KAIST School of Computing

Web3@KAIST

Building Web3 Apps to Solve Real Problems

Building Web3 & Blockchain Applications
(CS492 Special Topics in Computer Science)
Spring 2023

Web3 Stack and Apps

Lecture 2 (2023-03-08)

Jason Han, Ph.D

Adjunct Professor of KAIST School of Computing
Founder of Ground X & Klaytn

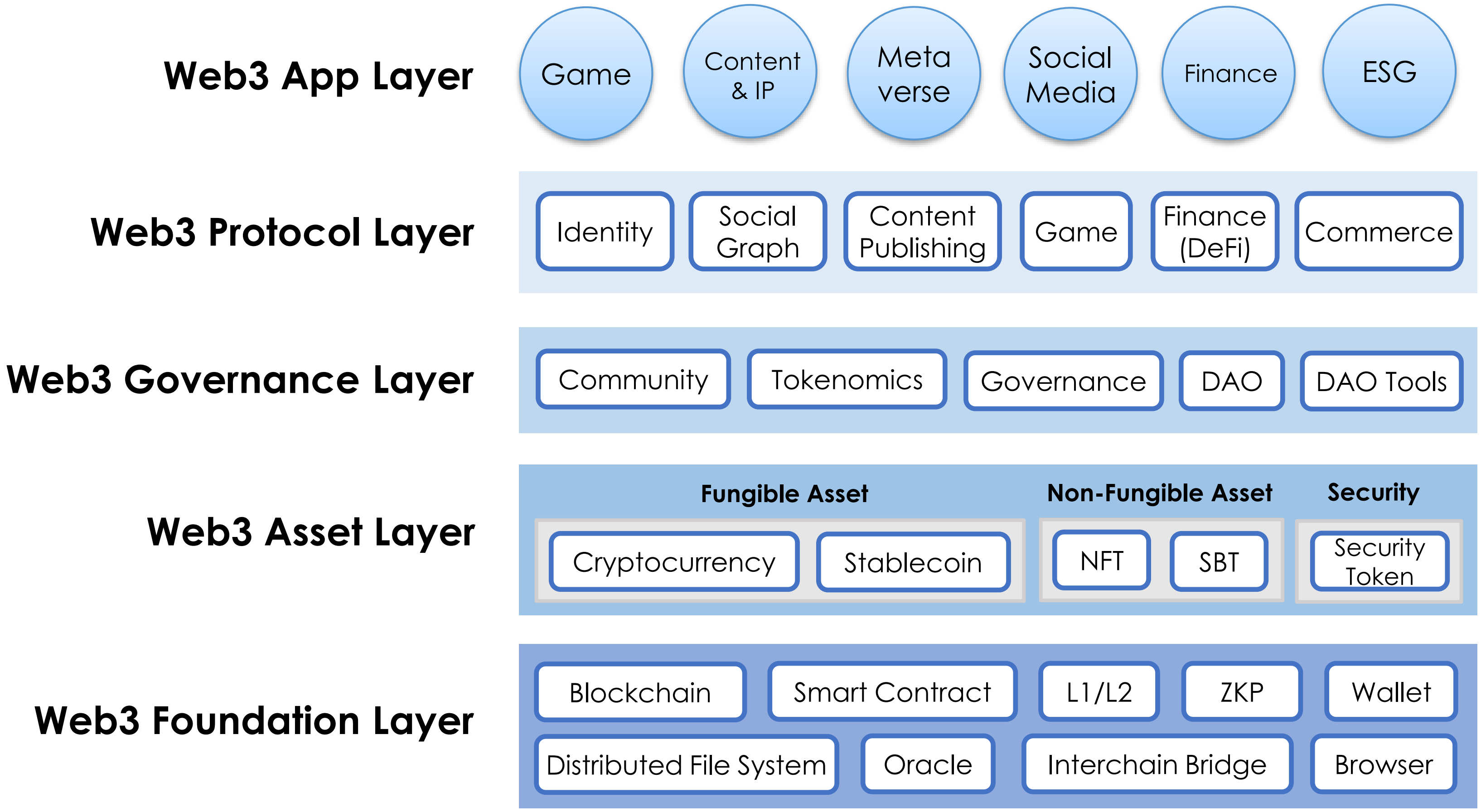
web3classdao@gmail.com
http://web3classdao.xyz/kaist/

Disclaimer: The information provided in this presentation is for educational and informational purposes only and should not be construed as investment or purchase advice. The content of this presentation does not constitute an offer to buy or sell any securities or financial instruments, nor does it provide any recommendations regarding the suitability of any particular investment strategy or product. Any investment decision you make should be based on your own individual research, analysis, and judgment. We do not guarantee the accuracy, completeness, or reliability of any information contained in this presentation, and we shall not be held responsible for any loss or damage arising from reliance on the content of this presentation. Please consult with a qualified investment advisor or financial professional before making any investment decisions.

By chatGPT

Web3 Stack

Web3 Stack (in the view of data)



Web3 App Layer

Game | Content & IP | Meta verse | Social Media | Finance | ESG

Web3 Protocol Layer

Identity | Social Graph | Content Publishing | Game | Finance (DeFi) | Commerce

Web3 Governance Layer

Community | Tokenomics | Governance | DAO | DAO Tools

Web3 Asset Layer

Fungible Asset: Cryptocurrency | Stablecoin

Non-Fungible Asset: NFT | SBT

Security: Security Token

Web3 Foundation Layer

Blockchain | Smart Contract | L1/L2 | ZKP | Wallet

Distributed File System | Oracle | Interchain Bridge | Browser

This class (Web3@KAIST) will address all these layers in detail

Today’s lecture will preview all these layers in the viewpoint of users

Web3 Foundation Layer

- Providing basic technologies to implement Web3
- Enhancing trust and transparency of applications
- Enabling data ownership and community governance

This class will cover

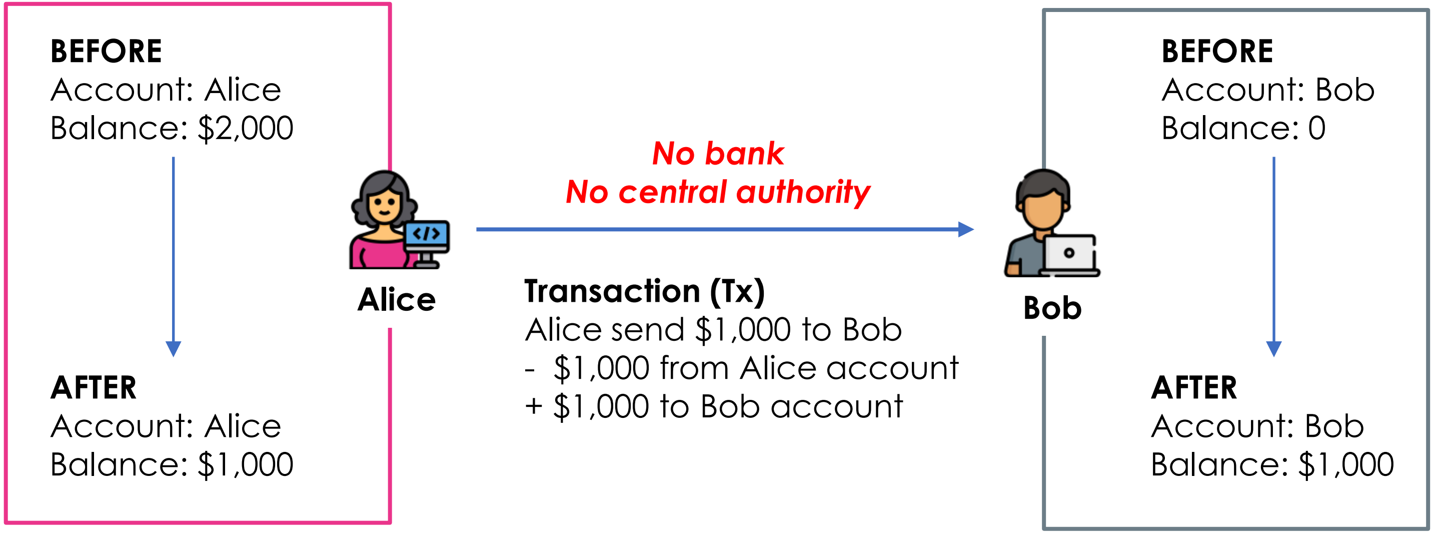
- Blockchain platforms
- Bitcoin and Ethereum
- Smart contracts
- Programming solidity
- Developing Web3 apps
- Web3 security

Tools and services

- Ethereum (platform)
- etherscan (block explorer)
- metamask (wallet)
- remix (solidity IDE)
- truffle and hardhat (web3 framework)

Trusted transactions between untrusted parties without central authorities

Alice wants to send $1,000 to Bob on Internet without banks



BEFORE
Account: Alice
Balance: $2,000

AFTER
Account: Alice
Balance: $1,000

Alice

No bank
No central authority

Transaction (Tx)
Alice send $1,000 to Bob
- $1,000 from Alice account
+ $1,000 to Bob account

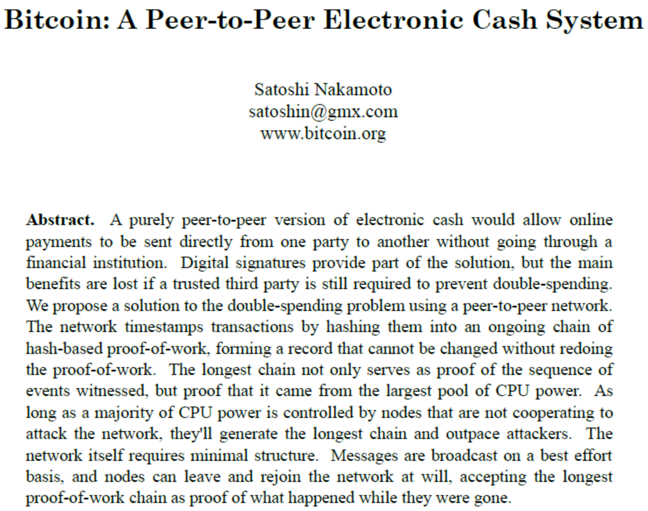
Bob

BEFORE
Account: Bob
Balance: 0

AFTER
Account: Bob
Balance: $1,000

The rise of Bitcoin

Solved
double-spending problem
of electronic cash
(Oct, 2008)



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

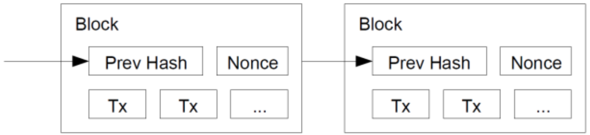
https://bitcoin.org/bitcoin.pdf

Electronic Cash (Coin)

A single app

Preventing double-spending

- Proof of Work
- Cryptographic proof of txs
- P2P network

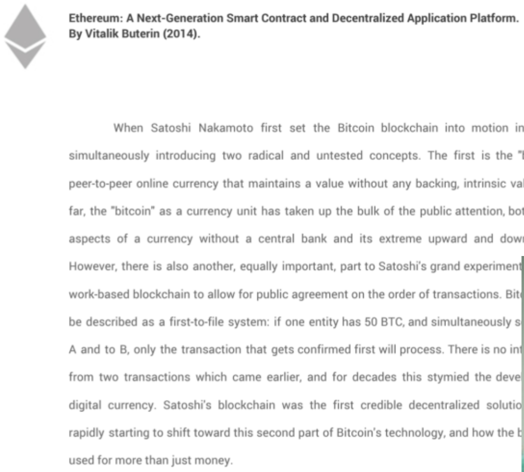


No term "blockchain"
It coined later

Bitcoin to Ethereum

Single purpose to **general-purpose blockchain**

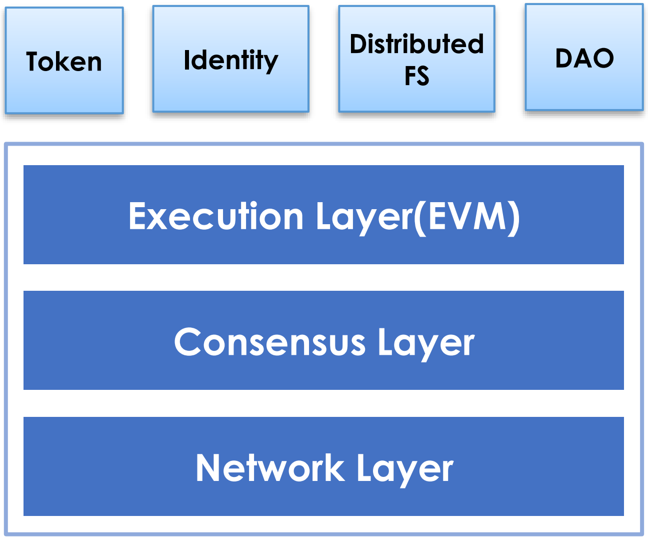
Ethereum:
A Next-Generation **Smart Contract** and
Decentralized Application Platform
(Dec, 2014)



Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.
By Vitalik Buterin (2014).

When Satoshi Nakamoto first set the Bitcoin blockchain into motion in January 2009, he was
simultaneously introducing two radical and untested concepts. The first is the "bitcoin", a decentralized
peer-to-peer online currency that maintains a value without any backing, intrinsic value or central issuer. So
far, the "bitcoin" as a currency unit has taken up the bulk of the public attention, both in terms of the political
aspects of a currency without a central bank and its extreme upward and downward volatility in price.
However, there is also another, equally important, part to Satoshi's grand experiment
work-based blockchain to allow for public agreement on the order of transactions. Bit
be described as a first-to-file system: if one entity has 50 BTC, and simultaneously s
A and to B, only the transaction that gets confirmed first will process. There is no int
from two transactions which came earlier, and for decades this stymied the deve
digital currency. Satoshi's blockchain was the first credible decentralized solutio
rapidly starting to shift toward this second part of Bitcoin's technology, and how the b
used for more than just money.

Vitalik Buterin



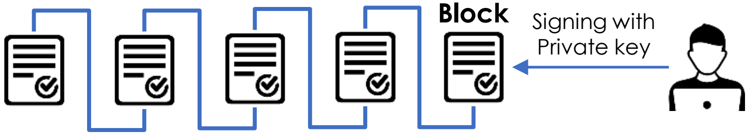
Multiple apps

Ethereum Blockchain

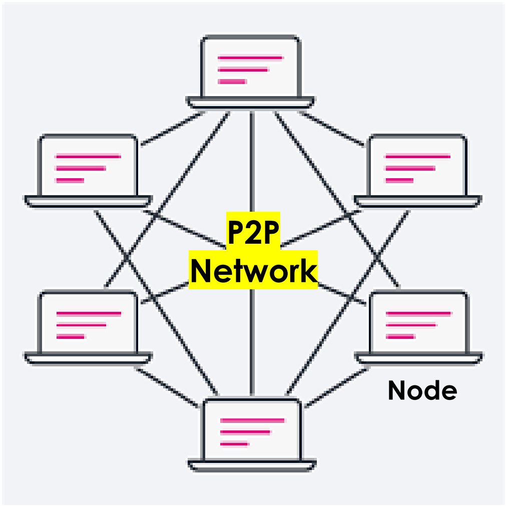
Blockchain 101

Each block cryptographically references its parent

Chain of Blocks



Managing blocks with **Consensus**



Distributed System

Cryptography

Economics

Incentive scheme
for nodes and participant

PoW, PoS, etc

Blockchain
Immutable
Open (Transparent)
Shared (Permissionless)
Distributed
Digital **Ledger**

Trust & Transparency

Since Ethereum,
hundreds of blockchain platforms
have emerged and competed.

In this class,
we'll use Ethereum as a reference.

