NOTE

CLOSING THE GATES ON MONEY LAUNDERING: BIG TECH AS GATEKEEPERS IN THE METAVERSE

Jenny Zhang*

The rise of the metaverse has created meaningful growth opportunities for the digital economy and the use of digital assets. The conditions that have facilitated the metaverse's growth, however, have simultaneously given rise to unchecked money laundering risk. This Note reviews the existing Anti-Money Laundering ("AML") framework in the United States and argues that the metaverse's inherent design features disable the efficacy of the regulatory regime. In order to improve the reach of the AML framework, this Note proposes a system of gatekeeper liability that utilizes technology corporations to curb illicit activity in the metaverse.

*J.D. Candidate 2024, Columbia Law School; B.S. 2019, Duke University. I would like to thank Professor Kathryn Judge for her invaluable guidance and feedback. I would also like to thank the *Columbia Business Law Review* staff for their thoughtful edits.

I. INTRODUCTION

On October 28, 2021, Mark Zuckerberg announced that Facebook was changing its name to Meta in order to reflect its new focus on building the metaverse: a vast, immersive, online realm that would encompass entire digital societies and economies.[1] This announcement propelled public interest in the metaverse; in the two months following the name change, the term "metaverse" appeared in more than 12,000 English-language news articles, as compared to 4,000 in the first nine months of 2021 and fewer than 400 in any prior year.[2]

The metaverse's growth since 2021 is particularly evident in the realm of consumer brands. For instance, Gucci "sold a virtual-only digital twin of a . . . purse for a higher price than its real-world counterpart."[3] With respect to music and entertainment, "[a] Travis Scott Fortnite concert had 27.7 million unique attendees—far more than a typical concert venue can accommodate."[4] As for consumer-facing real estate transactions, Decentraland, "a user-owned Ethereum-based virtual

[1] Will Oremus, *In 2021, Tech Talked Up 'The Metaverse.' One Problem: It Doesn't Exist.*, WASH. POST (Dec. 30, 2021), https://www.washingtonpost.com/technology/2021/12/30/metaverse-definition-facebook-horizon-worlds [https://perma.cc/8YGW-ULYF].

[2] *Id.*

[3] ACCENTURE, TECHNOLOGY VISION 2022: MEET ME IN THE METAVERSE 9, https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF-5/Accenture-Meet-Me-in-the-Metaverse-Full-Report.pdf [https://perma.cc/NSY3-LLT5].

[4] *Id.*

world," saw 21,000 transactions worth $110 million in 2021.[5] Beyond consumer and retail, financial institutions have also begun to invest in the metaverse as they realize the vast business potential that can be unlocked. In February 2022, JPMorgan Chase became the first bank to buy land and open a lounge in the metaverse.[6] Other players, such as American Express and HSBC, followed suit shortly thereafter.[7]

Although the metaverse presents meaningful growth opportunities for the digital economy, the increased use of digital assets leaves the metaverse more vulnerable to financial crime. This Note argues that the metaverse's inherent design features disable the efficacy of the domestic anti-money laundering ("AML") regime. In order to address this shortcoming in the AML framework, regulators should use the law as a tool to shape the architecture of the metaverse, thereby rendering the platform more regulable. A system of gatekeeper liability in which technology companies, as opposed to financial intermediaries, are gatekeepers would allow regulators to achieve that aim. Part II of this Note provides an overview of financial transactions in the metaverse. Part III discusses the evolution of the United States AML regime and argues that the metaverse's design features limit the efficacy of existing AML laws. Part IV proposes a system of gatekeeper liability that can functionally influence the architecture of the metaverse in order to effectuate the aims of the AML regime.

[5] *Id.*

[6] Carla Calandra, *Banking in the Metaverse*, VML (Aug. 15, 2022), https://www.wundermanthompson.com/insight/banking-in-the-metaverse [https://perma.cc/F9VG-K737].

[7] *Id.*

II. BACKGROUND ON THE METAVERSE

A. What is the Metaverse?

The term "metaverse" was coined by the science-fiction author Neal Stephenson in his 1992 novel titled Snow Crash.[8] The idea did not gain meaningful traction, however, until 2021 when Facebook rebranded itself as "Meta."[9] Today, the metaverse refers to the "concept of an immersive and persistent virtual world where users can communicate and interact with other users and the surrounding environment and engage in social activities."[10] Another widely cited definition relies on the premise that the metaverse is a "massively scaled and interoperable network of real-time rendered 3D virtual worlds."[11] In contrast, some business and technology leaders believe "that the metaverse does not refer to any specific technology but rather a shift in how users interact with online technologies, services, platforms, and each other."[12]

Although the definitions of "metaverse" used by academics and practitioners may vary, the metaverse features "three key characteristics that differentiate it from two-dimensional online applications: (1) an immersive, three-dimensional user experience; (2) real-time, persistent network access; and (3) interoperability across networked platforms."[13] First, the metaverse's enhanced immersion provides users with a feeling of being "within the internet" as opposed to "just looking at it."[14] Second, persistence refers to the dual ideas that the metaverse continues to exist even when no users are using it, and the metaverse is available to users whenever and

8 Janna Anderson & Lee Rainie, *The Metaverse in 2040*, PEW RSCH. CTR. (June 30, 2022), https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040 [https://perma.cc/7388-KKP6].

