FTEC 5520 – Week 7

Agenda – Cryptocurrencies technology and Lab exercise – Week 7

1. Decentralized Apps

2. Online Wallets, Exchanges

3. Initial Token Offerings

Decentralized Existing Services

Services that are traditionally centralized can be decentralized using Ethereum. This will lead to reduced costs and fees by connecting individuals directly and removing 3rd parties.

Imagine a service like Uber or eBay without a company in the middle collecting fees!

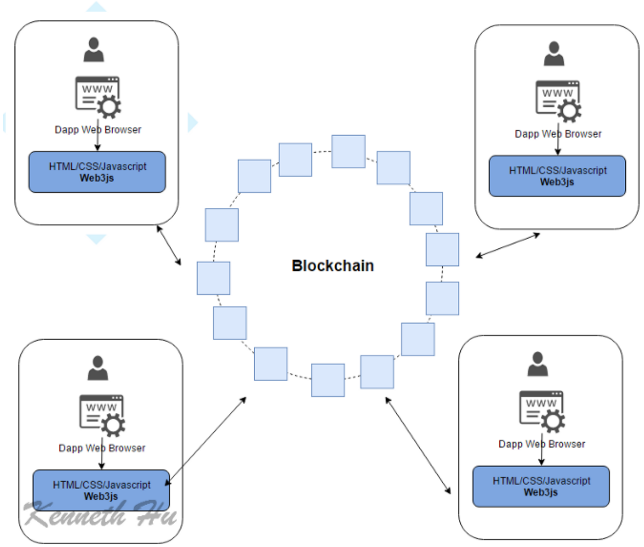
Decentralized Applications (DApps)

A DApp is an application whose core logic resides in smart contracts and where the code is accessible to the users (typically as open-source).

A DApp, like a normal app, can have frontend code and user interfaces that interact with its backend through an API. The frontend can be hosted as a website on a centralized server

A DApp is composed of at least:

- Smart contracts on a blockchain. Smart contracts sit on the blockchain, waiting for a sender to send in an input.
- A web frontend user interface



Decentralized Applications (DApps)

A DApp has its backend code running on a decentralized peer-to-peer network. Contrast this with an app where the backend code is running on centralized servers.

A DApp can have its frontend code written in any programming language that makes API calls to its backend.

DApp is a decentralized application, that is, a more reliable and secure system for storing and managing any type of data.

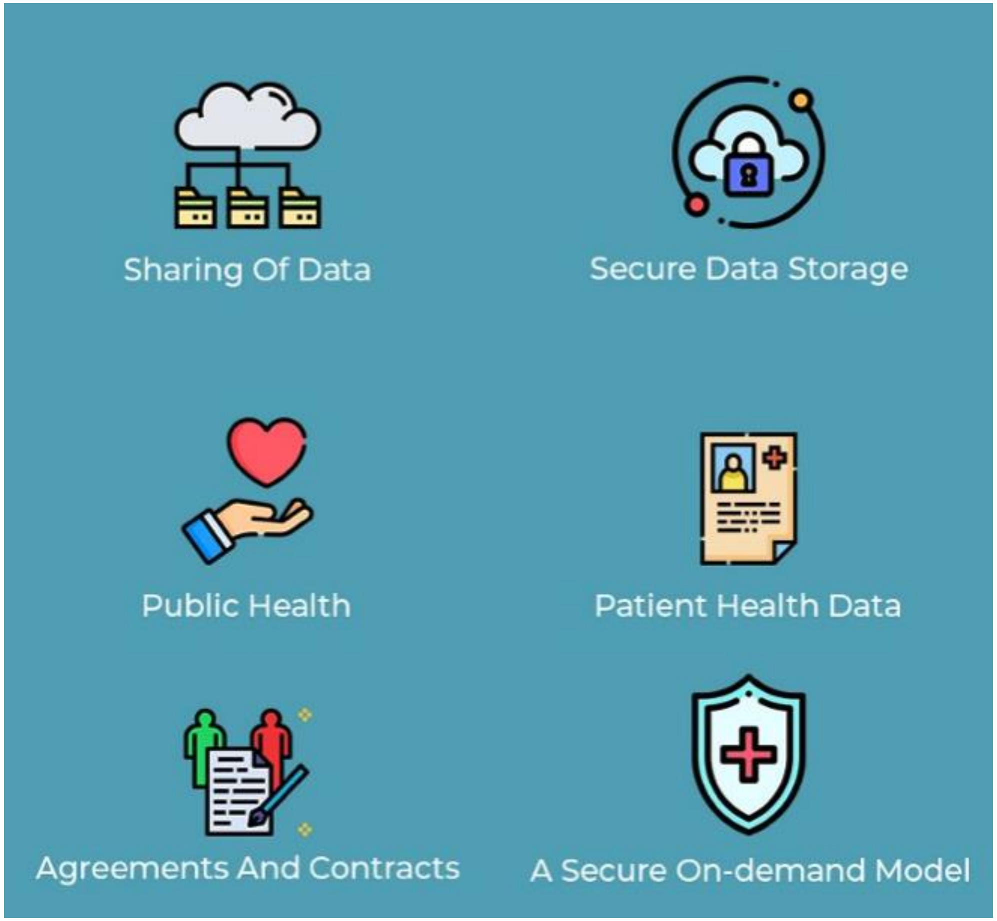
Unlike other apps, there is no central ownership or managing body.

All the users of the app maintain the app.

Any new addition or change is made through mutual consent. A copy of the app gets stored in the computers of all the users.

Bitcoin is probably the first dApp which runs on the Blockchain. It is a dApp for financial transactions.

Benefits of using DApps in Healthcare



Dapp framework

Truffle

- An Ethereum development maintained by ConsenSys

Embark

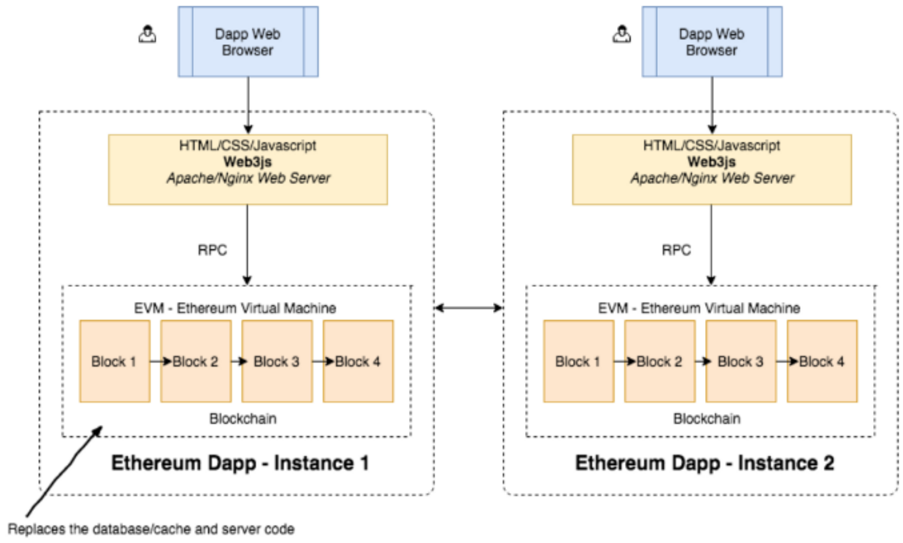
- A framework for serverless Decentralized Applications using Ethereum, IPFS and other platforms

Populus

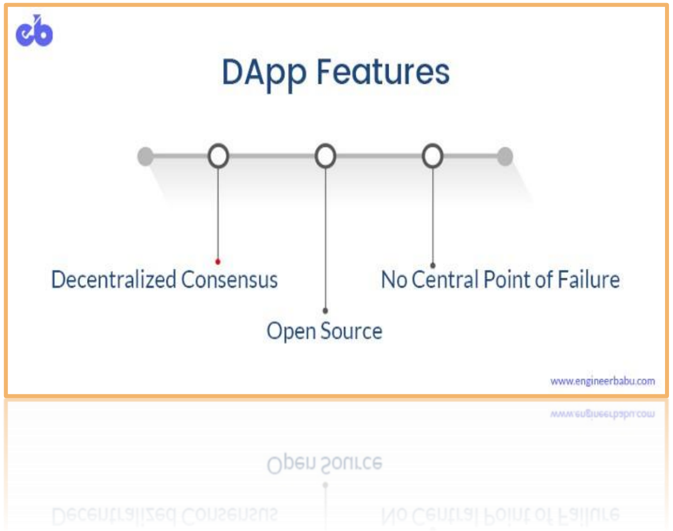
- A smart contract development framework for the Ethereum blockchain

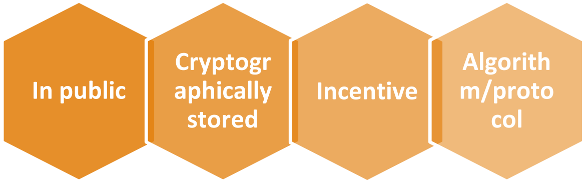
Ethereum Dapps Architecture (example)

The purpose for decentralisation is to not rely on a centralised server. So, the community has come up with solutions (hosted blockchain servers, metamask etc.)



Decentralized Applications (DApps)




In public

Cryptographically stored

Incentive

Algorithm/protocol

Dapps Classification

- Financial Blockchain Applications
  - E.g. Bitcoin, Altcoins
- Semi-financial Blockchain Applications
  - E.g. Insurance Application, ICO,
- Fully Functioning DApps
  - Applications for online voting or decentralized governance

What can be decentralized ?

- Backend software (app logic)
- Frontend software
- Data storage
- Message communications
- Name resolution

Decentralized Applications (DApps)

Token Distribution Mechanisms

Mining

- works on the consensus principle and it allows the maximum number of tokens to be distributed to the people who contribute the most of their work to the operation of the application

Fundraising

- a method to raise money for the initial development of the application. This is carried out with the help of ICO, Initial Coin Offering process
- People are presented with the app idea through a white paper, website, and proof of concepts and if they seem convinced with it

Development

- tokens are generated by utilizing a predefined mechanism.
- tokens are available only for the development of the DApp

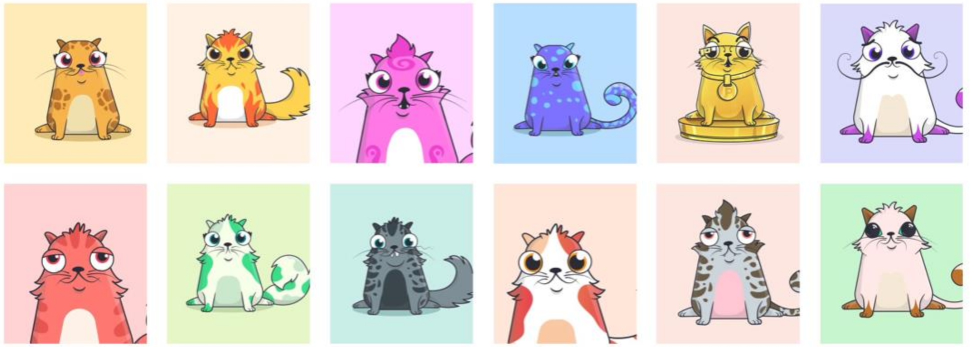
> Bitcoin allows token distribution in the form of rewards when miners solve a mathematical problem by using their computing power to verify a transaction and maintain the Bitcoin blockchain.

Decentralized Applications (DApps)

CryptoKitties has done a great job of demonstrating what blockchains can be used for beyond just simple financial transactions.

It's basically a game for buying, selling, and breeding digital cats. Each cat has a unique appearance that is defined by its genes, and when you breed 2 cats together, their genes combine in a unique way to produce an offspring, which you can then breed or sell.

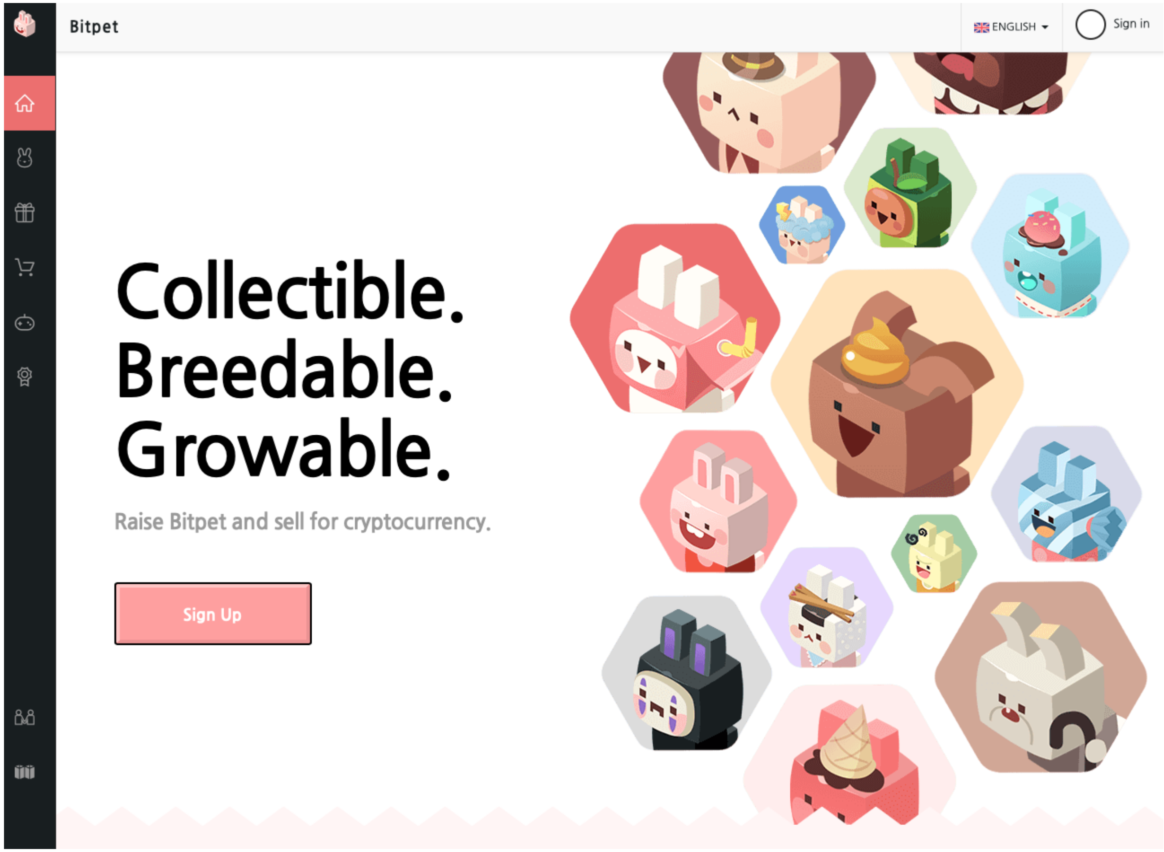
CryptoKitties conforms to the the ERC721 token spec, a non-fungible token type that lends itself really well to tracking ownership of digital collectables like digital playing cards or rare items in an MMORPG.



https://ethfiddle.com/09YbyJRfiI?source=post_page-----7c8ac86a4eb3---------------------

https://www.youtube.com/watch?v=3PTstAK-cH8

Decentralized Applications (DApps) Example



Bitpet

ENGLISH

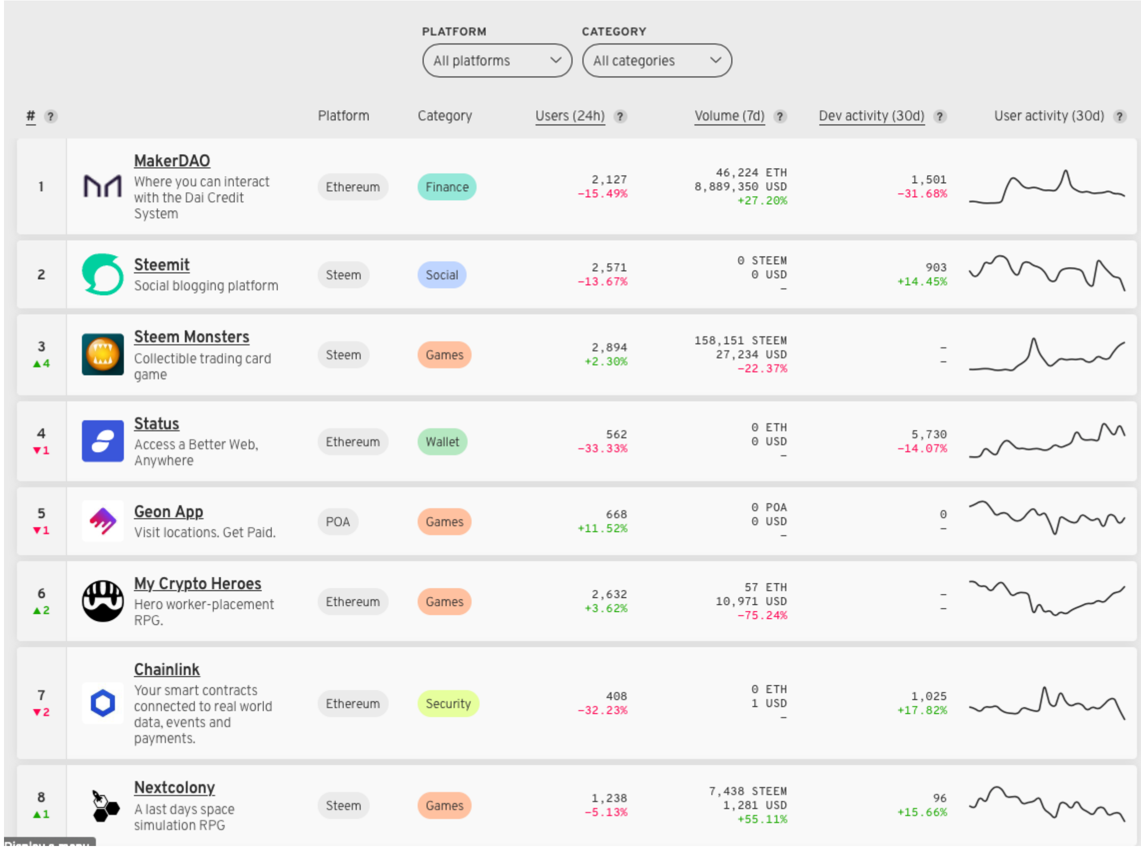
Sign in

Collectible.
Breedable.
Growable.

Raise Bitpet and sell for cryptocurrency.

Sign Up

State of the DApps Ranking



PLATFORM: All platforms

CATEGORY: All categories

#		Platform	Category	Users (24h)	Volume (7d)	Dev activity (30d)	User activity (30d)
1	**MakerDAO** Where you can interact with the Dai Credit System	Ethereum	Finance	2,127 -15.49%	46,224 ETH 8,889,350 USD +27.20%	1,501 -31.68%	
2	**Steemit** Social blogging platform	Steem	Social	2,571 -13.67%	0 STEEM 0 USD -	903 +14.45%	
3 ▲4	**Steem Monsters** Collectible trading card game	Steem	Games	2,894 +2.30%	158,151 STEEM 27,234 USD -22.37%	- -	
4 ▼1	**Status** Access a Better Web, Anywhere	Ethereum	Wallet	562 -33.33%	0 ETH 0 USD -	5,730 -14.07%	
5 ▼1	**Geon App** Visit locations. Get Paid.	POA	Games	668 +11.52%	0 POA 0 USD -	0 -	
6 ▲2	**My Crypto Heroes** Hero worker-placement RPG.	Ethereum	Games	2,632 +3.62%	57 ETH 10,971 USD -75.24%	- -	
7 ▼2	**Chainlink** Your smart contracts connected to real world data, events and payments.	Ethereum	Security	408 -32.23%	0 ETH 1 USD -	1,025 +17.82%	
8 ▲1	**Nextcolony** A last days space simulation RPG	Steem	Games	1,238 -5.13%	7,438 STEEM 1,281 USD +55.11%	96 +15.66%	

https://www.stateofthedapps.com/rankings

Major Investors Live Dapps Status (2018)

Dapp	Key Investors	Raised	Market Cap.	Peak	Current	% Drop
CryptoKitties	A16Z, DCG	$12Mn	-	14194	510	-96
Bancor	Blockchain Capital	$153Mn	$82Mn	1747	457	-74
Kyber Network	Julian Sarokin	$49Mn	$57Mn	422	165	-61
Numerai	Fred Ehrsam, USV	$7.5Mn	$8.4Mn	419	14	-97
AirSwap	B.Pierce, M.Novogratz	$36Mn	$12Mn	172	45	-74
Decentraland	DCG	$25Mn	$70Mn	163	23	-86
LivePeer	DCG, Pantera	-	-	46	33	-28

Comparison between DApps and normal Apps

Silo Apps	DApps
Can be shut down	Cannot be shut down
Have downtime	No downtime
Owned and managed by computer user	Not owned by anyone
Can be upgraded	Cannot be upgraded or altered

Can Smart Contract and DApps be changed?

