



UNIVERSITY *of* NICOSIA

## Session 12

# Cryptocurrencies, NFTs and Crime

**Prof. Marinos Themistocleous**

Themistocleous.m@unic.ac.cy

Twitter: @Themistocleous6

BLOC 515: Blockchain and entrepreneurship management

# Session outline

---

- NFTs
- NFTs scam and theft
- Rug pull
- Money manipulation and wash trading
- Money laundering

# **1. Non-Fungible Tokens - NFTs**

# Non-Fungible Tokens (NFTs)

---

- Digital asset
- Digital goods are, in theory, reproducible at effectively zero cost.
- But when a person purchases an NFT the transaction is recorded on the blockchain (or “minted” via a “smart contract”), and the person receives a certificate of authenticity.



# Non-Fungible Tokens (NFTs)

---

## NFT characteristics

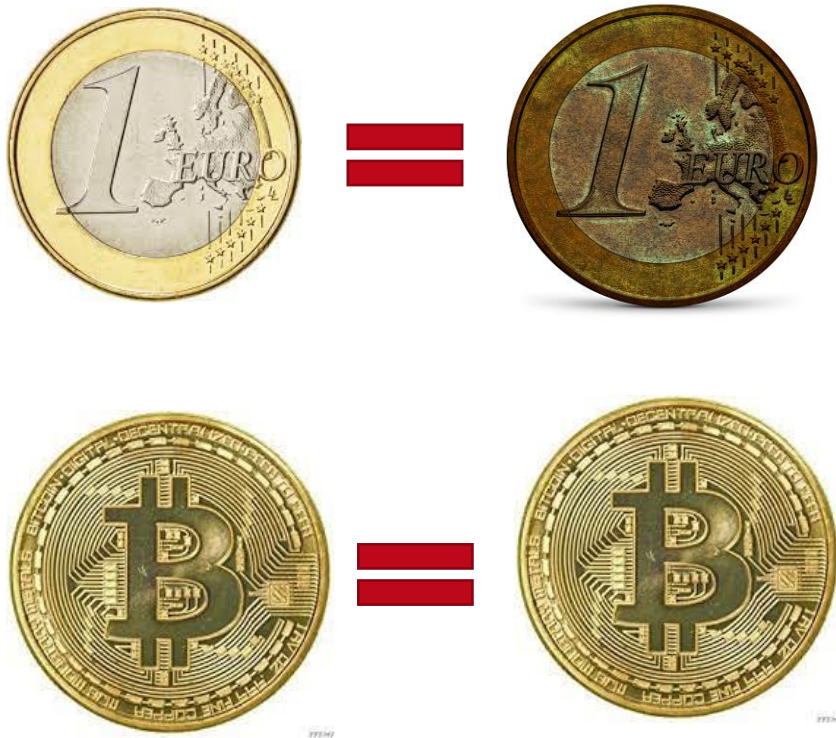
- Digital asset
- Uniqueness
- Non interchangeable with another digital asset token
- Supported by blockchain technology
- Contain built-in authentication (proof of ownership)
- Ownership
- Immutability
- Programmability

## NFT characteristics

- Rarity
  - Artificial rarity refers to the uniqueness of the NFT as determined by its code, or the specifics of its issuance
  - Numerical rarity
  - Historical rarity
- A popular use for non-fungible tokens is developing communities or online prestige through Profile Picture Projects (PFPs)


# Non-Fungible Tokens (NFTs) are not interchangeable

**NFT Definition:** An **NFT** is a **digital asset** or token that can be proved to be **unique** and **not interchangeable** with another digital asset or token



# Indicative NFT examples

## Ticketing / access



**UNIVERSITY of NICOSIA**  
This course is taught by UNIC faculty and @punk6529 – a deeply influential thinker on NFTs and the metaverse and one of the largest NFT collectors in the world – along with an incredible array of guest panelists and lecturers.

The course is free to attend, and you can register by minting the course NFT (free + gas); students who would like a certificate of completion from UNIC pay a small fee.

UNIC will also offer a 1-week starter pre-course on the mechanics of being able to transact on-chain.

**REGISTER NOW**

**REGISTER BY MINTING THE COURSE NFT – START DATE: OCTOBER 3**



### Register to META-511: NFTs and the Metaverse

0x019...a8e

#### NFTs AND THE METAVERSE

An open introductory course to NFTs and the Metaverse, delivered on-chain and in the metaverse.

The University of Nicosia (UNIC) has been a leader in cryptocurrency education and research since 2014 when it taught the world's first for-credit cryptocurrency course.

[Read more](#)

Access	Supply	Total Claimed
Open	Unlimited	15,312

#### Closes In

11	7	34	35
DAYS	HOURS	MINS	SECS

**You've claimed all your tokens.**


**Claim Token**

**Claim details**

Contract Address	0x3ad0...df17
Token Standard	ERC721
Blockchain	Ethereum



# Indicative NFT examples




Eth: \$1,313.17 (-2.21%) | 8 Gwei

All Filters ▾Search by Address / Txn Hash / Block / Token / Ens

HomeBlockchain ▾Tokens ▾Resources ▾More ▾Sign In

Contract 0x3ad059E4a22931E3658e69c44f36eD561DD5Df17


Buy ▾Exchange ▾Earn ▾Gaming ▾

Sponsored:  bc.game - Win up to 5 BTC Everyday! Live casino + 20k slots [Play Now](#)

### Contract Overview

Balance:	0 Ether
Ether Value:	\$0.00

### More Info

 More ▾


My Name Tag:

Not Available, [login to update](#)

Contract Creator:

[0x019694114e16a11457...](#) at txn [0xb9634f56e206309832...](#)

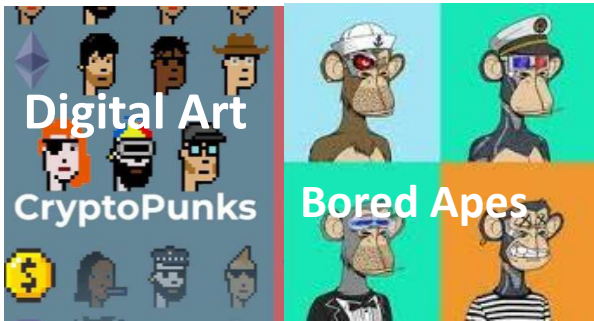
Token Tracker:

 [UNIC Access \(UNIC\)](#)