9 *Id.*

10 LING ZHU, CONG. RSCH. SERV., R47224, THE METAVERSE: CONCEPTS AND ISSUES FOR CONGRESS 3 (2022).

11 Oremus, *supra* note 1.

12 ZHU, *supra* note 10, at 3.

13 *Id.* at 4.

14 *Id.* at 5.

wherever they want to access it.[15] Third, interoperability refers to the "ability to deliver an immersive and persistent virtual experience seamlessly across multiple networked platforms or interconnected virtual spaces."[16] In other words, interoperability "allow[s] users to move between different virtual spaces and access different platforms and services using the same devices and digital assets (e.g., digital identity, currency, and objects)."[17]

B. Financial Transactions in the Metaverse

Decentralized technologies, which include cryptocurrency and non-fungible tokens ("NFTs"), are the building blocks of the metaverse.[18] Cryptocurrency and NFTs are both powered by blockchain, which is "a technology that permanently records information (e.g., commercial transactions) in an interconnected database called a ledger."[19] Notably, blockchain-based cryptocurrencies already serve as payment methods in metaverse transactions.[20] Proponents of blockchain argue that its use in the metaverse "could facilitate fast, secure, trusted, and transparent online transactions without a centralized oversight body."[21] The ability to bypass a centralized oversight body, however, gives rise to significant AML risks. Regulators have expressed concern "about the potential for anonymized criminal transactions and financial fraud" with respect to digital assets.[22] In fact, two main forms of NFT-

[15] *Id.* at 5.

[16] *Id.* at 7.

[17] *Id.* at 7.

[18] Sudhir Pai, *Banking on the Metaverse*, FORBES (Mar. 15, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/03/15/banking-on-the-metaverse/?sh=11609d156068 [https://perma.cc/PW2S-TSMU].

[19] ZHU, *supra* note 10, at 14.

[20] Patrick Bucquet, *Payment Rails in the Metaverse: New Opportunities for Financial Institutions*, PAYMENTSJOURNAL (June 12, 2023), https://www.paymentsjournal.com/payment-rails-in-the-metaverse-new-opportunities-for-financial-institutions/ [https://perma.cc/SZ6V-RB87].

[21] ZHU, *supra* note 10, at 15.

[22] Derek Robertson, *Does the Metaverse Need Crypto?*, POLITICO (Apr. 27, 2022), https://www.politico.com/newsletters/digital-future-

driven illicit activity in 2022 included "[w]ash trading to artificially increase the value of NFTs and money laundering through the purchase of NFTs."[23] Moreover, the metaverse-related digital currencies MANA and SAND have already been linked to illicit activity.[24]

As the metaverse continues to grow, the volume of financial transactions will likely increase accordingly. The market size of the metaverse is expected to reach $800 billion by 2024,[25] and by 2026, it is predicted that "25% of people will spend at least one hour a day in the metaverse for work, shopping, education, social and/or entertainment."[26] The metaverse has even shown its economic potential more recently. From June 2021 to December 2021, the average price of a parcel of virtual land jumped from $6,000 to $12,000 across the four main Web 3.0 metaverses (i.e., Decentraland, The Sandbox, Somnium Space, and Cryptovoxels).[27]

Banks have invested in the metaverse precisely because they expect attractive financial opportunities to accompany the metaverse's growth. After JPMorgan Chase's entry into Decentraland in February 2022,[28] "American Express filed trademarks for a virtual marketplace and cryptocurrency services in the metaverse in March [2022]. Its filings for real-world services in the digital world include card payment

daily/2022/04/27/does-the-metaverse-need-crypto-00028273 [https://perma.cc/P8X8-3MH8].

[23] Raluca Ochiana, *RegTech in the Metaverse*, THE PAYPERS (Aug. 3, 2022), https://thepaypers.com/expert-opinion/regtech-in-the-metaverse—1257786 [https://perma.cc/7UHZ-QGJG].

[24] TARA ANNISON, ELLIPTIC METAVERSE REPORT 2022: THE FUTURE OF FINANCIAL CRIME IN THE METAVERSE 15 (2022), https://www.elliptic.co/hubfs/Crime%20in%20the%20Metaverse%202022%20final.pdf [https://perma.cc/W93Z-UHAL].

[25] Pai, *supra* note 18.

[26] *Id.*

[27] CHRISTINE MOY, J.P. MORGAN, OPPORTUNITIES IN THE METAVERSE 7 (2022), https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf [https://perma.cc/2S3Y-RWMB].

[28] *See* Calandra, *supra* note 6.

services, an ATM, [and] banking and fraud detection services."[29] That same month, HSBC and Siam both announced plans to open an office in the virtual world Sandbox.[30] Finally, in April 2022, Fidelity launched Fidelity Stack in Decentraland in order to attract young investors and Fidelity Metaverse ETF in order to provide opportunities to invest in metaverse-related businesses.[31] Despite financial institutions' growing presence in the metaverse, bank platforms remain in their infancy and continue to serve informational and marketing purposes rather than offer true financial services.[32]

III. THE CURRENT ANTI-MONEY LAUNDERING FRAMEWORK IN THE METAVERSE

A. Statutory History and Framework

Financial transactions in the metaverse are currently subject to existing AML regulations.[33] In the United States, the Bank Secrecy Act of 1970 ("BSA" or "BSA/AML") "remains the statutory foundation for the existing federal [AML] regulatory framework."[34] The BSA requires U.S. financial institutions to

[29] *Id.*

[30] *Id.*

[31] John Mccrank, *Fidelity Enters the Metaverse in Search of Young Investors*, REUTERS (Apr. 25, 2022), https://www.reuters.com/technology/fidelity-enters-metaverse-search-young-investors-2022-04-21/#:~:text=The%20Fidelity%20Stack%2C%20which%20was,of%20emerging%20customers%20at%20Fidelity [https://perma.cc/B3YU-E5QS].