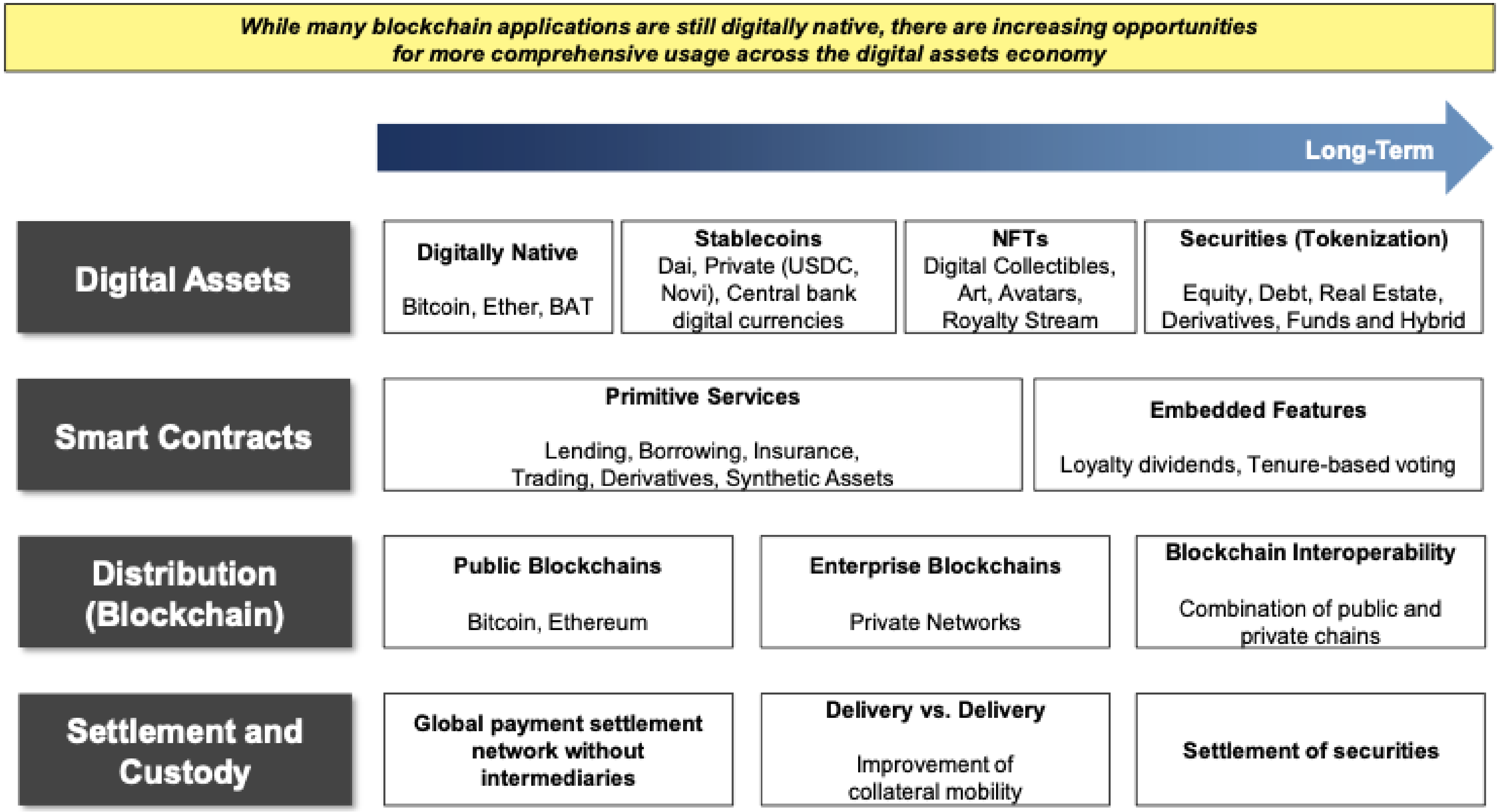
Smart Contract is code that deployed in the network that deals with elements of the DApp that need provability, immutability.

DApp is made of smart contracts and additional framework. So elements that stored in servers outside the blockchain and smart contract can be changed.

One of the main ideas behind decentralized applications is that the way they work cannot be altered. Once they have been deployed, they should be almost impossible to take down.

Crypto-Token (or Token)

Digital Assets Economy



While many blockchain applications are still digitally native, there are increasing opportunities for more comprehensive usage across the digital assets economy

Digital Assets

- **Digitally Native**
Bitcoin, Ether, BAT
- **Stablecoins**
Dai, Private (USDC, Novi), Central bank digital currencies
- **NFTs**
Digital Collectibles, Art, Avatars, Royalty Stream
- **Securities (Tokenization)**
Equity, Debt, Real Estate, Derivatives, Funds and Hybrid

Smart Contracts

- **Primitive Services**
Lending, Borrowing, Insurance, Trading, Derivatives, Synthetic Assets
- **Embedded Features**
Loyalty dividends, Tenure-based voting

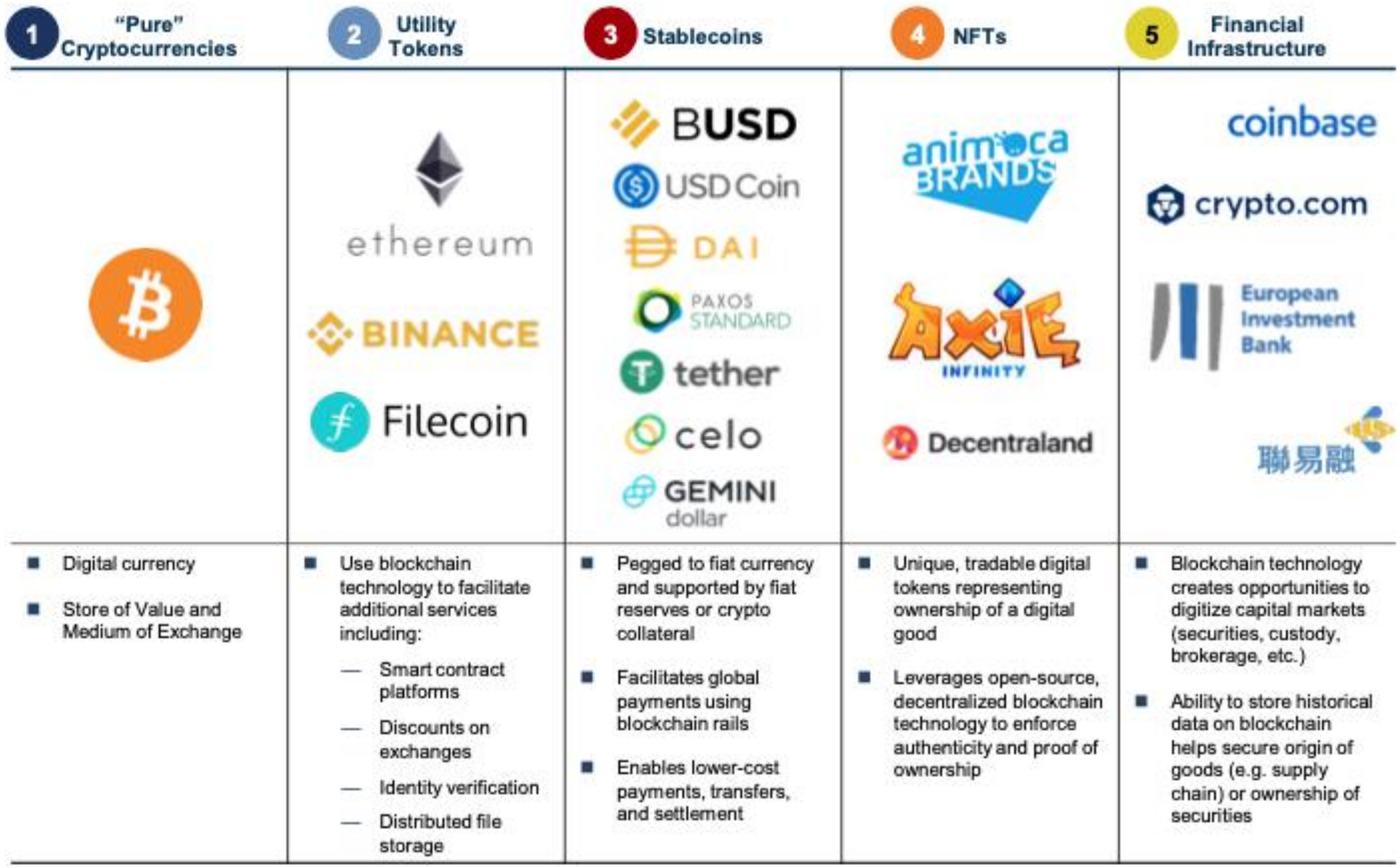
Distribution (Blockchain)

- **Public Blockchains**
Bitcoin, Ethereum
- **Enterprise Blockchains**
Private Networks
- **Blockchain Interoperability**
Combination of public and private chains

Settlement and Custody

- **Global payment settlement network without intermediaries**
- **Delivery vs. Delivery**
Improvement of collateral mobility
- **Settlement of securities**

Different types of Crypto-Token



1 "Pure" Cryptocurrencies	2 Utility Tokens	3 Stablecoins	4 NFTs	5 Financial Infrastructure
	ethereum BINANCE Filecoin	BUSD USD Coin DAI PAXOS STANDARD tether celo GEMINI dollar	animoca BRANDS Axie INFINITY Decentraland	coinbase crypto.com European Investment Bank 聯易融
■ Digital currency ■ Store of Value and Medium of Exchange	■ Use blockchain technology to facilitate additional services including: — Smart contract platforms — Discounts on exchanges — Identity verification — Distributed file storage	■ Pegged to fiat currency and supported by fiat reserves or crypto collateral ■ Facilitates global payments using blockchain rails ■ Enables lower-cost payments, transfers, and settlement	■ Unique, tradable digital tokens representing ownership of a digital good ■ Leverages open-source, decentralized blockchain technology to enforce authenticity and proof of ownership	■ Blockchain technology creates opportunities to digitize capital markets (securities, custody, brokerage, etc.) ■ Ability to store historical data on blockchain helps secure origin of goods (e.g. supply chain) or ownership of securities

What is “Token”

A token is a representation of value, such as an asset (monetary value or data) or identity.

Tokens are created and conferred through contractual agreements defined by the underlying company, institution, industry or protocol

Digitalization and the demand for a more flexible medium of exchange have caused tokens to rapidly evolve in response.

Tokens will do more than replace fiat currency, and will drive the decentralization of finance as well as new asset creation models.

Token Standard

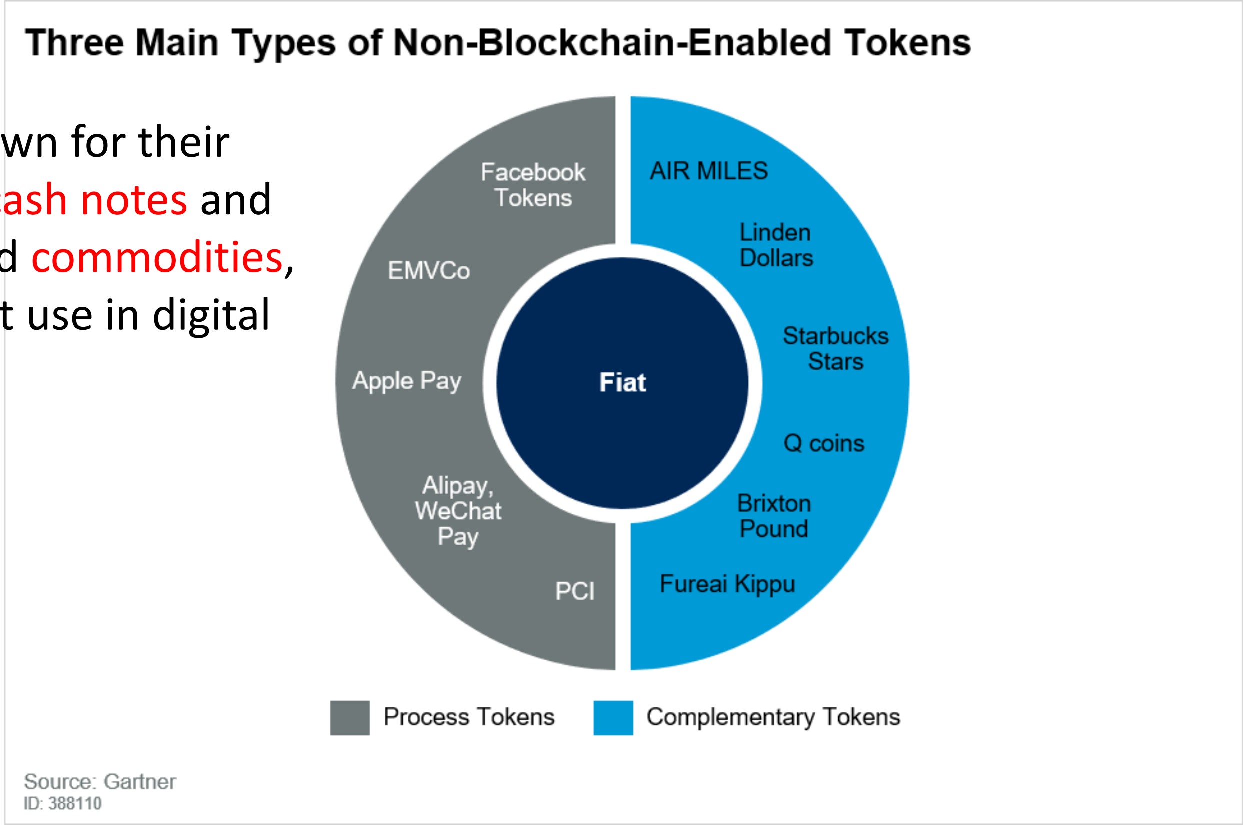
Smart contract standards describe rules that the smart contract must comply with in order to utilize the underlying blockchain network. The standards are application-level for blockchains built for smart contract or other decentralized applications (dApp).

Smart contract standard can include token standards, name registries, library/package formats, and more.

Smart contracts must obey the requirements in order to enable some basic functions like creation of tokens, performing transactions, spending and so on. Token standard is the subsidiary of smart contract standard.

Categories of Token (Non-Blockchain-Enabled Tokens)

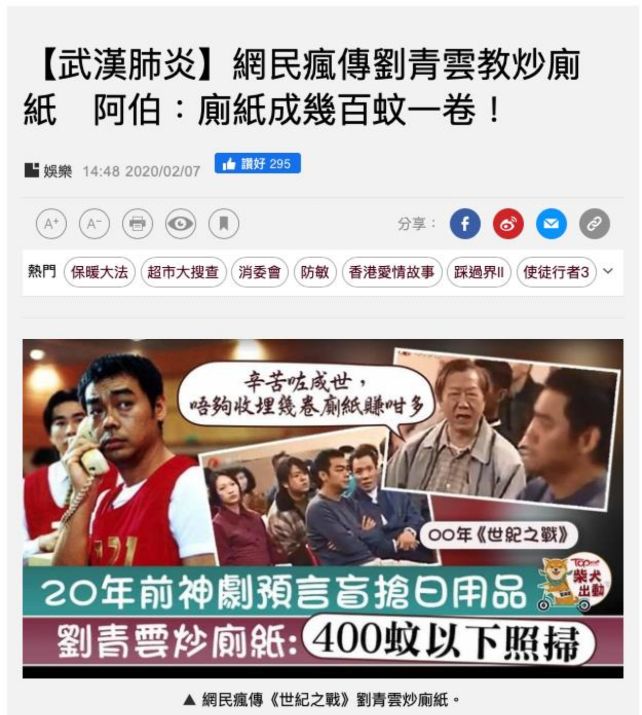
These tokens are best known for their physical forms, including cash notes and coins, precious metals, and commodities, which can limit their direct use in digital environments.



Three Main Types of Non-Blockchain-Enabled Tokens

Source: Gartner
ID: 388110

What is Token?



【武漢肺炎】網民瘋傳劉青雲教炒廁紙　阿伯：廁紙成幾百蚊一卷！

娛樂 14:48 2020/02/07 讚好 295

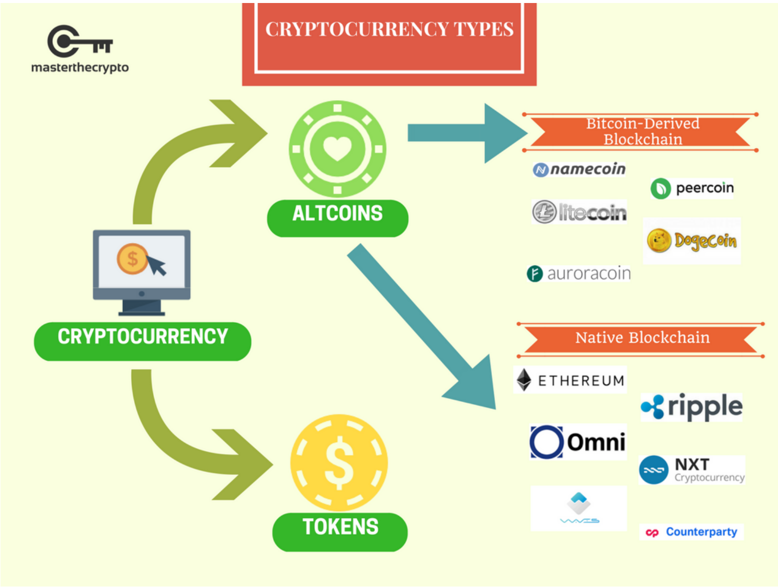
A⁺ A⁻
分享：
熱門 保暖大法 超市大搜查 消委會 防敏 香港愛情故事 踩過界II 使徒行者3
辛苦咗成世，
唔夠收埋幾卷廁紙賺咁多
00年《世紀之戰》
柴犬出動
20年前神劇預言盲搶日用品
劉青雲炒廁紙：400蚊以下照掃

▲ 網民瘋傳《世紀之戰》劉青雲炒廁紙。

Toilet paper can be trade as “Token”?

