Evolution of the Internet from Web 1.0 to Metaverse: The Good, The Bad and The Ugly

SUBMISSION DATE / POSTED DATE

11-05-2022 / 16-05-2022

DOI

10.36227/techrxiv.19743676.v1

Evolution of the Internet from Web 1.0 to Metaverse: The Good, The Bad and The Ugly

Keshab Nath
Department of Computer Science and Engineering
Indian Institute of Information Technology, Kottayam
Kerala, India, 686635.
E-mail: keshabnath@iiitkottayam.ac.in

***Abstract*—The World Wide Web as the largest global information media through which user can share, read, and writes data through computers connected with internet. In last few years, internet has had much progress from web1.0 to web 3.0. The first iteration of the web or web 1.0, also known as the Classic Web, arrived in 1991. Web1.0 was all about connecting and getting information on the net. Then came web 2.0, enabling users to read as well as create and deliver content. Due to the read and write functionalities of web 2.0, there was an immense growth in the on the internet, specially in social media alongside E-commerce. Web3.0 is generally regarded as the emergence of the semantic web, where computer will generating and thinking new information rather than humans. Using artificial intelligence and machine learning technologies, users will be able to interact with data. The Metaverse is the future iteration of the internet. It will combines multiple different virtual spaces that provides access to a diverse variety of entertainment and projects utilizing the full range of augmented reality.**

***Index Terms*—Web1.0, Web2.0, Web3.0, Metaverse, Augmented reality, 3D universe, Virtual space, Privacy and Security, Data confidentiality**

I. Introduction

The internet and the web is not synonymous both are two separate but related thing. Internet is simply a network of networks where millions of computer are globally connected forming a network in which any computer can communicate with any other computer. World Wide Web is a way of accessing information over the medium of the internet by displaying web pages on a browser, information are connected by hyperlinks, can contains text, graphics, audio, video.

Web1.0 is the first generation of the web, also known as informational web, which developed from 1991 onwards, following its invention by Tim Berners-Lee in 1989-1991. Users can only read and share information on web pages in this environment. Web 1.0 was essentially an information source created by a small number of authors for a large number of relatively oblivious users. It mostly consisted of static webpages with little room for genuine interactivity. Web2.0 is the environment in which we can create, share, and modify the content.The term Web 2.0 first came into use in 1999 as the Internet pivoted toward a system that actively engaged the user. The term Web 2.0 became notable after the first O'Reilly Media Web 2.0 conference in 2004 [11]. Web 3.0 is the third generation of the internet where websites and apps will be able to process information in a smart human-like way through technologies like machine learning (ML), Big Data, decentralized ledger technology (DLT), etc. Web 3.0 was originally called the Semantic Web by World Wide Web inventor Tim Berners-Lee, and was aimed at being a more autonomous, intelligent, and open internet.

Along with the evolution of the web3.0, large tech platforms look towards the augmented reality as the next computing platform shift. The blending of elements of the physical and digital worlds via virtual reality, augmented reality, gaming and immersive online communities is contributing to the rise of a more decentralized Web 3.0. As a result, the fusion of several technologies including software, hardware devices, and AR/VR/MR along with special sound and geospatial capabilities create a new era of technology called metaverse.

II. Web1.0 to Web3.0- Evolution of the Internet

The first iteration of the web represents the web 1.0, which, according to Berners-Lee, is the "*read-only web*". Web 1.0 began as an information place for businesses to broadcast their information and only allowed users to search for information and read it through web pages. Here user cannot interact with the content of the page (no comments, no responses, no quotes, etc).

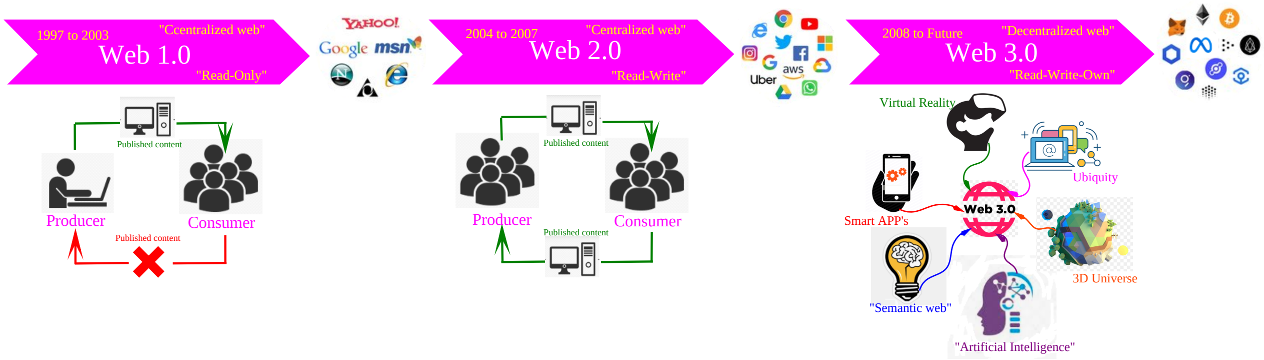


Fig. 1. Web1.0 to Web3.0- Evolution of the Internet

A. *The Good About Web 1.0*

It has single access, which means that only the content creator can make changes to it. As a result, without the creator's permission, the contents are left untouched. Student autonomy, authentic materials and scenarios, multiliteracies exposure, and a limited level of interactivity are all advantages of web 1.0.

B. *The Bad About Web 1.0*

Web applications, particularly dynamic web applications, require a high level of interactivity. We may require auto refresh content retrieved from a database, which will allow users to access updated content in seconds. Because this type of interactivity is critical for applications, Web 1.0 failed in this area, allowing only clicks and page refreshes. Rich user experiences will not be possible with Web 1.0, and we will have to refresh every time we want to check the content. Additionally, Web 1.0 applications could not be loaded in mobile browsers (which is called WAP browsing). This is yet another drawback of Web 1.0 technology.

