Elements of DeFi

https://web3.princeton.edu/elements-of-defi/

Professor Pramod Viswanath

Princeton University

Lecture 17

Non Fungible Tokens

Last Lecture: Derivatives and Synthetics

- Derivatives
  - Futures
  - Options
  - Swaps
- Synthetics are tokenized derivatives
  - Wrapped asset-backed tokens
  - CDP based synthetics
  - Perpetuals
  - Options

This lecture: NFTs

- Fungible vs Non-fungible assets
- Non fungible assets in real world
- Tokenized Non Fungible assets: NFTs
- Use cases of NFTs:
  - Tokenizing RWA
  - Art
  - Games
  - Supply chain tracking
- Challenges

Fungible vs Non Fungible assets

- Fungible assets: Assets that aren't differentiated – can be interchanged with one-another
  - Fiat currency: USD
  - Commodities: Gold
  - Futures and derivatives
- Easy to set up markets since there is typically high liquidity

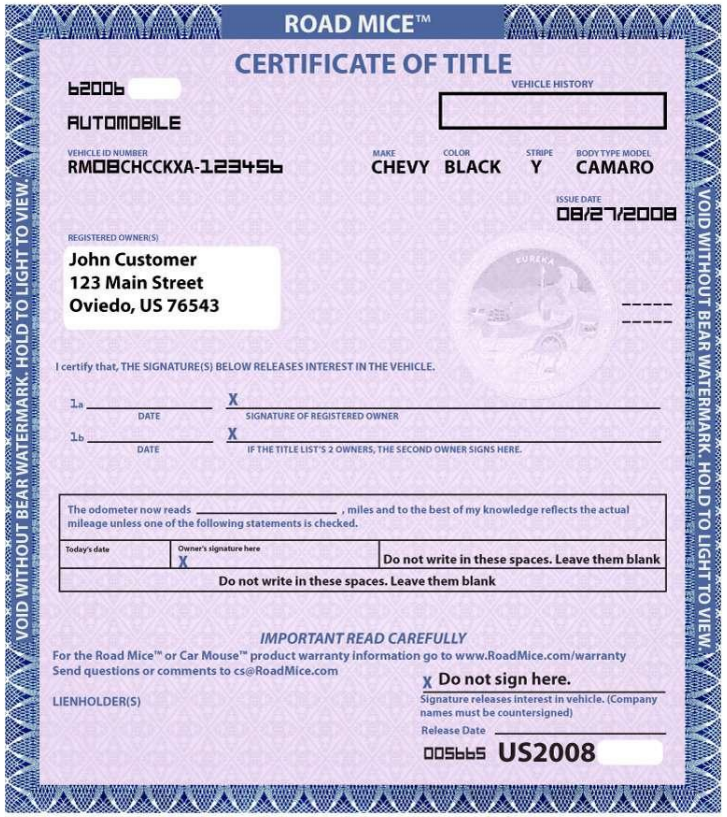
- Non-fungible assets: One-of-a-kind assets that cannot be replaced by another asset of the same category

Non fungible assets in real world

- Real estate – A piece of land marked by a geographic boundary is unique
- Art – Paintings by famous artists
- Graduation certificates – Unique to the program and the person
- Wireless spectrum – Rights to transmit at a particular frequency in a county

Non fungible tokens

- NFTs tokenize non-fungible assets
- Once tokenized, the assets ownership can then be programmed to behave in arbitrary ways – fractional ownership, royalty sharing, etc.
- Assets that live in a virtual format are best suited to be tokenized – Digital art, game assets
- Token standards ensure that each individual minted token unique



ERC 721 token standard

- ERC20 equivalent token standard for NFTs
- An ERC721 contract defines a NFT collection
- Each NFT withing the collection is assigned a tokenID
- Standardization ensures compatibility across different applications

ERC 721

- Some functions are similar to ERC-20 contract
  - *Approve* – Approve some contract to manage the NFT
  - *Transfer* – Transfer NFT to another owner
  - *TransferFrom* – Transfer asset on behalf of the NFT owner if approved
  - *BalanceOf* – Returns the number of NFTs owned by an address
- *Mint* – Essential but not part of the standard – encodes access control rules to ensure integrity of the collection
- Main difference: Each token has an ID and an associated metadata (URI)

Typical NFT add-ons

- Minting authority: Each NFT contract has its own rules on who can mint tokens – typically contract owner
- Ownership transfers and royalties: Some contracts/marketplaces enforce rules on royalty payment. Eg. 10% of sale proceeds should go to the artist
- Fractionalization: Some NFT contracts allow for each token to be fractionalized and owned by multiple entities – Fractional ownership of paintings

