

Introduction
to Bitcoins,
Blockchains,
Ethereum,
Smart
Contracts
and NFTs



UNIVERSITY of HAWAII®
MAUI COLLEGE



Debasis Bhattacharya (debasisb@hawaii.edu)
<http://maui.hawaii.edu/cybersecurity/>

Supported by National Convergence Tech Center
and NSF Award # 1700562

July 26, 2022

Agenda

- Background
- Basics of Crypto
 - Bitcoins
 - Blockchains
 - Ethereum
 - Smart Contracts
 - NFTs
- Lab and Demonstration
 - Creating your first Smart Contract
 - Creating NFTs on Open Sea
- Lessons Learned
- Q&A



Background - College

- University of Hawaii Maui College
 - Serves Maui County - islands of Maui, Molokai and Lanai
 - 165,000 or so resident population
 - 2 Million or so tourists per year (pre-Covid)
 - Dropped 95% after March 2020!
 - Currently, ther
 - 2000+ full-time commuter students
 - 20 or so Associate Degrees
 - 2 Baccalaureate Degrees
 - 60% or so women students
 - Median age of students ~26 years
 - Non-traditional students
 - Commuter island college



Cybersecurity Education - Traditional

- Certificates in Cybersecurity
 - Low Level - Intro, Network+, Security+
 - Higher Level - Ethical Hacking, Forensics
- Internships
 - Government, banks, utilities
- Baccalaureate Degree
 - Applied Business and Info Tech (ABIT)
 - ABIT BAS is a NSA/DHS CAE-CDE program
 - Cybersecurity courses are embedded
- Cyber competitions and Workshops
 - NSA GenCyber, US AFA CyberPatriot
- Supported by NSF Grants
 - ATE Program Award# 1700562



Cybersecurity Education across Disciplines

- Cybersecurity education cuts across various segments
 - Community College program disciplines
 - Gender
 - Minorities
 - Background - high schools, professionals, returning veterans etc
 - Applicable to various programs
 - Accounting, Allied Health, Administration of Justice, Electronics, Tourism etc.
- One size education does not fit all types of students!
- Supported by NSF
 - ATE Grant, Award# 1700562
 - SFS Capacity Building Grant, Award# 1437514



Cybersecurity Education – During Covid-19!

- Online education via Zoom!
 - Students were engaged as they felt safe
 - Higher attendance in classes
- Lab sessions
 - Difficult without a physical space and equipment
 - Students need to rely on their Internet connectivity
 - Cloud assignments required students to log in from their homes
- Hands-on activities - Fun Stuff in a Remote, Online Environment!
 - Creating NFTs on OpenSea.io
 - Lock Picking Activities
 - Pen Testing Tools from www.Hak5.org
 - USB Rubber Ducky – writing Ducky Scripts
 - Bash Bunny - Pen testing tool to emulate various devices
 - LAN Turtle – Provides stealth remote shell access

Bitcoin.org needs your support!



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

[Get started with Bitcoin](#)

[Choose your wallet](#)

[Buy Bitcoin](#)



What is Bitcoin?



Currencies - Online Transactions

- Physical cash
 - Non-traceable (well, mostly!)
 - Secure (mostly)
 - Low inflation
 - Fiat Currency – legal tender whose value is backed by a government
 - Note that since 1971, the US\$ has no backing with gold!
 - Cryptocurrencies are not fiat currencies!
 - Physical currencies can't be used online directly
- Electronic credit or debit transactions
- ◆ Bank sees all transactions
 - ◆ Merchants can track/profile customers
 - ◆ Cryptocurrencies are not associated with any bank or regulatory agency!

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:
 - \$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 and speculative.

Bitcoin Transactions

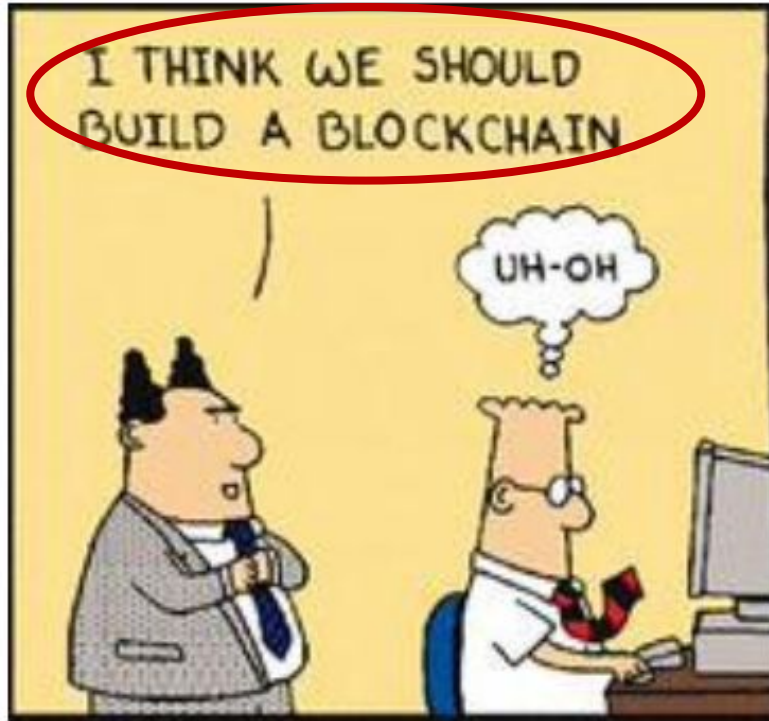


Bitcoin Network

- 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



S. Adams E-mail: SCOTTADAMS@AOL.COM



11/17 © 1995 United Feature Syndicate, Inc. (NYC)

