The Future of the Metaverse

MARCH 2023

RANE
Risk Assistance Network + Exchange

The Future of the Metaverse

April 2023

The Future of the Metaverse, Part 1

The metaverse's expected growth in the coming years will create a host of new business opportunities, but its use of decentralized technologies and data will also make it very hard for governments to regulate. In recent weeks, Meta — the U.S. tech giant formerly known as Facebook — has de-emphasized the metaverse in company briefings and statements and is now touting its investments in generative artificial intelligence (AI). Meta's shift in tone is no surprise. Since its release in November 2022, OpenAI's chatbot ChatGPT has kicked off an arms race among tech companies over chatbots and large language models. In February, Meta unveiled LLaMA to compete with Microsoft-backed ChatGPT and Google's Bard AI. Meanwhile, slowing economic conditions and the U.S. Federal Reserve's attempts to curb stubbornly high inflation by hiking interest rates have started to weigh on U.S. companies' bottom lines. This has seen a growing number of U.S. firms — especially in tech — reduce their workforces in recent weeks. Since November, Meta has announced two major rounds of layoffs and other cost-cutting measures, like making long-term pet projects (like Meta CEO Mark Zuckerberg's metaverse) subject to cancellation or budget cuts. The 2022 crypto crash only adds more reasons for Meta to de-emphasize the metaverse to placate Wall Street and investors. Despite this pivot, the metaverse and its associated technologies will still be crucial in the future and there will be many applications of Generative AI in the metaverse.

- Facebook's rebranding as Meta in October 2021 followed 18 months of COVID-19 lockdowns, which led to a surge of interest and investment into the metaverse and virtual worlds between late 2021 and early 2022. But interest waned following the crypto crisis in 2022 that culminated with the highly publicized collapse of the crypto exchange FTX in November.

What is the Metaverse?

Despite being a common term thrown around over the last two years, there is no commonly agreed upon

definition of the "metaverse." The term has been used to describe augmented and virtual reality technologies, virtual worlds, and many other technologies. Given that the concept is relatively new, it will be a while before there's a universally accepted definition. Meta defines the metaverse as the "next evolution in social connection and the successor to the mobile internet." Merriam-Webster defines it to be "a persistent virtual environment that allows access to and interoperability of multiple individual virtual realities." Meanwhile, the European Parliament's research arm has called it "an immersive and constant virtual 3D world where people interact through an avatar to enjoy entertainment, make purchases and carry out transactions with crypto-assets, or work without leaving their seat." These definitions are overly broad, but generally speaking the metaverse can be thought of as digital worlds or digital ecosystems that use or, in a fully developed environment, bring together the following technology areas:

- **3D modeling:** 3D modeling will allow for the creation of digital twins of various objects, including a person's digital avatar or recreated objects from life (such as a chair, classroom or venue), and for creating digital assets unlike those found in our world, like dragons. The Polynesian country of Tuvalu, for example, is creating a digital twin of its islands as a way to preserve its heritage and speak out about climate change, as rising sea levels threaten to submerge the island nation under water.

- **Artificial intelligence (AI):** AI, and all of the associated technologies therein — including generative AI, voice recognition, natural language processing, and real-time language translation — will increase the functionality of metaverse applications and, in turn, the metaverse's value to users.

- **Augmented reality (AR):** Augmented reality technologies will help bridge the gap between the real world and the metaverse. This could, for example, enable two different spectators to attend the same event seemingly side by side, but with only one spectator doing so in person.

- **Brain-computer interfaces:** Computers that can directly communicate with the human brain's electrical activity, as envisioned by Elon Musk's

Neuralink project, are likely a more distant prospect compared with the other technologies on this list. But at some point in the future, such brain-computer interface technologies will probably help people control their avatars and input (and receive) information.

