

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH

# Krypto-Assets und NFTs

Dr. Ross King

Head of Competence Unit

Data Science & Artificial Intelligence

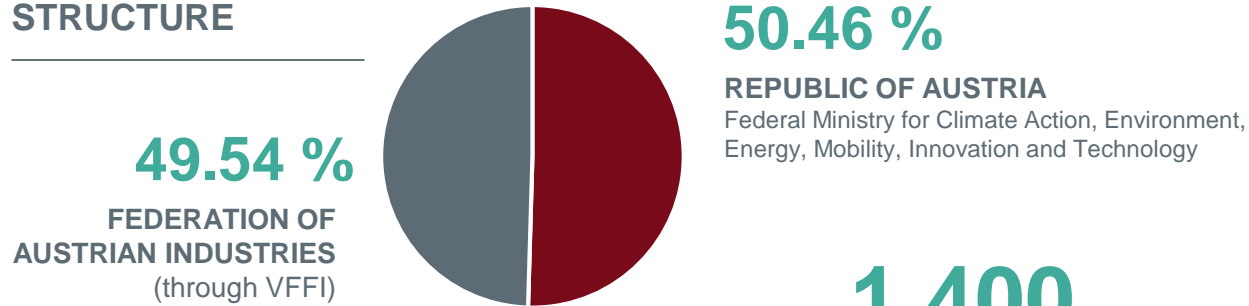
AIT Austrian Institute of Technology



# AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

## OWNERSHIP STRUCTURE

---



**49.54 %**

FEDERATION OF  
AUSTRIAN INDUSTRIES  
(through VFFI)

**50.46 %**

REPUBLIC OF AUSTRIA

Federal Ministry for Climate Action, Environment,  
Energy, Mobility, Innovation and Technology

**1.400**

---

EMPLOYEES

**165 m EUR**

---

## TOTAL REVENUES

as of YE 2020

88,6 m EUR Contract research revenues (incl. grants)

48,9 m EUR BMK funding

23,7 m EUR Other operating income,  
incl. Nuclear Engineering Seibersdorf

3,7 m EUR Profactor (51% of 7,9 m EUR)

# AIT CENTERS

<p><b>Energy</b></p> <ul style="list-style-type: none"> <li>• Electric Energy Systems</li> <li>• Integrated Energy Systems</li> <li>• Energy Conversion and Hydrogen</li> <li>• Digital Resilient Cities</li> <li>• Sustainable Thermal Energy Systems</li> </ul>	<p><b>Health &amp; Bioresources</b></p> <ul style="list-style-type: none"> <li>• Biomedical Systems</li> <li>• Bioresources</li> <li>• Digital Health Information Systems</li> <li>• Molecular Diagnostics</li> </ul>	<p><b>Vision, Automation &amp; Control</b></p> <ul style="list-style-type: none"> <li>• Assistive &amp; Autonomous Systems</li> <li>• Complex Dynamical Systems</li> <li>• High-Performance Vision Systems</li> </ul>
<p><b>Low-Emission Transport</b></p> <ul style="list-style-type: none"> <li>• Electric Drive Technologies</li> <li>• Transportation Infrastructure Technologies</li> <li>• Light Metals Technologies Ranshofen</li> </ul>	<p><b>Technology Experience</b></p> <ul style="list-style-type: none"> <li>• Experience Contexts and Tools</li> <li>• Experience Business Transformation</li> </ul>	<p><b>Innovation Systems &amp; Policy</b></p> <ul style="list-style-type: none"> <li>• Digital Innovation</li> <li>• Foresight &amp; Institutional Change</li> <li>• Policies for Change</li> </ul>

## Digital Safety & Security

- Security & Communication Technologies
- Sensing & Vision Solutions
- **Data Science & Artificial Intelligence**
- Cooperative Digital Technologies

# AIT KRYPTO-ASSET FORSCHUNG

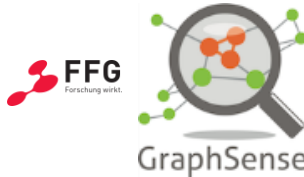
2015 — 2016 — 2017 — 2018 — 2019 — 2020 — 2021 — 2022 — 2023 →



KRYPTOMONITOR



VIRTCRIME



TITANIUM



Anti-FinTer



Bundesministerium  
Verkehr, Innovation  
und Technologie



KRYPTOMONITOR wird im Sicherheitsforschungs-Förderprogramm KIRAS vom Bundesministerium für Verkehr, Innovation und Technologie finanziert.