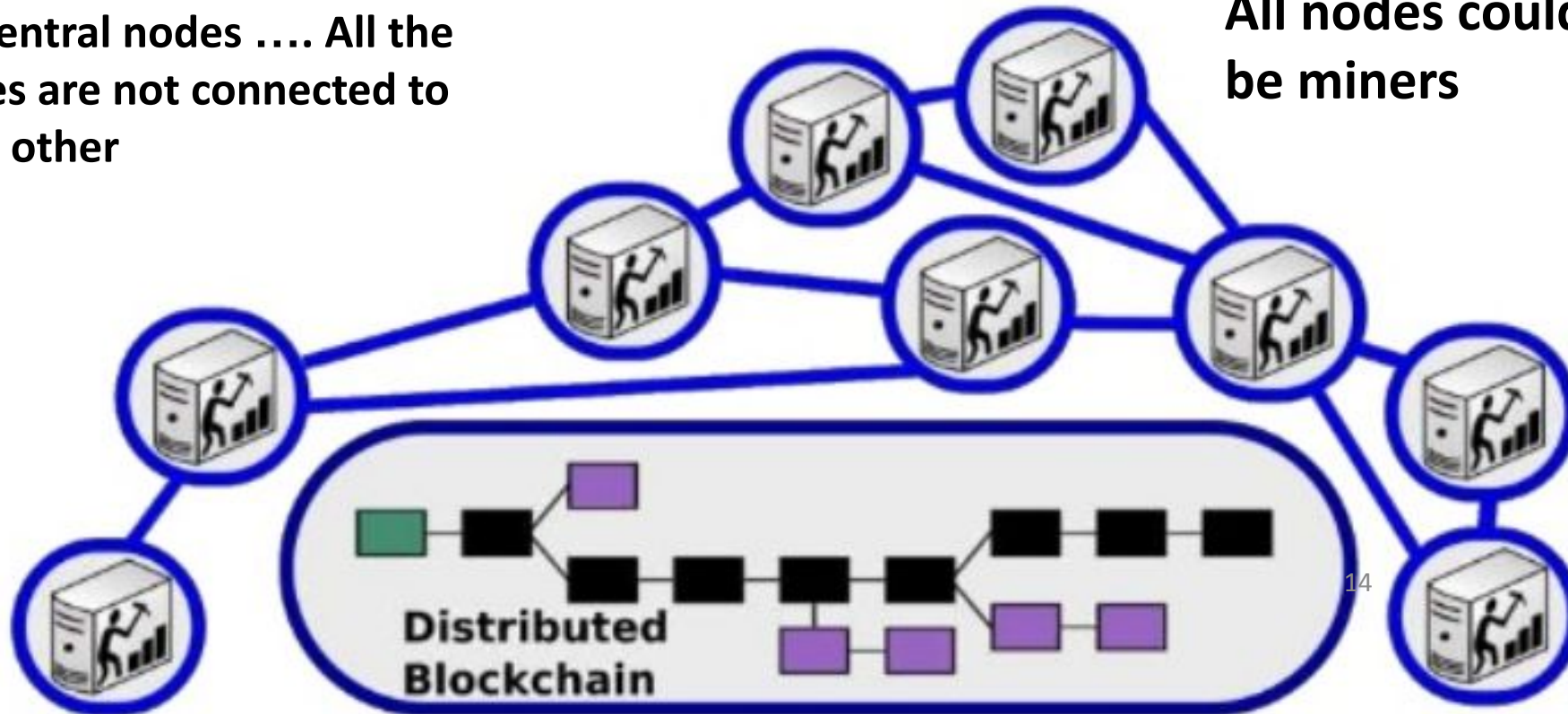


Blockchain Process... Decentralization

- > 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")**. 16
- **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.**

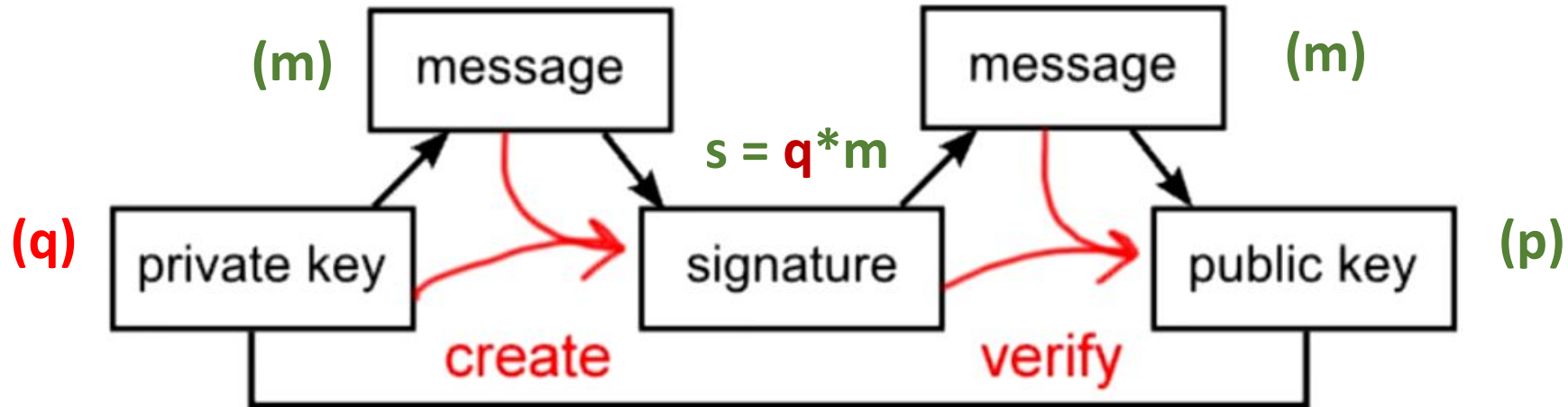
- **Data Security**
 - **Keys**
 - **Signatures**
 - **Hashing**
- **Redundancy**
- **Improved workflow**

p = public key

q = private key

p*q = N also publicly shared

m = message

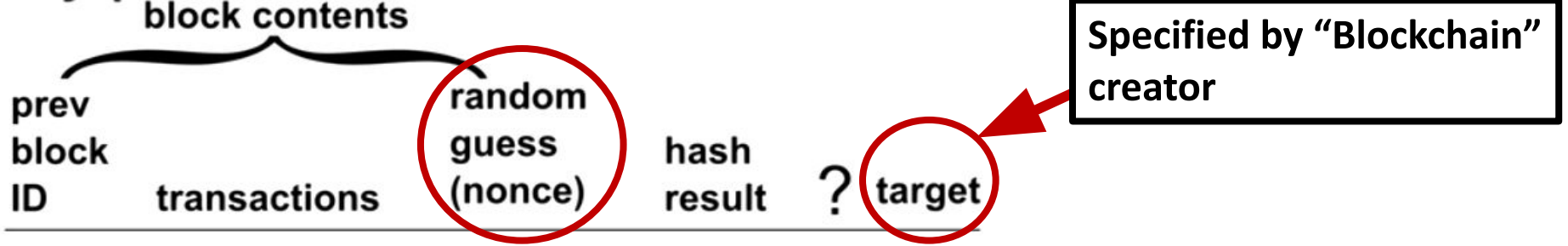


signature = f(message, private key)unique for every transaction

Verify = f(signature, message, public key) = { 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

