Kshetri, Nir

Conference Paper

Privacy violations, security breaches and other threats of Web3 and the metaverse

32nd European Conference of the International Telecommunications Society (ITS): "Realising the digital decade in the European Union – Easier said than done?", Madrid, Spain, 19th - 20th June 2023

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Kshetri, Nir (2023) : Privacy violations, security breaches and other threats of Web3 and the metaverse, 32nd European Conference of the International Telecommunications Society (ITS): "Realising the digital decade in the European Union – Easier said than done?", Madrid, Spain, 19th - 20th June 2023, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/277993

Privacy violations, security breaches and other threats of Web3 and the metaverse

Abstract

Web3 and the metaverse present several unique challenges from security and privacy standpoints. This paper looks at key features of these technological innovations from privacy and security angles and discusses how they are vulnerable to various types of breaches, bugs and attacks as well as other types of scams, frauds, and deceits. It offers a detailed description of technological environment and institutional level factors that can lead to increased privacy violations and security breaches in Web3 and the metaverse. The paper will discuss how newness, novelty and complexity of technologies involved and weak architectural security of Web3, and the metaverse are likely to provide a fruitful environment for cybercriminals and other perpetrators. On the regulatory front, it points out that privacy and security laws of the Web2 era are not sufficient to deal with the environments of Web3 and the metaverse. The paper also argues that the preparedness to provide security and privacy in the metaverse's multidimensional and multi-sensory environment is currently lacking at the industry level. It analyzes the level and nature of the impacts of privacy violations and security breaches on consumers and victims in the Web 3 and the metaverse environments. It gives special consideration to the multisensory environment of the metaverse which can lead to more adverse impacts on users and victims in case of privacy violations and security breaches. The paper also demonstrates how security breaches in Web3 and the metaverse are likely to lead to immediate harms to victims. It promotes an understanding of how blockchain, which is the key building block of Web 3 and the metaverse, can be vulnerable under certain conditions. The paper also delves into cyberattacks and other malicious behaviors targeting crypto-assets such as cryptocurrencies and non-fungible tokens (NFTs), which are key enabling technologies of Web3 and the metaverse economies. It provides guidelines and suggestions for consumers, businesses, industries and nations to enhance security of Web3 and the metaverse.

Keywords: Metaverse; privacy; security; self-sovereign identity; Web3

Introduction

A commonly held view is that Web3 solutions have cybersecurity baked into them[1]. Pivotal to this view are various features of Web3 such as user-controlled wallets, ID portability and data minimization can reduce some of the security and privacy risks and associated impacts of Web2 since individuals are offered higher degree of control over their data[2]. Web3 solutions are being deployed to strengthen cybersecurity (In Focus 1).

In Focus 1: The Taiwanese Ministry of Digital Affairs uses Web3 to strengthen cybersecurity

In 2021, Taiwan experienced about 5 million daily cyberattacks or scans for system vulnerabilities. Many of them involve distributed denial-of-service (DDoS) attacks, which render the sites inaccessible[3]. Following the speaker of the U.S. House of Representatives Nancy Pelosi's Taiwan visit in August 2022, China allegedly combined physical and digital warfare. The PLA conducted military drills around Taiwan (Haldane & Shen, 2022)[4]. On August 2, 2022, the day Pelosi arrived Taiwan, cyberattacks against the island nation reached 15,000 gigabits, which was 23 times the previous daily record[5]. Multiple government websites became inaccessible due to the distributed denial-of-service (DDoS) attacks. The island also experienced public digital *signage hacks.* a local railway station displayed a message, which referred to Pelosi as a "witch", who wanted to divide the Chinese people and challenge China's sovereignty – as "psychological warfare"[6].

In an effort to fight cyberattacks originated from China, the Taiwanese Ministry of Digital Affairs (MODA) announced plans to implement decentralized technology into its web portal. The MODA has used InterPlanetary File System (IPFS), which is a Web3 technology for decentralized file sharing. IPFS identifies content through file hashes, which makes it possible for files stored by multiple parties to be found anywhere. The files can be accessed by simple HTTP. The files and the original site index were available on IPFS and were publicly accessible.

A limitation of IPFS is that it is designed to make static content discoverable based on file hashes. It is thus not suitable for dynamic content. For instance, the hash changes when files are updated. It is not thus suitable for constantly changing, dynamic web content. For such contents, the MoDA was still using Web2 technologies.

Taiwan's Digital Minister noted that the MODA site had not been attacked since it started combining Web3 and Web2 tools. It uses a Web3 structure and the global Web2 backbone network. The minister explained that in order to take it down, blockchain networks such as Ethereum and NFTs have to be taken down, which is unlikely[7].

Nonetheless, self-sovereign identity (SSI), pseudonymity and anonymity have a number of drawbacks. Security researchers have highlighted various weaknesses in Web3. The speakers at the Black Hat conference held in Las Vegas, the U.S. from August 6-11, 2022 extensively discussed high-profile Web3 hacks that have led to the theft of hundreds of millions of dollars' worth of cryptocurrencies. Among major points made by the speakers were: a) Most Web3 developers lack experience and they are building applications on new platforms that are publicly viewable; b) An attacker can quickly monetize a vulnerability; c) A simple mistake can have severe consequences [8].

A key challenge is that since Web3 builds trust without an intermediary[9], accountability cannot be established. Commenting on the cyberattack on the play-to-earn (P2E) game Axie Infinity in March 2022, in which hackers stole US$625 million and Axie Infinity's post breach response, a decrypt article noted that if a cybersecurity team at a Web2 company behaved that way, they would be "fired and face charges of civil or even

criminal negligence". The article goes on saying: "Web3 risks inheriting the worst security failures of the previous internet but none of the accountability" [10].

In the Web2 environment, hackers can monetize only a small proportion of stolen bank passwords. Most passwords stolen from nonbank institutions are virtually worthless[11]. In the Web3 environment, cybercriminals such as those hacking Axie Infinity (In Focus 2) are not required to do virtually anything to monetize stolen data.

In Focus 2: Axie Infinity faces the biggest hack in decentralized finance history

On March 23, 2022, the crypto metaverse P2E game Axie Infinity became the victim of what is considered to be the biggest hack in decentralized finance's (DeFi) history[12]. The hackers compromised Sky Mavis's Ethereum-linked sidechain Ronin, which was specifically made for Axie Infinity.

Note that a sidechain is a separate blockchain that operates independently and runs in parallel to Ethereum Mainnet (the parent blockchai*n*) via a two-way *peg*. A two-way peg allows the transfer of digital assets such as ETH back and forth--between the mainnet and the sidechain. A point to be noted, however, is that the assets are not actually transferred. They are just locked on the mainnet while an equal amount is unlocked in the sidechain.[13] A sidechain is less decentralized, uses a separate consensus mechanism and is not secured by layer 1 (that is, a sidechain is not layer 2). Thus, it is possible for a quorum of sidechain validators to commit a fraud.[14]

Sidechains increase blockchains' scalability and help them develop and interact. For instance, Ethereum and Bitcoin networks require every node to validate new transactions. The sidechain networks take responsibility for validating their own transactions. They update the parent (root) chain only periodically, which increases transaction throughput[15]. Sidechains facilitate faster as well as cheaper transactions since the game players are not required to pay expensive gas fees.

As of March 2022, more than US$21 billion was locked on Ethereum bridges. According to Chainalysis, in a little more than a year, seven different security breaches associated with bridges had led to more than US$1 billion in stolen cryptocurrency. Developers can be anonymous, and the names of the validators are purposefully kept secret. Many are run by organizations that lack security staff . Most bridges do not have insurance, which means that there is no guarantee of a reimbursement of funds if they are lost[16].

Whereas Ethereum's network as of March 2022 consisted of 222,052 validators to secure over 7 million ETH[17], the Ronin sidechain was secured by only nine validator nodes. Hackers had compromised five of these nodes. Using the compromised nodes' signatures, the attacker withdrew 173,600 ETH and 25.5 million USDC, which amounted US$625 million. Two-thirds of the stolen funds belonged to users and the remaining was the Axie Infinity treasury of revenues[18].

The Ronin bridge attack is described as a multi-signature compromise[19]. The attacks went unnoticed for six days. On March 29, one user reported that they could not withdraw 5000 ETH via the Ronin bridge. Only then the Sky Mavis team knew that the funds had been stolen from the bridge. Axie Infinity's other assets had not been compromised[20]. That is, the Axies were not been stolen

Sky Mavis replaced its validators following the attacks. To prevent similar attacks in the future, it announced plans to expand the network from nine to 21 distinct validator nodes consisting of various stakeholders such as partners, community members, and long-term allies[21].

There is an additional point that deserves attention. It is extremely rare for funds to be recovered after a crypto hack since there is no information about the hacker readily available except for the wallet address.

A reason why Web3 projects are insecure is also the fact that the such projects rely on web2 infrastructures. That is, Web3 projects are also compromised through web2 vulnerabilities[22]. For instance, according to the FTC, about half of the victims who reported losing crypto since 2021, scams started with ads, posts, or messages on Web2 social media platforms[23].

Likewise, metaverse activities create more and richer data, which are attractive to nefarious actors. According to a 2022 report of Credit Suisse, the metaverse revolution will increase the average data usage worldwide to 20 times by 2032[24]. For instance, 20 minutes of virtual reality (VR) use can generate about 2 million unique data elements related to the way the user breathes, walks, thinks, moves or stare[25]. In addition to the data that is already on the web, new data related to NFTs, cryptocurrency transactions, avatars, experiences and other aspects will be created. One study found that metaverse companies experienced a 40% increase bot-driven as well as human-driven attacks. Such attacks are likely to increase as more people join the metaverse and more data are created[26].

Consumers are rightly concerned about privacy and security in the metaverse. Market research company Propeller Insights' December 2021 survey of 1,002 U.S. consumers, which was conducted on behalf of VPN service provider NordVPN, found that 55% did not know what the metaverse is. Yet 87% expressed privacy concerns about the metaverse and 50% thought that the metaverse would provide an ideal means for hackers to impersonate others. Likewise, 47% of the respondents were of the view that there would be no legal protections for users' identities,

and 45% viewed that the metaverse would force them to share more of their private data that could be misused and abused[27].