Anti-FinTer has received funding from the European Union's ISFP-2020-AG-TERFIN program under the Grant Agreement No. 101036262.













































# KRYPTO-ASSETS UND NFTS EINFÜHRUNG

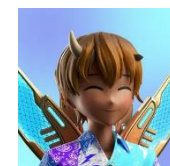
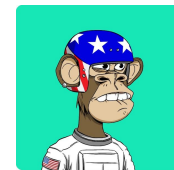


# EINFÜHRUNG: VIRTUAL ASSETS

- Ein **Virtual Asset** ist eine digitale Repräsentation eines Wertes, der digital gehandelt oder übertragen werden kann und zu Zahlungs- oder Investitionszwecken verwendet werden kann.
- Zu den Virtual Assets gehören keine digitalen Darstellungen von Fiat-Währungen, Wertpapieren oder anderen finanziellen Vermögenswerten.

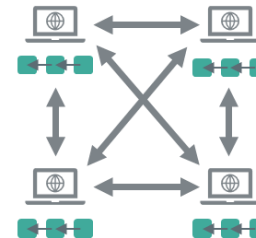
- FATF Recommendations 2012, Updated October 2021

 BNT	 QNT	 cDAI	 Multi-collateral DAI
 CVC	 RCN	 cSAI	 KCS
 EURS	 REP	 ENJ	 LEND
 GNT	 RLC	 OXT	 LOOM
 GYEN	 SAI	 CEL	 LRC
 KNC	 SNT	 CELR	 NEXO
 MANA	 STORJ	 tUSD	 NPXS
 MATIC	 sUSD	 ELF	 PAY
 MTL	 WBTC	 ENG	 POWR
 NMR	 WTC	 FET	 REN
 OKB	 ZUSD	 HOT	 VGX



# EINFÜHRUNG: KRYPTO-ASSETS

Was sind Krypto-Assets (Cryptoassets)?



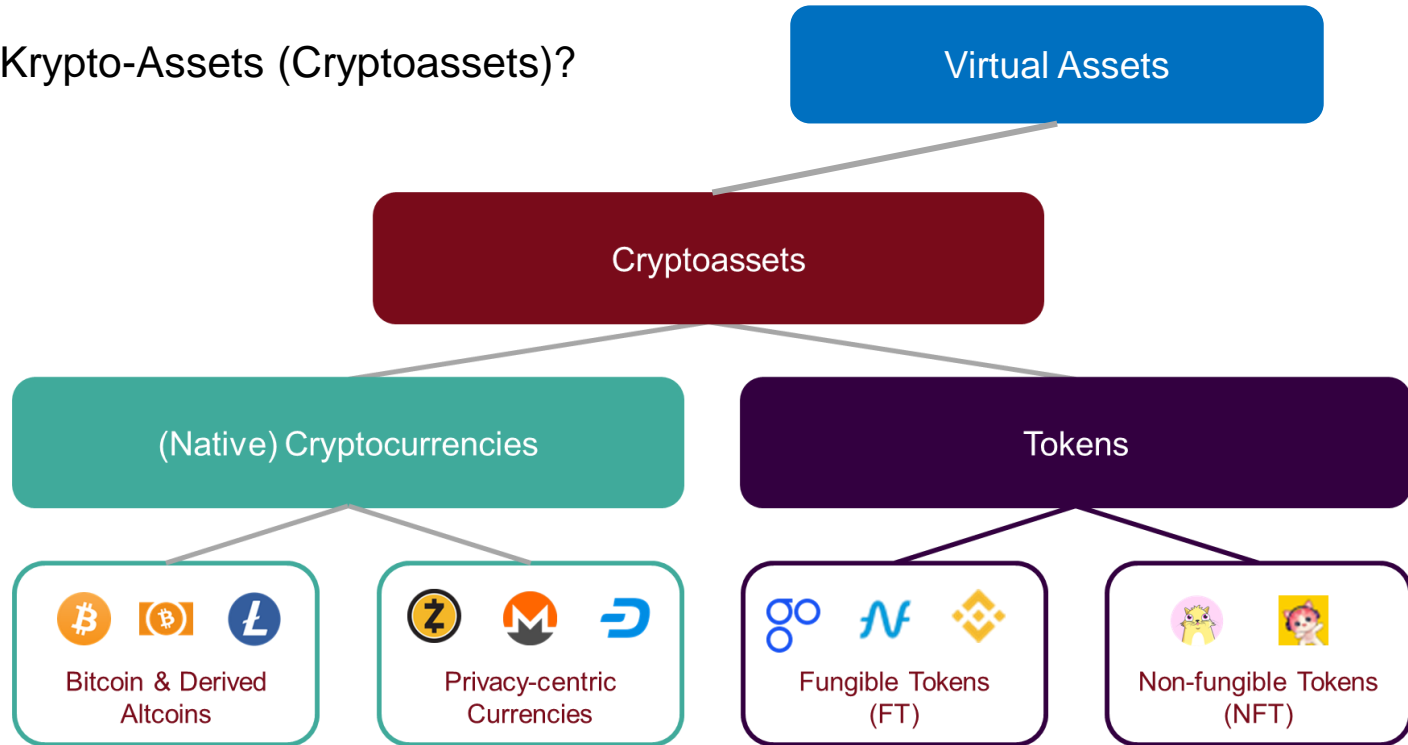
An exchangeable virtual asset...