C. *The Ugly About Web 1.0*

Web 1.0, with the vast majority of users being content consumers. To create their website, the creators needed access to a server, need strong programming skills, and have to write large and complex code for creating contents. Moreover, in web1.0, the data can't be edited by users, and the audience can't interact with it. As a result, there is less traffic on the internet and less advertising. Advertisers are looking for new ways to connect with their target audiences using traditional media.

To be more specific, Web 1.0 is a simple information portal in which users receive information without having the opportunity to post, review, or provide feedback. It's primarily a closed website that isn't very user-friendly. When it comes to defining web 2.0, there are a few things to consider. The term refers to internet applications that allow people to share and collaborate while also allowing them to express themselves online. Instead of web1.0, web2.0 allows users to not only read but also write, modify, and update content online. It also encourages collaboration and helps to gather collective intelligence.

D. *The Good About Web 2.0*

Web 2.0 facilitates great user interaction by allowing users to easily navigate through options. Web 2.0 technology, such as social networks, blogs, forums, and Second Life, could be used to achieve this simple and effective way of publicising things.

Web 2.0 technologies allow a teacher to become a facilitator of learning rather than a distributor of information. It has the potential to create more interactive and powerful learning environments in which learners can create, produce, edit, and evaluate knowledge [14]. Web 2.0 facilitates social interactions and collaboration among students, teachers, subject matter experts, professionals from various fields, and a variety of others who share common interests. With the introduction of Web 2.0 technologies, a paradigm shift has occurred from teachers and teaching to students and learning [1], resulting in "student-centered" learning [4].

Advertising on electronic media can be expensive, but using Web 2.0 technologies such as web blogs and social networks, we can reach thousands of people for less than a dollar. Companies have gained business benefits in several areas of operation as a result of using Web 2.0 technologies. It is now easier to conduct business due to improved ability to share ideas, increased access to knowledge experts, and lower costs of communication technologies, travel, and operations. Web2.0 tools have also reduced the amount of time needed for marketing and expanded the marketing domain's scope. It enables businesses to more easily disseminate product information and, perhaps more importantly, to invite customer feedback and even participation in product development. The explosion of online business, or e-commerce, has resulted from Web 2.0. This prompted a number of companies to launch e-commerce ventures that make use of Internet banking, payment gateways, SEO experts, cloud product marketing, digital marketing, and other services that are now integrated into supply chain transactions. An increased level of employee satisfaction as well as significant improvement in customer relationship management is also observed. This was due to the companies' ability to form stronger bonds with their customers, resulting in increased brand awareness and recall. Similar improvements can be seen in relationships with suppliers and partners.

Moreover, the health and medical sector is slowly but surely beginning to embrace Web 2.0 technologies and tactics such as social networking, blogging, and sharing health information, such usage may become an everyday occurrence. This new trend is emerging under the umbrella of Health 2.0, and it has significant implications for the future of medicine. Unlike traditional e-Health technologies, that only allow web users to accept information passively, Health 2.0 provides web users with the ability to actively modify web information.

Furthermore, Web 2.0 has the potential to significantly improve the state of e-health in rural communities. A comprehensive list of medical Web 2.0 applications (e.g., Ves Dimov's Clinical Cases and Images Blog; Ask Dr. Wiki; Ganfyd; and PubDrug) can be found in the Giustini [6] research work. Information about best Web 2.0 applications in medicine (e.g., PatientsLikeMe; Sermo; DoubleCheckMD; Vitals.com; Carol.com; and MyMedLab) can be found in research article by richard macmanus [13]. Besides various medical websites and portals offering different medical and health services, there are various kinds of e-health systems focusing on:

- Virtual communities and online support groups are created where people can share their experiences and information about numerous diseases, while also providing emotional support to one another.
- Open source, web based Electronic Health Records (EHR) system, with a Web 2.0 facilitated e-learning component for supporting continuing medical education and promoting public awareness.
- Telehealth/Telemedicine allows doctors to see and treat patients virtually. With virtual doctor visits, people can see a doctor online and get medical advice along with necessary prescriptions.

Web2.0 is rapidly becoming an important source of information for international travellers seeking travel advice and tourism supplier recommendations. Along with the web2.0 trend, the concept of "Tourism 2.0" was created to describe a new and modern way of tourism. Web 2.0 technologies, such as social networks (Facebook, Twitter, MySpace), podcasting, RSS, and others, have enabled many people who travel for tourism to obtain information and interact with tourism service providers at any time, without incurring high costs, and in a variety of ways, ranging from writing in chat rooms to audio-visual elements related to tourism demand and supply.

Apart from the aforementioned areas, web2.0 has made a significant contribution to various sectors such as agriculture, online education, financial services, and so on.

On the other hand, according to Billy Hoffman, lead engineer at Web security specialist SPI Dynamics. *"People are buying into this web2.0 hype and throwing together ideas for Web applications, but they are not thinking about security, and they are not realizing how badly they are exposing their users."*

E. The Bad About Web 2.0

Web 2.0 has are venerable to vandalism as many people have the capability to own and control data that is on the web 2.0 site. A person can intentionally damage or destroy the contents of the website including impersonation of other websites which can lead to distorted information which has raised questions on the credibility of information that is available on the sites [15].

Today's web2.0 [10] applications are openly accessible and dynamically generated; this feature of web2.0 makes it more interesting, but it also increases the risk of security breaches. Many website owners frequently request that developers concentrate on functionality rather than security. As a result, developers may not always take precautions such as validating user input on web pages. As a result of their popularity and the fact that security vendors have reduced the effectiveness of other, more traditional attack vectors like e-mail attachments, these pages are attractive to hackers.

Hackers have taken advantage of Web 2.0 to distribute worms that carry out harmful operations outside of the browser, leaving users completely unaware of their actions. They also post malicious content that appears to be legitimate on social media. This could happen, for example, a User/Hacker may upload content that contains code or malware that can be used to carry out a malicious task. Sometimes hackers will upload software that is supposed to be virus removal software but instead loads a Trojan horse to social networking sites like facebook (Now-a-days people are too addicted to facebook or other social networking sites and users are blindly clicking each and every link and every application and hacker takes advantage of this stupidity) or any other web sites. Hackers may upload malicious code, such as key loggers, which record victims' keystrokes, including credit card information and passwords, and send them back to the hacker.

