2022
PRAGUE

28 - 30 September, 2022

# WEB3 + SCAMS = IT’S A MATCH!

**Zoltán Balázs**
CUJO AI, Hungary

zoltan.balazs@cujo.com

www.virusbulletin.com

## ABSTRACT

Most cryptocurrency-related scams are unsophisticated, yet they are of paramount importance due to the damage they can cause. While researching the magical world of crypto scams, I have identified at least 35 different types. These range from cheap replicas from the 'pre-Web3' world to those that are novel and specific to Web3 and smart contracts. Pump-and-dump or rug pull scams are not unknown, but Proof of Weak Hands or NFT airdrop scams are products of the new Web3 world order.

In this presentation I will categorize the different scam types, after which I will present tips and tricks on surviving the wild, wild west of the Web3 world.

In 2022 rarely a week goes by without a stolen JPEG worth USD 100,000, yet most consumer-grade endpoint protection does not even know what a dApp looks like. Even IT security professionals don't understand or agree on what a dApp looks like, or even what Web3 is.

Warning: this research includes blockchain mumbo jumbo, but I will turn down the hype factor.

## INTRODUCTION

Blockchain technology has evolved significantly since the original white paper about Bitcoin was published in 2008 [1]. One significant improvement has been the introduction of smart contracts. But, as is the case with all new technology, 'where money is involved, scammers are involved', and blockchain attracts a lot of money and many scammers. Since I am enthusiastic about the technology around blockchains and smart contracts, it seemed natural as a security researcher that I investigate the different scam types around this technology. I identified ~35 scam types related to this topic. As many people rush to 'get rich quick' with cryptocurrency/Web3, some will fall for these scams and lose substantial amounts of money.

## WEB3 SCAMS

This presentation will walk through the different types of scams and how they work, look at some notable cases from the past, provide valuable tips and tricks for Web3 users, and some machine learning stats on Web3 scam sites.

If you are unfamiliar with Web3 terms such as WAGMI, HODL, diamond hands, or BTFD, please refer to the short glossary at the end of this paper.

The following topics are out of scope:

- Smart contract hacking
- Crypto exchange hacking
- L1-L2 gateway hacking
- Malware on the PC where the wallet is stored
- Situations where cryptocurrency is only used as a comfortable way of paying the hackers (e.g. ransomware).

In scope are the scams that average cryptocurrency and Web3 users face daily. Besides publicly known and documented scams, we will cover the first documented case of an NFT phishing kit sold as a service, which had some extra backdoor functionality.

### The NFT stealer

Although I provide a detailed methodology to categorize these scams, the presentation will focus on one specific attack, where users can lose their precious NFTs due to hard-to-decode wallet UI. In an added twist, the operator of the scam is also scammed by the scam kit developer.

The NFT stealer scam workflow is as follows:

1. Victims are lured to a lookalike website, where they are promised they can mint new NFTs for a particular collection.

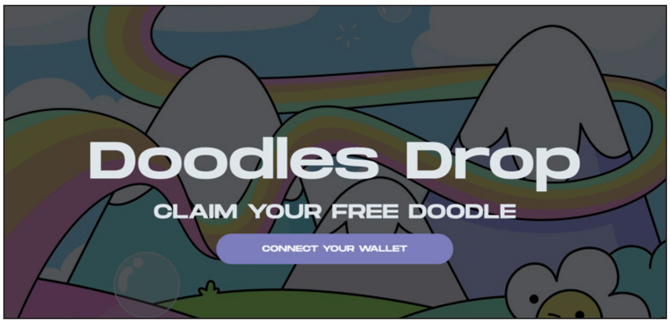
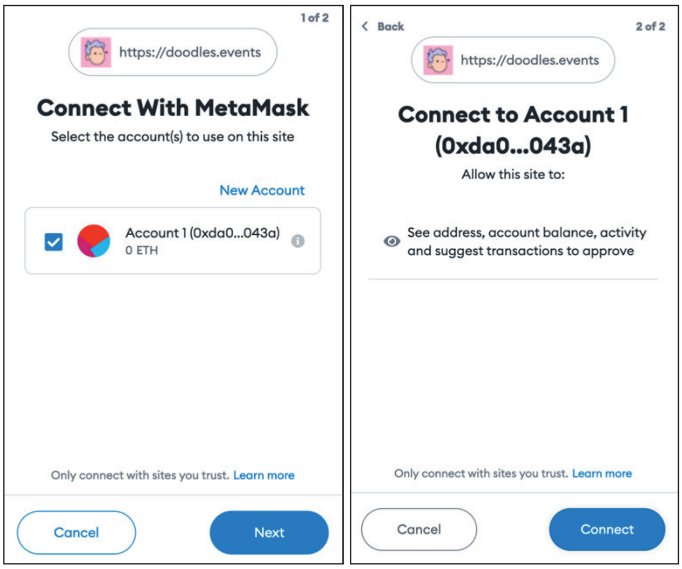


*Figure 1: Scam NFT website.*

2. The victim connects the wallet to the website. This is similar to providing the username in a login form.



1 of 2

https://doodles.events

Connect With MetaMask

Select the account(s) to use on this site

☑ Account 1 (0xda0...043a)
0 ETH

Only connect with sites you trust. Learn more

Back 2 of 2

https://doodles.events

Connect to Account 1 (0xda0...043a)

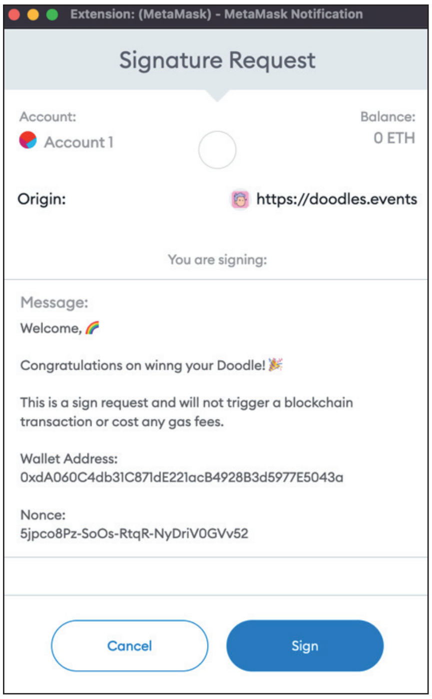
Allow this site to:

See address, account balance, activity and suggest transactions to approve

Only connect with sites you trust. Learn more

*Figure 2: Connecting MetaMask wallet to the website.*

3. Optionally, the victim signs a message. This is not a malicious action. This is similar to providing the password in a login form. It proves that the user has access to the corresponding private key.



Extension: (MetaMask) - MetaMask Notification

Signature Request

Account: Account 1

Balance: 0 ETH

Origin: https://doodles.events

You are signing:

Message:

Welcome, 🌈

Congratulations on winng your Doodle! 🎉

This is a sign request and will not trigger a blockchain transaction or cost any gas fees.

Wallet Address:
0xdA060C4db31C871dE221acB4928B3d5977E5043a

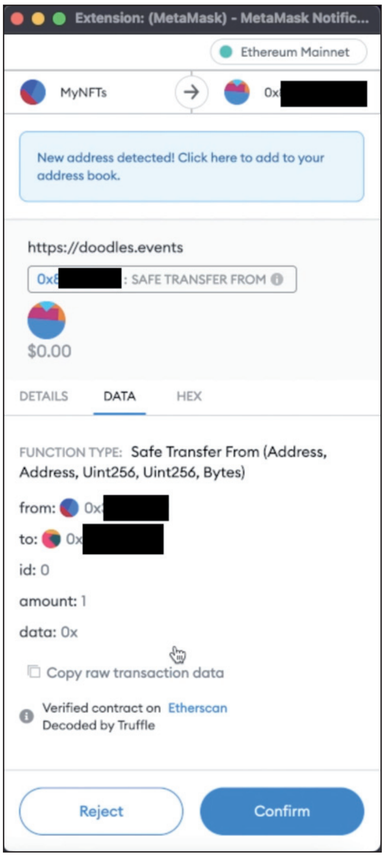
Nonce:
5jpco8Pz-SoOs-RtqR-NyDriV0GVv52

*Figure 3: Message signing.*

4. The website checks the wallet's content and searches for NFTs worth more than ~0.1 ETH. The OpenSea API is used in the background.

