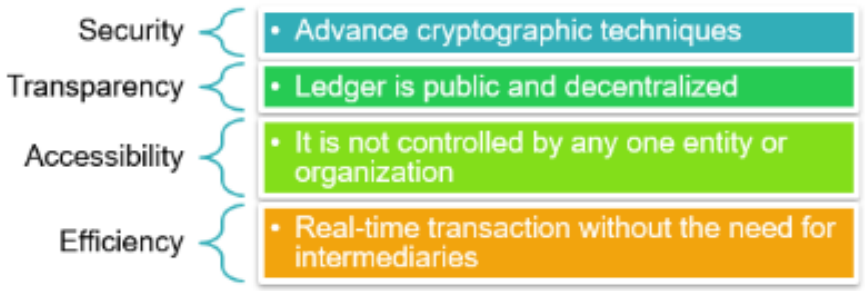
Rise of Security Token	• A growing interest in using blockchain technology to create more secured and regulated tokens. • These security tokens, which are backed by real-world assets such as stocks or property, offer a way for investors to participate in the benefits of blockchain technology while also enjoying greater legal protection.
Decentralized Finance(DeFi)	• One of the most exciting applications of crypto tokens is in the realm of decentralized finance (DeFi). • This refers to a range of financial services that are built on blockchain platforms and are designed to be open, transparent, and accessible to anyone with an internet connection. • Crypto tokens play a central role in DeFi, enabling everything from peer to peer to decentralized exchanges.

Emergence of non-fungible tokens(NFTs)	• While most crypto tokens are fungible, meaning that they can be exchanged for other tokens of the same value, there is also a growing market for non-fungible tokens (NFTs). • These unique digital assets, which are often used to represent artworks or collectibles, are built on blockchain platforms and offer a way for creators to monetize their work in a new and innovative way.

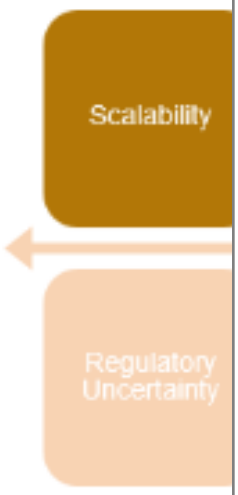
Impact of Crypto Token on Blockchain Technology

1. Encouraging adoption: Crypto tokens have the potential to encourage the adoption of blockchain technology by making it more accessible to the general public.
2. Building communities:By issuing tokens to users, projects can incentivize them to participate in the development of the project, whether it be by contributing code, providing feedback, or simply spreading the word. This can help to create a sense of ownership and belonging among users, which can be a powerful motivator for continues engagement.
3. Enhancing security: Crypto tokens can also enhance the security of blockchain networks by incentivizing users to act in the best interests of the network through networks use Proof-of-Stake (PoS) or delegated proof-of-stake(dPOS) consensus mechanisms.
4. Enabling new use cases: crypto tokens have the potential to enable new use cases, tokens can be used to represent ownership in physical assets or artwork which could help to revolutionize the way we think about ownership and transfer of assets.

Advantages of Crypto Token on Blockchain



Challenges of Crypto Token

• Scalability is a major challenge when it comes to implementing crypto tokens to alleviate congestion on main blockchain network. • Regulatory Uncertainty, the regulatory landscape surrounding crypto tokens can be difficult to navigate, as laws and regulations vary by jurisdiction. This can make it challenging for businesses to launch crypto token projects and comply with relevant laws. • Links to an external site. •		• Security,there have been instances of hacks and vulnerabilities that have resulted in the loss of funds. One way to address this challenge is to use multi-signature wallets which require multiple signatures. • Interoperability, different blockchains may have different standards for creating and managing tokens, which can make it difficult for tokens to work across multiple blockchains.

Regulatory Environment of Crypto Token in Blockchain

Ethereum Request Comment (ERC) in Blockchain Technology

- ERC stands for Ethereum Request for Comments.
- It is the set of rulebooks or technical blueprints that tell a smart contract how to behave so it can talk to other apps, wallets, and exchanges.

What exactly is an ERC?

- ERCs are technical documents written by developers for the Ethereum community.
- They start as EIPs (Ethereum Improvement Proposals).
- Once the community agrees that a proposal is useful and stable, it becomes an official ERC Standard.

Importance of ERC:

- Without ERCs, the blockchain be every developer would create tokens using different code, meaning:
    - Wallets (like MetaMask) wouldn't know how to show your balance.
    - Exchanges (like Coinbase) would have to write custom code for every single new token.
    - DeFi Apps wouldn't be able to swap one token for another.

Rules:

- Interoperability: One of the primary reasons for ERC standards is to ensure that different dApps and tokens can easily interact with one another. If everyone follows the same set of rules, there are fewer compatibility issues.
- Developer Guidelines: These standards offer developers clear instructions on how to create tokens and smart contracts, which can help streamline development.
- Security: ERC standards often include security features that protect smart contracts from vulnerabilities, reducing the risk of hacking or loss of assets.

ERC (Ethereum Request for Comments) refers to technical standards used for smart contracts on the Ethereum blockchain. These standards define rules and functions that developers can follow to ensure compatibility across decentralized applications (dApps) and tokens. ERC standards are proposals for changes and improvements to the Ethereum ecosystem, submitted by developers, and once accepted, they become guidelines for the Ethereum community.