Cybersecurity challenges facing new and emerging technologies are well known. Most obviously, criminals target sources of value (Kshetri, 2005)[1]. Web3 and the metaverse are becoming attractive targets for cybercriminals and other malicious cyber actors with a rapid increase in investments and their uses in a wide range of activities. For instance, DeFi, which is currently among major Web3 applications, has faced a number of high-profile cyberattacks, which have led to substantial losses. According to bug bounty platform Immunefi, the DeFi market lost over US$1.22 billion to hackers in the first three months of 2022 alone[28]**.** As of the first quarter of 2022**,** losses to **c**rypto-bridge hacks had exceeded US$1 Billion in little over a year[29]. Such hacks victimized high-profile companies such as the crypto metaverse P2E game Axie Infinity and DeFi platform Poly network.

Due primarily to the newness of Web3 and the metaverse, most organizations lack appropriate frameworks to deal with privacy and governance issues related to customer and employee data. For instance, during metaverse-based training scores and modules, data such as those related to the amount of time taken by an employee to hover over an item or answer a question are sensitive[30]. Yet companies lack appropriate policies regarding the types of data that can be collected from and about employees when they participate in in training and education in the metaverse.

Security and privacy concerns of Web3 and the metaverse may also be attributable to the fact that companies are building projects and protocols as fast as possible in order to attract

---

[1] Kshetri, N. (2005). Pattern of Global Cyber War and Crime: A Conceptual Framework, *Journal of International Management*, 11(4), *541-562*.

investment and be the first to market. However, they have not paid attention to cybersecurity practices[31]. The upshot of these tendencies is that Web3, and the metaverse are vulnerable to breaches, bugs and attacks. Compared to traditional security threats that were mainly related to phishing or endpoint attacks, Web3 security attacks such as rug pulls, ice phishing, cryptojacking, virtual sexual assault and bridge exploits are more serious[32]. An article published in blockchain newspaper Decrypt suggested that Web3 is becoming a "security nightmare" and explained wide open security holes in Web3 platforms[33].

Web3 and the metaverse will involve increased adoption of the blockchain architecture as well as more widespread use of cryptocurrency as a means of value exchange[34]. A current challenge is that only a small number of people understand blockchain security, and an even smaller number possess skills to assess and fix it[35]. The lack of human resources to tackle security issues is particularly challenging. This and other uncertainties have clouded the future of Web3, and the metaverse. Some have thus gone as far as to say that cybersecurity "Will Make Or Break The Metaverse" (Merre, 2022)[2].

Turning now to the regulatory context, laws such as the California Consumer Privacy Act (CCPA), the General Data Protection Regulation (GDPR) and China's Personal Information Protection Law (PRPL) require organizations to secure personally identifiable information (PII). In order to deliver metaverse experiences, which involves the blurring of the digital and physical worlds, organizations need to collect, store and manage PII and other data that are much more sensitive than in the Web2 era. Such data come from various sources such as biometric devices,

[2] Merre, R. (2022). Security Will Make Or Break The Metaverse, March 24, https://www.nasdaq.com/articles/security-will-make-or-break-the-metaverse

smart speakers and microphones and virtual reality headset[36]. For instance, a company cannot convincingly argue that tracking users' movements is needed for mobile app. Such data, on the other hand, can become an integral part of the metaverse experience. For instance, metaverse companies might argue that data related to users' movements need to be stored for troubleshooting. The existing privacy laws thus can be interpreted differently due to different data needs[37].

It is also perhaps worth noting that many metaverse activities involve real-time transfer of data, which cannot be anonymized unlike a data package being sent[38]. Addressing security and privacy challenge and complying with these regulations may be no small feat in the metaverse environment.

On the plus side, investments in web3 and metaverse security have been rapidly increasing. For instance, according Crunchbase data, investments in cryptosecurity, which deals with technologies to secure digital wallets and cryptocurrency transactions, exceeded US$1 billion in the first seven and half months of 2021, compared to less than US$100 million invested in the sector in 2020[39].

Key features of Web3 and the metaverse from the privacy and security standpoints

In this section, we highlight several key challenges that affect Web3 and the metaverse from the privacy and security standpoint. Specifically, we focus on the technological environment, institutional level factors and the level and nature of impacts on consumers and victims.

Technological environment

Newness and novelty of technologies involved

Perpetrators can take advantage of the relative newness of Web3 and the metaverse, and potential victims' lack of understanding of these environments. An understanding of

manipulative techniques used by various creatures to fool their enemies is of particular relevance in situations such as this. In particular, a phenomenon proposed by Dawkins (1982)[40] called the "rare enemy syndrome," provides a helpful theoretical perspective for understanding how victims often fall to new unfamiliar baits or lures. The basic idea behind rare enemy syndrome is simple. The enemy's manipulation is so rare that evolutionary development has not yet progressed to the point that the victim has an effective counter poison (de Jong, 2001)[41]. For instance, perpetrators are applying new techniques such as ice phishing to manipulate the victims (In Focus 3).

Some experiences in the metaverse replace ads. Users can wear virtual clothes or test drive virtual cars. All the relevant data such as moves that users make, what they are wearing, seeing, driving, and related time period can be recorded and potentially be sold[42].

In Focus 3: BadgerDAO becomes a victim of ice phishing

An 'ice phishing' technique entails manipulating users into signing a transaction that delegates approval of the user's tokens to the attacker. That is, the perpetrator tricks unsuspecting users to sign a malicious smart contract that would redirect tokens from non-custodial wallets to an attacker-controlled address. The attacker thus does not steal one's private keys. The attacker just needs to modify the spender address to attacker's address. From the attacker's perspective this approach is attractive since the user interface does not show all relevant information to indicate that the transaction has been tampered with[43]. The lack of transparency on the transactional interface in Web3 makes it difficult to detect the displacement of tokens[44].

Among a high-profile example of ice phishing attack victim is BadgerDAO. Perpetrators compromised the front-end of BadgerDAO and malicious scripts were then injected. Users with high balances were targeted and asked to sign fraudulent transaction approvals. BadgerDAO noted that that "the script intercepted Web3 transactions and prompted users to allow a foreign address approval to operate on ERC-20 tokens in their wallet"[45]. The attacker moved funds to other accounts on behalf of the users. The criminals then liquidated the funds and used Badger Bridge to convert to BTC and exit. About US$121 million was stolen.[46]

Some view the metaverse and artificial intelligence (AI) as two areas in which perpetrators can effectively deceive and victimize users. In this regard, it is important to note that AI is playing an increasingly important role in Web3 and the metaverse. Critics have drawn attention to the potential negative impacts of various technologies associated with the metaverse. It is also argued that the goal of VR and augmented reality (AR) technologies in the metaverse is

to fool the senses by making computer-generated content seem like real-world experiences. Likewise, mathematician, logician and cryptographer, Alan Turing stated that a human-level AI's ultimate test would be to successfully fool consumers into believing that the AI is human. The power of these technologies to deceive users will soon transform society. AI-driven avatars are more and more likely to look, sound, and act like humans, which means that consumers will not be able to tell the difference between actual people and virtual people. Researchers have been able to use a sophisticated form of AI known as a generative adversarial network (GAN) to create effective artificial human faces (i.e. photorealistic fakes). The researchers found that humans cannot tell the difference between real and virtual faces. But there is another point that is perhaps even more important. When the pictures of those fakes and real persons were presented and asked to rate for the "trustworthiness", the research participants viewed AI generated faces to be significantly more trustworthy. Thus, advertisers are likely to find it attractive to use AI generated people in place of human actors and models to deceive users in the metaverse. In addition to the fact that virtual people are perceived to be more trustworthy and thus more persuasive, using them will also be cheaper and faster. These technologies are likely to give large corporations and adversaries more power[47]. Using an analogy of rare enemy syndrome discussed above, the poison itself is more deadly in addition to the fact that the victims lack a counter poison for providing protection against and destroying the poison,

From a criminal's perspective, the novelty of a new technology provides an attractive opportunity to engage in social engineering frauds. The metaverse is also likely to open the possibility of new attacks involving fraud and phishing such as a hacked avatar or deepfake of a familiar person such as a CEO of a company. Hackers can use them to authorize fund

transfers or disclose confidential information[48]. Such attacks can also involve a face such as an avatar who impersonates a coworker[49].

Due to the newness and complexity, monitoring the metaverse and detecting attacks on these new platforms is also more challenging than on current platforms (Alspach, 2022)[50]. One of the biggest challenges is that there are not enough qualified people to deal with the complexity of the architecture and develop secure solutions for the metaverse (Vellante, 2022)[51].

Complexity of Web3 and metaverse technologies and weak architectural security

Web3 and the metaverse are being built on many advanced technologies such as blockchain, VR, AR, AI, machine learning (ML), natural language processing (NLP), 3D graphics and sensors of various types. Many of these technologies have been in use for many years. But what is different in the metaverse is that they are being used together for the first time. Different organizations built these technologies without an understanding of the end use, which can increase the security risk[52]. The increasing number of layers and complexity of technologies used for diverse purposes in the metaverse such as gaming, remote workforce collaboration, virtual communities, and shopping would amplify potential cybersecurity vulnerabilities (Thompson, 2022)[53]. It is possible for nefarious actors to find new and more advanced ways to attack organizations[54].

While the metaverse is heralded as the next evolution of the internet, concerns have been raised about architectural security and insecure system designs. Architectural security entails providing an appropriate level of protection depending on the specific type of data and the security environment involved (Rahimi & Haug, 2010)[55]. In the Open Web Application Security Project (OWASP) Top 10, which is a standard awareness document for developers and web application security representing a broad consensus about the most critical security risks to web applications (OWASP 2021b)[56], insecure design was identified as a new category for 2021.