...that utilizes cryptography...

...and is shared via some distributed ledger.

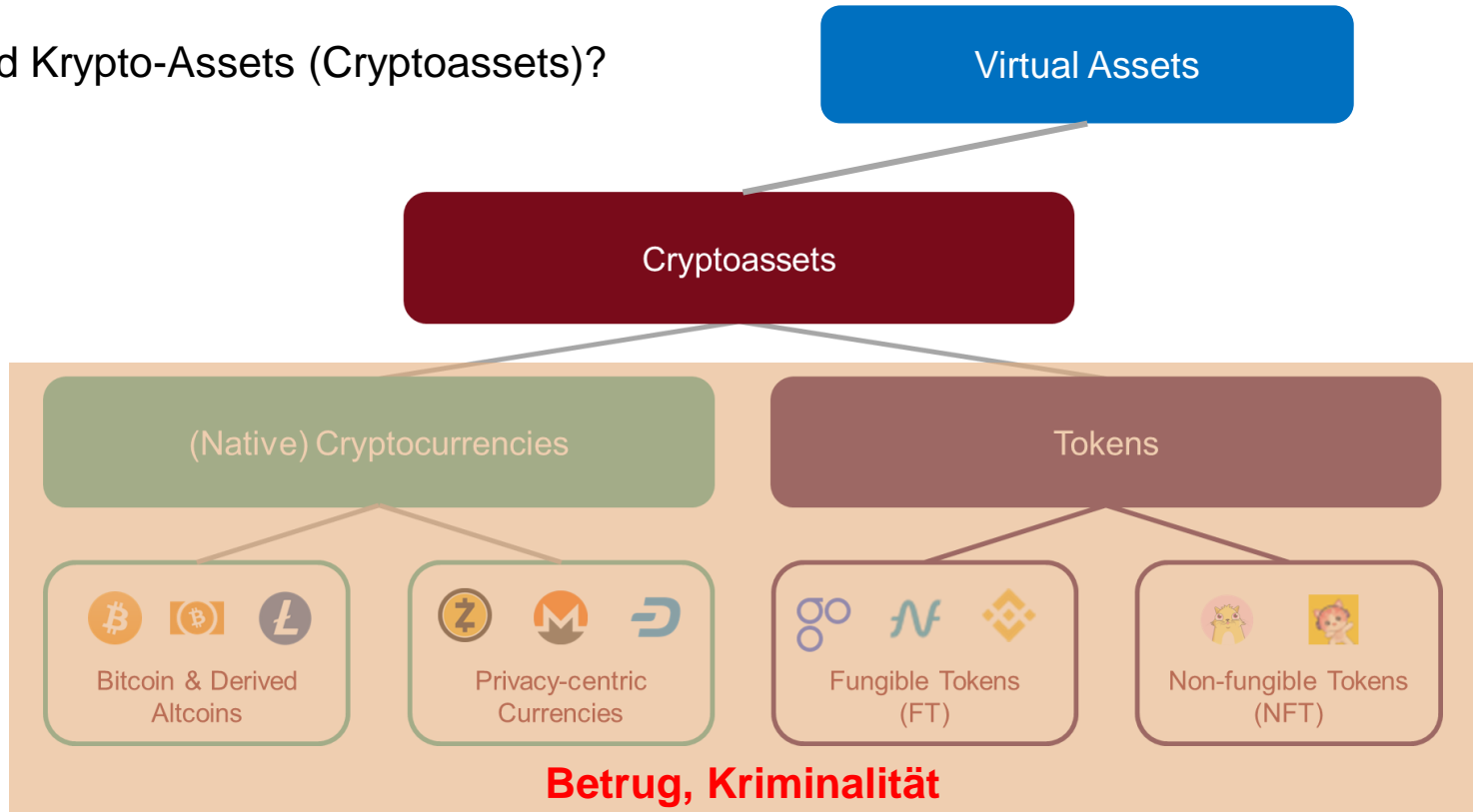
# EINFÜHRUNG: KRYPTO-ASSETS

Was sind Krypto-Assets (Cryptoassets)?