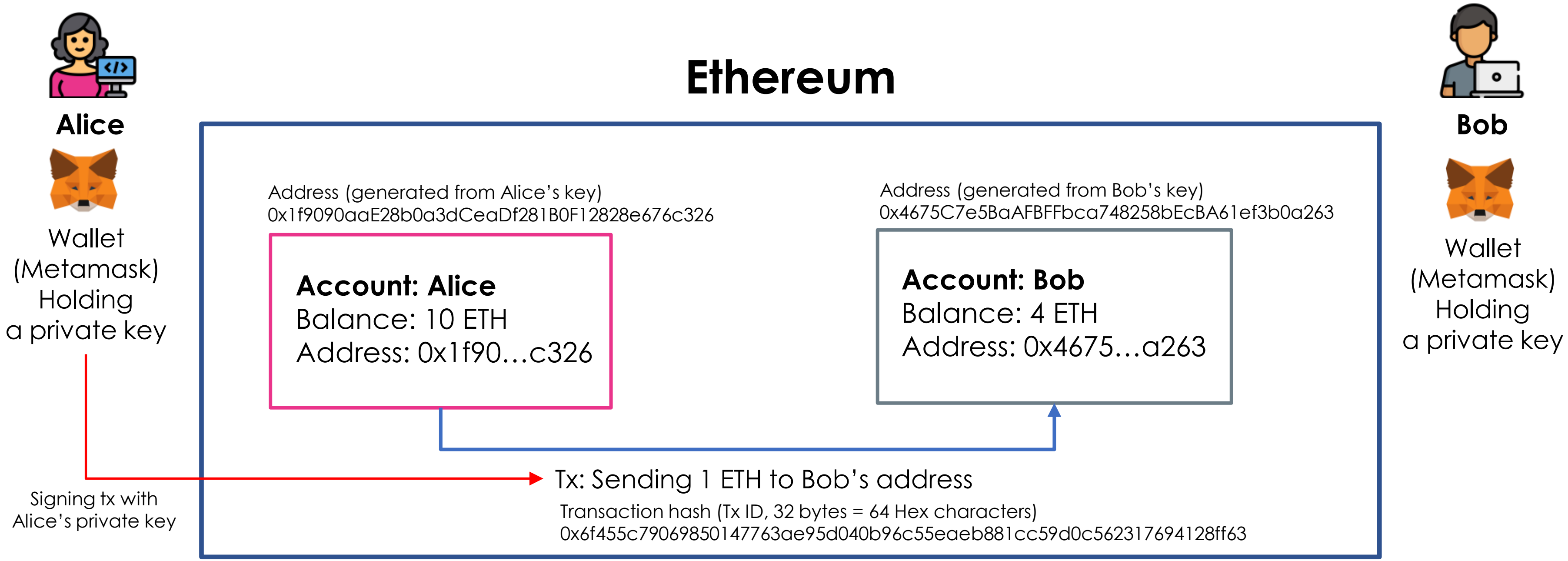
Basic terms of Ethereum, Part 1

- **Account:** An object containing an address, balance, nonce, and optional storage and code
- **externally owned account (EOA):** accounts without any code associated with them. These are controlled by private keys with a wallet.
- **Address:** Most generally, this represents an account(EOA) or contract that can receive (destination address) or send (source address) transactions on the blockchain. More specifically, it is the rightmost 160 bits(20 bytes, 40 hex characters) of a Keccak hash of an ECDSA public key. (e.g. 0x1f9090aaE28b0a3dCeaDf281B0F12828e676c326)
- **Private key (Secret key):** A secret number that allows Ethereum users to prove ownership of an account or contracts, by producing a digital signature
- **Public key**: A number, derived via a one-way function from a private key, which can be shared publicly and used by anyone to verify a digital signature made with the corresponding private key
- **Keystore:** Every account's private key/address pair exists as a single keyfile in an Ethereum client
- **Gas:** A virtual fuel used in Ethereum to execute smart contracts
- **Transaction fee**: A fee you need to pay whenever you use the Ethereum network
- **ether (ETH):** The native cryptocurrency used by the Ethereum ecosystem, which covers gas costs when executing transactions
- **wei:** The smallest denomination of ether. 10^{18} wei = 1 ether.
- **Token:** A tradable virtual good defined in smart contracts on the Ethereum blockchain
- **Wallet:** Software that holds private keys. Used to access and control Ethereum accounts and interact with smart contracts. Despite the name, wallets never store the actual coins or tokens.
- **Block explorer**: An application that allows a user to search for information from, and about, a blockchain

https://ethereum.org/en/glossary/

Sending ETH or tokens on Ethereum

Alice wants to send 1 ETH to Bob on Ethereum



Alice

Wallet
(Metamask)
Holding
a private key

Signing tx with
Alice's private key

Ethereum

Address (generated from Alice's key)
0x1f9090aaE28b0a3dCeaDf281B0F12828e676c326

Account: Alice
Balance: 10 ETH
Address: 0x1f90…c326

Address (generated from Bob's key)
0x4675C7e5BaAFBFFbca748258bEcBA61ef3b0a263

Account: Bob
Balance: 4 ETH
Address: 0x4675…a263

Tx: Sending 1 ETH to Bob's address

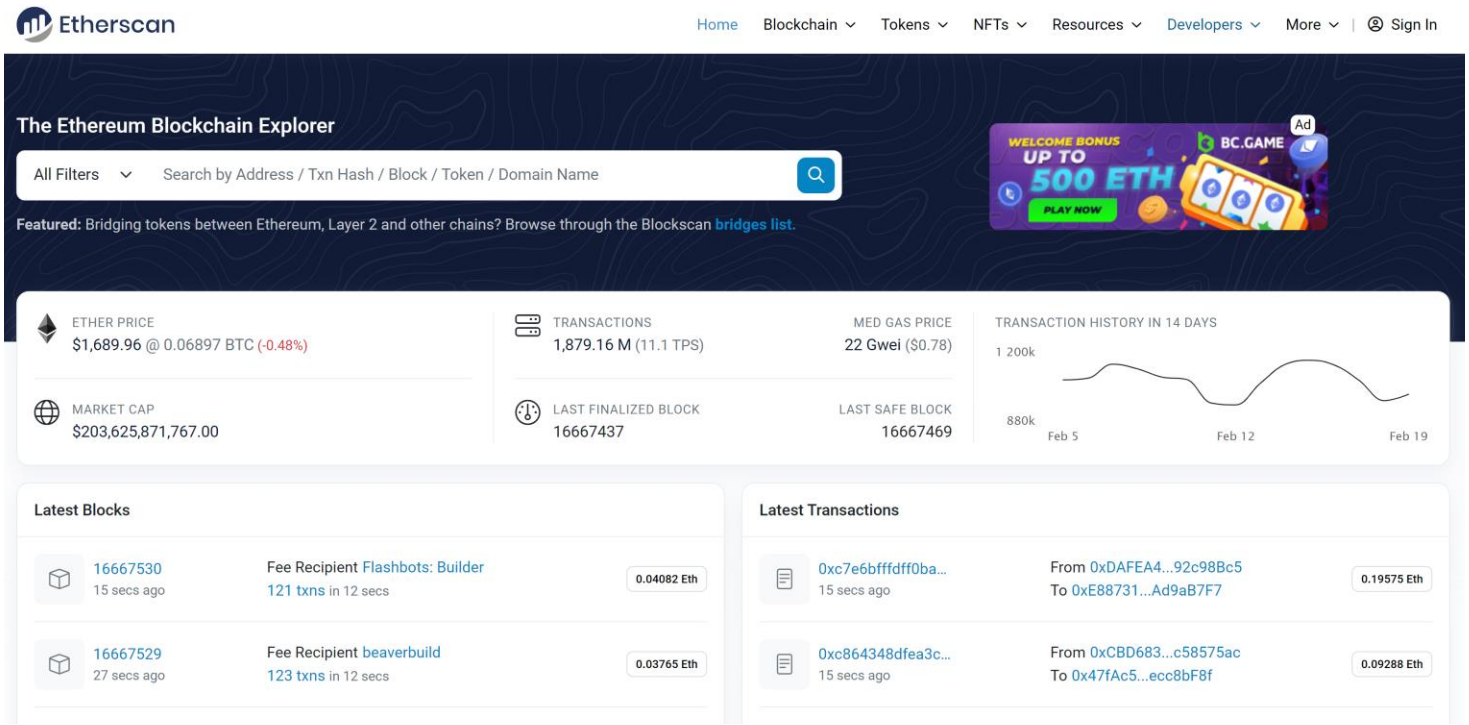
Transaction hash (Tx ID, 32 bytes = 64 Hex characters)
0x6f455c79069850147763ae95d040b96c55eaeb881cc59d0c562317694128ff63

Bob

Wallet
(Metamask)
Holding
a private key

Etherscan: Ethereum Block Explorer

You can search for all information on Ethereum



The Ethereum Blockchain Explorer

Featured: Bridging tokens between Ethereum, Layer 2 and other chains? Browse through the Blockscan bridges list.

ETHER PRICE
$1,689.96 @ 0.06897 BTC (-0.48%)

TRANSACTIONS
1,879.16 M (11.1 TPS)

MED GAS PRICE
22 Gwei ($0.78)

TRANSACTION HISTORY IN 14 DAYS

MARKET CAP
$203,625,871,767.00

LAST FINALIZED BLOCK
16667437

LAST SAFE BLOCK
16667469

Latest Blocks

16667530 15 secs ago	Fee Recipient Flashbots: Builder 121 txns in 12 secs	0.04082 Eth
16667529 27 secs ago	Fee Recipient beaverbuild 123 txns in 12 secs	0.03765 Eth

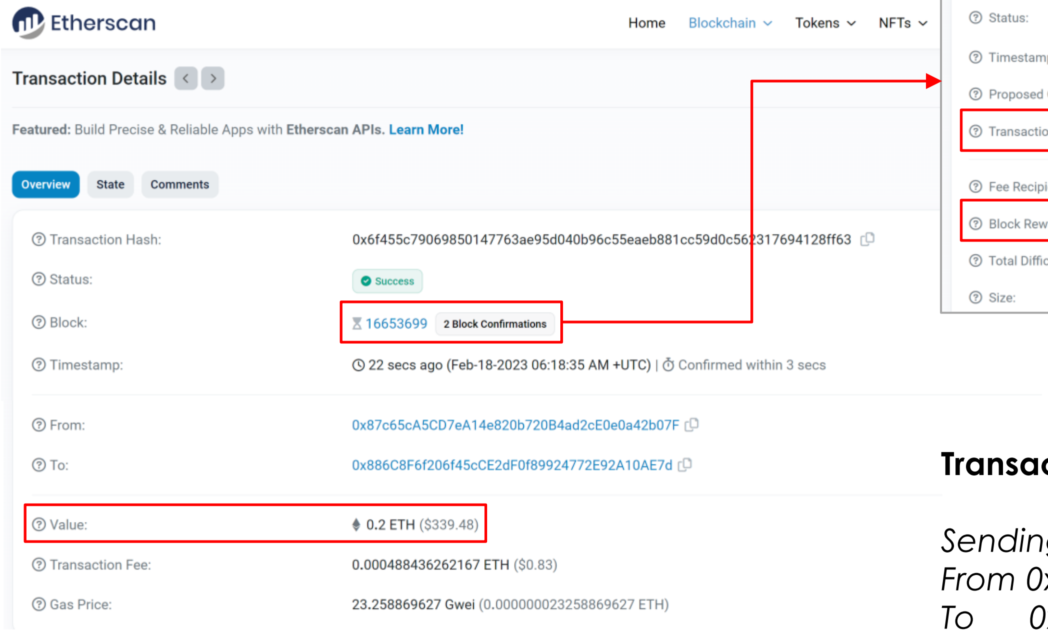
Latest Transactions

0xc7e6bfffdff0ba... 15 secs ago	From 0xDAFEA4...92c98Bc5 To 0xE88731...Ad9aB7F7	0.19575 Eth
0xc864348dfea3c... 15 secs ago	From 0xCBD683...c58575ac To 0x47fAc5...ecc8bF8f	0.09288 Eth

https://etherscan.io/

Sending Transaction on Ethereum

Transaction(tx)



Transaction Details

Featured: Build Precise & Reliable Apps with **Etherscan APIs.** **Learn More!**

Transaction Hash: 0x6f455c79069850147763ae95d040b96c55eaeb881cc59d0c562317694128ff63

Status: Success

Block: 16653699 2 Block Confirmations

Timestamp: 22 secs ago (Feb-18-2023 06:18:35 AM +UTC) | Confirmed within 3 secs

From: 0x87c65cA5CD7eA14e820b720B4ad2cE0e0a42b07F

To: 0x886C8F6f206f45cCE2dF0f89924772E92A10AE7d

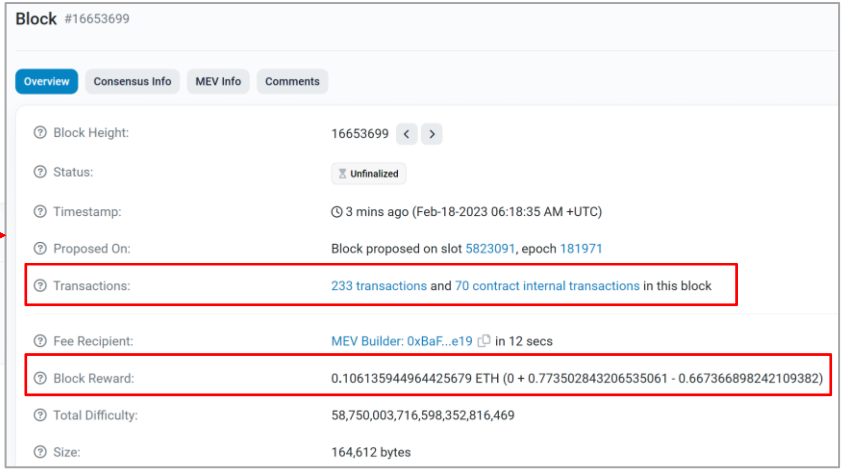
Value: 0.2 ETH ($339.48)

Transaction Fee: 0.000488436262167 ETH ($0.83)

Gas Price: 23.258869627 Gwei (0.000000023258869627 ETH)

https://etherscan.io/tx/0x6f455c79069850147763ae95d040b96c55e
aeb881cc59d0c562317694128ff63

Block



Block #16653699

Block Height: 16653699

Status: Unfinalized

Timestamp: 3 mins ago (Feb-18-2023 06:18:35 AM +UTC)

Proposed On: Block proposed on slot 5823091, epoch 181971

Transactions: 233 transactions and 70 contract internal transactions in this block

Fee Recipient: MEV Builder: 0xBaF...e19 in 12 secs

Block Reward: 0.106135944964425679 ETH (0 + 0.773502843206535061 - 0.667366898242109382)

Total Difficulty: 58,750,003,716,598,352,816,469

Size: 164,612 bytes

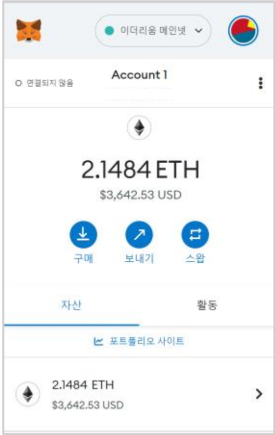
https://etherscan.io/block/16653699

Transaction 0x6f45…ff63

Sending 0.2 ETH
*From 0x87c6…b07F (**Account**)*
To 0x886C…AE7d (Account)
with the transaction fee of 0.00048 ETH ($0.83)

Metamask: A Major Ethereum Wallet

- *30 millions users worldwide*
- *Generate passwords and keys on your device (Keep it secure!)*
- *Enable users to store Ether and other ERC-20 tokens*
- *Allow users to grant access and approvals to blockchain-based applications*
- *Support multiple mainnets (L1 / L2) and testnets*