Embedded systems security can help protect the Internet of things (IoT), VR, AR, and other metaverse technologies from malicious behaviors (Madou, 2022)[57]. A key concern is that an insecure design that lacks such systems and needed security to defend against specific attacks, cannot be fixed just by implementing the systems perfectly (OWASP 2021a)[58].

Due to the newness of Web3, the metaverse and associated technologies, consumers and investors have a high likelihood to be victims of various scams. Especially social engineering, which involves emotional appeals such as fear, pity, or excitement to victimize the targets, has been a major modus operandi of many fraudsters operating in the Web3 and metaverse environment They establish interpersonal relationships or create a feeling of trust and commitment in order to achieve these goals. For instance, social engineering tricks are used to gain access to a victim's private key of the account associated with the NFT. In other cases, victims may be lured to click malicious links, or download files containing malware.

Some scammers use fake NFT customer service pages to lure NFT owners to divulge sensitive information. When creative producer and director Jeff Nicholas was trying to get help for a royalty issue from OpenSea in August 2021, some scammers masquerading as OpenSea employees invited him into a channel of the Voice over Internet Protocol (VoIP), instant messaging and digital distribution platform Discord called "OpenSea Support Server". After hours of interaction, the scammers convinced him to share his screen with them. When he shared the screen, they were able to take a picture of the QR code synced to his private key, or "seed phrase", which allowed them to gain full access to his crypto-assets. They stole 150 ether (ETH), which was valued about US$480,000 that time[59].

Scammers also trick consumers into buying fake NFTs. They copy social media accounts of reputable companies and create fake pages that closely resemble the originals. Using the fake accounts, scammers can convince their legitimacy to potential victims and sell fake NFTs[60].

Institutional level factors

Various participants in the metaverse are nested within institutional structures, such as nations and industries.

Weak and underdeveloped regulatory environment

Web3 and the metaverse raise many complex issues from privacy and security standpoints. On the regulatory front, privacy and security laws of the Web2 era are not sufficient to deal with these complexities and challenges. Data privacy and cybersecurity regulations lag behind innovations in the metaverse. Global regulations such as the European Union's (EU) General Data Protection Regulation (GDPR) are insufficient to regulate privacy issues in the metaverse. For instance, since the metaverse is boundaryless and thus is not divided into individual countries, it is not clear how the GDPR's clauses dealing with transfer and processing of data outside the EU can be applied. The GDPR is applied based on where the subject is located when their data is processed. When an avatar's data is being processed, a confusion that can arise is whether the location is determined based on the person operating the avatar, or the avatar itself. In the latter case, the jurisdiction of avatar's location is not easy to determine (Lau, 2022)[61].

Likewise, when individuals engage in activities such as purchasing real estate or shoes for their avatars and playing games, no clear regulatory guidelines exist as to how much information to put out there and collect. While these issues are being actively explored by regulators and new regulations are likely to be developed, the current regulatory uncertainty is a concern [62].

There are also compliance-related challenges due to Web3's pseudonymity, which can potentially increase money laundering and terrorist financing. Decentralized IDs also complicates existing regulations, such as GDPR. Web3's anonymity can create challenges related to accountability, liability, legal recourse and consumer protections[63].

Lack of preparedness at the industry level

The industry level preparedness to tackle the privacy and security issues facing Web3 and the metaverse is not satisfactory. Especially industry level guidelines have not been established yet. For instance, standards and norms have not been well developed as to how much information to put out there and collect[64], what information is stored on-chain vs. off-chain, who needs to know when and how to authenticate transactions and who the decision maker will be and what parameters are used[65]. While privacy advocates are also looking at these issues, clear guidelines have not yet been developed[66].

The demographic composition of the metaverse also creates cybersecurity risks. Most metaverse users currently are young. Cybersecurity strategies of most banks and financial technology companies, on the other hand, have been developed keeping older consumer in mind. Younger customers tend to behave differently. For example, it is reported that many young consumers tend to share their credentials with others, which can create new risks for banks and financial technology companies [67].

The level and nature of impacts on consumers and victims

A question that naturally arises is how privacy violations and security breaches in Web3 and the metaverse environments affect the users. This section deals with the level and nature of impacts of such incidents on consumers and victims.

Immediate harms to victims

In traditional environments, nefarious actors often exploit services and data without clear or immediate monetary benefits. In blockchain applications, significant value is often encoded directly into the software. It is much easier and attractive to monetize exploits in smart contracts as they deal with money. This also means that hacking could lead to immediate and guaranteed harms to the target[68]. For instance, a user's ID in the metaverse is linked to cryptocurrency wallets, NFTs, and various smart contracts.

Amplified impact on consumers and victims

The metaverse involves a multisensory environment. Due to complex and sophisticated features such as more graphic, 3D design, immersive visual and auditory experience, when unwanted and privacy-invasive contents proliferate in the metaverse, they may be felt as more intrusive and are likely to have a greater negative impact on the users or victims. For many uses, the intense, immersive nature of the virtual world makes negative virtual experiences as traumatizing as in the physical world[69]. Thus, privacy violations in the metaverse are likely to lead to more severe consequences, which are also referred to as an amplified technical impact (ISACA.2014; Kshetri, 2014)[70].

Information of users and their activities in the metaverse can be used to construct much more detailed and intimate profiles, which lead to a much higher cost of privacy violations. For instance, VR and AR devices can collect more and richer data about users compared to traditional methods. In addition to standard personally identifiable information (PII) such as names and social security numbers, metaverse platforms can collect biometric data and 3D content. Such data include body shape constructions such as height and arm length, language, voice, vision, and health statistics. Other vital signs such as heart rate could also be tracked in order to form more accurate digital profiles of users[71].

Contextual data such as information about the room in which the user is operating in can also be collected. Existing VR and AR devices have been mainly used for entertainment purposes and they rarely have integrated security provisions. Device manufacturers can help strengthen the security of the metaverse by including security provisions into hardware. Organizations need to be more careful in selecting devices and should select devices with adequate security in order to protect users[72].More advanced AR and VR technologies can access more sensitive information. For instance, gaze-tracking technology can allow the use of eyes to control and interact with the metaverse. Companies can collect gaze data such as pupil size and eye openness[73]. Meta has patented technology to integrate eye tracking into its optical equipment that is worn by users to access the metaverse[74]. Disney's Disneyland metaverse plans to use its patented gaze tracking technology, which would use cameras to detect where riders are looking. For instance, if a rider stares too long at an animatronic character, it might talk to the rider using their name. Disney also envisions using the technology with droids in the new Galactic Starcruiser hotel at Disney World, which is expected to facilitate lifelike conversations between droid bartenders and guests[75].

Some technologies have been adapted from other areas to develop new tools for marketers to more effectively track consumers. One such technology is the brain-computer interface (BCI) system. BCI is used to record, process, and analyze human brain activity in the form of neurodata, which is then translated into an output command to machines[76]. The main use of BCI has been in improving the daily lives of people with prosthetic limbs. French neuro-technology startup NextMind has developed a BCI tool, which utilizes non-invasive electroencephalogram (EEG) technology to detect electrical signals from the brain[77]. The signals can be translated into readable commands such as a specific movement in a VR game[78]. In

March 2022, visual social media platform Snapchat's parent company Snap acquired NextMind. Snap hopes to incorporate NextMind's BCI in its future products including its Spectacles AR glasses[79].

BCI allows companies to collect and share sensitive information related to individuals' psychological states such as emotions and intent. By combining neurodata with other personal information, companies can build more granular and sensitive profiles about consumers, which can be potentially used for behavioral advertising and other invasive and exploitative ways. In heavily surveilled states, surveillance tools that are based on sensitive neurodata can help authoritarian regimes increase the degree of control over citizens [80]

Companies thus have more incentives to collect user data and share such data with third parties which can be used for profiling to deliver customized advertising. To take an example, Meta announced that it was working on a high-end VR headset Project Cambria, which will have capabilities that are not possible with headsets currently being used. New sensors in the device will allow the user's virtual avatar to maintain eye contact and reflect facial expressions (Bonifacic, 2021)[81]. In this way, Project Cambria would have the capability to mirror a person's face and eye movements in VR. Meta can give this information to advertisers, which can help the latter measure users' attention more accurately. The measurement can help target users with ads and influence them to buy products. Meta has stated that the company currently does not share eye-tracking data with advertisers. The company, however, has not committed that it will not collect and share such data in the future (Hunter, 2022)[82].

Likewise, security breaches in the metaverse may be associated with more adverse consequences compared to Web2. For instance, perpetrators in the metaverse can target financial data, crypto-assets and highly sensitive personal data (Merre, 2022)[83]. More importantly

these harms go beyond financial harms and privacy violations. Cyberattacks against metaverse systems may also extend to physical harms. For instance, VR headsets, which are a gateway to user data, and AR headset can be hacked (Creamer Media Engineering News 2022), which may lead to physical harms to victims.

Researchers found that by exploiting VR systems, it is possible to control the activities of immersed users and physically move them to a location without their knowledge (Casey et al., 2021)[84]. For instance, by manipulating a VR platform and resetting the hardware's physical boundaries, an adversary can influence a user to take actions that make them fall down a flight of stairs and cause serious injuries.

AR involves using some type of lens to add virtual overlays on top of the real world. Compared to VR, AR is less immersive since users can have their surroundings' normal view. Some AR examples include wearables such as Microsoft's HoloLens or simply a smartphone using the Waze app. It is possible for the host to see the user's location and have some interpretation of their intentions[85].

AR often involves overlaying data provided by a third-party. Any compromise in data integrity can have serious consequences. For instance, if a location app overlaid onto a headset uses flawed location data, the user gets incorrect directions[86]. Users that are too immersed in the virtual world could potentially be misdirected into a street, which can lead to a physical harm. The AR headset wearer can be a victim of violent crimes such as robbery, mugging, and assault (Nichols, 2022)[87].