[32] Hyunkoo Kang, Hwan Kyoung Ko, Chloe Jyung-Myung Lee & Sihong Kim, *Digital Finance: Current Issues and Laws*, CHAMBERS & PARTNERS (Feb. 7, 2022), https://chambers.com/articles/digital-finance-current-issues-and-laws-2 [https://perma.cc/2FWQ-LQ37].

[33] Heidi Wicker, *Transacting in the Metaverse, But Getting Paid in Reality: Legal Considerations for Companies Establishing Payments Infrastructure*, N.Y. L.J. (Nov. 16, 2022), https://www.law.com/newyorklawjournal/2022/11/16/transacting-in-the-metaverse-but-getting-paid-in-reality-legal-considerations-for-companies-establishing-payments-infrastructure/ [https://perma.cc/N3Z5-2T5U].

[34] Norbert J. Michel & Jennifer J. Schulp, *Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals*, CATO INST., July 26, 2022, at 2.

assist U.S. government agencies to detect and prevent money laundering. Specifically, the act requires financial institutions to "keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities."[35] At the time of passage, the recordkeeping and reporting requirements were the most significant statutory changes implemented by the BSA.[36]

Since the passage of the BSA in 1970, several laws have been enacted to expand the federal AML regime. In 1986, Congress passed the Money Laundering Control Act, which, among other measures, "established money laundering as a criminal offense," "made it a criminal offense to structure transactions to evade the BSA reporting requirements," and "require[d] essentially all banks subject to federal regulation to 'establish and maintain procedures reasonably designed to assure and monitor the compliance' with the BSA provisions and to include a review of banks' BSA compliance procedures in all federal bank examinations."[37] Congress subsequently passed the Annunzio-Wylie Anti-Money Laundering Act in 1992, which granted federal banking regulators powers such as the ability to "revoke a federal banking charter for banks guilty of a money laundering offense."[38] The most consequential change, however, was the statutory mandate requiring financial institutions to file suspicious activity reports (SARs).[39] Under Section 1517, the Treasury secretary is authorized to "require any financial institution, and any director, officer, employee, or agent of any financial institution, to report any suspicious transaction relevant to a possible violation of law or regulation."[40]

---

35 *The Bank Secrecy Act*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act [on file with the Columbia Business Law Review].

36 *See* Michel & Schulp, *supra* note 34, at 4.

37 *Id.* at 7 (quoting 12 U.S.C. § 1818(s)).

38 *Id.*

39 *Id.*

40 *Id.* (quoting 31 U.S.C. § 5318(g)(1)).

More recently, Title III of the USA PATRIOT Act of 2001 ("USAPA") expanded the scope of the AML regime in order to enhance the federal government's ability to combat terrorist financing. Among its key provisions, the USAPA "prohibited U.S. financial institutions from establishing correspondent accounts with foreign shell banks" and set forth enhanced customer identification programs ("CIP") and customer due diligence ("CDD") requirements.[41] Finally, the most recent changes to the BSA were set forth in the Anti-Money Laundering Act of 2020 ("AMLA"), and those changes represent the most significant overhaul of the BSA/AML regime since the USAPA.[42] The key provisions of the AMLA established a beneficial ownership information ("BOI") database, broadened law enforcement subpoena powers, expanded whistleblower rewards and protections, enhanced BSA penalties for repeat and egregious violators, expanded BSA/AML into the trade of antiquities and art, and emphasized the use of new technologies.[43] Notably, the AMLA expanded the BSA to include the term "value that substitutes for currency."[44]

B. Legislative Purpose

As the statutory framework for the BSA/AML regime evolved, the nature of the illicit activity that Congress intended to target expanded concurrently. According to Representative Wright Patman, the chairman of the House Committee on Banking and Currency in 1968 and a staunch

41 *Id.* at 8.

42 *Id.*

43 *Four Takeaways on BSA/AML Reform Under the Anti-Money Laundering Act of 2020*, THOMSON REUTERS (Aug. 9, 2021), https://legal.thomsonreuters.com/en/insights/articles/4-takeaways-on-bsa-aml-reform [https://perma.cc/5P5T-54LV]. *See also* Stephanie Brooker, M. Kendall Day, Linda Noonan, Ella Alves Capone, Chris Jones & Alexander Moss, *The Top 10 Takeaways for Financial Institutions from the Anti-Money Laundering Act of 2020*, GIBSON DUNN (Jan. 1, 2021), https://www.gibsondunn.com/the-top-10-takeaways-for-financial-institutions-from-the-anti-money-laundering-act-of-2020/ [https://perma.cc/9Z5L-59M9].