NFT storage

- Fully on-chain storage and generation: All data is stored and generated – Uniswap LP tokens
- Partial on-chain storage: Store “genes” of the NFT on-chain, logic to convert genes to images is stored off-chain and implemented on a web server
- Off-chain storage: Only metadata pointing to the off-chain storage is stored on-chain

Off-chain storage

- Centralized storage: Stored on a central server; Eg. AWS S3
- IPFS storage: Inter Planetary File System is a P2P storage mechanism where files are addressed by their content hash – content of the NFT is frozen once its IPFS address is posted on chain.
- Incentivized decentralized storage: Stored on storage nodes run by an incentivization layers like Filecoin (+ IPFS) or Arweave

ERC 1155 standard

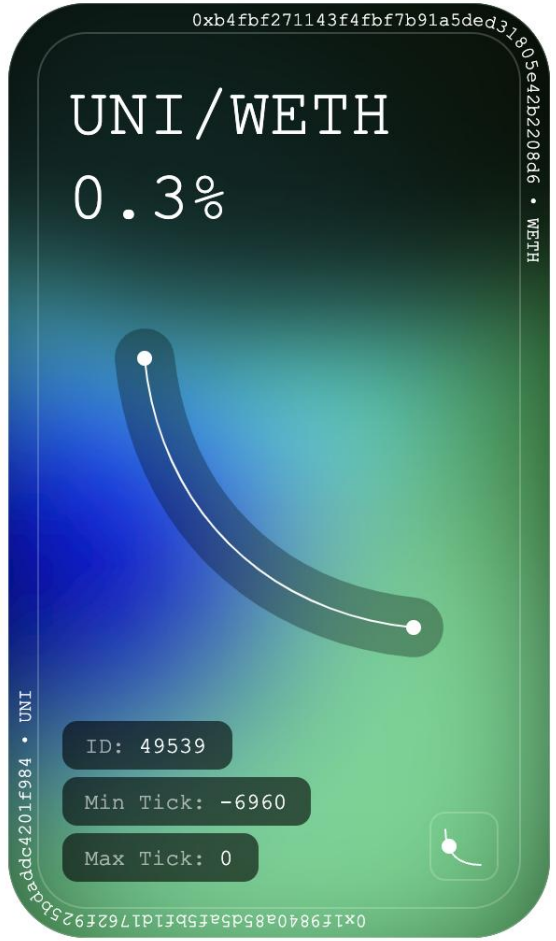
- Supports both Fungible and Non-fungible tokens
- Tokens have an identifier (similar to ERC 721) and token count (similar to ERC 20)
- Supports batch transfers and approval of tokens for reduced gas costs

NFT use cases

- LP token for Uniswap V3
- Art
- Membership
- Games & Metaverse
- Tokenized RWAs

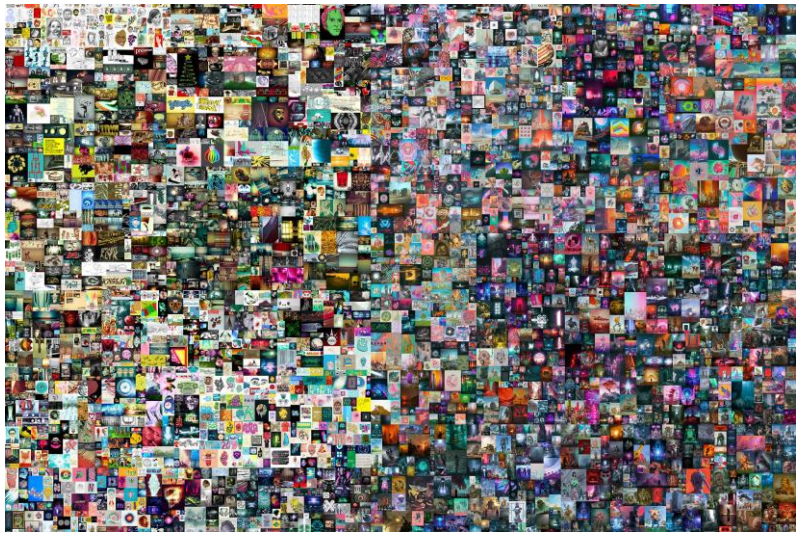
LP token on Uniswap V3

- Unique tokens since LP can provide liquidity over a wide range of assets
- Token metadata contains information on the ticks
- Fee payout is determined from the metadata at the time of LP redemption

