

Teaching in the Classroom - Cryptocurrencies, Blockchains and NFTs



Debasis Bhattacharya, DBA, JD

University of Hawaii Maui College

March 3, 2023

debasisb@hawaii.edu

maui.hawaii.edu/cybersecurity

Agenda

- Basics of Cryptocurrencies
- Blockchains
 - Ethereum
 - Smart Contracts
 - NFTs
- Labs
 - Creating your first Smart Contract
 - Creating NFTs on Open Sea
- Q&A



Bitcoin.org needs your support!



Introduction ▾

Resources ▾

Innovation

Participate ▾

FAQ

English ▾

Bitcoin is an innovative payment network and a new kind of money.

Get started with Bitcoin

Choose your wallet

Buy Bitcoin

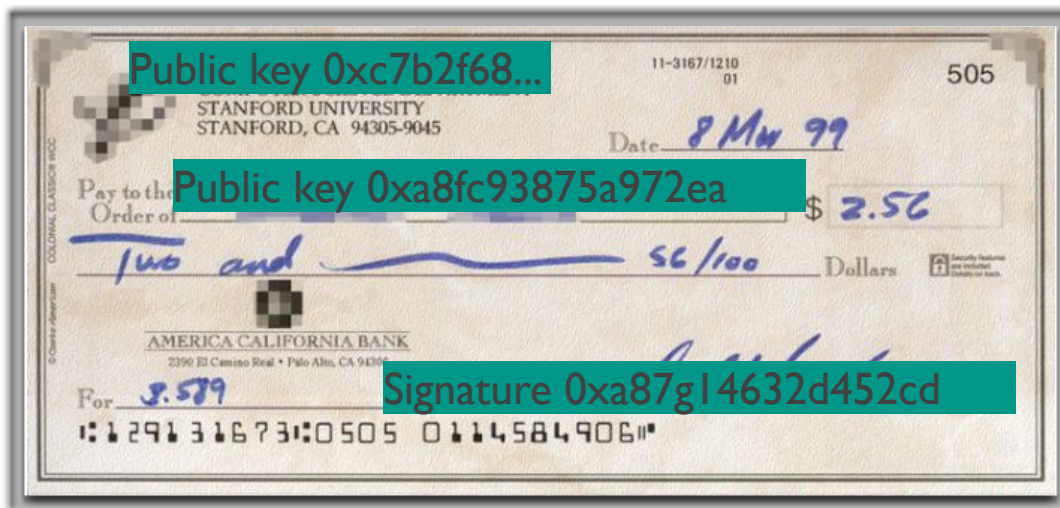


What is Bitcoin?

Bitcoin

- Bitcoin paper by Satoshi Nakamoto on October 31, 2008.
- First bitcoin transaction on January 12, 2009
- Number of BitCoins in circulation ~19.1 million (July 2022)
- Total number of BitCoins generated cannot exceed 21 million.
 - New blocks created every 10 minutes (very slow in # of transactions compared to credit cards)
 - Currently, each block adds 6.25 bitcoins into circulation
 - Mining will end in the year 2140...
- Average price of a Bitcoin:
 - \$23,146 on February 24, 2023
 - \$16,481 on November 26, 2022
 - \$22,507 on July 23, 2022
 - \$48,117 on December 11, 2021
 - \$43,819.54 on September 21, 2021
 - \$43,045.91 on May 18, 2021
 - \$10,360.45 on July 1, 2019
 - \$4,110 on February 23, 2019
 - \$3,729 on Dec 29, 2018
 - \$8,522 on May 15, 2018
 - \$18,000 on December, 2017
 - \$3,867 on September 25, 2017
 - \$2,350 on June 27, 2017
- Price has been very unstable!