- **Digital assets and/or non-fungible tokens (NFTs):** Digital assets and NFTs are also crucial for many virtual worlds, ranging from various pieces of artwork displayed in a world to the digital land that is sold and bought as a commodity in virtual worlds.

- **Digital currencies and/or cryptocurrencies:** Digital currencies, cryptocurrencies and the different platforms necessary to transact in them (such as digital wallets or cryptocurrency exchanges) are also crucial for the digital world, where assets (such as land) are often priced and transacted in cryptocurrencies.

- **Distributed ledger technologies (i.e. blockchain):** Distributed ledger technologies , ranging from smart contracts to cryptocurrencies, are central to a number of virtual worlds in not only providing the technology to host the in-world economy, but also in building some of the applications themselves through decentralized applications, or dApps.

- **Internet of Things (IoT):** The Internet of Things will help combine virtual worlds with physical worlds as various sensors and other IoT devices record and transmit information to the real world. For example, in a simple use case, IoT devices could record and transmit data from a sporting event and convert it to a digital version displayed in 3D for people attending a virtual event.

- **Virtual reality (VR):** Although far from the only way to experience digital worlds, VR technologies currently represent the most immersive way for people to explore and engage with the metaverse.

- **5G, 6G & beyond:** Having people seamlessly integrate themselves into a virtual world will require high bandwidth. And as the technologies become more data-centric and mobile (with, for example, the use of more AR or VR headsets), more advanced telecommunications and wifi technologies

will be needed to underpin it. Some use cases, such as using metaverse applications for surgeries, will require reliable low-latency connections as well.

Although the more sophisticated applications that fully integrate a host of different technologies remain years away, the metaverse is already here, thanks largely to advancements in online gaming. In the last 20 years, the gaming industry has been at the forefront of creating immersive worlds that are increasingly being utilized for metaverse-like applications. Massively multiplayer online games, for example, can often have in-depth systems for building digital houses. And companies can also use building artwork as marketing platforms and advertise IP with certain in-game characters. The gaming industry is by far the largest industry in the entertainment sector, and while the vast majority of games are not persistent real-world environments, video gaming offers prime real estate for advertising and product placement akin to that in filmed entertainment. The free-to-play battle royale game Fortnite, for example, has hosted several in-game concerts, including concerts by popular rapper Travis Scott and electronic music producer Marshmello.

The first online games started appearing around 2000. But the genre began really taking off in the early 2000s with the release of games like the still popular World of Warcraft. In 2006, the online game platform Roblox allowed users to upload and create their own games, as well as host their own digital events. Roblox's popularity boomed during the COVID-19 pandemic and the subsequent surge in demand for virtual spaces. In July 2020, the company estimated that half of all U.S. kids and teens under the age of 16 were playing its game; that same month, Roblox launched a new ''Party Place'' feature allowing players to hold social gatherings like birthday parties.

Beyond video games, over the last decade a number of different digital worlds centering on NFTs have also emerged, such as Decentraland (where people buy plots of land using an Ethereum-based cryptocurrency) and Somnium Space (where people can attend events, play games and own land). In such platforms, a number of companies — including Samsung, Adidas, Miller Lite and PricewaterhouseCoopers — have also bought NFT land.

While these types of platforms are important for the metaverse, so are the underlying technologies supporting them. The advancement of VR headsets, release of 5G, expansion of Ethereum and distributed ledger technologies, innovation in AI technologies, and continued advancement of computing power all continue to enable the growth in virtual worlds and metaverse platforms, improving the experience.