Furthermore, since vendors have improved browser security, according to Fred Cohen, research professor at the University of New Haven and founder of the information-security consultancy Fred Cohen Associates. As a result, hacker intrusions into systems are not limited to browsers; applications like Flash, QuickTime, and inZip, which are used in many Web 2.0 sites to play video clips, view documents, and otherwise handle files, are also used by hackers.

F. The Ugly About Web 2.0

Web 2.0 is causing a splash as it stretches the boundaries of what Web sites can do. But in the rush to add features, security has become an afterthought, experts say. As a results, if a user visits an infected site, Web 2.0 worms can spread in the background of the user's browser without being visible in an open window. Web 2.0 worms like the Samy worm, which is a cross-site scripting worm (XSS worm) hit MySpace in October 4, 2005 and within just 20 hours of its release, over one million users had run the payload making Samy the fastest-spreading virus of all time.

In 2006, a new worm that targets Yahoo e-mail users is on the loose, taking advantage of one of the web2.0 tools (JavaScript) flaws. The Yamanner worm targets all versions of Yahoo Web-based mail. Yamanner arrives in a Yahoo mailbox bearing the subject header "New Graphic Site." The computer becomes infected once the message is opened, and the worm spreads to people on the Yahoo e-mail contact list. The collected e-mail addresses are also sent to a remote online server, which Symantec believes will be used for spam campaigns.

Typically, social platform attacks gain access to users' accounts by stealing their authentication credentials when they log in.This information is then used to collect personal data from users' online friends and colleagues in a stealthy manner. A recent Stratecast study states that 22% of social media users have fallen victim to a security-related incident, and recent documented attacks support the numbers. More than 2 million user passwords were stolen by the Pony botnet, which targeted Facebook, Google, Yahoo, and other social media sites. The position of the most banned types of hacking is depicted in Fig. 2 [7]. According to Facebook, between 50 million and 100 million of its monthly active user accounts are fake duplicates, with up to 14 million of those deemed "undesirable" on the platform. moreover, businesses are also expected to use social platforms for "reconnaissance attacks," either directly or through third parties, in order to gather valuable user and organisation information about competitors. Businesses can use this information to gain a competitive advantage in future business ventures (*see* Fig.2), and these attacks are expected to increase in 2014.

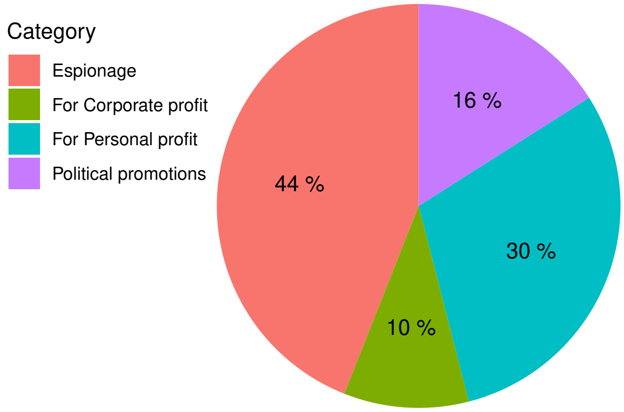


Fig. 2. Various types of hacking attacks carried out in 2021

According to a recent report, impersonation or stolen identities accounted for 91.6% of data breaches (*see* Fig.3). Geo-tagged photos have become increasingly popular in recent years. People tag their pictures with their geographic locations and share them on social media. Some applications have a Geo-tagging feature that automatically tags the user's current location inside a photo until the user turns it off manually. This can reveal personal information such as where one lives and travels, posing a threat to one's normal livelihood. Moreover, people who spend more time on social media are more likely to like their friends' posts. This trust is exploited by the cybercriminals. Hacking technique like *Likejacking, clickjacking, etc.*, in which attackers place fake Facebook like buttons on web pages, phishing sites, and spam emails, is one of the most common social media attacks. The percentage of internet users in the United States who have shared their online account passwords with friends and family is shown in Fig. 4. It's broken down into age groups. According to the survey's findings, the age group of 18-30 has shared their credentials, while 74% of those aged 65 and up do not share their online passwords with family or friends. With the advancement of internet tools and applications, the theft of user information and credentials is becoming more common. As of November 2020 [9], the collection of the most significant online information breaks via social media around the world is presented in Fig. 5.

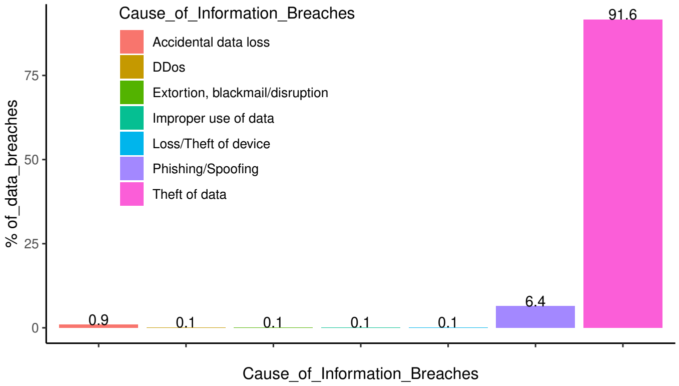


Fig. 3. Represent the most common reason for data breaches in 2020.

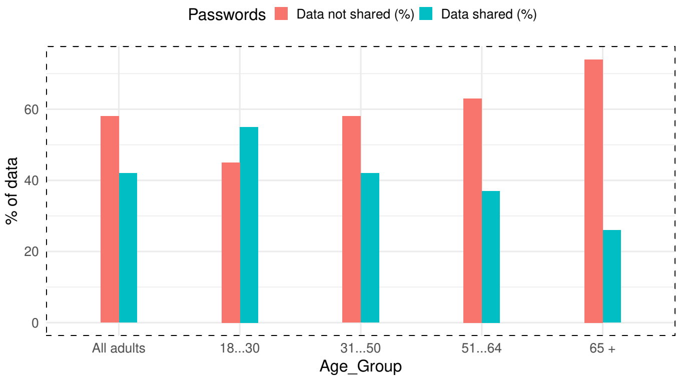


Fig. 4. Users who have shared passwords online with family or friends in 2020, US

The client-server architecture is one of the most significant flaws of Web 2.0 and Web 1.0. This centralised system possessed all of the data and was in charge of the lives of the users in a variety of ways. As a result, this scene poses a significant risk to people's privacy.