● 이더리움 메인넷

○ 연결되지 않음

Account 1

2.1484 ETH

$3,642.53 USD

구매 보내기 스왑

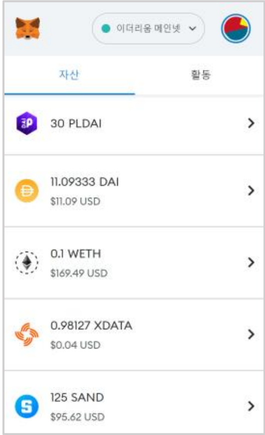
자산 활동

포트폴리오 사이트

2.1484 ETH

$3,642.53 USD

Ethereum



● 이더리움 메인넷

자산 활동

30 PLDAI

11.09333 DAI

$11.09 USD

0.1 WETH

$169.49 USD

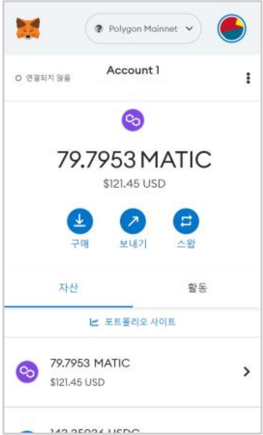
0.98127 XDATA

$0.04 USD

125 SAND

$95.62 USD

Ethereum Tokens



Polygon Mainnet

○ 연결되지 않음

Account 1

79.7953 MATIC

$121.45 USD

구매 보내기 스왑

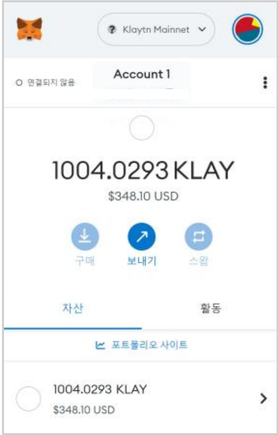
자산 활동

포트폴리오 사이트

79.7953 MATIC

$121.45 USD

Polygon



Klaytn Mainnet

○ 연결되지 않음

Account 1

1004.0293 KLAY

$348.10 USD

구매 보내기 스왑

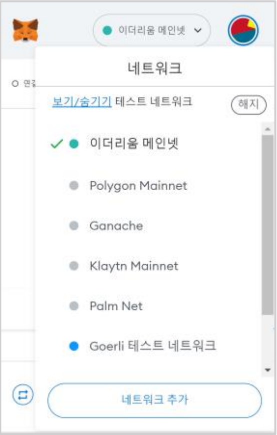
자산 활동

포트폴리오 사이트

1004.0293 KLAY

$348.10 USD

Klaytn



● 이더리움 메인넷

네트워크

보기/숨기기 테스트 네트워크 해지

✓ ● 이더리움 메인넷

● Polygon Mainnet

● Ganache

● Klaytn Mainnet

● Palm Net

● Goerli 테스트 네트워크

네트워크 추가

Multi Mainnet Support

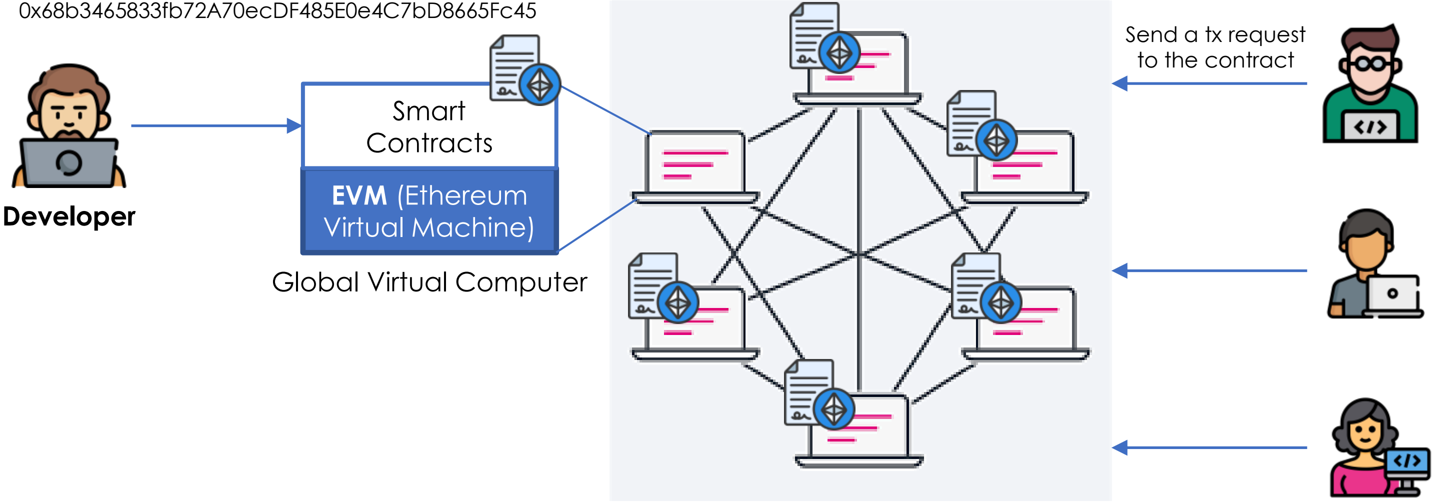
Basic terms of blockchain, Part 2

- **Smart contract:** A program that executes on the Ethereum computing infrastructure
- **Contract account:** An account containing code that executes whenever it receives a transaction from another account (EOA or contract)
- **Dapp**: Decentralized application. At a minimum, it is a smart contract and a web user interface
- **Ethereum Virtual Machine (EVM):** A stack-based virtual machine that executes bytecode
- **Internal transaction:** A transaction sent from a contract account to another contract account or an EOA
- **Solidity:** The most popular and most frequently used language for Ethereum smart contracts
- **Mainnet:** Short for "main network," this is the main public Ethereum blockchain
- **Testnet:** Short for "test network," a network used to simulate the behavior of the main Ethereum network
- **On-chain:** Data that is stored or a process that is implemented and executed within a blockchain system
- **Off-chain:** Data that is stored or a process that is implemented and executed outside of any blockchain system

https://ethereum.org/en/glossary/

Smart Contracts

A program that runs on the blockchain
Immutable and **irreversible**
Public and **permissionless**, enabling **composibility**



Smart Contract
Address
0x68b3465833fb72A70ecDF485E0e4C7bD8665Fc45

Smart Contracts

EVM (Ethereum Virtual Machine)

Global Virtual Computer

Developer

Send a tx request to the contract

Deployed to all Ethereum nodes

Users

Solidity

- Object-oriented, high-level language for implementing smart contracts.
- Curly-bracket language that has been most profoundly influenced by C++.
- Statically typed (the type of a variable is known at compile time).
- Supports:

  - Inheritance

  - Libraries

  - Complex user-defined types.
- Alternatives

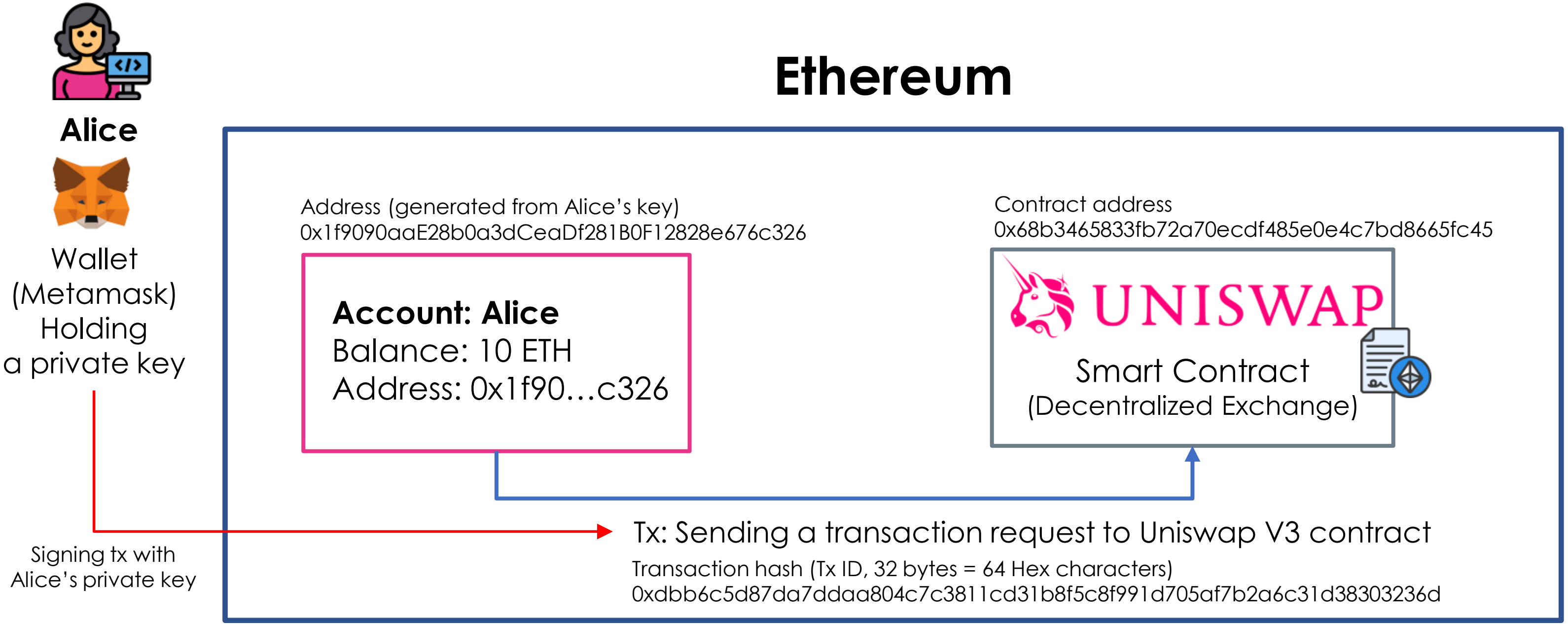
  - Vyper, Yul, Yul+, FE

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >= 0.7.0;

contract Coin {
    // The keyword "public" makes variables
    // accessible from other contracts
    address public minter;
    mapping (address => uint) public balances;

    // Events allow clients to react to specific
    // contract changes you declare
    event Sent(address from, address to, uint amount);

    // Constructor code is only run when the contract
    // is created
    constructor() {
        minter = msg.sender;
    }

    // Sends an amount of newly created coins to an address
    // Can only be called by the contract creator
    function mint(address receiver, uint amount) public {
        require(msg.sender == minter);
        require(amount < 1e60);
        balances[receiver] += amount;
    }

    // Sends an amount of existing coins
    // from any caller to an address
    function send(address receiver, uint amount) public {
        require(amount <= balances[msg.sender], "Insufficient balance.");
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
        emit Sent(msg.sender, receiver, amount);
    }
}
```

https://ethereum.org/en/developers/docs/smart-contracts/languages/

Call a smart contract on Ethereum

Alice wants to exchange 0.17 ETH to PKF tokens on Ethereum



Alice

Wallet
(Metamask)
Holding
a private key

Signing tx with
Alice's private key

Ethereum

Address (generated from Alice's key)
0x1f9090aaE28b0a3dCeaDf281B0F12828e676c326

Account: Alice
Balance: 10 ETH
Address: 0x1f90…c326

Contract address
0x68b3465833fb72a70ecdf485e0e4c7bd8665fc45

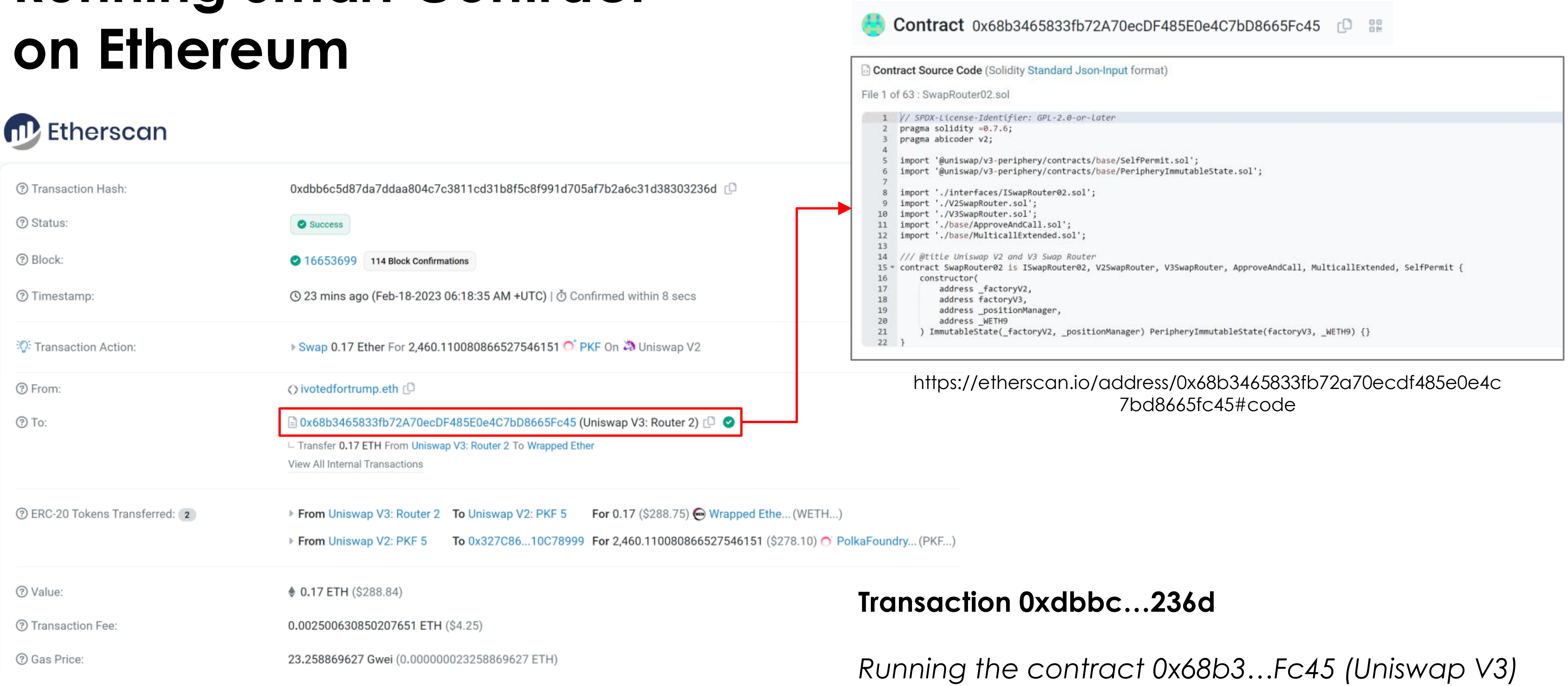
Smart Contract
(Decentralized Exchange)

Tx: Sending a transaction request to Uniswap V3 contract

Transaction hash (Tx ID, 32 bytes = 64 Hex characters)
0xdbb6c5d87da7ddaa804c7c3811cd31b8f5c8f991d705af7b2a6c31d38303236d

Running Smart Contract on Ethereum

Smart Contract



Transaction Hash: 0xdbb6c5d87da7ddaa804c7c3811cd31b8f5c8f991d705af7b2a6c31d38303236d

Status: ✓ Success

Block: ✓ 16653699 114 Block Confirmations

Timestamp: 23 mins ago (Feb-18-2023 06:18:35 AM +UTC) | Confirmed within 8 secs

Transaction Action: ▸ Swap 0.17 Ether For 2,460.110080866527546151 PKF On Uniswap V2

From: ivotedfortrump.eth

To: 0x68b3465833fb72A70ecDF485E0e4C7bD8665Fc45 (Uniswap V3: Router 2) ✓

└ Transfer 0.17 ETH From Uniswap V3: Router 2 To Wrapped Ether

View All Internal Transactions

ERC-20 Tokens Transferred: 2

▸ From Uniswap V3: Router 2 To Uniswap V2: PKF 5 For 0.17 ($288.75) Wrapped Ethe... (WETH...)

▸ From Uniswap V2: PKF 5 To 0x327C86...10C78999 For 2,460.110080866527546151 ($278.10) PolkaFoundry... (PKF...)

Value: 0.17 ETH ($288.84)

Transaction Fee: 0.002500630850207651 ETH ($4.25)

Gas Price: 23.258869627 Gwei (0.000000023258869627 ETH)

Contract 0x68b3465833fb72A70ecDF485E0e4C7bD8665Fc45

Contract Source Code (Solidity Standard Json-Input format)

File 1 of 63 : SwapRouter02.sol