44 Michel & Schulp, *supra* note 34, at 8.

advocate for the original BSA,[45] the BSA aimed to address the "'illicit financial manipulation of huge sums of money,' income tax evasion, fraudulent defense contracts, the theft of Treasury bills, corporate kickbacks by Vietnamese importers, various types of securities fraud, and the use of 'fictitious' and 'dummy' corporations."[46] In 1968, these crimes occurred against the backdrop of the increased utilization of Swiss bank accounts as a tool to evade U.S. laws and regulations.[47] By implementing recordkeeping and reporting requirements, the BSA aimed to increase the traceability of funds and improve law enforcement's ability to detect illegal activity. Moreover, by providing criminal penalties for reporting violations that could range up to $500,000 in fines or ten years of imprisonment,[48] or both, the BSA created a system that incentivized banks to become "vigilant in identifying suspect customers and transactions."[49] Today, private enforcement via banks and other financial institutions remains critical to the efficacy of the BSA/AML regime.

The types of illicit activity that the BSA originally targeted had a clear financial element.[50] As the BSA/AML regime was updated over time, however, the breadth of AML laws expanded meaningfully to include crimes that had a weaker financial hook. After the passage of the USAPA in 2001, the category of specified unlawful activity under 18 U.S.C. §§ 1956 and 1957 (known as the money laundering statutes) expanded dramatically.[51] It now includes, among other things, "any

45 *Id.* at 2.

46 *Id.* at 4 (quoting *Legal and Economic Impact of Foreign Banking Procedures on the United States: Hearing before the H. Comm. on Banking and Currency*, 90th Cong. 1, 2, 16 (1968) (statement of Wright Patman, Chairman of the House Committee on Banking and Currency)).

47 *Id.*

48 31 U.S.C. §§ 5322(a), (b).

49 Mariano-Florentino Cuéllar, *The Tenuous Relationship Between the Fight Against Money Laundering and the Disruption of Criminal Finance*, 93 J. CRIM. L. & CRIMINOLOGY 311, 353 (2003).

50 *See* Michel & Schulp, *supra* note 34, at 4.

51 Cuéllar, *supra* note 49, at 336-37 ("Section 1957 targets conduct involving knowing transactions with certain kinds of criminal proceeds. Section 1956 criminalizes the concealment of criminal proceeds or the

crime of violence, bribery of a public official, smuggling of munitions, any offense for which the United States is obligated to extradite or prosecute someone by multilateral treaty, firearms trafficking, computer fraud, and 'terrorism offenses' as defined in 18 U.S.C. § 2332(b)."[52]

The intuition underlying money laundering laws is that financial transactions can help further a crime. AML laws initially aimed to punish people for carrying out activities that rendered illegal profits rather than punishing the underlying criminal offense itself.[53] The USAPA's expansion of specified unlawful activity under 18 U.S.C. §§ 1956 and 1957, however, "tends to criminalize a range of conduct involving money obtained from crime regardless of whether the offense involves much concealing or elaborate financial footwork."[54] As a consequence of this one-way ratchet, prosecutors can use money laundering charges to substitute for charges of predicate crimes that may be more difficult to prove.[55] Although the USAPA framed anti-money laundering and countering terrorist financing as complementary goals that warranted increased regulatory authority,[56] the reality is that the USAPA extended the BSA/AML regime far beyond the criminalization of only terrorist activity. The BSA/AML's reach into nefarious activity that spans from "bribery of a public official"[57] to an

promotion of particular kinds of crime with monetary proceeds. Since money laundering penalties extended criminal liability in a way that seemed strange and unusual, one objective was to narrow the scope of conduct subject to criminal penalties under statutes. At the same time, investigators and prosecutors clamored for more discretion, resulting in the inclusion of certain vague terms (such as 'monetary transaction' and 'financial transaction') that enlarged the statutes' scope to the point that almost any post-crime activity undertaken by someone with money generated from some list of crimes risks criminal liability for money laundering.").

[52] *Id.* at 339.

[53] *Id.* at 419.

[54] *Id.*

[55] *Id.* at 406–07.

[56] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, H.R. 3162, 107th Cong. § 302 (2001).

[57] 18 U.S.C. § 1956(c)(7)(B)(iv).

offense "relating to computer fraud"[58]—activities that may be facially devoid of financial involvement—demonstrates a significant shift from the original BSA, which targeted illicit activity with a clear financial hook.

In addition to a general modernization of the BSA/AML framework, the AMLA had a particular focus on targeting the use of shell companies. According to Representative Carolyn Maloney, the author of the Corporate Transparency Act ("CTA"), the act within the AMLA that created a new BOI database, the CTA aimed to "crack down on terrorism financing and the illicit use of anonymous shell companies,"[59] which were "the vehicles of choice for money launderers, criminals, and terrorists."[60] Here, Congress intended to improve the AML regime's ability to disrupt terrorist financing, a framework that was put in place by the USAPA, by creating a BOI database to facilitate customer due diligence processes.[61] The BOI database further aimed to bolster law enforcement efforts to investigate money laundering crimes, as investigations under the status quo had "been impeded by the lack of available beneficial ownership information."[62]

To further support its proposal, Congress referenced international practices. At the time of the CTA's passage, all twenty-eight European Union countries were required to have corporate registries that included BOI, and in 2006 and again in 2016, the Financial Action Task Force ("FATF") issued a report criticizing the United States' lack of a BOI database.[63] Congress recognized that effective AML policies required international cooperation, so the absence of a BOI database in

58 18 U.S.C. § 1956(c)(7)(D).

59 116 CONG. REC. H3499 (daily ed. July 20, 2020) (statement of Rep. Carolyn B. Maloney).