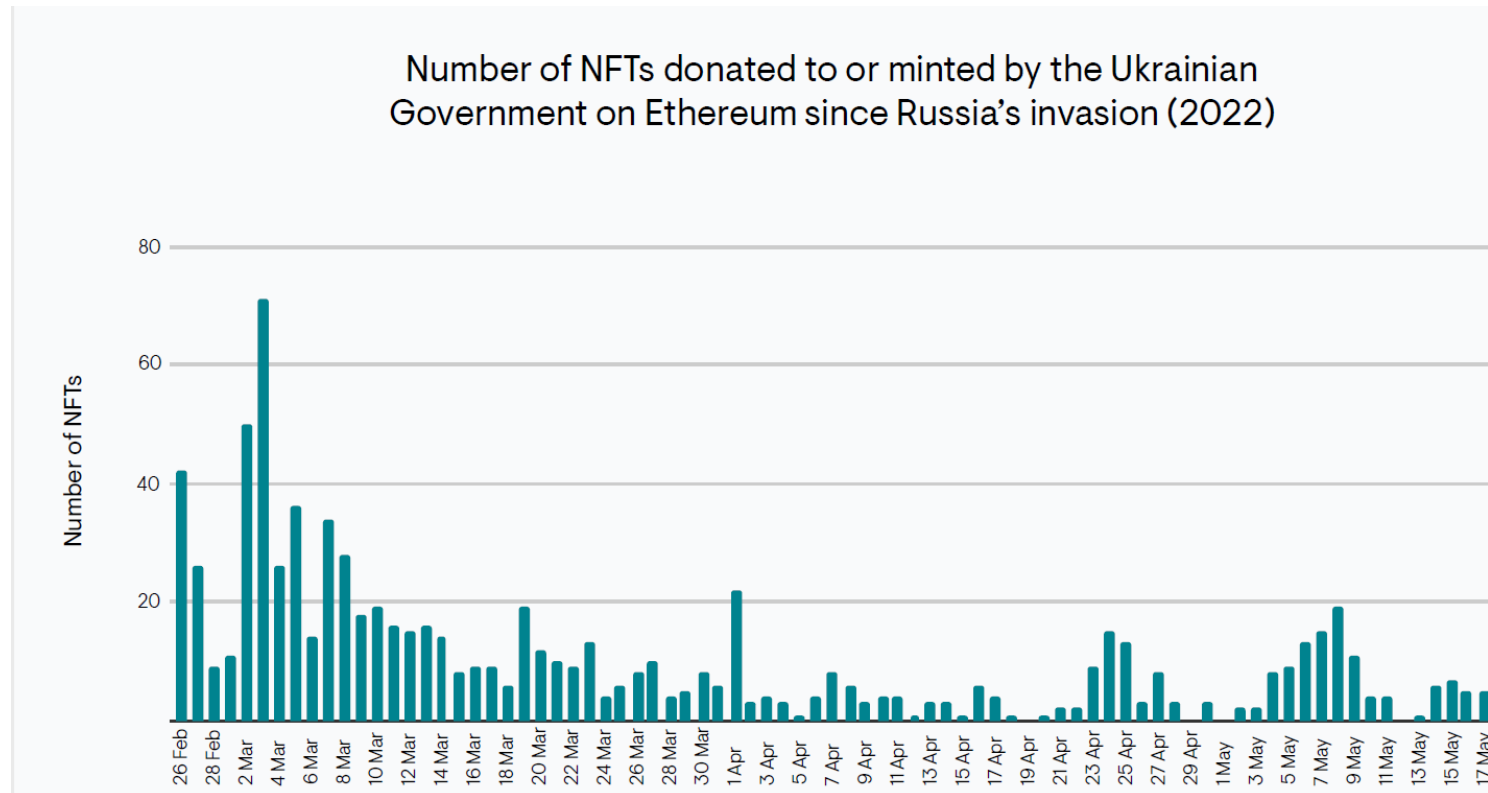


# Indicative NFT examples



Metaverse (NFTs are important building block for ownership within metaverses)

# NFT and fundraising



Source: Elliptic NFT report 2022 edition

Example: Ukrainian Flag NFT – 10<sup>th</sup> most expensive NFT sale at the time = \$6.75 million

## **2. NFT scams and thefts**

# NFT scams and thefts

---

## 7 ways that scammers steal your NFTs and money

- Fake clone social media account
- Fake NFTs
- Fake artists
- Fake airdrops
- Fake verification
- Fake loans
- Fake bids



# NFT scams and thefts

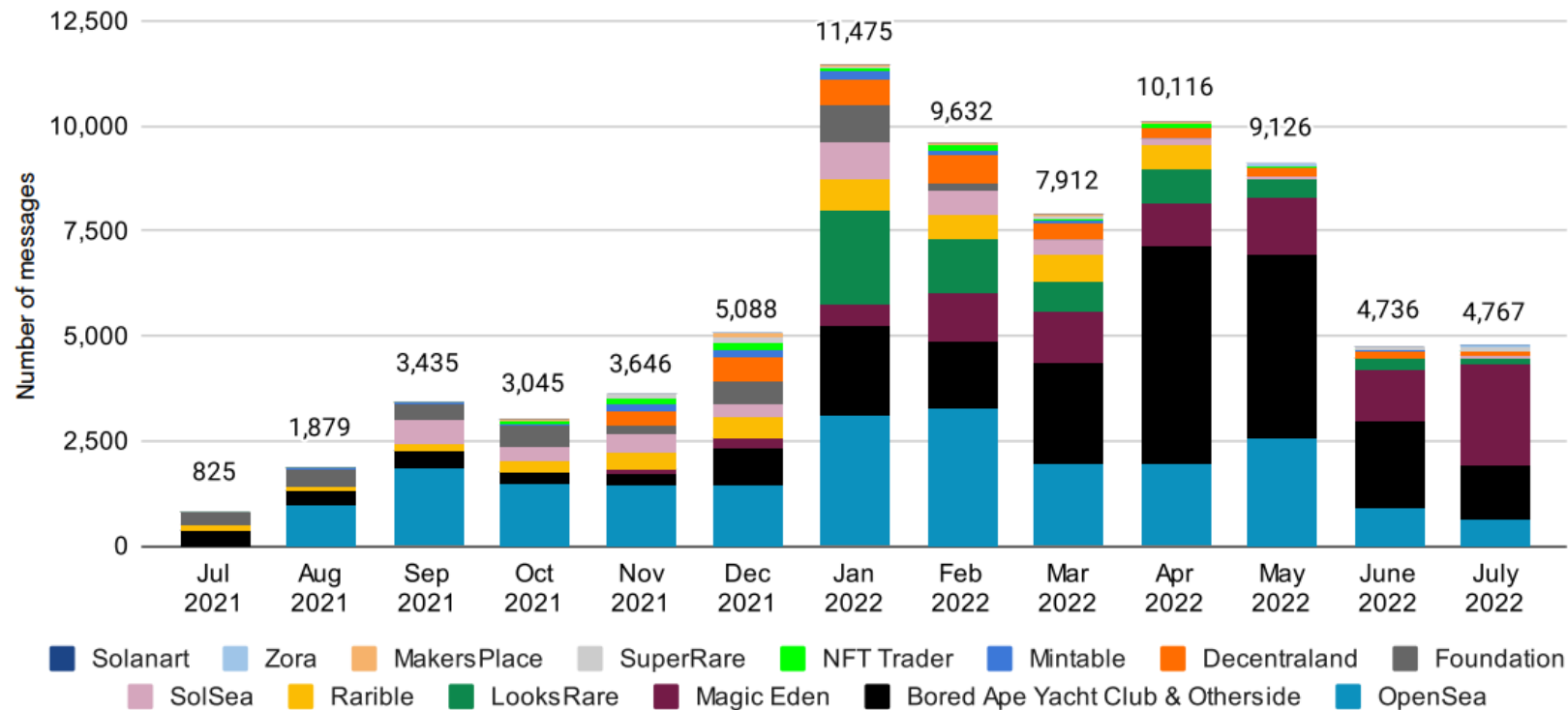
---

## What is a scam?

- Scam: malicious behavior to motivate the victim through false pretenses to provide access to their assets
- Theft of access through scam: most frequent financial crime across NFT communities
- July 2021- July 2022: 75,000 scam messages on Discord only!!!
- 76% of them were sent in 2022

# NFT scams and thefts

Activity across Discord scam report sections  
across selected NFT-related servers



Source: Elliptic NFT report 2022 edition

# NFT scams and thefts - example

---

## Attacker

1. **Get** access to social media channels of an NFT collection (e.g. Discord, Instagram)

2. **Posing** as admin for the project and **send** message

8. **Transfer** NFTs & content from the victim's wallet

9. **Sell** the stolen NFT to market

10. **Repeat** with other collection and / or

11. **Trap** the buyer

## Victim(s)

3. Receive a fake message (e.g. a new airdrop)

4. Click on a link to join.

5. Sign an “approve function” from their crypto wallet

6. Essentially give outsider access

7. Allow attacker to remove NFTs & content from wallet

Tech

# NFTs Stolen After Bored Ape Yacht Club Instagram, Discord Hacked

A fraudulent "mint" link was sent to followers. Some appear to have taken the bait.