```
// SPDX-License-Identifier: GPL-2.0-or-later
pragma solidity =0.7.6;
pragma abicoder v2;

import '@uniswap/v3-periphery/contracts/base/SelfPermit.sol';
import '@uniswap/v3-periphery/contracts/base/PeripheryImmutableState.sol';

import './interfaces/ISwapRouter02.sol';
import './V2SwapRouter.sol';
import './V3SwapRouter.sol';
import './base/ApproveAndCall.sol';
import './base/MulticallExtended.sol';

/// @title Uniswap V2 and V3 Swap Router
contract SwapRouter02 is ISwapRouter02, V2SwapRouter, V3SwapRouter, ApproveAndCall, MulticallExtended, SelfPermit {
    constructor(
        address _factoryV2,
        address factoryV3,
        address _positionManager,
        address _WETH9
    ) ImmutableState(_factoryV2, _positionManager) PeripheryImmutableState(factoryV3, _WETH9) {}
}
```

https://etherscan.io/address/0x68b3465833fb72a70ecdf485e0e4c7bd8665fc45#code

https://etherscan.io/tx/0xdbb6c5d87da7ddaa804c7c3811cd31b8f5c8f991d705af7b2a6c31d38303236d

Transaction 0xdbbc…236d

Running the contract 0x68b3…Fc45 (Uniswap V3) in order to exchange 0.17 ETH to PKF tokens with the transaction fee of 0.0025 ETH ($4.25)

Dapp (Decentralized Application)

An application that exist and run on a blockchain
without relying on a centralized authority

e.g.) decentralized advertisement, decentralized app store,
decentralized finance, decentralized car sharing etc

Why Dapp

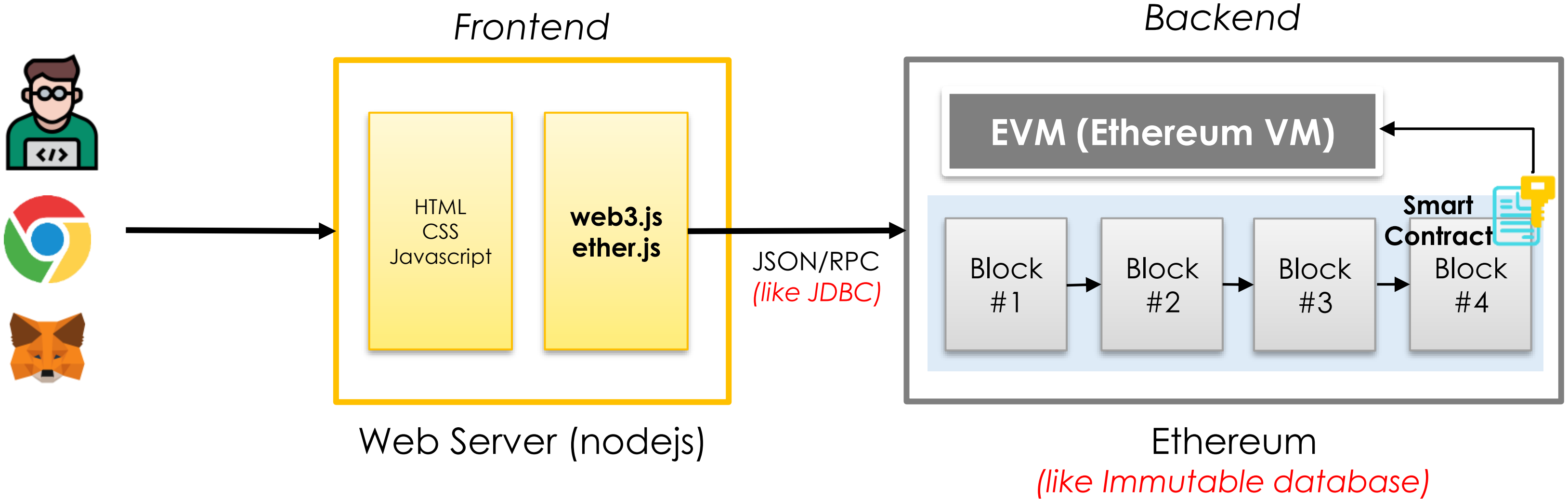
- Free from the control and interference of a single authority
- Protect user privacy
- Censorship-resistant
- Flexibility of development

Disadvantages

- Hard to scale
- Challenges in UX
- Difficulties in upgrading code
- Security risks
- Potentially ideal business model

Building Ethereuem-based Apps

Two parts: 1) smart contracts on Ethereum (on-chain part)
2) Web/App frontend as a user interface (off-chain part)
The frontend communicates with smart contracts through JSON/RPC



Web3 Asset Layer

- Providing technologies to create digital assets
- Including asset tools and services like exchanges and marketplaces

This class will cover

- Fungibility of asset
- Cryptocurrency
- Stablecoin
- NFT(Non-fungible token)
- SBT(Soulbound token)
- Minting ERC20 tokens
- Minting ERC721 NFTs
- NFT/SBT applications

Tools and services

- CEX (Central exchanges)
- DEX (Decentral exchanges), Uniswap
- OpenSea (NFT marketplace)
- OpenZeppelin
- IPFS and Pinata

Asset Types

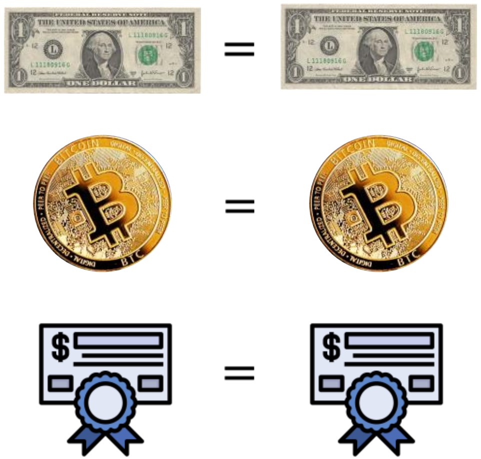
Asset Type

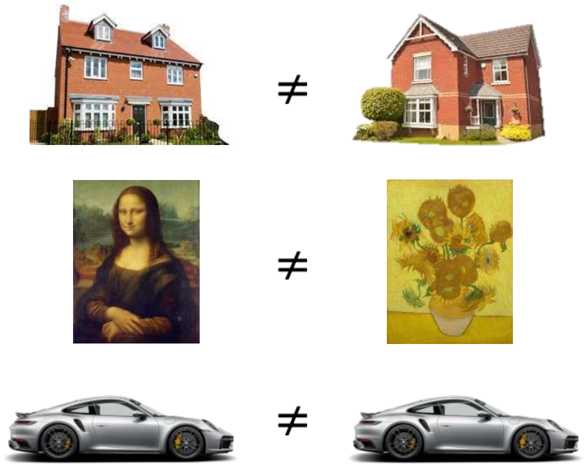
Fungible

- Non unique
- Interchangeable
- Divisible

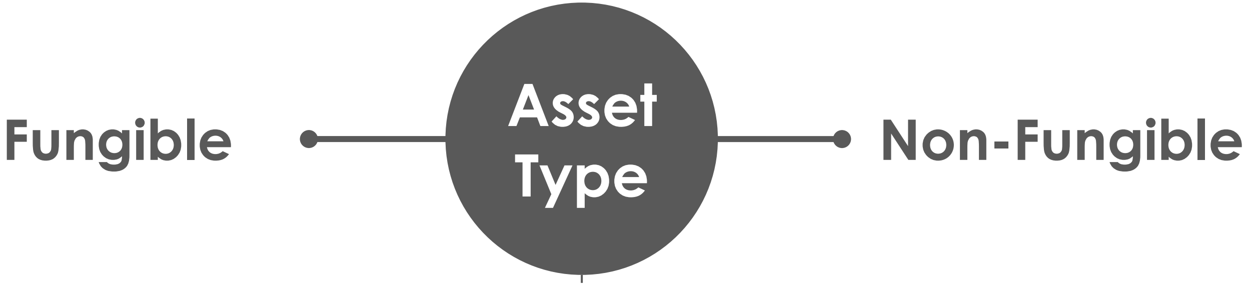
Non-Fungible

- Unique
- Irreplaceable
- Non divisible





Implementing Asset Types on Ethereum



Asset Type

Fungible

Non-Fungible

Fungible Token (FT)
ERC-20

Cryptocurrencies,
Token,
Stablecoin

Non-Fungible Token (NFT)
ERC-721

Digital Art, Collectibles,
Game items, etc

Minting ERC20 Token

ERC20 Interface: ERC20 token contract should implement this interface

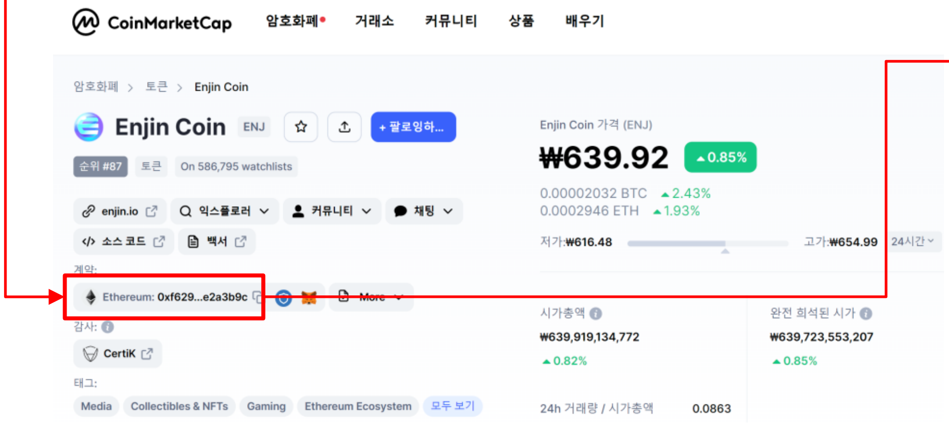
```
// SPDX-License-Identifier: MIT
// OpenZeppelin Contracts (last updated v4.6.0) (token/ERC20/IERC20.sol)
pragma solidity ^0.8.0;

interface IERC20 {
    event Transfer(address indexed from, address indexed to, uint256 value);
    event Approval(address indexed owner, address indexed spender, uint256 value);

    function totalSupply() external view returns (uint256);
    function balanceOf(address account) external view returns (uint256);
    function transfer(address to, uint256 amount) external returns (bool);
    function allowance(address owner, address spender) external view returns (uint256);
    function approve(address spender, uint256 amount) external returns (bool);
    function transferFrom(address from, address to, uint256 amount) external returns (bool);
}
```

https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC20/IERC20.sol

ERC20 token example

ENJIN

- name: Enjin Coin
- symbol: ENJ
- totalSupply: 1,000,000,000
- contract address: 0xf629cbd94d3791c9250152bd8dfbdf380e2a3b9c



Enjin Coin ENJ

순위 #87 토큰 On 586,795 watchlists

계약: Ethereum: 0xf629...e2a3b9c

감사: CertiK

태그: Media Collectibles & NFTs Gaming Ethereum Ecosystem

Enjin Coin 가격 (ENJ)

₩639.92 ▲0.85%

0.00002032 BTC ▲2.43%
0.0002946 ETH ▲1.93%

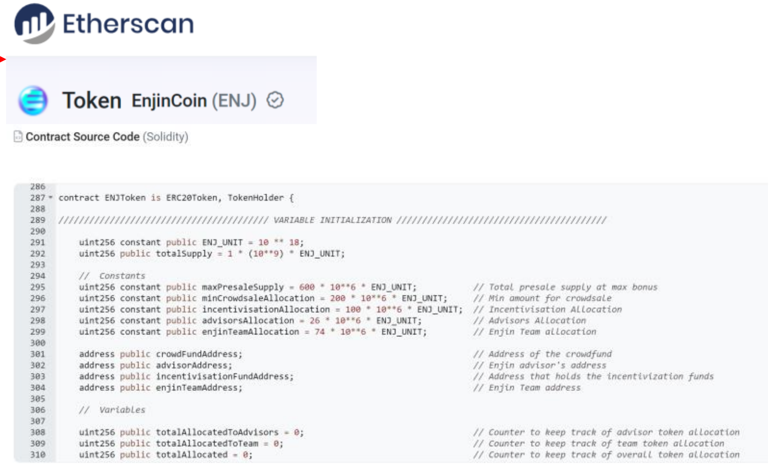
저가:₩616.48 고가:₩654.99

시가총액 ₩639,919,134,772 ▲0.82%

완전 희석된 시가 ₩639,723,553,207 ▲0.85%

24h 거래량 / 시가총액 0.0863

https://coinmarketcap.com/ko/currencies/enjin-coin/



Token EnjinCoin (ENJ)

Contract Source Code (Solidity)

```

contract ENJToken is ERC20Token, TokenHolder {

/////////////////////////////////////// VARIABLE INITIALIZATION ///////////////////////////////////////

    uint256 constant public ENJ_UNIT = 10 ** 18;
    uint256 public totalSupply = 1 * (10**9) * ENJ_UNIT;

    //  Constants
    uint256 constant public maxPresaleSupply = 600 * 10**6 * ENJ_UNIT;         // Total presale supply at max bonus
    uint256 constant public minCrowdsaleAllocation = 200 * 10**6 * ENJ_UNIT;   // Min amount for crowdsale
    uint256 constant public incentivisationAllocation = 100 * 10**6 * ENJ_UNIT; // Incentivisation Allocation
    uint256 constant public advisorsAllocation = 26 * 10**6 * ENJ_UNIT;        // Advisors Allocation
    uint256 constant public enjinTeamAllocation = 74 * 10**6 * ENJ_UNIT;       // Enjin Team allocation

    address public crowdFundAddress;                                           // Address of the crowdfund
    address public advisorAddress;                                             // Enjin advisor's address
    address public incentivisationFundAddress;                                 // Address that holds the incentivization funds
    address public enjinTeamAddress;                                           // Enjin Team address