Technical weaknesses and vulnerabilities of blockchain systems

While blockchain, the key building block of Web3, and the metaverse, has been long touted for its security, the technology can be vulnerable under certain condition[88]. Hackers have exploited

technical weaknesses in blockchain systems. Especially smart contract logic hacks target logics that are embedded in blockchain services to take advantage of functions and services, such as collaboration, crypto-loans, project management and functionality of wallets. Ethereum smart contracts, which are based on Solidity programming language, are vulnerable to reentrancy attacks. Note that a procedure is re-entrant if "its execution can be interrupted in the middle, initiated over (re-entered), and both runs can complete without any errors in execution"[89]. Minor mistakes can lead to serious consequences. For instance, in 2016, hackers exploited vulnerabilities in the decentralized autonomous organization's (DAO) code and hacked the Ethereum blockchain. Note that the DAO runs through smart contracts and do not need centralized management and the direct control of self-interested institutions. Hackers were able to steal US$60 million of Ether in "The DAO" hack due to a single misarranged line of code[90]. In 2016, the DAO smart contract had over US$150 million worth of ether. A project requesting funding could withdraw ether from that project's Ethereum address if it received sufficient support from the DAO community. A flaw in the code allowed the transfer of the ether to the external address before updating its internal state. It meant that the smart contract did not note that the balance was already transferred. The attackers thus withdrew more ether than they were eligible for.

Ethereum cofounder Vitalik Buterin's "blockchain trilemma"[91] proposed three main issues — decentralization, security and scalability — that blockchain developers encounter. He argues that it is easy to achieve two of the three goals, but very difficult to achieve all the three. Vitalik also warned that bridges are less secure than Layer 1 projects such as Ethereum or Bitcoin[92]. The cyberattacks against Axie Infinity (In Focus 2) and Poly Network (In Focus 5.4) highlight the vulnerability of bridges for projects using blockchain.

In Focus 4: Hacker exploits Poly Network's smart contract tools

Poly Network is a decentralized finance (DeFi) platform that facilitates peer-to-peer transactions. The company views its protocol as a tool for building Web3 infrastructure.

Its focus is on a cross-blockchain interoperable bridge, which allows users to swap tokens from one blockchain to another. For instance, users can trade Bitcoin for Ether. As of April 2022, Poly Network had integrated over 15 blockchains (https://poly.network/#/). Note that in a bridge, transfers involve locking tokens on a source blockchain. The tokens are then unlocked on a destination blockchain. After a transaction takes place on a source blockchain, the Poly Network Keepers sign blocks of the source blockchain containing the transaction. The signed block is then submitted by the keeper to a smart contract manager on the destination blockchain. The smart contract manager's job is to assess the signatures' validity. If the block is valid, the transaction is executed on the destination blockchain.

In August 2021, a hacker exploited a vulnerability in Poly network's EthCrossChainManager smart contract manager on the destination blockchain, which takes the incoming transaction, validates it and then executes the contract specified in the transaction [93]. The hackers had compromised trusted entities called "keepers" stored in the EthCrossChainData contract, which is owned by the EthCrossChainManager[94]. EthCrossChainData facilitate the cross chain transactions to unlock tokens on the destination blockchain without locking the tokens on the source blockchain, essentially managing to duplicate tokens across two blockchain networks. Fake transactions were created that allowed the hackers to unlock tokens on the destination blockchain without locking equivalent tokens on the source blockchain.

The attacker took control of the keepers and tricked EthCrossChainManager contract into executing cross-chain transactions that were not conducted on the source blockchain. The hacker stole over US$600 million worth of tokens[95].

The hacker later returned the funds to the Poly Network. The platform offered the anonymous hacker a job as its chief security advisor[96]. Poly Network also offered to pay the hacker a US$500,000 bug bounty for identifying the flaw that was exploited in the attack[97].

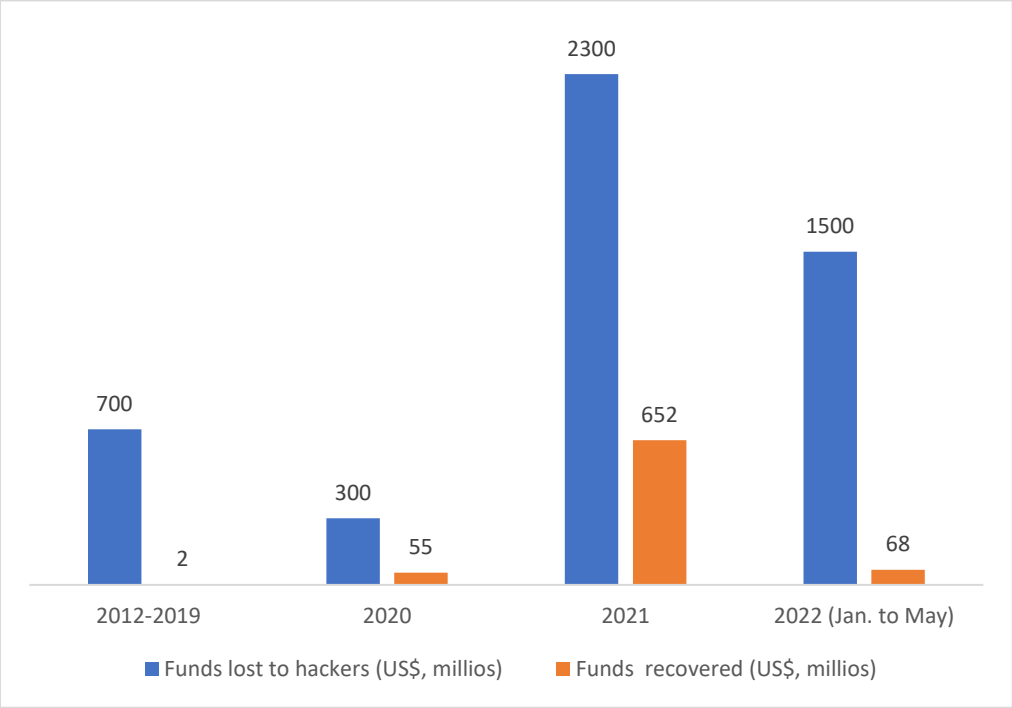
Cyberattacks and other malicious behaviors targeting crypto-assets

Crypto-assets such as cryptocurrencies and NFTs are the key building blocks of Web3 and the metaverse economy. NFTs represent ownership of virtual in-game items, virtual avatars, real estate properties and other assets and also enable the authentication of these assets and even identities. Cryptocurrencies play the same role in the metaverse economy that money does in the modern economy. For instance, cryptocurrencies are needed to buy NFTs such as real estate, and clothes and shoes for the avatar. Several metaverse platforms such as Sandbox and Decentraland have their own cryptocurrencies.

Crypto-assets face cyberattacks at various levels. First, as explained earlier, blockchain platforms behind cryptocurrencies and NFTs themselves could be vulnerable to hacking. That is, they face risks related to the platform on which smart contracts run[98]. In this regard, a key point that needs to be emphasized is that blockchain places a high priority on anonymity and privacy,

which makes it difficult for companies to track a hacker's identity. For instance, users' wallets and transactions are publicly visible on the blockchain address. However, they are not directly connected to owners' true identities. This lowers the cost of attacks and hackers face lower probability of arrest and conviction[99].

Figure 5.1: Funds lost to hackers and amount returned to victims (US$, million)



Data source: [100]

Some nefarious actors are making use of digital coins that have baked a higher degree of anonymity and untraceability into their designs, which further increases the difficulties involved in the recovery of stolen crypto-assets. According to a report by blockchain security company Beosin, Web3 experienced 48 major cyber attacks in 2022Q2, which resulted in losses of about US$718.34 million. Approximately US$418.89 million in stolen funds were transferred to a crypto mixing service Tornado.cash[101]. Tornado Cash is a service used to anonymize crypto transactions. The base code of privacy coin ZCash was forked to create Tornado Cash[102]. It was sanctioned by the U.S. Treasury Department in August 2022. *According to* the U.S. Treasury,

Tornado was used to launder US$7 billion worth of crypto[103]. U.S. treasury undersecretary for terrorism and financial intelligence criticized Tornado Cash arguing that it failed to implement adequate controls against money laundering[104].

An upshot of this difficulty in tracking a hacker's identity is that only a small proportion of stolen funds are recovered (Figure 5.1). The proportions of recovered funds in Web3 attacks were 0.28% during 2012-2019 and 4.5% in the first five months of 2022. While recovered fund accounted for 28.3% of stolen fuds in 2021, this was the exception rather than the rule. This very high proportion is attributable to the fact that A hacker, who stole over US$600 million worth of tokens[105] from the Poly Network in August 2021 returned most of the stolen funds[106]. The platform offered the anonymous hacker a job as its chief security advisor[107]. Poly Network also offered to pay the hacker a US$500,000 bug bounty for identifying the flaw that was exploited in the attack[108].

Cyberattacks targeting crypto-asset platforms

Online marketplaces such as OpenSea are a key component of Web3 and the metaverse ecosystems. For instance, Nike's first collection of shoes for the metaverse, known as CryptoKicks, is being traded as NFTs on OpenSea[109]. While crypto-assets such as NFTs are based on blockchain, exchanges and marketplaces such as Coinbase, OpenSea and Rarible function in a centralized manner[110]. Custom protocols are used for accounts in crypto-exchanges, which are often based on a non-blockchain Web2 technologies[111]. They thus cannot utilize the benefits of decentralized technologies such as peer review systems to identify and fix bugs. Consequently, these marketplaces are vulnerable to b*reaches,* bugs and attacks.

In September 2021, a bug in the OpenSea token market led to a disappearance of 42 NFTs that were valued more than US$100,000[112]. Israeli cybersecurity company Check Point

reported that it found vulnerabilities in OpenSea that could have allowed cybercriminals to sell malicious NFTs, or trojanized digital art. Check Point researchers said the flaw made it possible for hackers to offer a malware infected image file as an NFT. For instance, a user could be lured with a free NFT. When the victim opens the NFT file on their device, a series of malicious pop-ups pretending to be from OpenSea could be deployed. A pop-up requests the user to connect their digital wallet. When the user does so, the hackers steal funds in the wallet. OpenSea subsequently patched the security flaws when they were brought to its attention[113].