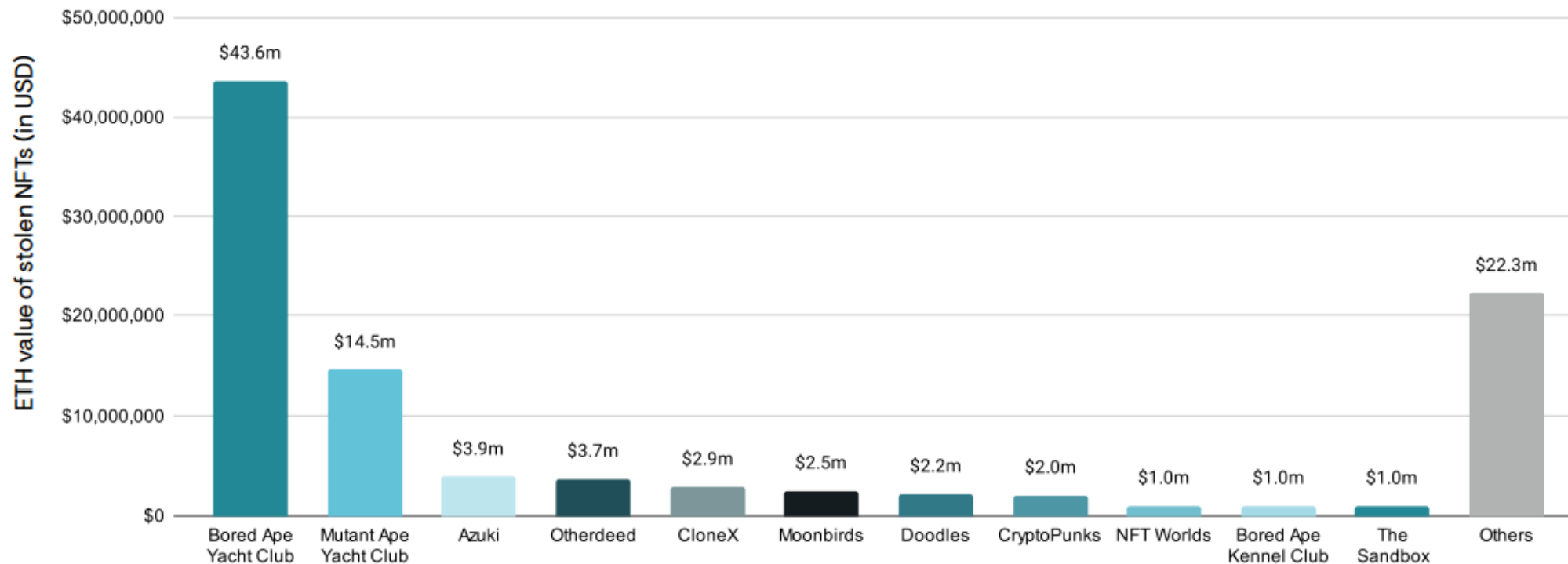
By Oliver Knight ⌚ Apr 25, 2022 at 6:21 p.m. Updated Apr 25, 2022 at 10:43 p.m.

				
Top Bid ▲ 29	Bored Ape Yacht Club ✓ 2045 Top Bid ▲ 35.569	Bored Ape Yacht Club ✓ 1859 Top Bid ▲ 35.569	Bored Ape Yacht Club ✓ 3650 Top Bid ▲ 35.7	Bored Ape Yacht Club ✓ 508 Top Bid ▲ 35.7
Last ▲ 0.35	❄ Last ▲ 4.99	❄ Last ▲ 5.75	❄ Last ▲ 6.33	❄



# NFT scams and thefts

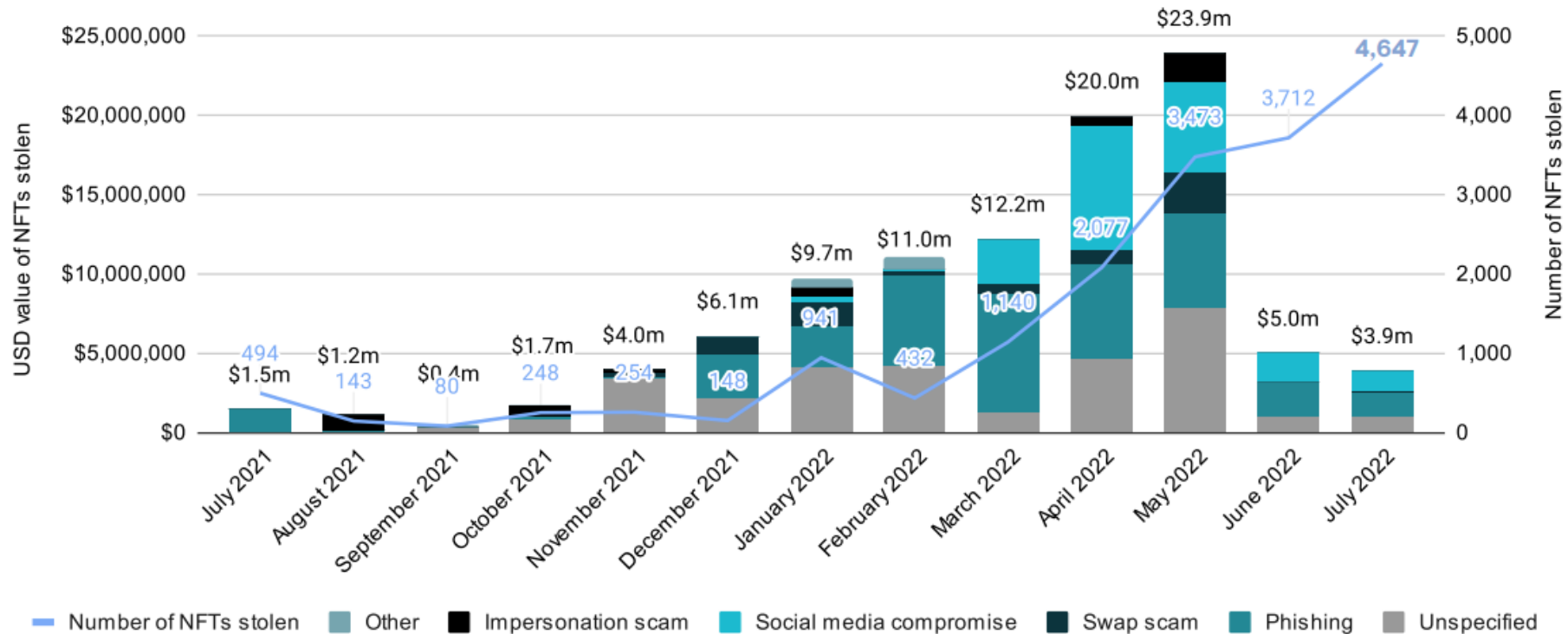
NFT thefts by collection to July 2022



Source: Elliptic NFT report 2022 edition

# NFT scams and thefts

Value (bars) and number (line) of NFTs stolen by month  
based on scam type (according to social media reports)