On the other hand, a decentralized network is free from the threat of data breaching. Nobody has authority over your personal information. There won't be any centralized server. The data will be dispersed across the entire network. With the revolution of the cryptocurrency, blockchain is taking this infrastructure to a whole new level. We can now move on to decentralising data structures from our traditional centralised system. As a result, people's personal data will no longer be sold as a commodity.

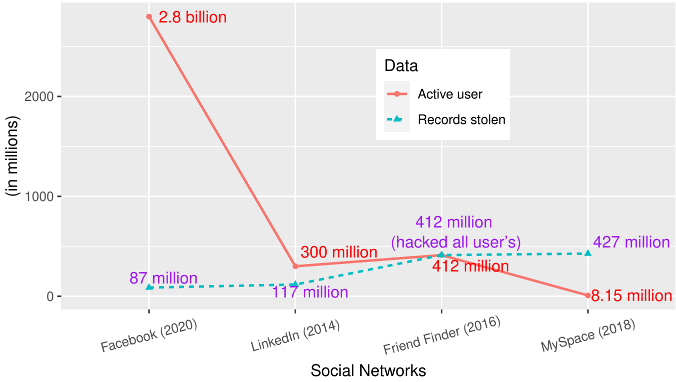


Fig. 5. Users who have shared passwords online with family or friends in 2020, US

G. *Web 3.0- A decentralized web*

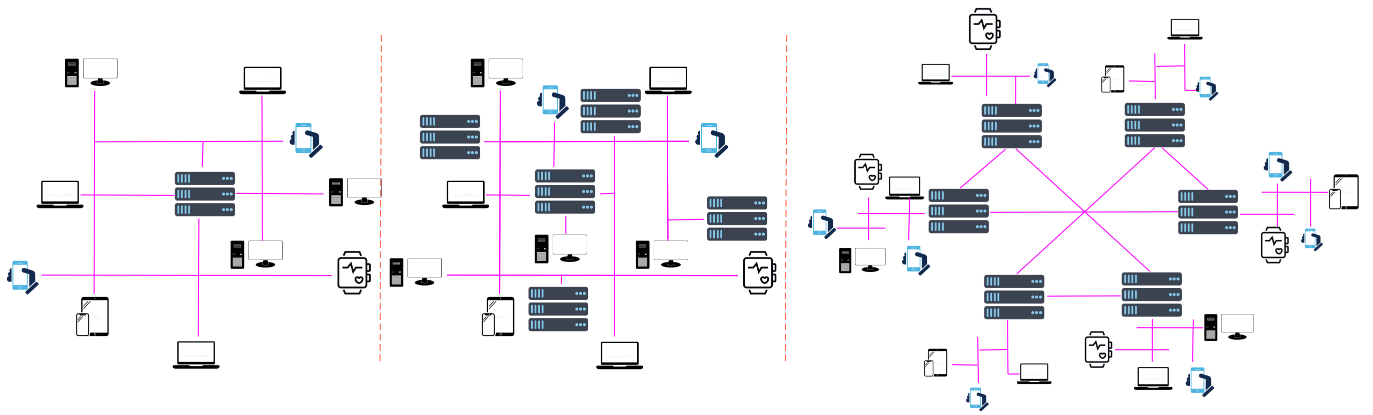
Web 2.0 and earlier versions had centralised servers, whereas Web 3.0 has a decentralised network that is more user-centric(*see* Fig. 6). Web3.0 manifests itself through new technologies like cryptocurrencies, virtual and augmented reality, artificial intelligence, and more. The Web3.0 movement is being driven by a shift in how we, as a society, view and value the Internet, which is being aided by new technologies. The goal of Web3.0 is to create an Internet that works for the people and is owned by them.

Web3.0 is about re-engineering existing the internet services and products to benefit the peoples. It can be considered as an open internet, built on open protocols and transparent blockchain networks that is accessible to all the users. Blended applications that provide convenient ways to interact with the underlying technologies could be used by consumers to interact with these protocols. It will fundamentally alter the way humans and machines interact by enabling secure data transfers, automated cryptocurrency payments, and simple ownership transfers.

H. *The Good About Web 3.0*

Despite the lack of a standardised definition for Web 3.0, it does have a few distinguishing characteristics.

- **Semantic Web:** Web 3.0, also known as the Semantic Web (as coined by Tim Berners-Lee), is the next step in the evolution of the internet, allowing it to process information with near-human intelligence by leveraging the power of Artificial Intelligence



Centralized System

Distributed System

Decentralized System

Fig. 6. Centralized vs. Distributed vs. Decentralized Systems

(AI). As a results, rather than processing text, a machine can process knowledge itself, using processes similar to human deductive reasoning and inference, resulting in more meaningful outcomes. They can learn what users are interested in, help find what people want faster and understand the relationship between things.