5. The website proposes new transactions to the victim.

6. The victim believes that, by approving these transactions, new NFTs will be minted into the wallet. Due to terrible UI, it is hard for users to decode what is going on. Users are interacting with verified, trusted smart contracts. The difference is the function called on the contract: mintApe would be the function expected to be called, but instead, safeTransferFrom is called. It is not trivial to see what happens when this function is called.



MyNFTs → 0x[redacted]

New address detected! Click here to add to your address book.

https://doodles.events

0x8[redacted] : SAFE TRANSFER FROM

$0.00

FUNCTION TYPE: Safe Transfer From (Address, Address, Uint256, Uint256, Bytes)

from: 0x[redacted]

to: 0x[redacted]

id: 0

amount: 1

data: 0x

□ Copy raw transaction data

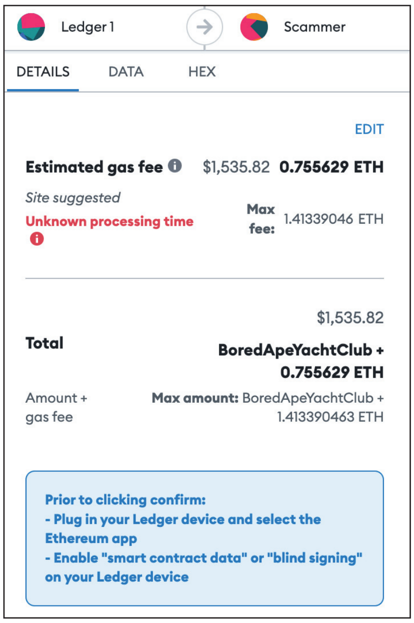
Verified contract on Etherscan
Decoded by Truffle

*Figure 4: Misleading MetaMask UI. Approving this transaction means NFTs will be lost. Users interact with legitimate, trusted contract, but calling the incorrect function.*

7. Instead, the victim approves the transfer of these NFTs to the scammer's wallet. And the victim pays the gas fees.

### *A note on hardware wallets*

This attack works even if the victim stores the private key connected to the NFT wallet in a hardware wallet. This is because the victim is tricked into 'signing' the transfer of the NFT from their wallet to the scammer's wallet. The private key never leaves the hardware wallet. Note that, for example, on the *Ledger* HW wallet, blind signing is disabled by default, and one has to enable blind signing before interacting with the smart contract via *MetaMask*. This is bad practice.



Estimated gas fee $1,535.82 **0.755629 ETH**

*Site suggested*

Unknown processing time

Max fee: 1.41339046 ETH

$1,535.82

**Total** **BoredApeYachtClub + 0.755629 ETH**

Amount + gas fee **Max amount:** BoredApeYachtClub + 1.413390463 ETH

**Prior to clicking confirm:**
**- Plug in your Ledger device and select the Ethereum app**
**- Enable "smart contract data" or "blind signing" on your Ledger device**

*Figure 5: Blind signing must be enabled.*

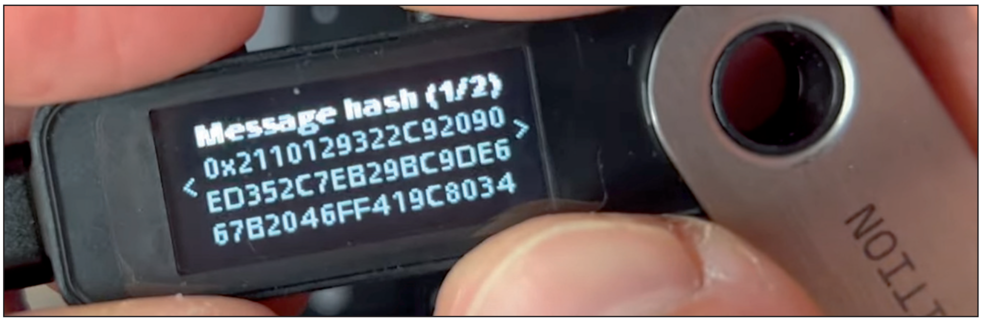
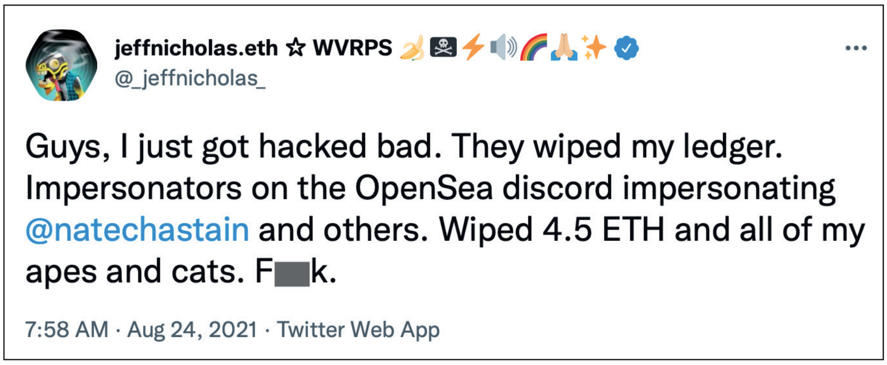


*Figure 6: 'Blind signing' in practice [2].*



jeffnicholas.eth ☆ WVRPS 🍌🏴‍☠️⚡🔊🌈🙏✨
@_jeffnicholas_

Guys, I just got hacked bad. They wiped my ledger. Impersonators on the OpenSea discord impersonating @natechastain and others. Wiped 4.5 ETH and all of my apes and cats. F[redacted]k.

7:58 AM · Aug 24, 2021 · Twitter Web App

*Figure 7: Victim who stored their private key a Ledger wallet [3].*

At the end of 2021 clear signing was introduced, where in the case of ERC-20 tokens (fungible tokens) the user sees on the HW wallet precisely what is going on. Since the beginning of 2022 this has been available for NFTs. The key takeaway here for HW wallet users is not to use *MetaMask*, but instead the official app with the HW wallet.

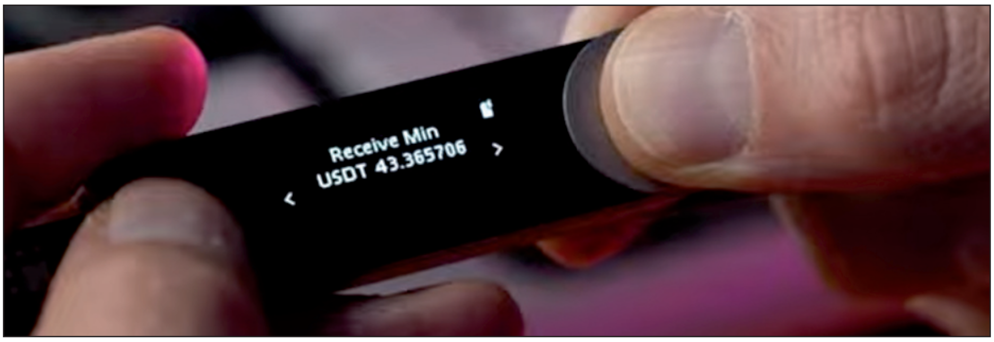
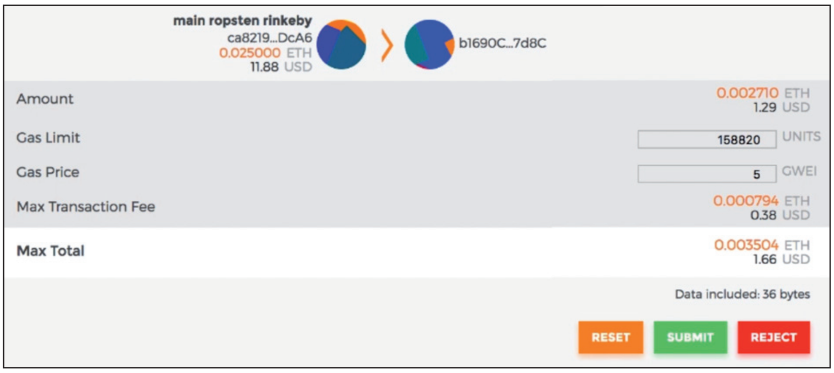