    //  Variables

    uint256 public totalAllocatedToAdvisors = 0;                               // Counter to keep track of advisor token allocation
    uint256 public totalAllocatedToTeam = 0;                                   // Counter to keep track of team token allocation
    uint256 public totalAllocated = 0;                                         // Counter to keep track of overall token allocation
```

https://etherscan.io/token/0xf629cbd94d3791c9250152bd8dfbdf380e2a3b9c#code

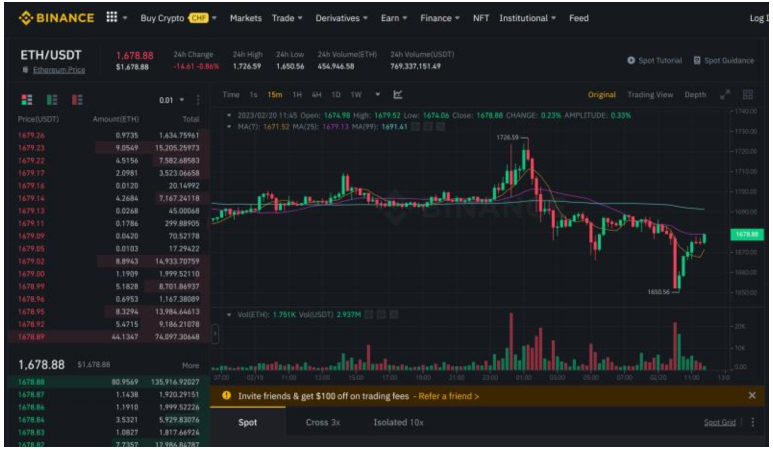
Crypto Exchange

Exchange coins and tokens to other coins, tokens and fiat money

Centralized Exchanges (CEX)

hold your assets in the exchanges
(custody)

BINANCE



ETH/USDT
Ethereum Price

	24h Change	24h High	24h Low	24h Volume(ETH)	24h Volume(USDT)
1,678.88 $1,678.88	-14.61 -0.86%	1,726.59	1,650.56	454,946.58	769,337,151.49

2023/02/20 11:45 Open: 1674.98 High: 1679.52 Low: 1674.06 Close: 1678.88 CHANGE: 0.23% AMPLITUDE: 0.33%

MA(7): 1671.52 MA(25): 1679.13 MA(99): 1691.41

Vol(ETH): 1.751K Vol(USDT): 2.937M

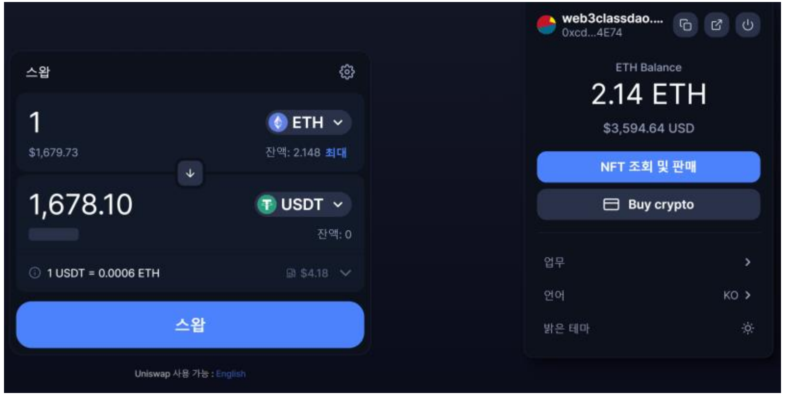
Price(USDT)	Amount(ETH)	Total
1679.26	0.9735	1,634.75961
1679.23	9.0549	15,205.25973
1679.22	4.5156	7,582.68583
1679.17	2.0981	3,523.06658
1679.16	0.0120	20.14992
1679.14	4.2684	7,167.24118
1679.13	0.0268	45.00068
1679.11	0.1786	299.88905
1679.09	0.0420	70.52178
1679.05	0.0103	17.29422
1679.02	8.8943	14,933.70759
1679.00	1.1909	1,999.52110
1678.99	5.1828	8,701.86937
1678.96	0.6953	1,167.38089
1678.95	8.3294	13,984.64613
1678.92	5.4715	9,186.21078
1678.89	44.1347	74,097.30648
1,678.88	$1,678.88	More
1678.88	80.9569	135,916.92027
1678.87	1.1438	1,920.29151
1678.86	1.1910	1,999.52226
1678.84	3.5321	5,929.83076
1678.83	1.0827	1,817.66924
1678.82	7.7357	12,986.84787

Invite friends & get $100 off on trading fees - Refer a friend >

Decentralized Exchanges (DEX)

hold your assets in your wallet
(non-custody)

UNISWAP



1
$1,679.73
잔액: 2.148 최대

1,678.10
잔액: 0

1 USDT = 0.0006 ETH
$4.18

Uniswap 사용 가능 : English

web3classdao....
0xcd...4E74

ETH Balance
2.14 ETH
$3,594.64 USD

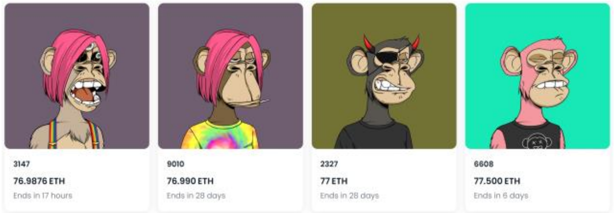
Minting ERC721 NFT

ERC721 Interface: ERC721 NFT contract should implement this interface

```
// SPDX-License-Identifier: MIT
// OpenZeppelin Contracts (last updated v4.6.0) (token/ERC20/IERC20.sol)
pragma solidity ^0.8.0;
import "../../utils/introspection/IERC165.sol";

interface IERC721 is IERC165 {
    event Transfer(address indexed from, address indexed to, uint256 indexed tokenId);
    event Approval(address indexed owner, address indexed approved, uint256 indexed tokenId);
    event ApprovalForAll(address indexed owner, address indexed operator, bool approved);

    function balanceOf(address owner) external view returns (uint256 balance);
    function ownerOf(uint256 tokenId) external view returns (address owner);
    function safeTransferFrom(address from, address to, uint256 tokenId, bytes calldata data) external;
    function safeTransferFrom(address from, address to, uint256 tokenId) external;
    function transferFrom(address from, address to, uint256 tokenId) external;
    function approve(address to, uint256 tokenId) external;
    function setApprovalForAll(address operator, bool approved) external;
    function getApproved(uint256 tokenId) external view returns (address operator);
    function isApprovedForAll(address owner, address operator) external view returns (bool);
}
```

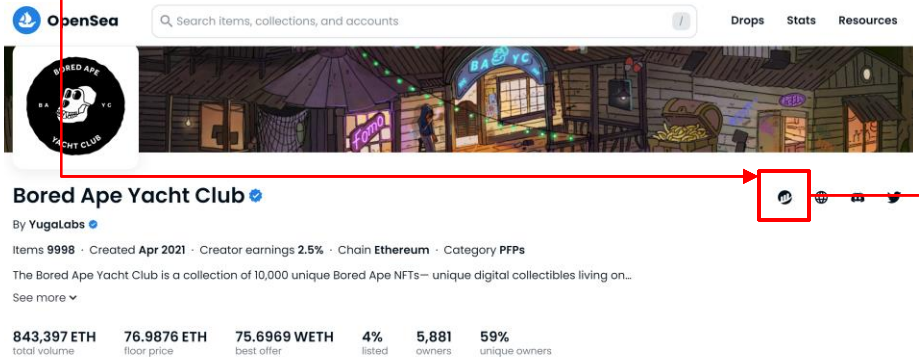
https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC721/IERC721.sol

ERC721 NFT example



3147	9010	2327	6608
76.9876 ETH	76.990 ETH	77 ETH	77.500 ETH
Ends in 17 hours	Ends in 28 days	Ends in 28 days	Ends in 6 days

- name: Bored Ape Yache Club
- symbol: BAYC
- totalSupply: 10,000
- contract address:
- 0xBC4CA0EdA7647A8aB7C2061c2E118A18a936f13D



Bored Ape Yacht Club

By YugaLabs

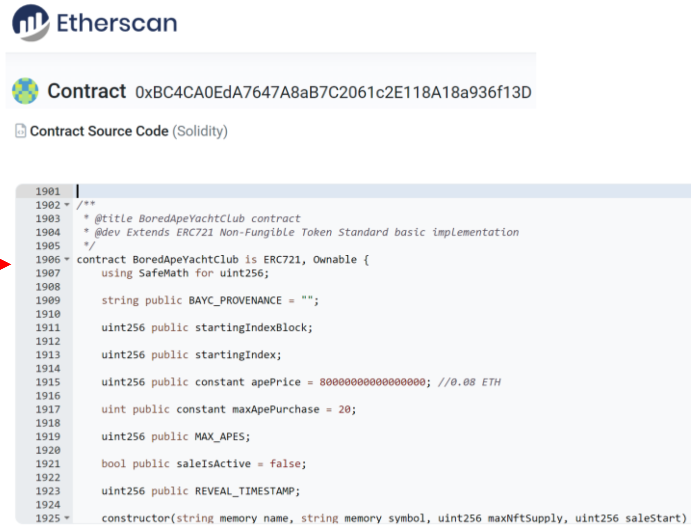
Items 9998 · Created Apr 2021 · Creator earnings 2.5% · Chain Ethereum · Category PFPs

The Bored Ape Yacht Club is a collection of 10,000 unique Bored Ape NFTs— unique digital collectibles living on...

See more

843,397 ETH	76.9876 ETH	75.6969 WETH	4%	5,881	59%
total volume	floor price	best offer	listed	owners	unique owners

https://opensea.io/collection/boredapeyachtclub



Contract 0xBC4CA0EdA7647A8aB7C2061c2E118A18a936f13D

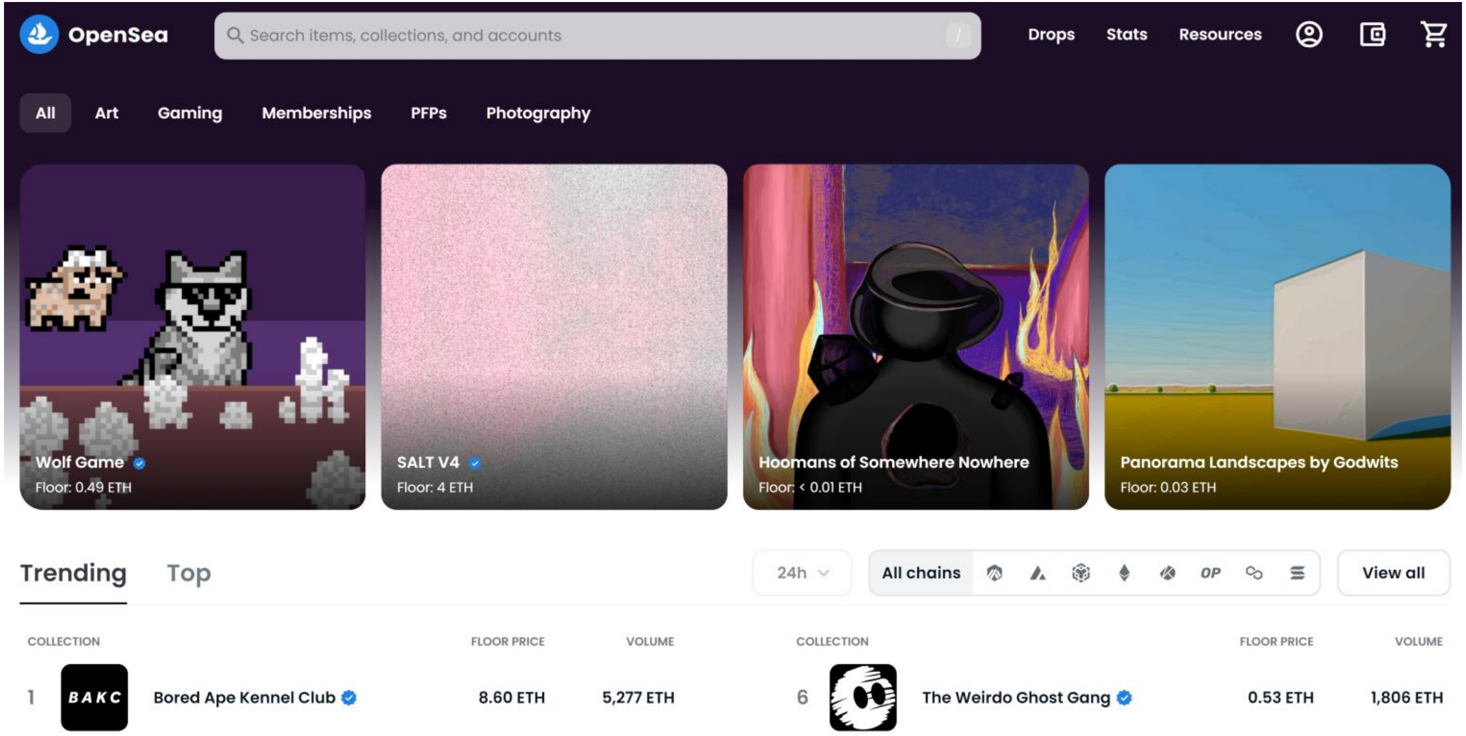
Contract Source Code (Solidity)

```

/**
 * @title BoredApeYachtClub contract
 * @dev Extends ERC721 Non-Fungible Token Standard basic implementation
 */
contract BoredApeYachtClub is ERC721, Ownable {
    using SafeMath for uint256;

    string public BAYC_PROVENANCE = "";

    uint256 public startingIndexBlock;

    uint256 public startingIndex;

    uint256 public constant apePrice = 80000000000000000; //0.08 ETH

    uint public constant maxApePurchase = 20;

    uint256 public MAX_APES;

    bool public saleIsActive = false;

    uint256 public REVEAL_TIMESTAMP;