60 *Id.*

61 *See* Beneficial Ownership Information Reporting Requirements, 87 Fed. Reg. 59498, 59506-07 (proposed Sept. 30, 2022) (codified at 31 C.F.R. pt. 1010). The BOI database requires reporting companies to submit "the individual's full legal name, date of birth, current residential or business street address, and a unique identifying number from an acceptable identification document . . . or the individual's FinCEN identifier." *Id.* at 59507.

62 H.R. REP. NO. 116-457, at 44 (2020).

63 *Id.*

the United States presented a glaring loophole in the global AML regime. Like the USAPA, which meaningfully expanded the BSA, the AMLA and CTA represented yet another expansion of the domestic BSA/AML regime by providing law enforcement with heightened authority to retrieve and share BOI with designated authorities domestically and internationally.[64]

In addition to the BOI provision, which was one of the most significant changes imposed by the AMLA, the AMLA extended the BSA/AML regime into novel territory: cryptocurrency. Specifically, the AMLA expanded BSA definitions in several places to include the term "value that substitutes for currency."[65] Thus, persons or businesses that engage in cryptocurrency transactions are now subject to AML obligations. This expansion into cryptocurrency reflects a patchwork approach that has guided previous statutory updates of AML laws, such as through the USAPA. Congress was reasonably unable to foresee the threats posed by terrorism or digital assets when the original BSA was passed in 1970. As a result, legislation since 1970 has continued to augment the original BSA/AML framework by responding to new threats, such as digital assets, as they arise.

C. BSA/AML in the Metaverse

From January through May of 2022, corporations, venture capital, and private equity firms invested over $120 billion

[64] *See* Beneficial Ownership Information Access and Safeguards, and Use of FinCEN Identifiers for Entities, 87 Fed. Reg. 77404, at 77411-77414 (proposed Dec. 16, 2022) (codified at 31 C.F.R. pt. 1010).

[65] See 31 U.S.C. § 5312(a)(1), which expands the definition of "financial agency" to include "a person . . . or a service provided with respect to . . . value that substitutes for currency"; § 5312(a)(2)(J), which expands the definition of "financial institution" to include "a business engaged in . . . value that substitutes for currency"; § 5312(a)(2)(R), which expands the definition of "financial institution" to include "a licensed sender of money or any other person who engages as a business in the transmission of . . . value that substitutes for currency"; § 5312(a)(3)(D), which adds the following to the definition of "monetary instruments": "as the Secretary shall provide by regulation, value that substitutes for any monetary instrument . . . ."

into the metaverse.[66] These investments only represent the tip of the iceberg, as the metaverse "has the potential to become a $13 trillion opportunity by 2030, with total global users of between one and five billion."[67] Despite the metaverse's potential to disrupt the digital economy, legislators have failed to enact new AML policies to regulate the platform. As a result, businesses that operate in the metaverse are currently subject to obligations imposed by existing AML laws, but the metaverse's architectural features—namely decentralization, interoperability, and anonymity—disable the efficacy of the current BSA/AML regime.

1. Decentralization and Interoperability

Decentralization and interoperability are closely-related design features that are central to the metaverse. In a decentralized metaverse, no single company or handful of companies owns and controls the platform.[68] In an interoperable metaverse, users can have an "immersive and persistent virtual experience seamlessly across multiple networked platforms or interconnected virtual spaces."[69] As it exists today, the metaverse is decentralized and lacks interoperability. The metaverse includes social platforms, such as Decentraland and Sandbox, and gaming platforms, such as Roblox and Fortnite, which are each run by different companies.[70] Because minimal interoperability exists between these platforms, users must create separate profiles and avatars, and they cannot import digital assets or exchange currencies between

66 Caroline D. Pham, Comm'r, CFTC, Keynote Address at the EUROFI Financial Forum Prague 2022: Money and Life, the Metaverse, and Everything (Sept. 7, 2022).

67 Robert G. Howard, David W. Wright & Craig A. de Ridder, *Investing in Metaverse Real Estate: Mind the Gap Between Recognized and Realized Potential*, 39 THE COMPUT. & INTERNET LAW, July-Aug. 2022, at 1.

68 ZHU, *supra* note 10, at 15.

69 *Id.* at 7.

70 Jason Cottrell, *Who Owns the Metaverse?*, FAST CO. (Nov. 7, 2022), https://www.fastcompany.com/90802867/who-owns-the-metaverse [https://perma.cc/5JA3-GMTW].

platforms.[71] In contrast, a user in an interoperable metaverse would be able to stop by a virtual currency exchange to convert Robux to V-Bux, for example, when he moves from Roblox to Fortnite.[72] Yet the metaverse's design is dynamic since it is a nascent platform, so it may not necessarily remain decentralized and minimally interoperable. Consider three possible governance systems that may be adopted in the future[73]:

1. Centralized with minimal interoperability ("Metaverse 1"): A few gatekeepers, like Meta or Microsoft, can restrict access to users of their respective metaverses, with little to no integration with other metaverses.
2. Decentralized with maximal interoperability ("Metaverse 2"): Users can move seamlessly between metaverses, carrying with them a universal profile and their unique digital assets and currencies.
3. Middle ground ("Metaverse 3"): Even if a few gatekeepers establish control over the metaverse, intermediaries or regulators can step in to promote interoperability.

With respect to BSA/AML, an effective mode of regulation will necessarily be influenced by the metaverse's governance system. This next section will evaluate AML laws in Metaverses 1, 2, and 3, as outlined above, with a particular focus on whether decentralization and interoperability will disable the efficacy of the current AML regime.