*Figure 8: 'Clear signing' ERC-20 token [4].*

Figure 9 shows how, before August 2018, *MetaMask* 'informed' users. No information was displayed regarding which function was called, what data was sent to the function, etc. Fortunately, this is a bit better now (see previous section), although still cryptic.



main ropsten rinkeby
ca8219...DcA6
0.025000 ETH
11.88 USD
b1690C...7d8C

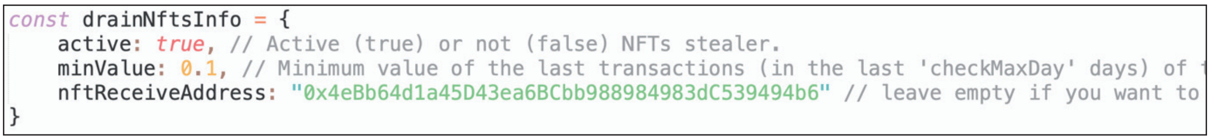
| | |
|---|---|
| Amount | 0.002710 ETH<br>1.29 USD |
| Gas Limit | 158820 UNITS |
| Gas Price | 5 GWEI |
| Max Transaction Fee | 0.000794 ETH<br>0.38 USD |
| Max Total | 0.003504 ETH<br>1.66 USD |

Data included: 36 bytes

*Figure 9: MetaMask before August 2018. True blind signing.*

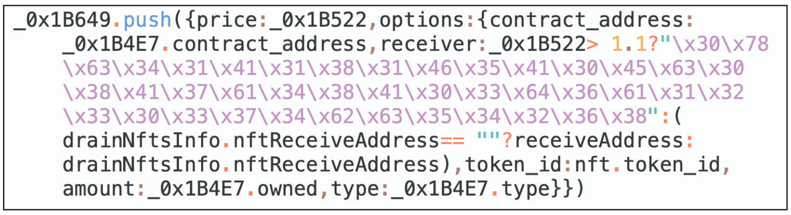
### The NFT scam kit

During my research into NFT scams I came across an NFT scam kit. It was available both free of charge on *GitHub* and on a web shop for USD 149. I contacted the seller on *Telegram* and asked what the difference was between the paid and the free version. The answer was that the paid version could steal Ethereums, not just NFTs. Part of the JavaScript code on *GitHub* was obfuscated, so I checked that part. It turned out that at least the *GitHub* version had a backdoor. The operator using this code could steal cheap NFTs, but if the price of the NFT reached a specific threshold (1 ETH in our case), the NFT was sent to the original developer of the scam kit, not to the operator.



```
const drainNftsInfo = {
    active: true, // Active (true) or not (false) NFTs stealer.
    minValue: 0.1, // Minimum value of the last transactions (in the last 'checkMaxDay' days) of t
    nftReceiveAddress: "0x4eBb64d1a45D43ea6BCbb988984983dC539494b6" // leave empty if you want to
}
```

*Figure 10: The operator of the scam believes the NFTs will be stolen to their address.*



```
_0x1B649.push({price:_0x1B522,options:{contract_address:
    _0x1B4E7.contract_address,receiver:_0x1B522> 1.1?"\x30\x78
    \x63\x34\x31\x41\x31\x38\x31\x46\x35\x41\x30\x45\x63\x30
    \x38\x41\x37\x61\x34\x38\x41\x30\x33\x64\x36\x61\x31\x32
    \x33\x30\x33\x37\x34\x62\x63\x35\x34\x32\x36\x38":(
    drainNftsInfo.nftReceiveAddress== ""?receiveAddress:
    drainNftsInfo.nftReceiveAddress),token_id:nft.token_id,
    amount:_0x1B4E7.owned,type:_0x1B4E7.type}})
```

*Figure 11: The more valuable NFTs will go to the developer of the scam kit.*

## METHODOLOGY

The scams are categorized according to the targets of the attack:

- Cryptocurrency
- Fungible tokens
- Non-fungible tokens
- Software wallets
- Hardware wallets

And the source of the attack:

- Email
- Twitter
- Discord
- Reddit
- Ads
- Hacked socials
- Airdrop

### Cryptocurrency

- Covert pre-mine:

  Before a cryptocurrency is launched to the public, most cryptocurrencies are already mined and controlled by the founding team – e.g. Ripple from 2012 [5].

- Fake crypto exchange:

  Users register to fake crypto exchanges. They send the money, it looks like they have bought cryptocurrency, but they can never withdraw the funds.

- Legit 'for a while' crypto exchange, a.k.a exit scam:

  The cryptocurrency exchange works perfectly, but the team disappears once it is big enough and funds are lost – e.g. the USD 3.6 billion Africrypt scam [6].

- Fake cryptocurrency wallet – PC:

  When the wallet software is downloaded from a non-official website the software might be backdoored, and the secret keys of the wallets are sent to the criminals.

- Fake cryptocurrency wallet – mobile:

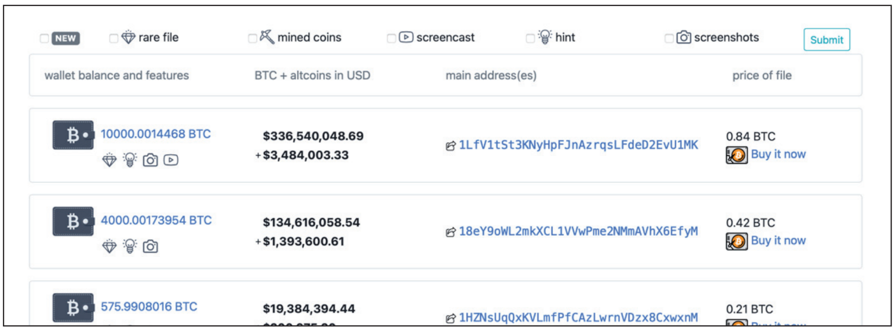
  This is similar to the fake crypto exchange scam, but instead the users have a fake mobile wallet, and they can never withdraw the cryptocurrencies stored in the fake wallet.

- Cloud-mining scam:

  Users are promised that they will pay for 'cloud mining' and will get money back for their investment. But they don't.

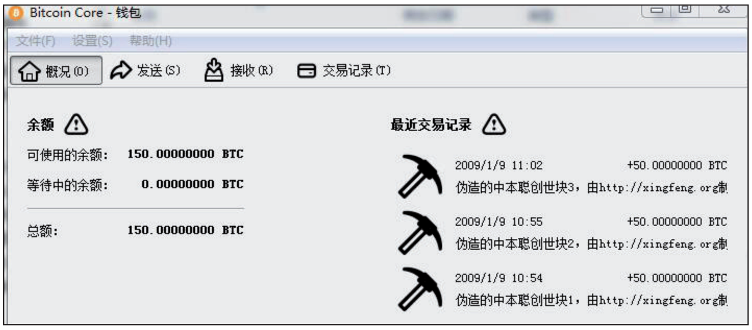
- Buy fake wallet.dat:

  Users can buy packs of wallet.dat files with the promise to hold a substantial amount of Bitcoins. The headers of the wallet files are faked to show these wallets are attractive, but they don't have the correct secret keys and thus are worthless. For reference [7, 8, 9].



| wallet balance and features | BTC + altcoins in USD | main address(es) | price of file |
|---|---|---|---|
| 10000.0014468 BTC | $336,540,048.69<br>+$3,484,003.33 | 1LfV1tSt3KNyHpFJnAzrqsLFdeD2EvU1MK | 0.84 BTC<br>Buy it now |
| 4000.00173954 BTC | $134,616,058.54<br>+$1,393,600.61 | 18eY9oWL2mkXCL1VVwPme2NMmAVhX6EfyM | 0.42 BTC<br>Buy it now |
| 575.9908016 BTC | $19,384,394.44 | 1HZNsUqQxKVLmfPfCAzLwrnVDzx8CxwxnM | 0.21 BTC |