Bitcoin Transactions

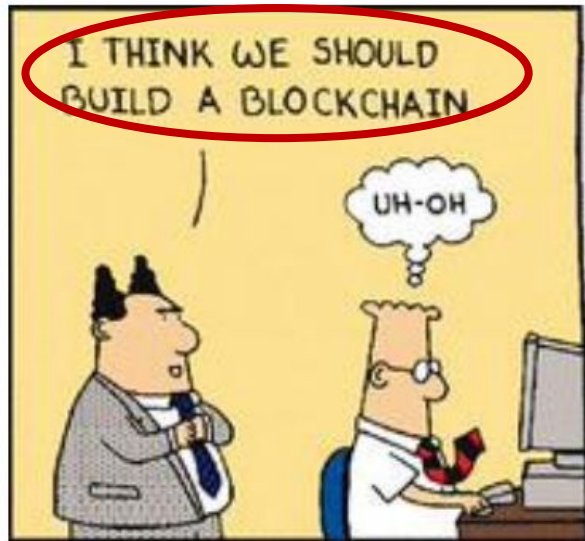


Bitcoin Network

- Each P2P node runs the following algorithm:
 - New transactions are broadcast to all nodes.
 - Each node (miners) collects new transactions into a block.
 - Each node works on finding a proof-of-work for its block. (Hard to do. Probabilistic. The one to finish early will probably win.)
 - When a node finds a proof-of-work, it broadcasts the block to all nodes.
 - Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions).
 - Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Bitcoin: Challenges

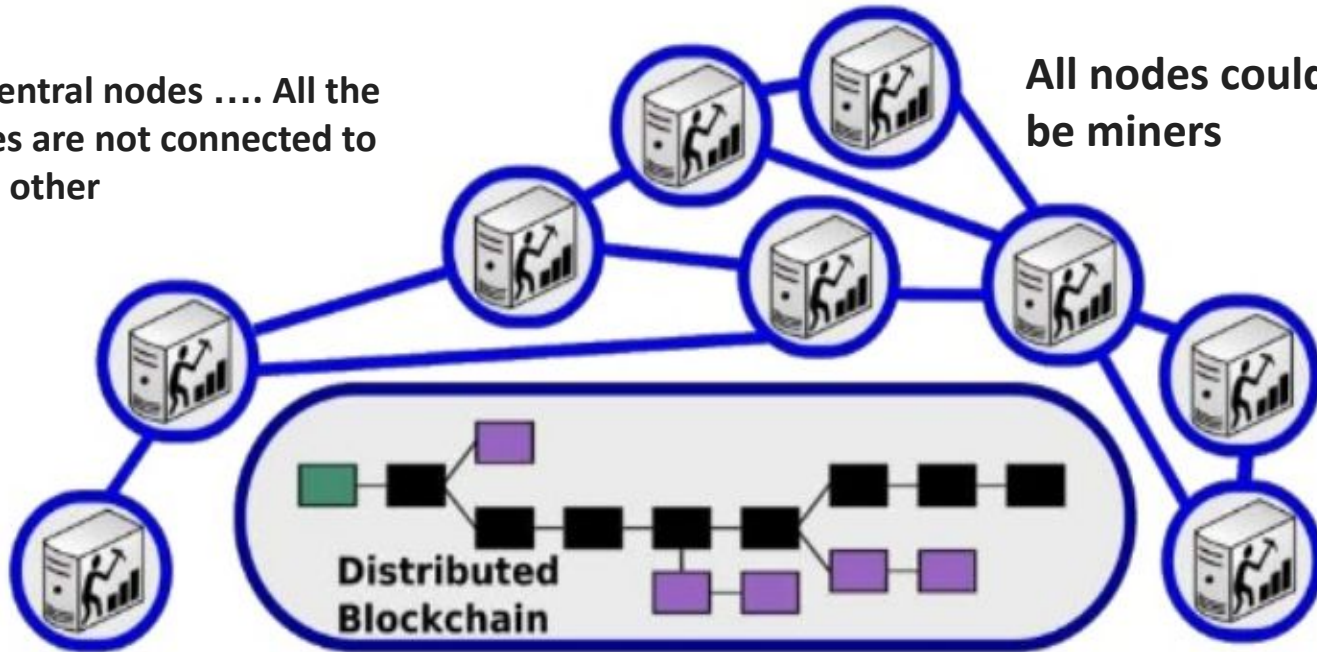
- Creation of a virtual coin/note
 - How is it created in the first place?
 - How do you prevent inflation? (What prevents anyone from creating lots of coins?)
- Validation
 - Is the coin legit? (proof-of-work)
 - How do you prevent a coin from double-spending?
- Buyer and Seller protection in online transactions
 - Buyer pays, but the seller doesn't deliver
 - Seller delivers, buyer pays, but the buyer makes a claim.
- Trust on third-parties
 - Rely on “proof of work” instead of trust
 - Verifiable by everyone – blockchain is visible to all
 - No central bank or clearing house



- > The blockchain network is a **peer-to-peer network** of independent nodes communicating together by message broadcasting.