To start, the limited interoperability in Metaverse 1 would present a significant challenge for existing AML laws. In a minimally interoperable metaverse, users would not have access to a universal digital wallet with digital currencies that can be used across all platforms. If users would like to participate and transact across platforms, they would need to hold the unique digital currencies that each platform accepts. Moreover, users would face the logistical burden of tracking

71 *Id.*

72 Oremus, *supra* note 1.

73 Cottrell, *supra* note 70.

their own digital assets.[74] The key AML challenge in Metaverse 1 would arise from regulators' inability to track the flows of a single currency. Although regulators would be able to view a blockchain ledger to determine the sources and uses of funds, the use of multiple currencies would provide criminals with numerous options for layering. If a criminal can convert MANA to SAND to THETA to AXS, then his ability to obscure the source of illicit funds increases substantially. In order to paint a full picture of the funds flows, regulators would need to determine the points at which MANA was converted to SAND, and so forth, and if those conversions stemmed from the same source of illicit activity. By forcing regulators to track the disparate flows of distinct digital currencies, regulators' ability to trace comprehensive money flows would be severely constricted.

On the contrary, the maximal interoperability in Metaverse 2 would aid regulators' ability to prevent money laundering. In order to illustrate the significance of interoperability as a design feature, consider a hypothetical in which Metaverse 2 has a single universal currency, and that is the only currency that exists across the entire metaverse. Here, criminals' ability to layer illicit funds via currency conversion would be eliminated. Of course, criminals would be able to employ layering techniques by purchasing digital assets like land or wearables, but the lack of multiple currencies would constrain the complexity of layering schemes. Even if criminals layer via purchases of digital assets, they would transact using the universal currency, and the transactions would be recorded on the ledger system. Therefore, regulators would be better equipped to trace the history of the funds flows because the data set would be more comprehensive.[75] Finally,

[74] Michael Abbott, *Why Money in the Metaverse is a Huge Opportunity for Banks*, ACCENTURE (June 14, 2022), https://bankingblog.accenture.com/why-money-in-the-metaverse-is-a-huge-opportunity-for-banks [https://perma.cc/NUH5-8TJC].

[75] Siobhan Roberts, *How 'Trustless' Is Bitcoin, Really?*, N.Y. TIMES (last modified June 22, 2023), https://www.nytimes.com/2022/06/06/science/bitcoin-nakamoto-blackburn-crypto.html [https://perma.cc/C38N-6BJ5] ("'If you have a big enough data set, it starts to leak information in

regulators would bypass the Metaverse 1 challenge of piecing together disparate flows of multiple currencies, thereby streamlining their ability to identify and detect illegal activity.

Decentralization is a second design feature that will impact the regulation of the metaverse.[76] Admittedly, regulators would face the same major challenge of regulating a blockchain-based currency in both a decentralized and centralized world. Cryptocurrency can be described as a "commons code"[77] that is inherently not subject to private ownership or control. The government therefore faces the steep challenge of regulating a public code because no single entity or group of entities has exclusive control over cryptocurrency.[78] This challenge would be exacerbated in a decentralized world like Metaverse 2.[79] In a decentralized metaverse, like the one that exists today, no single company or handful of companies control the platform. This design would remain true to the

unexpected ways.' Even more so when data from different sources are connected. . . . 'When you combine one data set with another to make a bigger data set, nonobvious linkages can arise.'").

[76] Julie Pattison-Gordon, *Should State and Local Governments Care About the Metaverse?*, GOV'T TECH. (Apr. 28, 2022), https://www.govtech.com/products/should-state-and-local-government-care-about-the-metaverse [https://perma.cc/AW2L-8D6R] ("'Do we have a decentralized model for the metaverse, where technically no one really owns it? . . . Or is it going to be a centralized approached, where a Meta owns it or a Microsoft owns it[]? Those are two totally different conversations.'").

[77] Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 536 (1999) ("The essence of a commons is that no single person exercises an exclusive right over the code.").

[78] *Id.* at 537 ("Relative to commons code, however, private code is more regulable. For if property law allocates the right to control, then private property makes the right exclusive; commons property makes the right non-exclusive. Commons property identifies no single entity with an exclusive right to control. Thus, commons code produces many sources of control, and constrains the power of the government to regulate.").

[79] *Id.* at 535 ("There is an increasingly significant limit on the government's power to regulate. In an odd way, the power depends upon who owns the code. To the extent that the 'application space' code of cyberspace is private . . . government's power is increased. To the extent that the 'application space' code of cyberspace is not private, but is instead held in a 'commons,' government's power is reduced.").

original libertarian spirit of the metaverse and the DeFi movement by adding a regulatory hurdle on top of the existing challenge of regulating cryptocurrency. In particular, it would be difficult for the government to determine which entities to regulate since control would be diffused across a broad array of actors. It is possible that regulators could employ a system of intermediary liability similar to the existing AML regime, which relies on a broad set of private actors to enforce the system. Yet cryptocurrency's anonymity is a major feature that would limit the efficacy of replicating the existing AML framework in the metaverse.[80]

2. Anonymity

The prevalence of cryptocurrency in the metaverse gives rise to regulatory challenges associated with anonymity. Cryptocurrency has a high degree of anonymity relative to fiat currency because it allows for direct, peer-to-peer transactions without an intermediary such as a bank.[81] This combination of anonymity and the absence of a centralized authority creates an environment ripe for money laundering.[82] If transactions bypass financial intermediaries altogether, then no regulated financial institution can "apply AML ex-ante preventive measures, such as customer due diligence, record-keeping, and suspicious transaction reporting."[83] At best,

[80] *See infra* Section III.C.2.