- **Ubiquitous:** Web 3.0 will allow us to access the Internet at any time and from any location. Web-connected devices will no longer be limited to computers and smartphones at some point in the future, as they were in web 2.0. Technology will enable the development of a plethora of new types of intelligent gadgets as a result of the Internet of Things (IoT).
- **Decentralized nature:** Web 3.0 will give creators and users more freedom in general. By utilising decentralised networks, Web 3.0 will ensure that users always have control over their online data. The next version of the internet is also expected to be more reliable due to its decentralized nature, which eliminates the possibility of a single point of failure.
- **Trustless governance system:** With Web3.0, we can overcome the limitations of our traditional governance system. Our current governance system uses legal contracts to guarantee the delivery of goods and services. However, enforcing these contracts is a time-consuming and costly process that involves intermediaries at every step. So, while a legal agreement protects you, the system is inefficient and prone to mistakes and delays.
  Web 3.0 can address this problem by implementing a trustless (i.e. users can interact publicly and privately on the network without having to go through an intermediary, which could put them at risk) governance system based on smart contracts. Smart contracts are open-source pieces of code that have conditions that both parties agree on before they start. The contract is automatically executed once the predefined conditions are met. Using smart contracts makes services verifiable and easily enforceable. User can get services from anywhere in the world, and can pay for them directly and automatically based on the contract's. This would drastically reduce the cost of contract monitoring and transaction auditing.
- **Blockchain technology:** Web3.0 offers unprecedented levels of security and privacy to the user data. The spread of a user's data across multiple computers can raise privacy concerns. Web 3.0 solves this problem through blockchain, as there is no single point of failure. Because each node in the network has a copy of the data ledger, a hack would require the hackers to have simultaneous access to a large number of nodes. Breaching that level of security is extremely difficult and costly.
- **Digital identities:** Secure digital identities, which are a new feature of Web 3.0, also help to protect data privacy. Digital identities will be fully encrypted, anonymous, and cross-platform. User consent will be coupled to these digital identities, which means that, unlike Web 2.0, users may be asked if they want to see advertisements or not.
- **Tokenization:** Moreover, the key to the innovation in Web 3.0 is the digitization of assets via tokenization. Tokenization is the process of converting assets and rights into a digital representation, or token, that can be used on a blockchain network. Cryptocurrency and fungible tokens are forms of

digital currency that can easily be exchanged across networks, driving a new business model that democratizes finance and commerce. Non fungible tokens (NFTs) are units of data that represent unique assets such as avatars, digital art, or trading cards, that can be owned by users and monetized for their own gain.

While the web 3.0 vision presents numerous opportunities for growth and development, it also raises security concerns.

I. The Bad About Web 3.0

Web3.0 has ushered in a new class of cyberthreats. While decentralised data and services reduce single points of attack, they also increase the risk of data being exposed to a wider range of threats. These involve traditional threats, as well as tactics unique to blockchain networks and interfaces.

- **Lack of oversight:** According to experts, decentralization will exacerbate the issues associated with monitoring and regulating Web 3.0. This may lead to an uptick in cybercrime, online abuse, and other issues.
- **Smart contract hacks:** Smart contract logic hacks, that targets the logic encoded in blockchain services. Attackers create their own malware, which is then distributed on the blockchain as malicious smart contract code. Malicious smart contracts have all of the standard smart contract functions, but they act strangely. Interoperability, crypto-loan services, project governance, and wallet functionality have all been targeted by these hacks. Smart contract logic hacks also raise serious legal issues, as smart contracts are often not protected by the law or are fragmented across jurisdictions.
- **Seed phrase attack:** Social engineering attacks like cloning wallets account for the vast majority of security incidents affecting Web 3.0 users. Hackers pose as customer service representatives and offer to respond to users' publicly posted Twitter or Discord server requests. Criminals will keep an eye on these channels and contact users to offer "assistance", eventually convincing them to share their seed phrases. Anyone with access to a cryptocurrency wallet's seed phrase (private key) can clone it and use it as their own.
- **Partial decentralization of dApps:** The Ethereum network, which powers the cryptocurrency ether (ETH) and provides access to thousands of decentralised Applications (dApps), is currently the largest community-run decentralised network. However, Decentralised Applications (dApps) are typically not distributed; instead, they are simply react websites with state and permissions stored on the blockchain rather than a centralised database. According to Moxie Marlinspike, the creator of signal and co-author of the signal protocol, point out that OpenSea, the largest NFT marketplace, removed one of his NFT, he created with no justification needed or provided, bringing light to the issue that even NFTs, a shining star of the web3.0 blockchain world, are controlled by web2.0 companies (centralized organisations). For instance, user-controlled cryptographic key management is a common feature of many blockchain technologies. User have a private key for their wallet, application, authentication server. It's devastating to lose this key, or to lose possession of this key. So many people use platforms (web2.0 platforms) such as Coinbase to act as a custodians or intermediaries to manage users private keys and wallets. That is to say, we are not fully equipped to work with a decentralised web, but a consideration for security experts in web 3.0 will be the management of many cryptographic keys without relying on centralised organisations. Moreover, most dApps today do not authenticate or sign their API responses, imagine a decentralised bank app that doesn't do API authentication or response signing.
- **Information quality:** In Web 1.0, accuracy was based on the reputation of publishers. Web 2.0 lowered data quality, leading to the efficacy of mis- and disinformation on the web. Will accuracy checks be included in the consensus to accept machine-managed data in web 3.0? Who makes the decision, what qualifications do they have, and what motivates them to be fact-based rather than pushing an agenda?

J. The Ugly About Web 3.0

There are multiple types of attacks in the web3.0 world. The technology is still nascent, and new types of attacks may emerge. Some attacks look similar to traditional credential attacks observed on web2.0, but some are unique to web3.0. Following that, we'll go over the various types of security risks associated with web3.0.

- **Wormhole Bridge:** During the relatively short lifespan of the underlying technologies, blockchains have already seen some significant security breaches. The Wormhole Bridge is a blockchain interoperability protocol that allows users and decentralised applications to transfer assets between blockchains, create a great deal of concern among web expert.