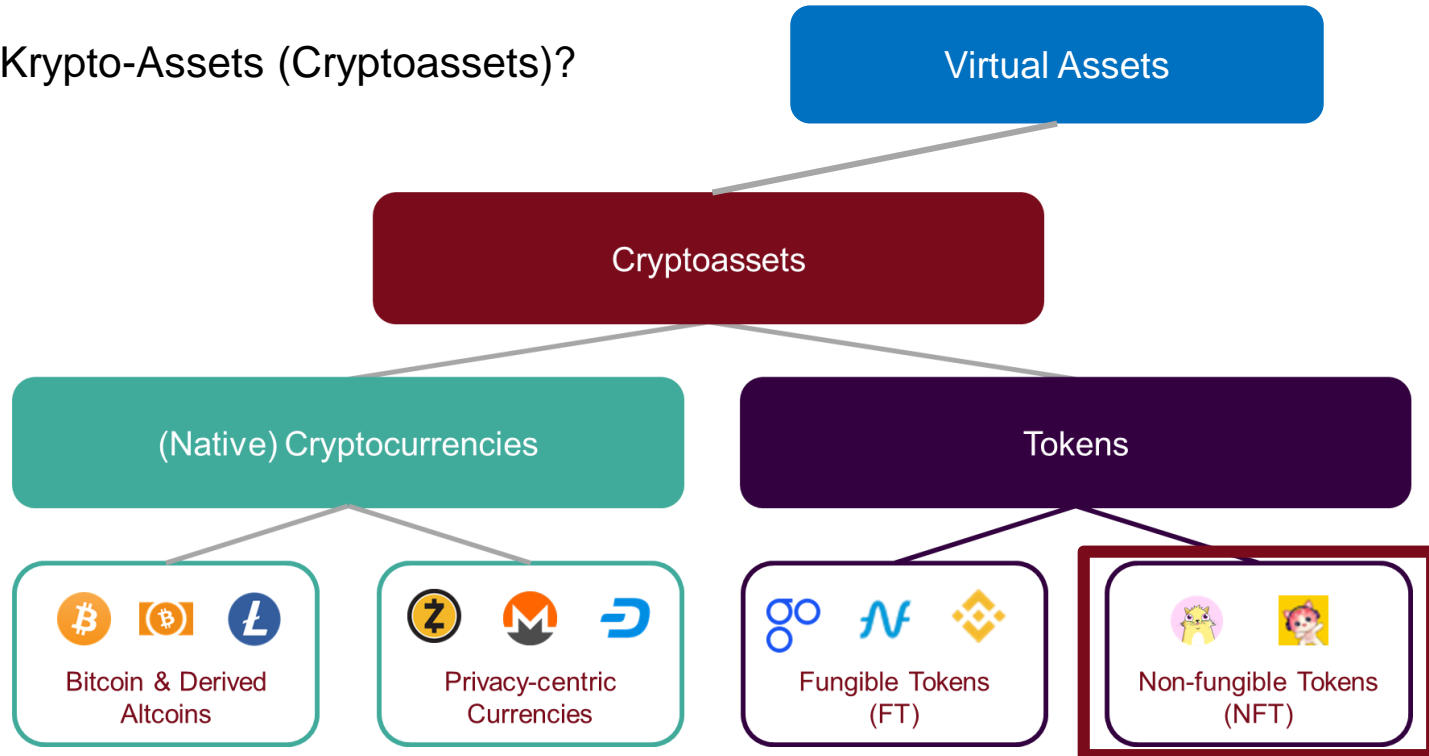
# EINFÜHRUNG: KRYPTO-ASSETS

Was sind Krypto-Assets (Cryptoassets)?



# EINFÜHRUNG: KRYPTO-ASSETS

Was sind Krypto-Assets (Cryptoassets)?



KRYPTO-ASSETS UND NFTS

ETHEREUM und SMART CONTRACTS



# ETHEREUM



- Zweitwichtigstes Blockchain-System nach **Marktkapitalisierung**
- Open-Source, öffentlich, verteilt
  - Ziel: dezentralisierte Anwendungen
  - Eingebaute Kryptowährung: Ether (ETH)
  - neue Implementierung, **kein** Bitcoin-Fork
- Online seit 30. Juli, 2015
- Unterscheidungsmerkmal: **Smart Contracts**
  - Smart Contracts sind Programme, die auf der **Ethereum Virtual Machine** laufen



# ETHEREUM



- 
- 
- 
- 



**widmit** 🍊  
@widmit



The cost of a kidney on the black market is around 46,000\$. There's approximately 8 billion people in the world each with 2 kidneys. From this we can imply the market capitalization of kidneys is 736,000,000,000,000\$

4:47 AM · May 4, 2022



🍷 22.5K    💬 Reply    🔗 Copy link

[Read 979 replies](#)