[81] Julian Dossett, *Are Cryptocurrency Transactions Actually Anonymous?*, CNET (June 7, 2022), https://www.cnet.com/personal-finance/crypto/are-cryptocurrency-transactions-actually-anonymous/ [https://perma.cc/VMY4-B2U3].

[82] ALESSIO FACCIA, LUIGI PIO LEONARDO CAVALIERE, NARCISA ROXANA MOSTEANU & LEONARDO JOSE MATARUNA-DOS-SANTOS, ELECTRONIC MONEY LAUNDERING, THE DARK SIDE OF FINTECH: AN OVERVIEW OF THE MOST RECENT CASES 30 (2020), https://dl.acm.org/doi/pdf/10.1145/3430279.3430284 [https://perma.cc/V3YD-CTNS].

[83] RODRIGO COELHO, JONATHAN FISHMAN & DENISE GARCIA OCAMPO, FIN. STABILITY INST., SUPERVISING CRYPTOASSETS FOR ANTI-MONEY LAUNDERING 3 (2021), https://www.bis.org/fsi/publ/insights31.pdf [https://perma.cc/K2BN-4L8N].

financial institutions would be left to carry out ex-post reactionary measures after money has already been laundered.

Relying on ex-post corrective action alone would likely be ineffectual given the shortcomings of AML detection under the status quo. Human-led check remains the primary method of detecting money laundering, but analysts responsible for evaluating alleged financial fraud cases "sometimes are not even able to recognize a case of money laundering."[84] Moreover, "[f]inancial institutions traditionally rel[y] on rule-based AML/CFT measures, which are shown to generate false positive alerts of around 90–95%."[85] Since financial institutions and regulators already struggle to detect the laundering of fiat currency, stripping financial intermediaries out of cryptocurrency transactions in the metaverse would eliminate a crucial source of information for regulators and cause a breakdown in the current BSA/AML framework.

It is worth noting that cryptocurrency transactions can be traced via a ledger, so transactions are technically pseudonymous instead of anonymous.[86] Therefore, regulators can trace transactions to a degree that they would not otherwise be able to if cryptocurrency was truly anonymous. Pseudonymity does not, however, address the critical concerns that arise from the absence of a regulated financial intermediary. There are even technologies that exploit cryptocurrency's pseudonymity, as "many cryptoassets or service providers specifically incorporate technology designed to prevent transparency, such as tumbling or mixing services or anonymity-enhanced coins."[87] These services equip money launderers with additional tools to carry out illicit activity.

84 FACCIA ET AL., *supra* note 82, at 32.

85 RODRIGO COELHO, MARCO DE SIMONI & JERMY PRENIO, FIN. STABILITY INST., SUPTECH APPLICATIONS FOR ANTI-MONEY LAUNDERING, 3 (2019), https://www.bis.org/fsi/publ/insights18.pdf [https://perma.cc/5VDW-9L3U].

86 Dossett, *supra* note 81.

87 COELHO, FISHMAN & OCAMPO, *supra* note 83, at 3.

IV. THE ARGUMENT FOR A SYSTEM OF BIG TECH GATEKEEPER LIABILITY

Given the metaverse's rapid growth and its potential to disrupt the digital economy, regulators must ensure that the platform is subject to sufficient AML controls. Although the metaverse's architectural features present AML challenges, regulators can create a system of gatekeeper liability involving technology companies in order to bypass key hurdles. This framework uses the law as a tool to shape the metaverse's design, thereby shaping the behavior of individuals and entities indirectly.

A. Designing a System of Gatekeeper Liability in the Metaverse

As discussed in Section III.C, a more centralized, interoperable metaverse would give rise to a more regulable environment. In order to create a more centralized metaverse, regulators should ensure that major stakeholders continue to invest in the space. Conveniently, private actors like Meta have already invested in the metaverse because they recognize the vast economic potential that can be unlocked,[88] particularly with a first-mover advantage. With industry estimates that value the metaverse as a $13 trillion opportunity by 2030,[89] the platform presents economic incentives that corporations may capitalize on even without a nudge from the government.

As key players in the metaverse emerge over time, regulators can begin to establish a system of gatekeeper liability. Under traditional gatekeeper liability, actors such as law firms and investment banks face liability for the wrongs committed by their corporate clients.[90] Gatekeeper liability is

88 Brayden Lindrea, *Zuckerberg's $100B Metaverse Gamble is 'Supersized and Terrifying' — Shareholder,* COINTELEGRAPH (Oct. 25, 2022), https://cointelegraph.com/news/zuckerberg-s-100b-metaverse-gamble-is-super-sized-and-terrifying-shareholder-says [https://perma.cc/F6V2-44HF].

89 *See* Howard et al., *supra* note 67, at 1.

