

NFT

Blockchain

- Wachsende Liste von Datensätzen, sogenannten Blöcken, die mithilfe von Kryptografie miteinander verknüpft sind
- Jeder Block enthält einen kryptografischen Hash des vorherigen Blocks
- Sind resistent gegen Datenänderungen.
- Blockchains werden in der Regel von einem Peer-to-Peer-Netzwerk verwaltet und als öffentlich verteiltes Hauptbuch verwendet.

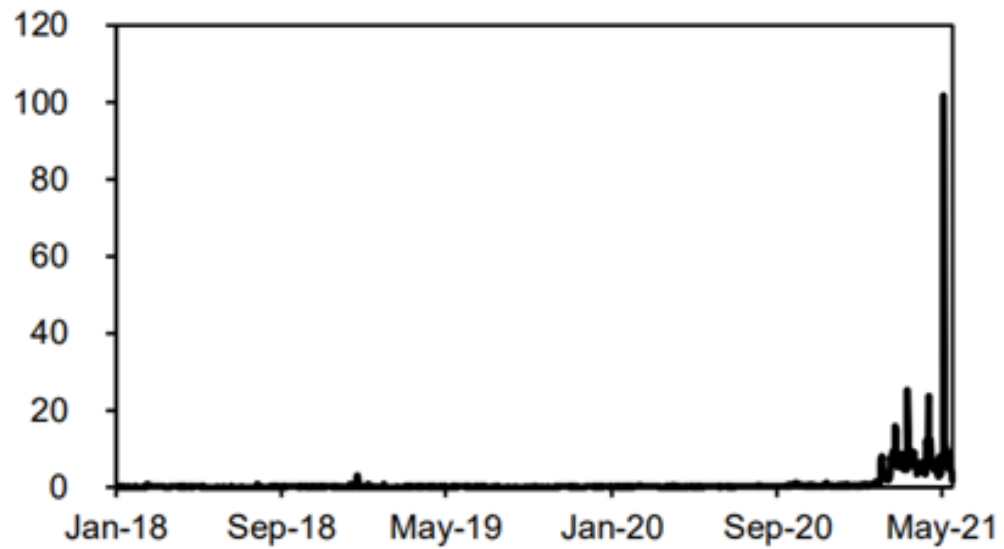
Non-fungible tokens (NFT)

- Übertragbare Rechte an digitalen Assets
- Einzigartige Echtheitszertifikate auf Blockchains
- In der Regel von den Schöpfern der zugrunde liegenden Vermögenswerte ausgegeben.
- Assets können digitaler oder physischer Natur sein

Fungible vs Non-Fungible

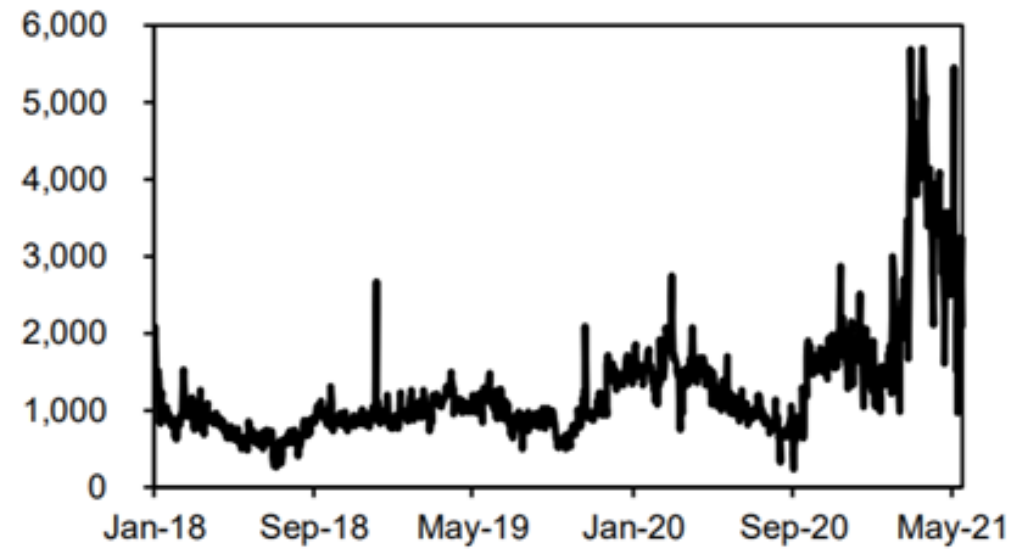
- Fungible Sachen
 - Geld oder Handelsgüter
 - Können gegen gleichartige Waren umgetauscht werden
- Non-Fungible Sachen
 - Künstlerische, historische Objekte, seltene Sammelkarten, ...
 - NFTs bieten die Möglichkeit mit einzigartigen Objekten in der digitalen Welt zu Handeln.