    constructor(string memory name, string memory symbol, uint256 maxNftSupply, uint256 saleStart)
```

https://etherscan.io/address/0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d#code

NFT Marketplace

Online marketplace for buying and selling NFTs



Wolf Game
Floor: 0.49 ETH

SALT V4
Floor: 4 ETH

Hoomans of Somewhere Nowhere
Floor: < 0.01 ETH

Panorama Landscapes by Godwits
Floor: 0.03 ETH

	COLLECTION	FLOOR PRICE	VOLUME		COLLECTION	FLOOR PRICE	VOLUME
1	Bored Ape Kennel Club	8.60 ETH	5,277 ETH	6	The Weirdo Ghost Gang	0.53 ETH	1,806 ETH

https://opensea.io/

Web3 Governance Layer

- Providing technologies to make programmed governance
- Providing various governance schemes by community
- Providing cryptoeconomics to incentivize participants

This class will cover

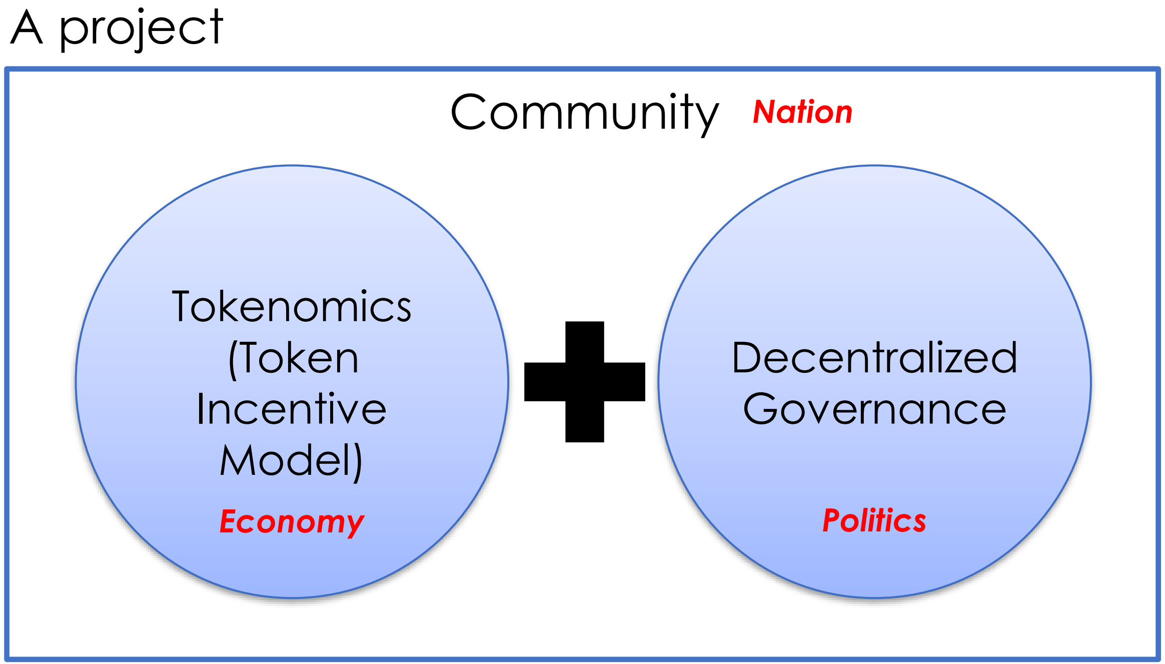
- Tokenomics
- Community
- Governance by community
- Governance schemes
- DAO (Decentralized Autonomous Organization)
- DAO tools

Tools and services

- Governance tools
- DAO tools

Web3 Governance

Hypothesis: A project can be governed by the community of participants with a token incentive model and decentralized governance.

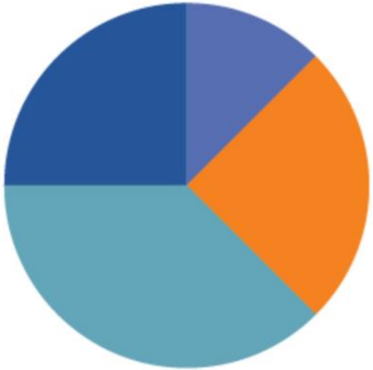


Token Economy (Tokenomics)

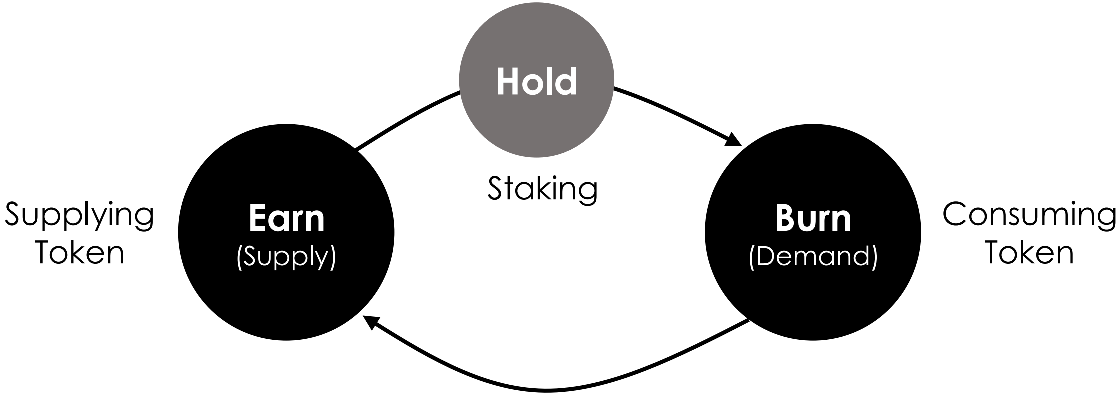
- Designing initial token distribution
- Balancing token supply and demand
- Creating token utility and value

Initial Token Distribution

e.g. public sale, investors, team, community, future use



After Initial Distribution



Building a **working token economy**
is the key of engagement but **isn't trivial**

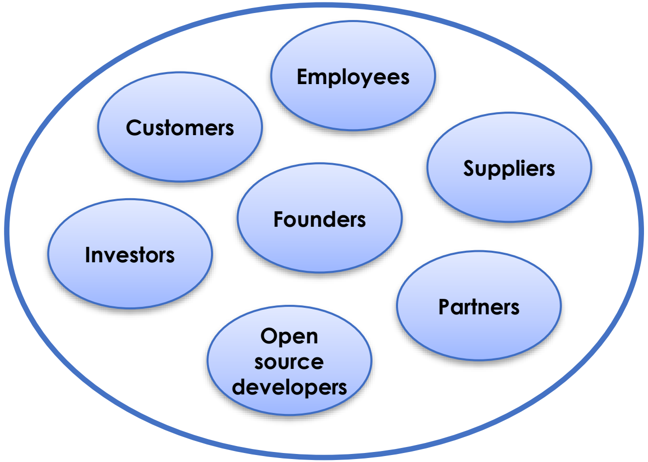
Governance by Community

A project is governed by a community

(★ the concept is under development)

Web3 Community

Openness, Transparency, Autonomy



1. Stakeholder community

- Any individual or orgs that participates in a project

2. Proof of participation

- Holding the tokens or NFTs of a project
- Join and leave freely with tokens

3. Decentralized governance

- Decentralized by design
- Autonomous governance by code
- Branching by forks when disagreements arise

Web3 Protocol & App Layer

- Providing various protocols that web3 apps can utilize
- Providing various Web3 app use cases

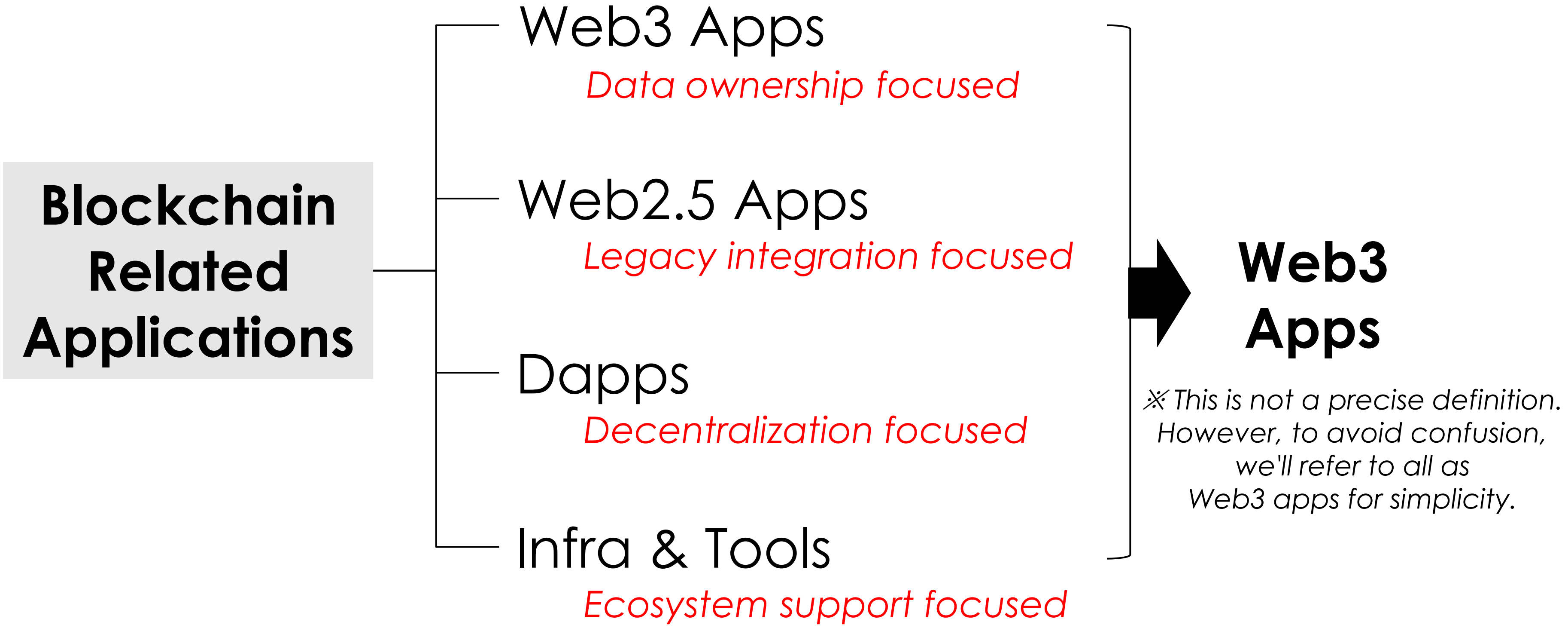
This class will cover

- Web3 protocol and app case studies
- Guest lectures from Web3 apps
- Design principles of Web3 protocol and apps

Tools and services

- Web3 protocol and app cases

Let’s remove confusion over jargon



Blockchain Related Applications

Web3 Apps

Data ownership focused

Web2.5 Apps

Legacy integration focused

Dapps

Decentralization focused

Infra & Tools

Ecosystem support focused

Web3 Apps

※ This is not a precise definition.
However, to avoid confusion,
we'll refer to all as
Web3 apps for simplicity.

The first question

you should ask when building a Web3 app

What problem

am I trying to solve?

If I solve the problem,

who will benefit? *Target Users*

How many people? *Market Size*

Where are they? *Target Market*

Only then

you should ask yourself

WHY BLOCKCHAIN for the problem

- *Transparency*
- *Immutability*
- *Traceability*
- *Anonymity*
- *Openness*
- *Incentive model*
- *Governance*
- *Digital assets*
- *ETC*

What features are you trying to take advantage of?

If you don't have an answer
on why blockchain,
Forget about blockchain.

Blockchain is not a panacea.

DON’T start with these ideas

Decentralizing existing centralized businesses will create big business

Minting new token and design nice tokenomics will solve the problem

Handing over governance to community will attract a lot of users

So many ICO and Dapp projects have failed already, proving that these ideas don’t work

DON’T Confuse means with ends

Blockchain, Decentralization,
Tokenomics, Digital Assets, Governance

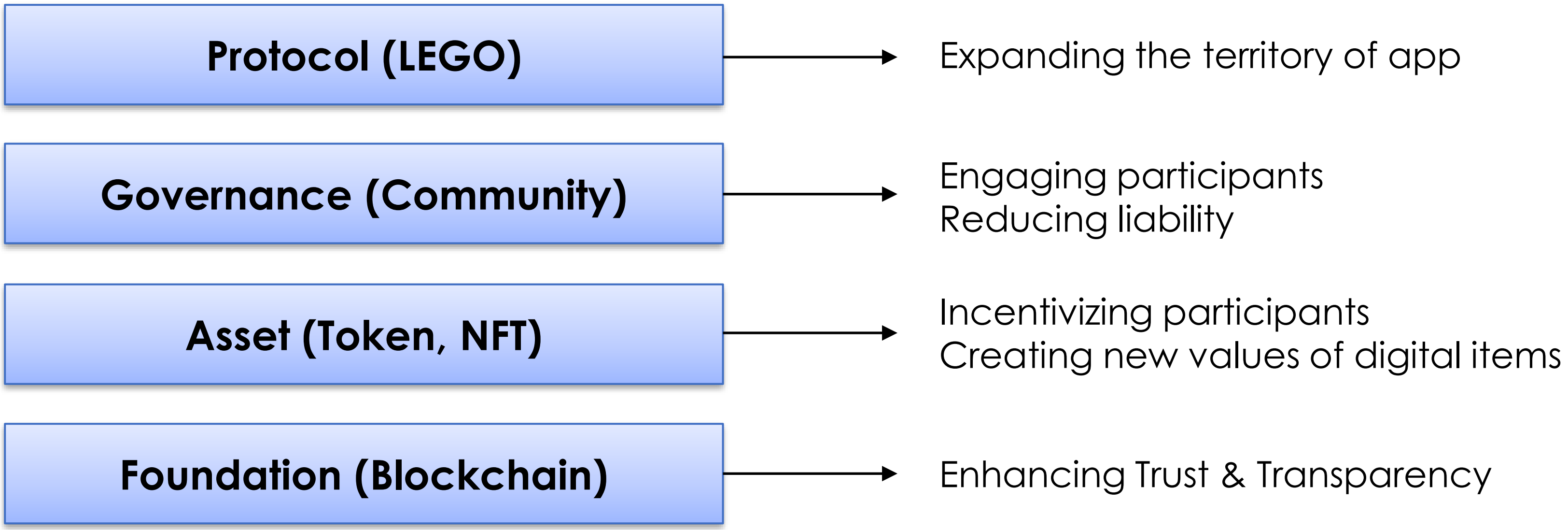
They are a means, not an ends

They are great tools
to solve real-world problems.
However, apply it wisely.

When you build a Web3 app,
You can **selectively apply each layer for your goal**.
Don’t apply everything at the same time.

Web3 Stack

Why applying



Protocol (LEGO) → Expanding the territory of app

Governance (Community) → Engaging participants
Reducing liability

Asset (Token, NFT) → Incentivizing participants
Creating new values of digital items

Foundation (Blockchain) → Enhancing Trust & Transparency

Web3 Apps
for real-world problems

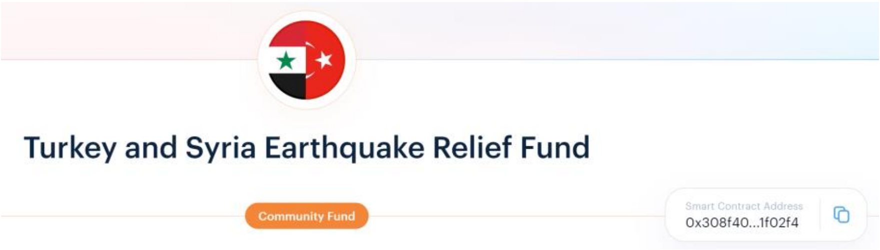
Endaoment

On-chain public charity

□ = Focused layer

- Easy-to-use crypto donation
- More transparency

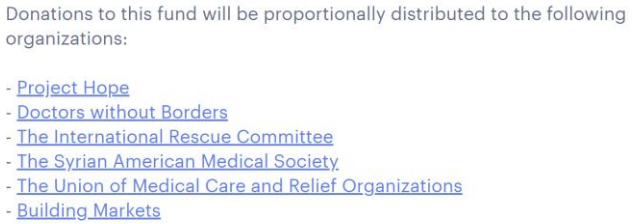
Foundation	Enhancing trust



Turkey and Syria Earthquake Relief Fund

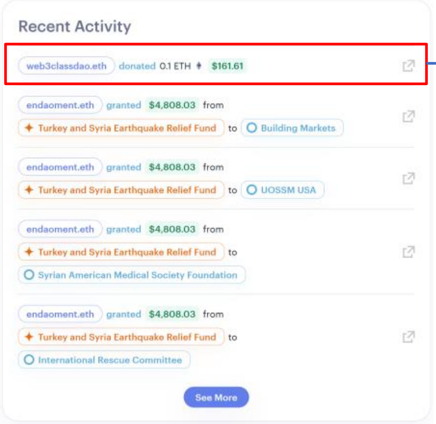
Community Fund

Smart Contract Address
0x308f40...1f02f4



Donations to this fund will be proportionally distributed to the following organizations:

- Project Hope
- Doctors without Borders
- The International Rescue Committee
- The Syrian American Medical Society
- The Union of Medical Care and Relief Organizations
- Building Markets



Recent Activity

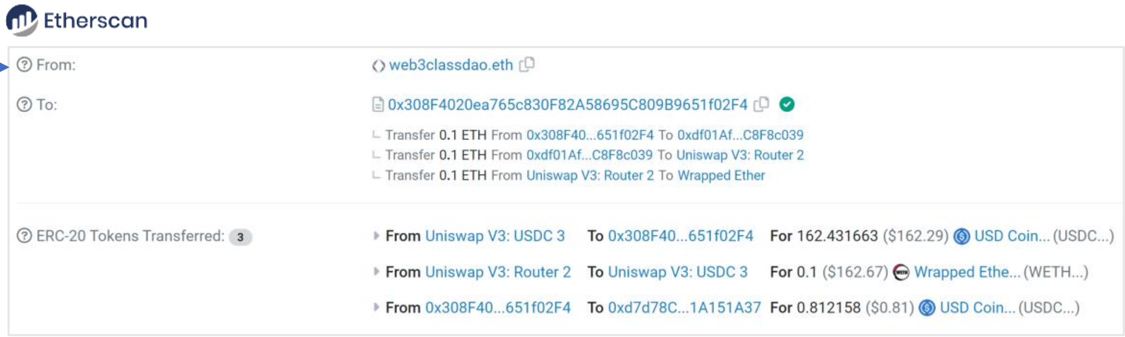
web3classdao.eth donated 0.1 ETH $161.61

endaoment.eth granted $4,808.03 from Turkey and Syria Earthquake Relief Fund to Building Markets