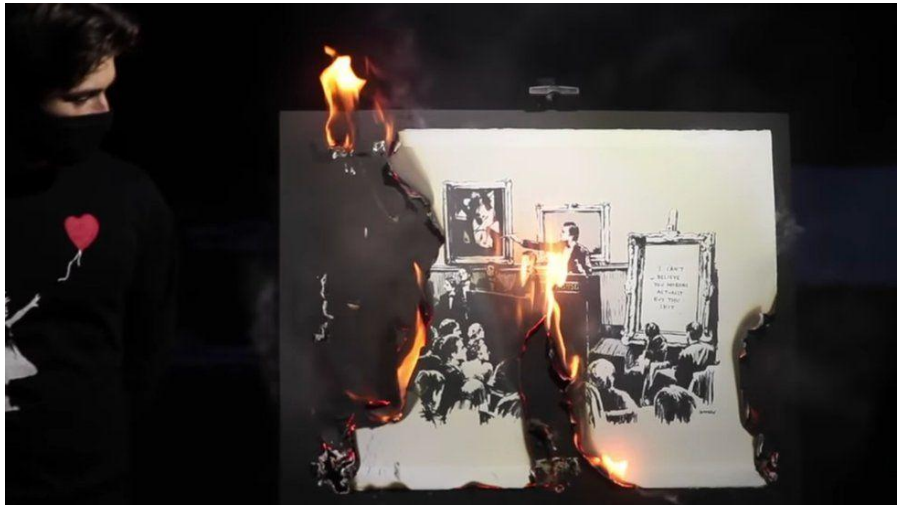


Art

- NFTs represent ownership of art
- Digital art: Beeple's art sold at aution held by Christie's
- Physical art: RWA wrapping mechanisms convert physical art to NFTs
- Royalty sharing: Artist gets a percentage of future sales



Beeple: "Everydays - The First 5000 Days"



Banksy art "Proof of Burn" to convert to NFT

Membership

- NFTs with limited supply create a “country club” effect with exclusive access to events and networking opportunities with fellow holders: Bored Ape Yacht club, CryptoPunks

$23.7M

- Some NFTs act as loyalty programs: Receive hotel discounts if you own NFTs

$3.4M

Games

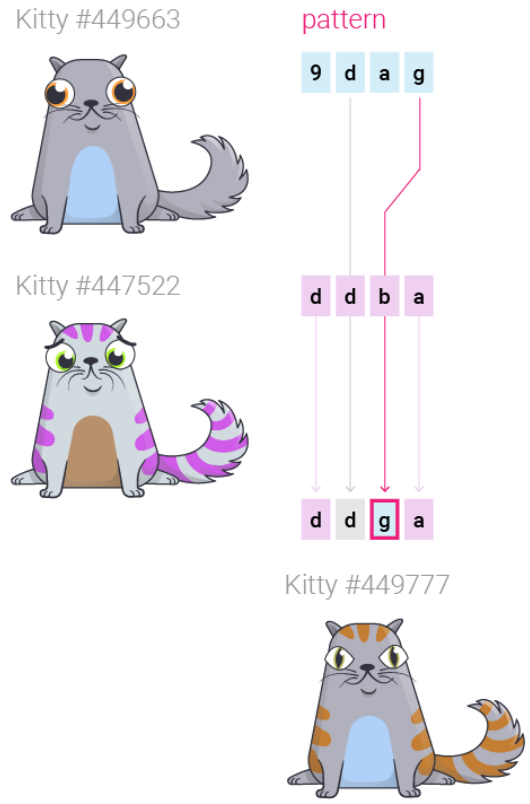
- Game assets can be tokenized to ensure open marketplaces for trading, support past depreciation of original game maintaining organization