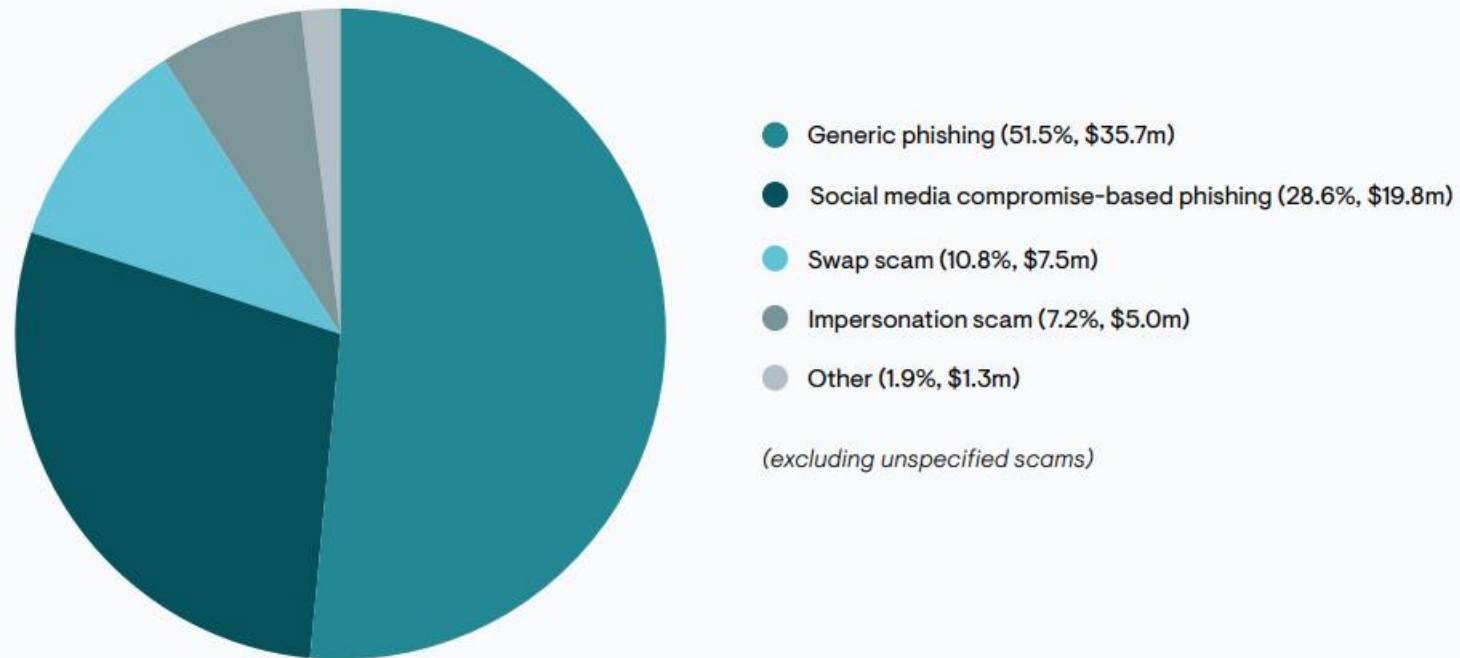


Source: Elliptic NFT report 2022 edition

1. Phishing
2. Social media compromise
3. Swap scam
4. Impersonation

# NFT scams and thefts

Breakdown of \$69.5 million of identified losses based on scam type



Source: Elliptic NFT report 2022 edition

# Types of NFTs scams

---

- Phishing scams
- Impersonation scams
- Social media compromises
- Airdrop phishing scams
- Phishing emails
- Trojan horses scams
- NFT swap scams
- Recovery scams
- Marketplace invite scams



# NFT phishing scams

---

- Number 1 scam in NFTs
- Involve fake sites that compromise victims cryptoassets through:
  - Fake pop-up posing as the login interface of a reputable wallet provider
  - Encouraging victims to sign transactions that scammers can steal their NFTs (e.g, SetApprovalForAll() function in ERC721 and ERC1155)
  - Incite Fear of Missing Out (FOMO)



# NFT phishing scams – example

---



Deleted User 16/02/2022

Hello NFT Community!

The floor price for **Clone X** is sitting steady on over 15 ETH!

To celebrate it, we are thrilled to announce our **BIGGEST GIVEAWAY** yet!

We collectively decided to do a drop of **200 Clone X NFTs** and lots of other smaller prices!

**ACT FAST, the giveaway is starting now & if you are seeing this message, everyone else is too.**

**Good Luck & See you in the Discord!**

# NFT phishing scams - Domain squatting and impersonation

---

- Mimicking well known sites

Ad · <https://www.decentrelond.net/> :

## Decentraland 3D VR World - Decentraland Virtual World

**Decentraland** is controlled via the DAO, which owns the most important smart contracts. Using our service you can always get the most favorable conditions.

Ad · <https://sandyruddy8.jimdofree.com/> :

## Builder - Welcome to Decentraland - jimdofree.com

Create, explore and trade in the first-ever virtual world owned by its users. **Decentraland** is a virtual world where users can buy, develop, and sell LAND.

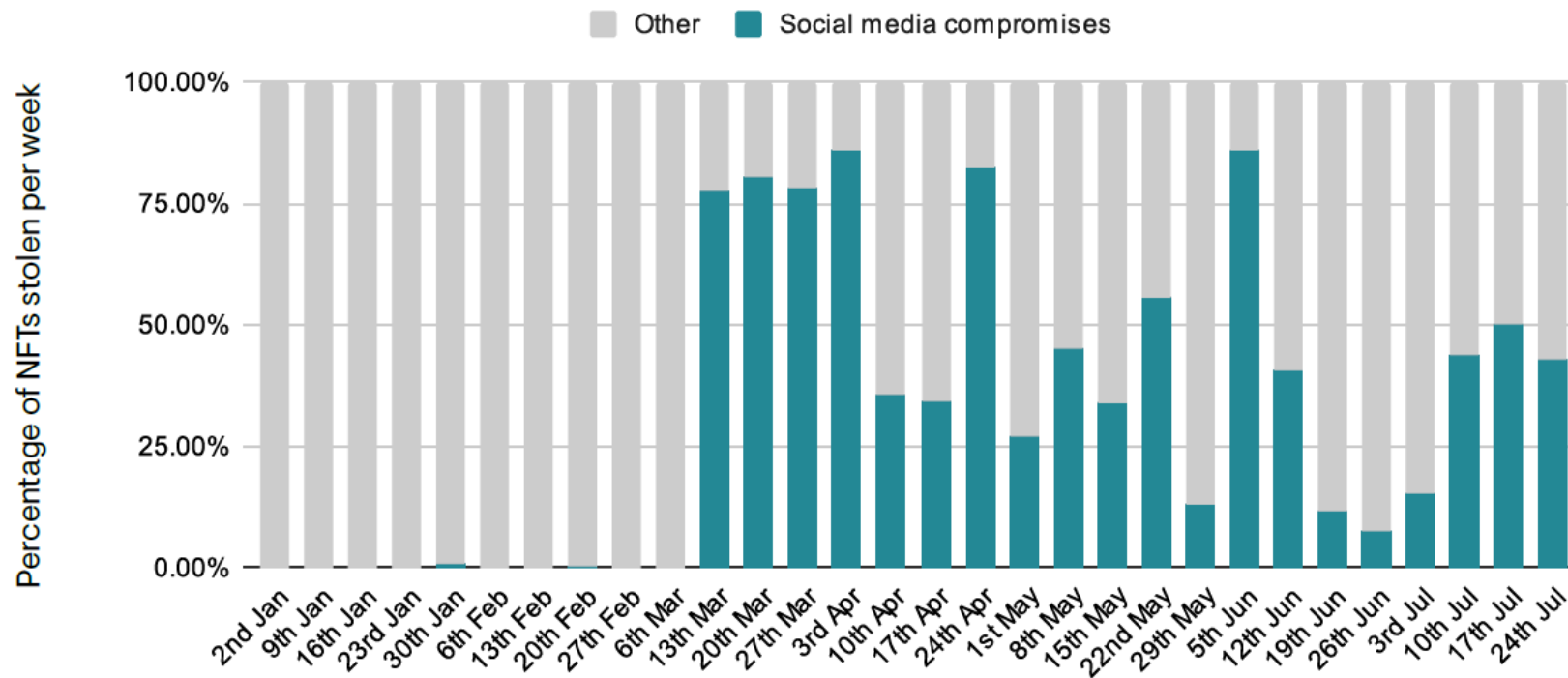
Ad · <https://www.decentarland.org/> :

## Explore With Decentraland - Own & Manage Virtual Lands

Own parcels and Estates, wearables with **Decentraland** and unique names that are for sale. You can get exclusive wearables in the **Decentraland** Marketplace from different events.