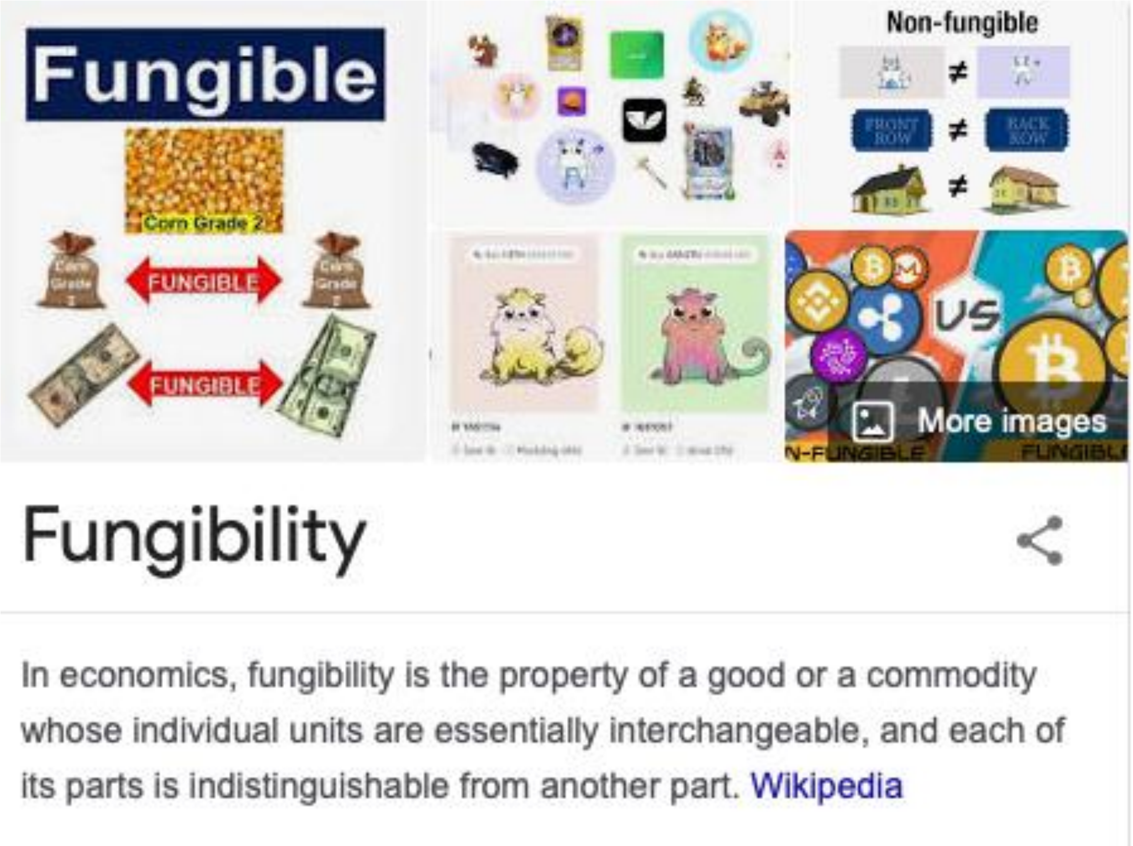
Crypto Token

- In computer security and cryptocurrency, the term token is generally referring to a cryptographic string of numbers and letters that contains no real data but relates back to real data (that cryptographic code is a "stand-in" for real data).
- The term token refers to the fact that the creation, transfer, and storage of cryptocurrencies use strings of numbers and letters called tokens
- Tokens can represent basically any assets that are fungible and tradable, from commodities to loyalty points to even other cryptocurrencies!
- Sidechains are emerging mechanisms that allow tokens and other digital assets from one blockchain to be securely used in a separate blockchain and then be moved back to the original blockchain if needed



https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/

Fungible



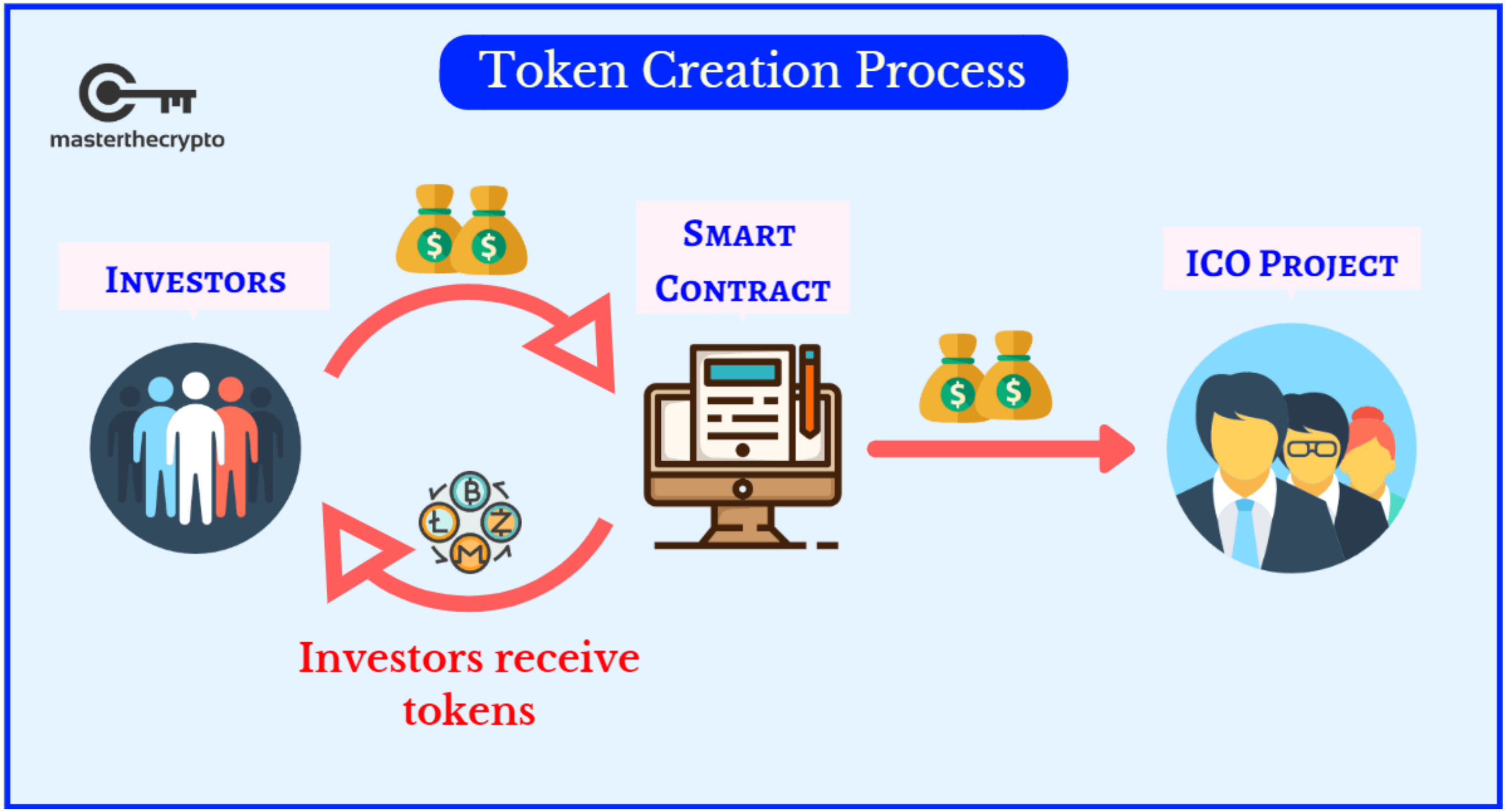
Fungibility

In economics, fungibility is the property of a good or a commodity whose individual units are essentially interchangeable, and each of its parts is indistinguishable from another part. Wikipedia

References information of CryptoAssets

- BitInfoCharts: https://bitinfocharts.com/
- Blockchain.info: https://blockchain.info/charts
- CoinCap: https://coincap.io/
- CoinDesk: http://www.coindesk.com/
- CoinMarketCap: https://coinmarketcap.com/
- CryptoCompare: https://www.cryptocompare.com/
- Etherscan: https://etherscan.io/charts

Crypto Token

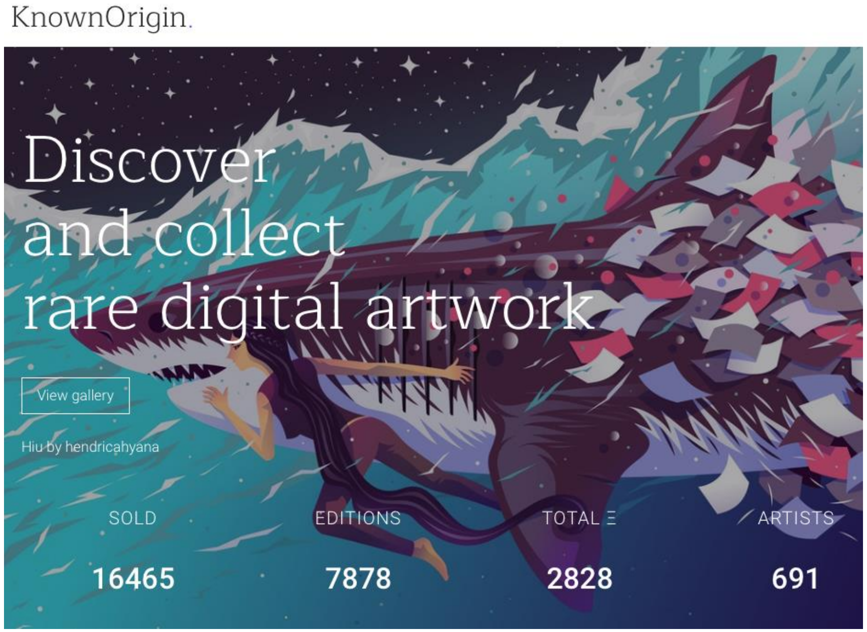


Can Digital Artwork be Token?

Digital art is endlessly multipliable without loss of quality.

Crypto-art works by adding a unique and indelible signature to a digital file, called “tokenizing” or “minting” it on the blockchain — a technology that acts like a permanent ledger or registry distributed across many computers instead of a central one

This non-fungible token (aka NFT) represents a value of scarcity for the associated artwork


KnownOrigin.

Discover and collect rare digital artwork

SOLD	EDITIONS	TOTAL Ξ	ARTISTS
16465	7878	2828	691

Some NFT sites:
https://www.hkd.com/en/nft_works/5
https://opensea.io

Non-fungible token (aka NFT)

A non-fungible token (NFT) is a unique and non-interchangeable unit of data stored on a blockchain, a form of digital ledger. Can be sold and traded but unique

NFTs can be associated with reproducible digital files such as photos, videos, and audio.

NFTs use a digital ledger to provide a public certificate of authenticity or proof of ownership, but do not restrict the sharing or copying of the underlying digital files.

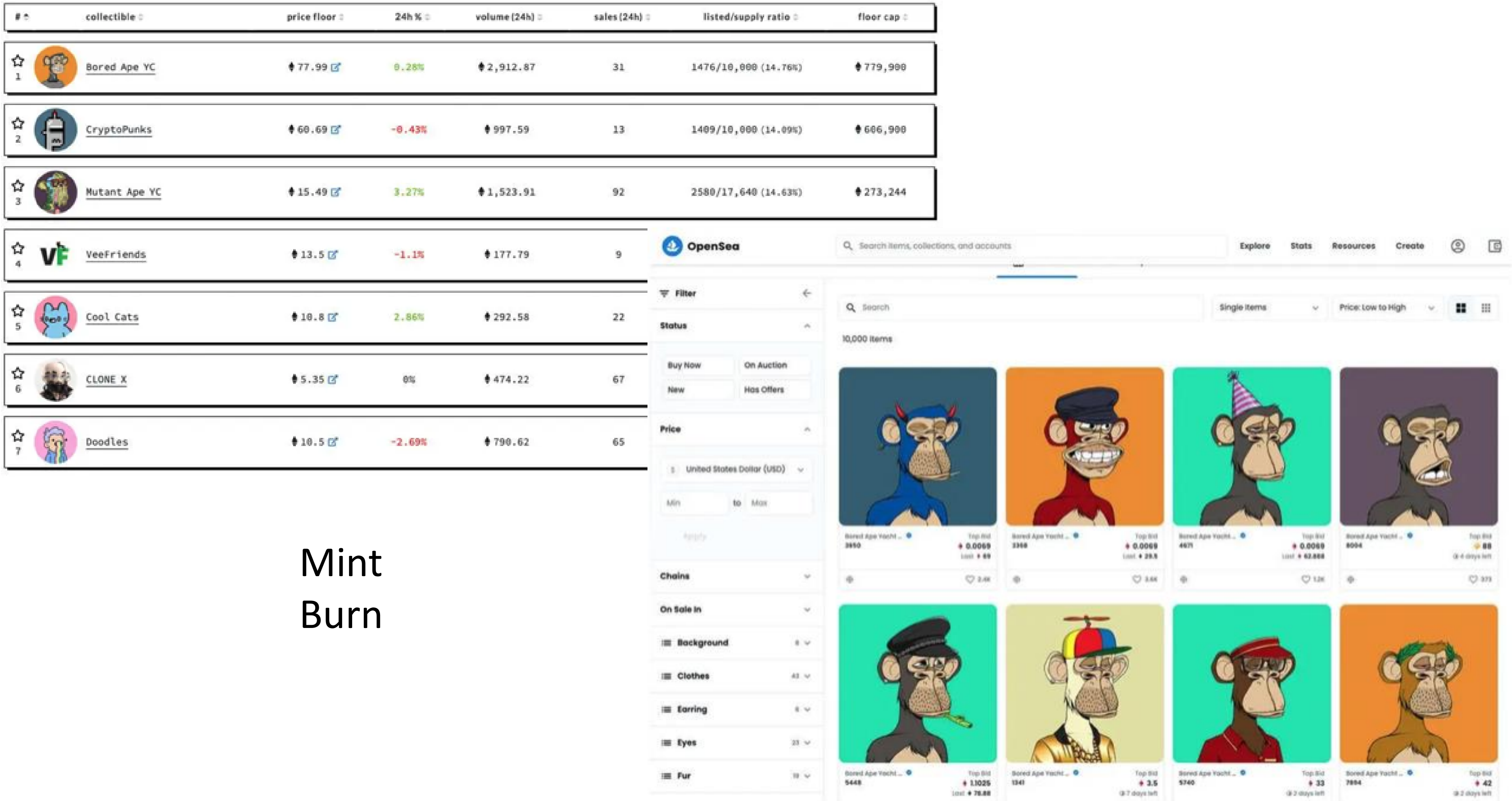
The lack of interchangeability (fungibility) distinguishes NFTs from blockchain cryptocurrencies, such as Bitcoin.

NFT is merely a proof of ownership that is separate from a copyright. Can be digital art, games, music, film, real estate, software title, concert tickets, KYC compliance, etc.

A NFT marketplace enables the creation, sale, and purchase of digital art as NFTs.

OpenSea and Rarible are two of the largest NFT marketplaces.

Non-fungible token (aka NFT)

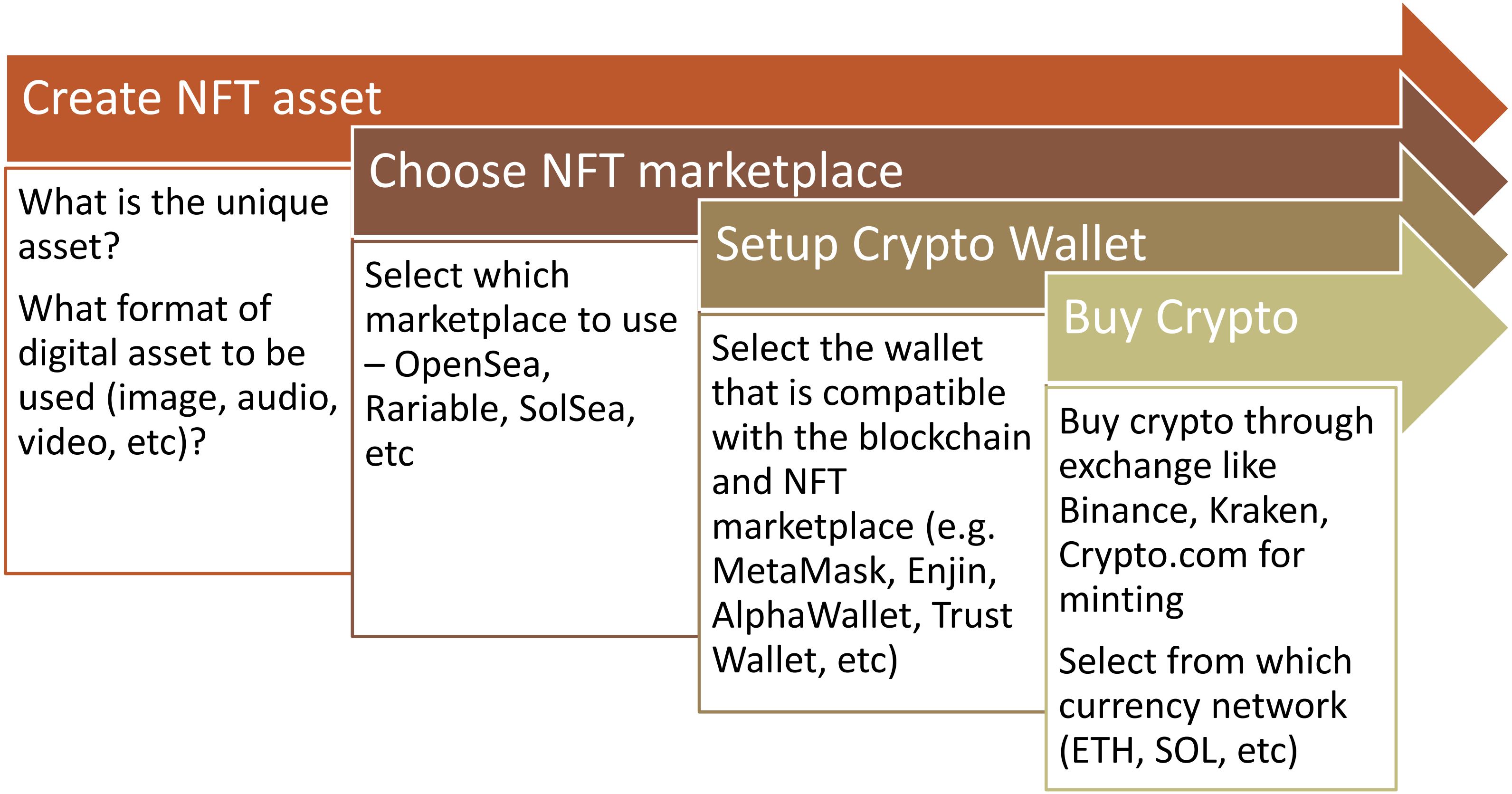


#	collectible	price floor	24h %	volume (24h)	sales (24h)	listed/supply ratio	floor cap
1	Bored Ape YC	⧫77.99	0.28%	⧫2,912.87	31	1476/10,000 (14.76%)	⧫779,900
2	CryptoPunks	⧫60.69	-0.43%	⧫997.59	13	1409/10,000 (14.09%)	⧫606,900
3	Mutant Ape YC	⧫15.49	3.27%	⧫1,523.91	92	2580/17,640 (14.63%)	⧫273,244
4	VeeFriends	⧫13.5	-1.1%	⧫177.79	9		
5	Cool Cats	⧫10.8	2.86%	⧫292.58	22		
6	CLONE X	⧫5.35	0%	⧫474.22	67		
7	Doodles	⧫10.5	-2.69%	⧫790.62	65		

OpenSea
Search items, collections, and accounts
Explore
Stats
Resources
Create
Filter
Status
Buy Now
On Auction
New
Has Offers
Price
United States Dollar (USD)
Min
to
Max
Apply
Chains
On Sale In
Background
Clothes
Earring
Eyes
Fur
Search
Single items
Price: Low to High
10,000 items
Bored Ape Yacht ... 3650 Top Bid ⧫ 0.0069 Last ⧫ 69
Bored Ape Yacht ... 3368 Top Bid ⧫ 0.0069 Last ⧫ 29.5
Bored Ape Yacht ... 4671 Top Bid ⧫ 0.0069 Last ⧫ 62.888
Bored Ape Yacht ... 8004 Top Bid 88 4 days left
Bored Ape Yacht ... 5448 Top Bid ⧫ 1.1025 Last ⧫ 78.88
Bored Ape Yacht ... 1341 Top Bid ⧫ 3.5 7 days left
Bored Ape Yacht ... 5740 Top Bid ⧫ 33 2 days left
Bored Ape Yacht ... 7894 Top Bid ⧫ 42 2 days left

Mint
Burn

NFT create and mint process



Create NFT asset

What is the unique asset?