Social engineering attacks targeting crypto-asset platforms are also rapidly increasing. In May 2022, Yuga Labs, creator of the popular NFT collection Bored Ape Yacht Club, launched a sale of virtual land deeds for its yet-to-be released metaverse project, Otherside[114]. Even before this official sales by Yuga Labs, scammers were reported to exploit a bug inside OpenSea to send multiple fake NFT land packages to various holders of blue-chip NFTs[115] and Web3 influencers under the BAYC developer contract. The scammer attempted to mask their identity by using an address that looked similar to an official BAYC affiliated address. They pulled the scam NFTs from the BAYC contract, which appeared as a legitimate source. They then sent the fake NFTs to various wallets in order to steal the victims' assets[116].

Cyberattacks targeting wallets

Cybercriminals can also launch attacks against wallets that are used to store crypto-assets. There are two options for a wallet: hot wallet (e.g., account in exchange/website-based wallet) and cold wallet (e.g., hardware or paper-based). Hot wallets play an important role in the metaverse. For example, in Decentraland, users are required to link their hot wallets in order to access and take advantage of full, customizable accounts[117]. Crypto-assets such as NFTs that are stored in hot

wallets are online by default under the control of the wallet provider. The majority of attacks involving crypto-assets such as NFTs have **been** carried out against hot wallets.

Cybercriminals are increasingly targeting crypto wallets. In a study released in early 2022, Trend Micro detected more than 2,000 scam NFT websites, many of which targeted crypto-wallets. For instance, unscrupulous actors had created a fake copy of Decentralized Organization Metaverse.Pro. The fake website metaverses-pro.com, users are asked to download an APP to "manage your assets". If an unsuspecting user follows the instructions, malware will start to download to their device and install keylogger, which is designed to steal the user's stored credentials. Scammers then get access to the victim's crypto wallet and transfer all cryptocurrencies and NFT collections[118].

In June 2021, an NFT artist Fvckrender reported that he was tricked into opening a file containing a virus delivered to his social media account[119], which allowed the criminal to access the artist's digital wallets. The artist reported that the hacker stole 40,000 Axie Infinity (AXS) tokens valued at US$4 million within minutes[120]. In a similar incident, in December 2021, an art curator and NFT collector reported that 16 of their NFT tokens were stolen in a phishing attack. NFTs worth about US$2.2 million were stolen from the collector's hot wallet[121].

Another category of scams involves giveaways or airdrops, in which the fraudsters lure victims by offering free NFTs. In this scam, a fake NFT account will send a message to users on social media such as Twitter telling them that they have won an NFT. Users are given a link to a fake NFT website, which will ask them to connect their crypto wallet and enter their seed phrase[122]. The criminals steal existing NFTs as well as other digital currencies or tokens stored in the wallet[123].

Protecting and defending against various threats in Web3 and the metaverse

The rapid growth of Web3 and the metaverse has offered a wide variety of opportunities for scammers, fraudsters and cybercriminals. These environments are rapidly becoming an emerging attack vector. There is the need for various participants to be aware of a wide variety of crimes and scams taking place in these environments and exercise necessary privacy and security precautions and other measures.

Consumers and investors

Consumers should understand different types of risks they are likely to face in Web3 and the metaverse environments. For instance, buying an NFT is different from buying things on e-commerce websites. There is little recourse for victims of NFT scams. There are often no refunds and little protections. Important risk sharing and transfer mechanisms such as insurance do not exist in Web3.

In light of the proliferation of a wide range of investment scams**,** it is important to undertake due diligence of investment schemes. For instance**,** investors can use Discord platform to understand the community behind the NFT project and get a feel for the project. Investors should interact with other members and follow topics of conversation. It is important to ask the creators questions about the project's technical aspects. The lack of substance in the discussion in the channels can raise a red flag. If the creators have a presence in the Discord channels and they respond with substance when someone ask questions, these may indicate that the project is genuine. People associated with a fake project may try to create distractions. It is also important to check if the project creator has an inflated social media following with a high proportion of fake Twitter followers. For instance, Followeraudit.com

(https://www.followeraudit.com/?ref=alternativeassets.club) can be used to track the number of active, inactive, and fake followers of a project.

A unique feature of the metaverse is the powerful immersion and rich interaction between users, devices, and software. Organizations can capture even more and richer data in Web2. Important tradeoffs need to be made to have the metaverse experience and ensure security and privacy.

The metaverse is viewed as a future technology created for kids. Concerns of online safety is likely to grow as the experience becomes more immersive. Child safety is thus important[124]. Parents need to take the initiative to enhance children's safety in the metaverse.

Organizational measures

As the metaverse involves far more sensitive PII data, issues such as data governance, endpoint security and network security become significantly more important. Businesses should protect themselves against possible threats by taking appropriate measures that are consistent with the nature of Web3 and the metaverse and threats faced. Web3 and metaverse security must become a key component of a company's overall cybersecurity strategy rather than an afterthought[125]. Organizations should pressure metaverse technology developers to incorporate security features[126].

It is important for companies to team up with strong cybersecurity partners to protect their digital assets in Web3 and the metaverse[127]. As mentioned, AI is one area in which perpetrators can effectively deceive users. Given AI's increasingly important role in Web3 and the metaverse, partnership with specialist firms that combine AI with human judgment[128] is critical.

Among best-practice organizations is metaverse gaming firm The Sandbox. The Sandbox allows users to monetize their activity on virtual lands recorded on blockchain. It has teamed up with online threat detection company BrandShield to strengthen the safety of crypto wallets and NFTs on its marketplace. BrandShield analyses and classifies various threats to eliminate crypto wallet attacks. It evaluates threat levels from different digital entities and platforms, such as websites and NFT marketplaces, which are rarely detected by traditional cybersecurity technology. The Sandbox said that BrandShield neutralized 120 phishing sites and 58 fake social media accounts impersonating the metaverse platform In March and April 2022. The Sandbox has also announced plans to educate its users about fraud prevention methods[129].

Implementations of Web3 and the metaverse often involve networks and partner ecosystems, which can expand the surface area of vulnerability[130]. Many bugs in smart contracts are associated with external interactions with other contracts. This means that even if the code for an application of a company is secure, the codes of other companies may be vulnerable, which can be exploited by attackers[131]. The high-profile hackings discussed above also underscore the importance and role of a third-party independent audit in order to ensure the security of the metaverse[132].

Fraudsters are also taking advantage of the lack of clear regulations regarding the ownership of an NFT versus the ownership of the physical or digital object represented by the NFT[133]. Scammers are creating and selling NFTs in the metaverse that falsely appear to be created by luxury brands. In the metaverse and gaming platform Roblox, brands such as Gucci, Stella McCartney and Nike have sold digital items. Users can also buy items that appear to be related to brands such as Burberry, Chanel, Prada, Dior and Louis Vuitton, despite the fact that these brands may not have participated in the creating or selling of most of the items[134]. For

instance, Disney's former chief executive officer and chairman Bob Iger noted that OpenSea had all the "poached" Disney-themed collectibles[135]. Owners of assets that can be minted to NFTs for the metaverse need to be vigilant and take appropriate measures to ensure that their assets have not been misused in the metaverse. In February 2022, Blockchain game company Animoca Brands published a statement about the fake token that was being offered with the name "Animoca Brands Metaverse".[136] As of February 17, 2022, the token had appeared on Block Explorer and Analytics Platform Etherscan and on decentralized crypto trading platform UniSwap V2. As of that day, the token had 53 holders and there were 83 transfers[137].

Industry level initiatives

In many cases, a company cannot singly address all the requirements of security in Web3 and the metaverse. Firms thus should act jointly at the industry level. For instance, with the emergence of the metaverse, it is important to have built in safety features. Leading metaverse developers have important roles to play.

Industry-level initiatives need to be taken to develop mechanisms to verify and validate intellectual property created, bought and sold to a real-world identity. For instance, industry bodies can engage in lobbying and other activities to pressure their governments to enact new regulations. Likewise, in order to ensure legitimacy of a virtual avatar, it is important to associate it to a distinct real-world identity using enhanced biometric data and other verification methods[138]. Especially with the emergence of multiple metaverses, it is important to close the current governance and verification gaps or silos between them[139].

Regulators

Many of the current challenges of Web3 and the metaverse can partially be attributed to underdeveloped regulations and guidelines. For instance, there is no clear answer as to

whether the sales of branded digital items are legal if the brand did not participate in creating them. The fact that scammers are selling NFTs that falsely appear to be created by luxury brands has raised questions around ownership and legality. It is thus important for governments to enact regulations to protect intellectual property rights in Web3 and the metaverse.

The lack of boundary in the metaverse makes it difficult to establish jurisdiction and apply regulations such as the GDPR. International coordination and cooperation are thus even more important to tackle metaverse security. Governments should also hold metaverse technology developers accountable for unsafe metaverse technologies[140].

Conclusion

The Web3 and metaverse ecosystems involve a number of complex mechanisms and interconnected key elements that rely on centralized Web2 technologies, which have their own security challenges. They have created many questions related to security and privacy. This paper identified some of the main threats that the Web3 and metaverse ecosystems face.

A wide range of fraudulent acts are likely to exploit flaws in Web3 and the metaverse, which provide a number of avenues for criminals to victimize users of these technologies. While hacking skills are require for some crimes, only social engineering are sufficient to victimize targets in others. For instance, NFT platforms face protocol risks such as hacking. Exchanges which facilitate the trading of cryptocurrencies and NFTs (e.g., OpenSea) have their own vulnerabilities, which can be exploited by hackers. Other malevolent actors rely on novel but simple social engineering *scams* to convince victims to invest in fake schemes involving NFTs or to divulge sensitive information that can be used to breach crypto accounts.