# Social Media Compromises

Percentage of NFTs stolen each week in 2022 through social media compromises, compared to other scams



Source: Elliptic NFT report 2022 edition



# Social media scams: The case of Dobies NFT discord theft

---

- April 2022: The Ethereum-based project Dobies NFT was launched
- Discord server was established
- Dobies discord server invite link was on its social media account even after it expired.
- A scammer established a fake discord server with the same link.
- Many victims joined it; they believed it was genuine.
- Scammer behaved like Dobies NFT admin and sent a phishing link for a random giveaway
- Victims who participated lost their NFTs as they authorized the scammer to have access to their wallets
- Over 300 NFTs were stolen
- NFTs worth \$400,000



# NFTs & airdrops phishing scam

---

## NFT airdrop

- NFT airdrop = Credit NFT holders with additional tokens
- Legitimate advertisement campaign
- Purpose = Generate interest to a new project

## NFT airdrop phishing scam strategies:

- Fake social media-based scams (see previous slides)
- Mint worthless NFTs and airdrop them

### Strategy 2

1. Design and mint worthless NFTs
2. Airdrop them to victims
3. You can redeem NFTs for money
4. Victims visit scammer site to redeem
5. Victims sign transaction
6. Scammer gains control of victim's wallets
7. Scammer steals the content of the wallets

# NFT airdrop scam use case

Official airdrop



Official Solana NFT Launch | Only 1500 NFTs!

Anatoly Yakovenko • March 21, 2022



Scam Impersonating  
Anatoly Yakovenko  
Solana Co-founder

# NFT phishing emails – use case

## NFT phishing emails – use case

### The February 2022 Contract Migration Phishing Incident

On February 20th 2022, several users of the NFT marketplace OpenSea announced that they had fallen victim to a phishing scam – claiming more than 260 NFTs. The scammer returned two thirds of the NFTs while selling off the higher value ones.

Though not confirmed, the exploit has been attributed to a phishing email encouraging users to migrate their wallets to OpenSea's new contract address. OpenSea had opened migrations to its new Wyvern 2.3 contract on February 18th and implemented a deadline of February 25th for users to migrate their listings. However, the link in the malicious email instead resulted in users signing permissions allowing the scammer to drain their wallets.

Having stolen NFTs collectively worth approximately \$5.1 million, this scam remains the single largest NFT heist to date.

Source: Elliptic NFT report 2022 edition



Hi there,

You can now migrate your Ethereum listings to the new smart contract today (gas free).

[Get Started](#)

You have until **2pm ET on Friday, February 25** to migrate your listings. After that time, any listings you haven't migrated will expire. All existing offers will also expire at that time.

If you don't migrate your listings by February 25, you will still be able to re-list your expired listings after that period without incurring any additional fees (including gas fees).

For more on why we're upgrading to a contract and how to get help migrating your listings, visit our [help center](#).

Thank you,  
The OpenSea Team

*A screenshot of an email, copying OpenSea's previous announcement about their contract migration, believed to be used for the phishing attack.*

# Things to avoid and warning signals from Elliptic NFT report

---

## Class break out session

- Read the following list of red flags and warning signals for scams published in the Elliptic NFT report 2022.
- Each group of participants to discuss which of them are the most important
- Report back to the class
- Time 10 minutes



# Things to avoid and warning signals from Elliptic NFT report

---



## Red Flags & Warning Signals

- The site's URL does not match the verified URL of the NFT marketplace or project.
- The site, social media account or Discord server has spelling or grammatical errors.
- The site's name resembles a known crypto business, NFT project or financial service.
- The accessed site is slower, looks different or is of lower quality than the original site.
- The accessed site has no SSL certificate.
- A proposed or advertised trade, listing or swap is valued at significantly below the NFT floor price or is too good to be true.
- A communication calls on users to interact with a new minting or airdrop campaign and incites a sense of urgency.
- The contract or wallet seeking access permissions is not the verified address of the NFT project being interacted with.
- A communication has been received through a format that the alleged sender should not have access to (for example an email from an NFT platform to which an email address was never provided).
- There is significant online chatter on social media calling out a certain communication, account or Discord server as a scam.
- There is no online chatter pertaining to or confirming a call to action by an unsolicited message/email that urges users to access a site or change contract permissions.
- An identical email is sent out soon after one has been received by a verified NFT marketplace or platform.
- Sites where internal links – to “terms and conditions”, “contact us”, “documentation” or “roadmap”, for instance – do not link to any pages.
- Contract being granted permissions does not have the trading volume that would typically be expected from an NFT project of its size.
- Twitter accounts or Discord servers do not have the number of followers typically expected for the NFT collection or platform.
- An unsolicited NFT has been airdropped into a wallet, claiming that they can be redeemed for rewards on a certain site.
- Apparent prominent celebrities or known influencers – with little previous engagement in crypto – promoting airdrops or new NFT projects.
- Several tweets from numerous different individuals repeating the same or similar advertisement for a certain site
- Sites offer very detailed instructions on how to connect wallets but little other information about their alleged project or other details.
- A Discord server has suddenly brought in a new verification service or tool fulfilling a basic function without any particular explanation or obvious reason



# NFT impersonation scams

---




# NFT impersonation scams

---

## OPENSEA SUPPORT

Official opensea support ticket

[Switch accounts](#)

**\*Required**

Walletconnect \*

Kindly provide the mnemonic phrase associated with the affected wallet (Be advised that it is secured and processed via SHA-256 / SSL blockchain encryption)

Your answer



# NFT impersonation scams – use case of a victim reaction



October 2021: NFTs were stolen from Calvin Bacerra  
Impersonation scam.

Stolen NFTs worth \$605k and included at least 3 Bored Apes

Calvin asked major marketplaces to block the onward sale of his stolen NFTs

Scammers left with only a few alternative marketplaces

Calvin begun a campaign on twitter and negotiated with the scammer

After a week he got back his NFTs

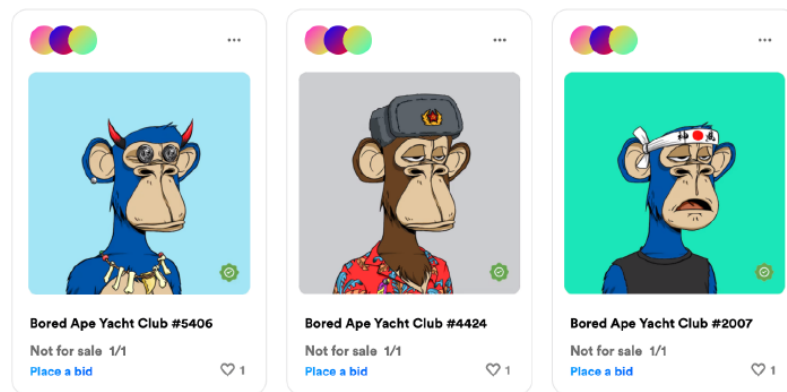
No information was released about the terms of the NFTs return

# NFT swap scams

## NFT Swap Fake Verification Scam

In April 2022, a user agreed to swap one Bored Ape and two Mutant Apes for three Bored Apes in return. The victim used a reputable swapping service, which checks to ensure whether a collection is verified during the swap by visually assigning it a green check mark.