No central nodes All the nodes are not connected to each other

All nodes could be miners



- > A node is not necessarily connected to every other node, but at least some of them.

How Blockchain Works

Here are five basic principles underlying the technology.

1. Distributed Database

- Each party on a blockchain has access to the entire database and its complete history.
- No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.

2. Peer-to-Peer Transmission

- Communication occurs directly between peers instead of through a central node.
- Each node stores and forwards information to all other nodes.

3. Transparency with Pseudonymity

- Every transaction and its associated value are visible to anyone with access to the system. (**public key**)
- Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. (**private key**)
- Users can choose to remain anonymous or provide proof of their identity to others. (**signatures**) Transactions occur between blockchain addresses.

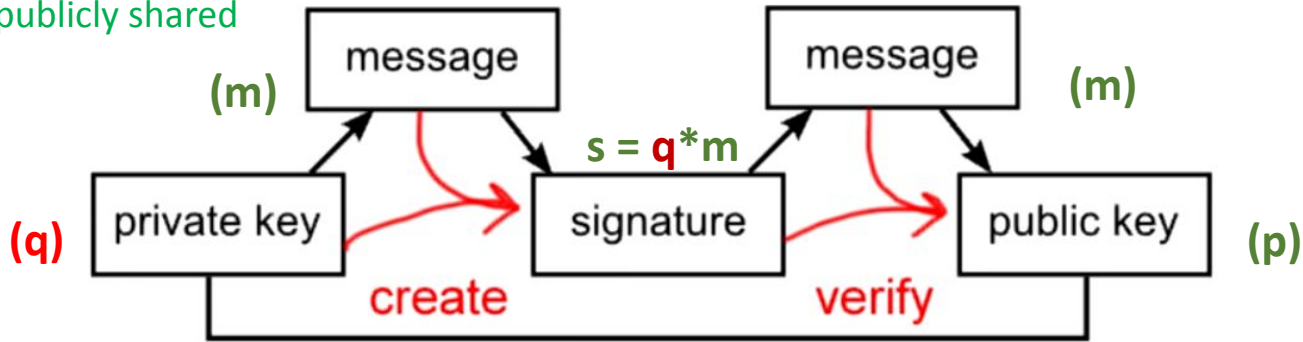
4. Irreversibility of Records

- Once a transaction is entered in the database and the accounts are updated, the records cannot be altered, **because they're linked to every transaction record that came before them (hence the term "chain")**.
- **Various computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.**

5. Computational Logic

- The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed.
- **users can set up algorithms and rules that automatically trigger transactions between nodes.**
 - **Data Security**
 - **Keys**
 - **Signatures**
 - **Hashing**
 - **Redundancy**
 - **Improved workflow**