endaoment.eth granted $4,808.03 from Turkey and Syria Earthquake Relief Fund to UOSSM USA

endaoment.eth granted $4,808.03 from Turkey and Syria Earthquake Relief Fund to Syrian American Medical Society Foundation

endaoment.eth granted $4,808.03 from Turkey and Syria Earthquake Relief Fund to International Rescue Committee



Etherscan

From: web3classdao.eth

To: 0x308F4020ea765c830F82A58695C809B9651f02F4

∟ Transfer 0.1 ETH From 0x308F40...651f02F4 To 0xdf01Af...C8F8c039
∟ Transfer 0.1 ETH From 0xdf01Af...C8F8c039 To Uniswap V3: Router 2
∟ Transfer 0.1 ETH From Uniswap V3: Router 2 To Wrapped Ether

ERC-20 Tokens Transferred: 3

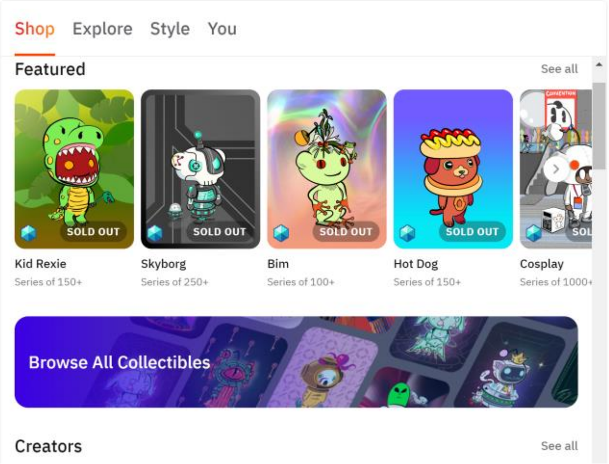
From Uniswap V3: USDC 3 To 0x308F40...651f02F4 For 162.431663 ($162.29) USD Coin... (USDC...)
From Uniswap V3: Router 2 To Uniswap V3: USDC 3 For 0.1 ($162.67) Wrapped Ethe... (WETH...)
From 0x308F40...651f02F4 To 0xd7d78C...1A151A37 For 0.812158 ($0.81) USD Coin... (USDC...)

- https://endaoment.org/
- https://www.philanthropy.com/article/crypto-meet-donor-advised-funds-a-new-way-of-giving
- https://time.com/6153320/crypto-ukraine-charity/

reddit *Empowering communities with assets*

- Collectible avatars as NFT
- Community points as tokens controlled by subreddit communities (beta)
- Vault, an internal wallet
- Coins, an internal virtual currency (Not crypto)

Asset	Avatar NFT, Community points
Foundation	Asset transactions



Smart Web3 transformation

Hassle-free UX

- Easy wallet
- No jargon (NFT, tokens)
- No crypto

Attracting mass

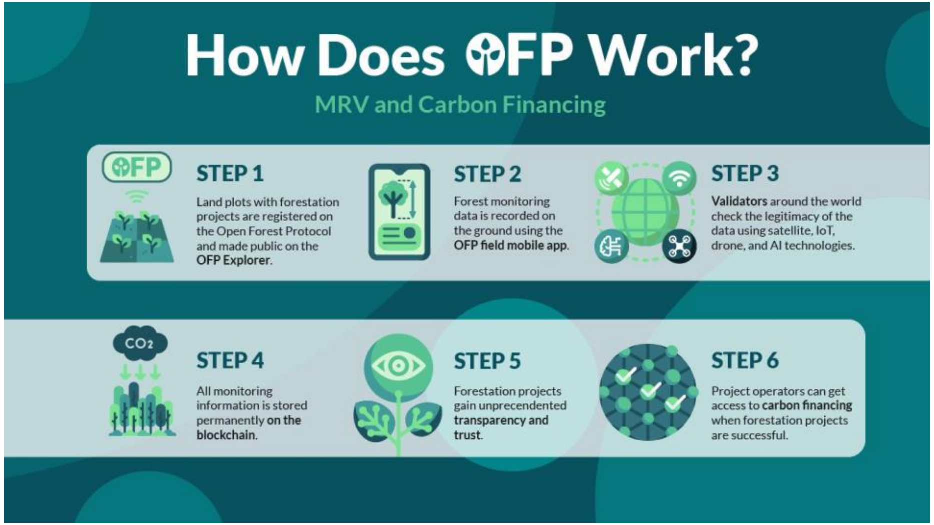
- 7+ M avatar holders (wallet users)
- 10+ M avatar minted
- $48 M market cap of avatar

- https://www.reddit.com/community-points/
- https://ancient8.gg/research/en/articles/reddit-collectible-avatars
- https://www.redditinc.com/blog/blockchain-backed-collectible-avatars-coming-to-reddit-via-new-storefront
- https://dune.com/polygon_analytics/reddit-collectible-avatars

Open Forestation MRV

- MRV (Measure, Report, and Verify)
- Affordable MRV with community of validators
- Forest data on blockchain for trust and transparency
- Access to funding and carbon financing

Governance	Open Forest Congress (DAO)
Asset	OPN (utility & governance token)
Foundation	Tracing forest data



How Does OFP Work?

MRV and Carbon Financing

STEP 1
Land plots with forestation projects are registered on the Open Forest Protocol and made public on the **OFP Explorer.**

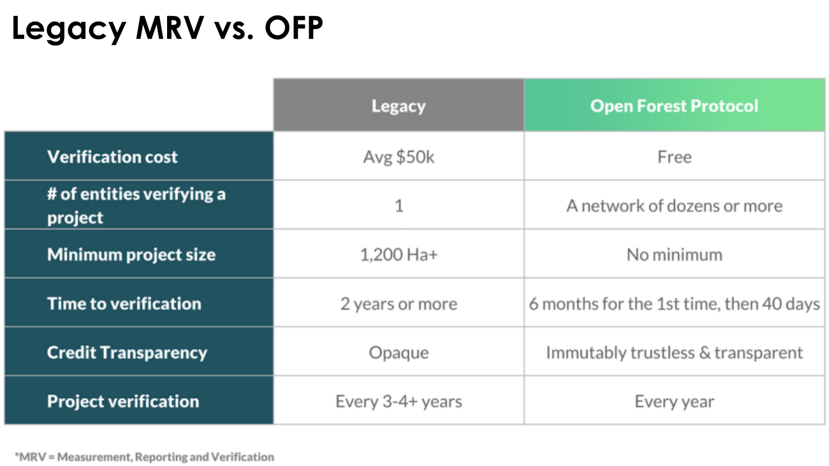
STEP 2
Forest monitoring data is recorded on the ground using the **OFP field mobile app.**

STEP 3
Validators around the world check the legitimacy of the data using satellite, IoT, drone, and AI technologies.

STEP 4
All monitoring information is stored permanently **on the blockchain.**

STEP 5
Forestation projects gain unprecedented **transparency and trust.**

STEP 6
Project operators can get access to **carbon financing** when forestation projects are successful.



Legacy MRV vs. OFP

	Legacy	Open Forest Protocol
Verification cost	Avg $50k	Free
# of entities verifying a project	1	A network of dozens or more
Minimum project size	1,200 Ha+	No minimum
Time to verification	2 years or more	6 months for the 1st time, then 40 days
Credit Transparency	Opaque	Immutably trustless & transparent
Project verification	Every 3-4+ years	Every year

*MRV = Measurement, Reporting and Verification

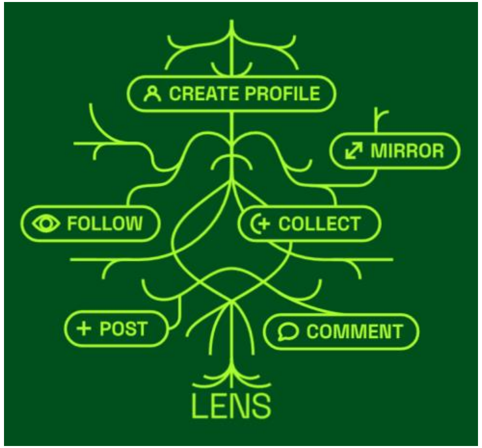
- https://www.openforestprotocol.org/
- https://openforestprotocol.medium.com/opening-forests-with-a-new-standard-of-mrv-9f43f16f8a8c

Open Social Graph Protocol

- Profile NFT to store user social data
- Monetization schemes with social data
- Governance with Lens community (Plan)
- Protocol from the start

Protocol	Open Social Graph
Governance	Community Multisig
Asset	Profile NFT, Follow NFT
Foundation	Storing user data

A user-owned,
open social graph



https://www.lens.xyz/

Lensverse

Hundreds of applications built on top of Lens Protocol

Web3 Twitter

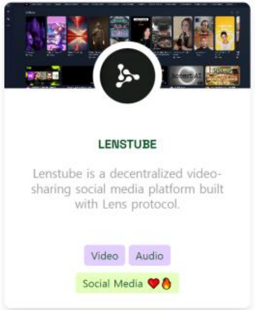
LENSTER

Lenster is a composable, decentralized, and permissionless social media web app built with Lens Protocol 🌿

Text Images Video Audio

Social Media ❤️🔥

Web3 Youtube



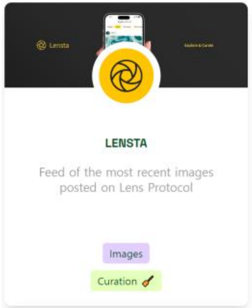
LENSTUBE

Lenstube is a decentralized video-sharing social media platform built with Lens protocol.

Video Audio

Social Media ❤️🔥

Web3 Instagram



LENSTA

Feed of the most recent images posted on Lens Protocol

Images

Curation 🖌

https://www.lens.xyz/apps

GITCOIN

Granting protocol for digital public goods

- Grant open source projects ($50+M)
- Apply quadratic funding
- Mint GTC tokens and DAO it
- Make gitcoin protocols

Protocol	Passport and Allo
Governance	GitcoinDAO
Asset	GTC (governance token)
Foundation	Granting by smart contract

Progressive evolution

2017 – Gitcoin MVP
Built on blockchain

2021 – GTC & GitcoinDAO
Switch to DAO
Mint GTC governance token

2023 – Gitcoin protocols
Gitcoin Grants Stack
to manage a grant program

- https://primer.gitcoindao.com/
- https://gov.gitcoin.co/t/a-brief-history-of-gitcoin-from-2017-2022/9431
- https://www.gitcoin.co/grants-stack
- https://gov.gitcoin.co/t/gitcoin-dao-governance-process-v3/10358

https://www.youtube.com/watch?v=3TQd2ahq6oU