*Figure 12: Legitimate website selling wallet.dat files.*



余额

可使用的余额: 150.00000000 BTC

等待中的余额: 0.00000000 BTC

总额: 150.00000000 BTC

最近交易记录

2009/1/9 11:02 +50.00000000 BTC
伪造的中本聪创世块3，由http://xingfeng.org制

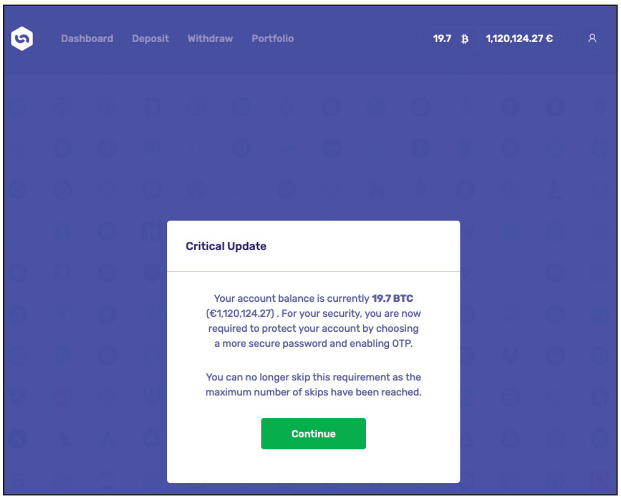
2009/1/9 10:55 +50.00000000 BTC
伪造的中本聪创世块2，由http://xingfeng.org制

2009/1/9 10:54 +50.00000000 BTC
伪造的中本聪创世块1，由http://xingfeng.org制

*Figure 13: Fake wallet.dat file, missing private key.*

- Advance fee fraud:

  Usually, the scam arrives in the form of mail spam. Users are provided with a username, password and URL. After logging in, or even setting up MFA, the user is informed they have cryptocurrency in the wallet. But when the user tries to withdraw the money they are told that, first, they need to send some cryptocurrency to the platform before they can withdraw the rest. If someone pays this advanced fee, they will not be able to withdraw the rest. When this scam was running, it asked for an equivalent of USD 1,400 in BTC [10].



Critical Update

Your account balance is currently **19.7 BTC** (€1,120,124.27) . For your security, you are now required to protect your account by choosing a more secure password and enabling OTP.

You can no longer skip this requirement as the maximum number of skips have been reached.

*Figure 14: Registration form for an advance fee scam.*

### Fungible tokens

- Proof of Weak Hands:

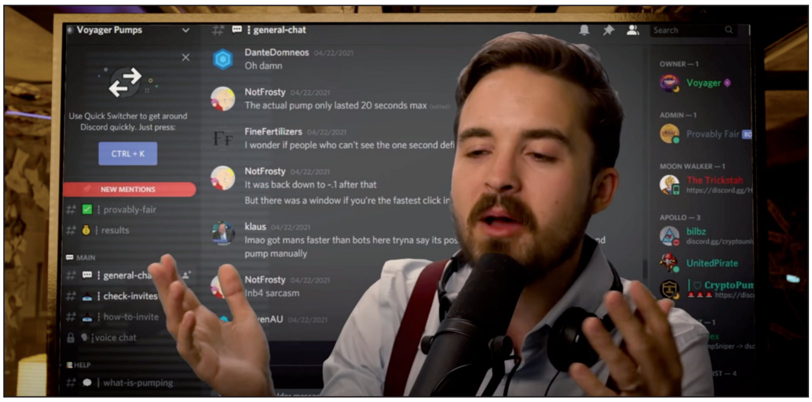
  This smart contract is practically a scam that lives on the blockchain forever. The catch is that 10% of all purchases and sales go back to the token holders. Thus people are incentivized to HODL forever and are paid by the newcomers. This is the definition of a Ponzi scheme. It is hard to estimate how much cryptocurrency was lost during these scams, as many similar projects were (are) running. But due to an integer overflow in the poorly coded smart contract, an attacker was able to withdraw 866 ETH from one of these contracts. This is an example of when a hacker steals from a scammer [11].

- Pump and dump token:

  The scammers first find a token (or sometimes even a cryptocurrency) where daily volume and total market capitalization is low. They slowly buy a substantial amount of these assets. Then they start to promote these as the 'next big thing', and as soon as the price surges they sell their assets at the inflated price. This is similar to 'penny stocks' from the movie *The Wolf of Wall Street*. As pump and dump has been a regular daily activity for some scammers, it is hard to estimate the damages caused by these scams.

- Get involved in pump and dump:

  This is similar to the previous scam, except here the victims know they are involved in a pump-and-dump scheme but believe others will be the victims. But that's not the case – they are the ones losing the money.



DanteDomneos 04/22/2021
Oh damn

NotFrosty 04/22/2021
The actual pump only lasted 20 seconds max (edited)

FineFertilizers 04/22/2021
I wonder if people who can't see the one second defi

NotFrosty 04/22/2021
It was back down to -.1 after that
But there was a window if you're the fastest click in

klaus 04/22/2021
lmao got mans faster than bots here tryna say its pos
pump manually

NotFrosty 04/22/2021
lnb4 sarcasm

enAU 04/22/2021

*Figure 15: You just can't be fast enough. Reference: [12].*

- Rug pull token:

  A new ERC-20 token is created, with some smokes and mirrors, maybe a roadmap, and some charity involved. Then people with lots of followers on social media are paid (either in hard money or in tokens) to promote the token. Once the prices are high enough, the founders and celebs cash out, the price drops, and the project is abandoned. Famous examples involve Safemoon [13], Squid Game [14], Save the Kids [15].

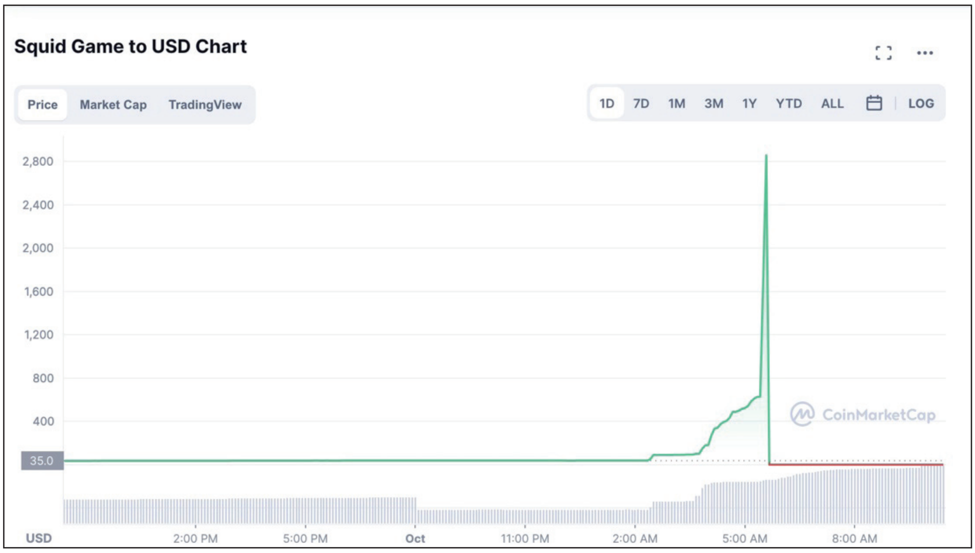


*Figure 16: Typical rug pull chart.*

- Giveaway scam:

  Wealthy people, such as Elon Musk, are impersonated. It is promised that the famous person will give away their fortune – but you have to send some cryptocurrency to the wallet first because of 'reasons'. This scam is typical of *Twitter*, where one scam involved USD 580,000 [16]. This trick is not popular nowadays.

  Also when *Twitter* was hacked through internal tools, attackers used this access for a fake giveaway scam and cashed in ~USD 105,000 [17].

- Hack the ICO website:

  An initial coin offering (ICO) is similar to an IPO. People rush to buy the 'next big thing'. If attackers can hack the website minutes before the ICO starts, they can replace the wallet address, and the victims will send the funds to the hacker's address. For example, the Coindash ICO hacker stole USD 6.4 million [17].

- Typosquat / homograph attacks:

  This scam is not specific to cryptocurrencies, but there are documented cases where lookalike domain names are registered, involving special lookalike 'homograph' characters.