What format of digital asset to be used (image, audio, video, etc)?

Choose NFT marketplace

Select which marketplace to use – OpenSea, Rariable, SolSea, etc

Setup Crypto Wallet

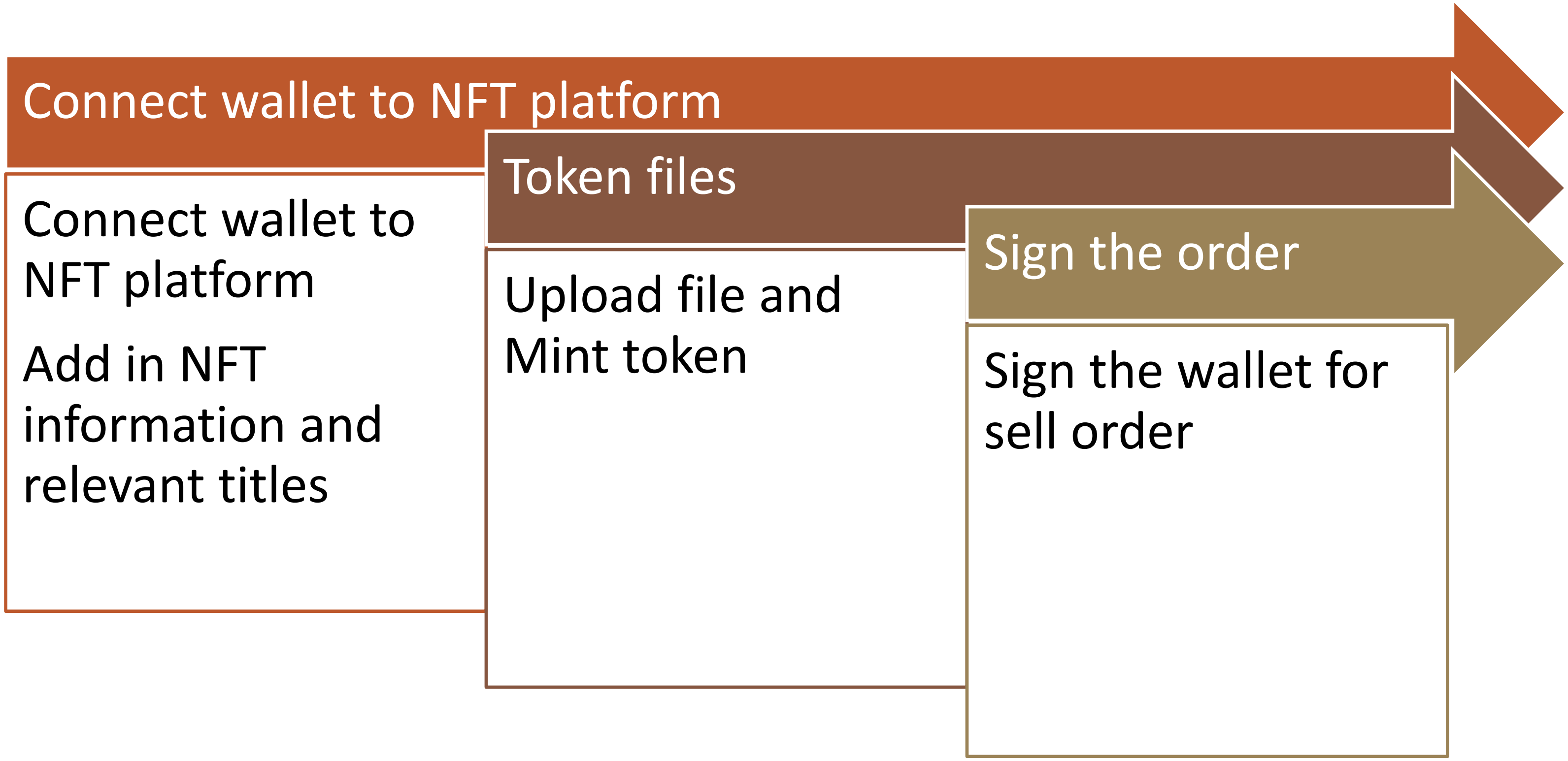
Select the wallet that is compatible with the blockchain and NFT marketplace (e.g. MetaMask, Enjin, AlphaWallet, Trust Wallet, etc)

Buy Crypto

Buy crypto through exchange like Binance, Kraken, Crypto.com for minting

Select from which currency network (ETH, SOL, etc)

NFT create and mint process (Cont.)



Connect wallet to NFT platform

Connect wallet to NFT platform

Add in NFT information and relevant titles

Token files

Upload file and Mint token

Sign the order

Sign the wallet for sell order

Sample NFT Contract

```
// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;


import "@openzeppelin/contracts/token/ERC721/ERC721.sol";


contract MyNFT is ERC721 {

    constructor() ERC721("MyNFT", "MNFT") {}


    function mint(address to, uint256 tokenId) public {

        _mint(to, tokenId);

    }

}
```

The constructor() function is called when the contract is deployed and sets the name and symbol of the NFT to "MyNFT" and "MNFT" respectively.

The mint() function is a simple example of how to create a new NFT.

It takes the address of the person who will receive the NFT (to) and a unique token ID (tokenId) as arguments, and then calls the _mint() function inherited from ERC721 to create a new token and assign ownership to the specified address.

From ChatGPT

Simple Step in creating NFT related Smart Contract

1. need to import the contract frameworks from Open Zeppelin
   - pragma solidity ^0.6.0;
   - import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
   - import "@openzeppelin/contracts/utils/Counters.sol";
   - contract UniqueAsset is ERC721 {
   - using Counters for Counters.Counter;
   -   Counters.Counter private _tokenIds;
   -   mapping(string => uint8) hashes;
   - constructor() public ERC721("UniqueAsset", "UNA") {}
   - }

2. Use Truffle to compiles the contract using the correct version of Solidity by editing the truffle-config.js file

3. Define the token name and symbol constructor for the contract to be used.

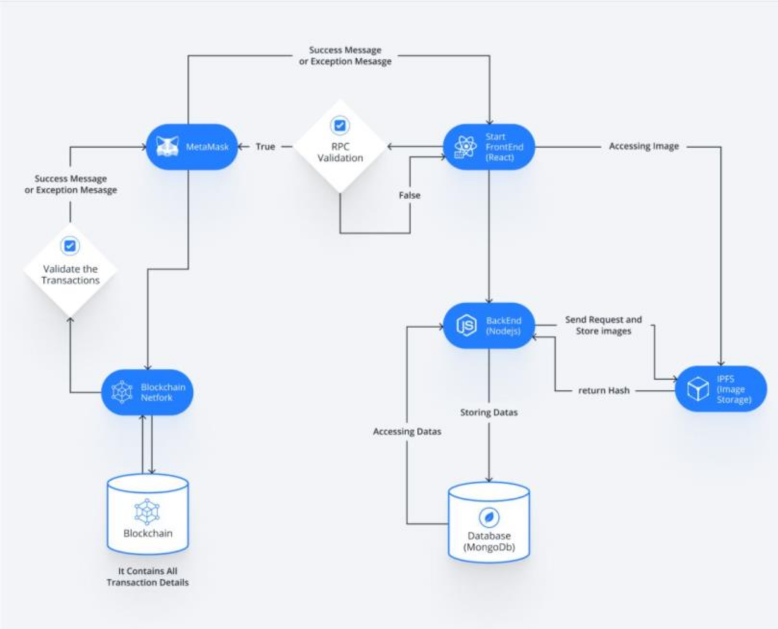
Non-fungible token (aka NFT)

ERC-721 is an open standard that describes how to build Non-Fungible tokens on Ethereum Virtual Machine compatible blockchains; ERC-721, ERC-1155, FA2, dGoods, and TRC-721 are the current NFT-supporting standards type.

An ERC-721 smart contracts contain a link pointing to a JSON file, that is publicly available and hosted digital asset file.

However, blockchains are not great for storing large pieces of data.

traditional cloud storage as we know it has not cryptographically verifiable



IPFS

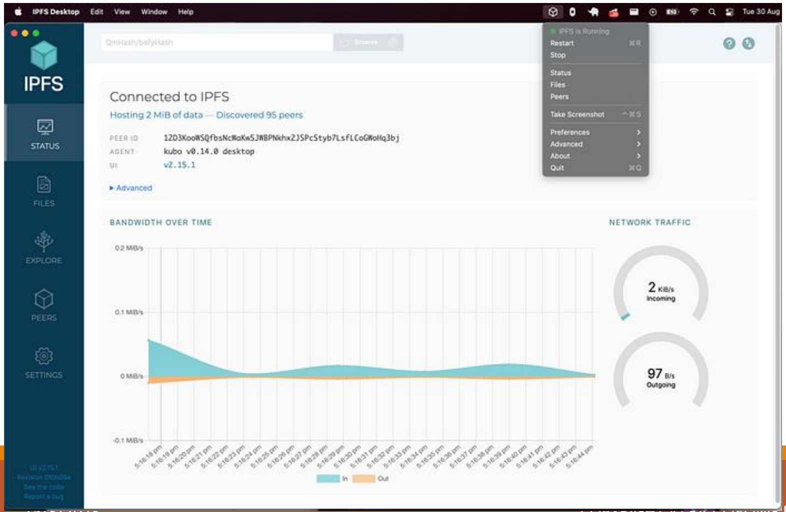
IPFS is a distributed storage network. It works in a similar way to cloud storage.

You make a request for content and that content is returned

IPFS leverages a tool called content addressability.

No longer have to rely on a single location for the retrieval of content. This is far more efficient for global blockchains.

IPFS also takes care of the verifiability for us



Connected to IPFS

Hosting 2 MiB of data — Discovered 95 peers

PEER ID 12D3KooWSQfbsNcWaKw5JWBPNkhx2JSPcStyb7LsfLCoGWoHq3bj
AGENT kubo v0.14.0 desktop
UI v2.15.1

Start the IPFS repo by typing the following in a terminal/cmd window.

- $ ipfs init

Start IPFS daemon, open a separate terminal/cmd window and type the following.

- $ ipfs daemon

Go to the first terminal window and add the image to IPFS (art.png here).

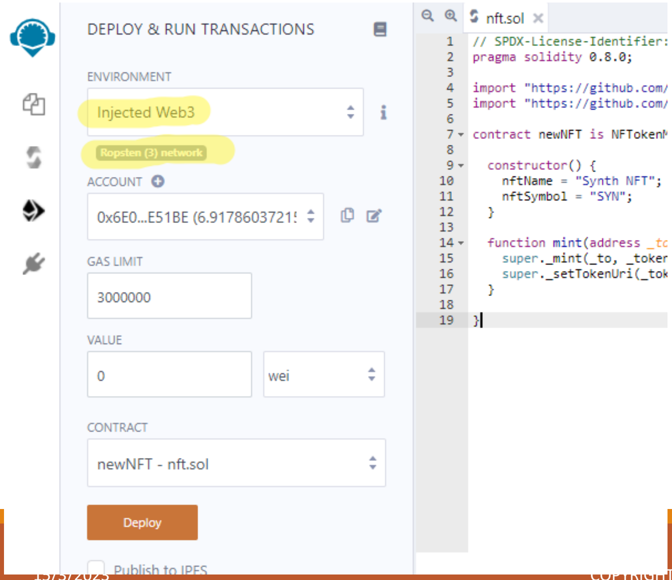
- $ ipfs add art.png

Copy the hash starting and add the https://ipfs.io/ipfs/

Create a JSON file nft.json and save it in the same directory as the image.

Create own token using ERC721

use the 0xcert/ethereum-erc721 contract to create our NFT. With 0xcert/ethereum-erc721, we don't need to write the whole ERC-721 interface. Instead, we can import the library contract and use its functions.



DEPLOY & RUN TRANSACTIONS

ENVIRONMENT: Injected Web3

Ropsten (3) network

ACCOUNT: 0x6E0...E51BE (6.9178603721!

GAS LIMIT: 3000000

VALUE: 0 wei

CONTRACT: newNFT - nft.sol

Deploy

Publish to IPFS

nft.sol

```
// SPDX-License-Identifier:
pragma solidity 0.8.0;

import "https://github.com/
import "https://github.com/

contract newNFT is NFTokenM

  constructor() {
    nftName = "Synth NFT";
    nftSymbol = "SYN";
  }

  function mint(address _to
    super._mint(_to, _toker
    super._setTokenUri(_tok
  }

}
```

Now go to the "Deployed Contracts" section in Remix and expand the deployed contract. You'll see a bunch of functions/methods.

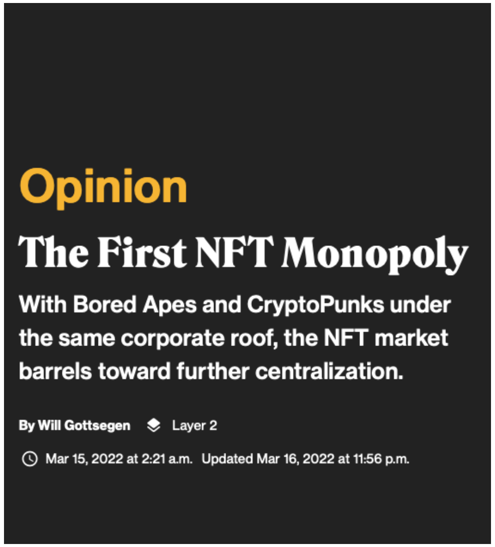
Then declared a custom mint function mintCollectionNFT() in order to implement NFT minting for the collection using the ERC721 internal functions.

Is NFT = Decentralization

The rhetoric around cryptocurrencies has to do with "decentralization" as a guiding ethos, the NFT sector is in fact already extremely centralized.

According to data from the blockchain analytics company DappRadar, the vast majority of all non-fungible token sales volume is concentrated on two platforms: OpenSea, the incumbent backed by venture capital firm Andreessen Horowitz, and LooksRare, a scrappy outsider that emerged a few months ago.

Larva Labs remains an independent company and retains the rights to its other major NFT project, Autoglyphs.



Opinion

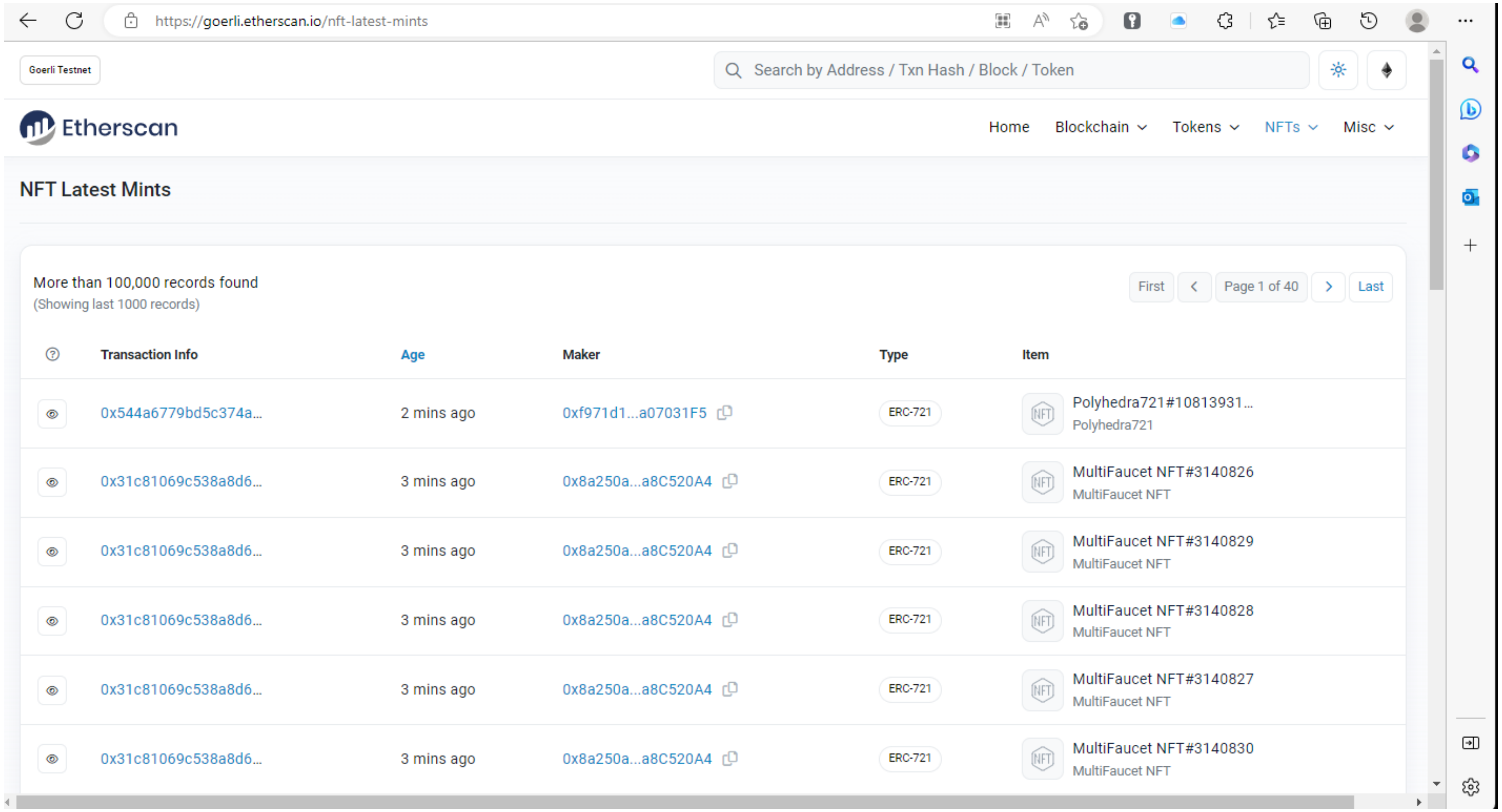
The First NFT Monopoly

With Bored Apes and CryptoPunks under the same corporate roof, the NFT market barrels toward further centralization.

By Will Gottsegen Layer 2

Mar 15, 2022 at 2:21 a.m. Updated Mar 16, 2022 at 11:56 p.m.