In general, security breaches and privacy violations associated with Web3 and metaverse have more adverse consequences than in the Web2 era. Users in the metaverse also face a higher susceptibility to manipulation by businesses. Law enforcement agencies are also likely to face challenges in fighting crimes at scale in Web3 and the metaverse, especially in the initial phase of development.

It is important to note some key points about blockchain, the main building block of Web3 and the metaverse. The so-called trilemma discussed above maintains that blockchain cannot simultaneously achieve security, decentralization and scalability. It is clear from the above discussion that while bridges have promoted scalability, they perform poorly in security. Moreover, public blockchains are transparent, which means that transactions are available for everyone to see. This means that the criminals know exactly their payoffs if their attacks are successful.

References

[1] M. Galash. Web3 is not dead. Here's what the crypto space will look like in 2030, June 7, 2022 https://fortune.com/2022/06/07/web3-crypto-crash-tech-finance-price-future-outlook-coinchange-maxim-galash/

[2] Groopman, J. (2022) "Top 3 Web3 security and business risks" https://www.techtarget.com/searchsecurity/tip/Top-3-Web3-security-and-business-risks (March 2022)

[3] Rob Pegoraro "Why Is Web3 Security Such a Garbage Fire? Let Us Count the Ways A Black Hat talk unpacks how blockchain-based projects can break so easily and inflict such catastrophic damage." August 12, 2022 https://www.pcmag.com/news/why-is-web3-security-such-a-garbage-fire-let-us-count-the-ways

4 Matt Haldane and Xinmei Shen 2022. Taiwan's Digital Affairs ministry turns to Web3 to guard against mainland China cyberattacks following Pelosi's visit11 August https://www.scmp.com/tech/tech-trends/article/3188434/taiwans-digital-affairs-ministry-turns-web3-guard-against-mainland

5 Matt Haldane and Xinmei Shen 2022. Taiwan's Digital

6 Matt Haldane and Xinmei Shen 2022. Taiwan's Digital

[7] Savannah Fortis 2022. Web3 helps Taiwan secure information against cyberattacks, August 11, https://cointelegraph.com/news/web3-helps-taiwan-secure-information-against-cyberattacks

[8] Rob Pegoraro "Why Is Web3"

[9] Groopman, J. (2022) "Top 3 Web3 security and business risks" https://www.techtarget.com/searchsecurity/tip/Top-3-Web3-security-and-business-risks (March 2022)

[10] Roberts, J (2022) "Web3 Is Supposed to Be Secure. What About All These Hacks?" https://decrypt.co/96727/web3-is-supposed-to-be-secure-what-about-all-these-hacks (2nd April, 2022)

[11] Security, cybercrime, and scale Author: Cormac Herley Authors Info & Claims Communications of the ACMVolume 57Issue 9September 2014 pp 64–71

[12] Dobos, L. (2022) “Axie Infinity Ronin bridge hacker moved 2000 ETH to the Tornado Cash tumbler” https://cryptoslate.com/ronin-hacker-moved-2000-eth-to-the-tornado-cash-tumbler/ (4th April 2022)

[13] Roth, S. “An Introduction to Sidechains” https://www.coindesk.com/learn/an-introduction-to-sidechains/

[14] Ethereum. (2022) “SIDECHAINS” https://ethereum.org/en/developers/docs/scaling/sidechains/ (2nd March 2022)

[15] Andrew Gazdecki “Sidechains: How To Scale And Improve Blockchains, Safely” Forbes Nov 27, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/11/27/sidechains-how-to-scale-and-improve-blockchains-safely/?sh=2afbf5834418

[16] The Straits Times (2022)“Cryptocurrency-bridge hacks top $1.36 billion in little over a year” https://www.straitstimes.com/tech/tech-news/cryptocurrency-bridge-hacks-top-136-billion-in-little-over-a-year (5th April 2022)

[17] Nambiampurath , R. (2022) “Ronin Hack Demonstrates the Dangers of Increasing Centralization in DeFi” https://www.fxempire.com/forecasts/article/ronin-hack-demonstrates-the-dangers-of-increasing-centralization-in-defi-953956 (31st March 2022)

[18] Tim Bradshaw 2022. Makers of Axie Infinity game raise $150mn after massive crypto hack, April 6, https://www.ft.com/content/a30186d7-5dd7-47cd-8f33-de0cffd3d500

[19] Peaster, V. “Analyzing the Ronin bridge hack” https://newsletter.banklesshq.com/p/analyzing-the-ronin-bridge-hack?s=r (29th March)

[20] Ronin. (2022) “After Axie Infinity Hack, Will other Play-2-Earn Games Be Hacked Soon?” https://www.financemagnates.com/thought-leadership/after-axie-infinity-hack-will-other-play-2-earn-games-be-hacked-soon/ (4th May 2022)

[21] Orland, K. (2022) “Axie Infinity raises $150M to help reimburse hacked user funds” https://arstechnica.com/gaming/2022/04/axie-infinity-raises-150m-to-help-reimburse-hacked-user-funds/ (4th July 2022)

[22] https://www.scmagazine.com/analysis/application-security/cryptocurrency-exchanges-thrown-another-curve-with-recent-dns-attack

[23] https://decrypt.co/resources/cybersecurity-in-web3-protecting-yourself-and-your-ape-jpeg

[24] Credit Suisse 2022. Metaverse: A Guide to the Next-Gen Internet https://www.credit-suisse.com/media/assets/corporate/docs/about-us/media/media-release/2022/03/metaverse-14032022.pdf

[25] “Data Privacy and Virtual Reality (VR)” June 10, 2021, https://wirewheel.io/blog/privacy-ai/

[26] Vanita Pandey How Attackers Target the Metaverse February 8, 2022. https://securityboulevard.com/2022/02/how-attackers-will-target-the-metaverse-in-2022-and-beyond/

[27] https://nordvpn.com/blog/metaverse-survey/

[28] Rahul Nambiampurath, “Hackers Stole Over $1.22 Billion From DeFi Market This Year Alone” 5 April 2022, https://beincrypto.com/hackers-stole-over-1-22-billion-from-defi-market-this-year-alone/

[29]Olga Kharif “Crypto-Bridge Hacks Reach Over $1 Billion in Little Over a Year”, March 30, 2022, https://www.bloomberg.com/news/articles/2022-03-30/crypto-bridge-hacks-reach-over-1-billion-in-little-over-a-year

[30] “Metaverse: Open for business? As the opportunities for metaverse start to emerge, companies are taking their first steps into a brave new world”. June 27, 2022 https://www.technologyreview.com/2022/06/27/1054974/metaverse-open-for-business/

[31] Franceschi-Bicchierai , L. (2022) “‘Web3’ Needs Hackers More Than Anything Else Right Now” https://www.vice.com/en/article/93bnvd/web3-needs-hackers-more-than-anything-else-right-now (10th January 2022)

[32] Jeff Goldman “How Secure Is Solana, Really? Industry Analysts Weigh in” 9 Aug 2022 https://thenewstack.io/how-secure-is-solana-really-industry-analysts-weigh-in/

[33] Roberts, J (2022) “Web3 Is Supposed to Be Secure. What About All These Hacks?” https://decrypt.co/96727/web3-is-supposed-to-be-secure-what-about-all-these-hacks (2nd April, 2022)

[34] M. Galash. Web3 is not dead. Here’s what the crypto space will look like in 2030, June 7, 2022 https://fortune.com/2022/06/07/web3-crypto-crash-tech-finance-price-future-outlook-coinchange-maxim-galash/

[35] T. Nolle “What Web3 and the Metaverse Have to Do With One Another” May 09, 2022, https://www.nojitter.com/enterprise-networking/what-web3-and-metaverse-have-do-one-another

[36] David Fairman “4questions every CISO should be asking about the metaverse” April 22, 2022, https://techcrunch.com/2022/04/22/4-questions-every-ciso-should-be-asking-about-the-metaverse/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALXikk7Qx1YcZMZJ-62NUvOdAxL9JUTkJzEzlQWPmwTNH-lIX0Zwar1ePk_Z9ZolNII1uXpBv3hw4eWHXVxl7UBCZslc46A7ZXwtCvEBf5xvZEEjpLkRvXLSwrxjo-b7ISUQ05sl5QehqrroGR-GA6C3fzLm-fwFUdNBVe0F-_q_

[37] Claburn, T. (n.d.). *Study outlines privacy risks in metaverse virtual worlds*. [online] www.theregister.com. Available at: https://www.theregister.com/2022/07/29/metaverse_privacy_study/

[38] L. Dobberstein “Metaverse privacy maturity lags enthusiasm for new virtual worlds” 2 June, 2022 https://www.theregister.com/2022/06/02/metaverse_privacy_immature/

[39] Metinko, C. (2021) “Venture Investment In Cryptosecurity Jumps 10x Over Last Year As Sector Hits Sweet Spot With Venture Capitalists” https://news.crunchbase.com/news/crypto-security-startups-vc-investment/ (17th August, 2021)

[40] Dawkins, R. (1982).The extended phenotype. Oxford University Press, New York.

[41] De Jong, W. M. (2001). “Manipulative tactics in budgetary games: The art and craft of getting the money you don’t deserve,” Knowledge, Technology & Policy, 14(1), 50–66.