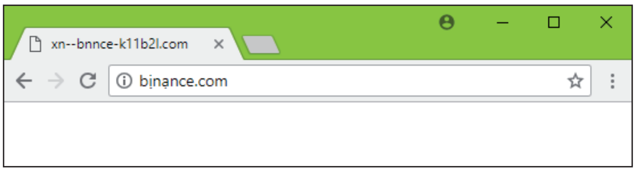


*Figure 17: Homograph domain for binance.com. Source: Bleeping Computer.*

- Buy token IRL, get fake ones:

  This scam typically involves a meeting in person, where cash is transferred to the scammers while the scammers provide fake tokens to the victim. For example, in Budapest scammers sold fake tokens for ~USD 82,000.

- Airdrop scam:

  See NFT section.

### Non-fungible tokens (NFT)

- NFT – market manipulation:

  Determining the value of an NFT is more challenging than determining the value of a piece of art, especially when people sell the NFTs to themselves for an inflated price then fool others that the last sale price of an NFT reflects its actual value. Sometimes these transactions involve flash loans, where the owner of the NFT does not even have to have the funds to carry out this transaction. But they should pay the fee as a percentage to the creator. An example is Cryptopunk #9998, which sold for USD 532 million [19].

- NFT – rug pull:

  For NFTs, rug pull is the most common scam technique: create 'hype and vibes', promise a vibrant community and milestones, sell the NFTs, and abandon the project. Famous examples include #rugpullmafia and Lana Rhoades' CryptoSis. An estimated USD 1.5 million was scammed out of the 'NFT investors' [20].

*Figure 18: CryptoSis NFT project rug pulled.*

- Buy a fake KYC-d wallet:

  When Bored Ape Yacht Club announced that people could buy land on the 'Otherside metaverse', people had to KYC (Know Your Customer) to get whitelisted. So there was demand ... and supply for KYCd wallets. Once you buy a wallet.dat file from someone, the other party still has access to the wallet and can drain anything from the wallet. Cryptocurrencies cannot be 'double-spend', but wallets with private keys can be copied.

- Insider trading/knowledge with airdrop:

  When someone knows which wallets are selected for airdrop before the whitelist happens, more wallets can be generated which are eligible for the airdrop. This happened with the Ribbon tokens airdrop, for example.
  USD 2.5 million is expected to be gained from this.

- Highly targeted phishing:

  Some phishing is more sophisticated than others. There are documented cases where the scammers played nice for weeks, even worked for a company, to gain the trust of a company founder before luring the victim into the scam. An example was reported by thomasg.eth in a thread on *Twitter* – luckily, there was no real loss in this case [21].

- Counterfeit NFT:

  Scammers copy the design of another popular NFT, start their own, and sell the counterfeit ones. Funny examples involve 'Slightly Tilted Bored Apes' and 'Mirrored Bored Apes' [22].

- NFT fake minting:

  A fake website promises users that they can mint a new NFT for some ETH/SOL. After the user pays, they don't get any NFTs. Sometimes they even lose their precious NFTs on the go (see the next scam for details). If only the fake mint element is involved, the damages are usually not too high.

- NFT scam site stealing NFTs:

  In my opinion this scam is the number 1 issue in the NFT space today. Due to the poor UI of wallet software, victims do not know what they are approving (see 'blind signing' in previous sections). People believe they are buying an NFT or trading it (swap sites). Meanwhile, the NFT is transferred to the scammer. Famous examples include the BAYC Otherside sale and the OpenSea phishing. For details see the NFT scam kit description above.

  - OpenSea phishing, USD 1.7 million or 200 million [23].
  - BAYC *Instagram* hack, USD 2.4 - 13.7 million [24].
  - Blind signing explained: [25].

- NFT airdrop scam:

  This is similar to the previous one, but first the victim receives a new NFT as an airdrop. Next, the victim checks the website for this NFT and tries to sell it. From this point, the workflow is the same as previously described.

### Software wallet

- Seed phrase phishing:

  A typical scam involves luring the user to a fake website where, in order to proceed, the user has to provide the seed phrase of the crypto wallet. The scam is hard to detect in some cases – for example, when scammers mimic the UI of *MetaMask*. It is easy for trained users to get confused about whether the user is interacting with the wallet software or with the website.

- Screen sharing while *MetaMask* is open:

  Calvin Beccera: 'All three of these @BoredApeYC were hacked tonight over discord. Guys posing as buyers in discord were helping me troubleshoot a problem we thought was happening. They walked me through language settings in my MetaMask and had me chose an option and took everything.' [26]

- *iCloud* backup – call from *Apple*:

  When wallet software is installed on *iOS*, the *iCloud* backup includes the wallet's secret key. Attackers have to take over the *iCloud* account (steal the password, bypass MFA), and last but not least, crack the *MetaMask* password. An example includes a loss of USD 650,000 [27].

### HW wallet

- HW wallet backup phrase phishing:

  Like SW wallets, scammers try to convince users to reveal their secret backup phrase to their HW wallets.

  Some people are lured into updating their HW wallet firmware from non-legitimate sites. The attack does not involve the firmware update itself due to digitally signed firmware updates. Instead, it asks for the passphrase.

- HW wallet with pre-generated secret key:

  This hack was made possible because the customer list for the *Ledger* HW wallet was leaked. Once attackers knew customer names and addresses, they sent legitimate HW wallets to these people. But, contrary to best practice, the HW wallets were already set up, and the backup phrase was printed. The scammers already had the backup phrase and waited for victims to send funds to these wallets.

- Modified HW wallet:

  This attack is probably the most sophisticated. Instead of pre-setup HW wallets, the HW wallet had some 'extra hardware' to steal the crypto assets on the device [28].

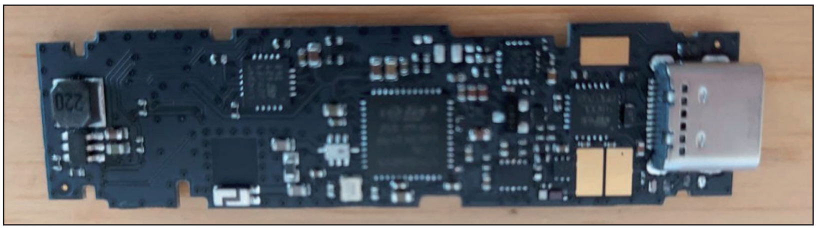
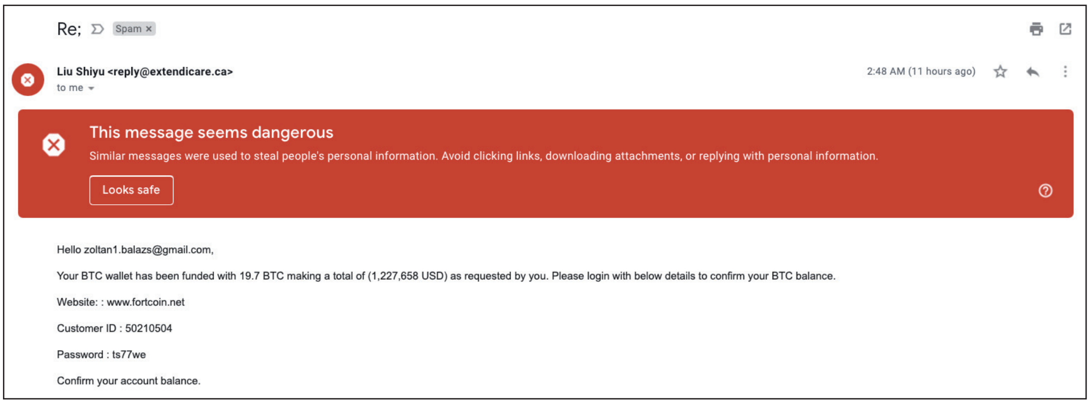


*Figure 19: Modified Ledger wallet.*

## Source of the attack

The following screenshots are some examples of the different sources from which scams can come. The scams themselves are not explained here, as they have already been discussed previously.

- Email spam



Liu Shiyu <reply@extendicare.ca>
to me

2:48 AM (11 hours ago)

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Hello zoltan1.balazs@gmail.com,

Your BTC wallet has been funded with 19.7 BTC making a total of (1,227,658 USD) as requested by you. Please login with below details to confirm your BTC balance.