NFT Latest Mints



https://goerli.etherscan.io/nft-latest-mints
Goerli Testnet
Search by Address / Txn Hash / Block / Token
Etherscan
Home
Blockchain
Tokens
NFTs
Misc

NFT Latest Mints

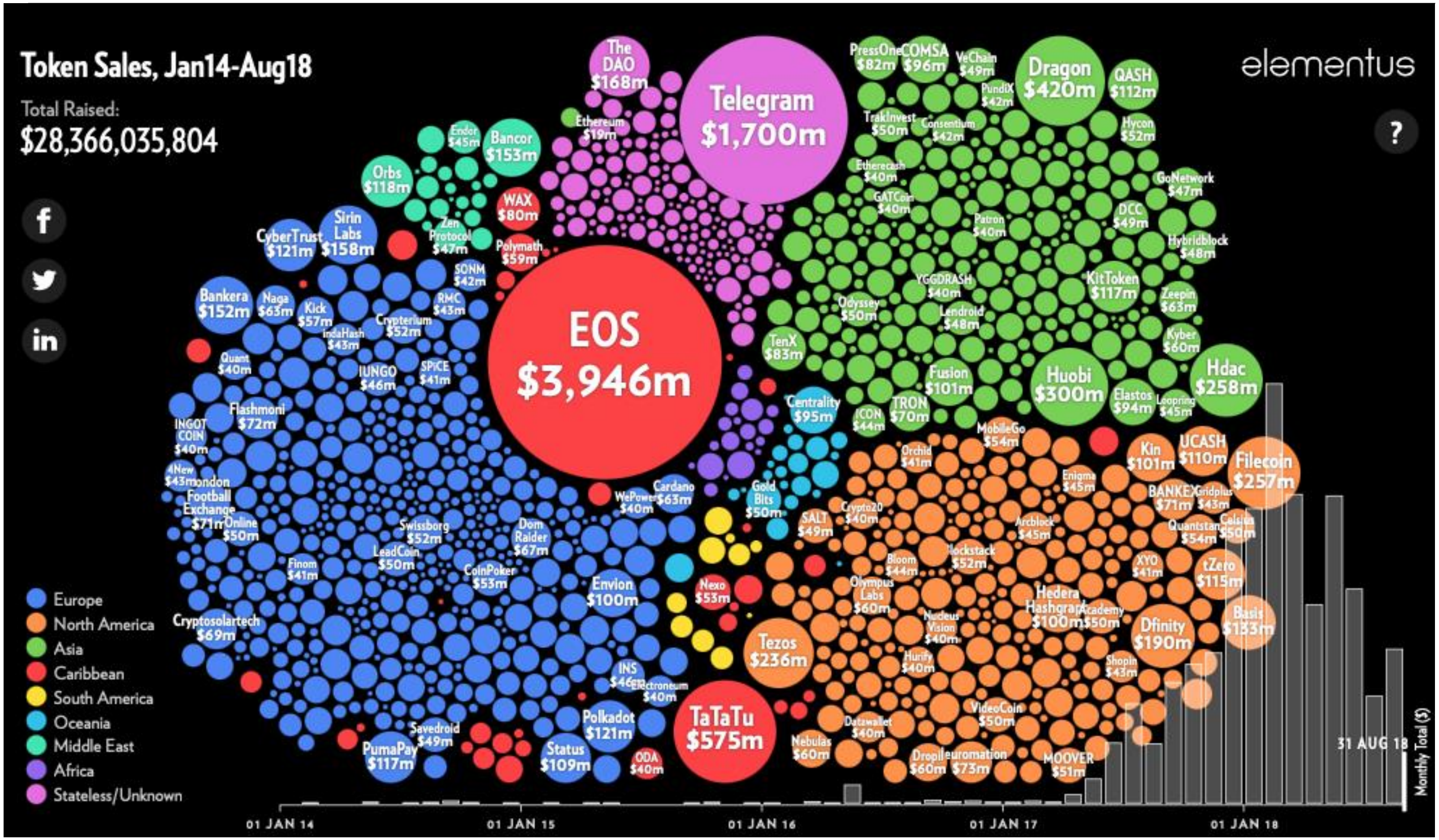
More than 100,000 records found
(Showing last 1000 records)

Transaction Info	Age	Maker	Type	Item
0x544a6779bd5c374a...	2 mins ago	0xf971d1...a07031F5	ERC-721	Polyhedra721#10813931... Polyhedra721
0x31c81069c538a8d6...	3 mins ago	0x8a250a...a8C520A4	ERC-721	MultiFaucet NFT#3140826 MultiFaucet NFT
0x31c81069c538a8d6...	3 mins ago	0x8a250a...a8C520A4	ERC-721	MultiFaucet NFT#3140829 MultiFaucet NFT
0x31c81069c538a8d6...	3 mins ago	0x8a250a...a8C520A4	ERC-721	MultiFaucet NFT#3140828 MultiFaucet NFT
0x31c81069c538a8d6...	3 mins ago	0x8a250a...a8C520A4	ERC-721	MultiFaucet NFT#3140827 MultiFaucet NFT
0x31c81069c538a8d6...	3 mins ago	0x8a250a...a8C520A4	ERC-721	MultiFaucet NFT#3140830 MultiFaucet NFT

Token properties

	Fungible tokens	Non-fungible tokens
Token exchange	Interchangeable – can be exchanged to any other token of the same type	Non interchangeable – can only be exchanged to same token but not another of the same type
Type of tokens	Uniform – All tokens of the same type are identical in specification	Unique – Each token is unique and different to all other tokens of the same type
Units	Divisible – divisible into smaller units	Non-divisible – cannot be divided
Example	ERC-20 standard ERC-223 standard	ERC-721 standard

Total Token sales



https://elementus.io/token-sales-history

Bitcoin UTXO is Token?

In Bitcoin transaction, transaction record and unspent transaction will be kept.

Storing a receipt of the transaction where someone sent you a Bitcoin. These receipts are called unspent transaction outputs (UTXOs).

Every Bitcoin only exists as a chain of receipts leading back to the valid block where that Bitcoin was originally mined and awarded as part of the block reward

Ethereum Classic (ETC)

Ethereum Classic came to be after members of the Ethereum community implemented a time-sensitive hard fork (codenamed “DAO”).

On July 20, 2016, at a block height of 1.92 million, Ethereum introduced an irregular state change via a hard fork in an effort to return approximately 3.6 million ether that had been taken from a smart contract known as The DAO.

Almost everyone agreed that the ether taken had been stolen and that leaving it all in the hands of the thief would be of significant detriment to the development of the Ethereum ecosystem as well as the platform itself.

A number of people in the ecosystem disagreed with this change, believing immutability should be a fundamental principle of the Ethereum blockchain without exception

They elected to continue the original chain under the moniker of Ethereum Classic.

Ethereum ERC-20

The Ethereum Improvement Proposal repository is located at https://github.com/ether eum/EIPs/.

A token can generally represent any asset that has a value attached to it. In this case, we are talking about tokens which represent a smart contract and use of the Ethereum blockchain

These tokens can be traded, bought or sold. ERC-20 is a token protocol for all tokens implemented by the Ethereum blockchain (Token protocol means rules or standards that the token must follow).

All tokens which implement the protocol become a compliant token of ERC-20.

The technical specification of this protocol comprises six functions that ensure that all tokens based on the Ethereum system work anywhere on the platform

ERC20 Token

ERC 20 is the most well-known among all the standards present within the entire crypto community, and most tokens issued on top of the Ethereum platform use it. Helping developers to accurately predict how new tokens will function within the larger Ethereum system.

```
contract ERC20 {
event Transfer(address indexed from, address indexed to, uint256 value);

event Approval(address indexed owner, address indexed spender, uint256 value);

function totalSupply() public view returns(uint256);

function balanceOf(address who) public view returns(uint256);

function transfer(address to, uint256 value) public returns(bool);

function allowance(address owner, address spender) public view returns (uint256);

function transferFrom(address from, address to, uint256 value) public returns (bool);

function approve(address spender, uint256 value) public returns (bool);

}
```

ERC20 Token

```
// its value is increased when new tokens are minted
uint256 totalSupply_;// access the value of totalSupply_
function totalSupply() public view returns (uint256) {
            return totalSupply_;
}


// Updated when tokens are minted or transferred
mapping(address => uint256) balances;// Returns tokens held by the address passed as _owner
function balanceOf(address _owner) public view returns (uint256 balance) {
            return balances[_owner];
}
```

ERC20 Token

```
function transfer(address _to, uint256 _value) public returns (bool) { // Check for blank addresses
            require(_to != address(0)); // Check to ensure valid transfer
            require(_value <= balances[msg.sender]); // SafeMath.sub will throw if there is not enough balance.
            balances[msg.sender] = balances[msg.sender].sub(_value);
            balances[_to] = balances[_to].add(_value);

// Event transfer defined in the ERC 20 interface above
            Transfer(msg.sender, _to, _value); return true;
}
```

Problem of lost tokens (ERC20)

When people mistakenly use the instructions for sending tokens to a wallet and send them to a smart contract which is not designed to handle it, their tokens get stuck in the smart contract

If you will send 100 ERC 20 tokens to a contract that is not intended to work with ERC 20 tokens, then it will not reject tokens because it can't recognize an incoming transaction.

ERC 223 Token

Basically, ERC223 is a superset of ERC20 containing all of its same functionality.

ERC223 is backward compatible with ERC20, thus, any platform working with ERC20 will also work with ERC223.

Its major difference is that in ERC223 the transfer function has an additional parameter checking whether the destination address is a smart contract.

If so, the transaction triggers the tokenFallback function in the smart contract.

Benefit of using ERC 223 Token

- No tokens are lost
- Smart contract developers can reject incoming tokens of unsupported types
- Transactions are less expensive (lower fee and energy usage)

ERC 223 Token

```
contract ERC223 {
event Transfer(address indexed from, address indexed to, uint value, bytes indexed data);

function totalSupply() public view returns(uint256);

function balanceOf(address _owner) public view returns(uint256);

function transfer(address _to, uint256 _value) public returns (bool);

function transfer(address to, uint value, bytes data) public returns (bool);
}
```

ERC 223 Token TokenFallBack

```
contract ERC223ReceivingContract {
/**
* @dev Standard ERC223 function that will handle
* incoming token transfers.
* @param _from Token sender address.
* @param _value Amount of tokens.
* @param _data Transaction metadata.
*/
function tokenFallback(
address _from,
uint _value,
bytes _data
) public;
}
```

ERC233 Token Revised Transfer

The token transfer will fail if the recipient is a contract but does not implement the tokenFallbackfunction or the fallback function to receive funds.

```
function transfer(address _to, uint _value, bytes _data)
public {

assembly {
codeLength := extcodesize(_to)
}

if (codeLength > 0) {
ERC223ReceivingContract receiver = ERC223ReceivingContract(_to);
receiver.tokenFallback(msg.sender, _value, _data);
}

require(super.transfer(_to, _value));
}
```

Utility Token

Utility tokens are like Ethereum’s Gas.

Can be sold but have no air of investment surrounding them.

Utility tokens are used by the blockchain as an internal means of operation.

Creating and trying to sell Utility tokens is risky, and you should talk to legal professionals, and seek to get a “no action” letter from the SEC.

Utility tokens do not appreciate, they may fall in value, but there is no reward associated with their purchase.

ERC-1155

A standard interface for contracts that manage multiple token types. A single deployed contract may include any combination of fungible tokens, non-fungible tokens or other configurations (e.g. semi-fungible tokens).

ERC-1155 Multi Token Standard allows for each token ID to represent a new configurable token type, which may have its own metadata, supply and other attributes.

Tokens standards like ERC-20 and ERC-721 require a separate contract to be deployed for each token type or collection. This places a lot of redundant bytecode on the Ethereum blockchain and limits certain functionality by the nature of separating each token contract into its own permissioned address.

With the rise of blockchain games and platforms like Enjin Coin, game developers may be creating thousands of token types, and a new type of token standard is needed to support them

ERC-4973

An interface for non-transferrable NFTs binding to an Ethereum account like a legendary World of Warcraft item binds to a character.

Proposes a standard API for account-bound Tokens (ABT) within smart contracts. An ABT is a non-fungible token bound to a single account. ABTs don't implement a canonical interface for transfers. This EIP defines basic functionality to mint, assign, revoke and track ABTs.

In the popular MMORPG World of Warcraft, its game designers intentionally took some items out of the world's auction house market system to prevent them from having a publicly-discovered price and limit their accessibility.

Vanilla WoW's "Thunderfury, Blessed Blade of the Windseeker" was one such legendary item, and it required a forty-person raid, among other sub-tasks, to slay the firelord "Ragnaros" to gain the "Essence of the Firelord," a material needed to craft the sword once.

Meta-transaction

In essence, meta transactions allow users to interact with a public blockchain without paying a transaction fee. This leads to a more seamless UX as users no longer have to understand the inner workings of public blockchains and market dynamics for transaction fees.

A third-party (called a relayer) can send another user's transactions and pay themselves for the gas cost.

In this scheme, users sign messages (not transactions) containing information about a transaction they would like to execute.

Relayers are then responsible for signing valid Ethereum transactions with this information and sending them to the network, paying for the gas cost.

A base contract preserves the identity of the user that originally requested the transaction. In this way, users can interact directly with smart contracts without needing to have a wallet or own Ether

Crypto Tokens Summary

Crypto Tokens in the world of blockchain are classified as cryptocurrency, security tokens, and utility tokens.

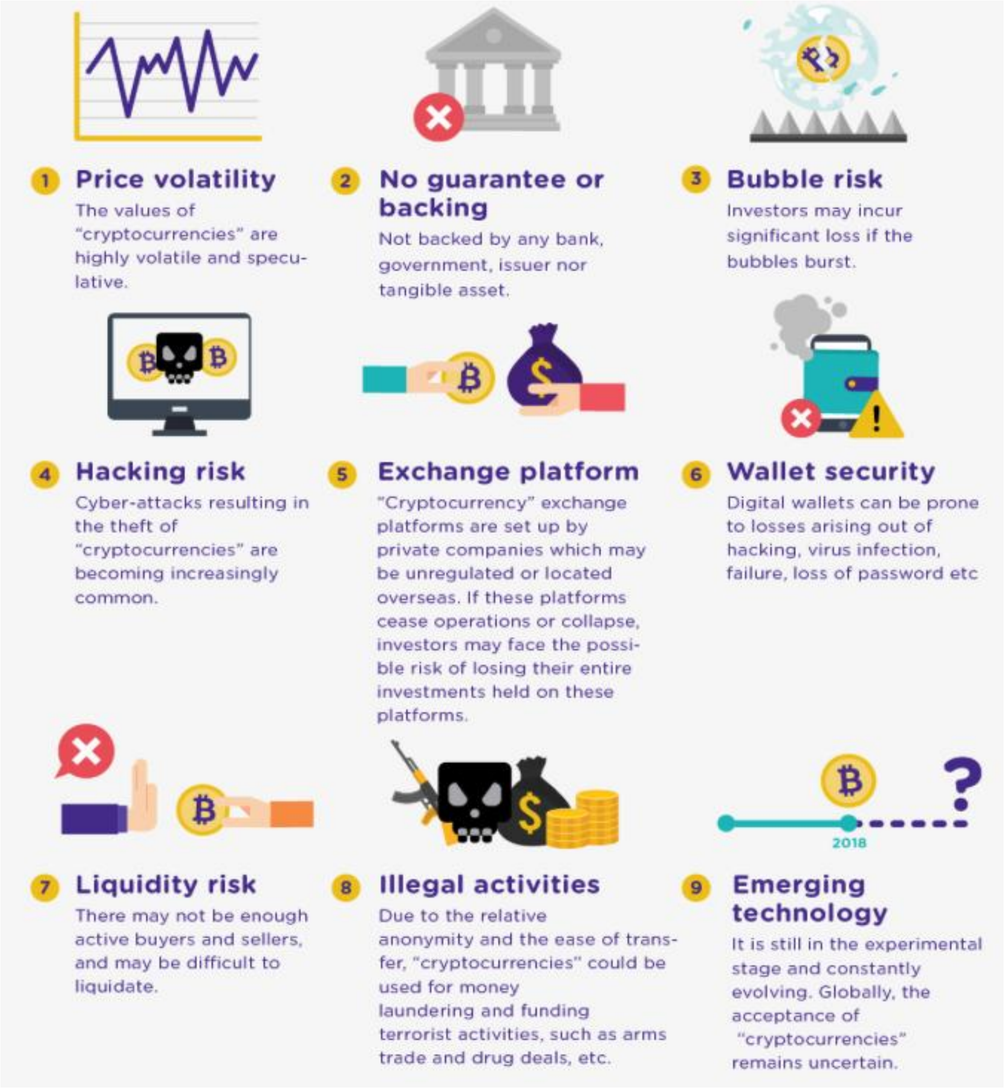
Security tokens are sold to investors through various means, including Initial Coin Offering (ICO) and Security Token Offering (STO).

Security tokens are considered securities, which are regulated by the Securities Exchange Commission (SEC).

Initial Coin Offering, Initial Token Offering,

Know about the risks - Bitcoin/"crypto currencies"

Bitcoin and other cryptocurrencies are high risk products



1 **Price volatility**

The values of "cryptocurrencies" are highly volatile and speculative.

2 **No guarantee or backing**

Not backed by any bank, government, issuer nor tangible asset.

3 **Bubble risk**

Investors may incur significant loss if the bubbles burst.

4 **Hacking risk**

Cyber-attacks resulting in the theft of "cryptocurrencies" are becoming increasingly common.

5 **Exchange platform**

"Cryptocurrency" exchange platforms are set up by private companies which may be unregulated or located overseas. If these platforms cease operations or collapse, investors may face the possible risk of losing their entire investments held on these platforms.

6 **Wallet security**

Digital wallets can be prone to losses arising out of hacking, virus infection, failure, loss of password etc

7 **Liquidity risk**

There may not be enough active buyers and sellers, and may be difficult to liquidate.

8 **Illegal activities**

Due to the relative anonymity and the ease of transfer, "cryptocurrencies" could be used for money laundering and funding terrorist activities, such as arms trade and drug deals, etc.

9 **Emerging technology**

It is still in the experimental stage and constantly evolving. Globally, the acceptance of "cryptocurrencies" remains uncertain.

ICO, Bitcoin and other "cryptocurrencies"

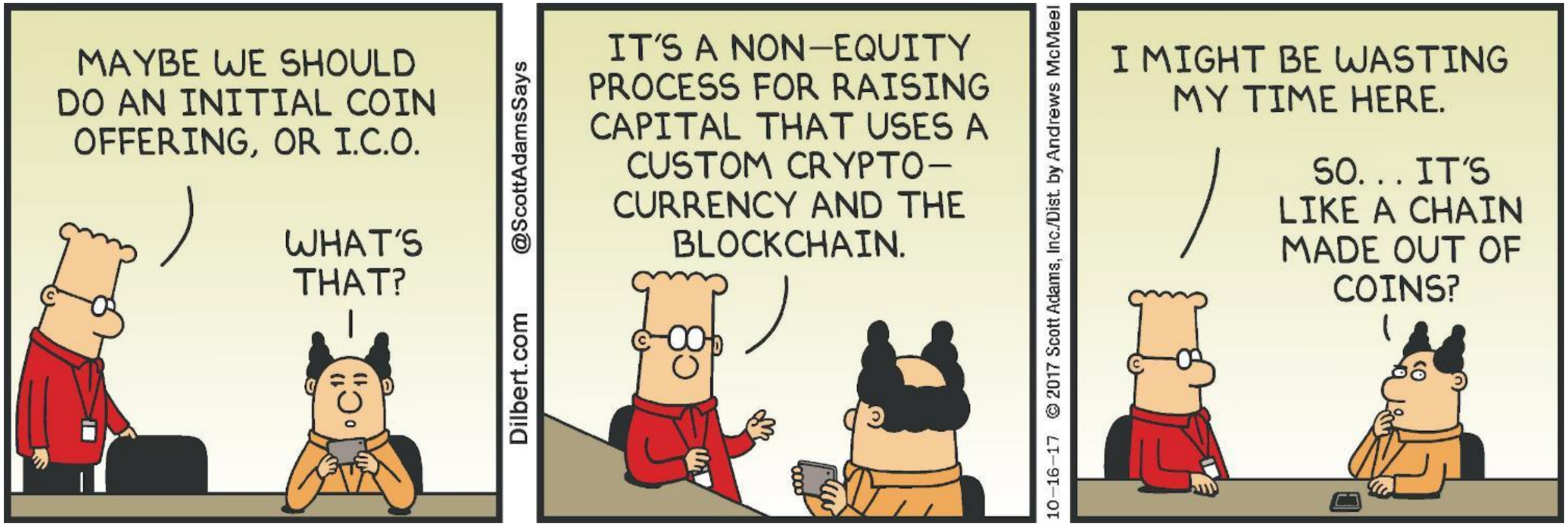
An **ICO** is a fundraising mechanism offered to investors whereby a project operator issues digital "tokens" or "coins" to fund a particular blockchain-related project

A digital token is a digital representation of the token holder's right to, e.g. an underlying asset, receipt of a benefit, or access a product.