# ETHEREUM



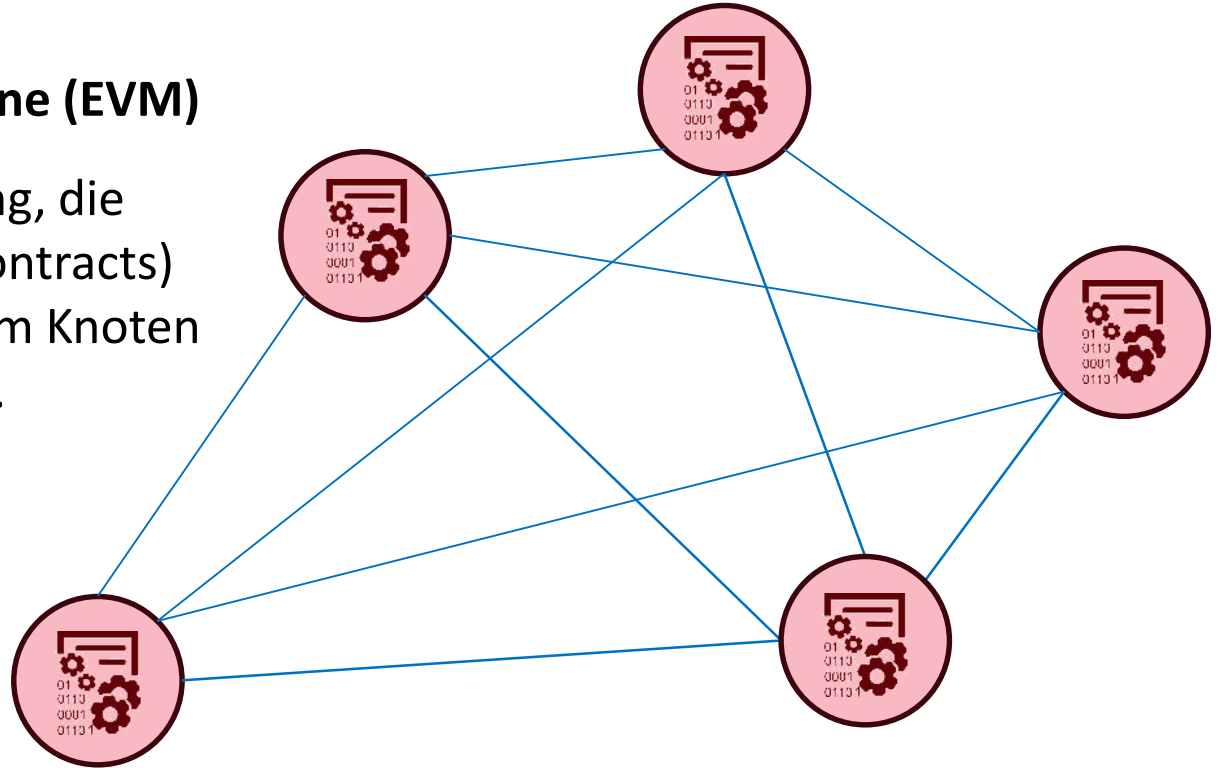
- Zweitwichtigstes Blockchain-System nach **Marktkapitalisierung**
- Open-Source, öffentlich, verteilt
  - Ziel: dezentralisierte Anwendungen
  - Eingebaute Kryptowährung: Ether (ETH)
  - neue Implementierung, **kein** Bitcoin-Fork
- Online seit 30. Juli, 2015
- Unterscheidungsmerkmal: **Smart Contracts**
  - Smart Contracts sind Programme, die auf der **Ethereum Virtual Machine** laufen





## Ethereum Virtual Machine (EVM)

- Eine Laufzeitumgebung, die Programme (Smart Contracts) ausführt, die auf jedem Knoten bereitgestellt werden.



# ETHEREUM



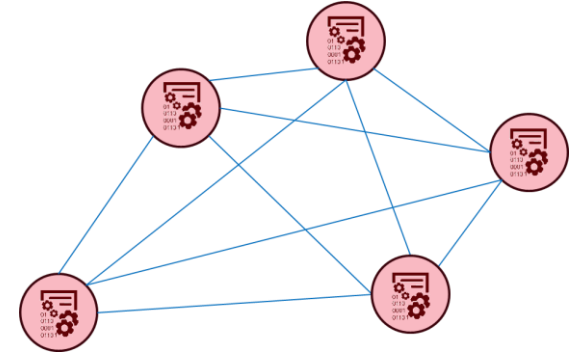
## Ethereum Virtual Machine (EVM)

- Fähig zu **600,000** einfachen Operationen (Addition) pro Sekunde
- Kosten: €225 pro Sekunde

## Raspberry Pi 4

- Fähig zu **3,000,000,000** einfachen Operationen (Addition) pro Sekunde
  - d.h., 5000 x stärker
- Kosten: €65 einmalig

Source: Nicholas Weaver Computer Security 161 Cryptocurrency Lecture  
<https://www.youtube.com/watch?v=J9nv0OI-R5Q>





## Smart Contracts

- Smart Contracts laufen auf der **Ethereum Virtual Machine**
- Aktivieren bei Erhalt einer Transaktion
- Speichern und Ändern des lokalen Zustands
- Beliebige Berechnungen durchführen
- Mögliche Anwendungen:
  - *Token systems*
  - *Decentralized exchanges*
  - ... USW.