Cyrpto Hash Locks Blocks in Place



$$f(\#78A\dots, tx\#839, tx\#a76\dots, 3001) = 438\dots < 100\dots$$

$$f(\#78A\dots, tx\#839, tx\#a76\dots, 3002) = 988\dots < 100\dots$$

$$f(\#78A\dots, tx\#839, tx\#a76\dots, 3003) = 587\dots < 100\dots$$

$$f(\#78A\dots, tx\#839, tx\#a76\dots, 3004) = 087\dots < 100\dots$$

OK to proceed

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



ಇಥಿರಿಯಾಂಸ್

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

Ether Currency Units

- Called ether (Ethereum is the system, ether is the currency)
- Symbols: ETH, Ξ , 
- The smallest unit of ether is known as wei
- 1 Ether = 1×10^{18} wei (1 quintillion wei)
- 1 Babbage = 10^3 wei
- 1 Lovelace = 10^6 wei
- 1 Shannon = 10^9 wei
- 1 Szabo = 10^{12} wei
- 1 Finney = 10^{15} wei
- 1 Grand = 10^{21} wei = 10^3 Ether

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: [@minimalism](#) , 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

Compiling with the Solidity Compiler (solc)

Now, we will use the Solidity compiler on the command line to compile our contract directly. The Solidity compiler solc offers a variety of options, which you can see by passing the `--help` argument.

We use the `--bin` and `--optimize` arguments of solc to produce an optimized binary of our example contract:

```
$ solc --optimize --bin Faucet.sol
===== Faucet.sol:Faucet =====
Binary:
6060604052341561000f57600080fd5b60cf8061001d6000396000f300606060405260043610603e5
763fffffffff7c010000000000000000000000000000000000000000000000000000006000350416
632e1a7d4d81146040575b005b3415604a57600080fd5b603e60043567016345785d8a00008111156
06357600080fd5b73ffffffffffffffffffffffffffffffffffffffff331681156108fc0282604051
600060405180830381858888f19350505050151560a057600080fd5b505600a165627a7a723058203
556d79355f2da19e773a9551e95f1ca7457f2b5fbbf4eacf7748ab59d2532130029
```

The result that solc produces is a hex-serialized binary that can be submitted to the Ethereum blockchain.

The Ethereum Contract ABI

In computer software, an *application binary interface* is an interface between two program modules; often, between the operating system and user programs. An ABI defines how data structures and functions are accessed in *machine code*; this is not to be confused with an API, which defines this access in high-level, often human-readable formats as *source code*. The ABI is thus the primary way of encoding and decoding data into and out of machine code.

In Ethereum, the ABI is used to encode contract calls for the EVM and to read data out of transactions. The purpose of an ABI is to define the functions in the contract that can be invoked and describe how each function will accept arguments and return its result.

A contract's ABI is specified as a JSON array of function descriptions (see [Functions](#)) and events (see [Events](#)). A function description is a JSON object with fields `type`, `name`, `inputs`, `outputs`, `constant`, and `payable`. An event description object has fields `type`, `name`, `inputs`, and `anonymous`.

We use the solc command-line Solidity compiler to produce the ABI for our *Faucet.sol* example contract:

```
$ solc --abi Faucet.sol
===== Faucet.sol:Faucet =====
Contract JSON ABI
[{"constant":false,"inputs":[{"name":"withdraw_amount","type":"uint256"}], \
"name":"withdraw","outputs":[],"payable":false,"stateMutability":"nonpayable", \
"type":"function"}, {"payable":true,"stateMutability":"payable", \
"type":"fallback"}]
```

Gas considerations

- Gas, described earlier, is an incredibly important consideration in smart contract programming. Gas is a resource constraining the maximum amount of computation that Ethereum will allow a transaction to consume.
- If the gas limit is exceeded during computation, the following series of events occurs:
 - An “out of gas” exception is thrown
 - The state of the contract prior to execution is restored (reverted)
 - All ether used to pay for the gas is taken as a transaction fee, it is not refunded
- Because gas is paid by the user who initiated the transaction, users are discouraged from calling functions that have a high gas cost. Thus, a programmer’s best interest is to minimize the gas cost of a contract’s functions.



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.

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.



OpenSea

🔍 Search items, collections, and accounts

Discover, collect, and sell extraordinary NFTs
















OpenSea is the world's first and largest NFT marketplace

Explore

Create

▶ [Learn more about OpenSea](#)

Top collections over last 24 hours ▼ On July 23, 2022

1		The Potatoz Floor price: \blacklozenge 0.84	-31.66%	\blacklozenge 1,144.96
2		Otherdeed for Others... Floor price: \blacklozenge 2.4	-0.01%	\blacklozenge 488.01
3		Isekai Meta Floor price: \blacklozenge 0.4	+256.05%	\blacklozenge 441.91
4		Mutant Ape Yacht Cl... Floor price: \blacklozenge 17.29	+3.62%	\blacklozenge 337.41
5		MysticsUniverse Floor price: \blacklozenge 0.17	—	\blacklozenge 309.45
6		Panda of kungfu pix ... Floor price: \blacklozenge 0.2	—	\blacklozenge 302.56
7		CryptoPunks Floor price: —	+7.77%	\blacklozenge 282
8		Bored Ape Yacht Club Floor price: \blacklozenge 91.88	-58.22%	\blacklozenge 276.89
9		Lady Ape Club Floor price: \blacklozenge 1.18	+47.31%	\blacklozenge 254.01
10		FrootsNFT Floor price: \blacklozenge 7.77	-50.27%	\blacklozenge 9,065.55
11		Casual Sloths Official Floor price: \blacklozenge 0.23	+1,170.04%	\blacklozenge 233.92
12		META KONGZ OFFICIAL Floor price: \blacklozenge 1.52	+56.5%	\blacklozenge 185.51
13		Moonbirds Oddities Floor price: \blacklozenge 1.54	-52.99%	\blacklozenge 183.44
14		KIKI - XxEBLIRVxW Floor price: \blacklozenge 1.2	+24.4K%	\blacklozenge 6,123.99
15		Art Blocks Curated Floor price: —	-29.61%	\blacklozenge 156.27