Possible Risk

- Possible scams
- Risks associated with money laundering, terrorist financing or misuse for criminal activities
- Project prospect and limited information
- Platform risk
- Wallet security
- Highly volatile and speculative
- Liquidity risk
- Not backed
- Cross-border risk

ICO - Initial Coin Offering


MAYBE WE SHOULD DO AN INITIAL COIN OFFERING, OR I.C.O.
WHAT'S THAT?
@ScottAdamsSays
Dilbert.com
IT'S A NON-EQUITY PROCESS FOR RAISING CAPITAL THAT USES A CUSTOM CRYPTO-CURRENCY AND THE BLOCKCHAIN.
10-16-17 © 2017 Scott Adams, Inc./Dist. by Andrews McMeel
I MIGHT BE WASTING MY TIME HERE.
SO... IT'S LIKE A CHAIN MADE OUT OF COINS?

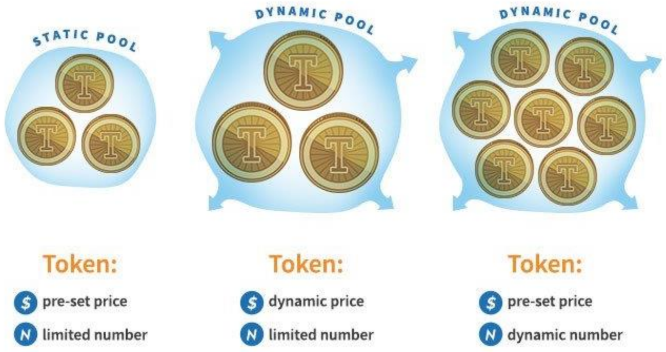
IPOs deal with investors
ICOs deal with supporters

IPOs deal with investors

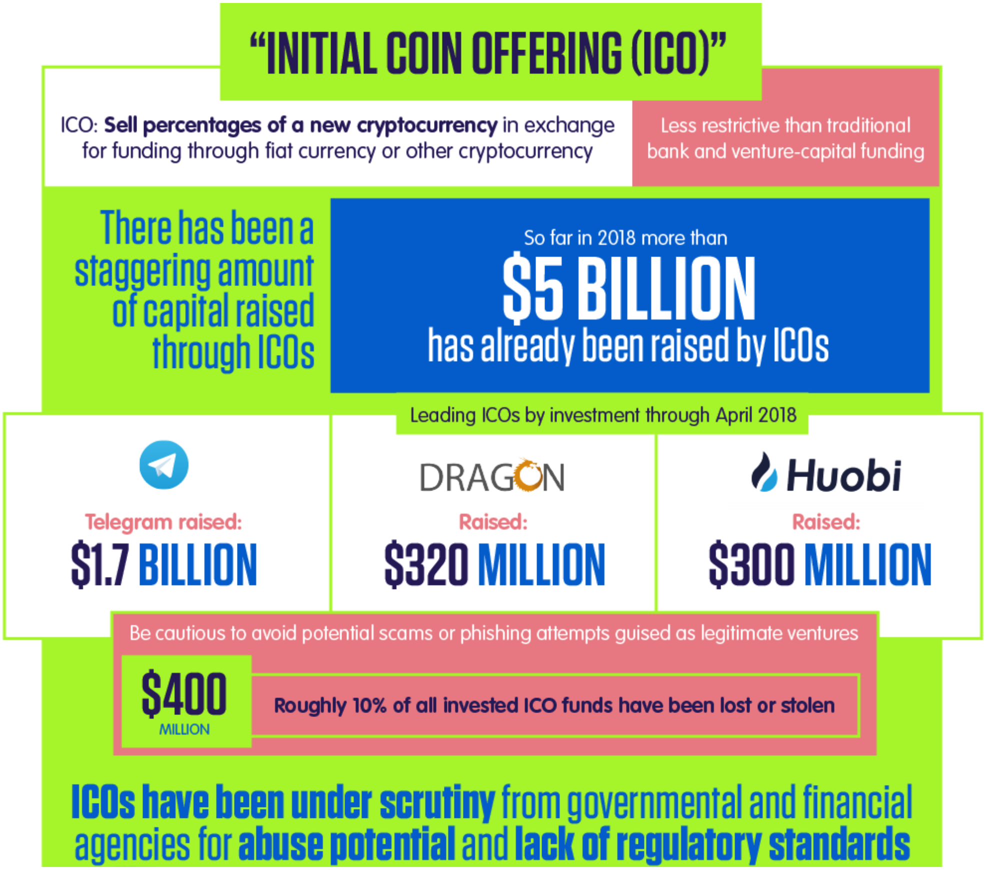
ICOs deal with supporters

- ICO has no central authority
- ICO is highly unregulated
- ICO terms is much freer

- ICO provides a blockchain equivalent to a share – a cryptocurrency token
- Usually, investors pay in popular existing token like bitcoin or ether and receive a commensurate number of new tokens in exchange.



Initial Coin Offering (ICO)



"INITIAL COIN OFFERING (ICO)"

ICO: **Sell percentages of a new cryptocurrency** in exchange for funding through fiat currency or other cryptocurrency

Less restrictive than traditional bank and venture-capital funding

There has been a staggering amount of capital raised through ICOs

So far in 2018 more than

$5 BILLION

has already been raised by ICOs

Leading ICOs by investment through April 2018

Telegram raised:	DRAGON Raised:	Huobi Raised:
$1.7 BILLION	**$320 MILLION**	**$300 MILLION**

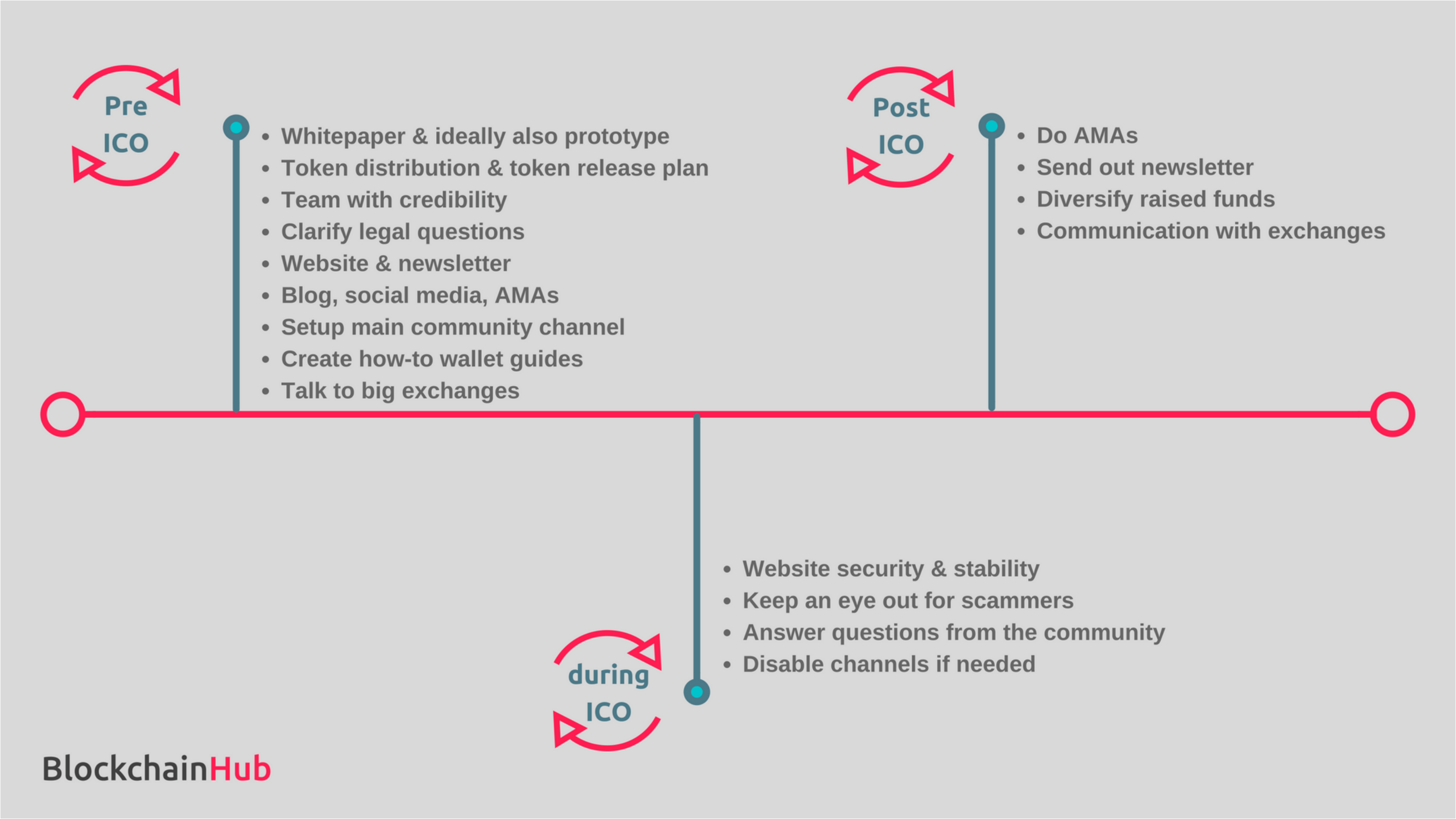
Be cautious to avoid potential scams or phishing attempts guised as legitimate ventures

$400 MILLION

Roughly 10% of all invested ICO funds have been lost or stolen

ICOs have been under scrutiny from governmental and financial agencies for **abuse potential** and **lack of regulatory standards**

How to raise funds via ICO?



Pre ICO

- Whitepaper & ideally also prototype
- Token distribution & token release plan
- Team with credibility
- Clarify legal questions
- Website & newsletter
- Blog, social media, AMAs
- Setup main community channel
- Create how-to wallet guides
- Talk to big exchanges

during ICO

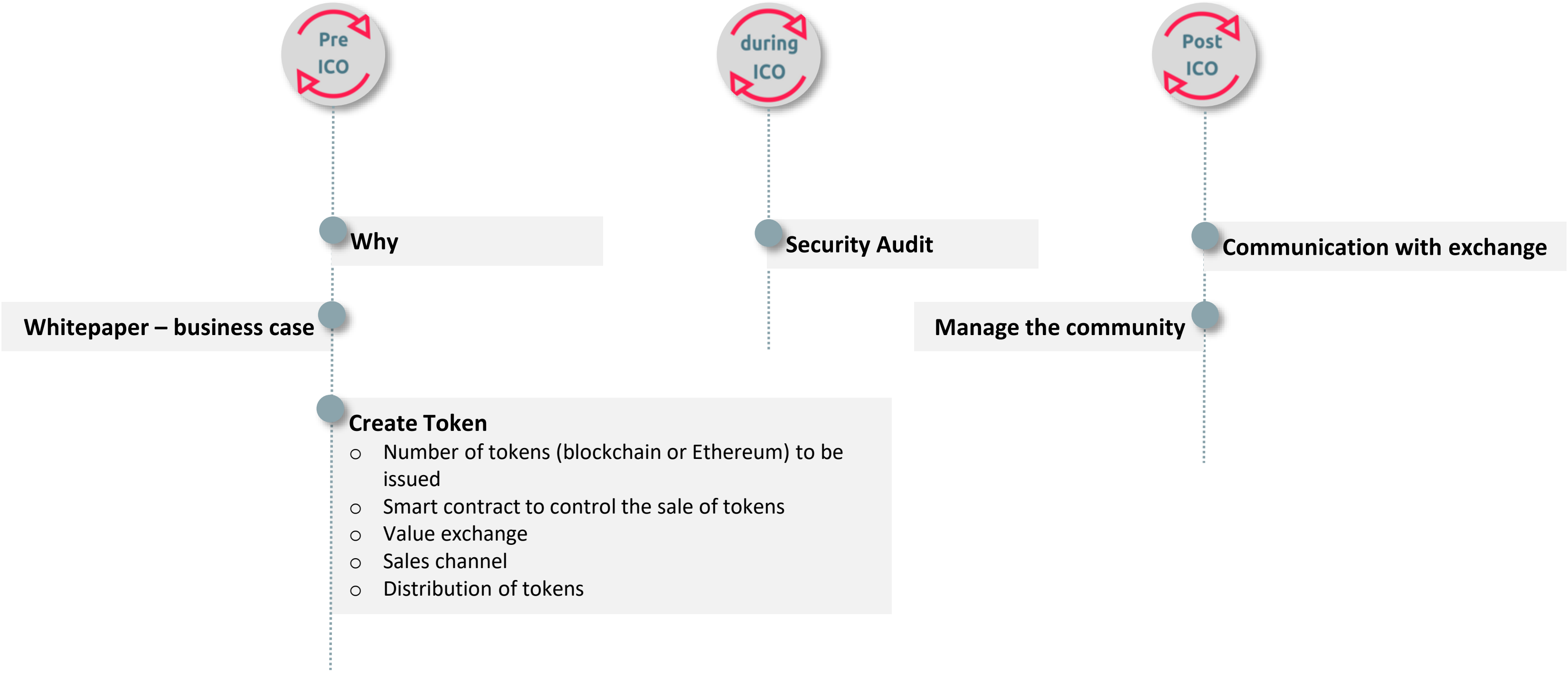
- Website security & stability
- Keep an eye out for scammers
- Answer questions from the community
- Disable channels if needed

Post ICO

- Do AMAs
- Send out newsletter
- Diversify raised funds
- Communication with exchanges

BlockchainHub

How to raise funds via ICO?



Pre ICO

Why

Whitepaper – business case

Create Token

- ○ Number of tokens (blockchain or Ethereum) to be issued
- ○ Smart contract to control the sale of tokens
- ○ Value exchange
- ○ Sales channel
- ○ Distribution of tokens

during ICO

Security Audit

Post ICO

Communication with exchange

Manage the community

ICO vs STO

A security token offering (STO) is similar to an initial coin offering (ICO), except that an STO involves security tokens. These security tokens are backed by real assets like commodities or equities

One major difference between STOs and ICOs is the regulatory treatment of the digital tokens they offer. The tokens offered through STOs are subject to federal securities regulations

ICOs are meant for raising funds in an unregulated environment, whereas STOs are regulated with government bodies and the investor is entitled to either a share of the profits or other forms of reward in exchange for their investment.

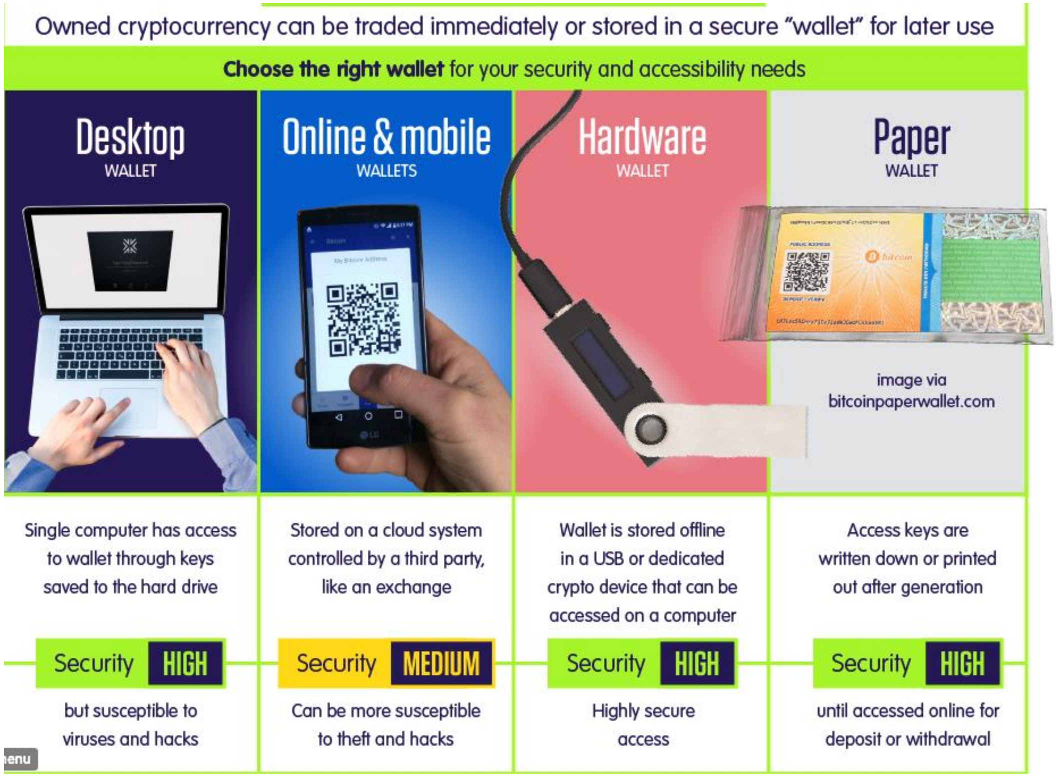
Hong Kong NFT project Monkey Kingdom loses (Dec 2021)

The exploited nonfungible token project is looking to make things right before the holidays with the help of a compensation fund.

Hackers then used the exploit to take over an administrative account, which posted a phishing link in the Monkey Kingdom Discord's announcement channel

Hong Kong-based gaming and venture capital company Animoca Brands and subsidiary Blowfish Studios have promised users that they will repay 265 Ether (ETH) or $1.1 million stolen in a fraudulent nonfungible token (NFT) sale on Discord.

CryptoWallets

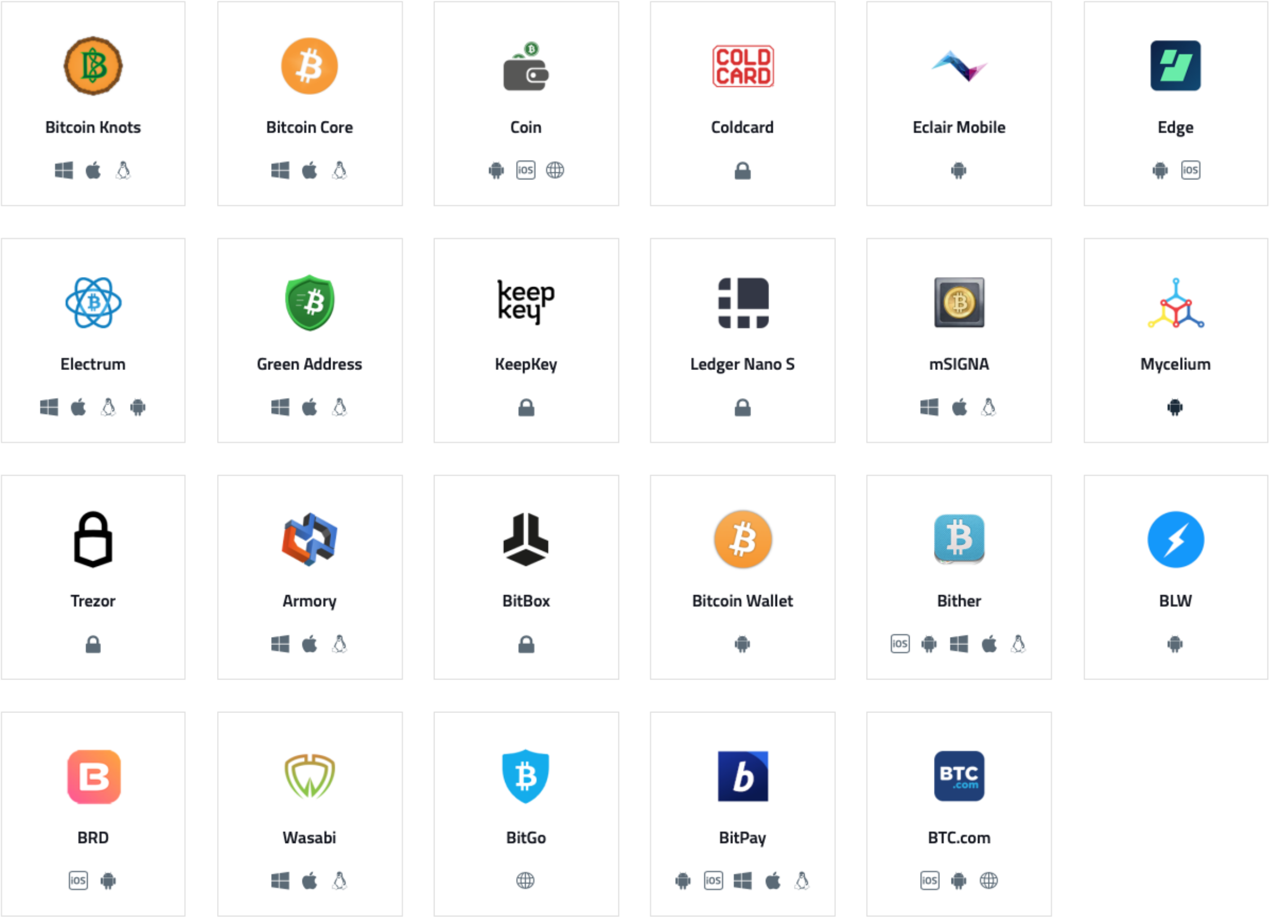


Owned cryptocurrency can be traded immediately or stored in a secure "wallet" for later use

Choose the right wallet for your security and accessibility needs

Desktop WALLET	Online & mobile WALLETS	Hardware WALLET	Paper WALLET
			image via bitcoinpaperwallet.com
Single computer has access to wallet through keys saved to the hard drive	Stored on a cloud system controlled by a third party, like an exchange	Wallet is stored offline in a USB or dedicated crypto device that can be accessed on a computer	Access keys are written down or printed out after generation
Security HIGH	Security MEDIUM	Security HIGH	Security HIGH
but susceptible to viruses and hacks	Can be more susceptible to theft and hacks	Highly secure access	until accessed online for deposit or withdrawal

Wallets for Bitcoins



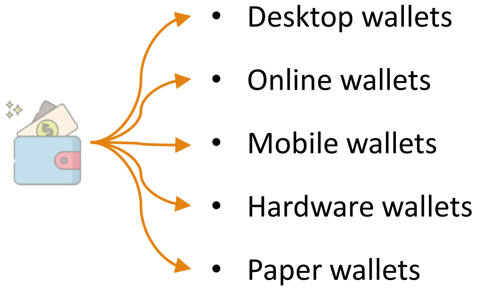
Bitcoin Knots
Bitcoin Core
Coin
Coldcard
Eclair Mobile
Edge
Electrum
Green Address
KeepKey
Ledger Nano S
mSIGNA
Mycelium
Trezor
Armory
BitBox
Bitcoin Wallet
Bither
BLW
BRD
Wasabi
BitGo
BitPay
BTC.com

Types of Wallets

Wallet store keys that user can access to cryptocurrency

Hot or Cold wallet?

