Blockchain Technology

Introduction to Ethereum Tokens

Ashutosh Bhatia

BITS Pilani

ashutosh.bhatia@pilani.bits-pilani.ac.in

Token on Blockchain

- Block chain based abstractions (logical entities) that can owned and that represent asset, currency access rights etc.

- Unlike physical token that are not really exchange and often restricted to specific businesses, organization and locations

How token are used in Blockchain

- **Currency :** A token can serve as a form of currency, with a value determined through private trade.
- **Resource** **:** A token can represent a resource earned or produced in a sharing economy. Ex. storage or CPU token representing resources
- **Asset:** A token can represent ownership of an intrinsic or extrinsic, tangible or intangible asset; Ex. gold, real estate, a car, oil, energy, etc.
- **Access:** A token can represent access rights and grant access to a digital or physical property, such as a discussion forum, an exclusive website, a hotel room, or a rental car.
- **Voting:** A token can represent voting rights in a digital or legal system.
- **Collectible:** A token can represent a digital collectible (e.g., CryptoPunks) or physical collectible (e.g., a painting).
- **Identity:** A token can represent a digital identity (e.g., avatar) or legal identity (e.g., national ID).

Tokens and Fungibility

- In economics, fungibility is the property of a good or a commodity whose individual units are essentially interchangeable.
- Tokens are fungible when we can substitute any single unit of the token for another without any difference in its value or function.
- Non-fungible tokens are tokens that each represent a unique tangible or intangible item and therefore are not interchangeable.
  - Digital Collectables: In CryptoKitties you can breed and adopt Kitties of all colours and shapes. Create Collections of your favourite cats and share them with our breeding community.

Counterparty Risks

- Counterparty risk is the risk that the *other* party in a transaction will fail to meet their obligations.
- when an asset is traded indirectly through the exchange of a token of ownership, there is additional counterparty risk from the custodian of the asset.
  - Do they have the asset?
  - Will they recognize (or allow) the transfer of ownership based on the transfer of a token (such as a certificate, deed, title, or digital token)?
  - In the world of digital tokens representing assets, as in the non-digital world, it is important to understand who holds the asset that is represented by the token and what rules apply to that underlying asset.

Tokens on Ethereum

- Blockchain tokens existed before Ethereum. In some ways, the first blockchain currency, Bitcoin, is a token itself.
- Many token platforms were also developed on Bitcoin and other cryptocurrencies before Ethereum.
- However, the introduction of the first token standard on Ethereum led to an explosion of tokens.
- Vitalik Buterin suggested tokens as one of the most obvious and useful applications of a generalized programmable blockchain such as Ethereum.

Tokens on Ethereum

- Tokens are different from ether because the Ethereum protocol does not know anything about them.
- Sending ether is an intrinsic action of the Ethereum platform, but sending or even owning tokens is not.
- The ether balance of Ethereum accounts is handled at the protocol level, whereas the token balance of Ethereum accounts is handled at the smart contract level.
- In order to create a new token on Ethereum, you must create a new smart contract.
- Once deployed, the smart contract handles everything, including ownership, transfers, and access rights.
- You can write your smart contract to perform all the necessary actions any way you want, but it is probably wisest to follow an existing standard.
- We will look at such standards next. We discuss the pros and cons of the following standards

The ERC20 Token Standard

- The first standard was introduced in November 2015 by Fabian Vogelsteller as an Ethereum Request for Comments (ERC).
- It was automatically assigned GitHub issue number 20, giving rise to the name “ERC20 token.”
- The vast majority of tokens are currently based on the ERC20 standard.
- ERC20 is a standard for *fungible tokens*
  - different units of an ERC20 token are interchangeable
- The ERC20 standard defines a common interface for contracts implementing a token, such that any compatible token can be accessed and used in the same way.
  - The interface consists of a number of functions that must be present in every implementation of the standard, as well as some optional functions and attributes that may be added by developers.

Using Tokens: Utility or Equity

- Almost all projects in Ethereum today launch with some kind of token. But do all these projects really need tokens?
- The majority of projects are using tokens in one of two ways: either as "**utility tokens**" or as "**equity tokens**."
- Utility tokens is required to gain access to a service, application, or resource.
  - Examples of utility tokens include tokens that represent resources such as shared storage, or access to services such as social media networks.
- Equity tokens represent shares in the control or ownership of something.
  - Equity tokens can be as limited as nonvoting shares for distribution of dividends and profits, or as expansive as voting shares in a decentralized autonomous organization

Utility Tokens: Who Needs Them?

- The real problem is that utility tokens introduce significant risks and adoption barriers for startups.
- Perhaps in a distant future “tokenize all the things” will become reality, but at present the set of people who have an understanding of and desire to use a token is a subset of the already small cryptocurrency market.
- For a startup, each innovation represents a risk that works as the barrier for the adoption of the technology by the users
  - Still a very small portion of the world believe in blockchain technology
  - Only a subset of those people would be ready to use the service offered by your innovation over this technology
  - Adding utility tokens to that may further reduce the degree of adoption of the project.
- Nevertheless, some of the most innovative business ideas are indeed taking place in the crypto realm.
  - If regulators are not quick enough to adopt laws and support new business models, entrepreneurs and associated talent will seek to operate in other jurisdictions that are more crypto-friendly. This is already happening.

ERC20: functions and events

- An ERC20-compliant token contract must provide at least the following functions and events:
- totalSupply : Returns the total units of this token that currently exist. ERC20 tokens can have a fixed or a variable supply.
- balanceOf: Given an address, returns the token balance of that address.
- transfer: Given an address and amount, transfers that amount of tokens to that address, from the balance of the address that executed the transfer.
- transferFrom : Given a sender, recipient, and amount, transfers tokens from one account to another. Used in combination with approve.
- Approve : Given a recipient address and amount, authorizes that address to execute several transfers up to that amount, from the account that issued the approval.
- Allowance : Given an owner address and a spender address, returns the remaining amount that the spender is approved to withdraw from the owner.
- Transfer: Event triggered upon a successful transfer (call to transfer or transferFrom) (even for zero-value transfers).
- Approval: Event logged upon a successful call to approve.