- **Data manipulation:** Intentional manipulation of data that will be used to train AI is a major concern in terms of cybersecurity. People can make up bad data to get the results they want, making AI the largest disinformation system on the planet. For example, When Microsoft decided to train their chatbot "Tay" by allowing it to learn from Twitter, malicious tweets were sent to the machine, training it to be racist. Imagine what a nation-state could do to cause havoc by feeding AI false data or altering the meaning of words. How will cybersecurity experts identify, block, and remove data intended to deceive?
- **Data confidentiality:** Data breaches compromise confidential information constantly. On top of that, content can be released inadvertently or stored in an insecure location. When machines scan data and store it in their knowledge base, the chances of private information being found and used increase dramatically. To prepare for a system that has the potential to spread confidential information faster than ever before, cybersecurity leaders must strengthen their defences.
- **Enhanced spam:** In a Web 3.0 world, the vast library of integrated and interconnected metadata will create more dangerous channels through which spam attacks can spread. With websites, search engines and applications using the entire internet's resources as databases to serve responses to users, adversaries can target, exploit and pollute specific resources to distribute spam. These spam campaigns could deliver malicious JavaScript code or ransomware to every user by embedding it in an application. Other potential spam risks include nation-states manipulating data on web pages in an attempt to feed disinformation to AI algorithms, which then spreads to a country's citizens.
- **Cryptojacking:** With the advancement of web3.0, the risks of cryptojacking will increase. Cryptojacking is a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency. Cybercriminals hack into devices to install cryptojacking software. The software works in the background, mining for cryptocurrencies or stealing from cryptocurrency wallets. Hackers have two main methods for secretly mining cryptocurrencies on a victim's device. Firstly, by convincing the victim to click on a malicious link in an email that instals cryptomining software on their computer. Second, by infecting a website or online advertisement with JavaScript code that executes automatically once the victim's browser is loaded.
- **Rug Pull:** Rug pulls are a lucrative scam in which a crypto developer promotes a new project—usually a new token—to investors, and then disappears with tens of millions or even hundreds of millions of dollars. This particular type of fraud accounted for $4 billion in lost money for victims [5], or 38% of all cryptocurrency scam revenue in 2021, according to Chainalysis [3], a blockchain analysis company. It's a fairly straightforward process to create new tokens on Ethereum or another blockchain, and get that token listed on decentralized exchanges (DEXes), or peer-to-peer marketplaces for crypto traders, without a code audit, according to the Chainalysis [3]. Some of the most popular rug pull scam are Squid game rug pull, which is cryptocurrency token associated with the hit Netflix series went from $2,586 to a penny [16], SnowDog rug pull [8], Mercenary rug pull [12], etc.
- **Ice phishing:** The "ice phishing" technique doesn't involve stealing one's private keys. Rather, it entails tricking a user into signing a transaction that delegates approval of the user's tokens to the attacker. Using an ice phishing attack, the attacker can gather approvals over time and then quickly drain all of the victim's wallets. This is exactly what happened with the Badger DAO attack that enabled the attacker to drain approximately $121 million in November-December 2021.

III. Metaverse

Metaverse (Meta=Beyond, Verse=Universe), a world beyond this universe, is a term intimidating enough on its own. The metaverse has recently become a hot topic of discussion, with both Facebook and Microsoft claiming ownership. At Microsoft Build, Microsoft CEO Satya Nadella announced innovation in the metaverse space by introducing its next generation mixed-reality device, HoloLens 2, its next platform Microsoft Mesh, and integration with other third-party Augmented Reality (AR)/Virtual Reality (VR) devices to connect and collaborate with people anywhere and anytime. Later, Facebook's CEO announced that Facebook will change its name to "meta" and will focus on the metaverse as their next goal in their product roadmap.

While defining the metaverse term is not easy, it will not be defined by one single person or company, it will be defined by many, and it will evolve.

In a presentation at the company's annual Connect conference, Zuckerberg announced the company is rebranding as Meta and detailed how his company aims to build a new version of the internet.

Zuckerberg, Chief Executive Officer of Facebook, says
"The metaverse is a set of virtual spaces where you can create and explore with other people who aren't in the same physical space as you. You'll be able to hang out with friends, work, play, learn, shop, create, and more."

Claire Kimber, Group Innovation Director at Posterscope
"I think the Metaverse is the all-encompassing space in which all digital experience sits; the observable digital universe made up of millions of digital galaxies"

Eric Redmond, Global Director, Technology Innovation, Nike
"My general description: The Metaverse crosses the physical/digital divide between actual and virtual realities."

Esther O'Callaghan OBE, Cofounder Hundo careers
"I hope it will be like the Oasis from ReadyPlayerOne where in the end; it's owned by young people who care more about community than profit and use it for the good of the real and virtual world. And if that sounds ludicrously naive and optimistic about it - I am and I'm not sorry!".

Luke Shabro, Futurist Deputy Director of the Mad Scientist Initiative - Army Futures Command
"A nebulous, digitally mixed reality with both non-fungible and infinite items and personas not bound by conventional physics and limitations."

Fabian Schmidt, Homo Digitalis, 2021
"The metaverse is a digital world that is meant to feel as real as possible and can represent all concerns of human existence. From leisure to work".

The idea of metaverse itself isn't new. Science fiction author Neal Stephenson coined the term "metaverse" in his 1992 cyberpunk novel Snow Crash, presenting a 3D virtual world in which people, represented as avatars, could interact with each other and artificially intelligent agents. It's a hybrid of technology elements such as virtual reality, augmented reality, and video in which users "live" in a digital universe.

The metaverse is currently being conceptualized in different sections and parts, but a complete metaverse is being seen as the next computing platform and the next extension of the internet.

The initial metaverse concept has been successfully implemented in the game Second Life. Second Life is a video game/website that was launched in 2003 and allows users to join and have a second life in the virtual world. They can take on any identity and play any role in the virtual world. Web3D allows people to take on the role of an avatar in a virtual world and explore, meet other residents, participate in individual and/or group activities, and so on, just as they would in real life. For a long time, the metaverse concept has been used in films. Gamer, Ready Player One, The Matrix, Minority Report, Terminator, and Surrogates are examples of metaverse-based films. All of these films feature a real person playing a role in a virtual world through the use of a gadget or device. *Free Guy* (2021), a recent film, is an example of a metaverse in which the main character is an AI character in a video game who falls in love with a real player.

While the idea of the metaverse has been around for years, the technology to make it a reality wasn't there. 3D objects require a much faster internet, larger data storage, better computing, and AR/VR/XR (Extended Reality) devices to present 3D objects in real-time.

A. The Good About Metaverse

The metaverse, according to some leaders, will be the next computing technology used to build and access digital systems. Digital spaces, digital objects, digital identities, and digital activities that mimic the real world will be part of the systems.