A Meta-Sized Headache for Regulators

The number of use cases for the metaverse will grow in the coming years, as will the size of the metaverse economy. The video game industry shrank in 2022 for the first time in over a decade, largely due to base effects from the staggering growth in 2020 and 2021 due to the pandemic. But the industry is still poised to expand and serve as the primary growth driver of the metaverse, at least initially. Video game industry data research service Newzoo estimated in 2022 that 3.2 billion people globally played video games and projected that number would grow to 3.5 billion people by 2025. Beyond the entertainment industry, metaverse technologies can also be used for a number of workplace situations, including remote work collaboration, job and educational training, as well as customer service operations. Governments and businesses can also create digital twins and recreations of their operations to simulate and test various scenarios, such as seeing how a certain city or factory would hold up in different environmental conditions (like severe flooding). Mark Zuckerberg's vision of a new social media platform where everyone walks around, talking to each other in a virtual world that Meta owns may be unrealistic over the next decade. But metaverse technologies and separated different platforms are poised to grow substantially in the coming years.

- Siemens says it created a digital twin of a factory the company is building in China to help simulate the plant's conditions, which Seimens claims increased productivity by 20% and production capacity by 200%.

- In April 2022 (right as the last year's crypto crash began to unfold), Citibank estimated the metaverse economy could reach $13 trillion by 2030. But even if the metaverse economy only reaches half or even a third of that estimated size over the next decade, it would still mark staggering growth that will force governments to respond.

Open internet policies in Western countries will enable the metaverse to flourish, but this will also lead to a decentralized network of virtual worlds that will be hard for governments to regulate. Unlike countries like China, Western countries have open internet policies that will make it easier for the metaverse to grow by enabling the advancement of supportive technologies like cryptocurrencies, digital assets and digital worlds. But Western governments will eventually have to step in. Governments have spent hundreds of years trying to regulate society and businesses, but prior to the last decade, this has mainly focused on regulating entities that are easy to identify or, at the very least, are centralized. The challenge with the metaverse is that many of the technologies associated with it are designed to be decentralized to ensure that no singular entity can easily run the metaverse or shut it down. In many cases, there may be an organization or foundation that is organizing a certain technology or platform. But much of the data in the infrastructure itself will utilize distributed ledger technologies, like the popular smart contract blockchain Ethereum. Such decentralized technology cannot be easily blocked by governments as there's often no singular server to shut down or organization that can manipulate information.

- U.S. regulators have already struggled to keep cybercriminals from using decentralized cryptocurrency technologies. In August 2022, the Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash, a popular Ethereum-based cryptocurrency mixer that is meant to obfuscate the flow of cryptocurrencies to increase anonymity, in connection to its use by the North Korean cybercrime organization Lazarus Group. Tornado Cash is open source and while its operations are managed by an organization. But the cryptocurrency mixer runs its code on a blockchain with smart contracts designed in a way that ensures they can't be reversed or changed by anyone, including even the organization managing Tornado Cash.

The growth of the metaverse will also create regulatory challenges connected to personal data, particularly as they deal with both centralized platforms and decentralized platforms. The metaverse will be extremely data-intensive as people increasingly own digital assets and use personal information to help generate their avatars and online personas. Understandably, governments will be suspicious of tech and social media giants (like Meta and Google) creating platforms in the metaverse that could provide them with yet another way to access more personal data and information on their users. In some cases, existing or upcoming regulations, such as the European Union's General Data Protection Regulation, can likely be adapted to monitor how these big companies collect and use data generated in the metaverse. But in other use cases, such regulations may be insufficient. Many of the metaverse's platforms and services will be decentralized, making it particularly hard for a single legal territory to regulate it. But ironically, in some cases, data decentralization in the metaverse can boost a person's data privacy, if adequately encrypted. Some metaverse technologies may use decentralized, encrypted and anonymized data that isn't owned by any singular company, government or organization. Many government regulations are based on the assumption that some organization is controlling the data and the flow of information. But this won't always be the case in the metaverse, where some technologies may use decentralized, encrypted and anonymized data that isn't owned by any singular company, government or organization. Governments will also be concerned about killer apps being developed in the metaverse that could become the next Google or Amazon. But breaking up such monopolies will be no easy feat, as a platform that gains a monopoly over a certain part of the metaverse could simultaneously be run by a non-profit organization and processed on a decentralized blockchain that no one controls — a situation that current antitrust legislation is almost certainly not equipped to address. □