- Efforts to establish standards for cross-game asset transferability

Pet Characters
are represented as NFTs

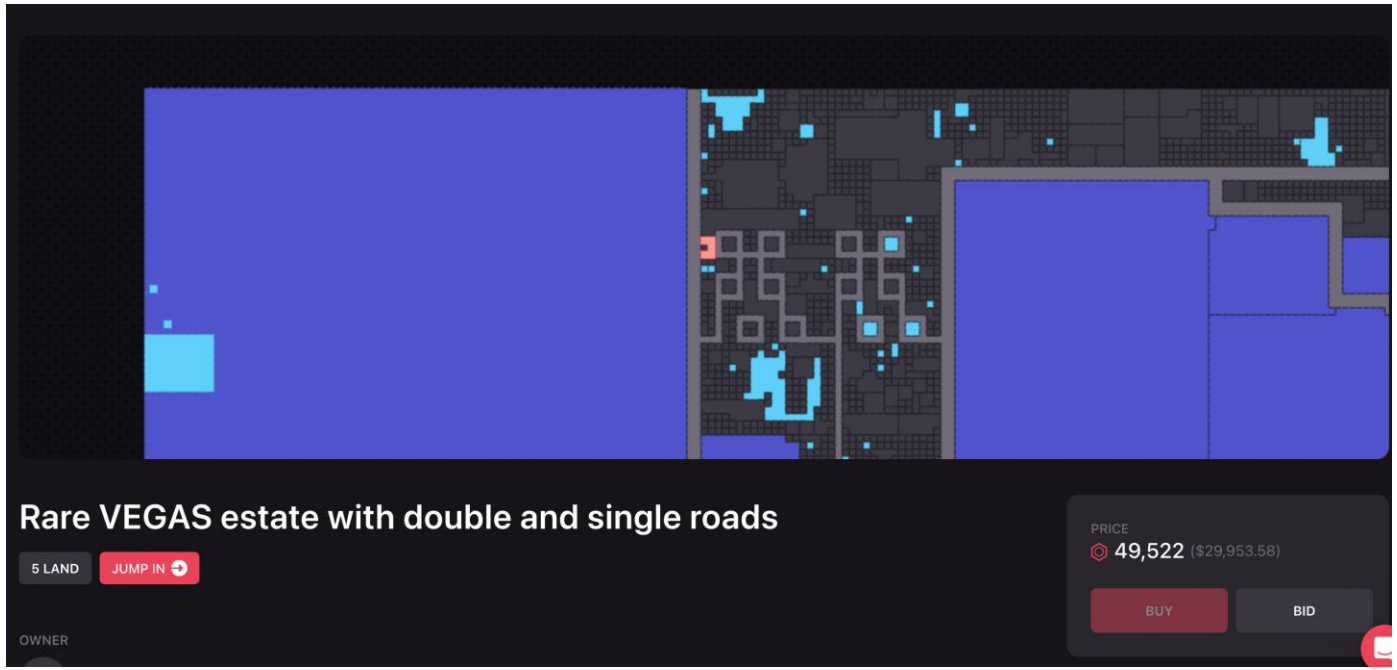
Games

- Evolving assets: Characters evolve traits over generations
- Rules for evolution of traits is encoded within smart contracts
- Example: Cryptokitties
  - Genes of virtual cats are stored on-chain – determine visual features
  - Evolution of genes determined by breeding



Games

- Metaverse asset ownership can be maintained through NFTs
- Eg. Land ownership on Decentraland
- Wearables, cars, etc. asset marketplaces can be established



Tokenized RWAs

- Real estate title, car titles can be tokenized to reduce fraud and intermediaries such as title insurance
- Enable additional features: Car unlock by token holder signature
- Regulatory hurdles in implementation

NFT marketplaces

- Listings – Fixed price, take it or leave it
- Auctions – Price discovery
- AMMs – Continuous price discovery

NFT auctions

- English Auction: Sell to the highest bidder
  - Seller sets a starting price, reserve price and auction expiry time
  - Bidders have to bid value higher than the previous bid (starting price = bid 0)
  - No obligation to sell if highest bid is less than reserve price
  - Bids around expiry time extend the auction (why?)
- Dutch Auctions: Sell to the first bidder at declining price
  - Seller sets the starting price (say 2 ETH), ending price (say 1 ETH) and duration
  - Price decreases linearly
  - First bidder gets the NFT

NFT AMMs

- NFT AMM:
  - Create a liquidity pool for an ERC-20/ERC-721 pair
  - All NFTs within the collection are listed at the same price set by the bonding curve
  - Price discovery for a collection – not individual NFTs
  - Not ideal for NFTs with unique features
- Fractional NFT AMM:
  - Create liquidity pool of an ERC-20/Fractional NFT pair
  - Traders can trade the ERC-20 token for a fractional ownership of the listed NFT/collection
  - Fractional owners get paid when the collection is auctioned

Challenges

- Copyright protection for art: Duplication is possible for the same piece of art in a different collection or on a different chain
- RWA data integrity: Importing data on real world asset transfer on-chain presents a single point of failure
- Interoperability: Inter-application translation of asset representation requires some standardization (A sword in D&D should be rendered as a sword in GTA)

LECTURE ENDS