Types of wallet:



- Desktop wallets
- Online wallets
- Mobile wallets
- Hardware wallets
- Paper wallets

Deterministic and non-deterministic wallets

- Deterministic start with a seed to the keys

Hierarchical deterministic wallets

About Wallets

WITHIN THE WALLET

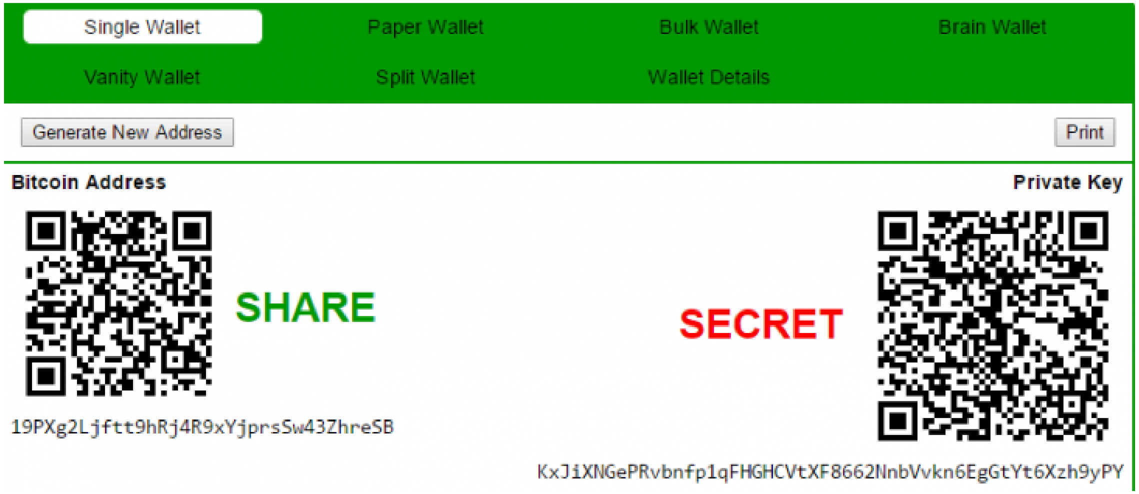
1. keypairs for each of your addresses (a keypair consists of a "public key" and a "private key”)
2. transactions done from/to your addresses
3. user preferences
4. default key
5. reserve keys
6. accounts
7. a version number
8. Key pool

Paper Wallet

A bitcoin paper wallet is simply a public and private key printed together.

It is an offline wallet, and is usually regarded as a type of “cold storage” (extra-secure storage that does not make contact with the hackable internet)

For load & verify



Bitcoin Address

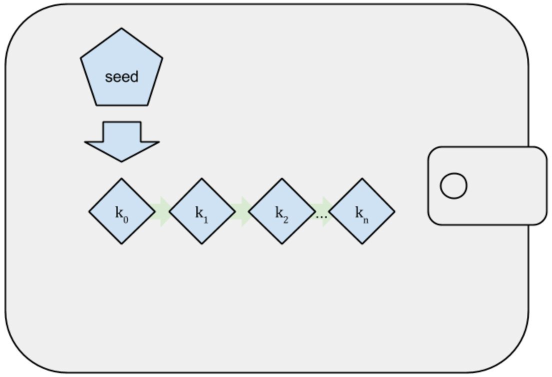
19PXg2Ljftt9hRj4R9xYjprsSw43ZhreSB

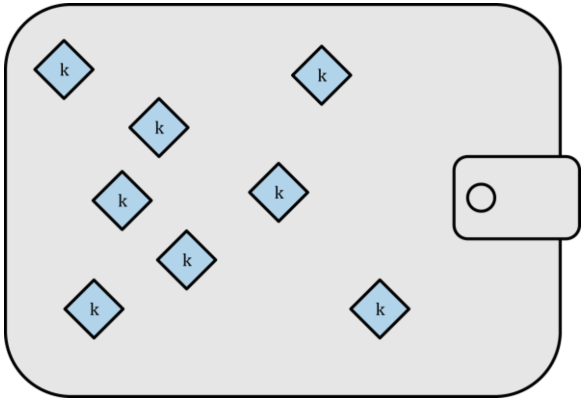
Private Key

KxJiXNGePRvbnfp1qFHGHCVtXF8662NnbVvkn6EgGtYt6Xzh9yPY

The private key used for signing the bitcoin for spending

Deterministic vs Non-deterministic wallet





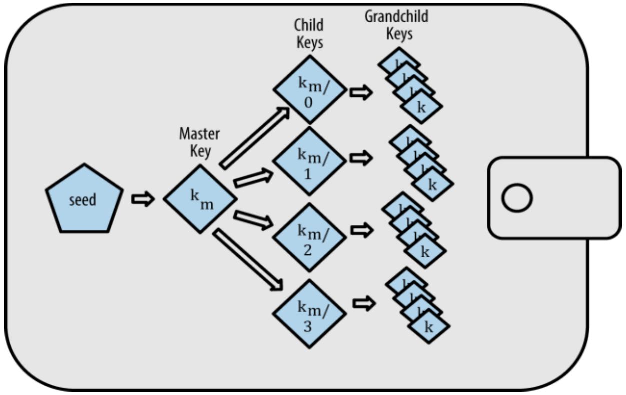
- Deterministic (seeded) Wallet
- Non-deterministic (random) Wallet

Hierarchical deterministic or HD wallet.

Deterministic wallets were developed to make it easy to derive many keys from a single "seed."

The most advanced form of deterministic wallets is the HD wallet defined by the BIP-32 standard.

HD wallets contain keys derived in a tree structure, such that a parent key can derive a sequence of children keys, each of which can derive a sequence of grandchildren keys, and so on, to an infinite depth.



BIP39, BIP32, BIP44

BIP39 is the the 39th Bitcoin Improvement Proposal (BIP). It is a common and useful standard in crypto wallets.

BIP39 defines how wallets create seed phrases and generate encryption keys

A BIP39 seed phrase created with appropriate randomness can not be guessed through brute force, because there are simply too many permutations.

A BIP39 mnemonic sentence is a set of words (most commonly 12 or 24) that humans can interact with more successfully than we do characters that are not words

BIP32 ("Hierarchical deterministic wallets") lays out a framework for Hierarchical Deterministic wallets (HD Wallets) so that they can be shared.

BIP44 ("Multi-account hierarchy for deterministic wallets") defines an organizational hierarchy for managing multiple accounts in deterministic wallets.

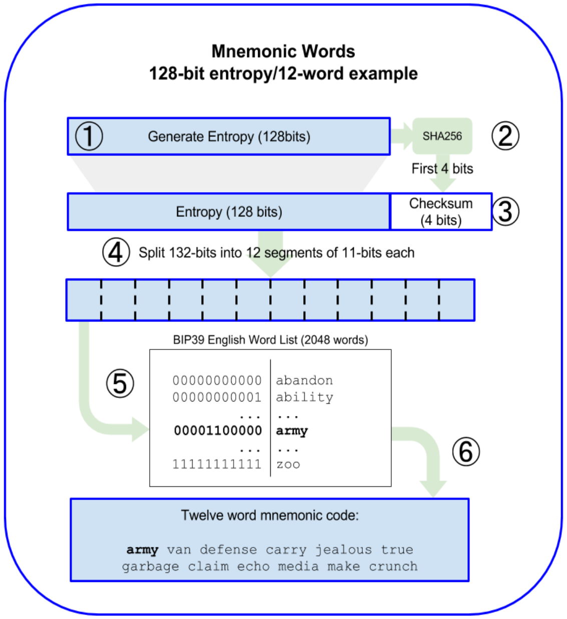
How to secure backup and retrieve private key

Mnemonic code words approach has been standardized by BIP-39.

The currently preferred method is using a sequence of words that, when taken together in the correct order, can uniquely recreate the private key.

Mnemonic code words are word sequences that encode a random number used as a seed to derive a deterministic wallet

A wallet application that implements deterministic wallets with mnemonic words will show the user a sequence of 12 to 24 words when first creating a wallet.


Mnemonic Words
128-bit entropy/12-word example
① Generate Entropy (128bits)
SHA256 ②
First 4 bits
Entropy (128 bits)
Checksum (4 bits) ③
④ Split 132-bits into 12 segments of 11-bits each
BIP39 English Word List (2048 words)
⑤
⑥

00000000000	abandon
00000000001	ability
...	...
00001100000	**army**
...	...
11111111111	zoo

Twelve word mnemonic code:

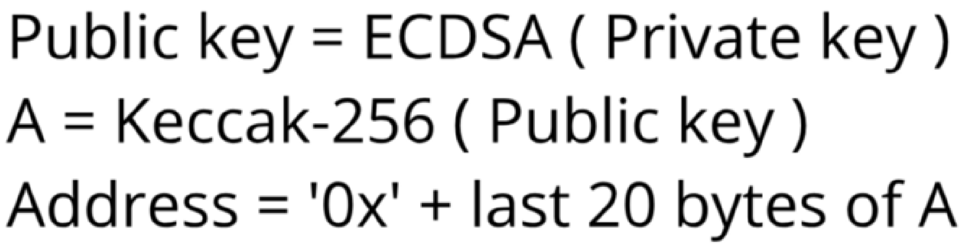
army van defense carry jealous true garbage claim echo media make crunch

https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

Extra notes about Wallet

Ethereum wallet address

- Made from public key
- Apply Keccak-256 to the key
- Then take the last 20 bytes of the result
- ‘0x’ at the start of address
- (No base58 conversion)



Public key = ECDSA (Private key)

A = Keccak-256 (Public key)

Address = '0x' + last 20 bytes of A

Ethereum Wallets

MetaMask

- MetaMask is a browser extension wallet that runs in your browser (Chrome, Firefox, Opera, or Brave Browser). It is easy to use and convenient for testing, as it is able to connect to a variety of Ethereum nodes and test blockchains. Meta- Mask is a web-based wallet.

Jaxx

- Jaxx is a multiplatform and multicurrency wallet that runs on a variety of operating systems, including Android, iOS, Windows, macOS, and Linux. It is often a good choice for new users as it is designed for simplicity and ease of use. Jaxx is either a mobile or a desktop wallet, depending on where you install it.

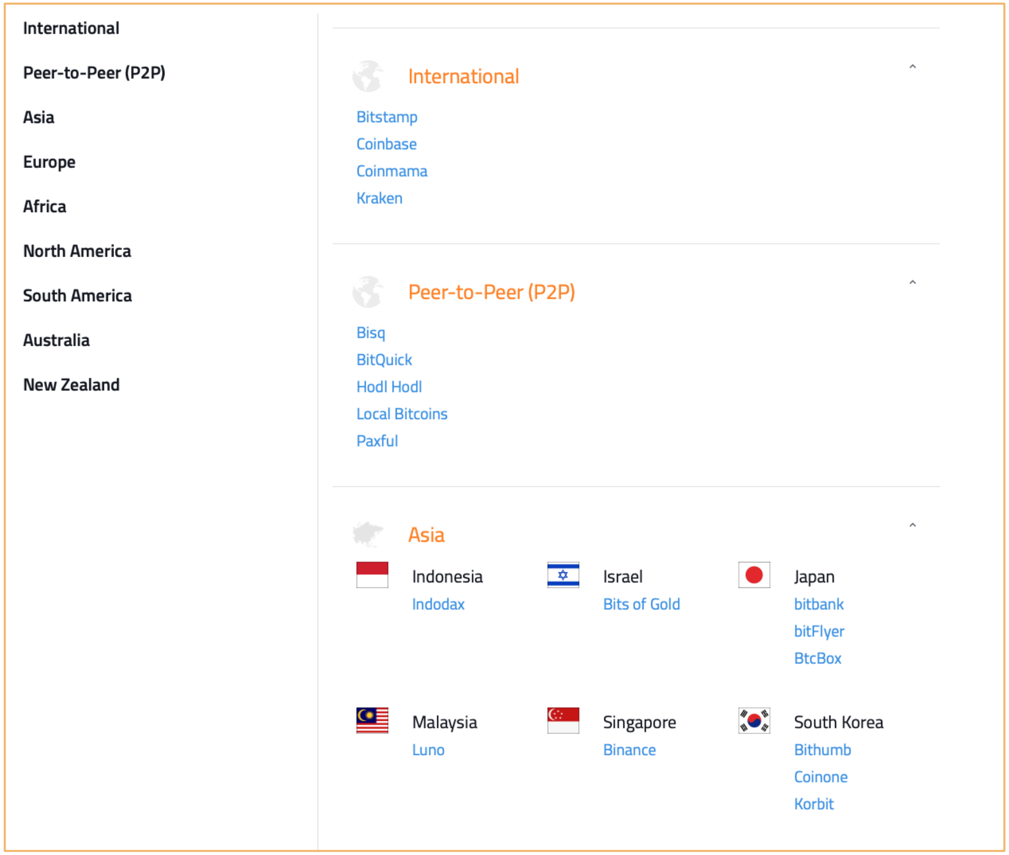
MyEtherWallet (MEW)

- MyEtherWallet is a web-based wallet that runs in any browser. It has multiple sophisticated features we will explore in many of our examples. MyEtherWallet is a web-based wallet.

Emerald Wallet

- Emerald Wallet is designed to work with the Ethereum Classic blockchain, but is compatible with other Ethereum-based blockchains. It's an open source desktop application and works under Windows, macOS, and Linux. Emerald Wallet can run a full node or connect to a public remote node, working in a "light" mode. It also has a companion tool to do all operations from the command line.

Bitcoin exchange



International

Peer-to-Peer (P2P)

Asia

Europe

Africa

North America

South America

Australia

New Zealand

International

Bitstamp
Coinbase
Coinmama
Kraken

Peer-to-Peer (P2P)

Bisq
BitQuick
Hodl Hodl
Local Bitcoins
Paxful

Asia

Country	Exchanges
Indonesia	Indodax
Israel	Bits of Gold
Japan	bitbank bitFlyer BtcBox
Malaysia	Luno
Singapore	Binance
South Korea	Bithumb Coinone Korbit

Online Wallets and Exchanges

Coinbase: San Francisco, CA

- Founded in 2012, Coinbase is a wallet, an exchange, and a set of tools for merchants, all built on the same platform

Binance: multiple locations in Asia

- Launched just last year by Changpeng " CZ" Zhao, Binance has quickly become one of the world’s largest crypto exchanges. After moving its offices out of China and its servers offshore, Binance now supports more than 130 coins and consistently processes over $1 billion in transaction value over a 24-hour period.
- Regulation: Little regulation. Has been warned by regulators in Japan and Hong Kong.

Kraken: San Francisco, California

- On the Kraken platform, users can deposit and withdraw funds using several fiat currencies, including the Euro, US Dollar, the British Pound, the Yen, and the Canadian dollar.
- Kraken offers proof-of-reserves audits and is a partner in the first cryptocurrency bank.

Online Wallets and Exchanges (Hong Kong)

BitMEX: Hong Kong

- BitMEX is the Bitcoin Mercantile Exchange, a platform intended for dedicated traders rather than retail investors. It consistently processes over $2 billion in transactions in a 24-hour period

OKEx: Hong Kong

- OKEx, based in Hong Kong and helmed by CEO Chris Lee, is a robust trading platform with access to 145 coins. The exchange announced in May that it will expand to Malta, citing the country's "comprehensive blockchain initiatives.
- OKEx does not serve customers certain countries, including Hong Kong, Cuba, Iran, North Korea, Sudan, Bolivia, Ecuador, Kyrgyzstan, and the United States, due to regulatory issues.
- Regulation: Not governed by U.S. entity. Will be subject to Maltese regulations following upcoming move.

Online Wallets and Exchanges (Hong Kong)

Bitfinex: Hong Kong

- Bitfinex, founded in 2012 and headquartered in Hong Kong, is also unavailable to US customers due to an uncertain regulatory environment.
- In 2016, Bitfinex lost more than $70 million in bitcoin after the exchange was compromised by hackers.
- Regulation: Incorporated in the U.S. Virgin Islands. Little regulation.

HitBTC: Hong Kong

- HitBTC launched in 2013 and is currently based in Hong Kong. It bills itself as the “most advanced cryptocurrency exchange,” and offers features like a rebate system for market makers and an advanced matching algorithm.
- Regulation: Little regulation. Preparing to launch a licensed subsidiary in Japan.

Bit-Z: Hong Kong, Beijing, Singapore

- Bit-Z was founded in 2016 and has offices in Hong Kong, Beijing, and Singapore. It caters to Chinese customers. According to CoinMarketCap, the exchange hosts 105 active markets.

Securing Wallet

Backup the Keys—Backing up your wallet keys can save you a lot of turmoil and trouble.

Cold Storage—Cold storage is achieved when crypto currency private keys are created and stored in a secure offline environment

Hardware Wallet—These are the physical devices created to keep your crypto currency safe.

Multi-Signature—Wallets are advanced security configuration available with most of the crypto currency platforms and supported by most of the popular wallets. Multi-signature wallets, m-of-n co-signers

Excerpt From: Sarah Swammy. “Crypto Uncovered”. Apple Books.

Digital Wallet and Payment

Payment method

- Secure Communication Medium (NFC payment)
- Fast Secure Authentication and Secure Tamper Proof Storage

Decentralized Finance (DeFi)

Decentralized finance (DeFi) is an emerging financial technology based on secure distributed ledgers similar to those used by cryptocurrencies.