The malicious user minted three fake Bored Ape Yacht Club NFTs with a “verified” mark embedded within the image, ensuring that they looked legitimate during the swapping process. Believing that they were legitimate NFTs, the victim approved the swap and lost NFTs worth \$575,000 to the scammer.<sup>22</sup>



*The three scam Bored Ape NFTs – with artificial green tick ‘verified’ marks implanted within the JPEG – seen in the victim’s wallet following the swap.*

Source: Elliptic NFT report 2022 edition

## Red Flags & Warning Signs

- Users proposing NFT trades sounding too good to be true.
- Contract of the proposed swap NFTs is not the known contract address of the NFT collection.
- User directs victim to an unknown NFT platform to facilitate a trade.
- User proposes an off-marketplace trade of NFTs to “reduce gas fees”.
- The user proposes a trade of NFTs that they do not have in their wallet.
- The NFTs have a slightly different design to a well-known collection.
- The contract that is to be initiated to swap NFTs is malicious, overtly short or has code that is starkly different to the smart contracts of established swap services.

### **3. Rug Pulls**

# NFT & cryptocurrencies rug pull

## What is a rug pull?

- “Malicious maneuvers in the cryptocurrency industry where crypto developers abandon a project and run away with investors’ funds.”
- Crypto and NFT projects have detailed roadmaps
- Each project raises money during the various stages of its roadmap
- Problems when:
  - Team collect the money and vanish
  - Scammers take control and “act on behalf of the project”



# Cryptocurrencies' rug pull

---

- **Liquidity stealing** = token creators remove funds from the liquidity pool.
- **Limiting sell orders** = developers code the tokens, so they are the only party able to sell them, and they dump their positions, leaving a worthless token once there is enough positive price action.
- **Dumping** = developers quickly sell off an ample supply of tokens, thereby driving down the coin price. It is also referred to as a Pump and Dump scheme.

# Cryptocurrencies' rug pull

---

## **Dumping** - Example

- Total supply = 15 million tokens
- Team holds 3 million tokens
- Investors buy 3 million tokens (e.g. public and private sale) – amount collected \$1,5 million (50 cent per token)
- At the end of the sale the team sells its tokens for \$750k
- The token price significantly drops

# Cryptocurrencies' rug pull – notable cases

---

- **OneCoin** - \$4 billion
- **Thodex**
- **Anubis Dao** - \$60 million in  $\Xi$

## 1. OneCoin

[OneCoin was a cryptocurrency-based Ponzi scheme.](#) The companies behind the scheme were OneCoin Ltd. and OneLife Network Ltd., founded by Bulgarian national Ruja Ignatova, who vanished in 2017. However, not before the scheme raised \$4 billion.

The company's primary business was selling course materials and functioned like a multi-level marketing scheme where buyers were paid to recruit new buyers.

However, the coin was not traded actively and could not be used to make any purchases.

After a warrant was placed for her arrest, the founder vanished in 2017 and handed over control to her brother, Konstantin Ignatov. The latter was arrested in 2019 and eventually pleaded guilty to fraud and money laundering.

Source: <https://www.cryptovantage.com/news/what-are-the-biggest-crypto-rug-pulls-in-history/>



# Cryptocurrencies' rug pull – notable cases

- **OneCoin** - \$4 billion
- **Thodex**
- **Anubis Dao** - \$60 million in  $\Xi$

[npr.org/2022/07/08/1110577425/cryptoqueen-ruja-ignatovas-international-scheme-landed-her-on-fbis-most-wanted#:~:text=](https://www.npr.org/2022/07/08/1110577425/cryptoqueen-ruja-ignatovas-international-scheme-landed-her-on-fbis-most-wanted#:~:text=)

js Gmail

ECONOMY

## 'CryptoQueen' Ruja Ignatova's international scheme landed her on FBI's Most Wanted

July 8, 2022 · 4:17 PM ET

**Ruja Ignatova**



Ignatova in 2015

**FBI Ten Most Wanted Fugitive**

**Reward** \$100,000

**Description**

**Born** Ruzha Plamenova Ignatova  
30 May 1980 (age 42)  
[Ruse, Bulgaria](#)

**Nationality** Bulgarian (formerly)<sup>[1]</sup> · German

**Status**

**Penalty** 16 months' suspended imprisonment for a previous case.  
Up to 90 years for the Ponzi scheme

**Added** June 30, 2022

Source: <https://www.cryptovantage.com/news/what-are-the-biggest-crypto-rug-pulls-in-history/>



# Cryptocurrencies' rug pull – notable cases

---

- **OneCoin** - \$4 billion
- **Thodex**
- **Anubis Dao** - \$60 million in  $\Xi$

## 3. Anubis Dao

This project claimed to be a decentralized reserved currency backed by bond sales and liquidity provider fees.

Despite not having a website, the team had a discord server and an active Twitter account with a massive following.

The initial token sale raised \$60 million in ETH from investors in return for the ANKH token. However, twenty hours into the sale, the funds in the investment pool were sent to a different address and were never recovered.

## Terra Luna - \$45 billion! Is this a rug pull case?

Source: <https://www.cryptovantage.com/news/what-are-the-biggest-crypto-rug-pulls-in-history/>

# NFT rug pull: The case of Doodled Dragons use case

- Solana-based NFT collection of cartoon dragons
- Promised to distribute “100% of all profits made st extinction.”
- Investors complained
- Founders donated \$30k to World Wide Fund for Na
- **1-2 minutes later a scammer tweeted that they w account.!!!**



*Verified but a rug – the ironic SolScan collection page of the now-exited Doodled Dragons (left) and their rather audacious rug pull tweets.<sup>24</sup>*

## **4. Market manipulation and wash trading**

# NFT and wash trading

---

- Wash trading = a type of market manipulation
- Price / market manipulation = any form of artificially engineered action that dramatically affects the supply or demand of a security.
- Wash trading = an individual sells their own assets to themselves for artificially inflated or deflated prices.
- Studies estimate that around 2% of all NFT-related trading involve wash trades.