NFT sales in million USD



(Ante 2021)

Number of active NFT wallets



Rechtliche Risiken und Herausforderungen

- IP-Rechte
 - Eigentum von NFT beinhaltet keine IP (Intellectual property)-Rechte
- Nicht registrierte Wertpapiere
 - Fraktionierte NFTs können von der SEC als nicht registrierte Wertpapiere eingestuft werden.
- Geldwäschebekämpfung
 - Für NFT-Marktplätze und Auktionshäuser werden strengere Know-Your-Customer-Verfahren eingeführt.
 - Die Vorschriften konzentrieren sich auf Transaktionen im Bereich von 10.000 USD oder mehr

Use Cases

- Ticketing
 - Eigene / Drittanbieter Infrastruktur einsparen
 - Verschlüssel- und Validierbar
 - Transparenz
- Gaming
 - Echtes Eigentum an digitalen Spielgegenständen möglich
 - Keine Währungs- und Strukturbeschränkungen
 - Publisherunabhängig nach Ausgabe
- Grundbuch / Grundbuchähnliche Systeme
 - Transferkosten sparen
 - Globalisiertes System möglich

Vorteile

- Dezentralisiert und damit unabhängig von Staaten und Unternehmen
- Direktvertrieb ohne Mittelsmann möglich (z.B. Künstler an Kunden)
- Als Eigentumszertifikat für echte Gegenstände verwendbar
- Schneller Eigentumswechsel möglich
- Keine Geographischen Beschränkungen
- Sicherheit

Neutral

- Nicht veränderbar
- Heterogenität
- Knappheit

Nachteile

- Nicht dezentrale Marktplätze widersprechen dem NFT Kerngedanke
- Vereinfacht Geldwäsche
- Integritätsprobleme (z.B. NFT auf Datei URL)
- Eigentumsprivilegien teilweise nicht privatisierbar (NFT auf Bild)
- Anfällig für Computerkriminalität (User & Plattform)
- Digitalverbrechen teilweise schwer aufzuklären
- Rechtlicher Rahmen fehlt
- Einfacherer identitätsbetrug möglich
- Momentan eher Spekulationsobjekte mit hohen Transaktionskosten

NFT Standards / Blockchains

- Verschiedene Blockchains
 - Ethereum; De-Facto Standard
 - Flow; POS
 - Tezos; POS
 - Solana; Schneller
- Verschiedene Standards auf der Gleichen Blockchains
 - Ethereum: ERC-721, ERC-1155, Selbst-Implementiert, etc..

Ethereum

- Benutzt Proof of Work
- Unterstützt Smart Contracts
- Mit ERC-721 NFT De-Facto Standard

- NFT Standards
 - Smart Contract Interface
 - Stellt Referenzimplementierung bereit
 - Erweiterbar (Vererbung / Optionale Erweiterungen)

Smart Contracts?

- Programm auf der Blockchain
 - Code und Application state auf der Blockchain verteilt
- Eigene Programmiersprachen
 - Solidity
 - Vyper
 - EVM-Bytecode
- Public functions global aufrufbar

Solidity Beispiel

```
1 // Our first contract is a faucet!
2 contract Faucet {
3
4     // Give out ether to anyone who asks
5     function withdraw(uint withdraw_amount) public {
6
7         // Limit withdrawal amount
8         require(withdraw_amount <= 1000000000000000000);
9
10        // Send the amount to the address that requested it
11        msg.sender.transfer(withdraw_amount);
12    }
13
14    // Accept any incoming amount
15    function () public payable {}
16
17 }
```

ERC-721

- 10 Core Functions
- Vielzahl an Optionalen features und funktionen
- Beispiele von Core Functions:
 - function safeTransferFrom(address _from, address _to, uint256 _tokenId) external payable;
 - function approve(address _approved, uint256 _tokenId) external payable;
 - function ownerOf(uint256 _tokenId) external view returns (address);

ERC-721 – Code walkthrough TODO: change

```
1 mapping (uint256 => address) internal idToOwner;
2
3 function safeTransferFrom(address _from, address _to, uint256 _tokenId) public {
4     // validate address and approval
5
6     address tokenOwner = idToOwner[_tokenId];
7     _transfer(_to, _tokenId);
8 }
9
10 function _transfer(address _to, uint256 _tokenId) private {
11     address from = idToOwner[_tokenId];
12     delete idToApproval[_tokenId]; // clear approval
13
14     // delete nft from old user
15     ownerToNFTTokenCount[_from] -= 1;
16     delete idToOwner[_tokenId];
17
18     // add nft to new user
19     idToOwner[_tokenId] = _to;
20     ownerToNFTTokenCount[_to] += 1;
21
22     emit Transfer(from, _to, _tokenId);
23 }
24
```

ERC-721 – Blockchain Result

	0xe3e1c7696b990a409d...	Atomic Match_	9 mins ago	*off-nfts.eth		jotpyrc.eth	3978
	0xbc61b399ed11d84c1c...	Transfer From	27 mins ago	bluecoffeexu.eth		0xd1130d0353902a8dd0...	4036
	0x3b062993bb596ddefdf...	Atomic Match_	35 mins ago	decentralizeit.eth		0x1415db333a0ab8a985...	6445

Overview Logs (2) State Comments

Transaction Hash: 0xbc61b399ed11d84c1c0c77665fb896e55d685c25482ad7bc35e81655dd37a84e

Status: Success

Block: 13979034 126 Block Confirmations

Timestamp: 28 mins ago (Jan-10-2022 05:11:20 PM +UTC) | Confirmed within 30 secs

Transaction Action:
Transfer of The Indiffer... (Indiff...) From ¹0xb705a2285e6a8c1abc... To ²0xd1130d0353902a8dd0...
↳ 1 of Token ID ³[4036]

From: bluecoffeexu.eth

Interacted With (To): Contract ⁴0xfac0b889703ab4db3426ef67d437bee3408941ac (The Indifferent Duck: IndifferentDuck Token)

Tokens Transferred:
From 0xb705a2285e6a8... To 0xd1130d0353902...
For ERC-721 TokenID [4036] The Indiffer... (Indiff...)

Value: 0 Ether ⁵(\$0.00)

Transaction Fee: 0.027413100510034326 Ether ⁶(\$81.87)

Gas Price: 0.000000279079077138 Ether (279.079077138 Gwei)