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

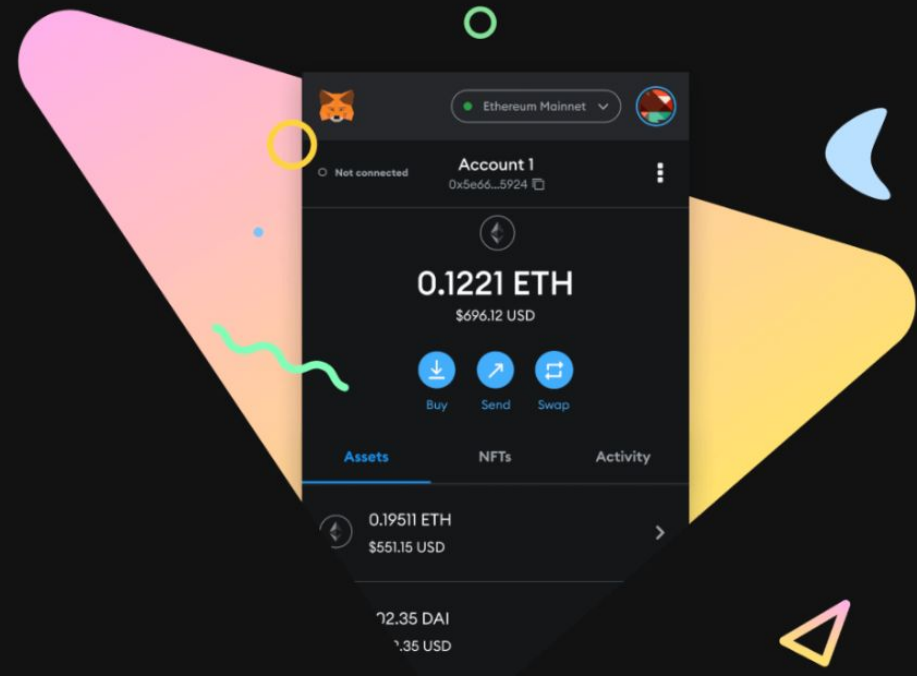
Choose between auctions, fixed-price listings, and declining-price listings. You choose how you want to sell your NFTs, and we help you sell them!



A crypto wallet & gateway to blockchain apps

Start exploring blockchain applications in seconds. Trusted by over 30 million users worldwide.

Download for 





OpenSea

Search items, collections, and accounts



Bored Ape Yacht Club



By YugaLabs

The Bored Ape Yacht Club is a collection of 10,000 unique Bored Ape NFTs— unique digital collectibles living on the Ethereum blockchain. Your Bored Ape doubles as your Yacht Club membership card, and grants access to members-only benefits, the first of which is access to THE BATHROOM, a collaborative graffiti board. Future areas and perks can be unlocked by the community through roadmap activation. Visit www.BoredApeYachtClub.com for more details.