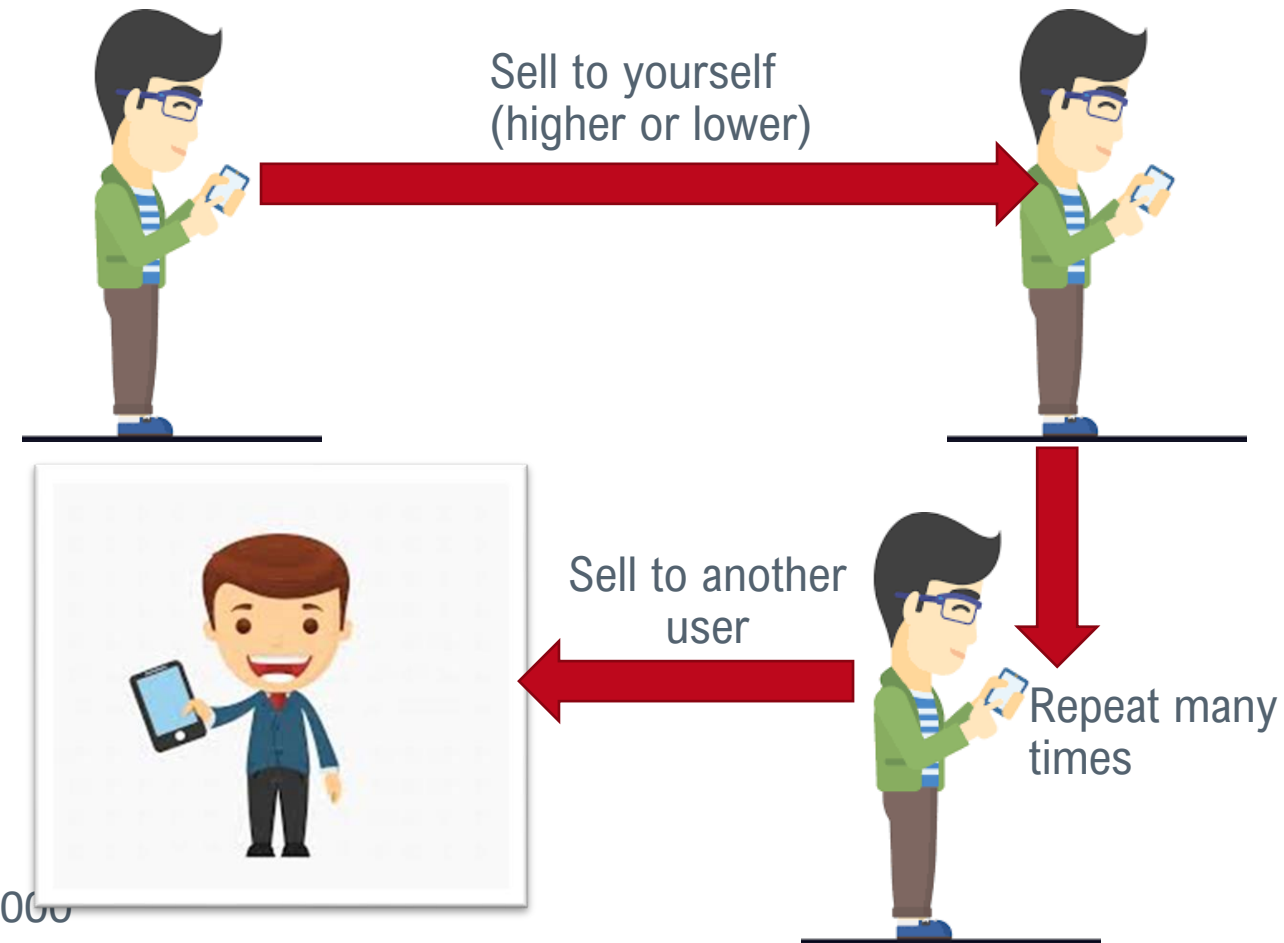
# NFT and wash trading

Example W = wallet

- NFT1 was bought for \$100 by W1
- NFT-1 is sold from W1 to W2 for \$2.500
- NFT-1 is sold from W2 to W3 for \$15.000
- NFT-1 is sold from W3 to W4 for \$50.000
- NFT-1 is sold from W4 to W5 for \$83.000
- NFT-1 is sold from W5 to W1 for \$111.500
- NFT-1 is sold from W1 to W6 for \$175,000
- NFT-1 is sold from W6 to W3 for \$250.000
- NFT-1 is sold from W3 to W7 for \$465.500
- NFT-1 is sold from W7 to W2 for \$785,000
- NFT-1 is sold from W2 to W-new buyer for \$1,000,000

Example W = wallet

NFT1 was bought for \$100 by W1



# NFT and wash trading – suggestions by Elliptic

---

## Red Flags & Warning Signs

- Wallets engaging with the transactions with each other are financed by the same wallet.
- NFTs are being sold at significantly above or below their floor or recent sale prices – often in rapid succession.
- The wallet has no sign of interaction with the community/game of the NFT they are buying/selling.
- The same wallets re-emerge in the chain of sales/transfers of the same NFT over time.
- An NFT influencer – known for their controversial involvement in different projects – abruptly withdraws support from a project.
- An NFT project is known to have disagreements within its development team.
- A celebrity promotes an NFT collection despite not being actively involved and without disclosing whether the promotion is paid.
- An NFT project with many transactions/sales that is not supported by any relevant social community.
- An NFT marketplace offering unusually high rewards.

## **5. Money laundering**

# Money Laundering

---

## Definitions:

- “Cleaning on Money”
- “Any financial transaction which generates an asset or value as the result of an illegal act”
- “is a process whereby the origin of funds generated by illegal means is concealed” *Swiss Bank*
- “the crime of moving money that has been obtained illegally through banks and other businesses to make it seem as if the money has been obtained legally” Cambridge Dictionary