Website: : www.fortcoin.net

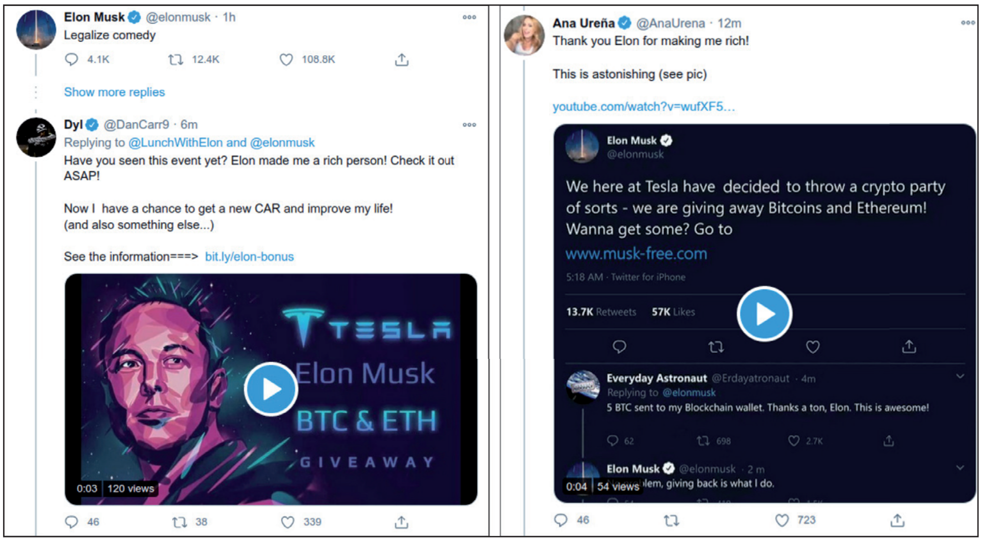
Customer ID : 50210504

Password : ts77we

Confirm your account balance.

*Figure 20: Advance fee fraud coming from email spam.*

- Twitter



Elon Musk @elonmusk · 1h
Legalize comedy

Dyl @DanCarr9 · 6m
Replying to @LunchWithElon and @elonmusk
Have you seen this event yet? Elon made me a rich person! Check it out ASAP!

Now I have a chance to get a new CAR and improve my life!
(and also something else...)

See the information===> bit.ly/elon-bonus

Ana Ureña @AnaUrena · 12m
Thank you Elon for making me rich!

This is astonishing (see pic)

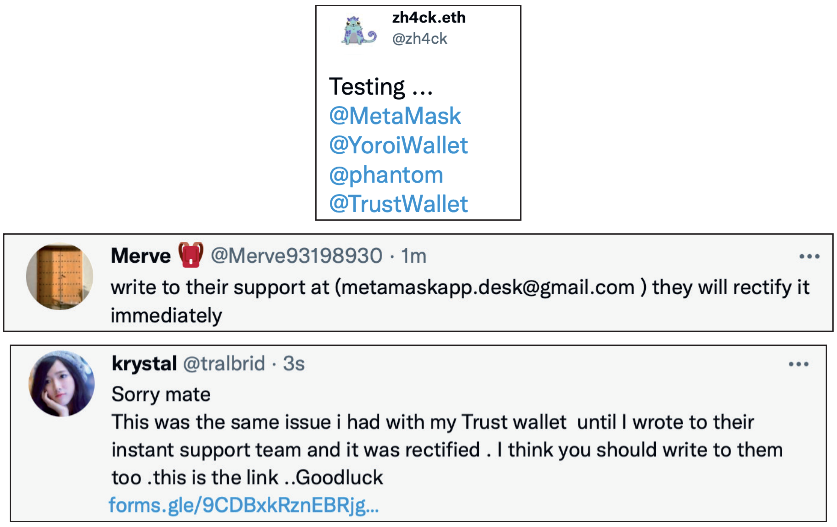
youtube.com/watch?v=wufXF5...

Elon Musk @elonmusk
We here at Tesla have decided to throw a crypto party of sorts - we are giving away Bitcoins and Ethereum! Wanna get some? Go to www.musk-free.com
5:18 AM · Twitter for iPhone

Everyday Astronaut @Erdayatronaut · 4m
Replying to @elonmusk
5 BTC sent to my Blockchain wallet. Thanks a ton, Elon. This is awesome!

Elon Musk @elonmusk · 2 m
lem, giving back is what I do.

*Figure 21: Typical Twitter giveaway scam. Source: Bleeping Computer.*



zh4ck.eth
@zh4ck

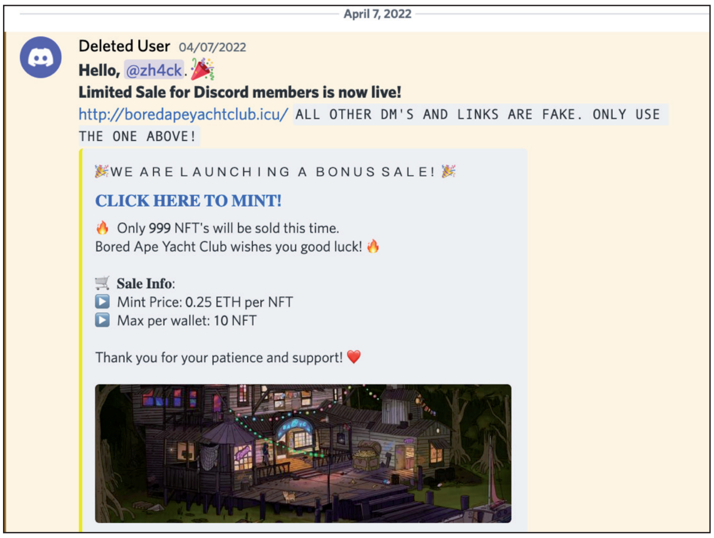
Testing ...
@MetaMask
@YoroiWallet
@phantom
@TrustWallet

**Merve** @Merve93198930 · 1m
write to their support at (metamaskapp.desk@gmail.com ) they will rectify it immediately

**krystal** @tralbrid · 3s
Sorry mate
This was the same issue i had with my Trust wallet until I wrote to their instant support team and it was rectified . I think you should write to them too .this is the link ..Goodluck
forms.gle/9CDBxkRznEBRjg...

*Figure 22: Typical Twitter support scam.*

- Discord



April 7, 2022

Deleted User 04/07/2022
**Hello,** @zh4ck. 🎉
**Limited Sale for Discord members is now live!**
http://boredapeyachtclub.icu/ `ALL OTHER DM'S AND LINKS ARE FAKE. ONLY USE THE ONE ABOVE!`

🎉WE ARE LAUNCHING A BONUS SALE! 🎉

**CLICK HERE TO MINT!**

🔥 Only 999 NFT's will be sold this time.
Bored Ape Yacht Club wishes you good luck! 🔥

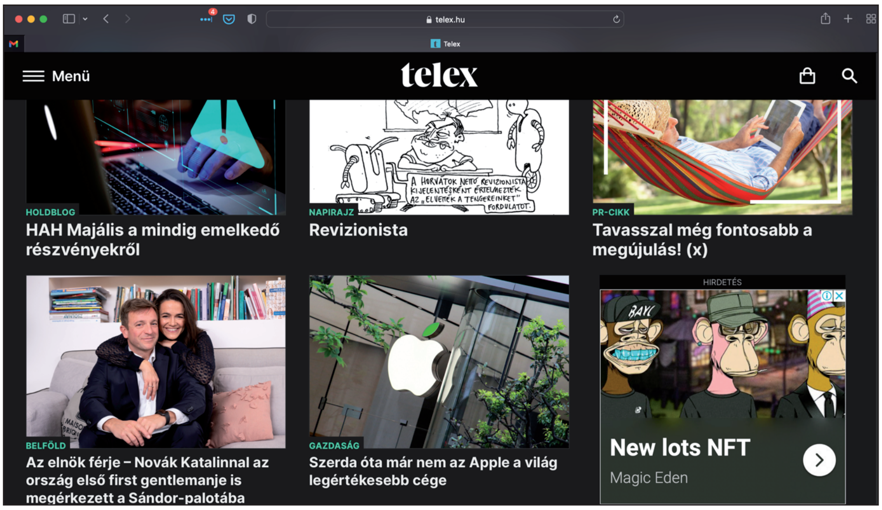
🛒 **Sale Info**:
▶ Mint Price: 0.25 ETH per NFT
▶ Max per wallet: 10 NFT

Thank you for your patience and support! ❤️

*Figure 23: Typical Discord scam message.*

One interesting *Discord* account takeover hack attack vector is the use of bookmarklets. For more details on this see [29].