Each ERC standard includes:

- Rules and Functions: A set of required methods or functions that must be implemented (e.g., balance inquiry, transfer of tokens, etc.).
- Event Logs: Events are triggered during certain actions (like transferring tokens), which helps keep the blockchain transparent.
- Compatibility: Smart contracts or tokens following an ERC standard are compatible with all wallets and dApps that support the standard.

Why ERC Matters

- Ecosystem Growth: ERC standards have significantly contributed to Ethereum's explosive growth by making it easier for developers to build dApps and issue tokens.
- Innovation: New ERC proposals encourage innovation and provide a way to introduce new functionality to the Ethereum network,

such as security enhancements, improved transaction handling, or new use cases like NFTs.
- Decentralized Finance (DeFi): Many DeFi protocols, which allow for decentralized lending, borrowing, and trading, are built on ERC-20 and ERC-721 toke

Popular ERC Standards: While there are many ERC standards, some of the most popular include:

- ERC-20: The standard for fungible tokens. ERC-20 tokens are interchangeable and have the same value (like traditional currencies). Most cryptocurrencies (besides Ethereum) use the ERC-20 token standard.
- ERC-721: The standard for non-fungible tokens (NFTs). ERC-721 tokens are unique and cannot be exchanged on a one-to-one basis. Each token represents a distinct asset, making this standard ideal for NFTs in areas like digital art or collectibles.
- ERC-1155: This standard allows for multi-token management, meaning it can handle both fungible and non-fungible tokens in one contract. This is more efficient for dApps dealing with both token types, such as games or marketplaces.
- ERC-777: An improvement over ERC-20, offering advanced features like operator-based permissions and backward compatibility. It adds flexibility and security to token transactions.
- ERC-1400: A standard for security tokens that includes functions like issuance, redemption, and compliance for regulated financial assets.

The future of ERC (Ethereum Request for Comment) standards, such as ERC-20, ERC-721, and ERC-1155

Increased Customization of Tokens	As blockchain adoption expands, businesses and developers are looking for more customizable token standards to meet their specific needs. Future ERC standards will likely allow for more modular and customizable features, giving projects the flexibility to tailor tokens to their unique requirements, such as adding governance features, automatic token burn mechanisms, or adaptive token supply. This customization could also lead to more sophisticated NFT (ERC-721) tokens that incorporate complex rights management, royalties, and even dynamic content that changes over time.
Interoperability and Cross-Chain Solutions	The interoperability between Ethereum and other blockchains is a critical area for future development. We are already seeing the rise of cross-chain bridges and Layer 2 solutions like Polygon, Optimism, and Arbitrum that allow ERC tokens to operate seamlessly across different platforms and reduce transaction costs.Future ERC standards may incorporate features that make tokens more natively interoperable with multiple blockchain networks. This will reduce fragmentation and create more fluid and efficient ecosystems for users.

Scalability and Gas Efficiency	One of the biggest issues facing Ethereum today is scalability and high gas fees. Future ERC standards will likely focus on creating gas-efficient token interactions. For example, standards like ERC-1155 have already reduced gas costs for minting and transferring multiple tokens, and this trend will continue with even more efficient protocols and standards. Ethereum's transition to Proof of Stake (Ethereum 2.0) will also address scalability issues, and future ERC standards will likely align with these advancements
Decentralized Finance (DeFi) Innovations	ERC-20 tokens are at the core of the DeFi ecosystem, which is expected to grow significantly. As DeFi platforms evolve, we may see the development of new ERC standards designed specifically for financial instruments, derivatives, yield farming, automated market makers (AMMs), and governance tokens. These new standards will bring increased security, transparency, and efficiency to decentralized financial products and services.

NFT and Metaverse Evolution	The future of ERC-721 (NFTs) and ERC-1155 will be closely tied to the growth of the Metaverse and the virtual economy. NFTs will expand beyond digital art and collectibles to represent virtual real estate, avatars, in-game assets, and even real-world assets like cars and property. Future ERC standards for NFTs may also include improvements in royalties management, fractional ownership, interoperability across metaverses, and embedded utility for NFTs that grant access to exclusive content or experiences
Governance and DAO (Decentralized Autonomous Organizations) Standards	As more projects move towards decentralized governance models, we may see the rise of new ERC standards that cater to DAOs. These standards could define how voting tokens and governance tokens are created, distributed, and utilized within decentralized communities. Future ERCs will focus on ensuring transparency, security, and decentralized control over governance, enabling more robust and scalable DAOs.

Security and Compliance Standards	As blockchain and token adoption continue to grow, the importance of security and regulatory compliance will become more pronounced. We may see new ERC standards aimed at improving token auditability, ensuring anti-money laundering (AML) and know-your-customer (KYC) compliance, and reducing smart contract vulnerabilities. There is likely to be more focus on developing ERC standards that can easily integrate with compliance systems and provide better security mechanisms for token issuance and transfers.
Sustainability and Eco-friendly Practices	As the blockchain industry continues to face criticism for its energy consumption, future ERC standards may explore more energy-efficient mechanisms or integrate eco-friendly practices like carbon credits or proof of green tokens, especially after Ethereum’s full transition to Proof of Stake (PoS). The demand for environmentally conscious blockchain applications could push the development of new token standards that prioritize sustainability.

Composable Tokens (NFTs and DeFi)	ERC standards may support composable tokens, which can interact with each other and be used across different platforms. For instance, a DeFi protocol could leverage both ERC-20 and ERC-721 tokens together in complex financial products, or NFTs could have programmable behaviors and interoperability across different ecosystems (e.g., in-game assets working across multiple games).