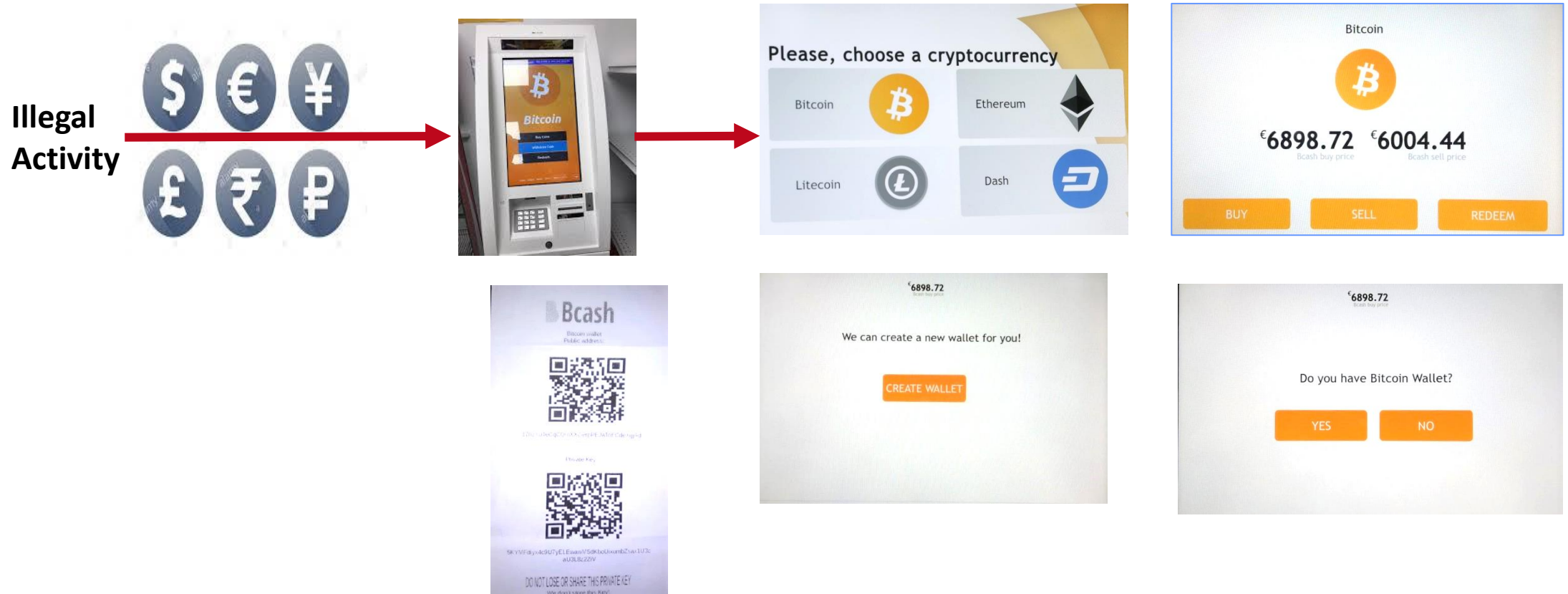


# Money Laundering

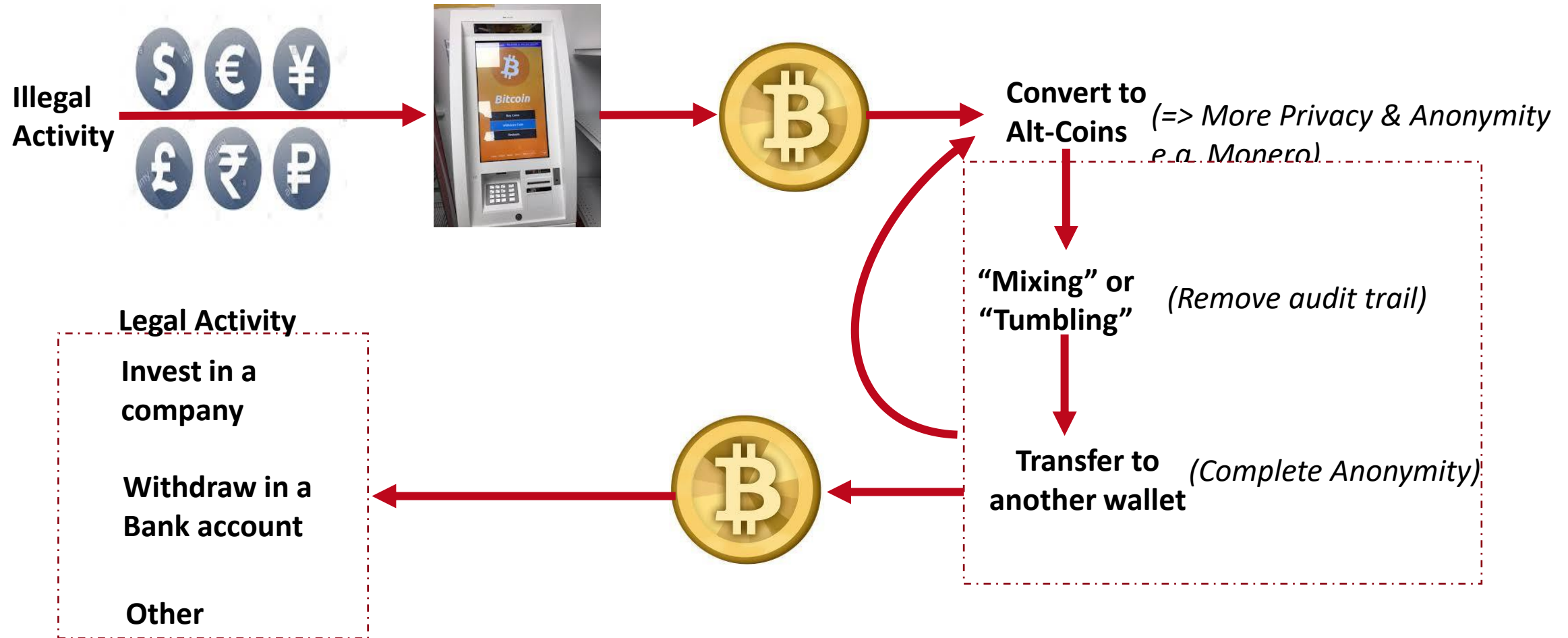
---

- Drug trafficking
  - People trafficking
  - Extortion
  - Corruption
  - Fraud
- 
- Around 80% of money laundering have an international dimension
  - Developments in ICT: Fast and easy money move around the globe
  - Digital Currencies may provide further support (e.g. anonymity)

# Money Laundering with Digital Currencies - Example



# Money Laundering with Digital Currencies - Example



# Money Laundering with Digital Currencies - Example



## CRIME

# Greece arrests Russian suspected of running \$4 billion bitcoin laundering ring

PUBLISHED WED, JUL 26 2017-11:07 AM EDT | UPDATED WED, JUL 26 2017-3:51 PM EDT

SHARE [f](#) [t](#) [in](#) [✉](#)

## KEY POINTS

- A Russian man suspected of laundering at least \$4 billion of criminal funds by switching them into the digital currency bitcoin has been arrested in Greece, police said on Wednesday.
- Police sources identified the individual as Alexander Vinnik, 38.



# Digital Currencies and Fraud

---

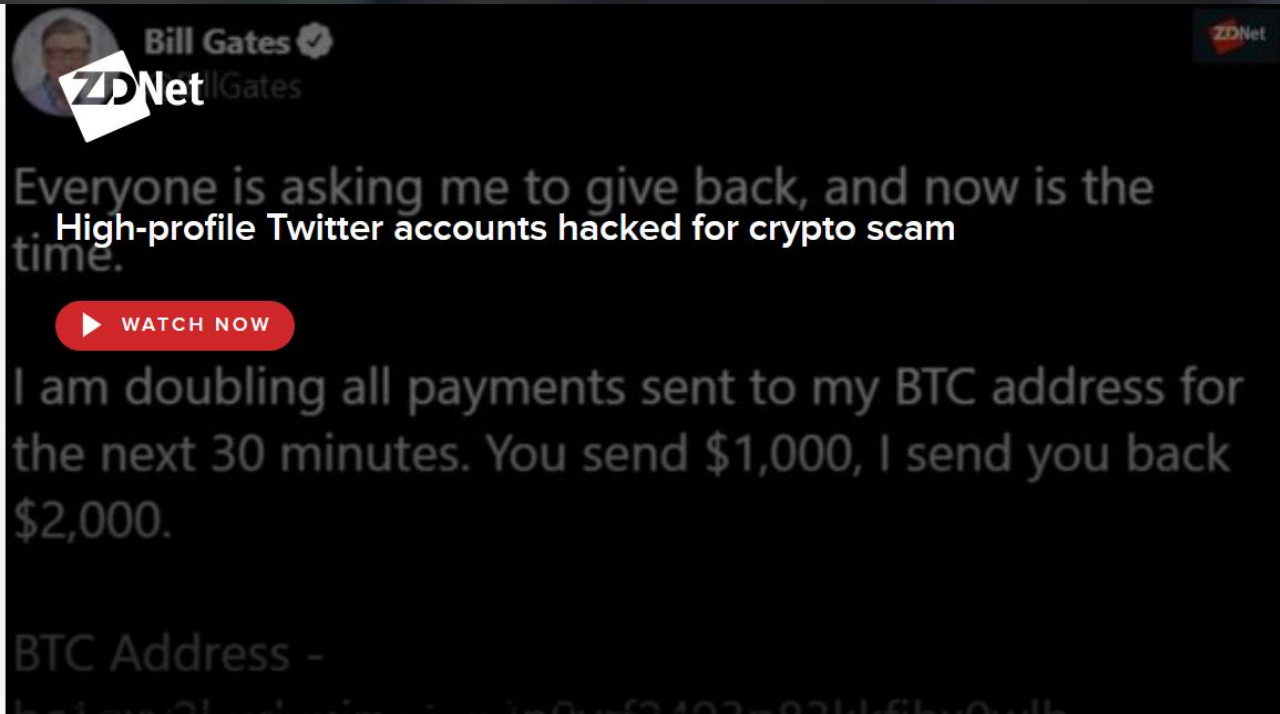
- Imposter websites
  - Fake mobile applications
  - Fake cryptocurrency exchanges
  - Ponzi Schemes
  - Fake cryptocurrencies
  - Scamming emails
  - Fake tweets or social media news
- 
- Please remember: Digital Currency transactions are permanent – we can not reverse them



MARKETS

# Cryptocurrency Scams Took in More Than \$4 Billion in 2019

Ponzi schemes are the latest form of bitcoin fraud, with big platforms like one called PlusToken drawing the most money



- In 2019 alone, cybercriminals were able to siphon away \$4.26 billion from cryptocurrency users and exchanges, according to a new report by [CipherTrace](#).
- BITPoint, a cryptocurrency exchange in Japan, suffered one of the biggest scams this year, losing \$28 million in July.
- Six people were arrested in the Netherlands and the UK over a \$27 million "typosquatting" scam, which involved making a fake website to gain access to user Bitcoin wallets.
- Binance, one of the world's largest cryptocurrency exchanges, had \$40 million of bitcoin stolen in May.

Questions?



UNIVERSITY *of* NICOSIA

## Questions?

Contact Us:

Twitter: @Themistocleous6

Instructor's Email: [themistocleous.m@unic.ac.cy](mailto:themistocleous.m@unic.ac.cy)

Course Support: [digitalcurrency@unic.ac.cy](mailto:digitalcurrency@unic.ac.cy)

IT & live session support: [dl.it@unic.ac.cy](mailto:dl.it@unic.ac.cy)