- **Avatars:** In the metaverse, users are represented by 3D avatars. Real people and their activities, such as talking, walking, working, dancing, playing, and other activities, are represented by these avatars. Touch, sense, and smell will all be possible to use with XR devices in the future. The term XR refers to a hybrid of augmented reality (AR), virtual reality (VR), and mixed reality (MR). To access the metaverses, metaverse users use one or more of these XR devices. These devices not only create a virtual world, but they also record geospatial data and the player's voice.
- **Collaboration and Linking:** A metaverse's primary function is to connect and collaborate with real-world people in the virtual world. People can not only connect, collaborate, and hang out in the virtual world, but they can also conduct business that can be used in the real world. Real people can hang out, party, have a meeting, attend a virtual conference or show using their avatars in the virtual world.

- **Virtual Representation of the Real World:** The metaverse's key concept is to represent real-world economies in a virtual world, transact with them in the virtual world, and then bring them back into the real world. People from the real world train in a virtual world, learning and applying the skills they acquire in the real world. Digital assets and NFTs are used in games where players earn digital currencies and then cash them out in real money.
- **High Performance Computing:** To support all the elements of metaverse, high-performance computing is required to build and run metaverses. The majority of metaverse businesses are concentrating on high-performance computing infrastructure, such as faster processing, storage, and high-speed internet.
- **Persistence:** This means user can access the virtual world whenever they want. User can alter it by adding new virtual buildings or other objects, and the changes will be retained the next time they visit. In the same way that social media relies on user-generated content today, the metaverse will rely on user-generated content, digital creations and personal stories.
- **Effective remote working:** Metaverse has the potential to address all of the existing remote work challenges. It gives managers a virtual environment in which they can meet employees (as avatars), communicate with them, read their body language, and maintain in-person interaction. Furthermore, by keeping track of the team inside a virtual office, the employer can resolve issues such as time theft and goldbrick at the workplace.
- **Healthcare tools:** A metaverse is a life-changing tool for healthcare professionals and medical personnel who were previously unable to visit patients due to geographic constraints. They can interact with the patient and gain a clear understanding of their health condition in the Metaverse's virtual world.
- **Monetization of benefits:** Some are developers looking to use the ecosystem to build their own business-specific projects, while others are looking for ways to make money. Fortunately, the Metaverse has the potential to meet both groups' needs. Because the Metaverse is open-source, anyone can create a useful project on top of it. People can also become common users of the ecosystem and earn money by creating and trading NFTs.

Just like every other new technology, the metaverse also has its fair share of setbacks in terms of metaverse challenges for security and privacy. The technologies that power metaverse platforms come with their own set of risks.

B. The Bad About Metaverse

The metaverse promises to usher in a new era of social and technological experiences that are unparalleled in terms of interoperability and immersiveness. However, there is a downside to interoperability and immersive experiences. People in the Metaverse may have a virtual office space, as well as a virtual laptop and other accessories, just as they would in a traditional office setting. Security and privacy issues will be a major concern in these environments. Intrusions, snooping, impostors, and breaches are all possibilities.

- **Reduced Perception of Physical Space:** Humans and societies are both real. Humans require a genuine social life, a family, and genuine friends. Virtual friends and families will not provide the same level of happiness and contentment as real ones. The real world's time and space are not the same as the virtual world's. This could have an impact on our perception of real-time and space. The exact side effects are unknown, but the more virtual worlds we live in, the further we distance ourselves from reality. Hanging out with real friends in a bar or at a football game is not the same as hanging out with virtual friends in a bar.
- **Massive data generation:** The metaverse is transforming the real world into virtual worlds, and the real economy is being replaced by digital economies. All of this necessitates a large amount of 2D and 3D content, which will inevitably increase the demand for data creation, storage, and transfer. The amount of data we generate each day is already causing issues, and while new hardware is being developed every day, this will continue to be a challenge in the future.
- **Cyber-attacks:** Every day, millions of cyber-attacks take place, and data security in the metaverse will remain a challenge. Many privacy and security concerns, such as network credential theft, identity theft, social engineering attacks, and ransomware attacks, can arise as a result of the AR and VR technologies that power the metaverse. Hackers could take advantage of security flaws in AR and VR devices to steal a user's identity in the metaverse.
- **Virtual identities:** Using avatars and creating virtual identities is the same as creating fake identities. You can be anyone and do anything in the virtual world that you would never be able to do in real life.

You can have multiple identities and participate in multiple metaverses. Because of the way our bodies and minds work, these virtual identities will have an impact on our real selves, and some of these habits may become ingrained in us.

- **Virtual assets:** Virtual asset ownership necessitates less legal due diligence, and millions of cryptocurrency hacks have already occurred. Because everything is online and connected, this problem will only get worse as we build more metaverses. In a connected world with digital assets, it is much easier for a hacker to hack from thousands of miles away than it is for a hacker to hack from a physical location.
- **Credential Theft:** One of the most difficult metaverse challenges you can face right now is detecting theft. Anyone who has your network credentials could easily impersonate you in the metaverse. Wearable devices can be used by hackers or criminals to compromise users' network credentials. Hacking is, in fact, one of the most serious concerns for retailers who use VR and AR-based shopping apps. Theft of network credentials can jeopardise users' financial and personal information stored in their metaverse user profiles.
- **Perennial threats:** Along with malicious attacks, metaverse developers will have to deal with a variety of other threats that are common on digital platforms. For example, how can younger users be protected from adult content?. Pornography was the original fuel for the internet. What do you think will most likely appear in the metaverse? Making sure that our young children don't have access to that in the metaverse will be a difficult task. Furthermore, for users to feel safe in the metaverse, sexual harassment will be an issue that must be addressed.

C. The Ugly About Metaverse

Since its inception, the metaverse has been plagued by privacy and security concerns, necessitating the development of a robust cybersecurity infrastructure tailored to the metaverse. Monitoring the metaverse and detecting attacks on new platforms will be more complicated than on existing platforms. There will be an explosion of devices with the metaverse. Infrastructure will explode. Apps and data will explode. As a result, the attack surface has just increased by an order of magnitude. Following that, we've listed a few security risks associated with the metaverse.