See less ^

10.0K items

6.5K owners

640.4K total volume

91.88 floor price

85.31 best offer

Collected 6 Created Favorited Activity More



Search by name

Recently received



Uaou Bay 6
North Shore Maui Collection



Uaou Bay 5
North Shore Maui Collection



Uaou Bay 4
North Shore Maui Collection



Uaou Bay 3
North Shore Maui Collection



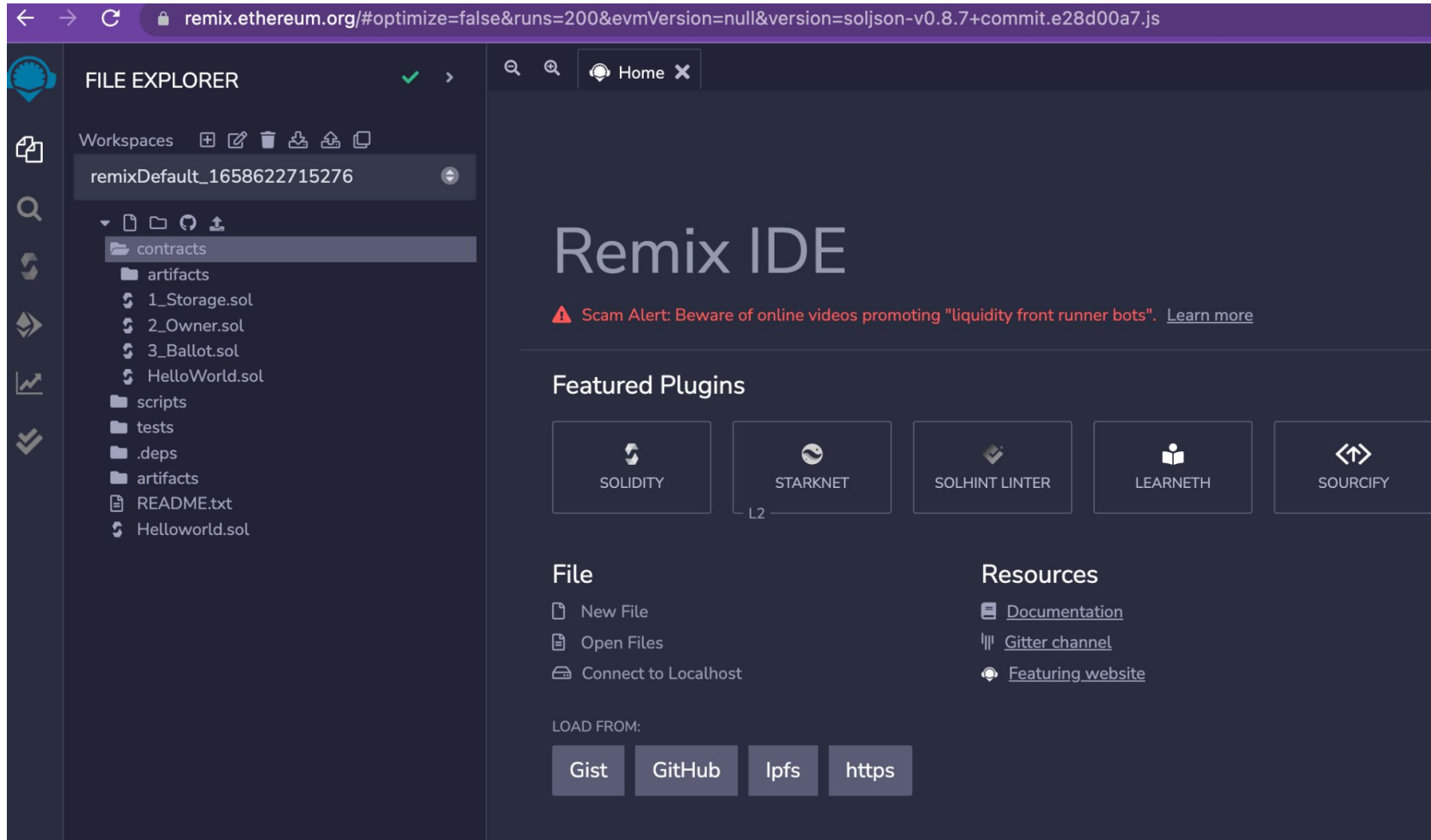
Uaou Bay 2
North Shore Maui Collection



Uaou Bay 1
North Shore Maui Collection

Lab/Demo - Remix IDE, Solidity Compiler and Code

<https://remix.ethereum.org>



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';
```

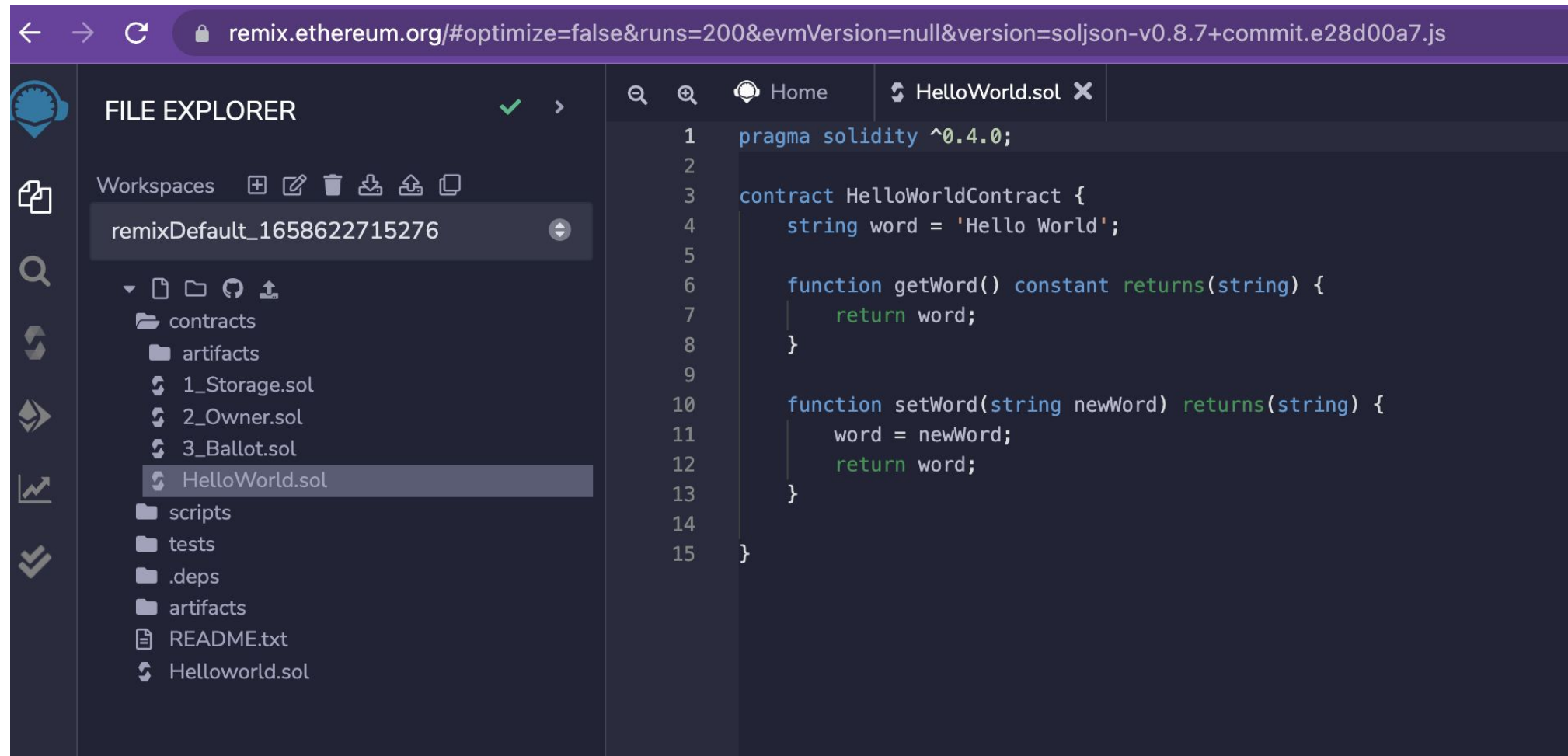
```
    function getWord() constant returns(string) {  
        return word;  
    }
```

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

Hello World Code 2