The Future of the Metaverse, Part 2

March 2023

Increasing regulatory and physical barriers in the metaverse will accelerate the fragmentation of the global internet. Divisions on how to regulate cyberspace are continuing to grow between the United States, Europe, Russia and China, as well as between various developing and middle-income countries. As discussed in the first part of this series, the United States and most other Western countries will remain champions of the open internet, which will enable decentralized metaverse technologies to flourish. But that will not be the case in China or other countries with authoritarian governments, where the decentralization of ideas and social platforms is viewed as a direct risk to political, social and regime stability. These countries will either develop their own metaverse technologies or increase the legal consequences for their citizens using the more decentralized platforms within the virtual world.

China will probably become a key example of metaverse centralization that similar regimes will likely follow. In China, the metaverse will probably evolve in a centralized manner as regulatory bodies have already scuttled and outlawed virtually every ave-

nue to a truly decentralized metaverse service. In 2020, China launched the blockchain-based Service Network (BSN), which is designed to be a blockchain-like system that Chinese developers can use when launching their own apps. But unlike many other blockchain systems, BSN is centralized and does not have a cryptocurrency associated with it. This past September, China launched a global version of the BSN called the BSN Spartan Network, with an apparent aim to internationalize Beijing's approach to blockchain technology and, in turn, set the standard for how like-minded governments seek to adopt the technology. The BSN Spartan Network could, in effect, become a blockchain component of Beijing's sprawling Belt and Road Initiative (BRI) by enabling Chinese companies to use the BSN Spartan Network in BRI countries to provide metaverse (and other) and other services. Chinese metaverse technologies could be adopted as a part of China's investment campaigns in BRI countries, which could then act as a force multiplier for Chinese investments overall by making it easier for Chinese companies, who already have some familiarity with China's metaverse-type technologies, to compete in the region. Beijing likely also hopes that apps developed by Chinese companies

to run on the Spartan Network, including metaverse apps, will eventually be able to easily compete overseas and become an alternative to those in the West. In addition, some of China's metaverse platforms may be more appealing to other authoritarian countries (though none of those other authoritarian countries have the same firewall that China has set up to keep out competition). In addition, Beijing will try to use the metaverse to increase social stability at home by ensuring platforms promote the Chinese Communist Party's narrative and further indoctrinate citizens on party-approved beliefs and attitudes.

- People in China (and Asia more broadly) will likely be faster to adopt more online, metaverse-type services than their counterparts in the United States and Europe, given that similar synthetic environments are more popular and culturally embedded in Asian societies compared with Western ones. Indeed, Chinese society has already embraced the concept of virtual personalities, complete with famous digital AI personas for media outlets and social media personalities. And a number of Chinese companies, including tech giants like Tencent and Alibaba, are investing in various virtual worlds.

- In the West, China's global BSN Spartan Network and the various metaverse apps that Chinese companies will export will almost certainly exacerbate fears about the Chinese government being able to access information and data through such apps. Former U.S. President Donald Trump singled out Chinese apps as a concern during his time in office, which his successor Joe Biden has since echoed. Recent U.S. moves to potentially ban the popular Chinese-owned video-sharing app TikTok — which itself will likely be closely intertwined with the metaverse — demonstrate Washington's focus on the issue, which will only deepen as Chinese digital services are increasingly used around the world.