- **Deepfake:** Techniques for fake video or audio are now advanced enough to be weaponized and used to create targeted content to manipulate opinions, stock prices or worse. Deepfakes use powerful machine learning and artificial intelligence techniques to manipulate or generate visual and audio content with a high potential for deception. This same technology could be used in the metaverse, making it impossible to tell if you're conversing and transacting with the human ostensibly on the other side of the technology.
- **Immersive attack:** It's a new type of attack that focuses on the unique properties of immersive VR and the vulnerabilities that come with it. An Immersive attack results in a VE that has been maliciously modified in order to harm or disrupt the user physically or mentally.
- **Human joystick attack:** According to Ibrahim Baggili, a professor of computer science at the University of New Haven, and a board member at XRSI syas *"Right now, we look at screens. With the metaverse, the screens are so close to our eyes that it makes us feel that we are inside of it. If we can control the world someone is in, then we can essentially control the person inside of it."*. According to their 2019 paper entitled "Immersive Virtual Reality Attacks and the Human Joystick" [2], the researchers discovered that it is possible to control immersed users and move them to a location in physical space without their knowledge using VR systems.
- **Overlay attack:** In such attacks, the hacker overlays unwanted images, video, or content on the player's virtual reality view. The player will have no option to remove the content. Persistent images and content that remains fixed in virtual space are included in this attack.
- **Spying in the metaverse:** The security expert discovered that in a virtual reality application, one can listen in on other users inside a virtual room without their knowledge or consent. The researchers have coined the term *"man in the room attack"* to describe this type of attack. An attacker can be lurking in the shadows, watching and listening to user every move, says the author [2].
- **Ransomware:** Ransomware is the next most prominent threat posed by VR in the metaverse. Hackers could most likely introduce features into VR platforms that trick users into disclosing personal information. Users' metaverse experiences could be easily compromised if hostile agents gain access to VR devices used to access the metaverse.

IV. Conclusion

This paper covered the evolution of the Web1.0 to metaverse. We go over each generation's strengths and weaknesses in detail. Since 1989, the web has advanced significantly, and it is now on its way to becoming a massive web of highly intelligent interaction platform. But the story didn't end there. Just as Web 1.0 resulted from how we used the read-only Web (eCommerce, search engines, etc.), Web 2.0 has resulted from the applications that have been built based on the interactive Web (blogs, wikis, social networks, etc.), and Web 3.0 is based on cutting-edge technologies such as cryptocurrencies, virtual and augmented reality, AI, and more. Likewise, the metaverse is the latest addition to the emerging technologies that is most likely to grow at a rapid pace in coming years. Not only Microsoft and Meta are on board, but a growing number of businesses and startups are as well. The metaverse's success will be determined over time, but it appears to be a natural extension of today's digital world as it moves from 2D to 3D.

Moreover, with the advancement of web technologies, there has been an increase in the number of people who use the internet. As a result, data privacy and security have long been a source of concern for people all over the world. Cyber attacks are on the rise, which privacy and security advocates are working to address. In the midst of all of this, the metaverse's emergence, while a technological revolution, may also pose a threat to data privacy. However, with the potential for development it presents, it is crucial to address the data privacy and security issue within the metaverse.

References

[1] S. A. Brown, "Seeing web 2.0 in context: A study of academic perceptions," *The Internet and Higher Education*, vol. 15, no. 1, pp. 50–57, 2012.

[2] P. Casey, I. Baggili, and A. Yarramreddy, "Immersive virtual reality attacks and the human joystick," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 550–562, 2021.

[3] Chainalysis, "The 2022 crypto crime report."

[4] W. D. Chawinga, "Taking social media to a university classroom: teaching and learning using twitter and blogs," *International Journal of Educational Technology in Higher Education*, vol. 14, no. 1, pp. 1–19, 2017.

[5] J. Eyers, "The 'rug pull': crypto investors lose $4b in new scam," https://www.afr.com/companies/financial-services/the-rug-pull-crypto-investors-lose-4b-in-a-new-scam-20220111-p59nan/, Jan 11, 2022 – 1.23pm, [Online; accessed 02-May-2022].

[6] D. Giustini, "How web 2.0 is changing medicine," pp. 1283–1284, 2006.

[7] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2157–2177, 2021.

[8] Joe, "First memecoin launched on Avalanche ends in $ 30 million scam," https://247newsbulletin.news/markets/53886.html, November 27, 2021, [Online; accessed 02-May-2022].

[9] J. Johnson, "U.S. internet users sharing passwords with friends and family 2016," https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/, 2021, [Online; accessed 02-April-2022].

[10] G. Lawton, "Web 2.0 creates security challenges," *Computer*, vol. 40, no. 10, pp. 13–16, 2007.

[11] T. O'reilly, *What is web 2.0.* " O'Reilly Media, Inc.", 2009.

[12] Reuters, "Coinbase removes cryptocurrency links after 'rug pull' warnings," https://www.deccanherald.com/business/business-news/coinbase -removes- cryptocurrency-links-after-rug-pull-warnings- 1080240.html, FEB 10 2022, [Online; accessed 02-May-2022].

[13] richard macmanus, "Top Health 2.0 Web Apps," https://readwrite.com/top_health_20_web_apps/, 21 Feb 2008, [Online; accessed 24-March-2022].

[14] W. Richardson, *Blogs, wikis, podcasts, and other powerful web tools for classrooms*. Corwin press, 2010.

[15] D. M. Scott, *The new rules of marketing and PR: how to use social media, blogs, news releases, online video, and viral marketing to reach buyers directly*. John Wiley & Sons, 2009.

[16] M. Sigalos, "There's a 'Squid Game' cryptocurrency – and it's up nearly 2,400% in the last 24 hours," https://www.cnbc.com/2021/10/28/squid-game-cryptocurrency-up-nearly-2400percent-in-the-last-24-hours.html, OCT 28 2021, [Online; accessed 02-May-2022].