The system removes the control banks and institutions have on money, financial products, and financial services.

A distributed database is accessible across various locations; it collects and aggregates data from all users and uses a consensus mechanism to verify it.

DeFi uses a layered architecture and highly composable building blocks

By Oct 2020, more than $11 billion (in cryptocurrency). In the first quarter of 2021, $217 billion in transactions flowed through decentralized exchanges

The DeFi space is rapidly expanding and their TVLs surpassed over USD 100 billion as of December 2021.

Benefit of DeFi

- eliminates the fees that banks and other financial companies charge
- hold money in a secure digital wallet
- Can perform transaction without need of approval
- can transfer funds in seconds and minutes
- Openness
- Accessibility

Types of DeFi

DeFi revolves around decentralized applications, also known as Dapps.

- Dapps that perform financial functions on distributed ledgers called blockchains, a technology that was made popular by Bitcoin and has since been adapted more broadly
- Transactions are directly made between participants, mediated by smart contract programs. These smart contracts, or DeFi protocols, typically run using open-source software that is built and maintained by a community of developers

Another DeFi is a decentralized exchange (DEX) set up to trade tokens issued on Ethereum.

- Rather than using a centralized exchange to fill orders, Uniswap pays users to form liquidity pools in exchange for a percentage of the fees that traders earn by swapping tokens in and out of the liquidity pools.

What is DeFi

DeFi applications include:

- Marketplaces
- Payment solutions
- Borrowing/Lending
- Exchange and liquidity
- Stablecoins
- Decentralized Autonomous Organizatin (DAO)
- Derivatives
- Insurance
- Etc…

Types of exchanges

Centralized exchanges

- Centralized exchange platform for swap between currencies and cryptocurrencies such as Coinbase, Huobi, Binance
- Use order books to match buyers and sellers on the open market and keep crypto assets in an exchange-based wallet

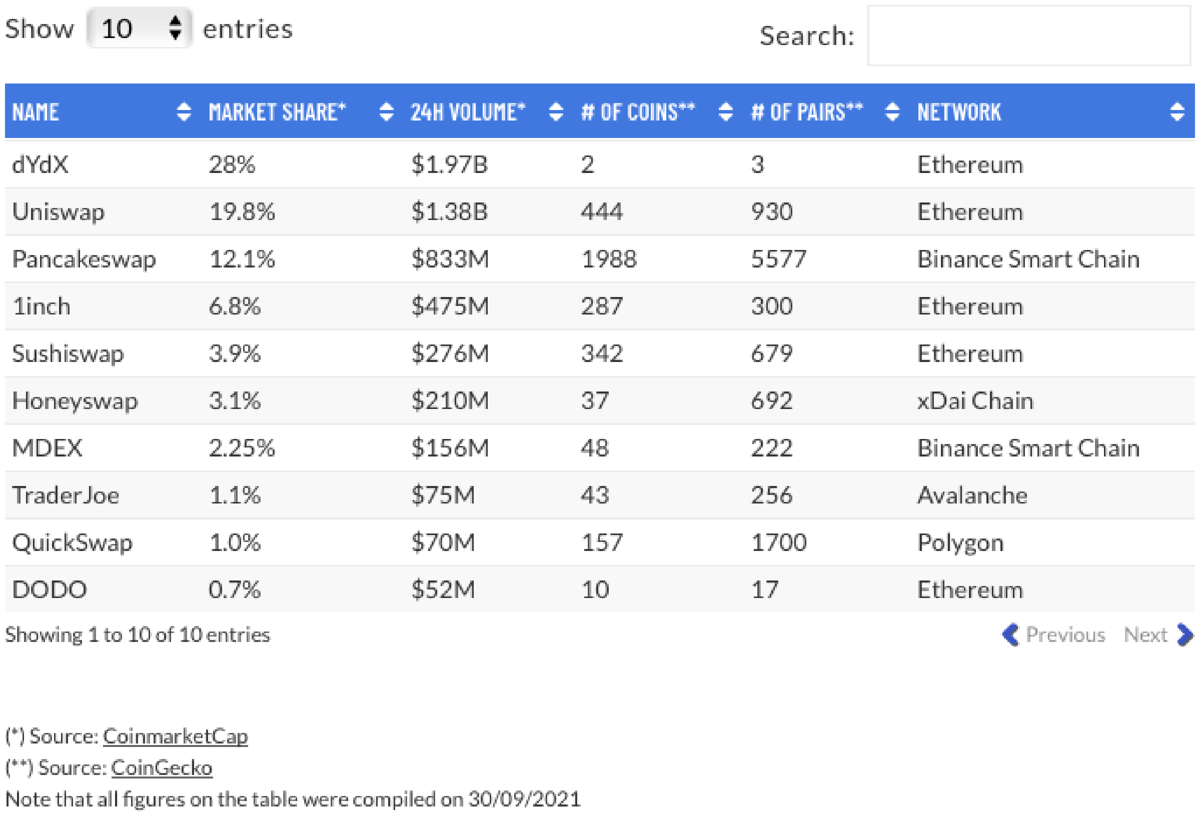
Decentralized exchanges (DEXs)

- DEXs allow users to swap one currency for another, such as USD for BTC or Ether (ETH) for Tether (USDT)
- Exchange that links users directly, so they can trade cryptocurrencies without entrusting their funds to an intermediary
- DEXs are non-custodial and leverage the functionality of self-executing smart contracts for peer-to-peer trading

Stablecoins

- A cryptocurrency that is linked to a non-cryptocurrency asset (USD, EUR, GBP, etc.) in order to keep its price stable.

Top 10 DeFi Exchanges

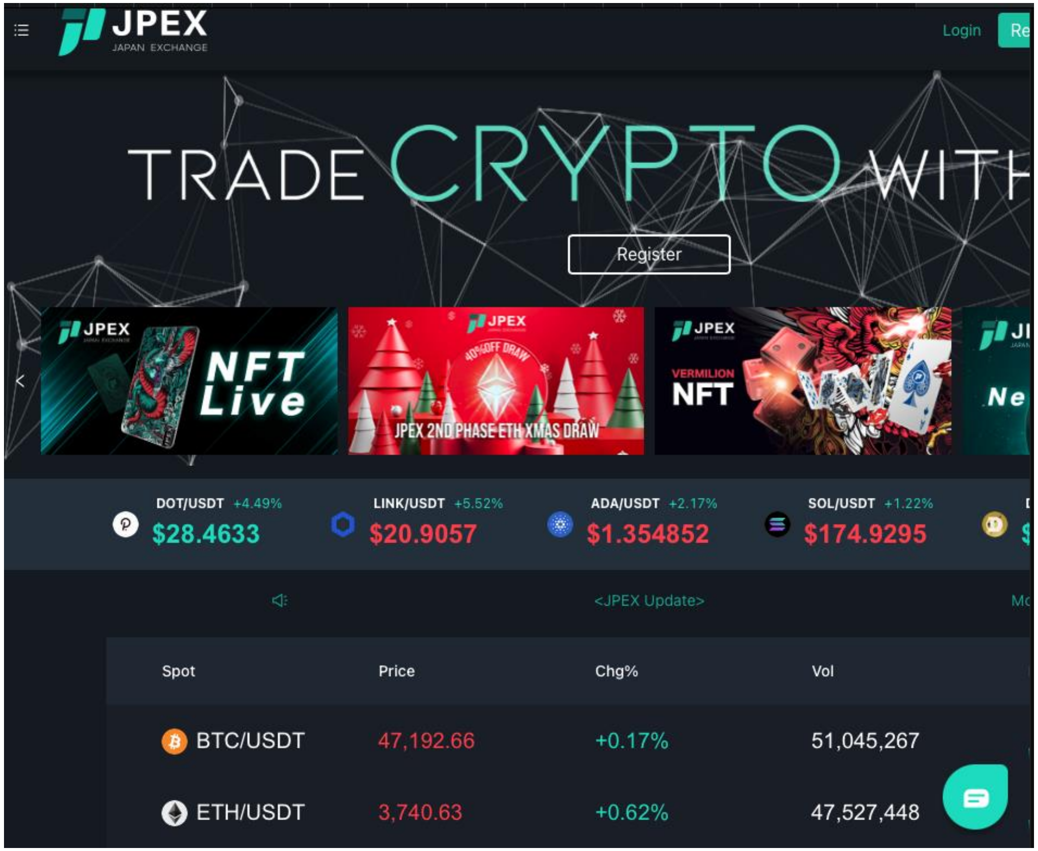


NAME	MARKET SHARE*	24H VOLUME*	# OF COINS**	# OF PAIRS**	NETWORK
dYdX	28%	$1.97B	2	3	Ethereum
Uniswap	19.8%	$1.38B	444	930	Ethereum
Pancakeswap	12.1%	$833M	1988	5577	Binance Smart Chain
1inch	6.8%	$475M	287	300	Ethereum
Sushiswap	3.9%	$276M	342	679	Ethereum
Honeyswap	3.1%	$210M	37	692	xDai Chain
MDEX	2.25%	$156M	48	222	Binance Smart Chain
TraderJoe	1.1%	$75M	43	256	Avalanche
QuickSwap	1.0%	$70M	157	1700	Polygon
DODO	0.7%	$52M	10	17	Ethereum

Showing 1 to 10 of 10 entries

(*) Source: CoinmarketCap
(**) Source: CoinGecko
Note that all figures on the table were compiled on 30/09/2021

New Exchange platform – JPEX (2021)



DOT/USDT +4.49% $28.4633

LINK/USDT +5.52% $20.9057

ADA/USDT +2.17% $1.354852

SOL/USDT +1.22% $174.9295

Spot	Price	Chg%	Vol
BTC/USDT	47,192.66	+0.17%	51,045,267
ETH/USDT	3,740.63	+0.62%	47,527,448

DeFi - MakerDAO

MakerDAO is a prominent lending DeFi platform based on a stablecoin that was established in 2017.

It is an open-source project on the Ethereum blockchain and a Decentralized Autonomous Organization

It allows users to borrow Dai. Dai is a decentralized, unbiased, collateral-backed cryptocurrency soft-pegged to the US Dollar. It is also known as a stablecoin.

The Maker Protocol is one of the largest dapps on the Ethereum blockchain.

Through a set of smart contracts that govern the loan, repayment, and liquidation processes, MakerDAO aims to maintain the stable value of Dai in a decentralized and autonomous manner.

DEXs - Uniswap

A decentralized exchange (better known as a DEX) is a peer-to-peer marketplace where transactions occur directly between crypto traders.

Uniswap is a decentralized finance protocol that is used to exchange cryptocurrencies.

As of October 2020, Uniswap was estimated to be the largest decentralized exchange and the fourth-largest cryptocurrency exchange overall by daily trading volume.

Uniswap uses liquidity pools rather than serving as market maker, also in contrast to centralized exchanges, with an aim to create more efficient markets.

Provide liquidity to the exchange by adding a pair of tokens to a smart contract which can be bought and sold by other users.

By supplying tokens to Uniswap liquidity pools, users can earn rewards while enabling peer-to-peer trading.

Utilize the Ethereum blockchain and are part of the growing suite of decentralized finance (DeFi) tools

DEXs - Uniswap

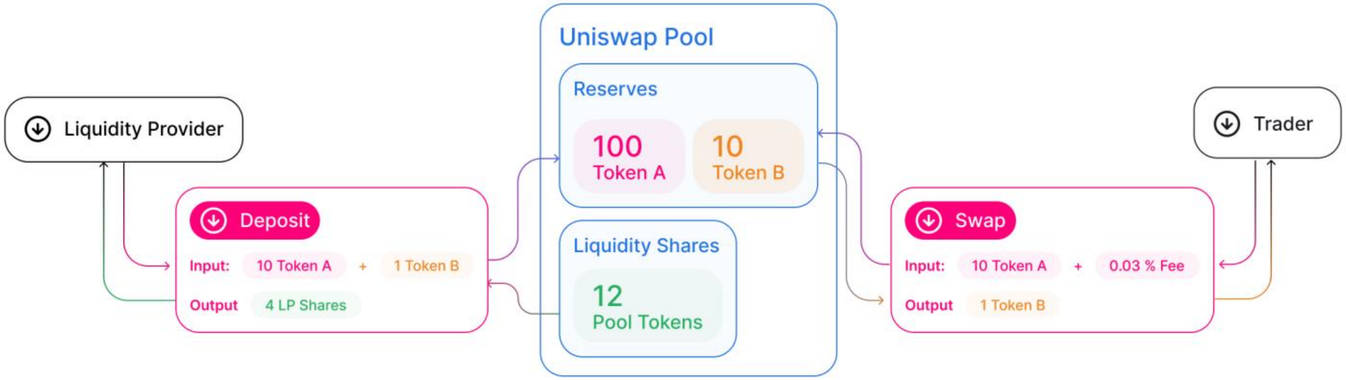
A liquidity pool can be thought of as a pot of cryptocurrency assets locked within a smart contract. The funds can then be used for exchanges, loans and for many other applications.

A liquidity provider (LP) is a user that supplies a liquidity pool with cryptocurrency assets so that the funds can then be used for the associated DeFi protocol.

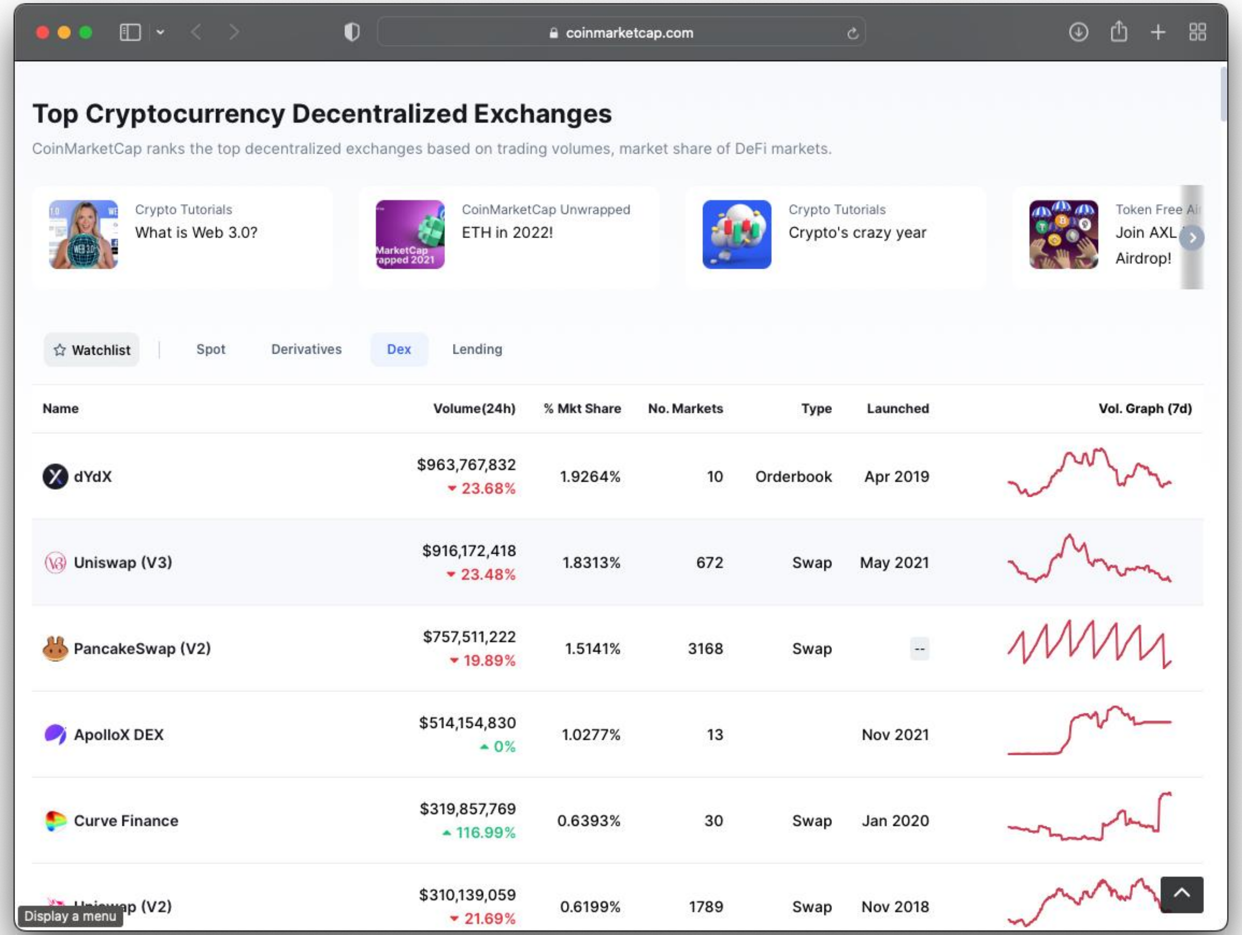
Liquidity providers are given a percentage of the trading fees earned for that trading pair. Use liquidity pools — in which investors lock funds in exchange for interest-like rewards — to facilitate trades.

Unlike centralized exchanges like Coinbase, DEXs do not allow for exchanges between fiat and crypto

DEX use crypto wallet such as Metamask or Coinbase Wallet. Then transaction will be processed through the wallet



Example of some DEXs



Top Cryptocurrency Decentralized Exchanges

CoinMarketCap ranks the top decentralized exchanges based on trading volumes, market share of DeFi markets.

Name	Volume(24h)	% Mkt Share	No. Markets	Type	Launched	Vol. Graph (7d)
dYdX	$963,767,832 ▾ 23.68%	1.9264%	10	Orderbook	Apr 2019	
Uniswap (V3)	$916,172,418 ▾ 23.48%	1.8313%	672	Swap	May 2021	
PancakeSwap (V2)	$757,511,222 ▾ 19.89%	1.5141%	3168	Swap	--	
ApolloX DEX	$514,154,830 ▴ 0%	1.0277%	13		Nov 2021	
Curve Finance	$319,857,769 ▴ 116.99%	0.6393%	30	Swap	Jan 2020	
Uniswap (V2)	$310,139,059 ▾ 21.69%	0.6199%	1789	Swap	Nov 2018	

Risks of DeFi

Technical Concerns

- DeFi/Smart contracts concern
- Availability concern in blockchain
- Hack and exploit attacks

Business Concerns

- cryptocurrency projects are merely finding new variations of unregistered securities

Liquidity Pools vs Order Books

ORDER BOOKS

The order book is a collection of the currently open orders for a given market

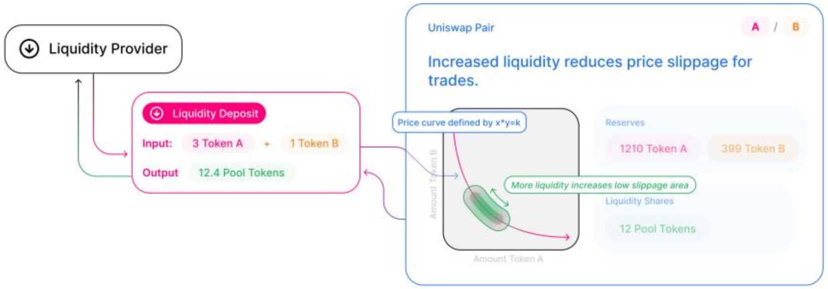
The system that matches orders with each other is called the matching engine.

Along with the matching engine, the order book is the core of any centralized exchange (CEX)

LIQUIDITY POOLS

Automated market makers (AMM) allows for on-chain trading without the need for an order book.

Traders can get in and out of positions on token pairs that likely would be highly illiquid on order book exchanges.


Liquidity Provider
Liquidity Deposit
Input:
3 Token A
+
1 Token B
Output
12.4 Pool Tokens
Uniswap Pair
A / B
Increased liquidity reduces price slippage for trades.
Price curve defined by x*y=k
Amount Token B
Amount Token A
More liquidity increases low slippage area
Reserves
1210 Token A
399 Token B
Liquidity Shares
12 Pool Tokens