- Ads



HAH Majális a mindig emelkedő részvényekről

Revizionista

Tavasszal még fontosabb a megújulás! (x)

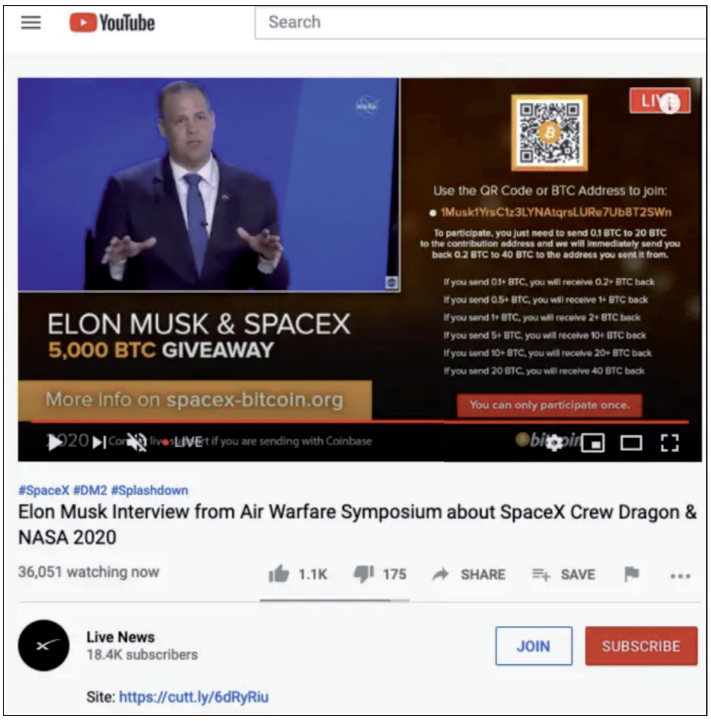
Az elnök férje – Novák Katalinnal az ország első first gentlemanje is megérkezett a Sándor-palotába

Szerda óta már nem az Apple a világ legértékesebb cége

New lots NFT
Magic Eden

*Figure 24: Ad leading to scam site.*

- Hacked social sites (*YouTube* channel, *Twitter* verified accounts, *Twitter* fake support, official *Instagram*, official *Discord*)



Use the QR Code or BTC Address to join:

1Musk1YrsC1z3LYNAtqrsLURe7Ub8T2SWn

To participate, you just need to send 0.1 BTC to 20 BTC to the contribution address and we will immediately send you back 0.2 BTC to 40 BTC to the address you sent it from.

If you send 0.1+ BTC, you will receive 0.2+ BTC back
If you send 0.5+ BTC, you will receive 1+ BTC back
If you send 1+ BTC, you will receive 2+ BTC back
If you send 5+ BTC, you will receive 10+ BTC back
If you send 10+ BTC, you will receive 20+ BTC back
If you send 20 BTC, you will receive 40 BTC back

You can only participate once.

ELON MUSK & SPACEX
5,000 BTC GIVEAWAY

More info on spacex-bitcoin.org

#SpaceX #DM2 #Splashdown

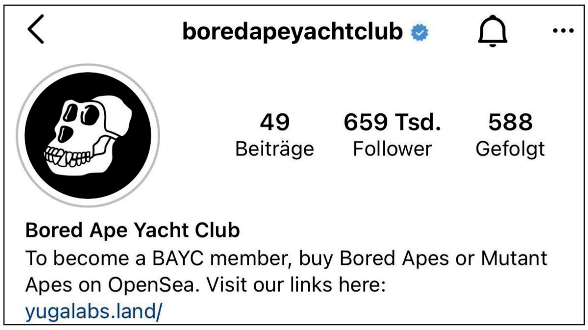
Elon Musk Interview from Air Warfare Symposium about SpaceX Crew Dragon & NASA 2020

36,051 watching now

Live News
18.4K subscribers

Site: https://cutt.ly/6dRyRiu

*Figure 25: Hacked YouTube channel promoting giveaway scam. Source [30].*

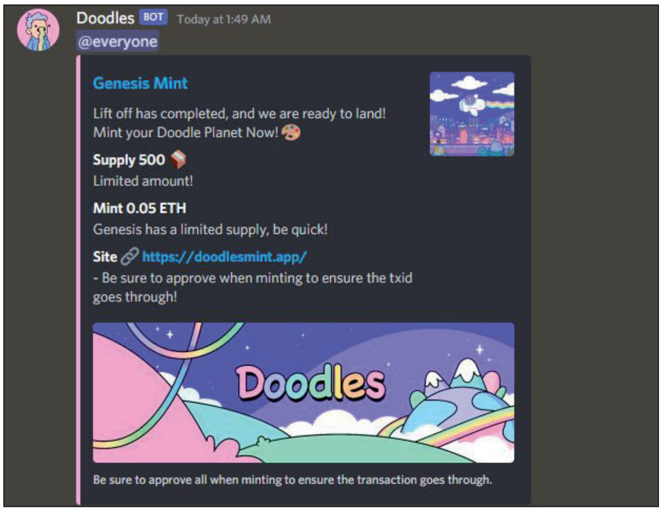


boredapeyachtclub

| 49 | 659 Tsd. | 588 |
|---|---|---|
| Beiträge | Follower | Gefolgt |

Bored Ape Yacht Club
To become a BAYC member, buy Bored Apes or Mutant Apes on OpenSea. Visit our links here:
yugalabs.land/

*Figure 26: Official BAYC Instagram account hacked [31].*



Doodles BOT Today at 1:49 AM
@everyone

**Genesis Mint**

Lift off has completed, and we are ready to land!
Mint your Doodle Planet Now! 🎨

**Supply 500** 💎
Limited amount!

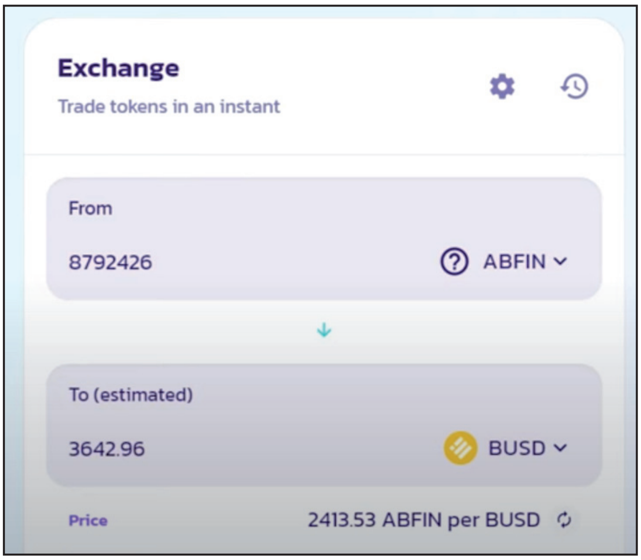
**Mint 0.05 ETH**
Genesis has a limited supply, be quick!

**Site** 🔗 https://doodlesmint.app/
- Be sure to approve when minting to ensure the txid goes through!

Be sure to approve all when minting to ensure the transaction goes through.

*Figure 27: Doodles Discord account hacked [32].*

- Airdrop



Exchange

Trade tokens in an instant

From

8792426 ABFIN

To (estimated)

3642.96 BUSD

Price 2413.53 ABFIN per BUSD

*Figure 28: Fake token airdropped into a wallet [33].*

## CONCLUSION

The Web3 itself is still in a beta phase, and multiple risks are involved for end-users. I identified the following main root problems based on this research:

- Complex and new technology
- Hard to understand, and even misleading UI (what am I signing here?)
- In-band signalling (e.g. is this the extension or the website?)
- 'Get rich quick'

## GLOSSARY

**Blockchain**: A database. A modern, distributed database. It is optimized for security. Thus it is slow and expensive. And it is append-only.