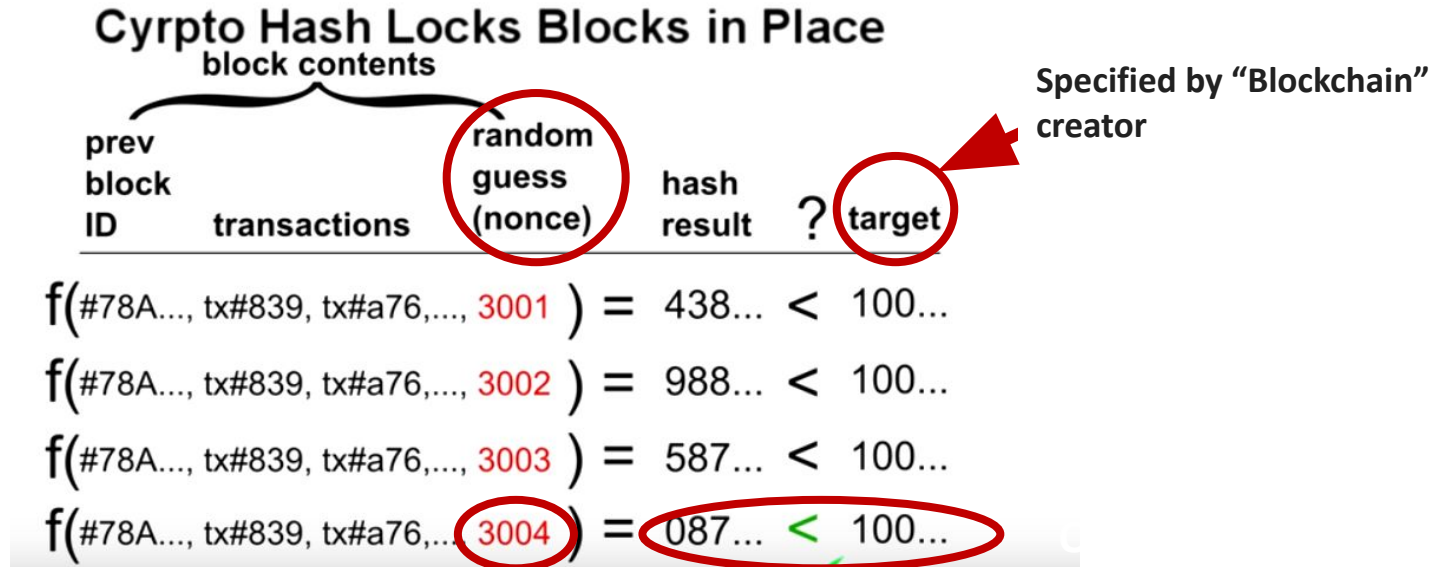
p = public key
 q = private key
 $p * q = N$ also publicly shared
 m = message



signature = $f(\text{message}, \text{private key})$ **unique** for every transaction

Verify = $f(\text{signature}, \text{message}, \text{public key}) = \{ \text{true or false} \}$

solving a block involves trying to get the cryptographic hash of the block to be below a certain value, and you do that by trying different random numbers . Once solved, the hash output is like a fingerprint that uniquely identifies that block. If even a single character in the block is changed, the block's hash would be completely different



The Merge is approaching, and comes with changes to Ethereum. [More on The Merge](#)



ಇಥಿರಿಯಾಂ

Welcome to Ethereum

Ethereum is the community-run technology powering the cryptocurrency ether (ETH) and thousands of decentralized applications.

Explore Ethereum

Compared to Bitcoin

- Ethereum and Bitcoin both share Byzantine fault-tolerant consensus algorithm for synchronization of state updates
- Ethereum and Bitcoin are both peer-to-peer networks
- Ethereum and Bitcoin both use cryptographic primitives such as digital signatures and hashes
- Ethereum and Bitcoin both use the concept of a digital currency. (Ether and Bitcoins)
- Ethereum has a general purpose programmable blockchain that runs a virtual machine capable of executing arbitrary code of unbounded complexity.
- Bitcoin's Script language is limited and restricted to true/false evaluations of spending conditions.

Ethereum's Components

- P2P network
- Consensus rules
- Transactions
- State machine
- Data structures
- Consensus algorithm
- Economic security
- Clients

Transaction History

- Since the blockchain is a public ledger of all transactions, it can be viewed by anyone
- Blockchain transactions can be viewed online through websites like etherscan
- Blockchain transactions can be viewed offline if you possess the Ethereum blockchain on your hard drive and use a client like Geth or other popular wallet software
- Since transactions are public, there have been privacy concerns regarding wallet activity and thus it's suggested to have balances spread around

DApps and the Third Age of the Internet

- Ethereum started as a general-purpose blockchain that soon became a platform for programming DApps.
- A DApp is composed of at least:
 - Smart contracts on a blockchain
 - A web frontend user interface
- In addition, many DApps include other decentralized components such as:
 - A decentralized storage protocol and platform
 - A decentralized messaging protocol and platform
- You may see DApps spelled as ÐApps, The Ð character is the Latin character called “ETH” alluding to Ethereum
- The third age of the Internet, or “web 3” is a rejection of centralized systems and the acceptance of decentralized systems for the serving of applications

INTRODUCTION TO SMART CONTRACTS



Last edit: [@minimalsm](#) ↗, July 11, 2022

[See contributors](#)

WHAT IS A SMART CONTRACT?