[42] L. Dobberstein “Metaverse privacy maturity lags enthusiasm for new virtual worlds” 2 June, 2022 https://www.theregister.com/2022/06/02/metaverse_privacy_immature/

[43] “‘Ice phishing’ on the blockchain” February 16, 2022 , https://www.microsoft.com/security/blog/2022/02/16/ice-phishing-on-the-blockchain/

[44] Syuzanna Papazyan “ What is an “Ice Phishing” attack?” March 22, 2022 https://powerdmarc.com/what-is-ice-phishing-attack/

[45] “BadgerDAO Exploit Technical Post Mortem” https://badger.com/technical-post-mortem

[46] Charlie Osborne, February 17, 2022 “Microsoft warns of emerging 'ice phishing' threat on blockchain, DeFi networks” https://www.zdnet.com/article/microsoft-warns-of-ice-phishing-on-blockchain-networks/

[47] Evil twins and digital elves: How the metaverse will create new forms of fraud and deception https://bigthink.com/the-future/metaverse-fraud-digital-twins/

[48] “Metaverse: Open for business? As the opportunities for metaverse start to emerge, companies are taking their first steps into a brave new world”. June 27, 2022 https://www.technologyreview.com/2022/06/27/1054974/metaverse-open-for-business/

[49] Charlie Bell The metaverse is coming. Here are the cornerstones for securing it. Mar 28, 2022, https://blogs.microsoft.com/blog/2022/03/28/the-metaverse-is-coming-here-are-the-cornerstones-for-securing-it/

[50] Alspach, K. (2022) Why the fate of the metaverse could hang on its security https://venturebeat.com/2022/01/26/why-the-fate-of-the-metaverse-could-hang-on-its-security/ 26 January

[51] Vellante, D. (2022) Cybersecurity, blockchain and NFTs meet the metaverse, 17 January 2022, https://siliconangle.com/2022/01/17/cybersecurity-blockchain-nfts-meet-metaverse/

[52] Laura Dobberstein Metaverse privacy maturity lags enthusiasm for new virtual worlds 2 Jun 2022. https://www.theregister.com/2022/06/02/metaverse_privacy_immature/

[53] Thompson, D. (2022) Virtual Metaverse: Real Vulnerability, January 11 https://www.techtimes.com/articles/270383/20220111/virtual-metaverse-real-vulnerability.htm

[54]Mike Elgan Will the Metaverse Usher in a Universe of Security Challenges? February 7, 2022, https://www2.deloitte.com/us/en/insights/industry/technology/web3-and-metaverse-the-future-of-the-internet.html

[55] Rahimi, S. K., & Haug, F. S. (2010). Distributed Database Management Systems: A Practical Approach Wiley-Blackwell

[56] OWASP (2021b). Top 10 Web Application Security Risks https://owasp.org/www-project-top-ten/

[57] Madou, M. (2022). The Cybersecurity Issues We Can't Ignore in 2022, 2 February 2022) https://www.infosecurity-magazine.com/opinions/cybersecurity-issues-cant-ignore/

[58] OWASP (2021a). What's changed in the Top 10 for 2021 Open Web Application Security Project (OWASP) https://owasp.org/Top10/

[59] A. Wang, "*The NFT scammers are here"*. The Verge. September 21, 2021, https://www.theverge.com/22683766/nft-scams-theft-social-engineering-opensea-community-recovery

[60] K. Rees. "*The 5 Biggest NFT Scams and How to Avoid Them*" October 21, 2021 https://www.makeuseof.com/biggest-nft-scams-how-to-avoid/

[61] Lau, P. L. (2022). The metaverse: three legal issues we need to address Published: February 1, , https://theconversation.com/the-metaverse-three-legal-issues-we-need-to-address-175891

[62]. Building Safe Playgrounds for the Legal Metaverse, May 13, 2022, https://www.jdsupra.com/legalnews/building-safe-playgrounds-for-the-legal-7246843/

[63] Groopman, J. (2022) "Top 3 Web3 security and business risks" https://www.techtarget.com/searchsecurity/tip/Top-3-Web3-security-and-business-risks (March 2022)

[64]. Building Safe Playgrounds for the Legal Metaverse, May 13, 2022, https://www.jdsupra.com/legalnews/building-safe-playgrounds-for-the-legal-7246843/

[65] Groopman, J. (2022) "Top 3 Web3"

[66]. Building Safe Playgrounds for the Legal Metaverse, May 13, 2022, https://www.jdsupra.com/legalnews/building-safe-playgrounds-for-the-legal-7246843/

[67] Joanna England "Security in the Metaverse and What Banks Need to Know" May 20, 2022, https://fintechmagazine.com/banking/security-in-the-metaverse-what-banks-need-to-know

[68] Groopman, J. (2022) "Top 3 Web3"

[69] https://www.insurancejournal.com/news/national/2022/11/16/695318.htm

[70] ISACA.(2014). *Generating value from big data analytics* [White paper]. Information Systems Audit and Control Association, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Generating-Value-From-Big-Data-Analytics.aspx

[71] Leon Hady "The Metaverse is a Huge Opportunity for Education. Big Tech Must Not Ruin It ", 04/06/22, HTTPS://WWW.NEWSWEEK.COM/METAVERSE-HUGE-OPPORTUNITY-EDUCATION-BIG-TECH-MUST-NOT-RUIN-IT-OPINION-1693962

[72] Allen, K. (2022). *Metaverse Privacy: Fact or Fiction?* [online] Acceleration Economy. Available at: https://accelerationeconomy.com/metaverse/metaverse-privacy-fact-or-fiction/

[73] Oriana Alexander, Wail Jihadi and Bryan Parker, "Cybersecurity, Privacy and Constitutional Concerns: Risks to Know Before Entering the Metaverse", March 29, 2022 , https://www.law.com/legaltechnews/2022/03/29/cybersecurity-privacy-and-constitutional-concerns-risks-to-know-before-entering-the-metaverse/?slreturn=20220714213359

[74]Tom Wheeler, " If the Metaverse Is Left Unregulated, Companies Will Track Your Gaze and Emotions", June 20, 2022, https://time.com/6188956/metaverse-is-left-unregulated-companies-will-track-gaze-emotions/

[75] Brady Macdonald "4 ways technology powers the Disneyland 'metaverse'" : November 18, 2020 https://www.ocregister.com/2020/11/18/4-ways-technology-powers-the-disneyland-metaverse/

[76] Jeremy Greenberg "Brain-Computer Interfaces: Privacy And Ethical Considerations For The Connected Mind," September 21, 2021 https://fpf.org/blog/brain-computer-interfaces-privacy-and-ethical-considerations-for-the-connected-mind/

[77] Oriana Alexander, Wail Jihadi and Bryan Parker, "Cybersecurity, Privacy and Constitutional Concerns: Risks to Know Before Entering the Metaverse", March 29, 2022, https://www.law.com/legaltechnews/2022/03/29/cybersecurity-privacy-and-constitutional-concerns-risks-to-know-before-entering-the-metaverse/?slreturn=20220714213359

[78] https://observer.com/2020/07/nextmind-ces-brain-sensing-interface-developer-kit-preorder-open/

[79] Sissi Cao Snap's Latest Acquisition Is a Bet on a Metaverse Controlled By Thoughts, 03/24/22. https://observer.com/2022/03/snap-acquire-nextmind-brain-computer-interface-metaverse/

[80] Jeremy Greenberg "Brain-Computer Interfaces: Privacy And Ethical Considerations For The Connected Mind," September 21, 2021 https://fpf.org/blog/brain-computer-interfaces-privacy-and-ethical-considerations-for-the-connected-mind/

[81] Bonifacic, I. (2021) 'Project Cambria' is a high-end VR headset designed for Facebook's metaverse https://techcrunch.com/2021/10/28/project-cambria-is-a-high-end-vr-headset-designed-for-facebooks-metaverse/ 28 October

[82] Hunter, T. (2022) Surveillance will follow us into 'the metaverse,' and our bodies could be its new data source, January 13, https://www.washingtonpost.com/technology/2022/01/13/privacy-vr-metaverse/

[83] Merre, R. (2022). Security Will Make Or Break The Metaverse, March 24, https://www.nasdaq.com/articles/security-will-make-or-break-the-metaverse

[84] Casey, P., Baggili, I., & Yarramreddy, A. (2021) Immersive Virtual Reality Attacks and the Human Joystick, IEEE Transactions on Dependable and Secure Computing, 18 (2), pp. 550-562

[85] A. Krishna "Top metaverse cybersecurity challenges to consider" June 2022, https://www.techtarget.com/searchsecurity/tip/Top-metaverse-cybersecurity-challenges-to-consider

[86] A. Krishna "Top metaverse "

[87] Nichols, S. (2022) Metaverse rollout brings new security risks, challenges https://www.techtarget.com/searchsecurity/news/252513072/Metaverse-rollout-brings-new-security-risks-challenges?utm_campaign=20220209_Metaverse+brings+new+security+challenges+to+businesses%3B+Plus%2C+manual+vs.+automated+pen+testing&utm_medium=EM&utm_source=NLN&track=NL-

[88] Mike Orcutt, "Once hailed as unhackable, blockchains are now getting hacked" (19 February 2019), online: MIT Technology Review <https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/>

[89] Quantstamp. (2019) "What is a Re-Entrancy Attack?" https://quantstamp.com/blog/what-is-a-re-entrancy-attack (19th August 2019)

[90] NewsBTC "Hacking Attacks: Ethereum vs Terra Flash Loans" https://www.newsbtc.com/news/company/hacking-attacks-ethereum-vs-terra-flash-loans/

[91] CoinMarketCap Alexandria. (n.d.). *Blockchain Trilemma | CoinMarketCap*. [online] Available at: https://coinmarketcap.com/alexandria/glossary/blockchain-trilemma.