```
pragma solidity >= 0.4.22 <0.6.0;
contract Mortal{
    address owner;
    constructor() public {
        owner = msg.sender;
    }
    function die() public {
        if(msg.sender == owner)
            selfdestruct(msg.sender);
    }
}
contract Helloworld is Mortal{
    string output = "Hello, World!";
    function printHello() public view returns (string memory) {
        return output;
    }
}
```

Cut and Paste Hello World Code into Remix

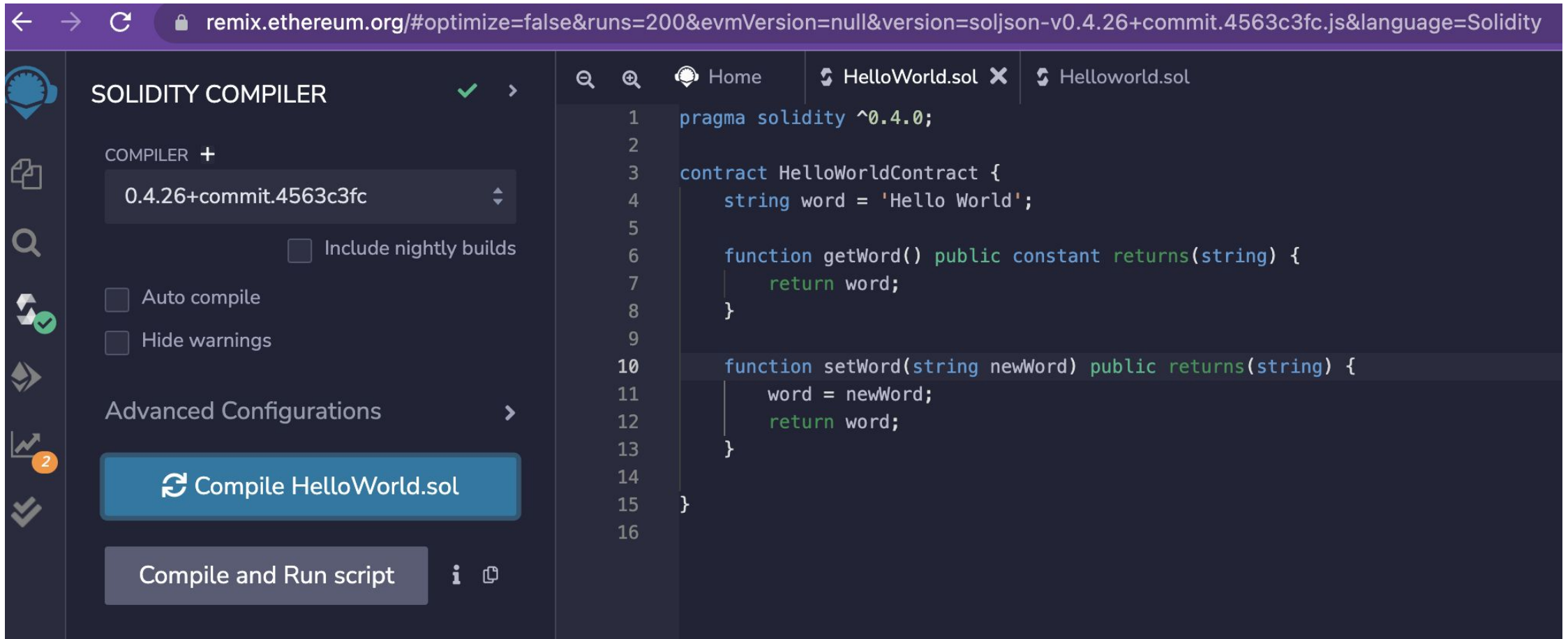


The screenshot displays the Remix IDE interface. The browser address bar shows the URL: `remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.7+commit.e28d00a7.js`. The interface is divided into three main sections:

- FILE EXPLORER (Left Panel):** Shows a workspace named `remixDefault_1658622715276`. The file tree includes folders for `contracts`, `scripts`, and `tests`, and files for `artifacts`, `1_Storage.sol`, `2_Owner.sol`, `3_Ballot.sol`, `>HelloWorld.sol` (highlighted), `README.txt`, and `Helloworld.sol`.
- Editor (Right Panel):** Displays the Solidity code for `HelloWorldContract`. The code is as follows:

```
1 pragma solidity ^0.4.0;
2
3 contract HelloWorldContract {
4     string word = 'Hello World';
5
6     function getWord() constant returns(string) {
7         return word;
8     }
9
10    function setWord(string newWord) returns(string) {
11        word = newWord;
12        return word;
13    }
14
15 }
```
- Top Panel:** Shows the Remix logo, a search icon, and tabs for `Home` and `HelloWorld.sol`.

Compile Solidity Code (use Public Function)



The screenshot displays the Remix Ethereum IDE interface. The browser address bar shows the URL: `remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.4.26+commit.4563c3fc.js&language=Solidity`. The left sidebar contains the "SOLIDITY COMPILER" panel, which is currently set to version "0.4.26+commit.4563c3fc". Below the version selector, there are checkboxes for "Include nightly builds", "Auto compile", and "Hide warnings", all of which are unchecked. A large blue button labeled "Compile HelloWorld.sol" is visible, along with a smaller button for "Compile and Run script". The main editor area shows the following Solidity code:

```
1 pragma solidity ^0.4.0;
2
3 contract HelloWorldContract {
4     string word = 'Hello World';
5
6     function getWord() public constant returns(string) {
7         return word;
8     }
9
10    function setWord(string newWord) public returns(string) {
11        word = newWord;
12        return word;
13    }
14 }
15
16
```

Deploy and Run Code, use Functions Set/Get

The screenshot displays the Remix IDE interface. On the left, the 'DEPLOY & RUN TRANSACTIONS' panel is active, showing the following configuration:

- ENVIRONMENT: Remix VM (London)
- ACCOUNT: 0x5B3...eddC4 (99.9999999%)
- GAS LIMIT: 3000000
- VALUE: 0 Wei
- CONTRACT: HelloWorldContract - contracts/Hello

The 'Deploy' button is highlighted in orange. Below it, there is an option to 'Publish to IPFS' (unchecked) and an 'OR' section with 'At Address' and 'Load contract from Address' buttons. A 'Transactions recorded' section shows 3 transactions. The 'Deployed Contracts' section shows a contract named 'HELLOWORLDCONTRACT AT 0XD9' with two functions: 'setWord' (highlighted in orange) and 'getWord'. The 'setWord' function is currently set to 'Hello World'. Below the function list, the output shows '0: string: Hello World'.

On the right, the Solidity code editor shows the following code:

```
1 pragma solidity ^0.4.0;
2
3 contract HelloWorldContract {
4     string word = 'Hello World';
5
6     function getWord() public constant returns(string) {
7         return word;
8     }
9
10    function setWord(string newWord) public returns(string) {
11        word = newWord;
12        return word;
13    }
14 }
15
16
```

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

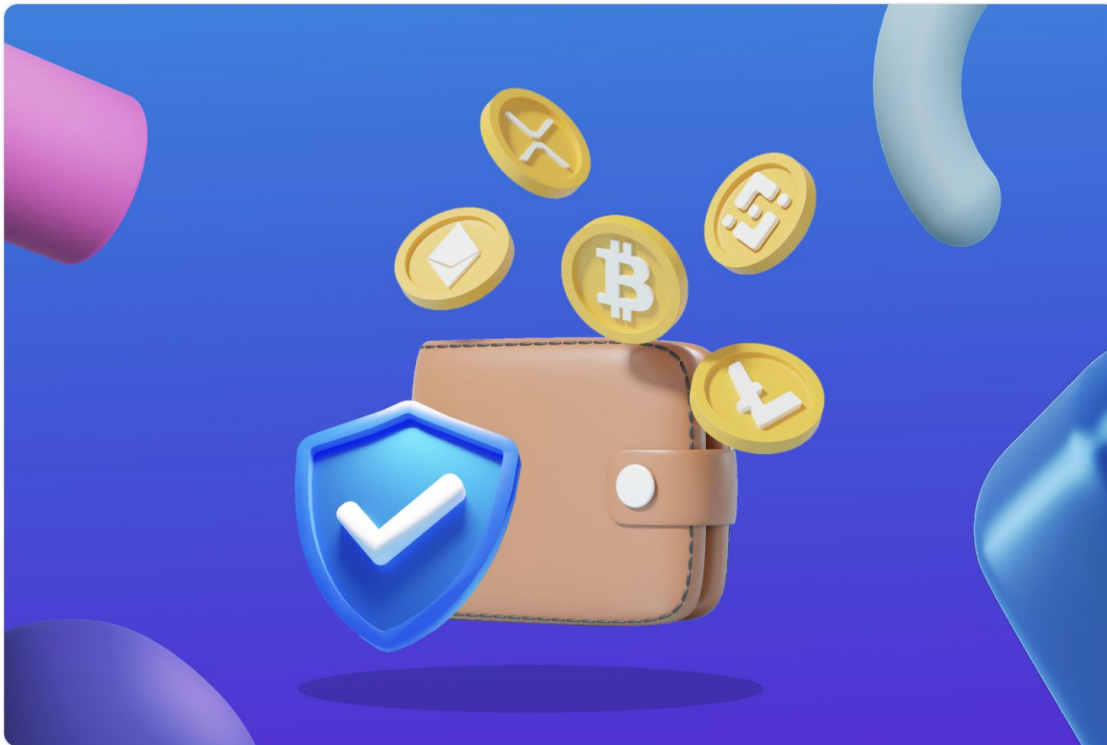
Choose between auctions, fixed-price listings, and declining-price listings. You choose how you want to sell your NFTs, and we help you sell them!

Setup Metamask Wallet

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

Intro to Crypto Wallets

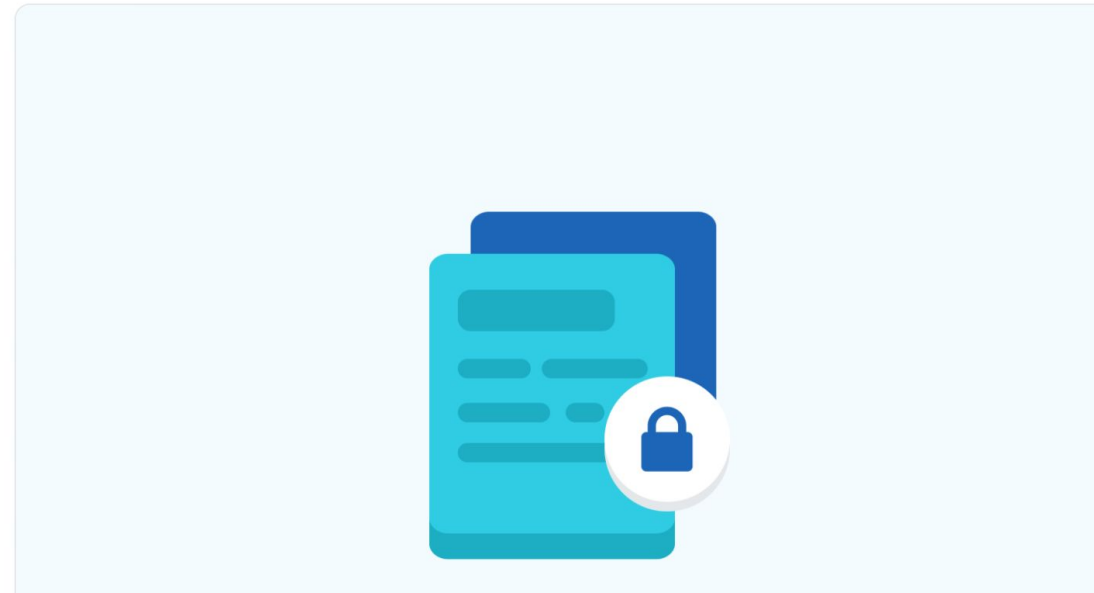
March 29, 2022 By Edric Barnes · Guide



<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 -

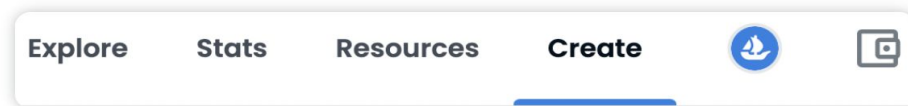
<https://support.opensea.io/hc/en-us/articles/360063498313-How-do-I-create-an-NFT->

How do I create an NFT?

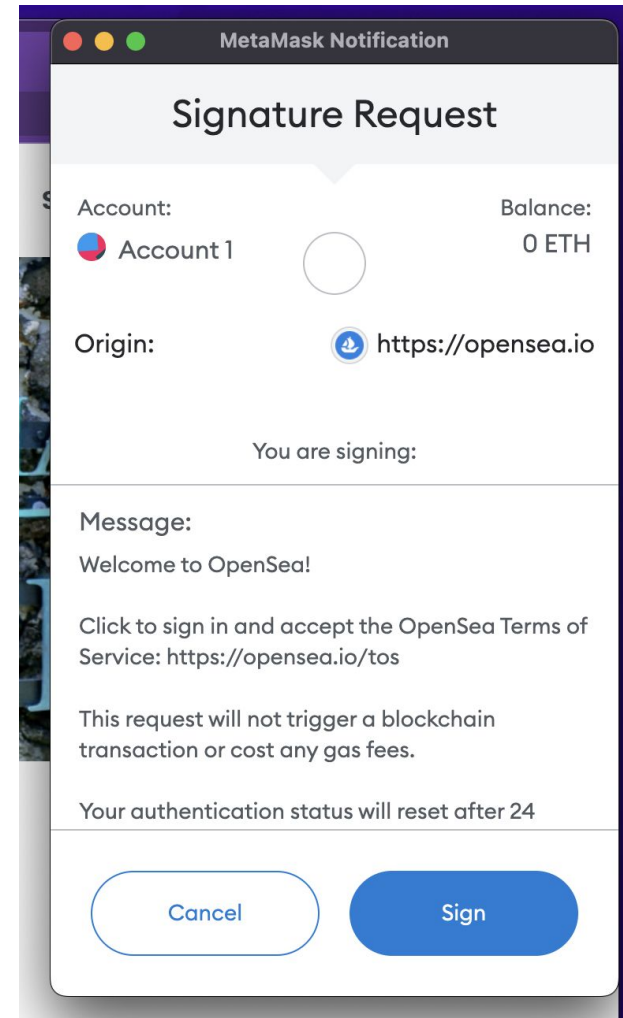
Creating an NFT on OpenSea is easy! This guide explains how to set up your first NFT.

Setting up your first NFT collection

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



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



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.

Lazy Minting!

Source:

<https://support.opensea.io/hc/en-us/articles/1500003076601-Can-I-list-an-item-without-paying-to-mint-it->

Can I list an item without paying to "mint" it?

The new OpenSea collection manager allows creators to make NFTs without any upfront [gas cost](#), as the NFT isn't transferred on-chain until the first purchase or transfer is made.

NFTs made with the Collection Manager follow the [ERC-1155 standard](#), partly to help with gas-free minting and partly to help us add exciting features in the near future.

If this is your [first listing on OpenSea](#) you'll need to pay gas fees associated with initializing your account.

For more information on lazy minting, check out this [helpful resource](#) created by our co-founder, Alex!

Wrapped Ethereum (WETH) - buy/sell with auctions

Source:
<https://support.opensea.io/hc/en-us/articles/360063498293-What-s-WETH-How-do-I-get-it->