A "smart contract" is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain.

What is a Smart Contract?

- There are two types of contracts in Ethereum
 - Externally owned accounts (EOA) - Controlled by users with wallet software
 - Contract accounts - Controlled by program code (called smart contracts) executed by the Ethereum Virtual Machine
- A smart contract was defined by Nick Szabo (the cryptographer that coined the term) as a “set of promises, specified in digital form, including protocols within which the parties perform on the other promises”
- Smart contracts are immutable computer programs that run deterministically in the context of an Ethereum Virtual Machine as part of the Ethereum network protocol on the decentralized Ethereum world computer

Programming in Solidity

- Selecting a Solidity Compiler and Language version - Programming smart contracts in Solidity requires the programmer to pay close attention to the Solidity compiler version and language version. Solidity development is still ongoing and its syntax is constantly changing, so compilers in later versions might not be able to compile smart contracts written for older versions of the language
- While backwards-compatibility is not guaranteed, a smart contract can be written for an older version of solidity and still exist in the Ethereum blockchain, however, older versions of the Solidity language may be prone to security exploits



Non-fungible tokens (NFT)

- A way to represent anything unique as an Ethereum-based asset.
- NFTs are giving more power to content creators than ever before.
- Powered by smart contracts on the Ethereum blockchain.

What's an NFT?

NFTs are tokens that we can use to represent ownership of unique items. They let us tokenise things like art, collectibles, even real estate. They can only have one official owner at a time and they're secured by the Ethereum blockchain – no one can modify the record of ownership or copy/paste a new NFT into existence.

NFT stands for non-fungible token. Non-fungible is an economic term that you could use to describe things like your furniture, a song file, or your computer. These things are not interchangeable for other items because they have unique properties.

Fungible items, on the other hand, can be exchanged because their value defines them rather than their unique properties. For example, ETH or dollars are fungible because 1 ETH / \$1 USD is exchangeable for another 1 ETH / \$1 USD.

Source: <https://ethereum.org/en/nft/>

An NFT internet

NFTs are digitally unique, no two NFTs are the same.

Every NFT must have an owner and this is of public record and easy for anyone to verify.

NFTs are compatible with anything built using Ethereum. An NFT ticket for an event can be traded on every Ethereum marketplace, for an entirely different NFT. You could trade a piece of art for a ticket!

Content creators can sell their work anywhere and can access a global market.

Creators can retain ownership rights over their own work, and claim resale royalties directly.

Items can be used in surprising ways. For example, you can use digital artwork as collateral in a decentralised loan.

The internet today

A copy of a file, like an .mp3 or .jpg, is the same as the original.

Ownership records of digital items are stored on servers controlled by institutions – you must take their word for it.

Companies with digital items must build their own infrastructure. For example an app that issues digital tickets for events would have to build their own ticket exchange.

Creators rely on the infrastructure and distribution of the platforms they use. These are often subject to terms of use and geographical restrictions.

Platforms, such as music streaming services, retain the majority of profits from sales.

Hello World Code 1 - GitHub

<https://github.com/magonicolas/Ethereum-Solidity/blob/master/HelloWorld.sol>

```
pragma solidity ^0.4.0;
```

```
contract HelloWorldContract {  
    string word = 'Hello World';
```

```
    function getWord() constant returns(string) {  
        return word;  
    }  
}
```

```
    function setWord(string newWord) returns(string) {  
        word = newWord;  
        return word;  
    }  
}
```

Lab/Demo - Create Wallet and NFT collection

Create and sell your NFTs



Set up your wallet

Once you've set up your wallet of choice, connect it to OpenSea by clicking the wallet icon in the top right corner. Learn about the [wallets we support](#).



Create your collection

Click [My Collections](#) and set up your collection. Add social links, a description, profile & banner images, and set a secondary sales fee.