[92] Haig, S. (2022) "Vitalik Sounds Alarm on Security of Cross-chain Bridges" https://thedefiant.io/vitalik-eth-cross-chain-bridges-security/ (11th January, 2022)

[93] Krakenfx. (2021) "Abusing Smart Contracts to Steal $600 million: How the Poly Network Hack Actually Happened" https://blog.kraken.com/post/11078/abusing-smart-contracts-to-steal-600-million-how-the-poly-network-hack-actually-happened/ (22nd September 2021)

[94] Ghosh, M. (2021)"Chinese DeFi platform Poly Network suffers US$600M hack" https://forkast.news/chinese-defi-poly-network-suffers-us600m-hack/ (11th August 2021)

[95] Blockchain vulnerabilities - crypto hacks, blockchain forensics and legal challenges Blog Techlex McCarthy Tétrault LL, November 19 2021 https://www.lexology.com/library/detail.aspx?g=d149175e-e73b-4b49-855a-54df7ddbb34c

[96] Brown, R. "Crypto platform hit by $600 million heist asks hacker to become its chief security advisor" https://www.cnbc.com/2021/08/17/poly-network-cryptocurrency-hack-latest.html?&doc=106930374

[97] https://www.infosecurity-magazine.com/news/poly-network-hacker-returns/

[98] M. Fox, “The NFT market is now worth more than $7 billion, but legal issues facing the nascent sector could hinder its growth, JPMorgan says” November 19, 2021, https://markets.businessinsider.com/news/currencies/nft-market-worth-7-billion-legal-issues-could-hinder-growth-2021-11

[99] Menghan Xiao_“Web3’s complexity a challenge for security as adoption of ‘the new internet’ grows ”August 3, 2022, https://www.scmagazine.com/analysis/zero-trust/web3s-complexity-a-challenge-for-security-as-adoption-of-the-new-internet-grows

[100] Dyma Budorin Web3 hacks equal San Marino’s GDP: Are audits the soft spot of the industry? August 09, 2022 https://www.datacenterdynamics.com/en/opinions/web3-hacks-equal-san-marinos-gdp/

[101] 2022 Q2 Web3 Security Report https://static.footprint.network/report/Q2_2022_Web3_Security_Report.pdf

[102] Wise, A. (2022). *Explainer: What to know about crypto mixer Tornado Cash*. [online] Protos. Available at: https://protos.com/explainer-what-to-know-about-crypto-mixer-tornado-cash/

[103] Kuhn, D. (2022). *An Alleged Tornado Cash Developer Was Arrested. Are You Next?* [online] www.coindesk.com. Available at: https://www.coindesk.com/layer2/2022/08/12/an-alleged-tornado-cash-developer-was-arrested-are-you-next/#:~:text=We%20know%20Tornado%20Cash%20is

[104] U.S. Department of the Treasury. (2022.). *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*. [online] Available at: https://home.treasury.gov/news/press-releases/jy0916.

[105] McCarthy Tétrault LL, Blockchain vulnerabilities - crypto hacks, blockchain forensics and legal challenges Blog Techlex November 19 2021 https://www.lexology.com/library/detail.aspx?g=d149175e-e73b-4b49-855a-54df7ddbb34c

[106] Ryan Browne Hacker behind $600 million crypto heist returns final slice of stolen funds, August 24 2021, https://www.cnbc.com/2021/08/23/poly-network-hacker-returns-remaining-cryptocurrency.html#:~:text=Hacker%20behind%20%24600%20million%20crypto%20heist%20returns%20final%20slice%20of%20stolen%20funds,-Published%20Mon%2C%20Aug&text=Cryptocurrency%20platform%20Poly%20Network%20was,nearly%20all%20of%20the%20money.

[107] Brown, R. “Crypto platform hit by $600 million heist asks hacker to become its chief security advisor” https://www.cnbc.com/2021/08/17/poly-network-cryptocurrency-hack-latest.html?&doc=106930374

[108] Coble, S. (2021). *Poly Network Hacker Returns Remaining Funds*. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/news/poly-network-hacker-returns/

[109] K. J. Brooks “Nike's new NFT sneakers selling for more than $100,000” April 28, 2022 https://www.cbsnews.com/news/nike-cryptokicks-nft-blockchain-metaverse-rtfkt/

[110] L. Keller “Does content moderation on platforms like OpenSea amount to censorship?”, December 17, 2021, https://forkast.news/does-opensea-censor-nft-content/

[111] I. Novikov, “The Three Layers Of Cryptocurrency Security” May 3, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/05/03/the-three-layers-of-cryptocurrency-security/?sh=12e0ec3e29aa

[112]“$100,000 worth of NFTs disappear forever, thanks to OpenSea bug Cryptocurrency” September 09, 2021 https://www.investing.com/news/cryptocurrency-news/100000-worth-of-nfts-disappear-forever-thanks-to-opensea-bug-2611477

[113] Gizmodo. (2021, March 28). *Gullible OpenSea Users Were Vulnerable to “Malicious NFT” Attacks, Researchers Say*. [online] Available at: https://gizmodo.com/gullible-opensea-users-were-vulnerable-to-malicious-nft-1847850437

[114] T. Locke “The Bored Ape Yacht Club metaverse sale was such a mess that it tanked the price of Bored Ape NFTs by 25%” May 6, 2022. https://fortune.com/2022/05/06/bored-ape-yacht-club-nfts-fall-after-metaverse-land-sale/

[115] These are NFTs that are believed to be able to retain their values into the future

[116] J. Neal “Beware: This Fake BAYC Metaverse Land NFT Exploits OpenSea Bug” April 3, 2022, https://nftevening.com/beware-this-fake-bayc-metaverse-land-nft-exploits-opensea-bug/

[117] Merre, R. (2022). Security Will Make Or Break The Metaverse, March 24, https://www.nasdaq.com/articles/security-will-make-or-break-the-metaverse

[118] Trend Micro News. (2022). *[NFT Scam] Fake MetaversePRO Website*. [online] Available at: https://news.trendmicro.com/2022/02/24/nft-scam-fake-metaversepro-website/

[119] K. Crow,” *NFT art the latest target for online fraudsters*” August 26, 2021 https://www.fnlondon.com/articles/nft-art-the-latest-target-for-fraudsters-20210826

[120] S. Millare “Four Tips for NFT Artists to Protect Themselves from Hacking and Online” 2 July 2021 https://bitpinas.com/feature/four-tips-for-nft-artists-to-protect-themselves-from-hacking-and-online-theft/

[121] V. Chawla “Bored Ape NFT Collector Loses $2.2M in Phishing Scam,” December 31, 2021, https://cryptobriefing.com/bored-ape-nft-collector-loses-2-2m-in-phishing-scam/

[122] K. Rees. “*The 5 Biggest NFT Scams and How to Avoid Them*” October 21, 2021 https://www.makeuseof.com/biggest-nft-scams-how-to-avoid/

[123] L. Alex. “*Evaluating NFTs: How to Know Whether an NFT Project is Legit*” October 9, 2021, https://cryptonews.com/exclusives/evaluating-nfts-how-to-know-whether-an-nft-project-is-legit.html

[124]Y. Smart, “What are the key metaverse safety concerns and how can brands respond?”, August 18, 2022, https://www.thedrum.com/profile/the-insights-family/news/what-are-the-key-metaverse-safety-concerns-and-how-can-brands-respond

[125]David Howell “What is metaverse security?”, 9 Jun 2022 https://www.itpro.co.uk/security/368221/what-is-metaverse-security

[126]Y. Smart, “What are the”

[127] The metaverse: Who will be securing it — and how? Reinhard Blaukovitsch, December 20, 2021 https://venturebeat.com/2021/12/20/the-metaverse-who-will-be-securing-it-and-how/

[128] Works, F. (2022). *How to establish a safe, secure metaverse from the ground up*. [online] Fast Company. Available at: https://www.fastcompany.com/90771773/how-to-establish-a-safe-secure-metaverse-from-the-ground-up

[129] Malwa, S. (2022). *The Sandbox Brings on Security Firm BrandShield to Prevent Rising NFT Fraud*. [online] www.coindesk.com. Available at: https://www.coindesk.com/business/2022/07/20/the-sandbox-brings-on-security-firm-brandshield-to-prevent-rising-nft-frauds/

[130]Mike Elgan Will the Metaverse Usher in a Universe of Security Challenges? February 7, 2022, https://www2.deloitte.com/us/en/insights/industry/technology/web3-and-metaverse-the-future-of-the-internet.html

[131] Franceschi-Bicchierai , L. (2022) “‘Web3’ Needs Hackers More Than Anything Else Right Now” https://www.vice.com/en/article/93bnvd/web3-needs-hackers-more-than-anything-else-right-now (10th January 2022)

[132]Mayank Sharma “Banking in the Metaverse Seems Like a Gimmick, Experts Say: At least for now” April 4, 2022, https://www.lifewire.com/banking-in-the-metaverse-seems-like-a-gimmick-experts-say-5224734

[133] M. Fox, “The NFT market is now worth more than $7 billion, but legal issues facing the nascent sector could hinder its growth, JPMorgan says” November 19, 2021, https://markets.businessinsider.com/news/currencies/nft-market-worth-7-billion-legal-issues-could-hinder-growth-2021-11

[134] M. Mcdowell “ The ‘Baby Birkin’ NFT and the legal scrutiny on digital fashion,” June 15, 2021, https://www.voguebusiness.com/technology/the-baby-birkin-nft-and-the-legal-scrutiny-on-digital-fashion

[135] Dailey, N. (2022) “Ex-Disney Chairman Bob Iger expects NFTs to explode and hints at the media conglomerate's push into the metaverse” https://markets.businessinsider.com/news/currencies/bob-iger-predicts-nft-explosion-disney-push-into-metaverse-2022-2 (1st February 2022)

[136]Yiğithan Demirçin Animoca Brands warns users of fake metaverse token “Animoca Brands Metaverse” February 22, 2022, https://mobidictum.biz/animoca-brands-warns-users-of-fake-metaverse-token/

[137] “Animoca Brands Warns of Fake Metaverse Token Attempted Sale” February 17, 2022 https://play2moon.com/animoca-brands-warns-of-fake-metaverse-token-attempting-sale/#:~:text=The%20company%20behind%20The%20Sandbox%20warned%20about%20attempted%20sales%20of,propagate%20it%20and%20scam%20users.

[138] Alan Smith, Bhavik Domadia, and Derrick Wang, The metaverse: Tech game-changer or security nightmare?, *May 17, 2022* https://www.securitymagazine.com/articles/97635-the-metaverse-tech-game-changer-or-security-nightmare

[139] “Metaverse: Open for business? As the opportunities for metaverse start to emerge, companies are taking their first steps into a brave new world”. June 27, 2022 https://www.technologyreview.com/2022/06/27/1054974/metaverse-open-for-business/

[140]Y. Smart, “What are the”