The screenshot shows a mobile application interface for buying crypto with a card. The title is "Buy crypto with card" with a close button (X). Below the title are two tabs: "Deposit crypto" (selected with a downward arrow) and "Buy ETH with card" (selected with a card icon). The main content area is titled "Buy ETH" and includes a menu icon (three horizontal lines). Under "Buy ETH", there is a section "I want to spend" with a text input field containing "300" and a currency dropdown menu showing "USD" with a US flag icon and a downward arrow. Below this is a "Summary" section with a refresh icon and the text "Quote updates in 9s". The summary text reads "You get 0.1854 ETH for \$304.17" with a downward arrow. At the bottom of the form is a large blue button labeled "Continue" with a right-pointing arrow. Below the button is the text "By continuing you agree to our cookie policy." and the "Powered by MoonPay" logo.

How to list and sell NFTs - Fixed Price, Auctions

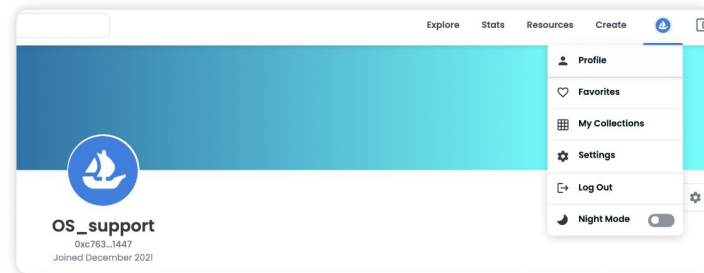
Tutorial -

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

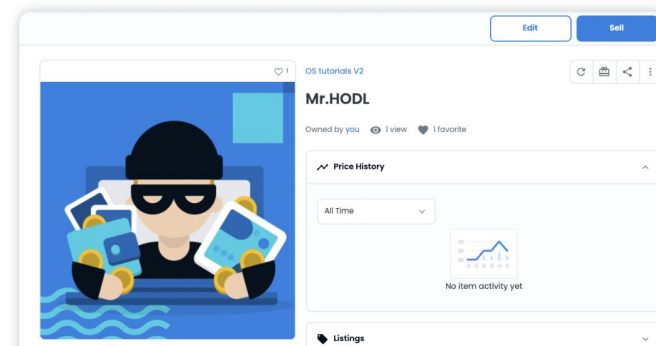
Selling an NFT using OpenSea

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



Uaoa Bay 6

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

Price History

All time 



No item activity yet

 Description

By you



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

List item for sale

Type



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

Price



📌 ETH

Duration

📅 1 month

[More options](#) ▾

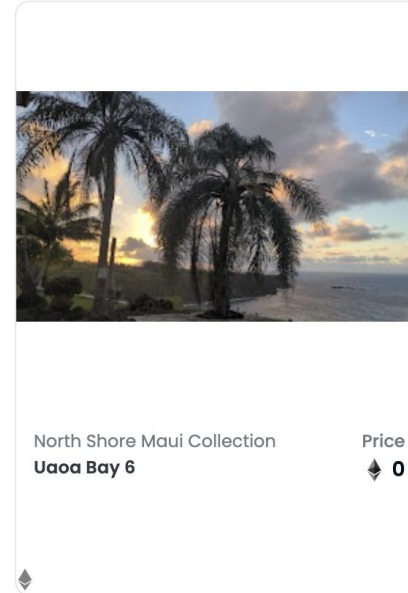
Fees



Service Fee	2.5%
Creator Fee	2.5%

Complete listing

Preview



Online Cybersecurity Education – Lessons Learned!

- Online education via Zoom!
 - Students feel safe
 - Students learn the theory
 - Students have to provide their own Internet connectivity and laptops
- Lab sessions
 - Cloud labs work, assuming they are free and no credit cards needed
 - Lab modules need to be transferred to a cloud environment
 - Students have to know about the cloud environment
- Hands-on activities – key to engagement!
 - Crypto and NFTs
 - Lockpicking
 - Pen Testing Tools from www.Hak5.org
- Students learn to adapt and survive...



Questions? Comments? Feedback?!

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



UNIVERSITY of HAWAII®
MAUI COLLEGE