Add your NFTs

Upload your work (image, video, audio, or 3D art), add a title and description, and customize your NFTs with properties, stats, and unlockable content.



List them for sale

Choose between auctions, fixed-price listings, and declining-price listings. You choose how you want to sell your NFTs, and we help you sell them!

Setup Metamask Wallet

<https://opensea.io/blog/guides/intro-to-crypto-walle>

Intro to Crypto Wallets

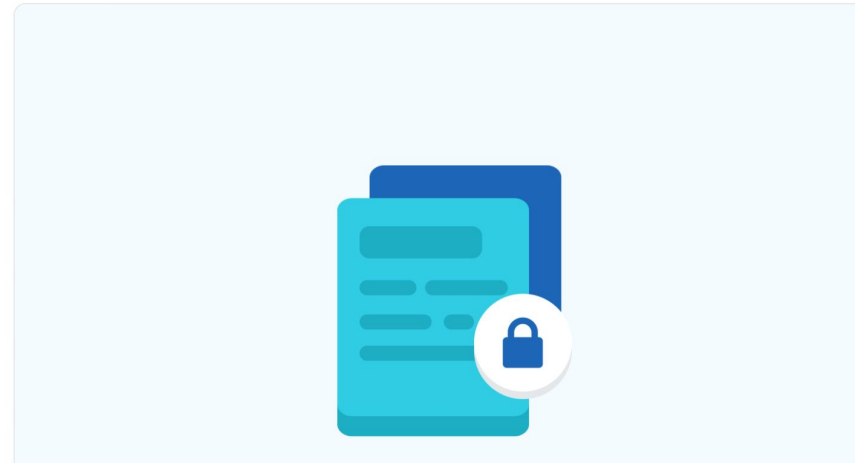
March 29, 2022 · By Edric Barnes · Guide



<https://opensea.io/blog/learn/how-to-easily-setup-a-metamask-wallet/>

How to Easily Setup a MetaMask Wallet

March 18, 2022 · By Gideon Welles · Learn



Sign up for OpenSea and Connect with Wallet



OpenSea

🔍 Search items, collections, and accounts

[Explore](#) [Stats](#)

Connect your wallet.

If you don't have a [wallet](#) yet, you can select a provider and create one now.



MetaMask

Popular

Use Wallet to authenticate and authorize NFT

Tutorial -

<https://support.opensea.io/hc/en-us/articles/360063498313-How-do-I-create-an-NFT->

How do I create an NFT?

Creating an NFT on OpenSea is easy! This guide explains how to set up your first NFT.

Setting up your first NFT collection

On OpenSea, click the **Create** tab in the top right corner.

Explore

Stats

Resources

Create

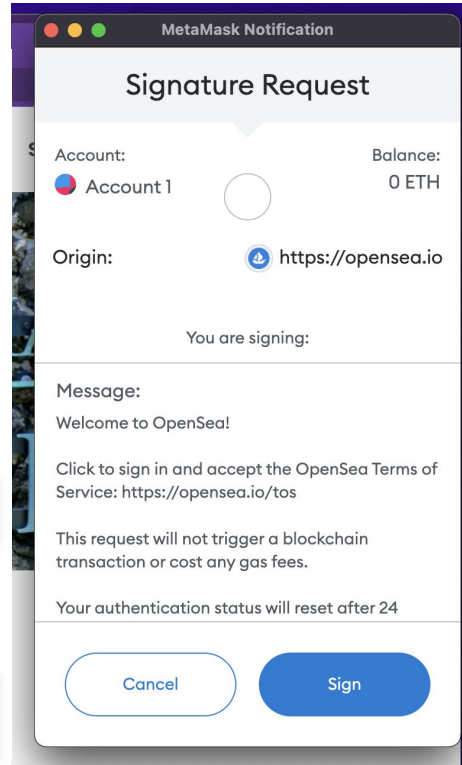


You'll be taken to the NFT item creation page, where you can upload your NFT file, name it, and add a description.

Create new item

Image, Video, Audio, or 3D Model

File types supported: JPG, PNG, GIF, SVG, MP4, WEBM, MP3, WAV, OGG, GLB, GLTF. Max size: 40 MB



Fill in the blanks to create a new NFT!