	A	B	C
1			
2		Address	0x68b3465833fb72A70ecDF485E0e4C7bD8665Fc45
3		Balance	259.529883570861248783
4		Nonce	54789
		Bytecode	608060405234801561001057600080fd5b506040516103d5 3803806103d5833981018060405281019080805182019291 905050508060009080519060200190610049929190610050 565b50506100f5565b828054600181600116156101000203 166002900490600052602060002...
5		State	Alice: 22.03 Bob: 16.85 Celia: 1.12 Doug: 0.02 Edward: 191.36 ...
6			
7			
8			
9			

Contract Account

# ETHEREUM



## ERC 20 Token Standard

- Vorgeschlagen Ende 2015
- Schnittstelle für **Fungible Tokens**
- Definiert gemeinsamen Funktionen:

Classification Signature First 4-byte Keccak hash

ERC20	Required	Method	Classification	Signature	First 4-byte Keccak hash
			Method	Signature	First 4-byte Keccak hash
Optional	Method	totalSupply()			18160ddd
		balanceOf(address)			70a08231
		transfer(address,uint256)			a9059cbb
		transferFrom(address,address,uint256)			23b872dd
		approve(address,uint256)			095ea7b3
		allowance(address,address)			dd62ed3e
		name()			06fdde03
Optional	Event	Transfer(address,address,uint256)			ddf252ad
		Approval(address,address,uint256)			8c5be1e5
		symbol()			95d89b41
Optional	Method	decimals()			313ce567

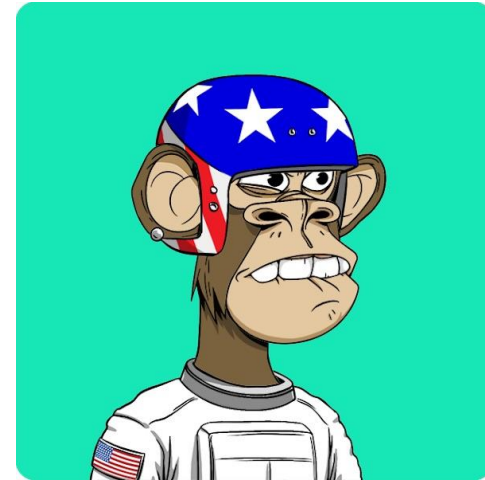
BNT	QNT	cDAI	Multi-collateral DAI
CVC	RCN	cSAI	KCS
EURS	REP	ENJ	LEND
GNT	RLC	OXT	LOOM
GYEN	SAI	CEL	LRC
KNC	SNT	CELR	NEXO
MANA	STORJ	cUSDC	NPXS
MATIC	sUSD	ELF	PAY
MTL	WBTC	ENG	POWR
NMR	WTC	FET	REN
OKB	ZUSD	HOT	VGX

from <https://nominex.io/blog/education/list-of-erc20-tokens/> (2021-09-05)



## ERC 721 Token Standard

- Ein offener Standard für die Erstellung von **Non-Fungible Tokens - NFTs** (einzigartigen)
- Definiert gemeinsamen Funktionen des NFT-Smart-Contracts
- Neue Schnittstellen für:
  - Ownership: **ownerOf**
  - (Safe) transfer of ownership: `safeTransferFrom` (e.g., check that `_to` is an actual contract)



# ETHEREUM



## ERC 721 Token Standard

- Das „Kunststück“, auf das im NFT-Smart Contract Bezug genommen wird, wird nicht im Smart Contract und somit auch nicht in der Ethereum-Blockchain gespeichert.
- Es wird nur ein **Link** zur NFT gespeichert!
- *“It is like you purchased a receipt. You have purchased a token that points to a picture.”*  
– David Gerard, author of *“Attack of the 50 Foot Blockchain”*

	A	B	C
1			
2		Address	0xb3016eaE8d9ab5c18405bbA45DCCf7396D91FD1D
3		Balance	0.00
4		Nonce	122
5		Bytecode	608060405234801561001057600080fd5b506040516103d53803806103d5833981018060405281019080805182019291905050508060009080519060200190610049929190610050565b50506100f5565b828054600181600116156101000203166002900490600052602060002...
6		State	<pre>{"name": "Smooth Dreamer", "description": "Spicy Pebble #10\n\nThis one is a big dreamer. Sleeping almost all the day. When it is awake, loves to tell his dream stories.\n\nTastes like ripe plums and smells of magical woodE\n\n\n2000x2000\n", "image": "ipfs://Qm2juJfKboeM2TnLh65WaYbktVmBHKxUhgZduYJFHKTPHx/nft.mp4"}</pre>
7		Creator	0x29f54ac74785349fc0750c216065ff221a6b8405
8		Owner	0xcd472070e455bb31c7690a170224ce43623d0b6f
9			

<https://etherscan.io/nft/0xb3016eaE8d9ab5c18405bbA45DCCf7396D91FD1D/10>  
<https://foundation.app/@ASiiiSA/pebbles/10>

# KRYPTO-ASSETS UND NFTS

## NFTs und FRAUD



# NFTS UND FRAUD

## Inhärenter Wert: Null

- Tokens können einen Marktwert ungleich Null haben, aber ihr fundamentaler Wert kann nie etwas anderes als Null sein.
- NFTs haben keinen inhärenten Wert - nur den Wert des „größeren Narren“ (*greater fool*), der bereit sein könnte, mehr dafür zu bezahlen.