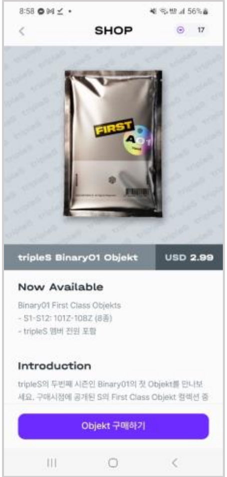
MODHAUS
The idol of all possibilities

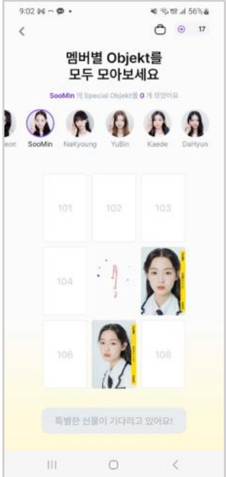
tripleS

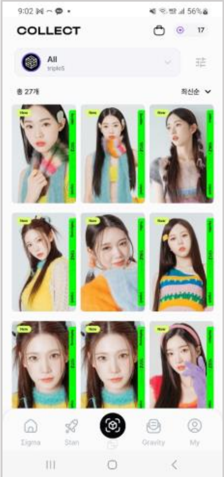
Open Architecture Entertainment

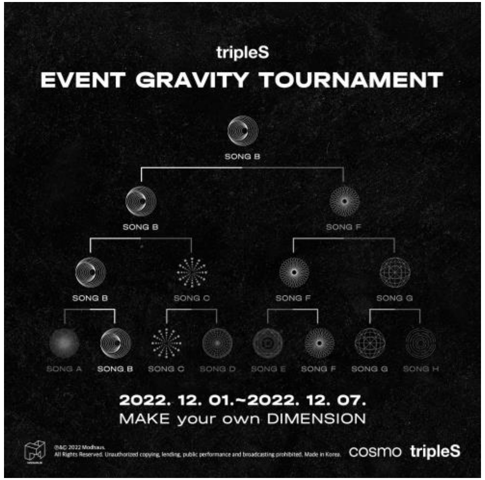
- COSMO app with hidden wallet
- Objekt(Photocard) as hidden NFT
- COMO as hidden governance token
- Gravity as on-chain voting for producing the idol

Governance	Fan governance by voting
Asset	Objekt, COMO
Foundation	On-chain voting, TXs


8:58 56%
SHOP
17
tripleS Binary01 Objekt
USD 2.99
Now Available
Binary01 First Class Objekts
- S1-S12: 101Z-108Z (8종)
- tripleS 멤버 전원 포함
Introduction
tripleS의 두번째 시즌인 Binary01의 첫 Objekt를 만나보세요. 구매시점에 공개된 S의 First Class Objekt 컬렉션 중
Objekt 구매하기


9:02 56%
17
멤버별 Objekt를
모두 모아보세요
SooMin 의 Special Objekt를 0 개 모았어요
eon SooMin NaKyoung YuBin Kaede DaHyun
101 102 103
104
106 108
특별한 선물이 기다리고 있어요!


9:02 56%
COLLECT
17
All
tripleS
총 27개
최신순
Eigma Stan Gravity My



- https://www.triplescosmos.com/
- https://medium.com/modhaus
- https://dune.com/hashed_official/triples
- https://moneybullsflag.substack.com/p/web3-triples

Smart blockchain usage in Web2

Hassle-free UX

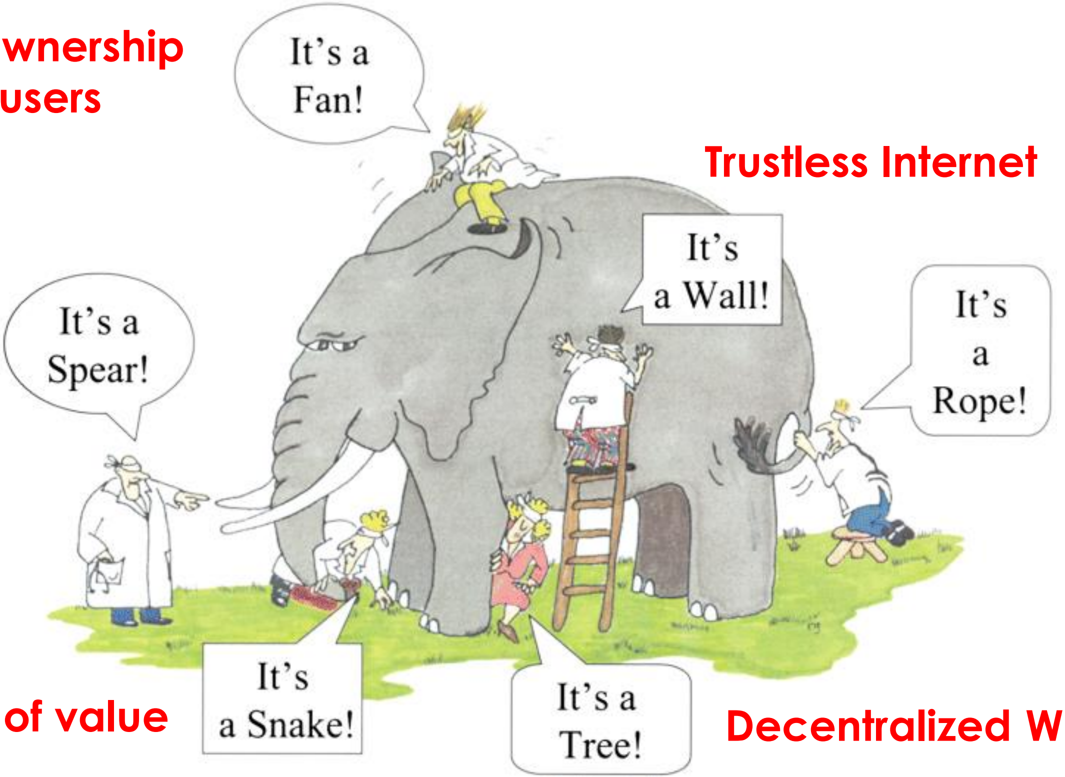
- Easy wallet
- No jargon (NFT, tokens)
- No crypto

Idol Production with Fan

- Voting by fan in production
- On-chain voting for governance transparency
- No decentralization, Empower fans

The Dark Side of Web3/Blockchain/Crypto

Web3 is …



Data ownership to users

Trustless Internet

Internet of assets

Equitable Internet

A network of value

Decentralized Web

Lots of criticisms

Web3 is
a marketing term,
hype, bubble,
and speculation

It's true
Web3 is still
in its infancy

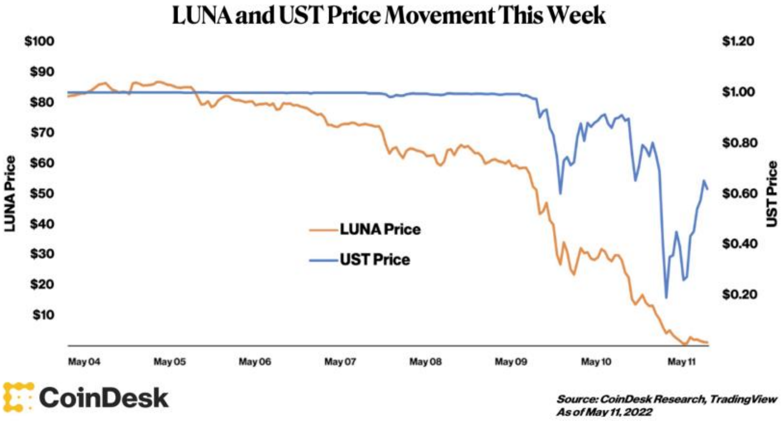
Big Collapses

May 2022

Crash of UST and LUNA

(The third largest stable coin)

the largest crypto crash ever
$60 billion got wiped out of the crypto market



Source: CoinDesk Research, TradingView
As of May 11, 2022

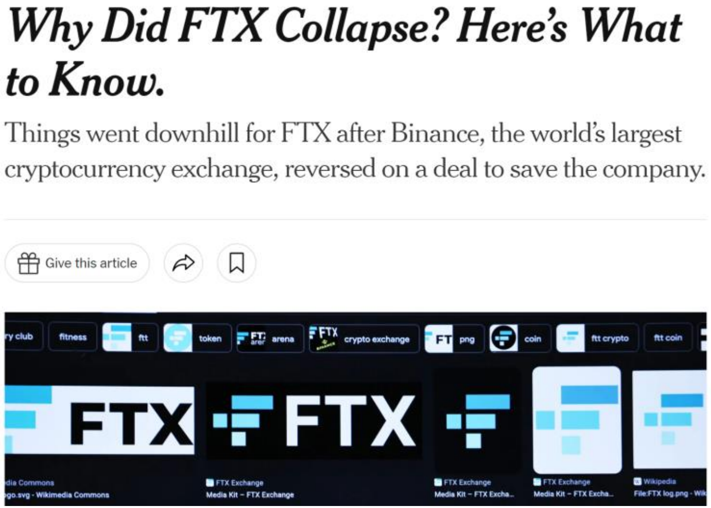
https://www.coindesk.com/layer2/2022/05/11/the-luna-and-ust-crash-explained-in-5-charts/

November 2022

Bankruptcy of FTX

(The second largest crypto exchange)

The crypto market lost billions



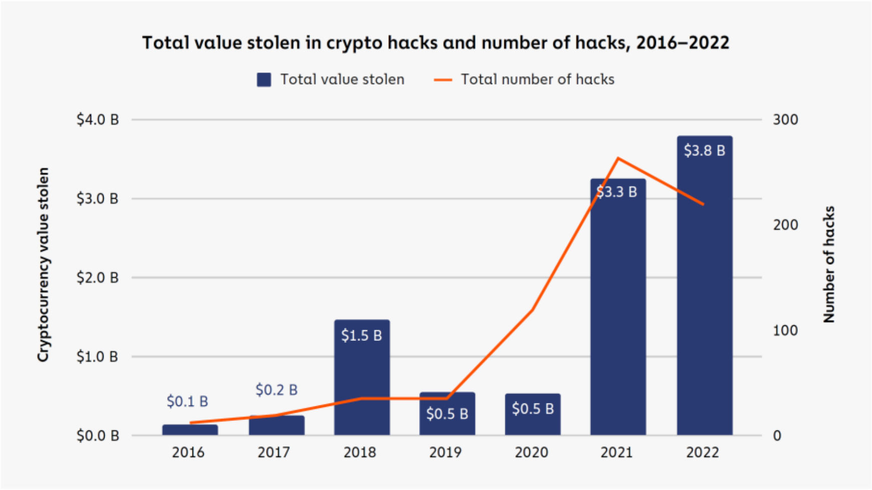
Why Did FTX Collapse? Here's What to Know.

Things went downhill for FTX after Binance, the world's largest cryptocurrency exchange, reversed on a deal to save the company.

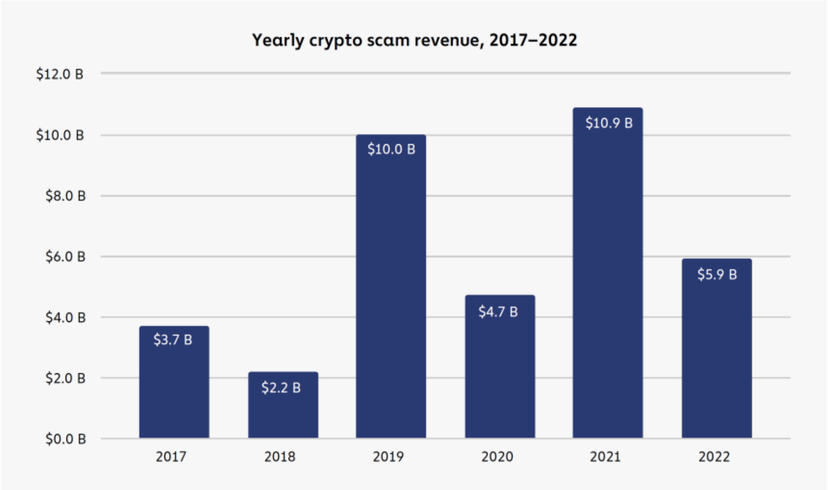
https://www.nytimes.com/2022/11/10/technology/ftx-binance-crypto-explained.html

Hacking and Scams

2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers



Crypto Scam Revenue Dropped 46% in 2022, While Blockchain Analysis Finds Links Between What Appear to be Distinct Scams



The Chainalysis 2023 Crypto Crime Report
https://go.chainalysis.com/2023-crypto-crime-report.html

Why is this happening in the blockchain industry?

Blockchain is a technology
that was born out of cryptocurrency

All these issues are
about cryptocurrency

Cryptocurrencies are
highly volatile and unregulated assets

Absorbing retail money

A lot of scams,
hype and inflated expectations

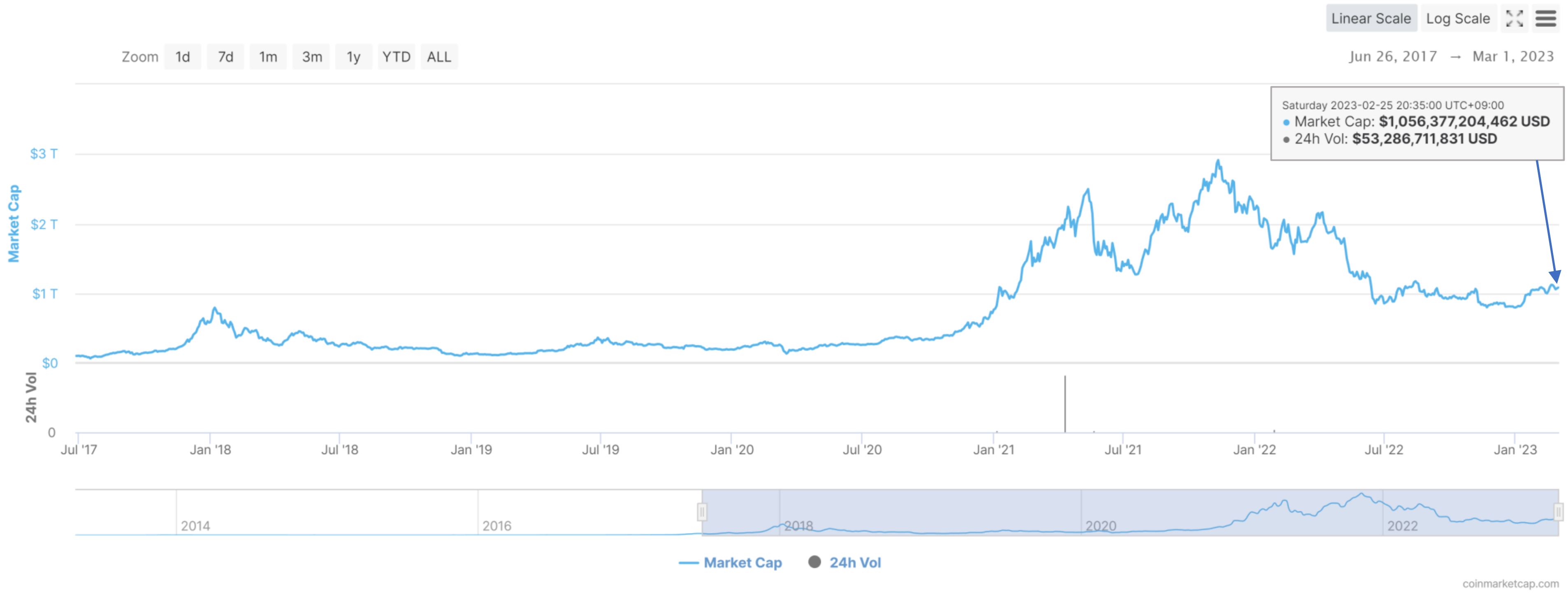
Other technology innovations
such as big data, cloud and AI
were funded by
institutional money like VCs

VS

Blockchain innovation
is being driven by **retail money**
before it has proven its utility

Total Cryptocurrency Market Cap

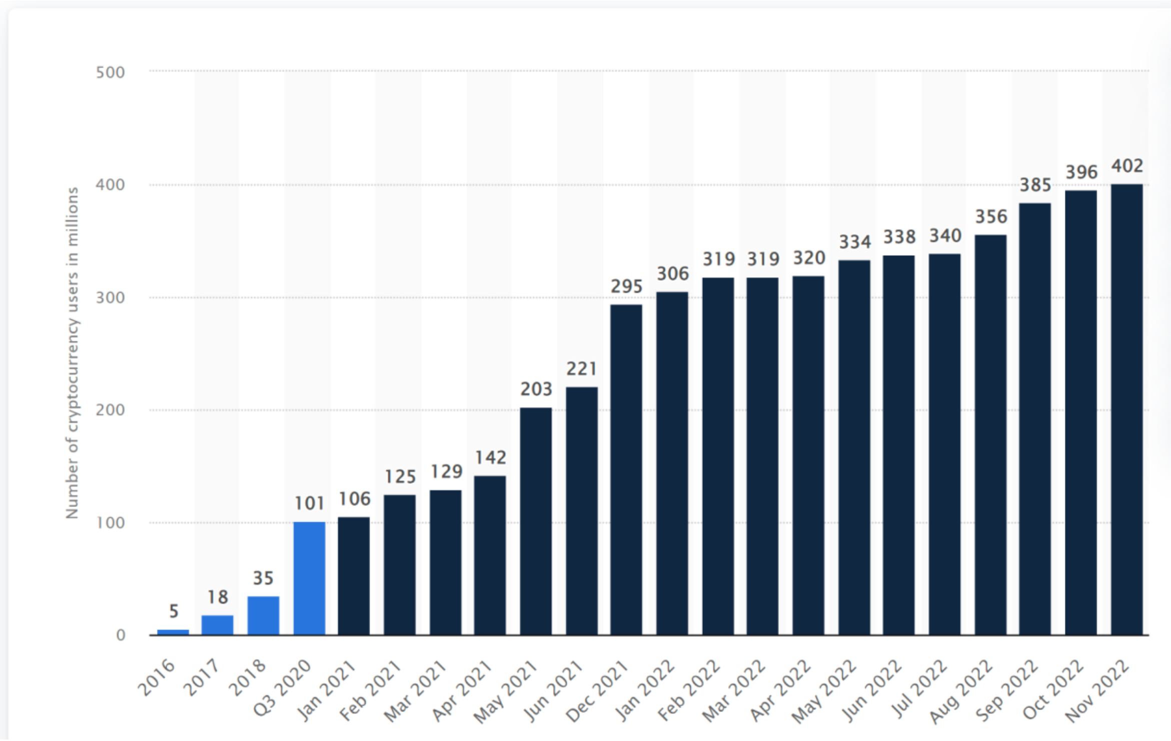
1 Trillion USD
= 1,300조원
(Double Korea’s budget in 2023)



Saturday 2023-02-25 20:35:00 UTC+09:00
● Market Cap: **$1,056,377,204,462 USD**
● 24h Vol: **$53,286,711,831 USD**

https://coinmarketcap.com/charts/

The increase of number of identity-verified cryptocurrency users

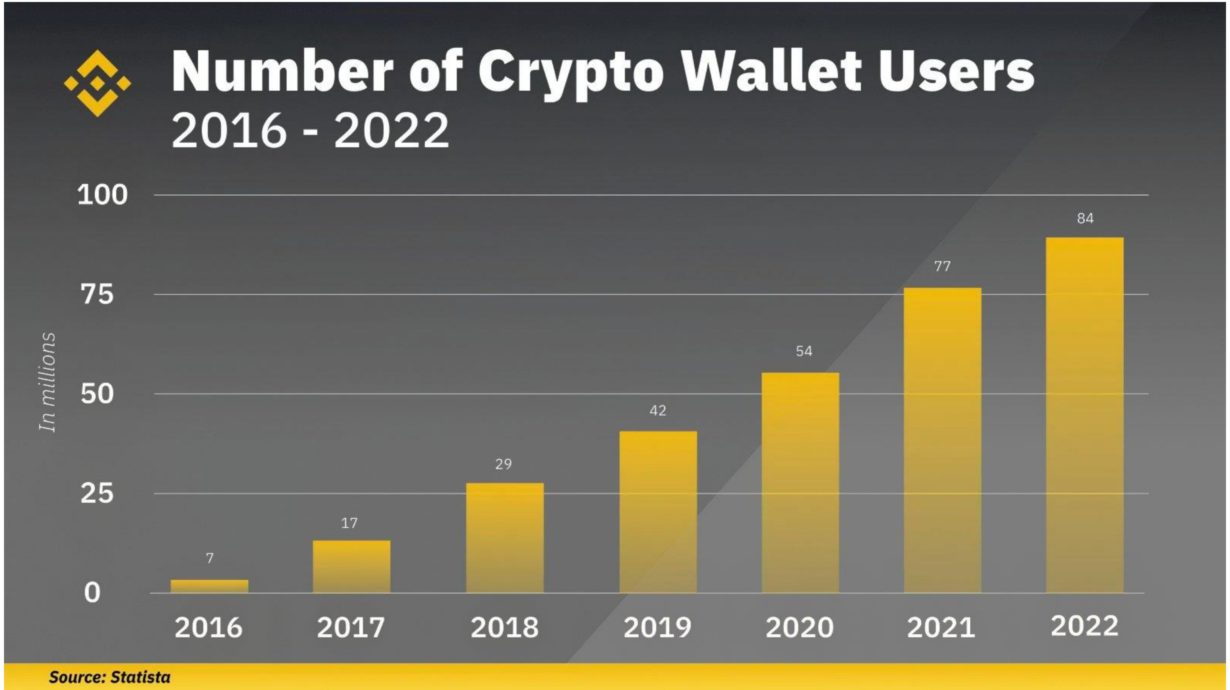


402 millions crypto users (who have cryptocurrencies in exchanges and on-chain wallets)

https://www.statista.com/statistics/1202503/global-cryptocurrency-user-base/

Crypto wallet users are real customers of Web3 apps
They are only 20% of crypto users

80% of crypto users don’t care about apps



Source: Statista

84 millions crypto wallet users
(20% of crypto users, 1.6% of Internet users (5.16 billions, Jan 2023))

https://twitter.com/binance/status/1573718946989187075

Barrier to prevent normal people from entering the blockchain

- Lack of user-friendly interface
- **Limited use cases**
- Lack of awareness
- Security concerns
- Lack of scalability
- Immature technology
- Lack of regulation
- Negative perceptions

<u>My Opinion</u>

The blockchain industry is heavily skewed toward cryptocurrencies

Time to Shift The Focus

Building a killer app for the masses

It will come from real-world problems

Back to Basics

What real-world problems are you trying to solve with blockchain?

My Thesis

Data ownership is
a powerful real-world problem to solve.
A killer app will come from Web3

Wrap Up

Summary

- **Learned about**

  - The history of the web and the emergence of Web3

  - 4 features of Web3 with Lens protocol

  - The preview of Web3 stack

  - Various Web3 apps (Endaoment, Reddit, Open Forest Protocol, Gitcoin, Modhaus, Mirror.xyz, POAP)

  - The dark side of Web3 & blockchain & crypto

Q & A

[Reminder] 9pm – 11pm today, Q&A session about the class
on Discord the channel #class-faq