Create New Item

* Required fields

Image, Video, Audio, or 3D Model *

File types supported: JPG, PNG, GIF, SVG, MP4, WEBM, MP3, WAV, OGG, GLB, GLTF. Max size: 100 MB



Name *

External link

OpenSea will include a link to this URL on this item's detail page, so that users can click to learn more about it. You are welcome to link to your own webpage with more details.

Description

The description will be included on the item's detail page underneath its image. [Markdown](#) syntax is supported.

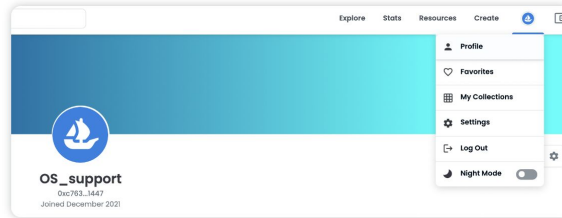
How to list and sell NFTs - Fixed Price, Auctions

Tutorial -
<https://support.opensea.io/hc/en-us/articles/360063498333-How-do-I-sell-an-NFT->

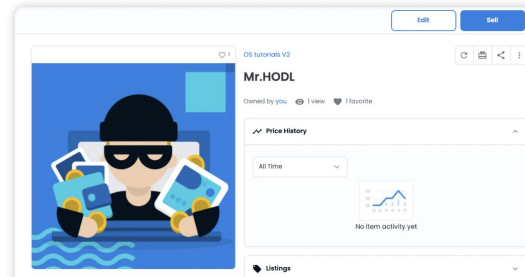
Selling an NFT using OpenSea

On OpenSea, navigate to the top right of the page and click your **profile icon**.

Select the NFT you would like to sell from your wallet. If you don't have an NFT available to sell, check out our [create an NFT tutorial](#) to get started.

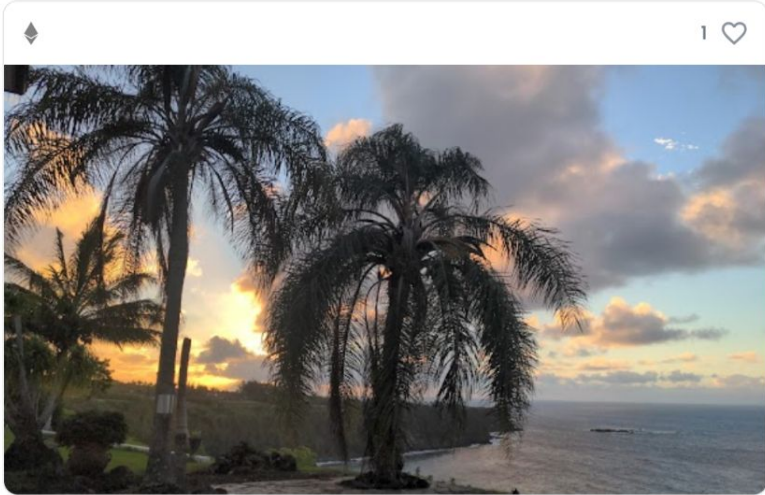


On the top right of the item page, click **Sell**.



Edit

Sell



1 

North Shore Maui Collection



Uaou Bay 6

Owned by [you](#)  4 views  1 favorite

Price History

All time 



No item activity yet

 Description

By [you](#)



North Shore Maui Collection

Uaoa Bay 6



Accept card payments to make it easier for others to purchase your NFTs.

List item for sale

Type



\$ Fixed Price	🕒 Timed Auction
--------------------------	---------------------------

Price



ETH ▼	Amount
------------------------------------------	--------

Duration

📅 1 month

[More options](#) ▼

Fees




Service Fee
Creator Fee

2.5%
2.5%

Complete listing

Preview



North Shore Maui Collection

Uaoa Bay 6

Price

🔼 0



UNIVERSITY of HAWAII®
MAUI COLLEGE



Questions, Comments,
Feedback?!

Debasis Bhattacharya JD, DBA
debasisb@hawaii.edu
maui.hawaii.edu/cybersecurity