April 13, 2022

### NFT collector gets \$280 top bid for the Jack Dorsey tweet NFT he bought for \$2.9 million last year

After Jack Dorsey made an NFT out of his first-ever tweet, then-cryptocurrency executive Sina Estavi won the auction in March 2021 with a 1,630 ETH bid (then around \$2.9 million). A little over a year later, on April 6, Estavi tweeted that he would be selling the NFT. He listed the NFT on Opensea for 14,969 ETH (around \$46 million), in an auction slated to last a week. When the auction closed, there were seven offers ranging from 0.0019 ETH (\$6) to 0.09 ETH (\$277). It's still up to Estavi whether or not to accept a bid.



NFT of Jack Dorsey's first tweet  
([attribution](#)).

- "['Jack Dorsey's First Tweet' NFT Went on Sale for \\$48M. It Ended With a Top Bid of Just \\$280](#)", *CoinDesk*

# Hmm Blockchain: Ethereum, Polygon | NFT

from <https://web3isgoinggreat.com/> (retrieved on 2022-04-18)

# NFTS UND FRAUD

## FRAUD Type 1: “Rug Pull”

- Ein "Rug Pull" ist eine Art von Betrug, bei dem die Entwickler und/oder Gründer eines Projekts ihre Versprechen nicht einhalten, sondern nach Erhalt einer Investition einfach verschwinden.
- Diese Art von Betrug findet auch bei Kryptowährungen und Token sowie bei NFT-Projekten statt.



<https://twitter.com/PeckShieldAlert/status/1486305364018556928>

# NFTS UND FRAUD

## FRAUD Type 2: “Pump and Dump”

- In Anlehnung an eine Form des Wertpapierbetrugs werden "Pump and Dump"-Prozesse eingesetzt, um den Preis eines NFT künstlich in die Höhe zu treiben.
- Dies geschieht durch mehrere Gebote innerhalb einer kurzen Zeitspanne, um den Anschein zu erwecken, dass der NFT wertvoll ist
- Sobald ein Vermögenswert den angestrebten Verkaufspreis erreicht hat, machen die Insider Kasse, indem sie an den nächsten „greater Fool“ verkaufen.



An example of a pump-and-dump scheme in action / Image Credit: TradingView

<https://vulcanpost.com/778953/how-investors-can-trade-cryptocurrency-nfts-safely/>

# NFTS UND FRAUD

## FRAUD Type 3: PHISHING

- Gefährliche Linke oder Anhänge
- Betrügerische Webseiten
  - NFT-Betrüger können beliebte NFT-Websites und/oder -Marktplätze nachbilden, um Benutzer zur Preisgabe ihrer Kontodaten zu verleiten.
- „Airdrop Scams“
  - Durch das Versprechen kostenloser NFTs verschaffen sich die Betrüger Zugang zu den Anmeldedaten und Konten der Benutzer

### NFT Scam Prevention Tips



Create strong passwords



Never click on suspicious links or attachments



Enable two-factor authentication



Always crosscheck NFT prices



Never share your seed/recovery phrase



Verify NFT seller accounts

# NFTS UND FRAUD

## FRAUD Type 4: Insider Trading

- Front-running
  - Handel mit Finanzanlagen durch einen Makler, der Insiderwissen über eine zukünftige Transaktion hat, die sich auf den Kurs auswirken wird.

*Empfehlung: David Gerard*

<https://davidgerard.co.uk/blockchain/>

### Former OpenSea executive Nate Chastain arrested for insider trading of NFTs

1st June 2022 - by David Gerard - [Leave a Comment](#)

*by Amy Castor and David Gerard*

A New York grand jury has charged former OpenSea executive Nathaniel Chastain, 31, with money laundering and wire fraud in connection with insider trading of NFTs. [[SDNY press release](#); [indictment](#), PDF]

Chastain was indicted on Tuesday 31 May, and arrested Wednesday 1 June in New York.