But the metaverse's fragmentation is unlikely to keep countries like Russia from weaponizing its technologies through information campaigns, cyberespionage and cyberattacks. In the West, the expanding web of virtual worlds will only reinforce the societal polarization that has occurred since the rise of social media over the last two decades by giving its rivals more divisions to exploit and more ways to exploit them. For threat actors in Russia and elsewhere that have increasingly deployed propaganda campaigns in the West in recent years, it will be open season — presenting an even greater challenge for Western governments that are already struggling to combat the growing tranche of false or misleading information being spread online by foreign governments and fringe groups. Western lawmakers are currently debating the extent to which social media platforms and internet companies should regulate disinformation and misinformation on their platforms. But this debate would become largely moot if social media becomes more decentralized in the metaverse, as there would be no entity that governments could force to regulate content. Countries like Russia, Iran and China could also create platforms on the unregulated and decentralized metaverse that cater to extremist groups in the West, like far-right or -left organizations. Such virtual communities could enable these extremist groups to collaborate and grow their support base, and with less government oversight and risk of censorship compared with today's social media platforms. In addition, real-time translation services using AI and synthetic (or copied) voices will likely eventually enable a Russian- or Chinese-speaking person to seamlessly communicate with an English- or French-speaking person on the metaverse, making it that much easier for threat actors to carry out their work.

The growth of the metaverse will also further compel non-Western states to establish an alternative to the existing conventions on cybercrime. The metaverse will exacerbate the fundamental differences in opinions and priorities between countries on what kind of cyber activities should be regulated and how by creating a whole new world for those activities to take place. While non-Western governments will try to limit their citizens' access to decentralized platforms on the metaverse, persistent users will still find workarounds to gain access, which will further drive their governments to increase the global means to enforce their more expansive view of cybercrime. The Western interpretation of cybercrime largely focuses

on illegal access to data, computer-related fraud, child pornography, illegal interception of information and copyright and IP theft — as reflected in the 2004 Budapest Convention on Cybercrime, a treaty that has largely only been ratified by Western countries. But over the last five years, China and Russia have called for a new international treaty that would expand what online activities are considered cybercrimes. This past January, during the latest round of global negotiations on a prospective new cybercrime treaty, both Moscow and Beijing pushed to include language like ''content-related'' crimes and ''incitement to subversive activities,'' which Western countries fear would cover any Chinese or Russian citizen criticizing the government and its policies. The more popular the metaverse becomes in the coming years, the more ''cybercrimes'' will be committed in the view of governments like China's and Russia's (as well as many other countries). And this will, in turn, only reinforce Beijing, Moscow and other like-minded governments' desire to negotiate a new treaty that would enable them to go after dissidents in foreign countries using the metaverse as a way to help organize protest movements or support opposition groups.

- Compared with the West, Russia, China and other like-minded countries take a more expansive view of cyber threats that also includes stopping the spread of dangerous information, in addition to preventing traditional malware or other attacks on networks and infrastructure. The United States and other liberal democracies have rejected this perspective, believing individual rights and freedom of expression should be protected in the cyber world. These differences between Western and non-Western countries are likely to only grow, which could lead to a scenario where there are multiple global cybercrime treaties.

As the metaverse grows and becomes a greater share of national GDPs, the risk of bubbles and financial crises in the metaverse will also increase. Most governments have spent the past decade trying to figure out how to regulate bitcoin and other cryptocurrencies, as well as explore the potential benefits of their own central bank digital currencies. However, these efforts have typically focused on taxation, know-your-customer and compliance issues, and how financial institutions should use and hold digital assets. While these are all important regulatory questions for fintech, the metaverse poses different challenges by suddenly raising the prospect of having real estate markets in digital worlds. Governments will need to approach this issue from a taxation perspective (i.e., how do you tax ''land'' in a decentralized virtual world), as well as from a systematic risk perspective, as bubbles in such areas are likely to occur and already have. The nearly 15-year-old history of bitcoin has shown repeated boom and bust cycles, with little sign of them going away, at least in the short term. Indeed, the financial risks of this emerging new environment were acutely demonstrated during last year's spectacular collapse of the crypto exchange FTX and the collapse of real estate prices in the metaverse, with the average land price on six leading Ethereum-based virtual worlds falling 85% from January 2022 to August 2022. □

RANE

Risk Assistance Network + Exchange