**Smart contracts**: Program code stored on the blockchain. When someone wants to run this code, all computers connected to the blockchain execute the same program code and agree on the output. Secure. Slow and expensive.

**ERC-20 tokens, Fungible Tokens**: 'Fungible' means that if you have one token and I have one token, they have the same value and there should be no difference between these. ERC-20 defines the standard of what the smart contract looks like, what functions it implements.

**ERC-721, ERC-1115, NFT, Non Fungible Tokens**: Unique piece of data which is stored on the blockchain. Usually, it is a pointer to an URL. Sometimes it is stored on a peer-to-peer network where the integrity of the token can be proved. ERC-721 is the old standard and ERC-1115 is the new standard on how to implement these smart contracts.

**NFT minting**: Paying some mint price to reveal the 'content' of an NFT. Like opening a *Kinder Surprise*. It might be fun, might be less fun.

**Wallet**: A safe storage for crypto-assets. Think of it as a bank account number but in your pocket, so be sure not to lose it. *MetaMask* (mentioned in the article) is a popular software wallet.

**Gas fee**: You have to pay this fee for transactions on the blockchain. You usually pay with ETH, short for Ethereum, the second-largest cryptocurrency.

**Web3**: Websites where users can interact with smart contracts through their wallet software. Their wallet address is their identity.

**Whitelist:** The crypto-bro world was not notified that using whitelist is not PC anymore. They use it to get a list of wallets allowed to mint a new NFT.

**WAGMI:** We All Gonna Make It [34].

**HODL:** Investment strategy for cryptocurrencies. Only buy, never sell. Mistyped form of hold [35].

**Diamond hands**: Similar to HODL. No matter how hard the market crashes, you don’t sell. Those who sell are paper hands.

**BTFD**: Buy The F*in Dip. If an asset crashes, buy it while it is low instead of panic selling like a paper hand [36].

**Moon**: ‘The promise’ that line goes up, chart prices are going to the moon. The cryptocurrency investment world is generally bullish.

## REFERENCES

[1] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. October 2008. https://bitcoin.org/bitcoin.pdf.

[2] DevMonkey. Ledger Nano S Plus Unboxing & Setup (sending NFTs and crypto). https://www.youtube.com/watch?v=N-3pUl52aWk.

[3] https://twitter.com/_jeffnicholas_/status/1430046727843717125.

[4] Ledger. Blind signing: the crypto vulnerability you should be aware of | School of Block. https://www.youtube.com/watch?v=iCwOyK2Ewdo.

[5] US Securities and Exchange Commission. SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering. December 2020. https://www.sec.gov/news/press-release/2020-338.

[6] Henderson, R.; Prinsloo, L. South African Brothers Vanish, and So Does $3.6 Billion in Bitcoin. Bloomberg. June 2021. https://www.bloomberg.com/news/articles/2021-06-23/s-african-brothers-vanish-and-so-does-3-6-billion-in-bitcoin.

[7] https://bitcointalk.org/index.php?topic=5315310.0.

[8] http://xingfeng.org/?p=517.

[9] https://allprivatekeys.com/10000btc.

[10] Canali, D.; Giering, C.; Kromphardt, T.; Scholten, S. Advance Fee Fraud: The Emergence of Elaborate Crypto Schemes. Proofpoint. September 2021. https://www.proofpoint.com/us/blog/threat-insight/advance-fee-fraud-emergence-elaborate-crypto-schemes.

[11] bitburner. Proof of Weak Hands (PoWH) Coin hacked, 866 eth stolen . Steemit. 2018. https://steemit.com/cryptocurrency/@bitburner/proof-of-weak-hands-powh-coin-hacked-866-eth-stolen.

[12] Coffeezilla. I Joined a Pump and Dump Scheme So You Don’t Have To. https://www.youtube.com/watch?v=ehDvr5vVGPg.

[13] Ferlin, J. The Truth About the SafeMoon Rug Pull. The Coin Times. February 2022. https://thecointimes.net/the-truth-about-the-safemoon-rug-pull/.

[14] Cheng, A. ‘Squid Game’-inspired cryptocurrency that soared by 23 million percent now worthless after apparent scam. The Washington Post. November 2021. https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/.

[15] Protos. Esports influencer fired for pumping and dumping ‘Save The Kids’ crypto. July 2021. https://protos.com/save-the-kids-faze-clan-kay-coffeezilla-proves-rug-pulls/.

[16] Abrams, L. Verified Twitter accounts hacked in $580k ‘Elon Musk’ crypto scam. Bleeping Computer. January 2021. https://www.bleepingcomputer.com/news/security/verified-twitter-accounts-hacked-in-580k-elon-musk-crypto-scam/.

[17] Arghire, I. Hackers Used Internal Twitter Tools to Hijack High-Profile Accounts. Security Week. July 2020. https://www.securityweek.com/hackers-used-internal-twitter-tools-hijack-high-profile-accounts.

[18] Wieczner, J. Hackers Just Stole $7 Million in a Brazen Ethereum Cryptocurrency Heist. Fortune. July 2017. https://fortune.com/2017/07/18/ethereum-coindash-ico-hack/.

[19] MRAMOR. NFT CryptoPunk owner sold it to himself for $ 532 million in Ethereum. Medium. October 2021. https://medium.com/@Mramor/nft-cryptopunk-owner-sold-it-to-himself-for-532-million-in-ethereum-b82ac3dfdefc.

[20] Irwin, K. Lana Rhoades Deletes Twitter Account After Allegedly ‘Rug Pulling’ Her NFT Project. Decrypt. February 2022. https://decrypt.co/93847/lana-rhoades-deletes-twitter-account-allegedly-rug-pulling-nft-project.

[21] https://twitter.com/thomasg_eth/thread/1492663192404779013.

[22] Redman, J. 2 Mirrored, Copycat Bored Ape NFT Projects Cause Copyright Infringement Controversy. Bitcoin.com. January 2022. https://news.bitcoin.com/2-mirrored-copycat-bored-ape-nft-projects-cause-copyright-infringement-controversy/.

[23] Deka, L. OpenSea is examining the phishing attack after labeling $200M loss to be 'False Rumors'. Tron Weekly. February 2022. https://www.tronweekly.com/opensea-phishing-attack-rumors-200m-loss/.

[24] Greig, J. Bored Ape Yacht Club says its Instagram was hacked to funnel users to NFT phishing sites. The Record. April 2022. https://therecord.media/bored-ape-yacht-club-says-instagram-hacked-nfts-stolen/.

[25] Ledger. Crypto's Greatest Weakness? Blind Signing, Explained. September 2021. https://www.ledger.com/academy/cryptos-greatest-weakness-blind-signing-explained.

[26] https://twitter.com/calvinbecerra/status/1454328591202721796.

[27] Van Boom, D. How an Apple iCloud Exploit Lost a Crypto Trader Over $650K. CNet. April 2022. https://www.cnet.com/personal-finance/crypto/how-an-apple-icloud-exploit-lost-a-crypto-trader-over-650k/#ftag=CAD590a51e.

[28] Abrams, L. Criminals are mailing altered Ledger devices to steal cryptocurrency. Bleeping Computer. June 2021. https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency/.

[29] https://twitter.com/Serpent/status/1485002655953211392.

[30] Holmes, A. Big YouTube accounts are being plagued by hackers promoting Bitcoin scams resembling the hack that compromised Twitter. Business Insider. August 2020. https://www.businessinsider.com/youtube-channels-bitcoin-scammers-twitter-hack-2020-8.

[31] https://twitter.com/zachxbt/status/1518609171796611072.

[32] https://twitter.com/zachxbt/status/1509770759006306305.

[33] https://medium.com/metamask/phisher-watch-airdrop-scams-82eea95d9b2a.

[34] Axie Sisters 'WAGMI' Official MV. https://www.youtube.com/watch?v=iUcwJzNFC1I.

[35] https://bitcointalk.org/index.php?topic=375643.0.

[36] Hoffman, G. A Brief History of BTFD. The Stocktwits Blog. June 2017. https://blog.stocktwits.com/a-brief-history-of-btfd-e318528cd0ac.