Chastain's name may be familiar – he's OpenSea's former head of product who was caught front-running OpenSea customers in September 2021. He bought NFTs just before they hit the front page of the site. His Twitter account, @natechastain, features a Twitter hexagon NFT avatar of a CryptoPunk. [[Twitter](#)]

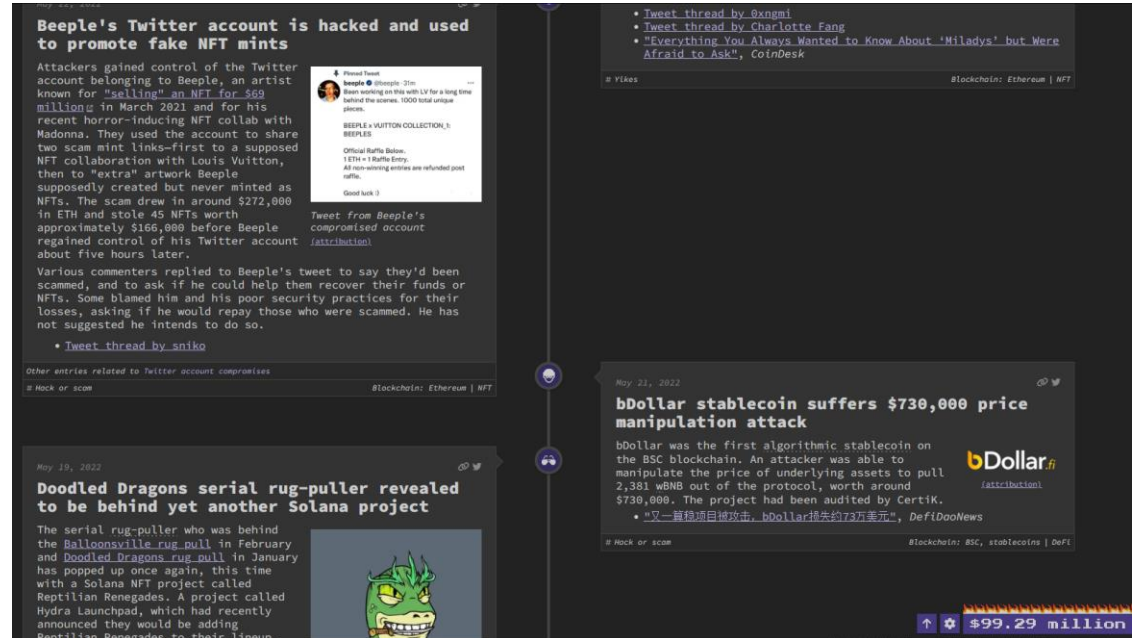
# NFTS UND FRAUD

## FRAUD Type X...

*Empfehlung: Molly White*

<https://web3isgoinggreat.com/>

<https://blog.mollywhite.net>



**Beeple's Twitter account is hacked and used to promote fake NFT mints**

Attackers gained control of the Twitter account belonging to Beeple, an artist known for "selling" an NFT for 569 million in March 2021 and for his recent horror-inducing NFT collab with Madonna. They used the account to share two scam mint links—first to a supposed NFT collaboration with Louis Vuitton, then to "extra" artwork Beeple supposedly created but never minted as NFTs. The scam drew in around \$272,000 in ETH and stole 45 NFTs worth approximately \$166,000 before Beeple regained control of his Twitter account about five hours later.

Various commenters replied to Beeple's tweet to say they'd been scammed, and to ask if he could help them recover their funds or NFTs. Some blamed him and his poor security practices for their losses, asking if he would repay those who were scammed. He has not suggested he intends to do so.

- [Tweet thread by sniko](#)


Other entries related to Twitter account compromises

# Hack or scam | Blockchain: Ethereum | NFT

---

**Doodled Dragons serial rug-puller revealed to be behind yet another Solana project**

The serial rug-puller who was behind the Balloonsville rug pull in February and Doodled Dragons rug pull in January has popped up once again, this time with a Solana NFT project called Reptilian Renegades. A project called Hydra Launchpad, which had recently announced they would be adding Reptilian Renegades to their lineup.



May 10, 2022

---

**bDollar stablecoin suffers \$730,000 price manipulation attack**

bDollar was the first algorithmic stablecoin on the BSC blockchain. An attacker was able to manipulate the price of underlying assets to pull 2,381 wBNB out of the protocol, worth around \$730,000. The project had been audited by CertiK.

- [又一盲移项目遭攻击, bDollar损失约73万美元](#), [DefiDooNews](#)

# Hack or scam | Blockchain: BSC, stablecoins | DeFi

\$99.29 million

from <https://web3isgoinggreat.com/> (retrieved on 2022-06-02)

## ZUSAMMENFASSUNG

- Non-fungible Tokens (NFTs) sind eine besondere Art von Virtual Assets
- Heute sind die meisten NFTs Ethereum Smart Contract Implementierungen des ERC-721 Standards
- NFTs haben keinen inhärenten Wert
- Im NFT-Ökosystem wimmelt es vor Betrug



# FRAGEN?

Ross King

[ross.king@ait.ac.at](mailto:ross.king@ait.ac.at)