90 *See* Andrew F. Tuch, *The Limits of Gatekeeper Liability*, 73 WASH. & LEE L. REV. ONLINE 619, 619-620 (2017).

based on four main premises: (1) "the incapacity of more direct forms of liability—namely, individual and enterprise liability—to effectively deter wrongdoing by corporate entities"; (2) "the inability of gatekeepers' reputations and of other market mechanisms to appropriately shape gatekeepers' conduct in the absence of liability"; (3) "the adequacy of gatekeepers' reputations . . . the idea that gatekeepers can 'stake' their reputations on the accuracy and completeness of their clients' assertions to investors"; and (4) "the ability of gatekeepers to influence their clients' conduct."[91] Evaluating these premises against the metaverse's architecture will aid regulators in creating a system of gatekeeper liability that is responsive to key AML challenges.

1. Big Tech as Gatekeepers

Under traditional gatekeeper liability, identifying a gatekeeper is relatively straightforward. Actors such as law firms and investment banks provide services directly to their corporate clients; the law firms and investment banks are the gatekeepers who may face liability for the wrongs that their clients commit. With respect to AML in the metaverse, the gatekeeper designation is not as clear-cut. Two potential gatekeepers include technology corporations, like Meta, or financial intermediaries, like JPMorgan Chase. Given the metaverse's current landscape and the AML regime's overarching mission to "safeguard the financial system from the abuses of financial crime,"[92] regulators should deploy technology corporations as gatekeepers rather than financial intermediaries.

A survey of the current players in the metaverse supports designating technology corporations as gatekeepers. As an overall industry, technology companies have a more established presence in the metaverse than financial intermediaries. Among companies such as Google, Apple, and Microsoft,

[91] *Id.* at 620.

[92] *History of Anti-Money Laundering Laws*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/history-anti-money-laundering-laws [https://perma.cc/D7NP-H7E2].

which have all invested in metaverse-related initiatives,[93] Meta has emerged as the front-runner.[94] Meanwhile, financial intermediaries' presence in the metaverse remains in its infancy. Banks such as JPMorgan Chase, HSBC, and American Express have opened lounges in the metaverse that showcase promotional materials but have yet to offer financial services. Due to the complex financial regulatory framework in the United States, it is unclear if or when banks will be truly operational in the metaverse. In contrast, Meta has already launched full-scale, and users can access a virtual world called Horizon Worlds, create avatars, interact with other players, and purchase virtual assets.[95] In order to respond to ongoing money laundering concerns in the metaverse, it is pragmatic to designate technology corporations as gatekeepers because their platforms are further developed than financial intermediaries, financial transactions occur on those platforms, and most importantly, technology corporations do not face the same regulatory constraints as banks.

If regulators designate technology corporations as gatekeepers, the argument for a system of gatekeeper liability, as opposed to an alternative liability system, becomes more compelling. Technology companies acting in isolation lack the requisite expertise to prevent money laundering. Historically, the regulatory challenges that companies such as Meta have

93 Josephine Walbank, *Top 10 Companies Investing in the Metaverse in 2023*, MOBILE (Jan. 20, 2023), https://mobile-magazine.com/articles/top-10-companies-investing-in-the-metaverse-in-2023 [https://perma.cc/5YD3-JNPG]; Brian Newar, *Apple Stock Jumps After CEO Reveals it's Investing in the Metaverse*, COINTELEGRAPH (Jan. 28, 2022), https://cointelegraph.com/news/apple-stock-jumps-after-ceo-reveals-it-s-investing-in-the-metaverse [https://perma.cc/C2QC-7NUS].

94 Kif Leswing, *2022 Will Be the Biggest Year for the Metaverse So Far*, CNBC (Jan. 1, 2022), https://www.cnbc.com/2022/01/01/meta-apple-google-microsoft-gear-up-for-big-augmented-reality-year.html [https://perma.cc/6UJN-JNVM] ("Meta has a lead over its Big Tech rivals: It's currently manufacturing and selling VR hardware, and accounted for 75% of the market in 2021[.]").

95 Sam Shead, *Meta Plans to Take a Nearly 50% Cut on Virtual Asset Sales in its Metaverse*, CNBC (Apr. 13, 2022), https://www.cnbc.com/2022/04/13/meta-plans-to-take-a-nearly-50percent-cut-on-nft-sales-in-its-metaverse.html [https://perma.cc/RV55-HK7L].

grappled with have been related to data, privacy, and free speech.[96] In contrast, the AML regime is quintessentially financial in nature and is based on a legal framework that is distinct from data privacy laws and First Amendment protections. Due to the legal morass that characterizes financial regulation and technology corporations' limited familiarity in this domain, technology companies in the status quo would be disincentivized from building out the compliance framework needed to comply with AML requirements.[97] If, however, Meta itself can face severe liability for money laundering that occurs on its platform, then its incentives will shift, and it may be more inclined to internalize the costs of AML compliance.

Admittedly, initial instinct may suggest that financial intermediaries are better equipped to act as gatekeepers due to their expertise and familiarity with the AML regime. Yet there are major drawbacks that render this position unworkable. As previously discussed, banks do not yet provide financial services in the metaverse, and it is unclear if or when they will do so. Since the metaverse banking infrastructure is nearly nonexistent, banks are not well-positioned to address money laundering in the short-term. This temporal concern is crucial because money laundering has already occurred on the platform. More importantly, the role of banks as an economic linchpin cautions against designating them as gatekeepers. The United States' financial regulatory framework recognizes banks' integral position in the economy by subjecting banks to safety and soundness requirements that "most other financial

96 *See, e.g.,* Sean Illing, *The First Amendment has a Facebook Problem*, VOX (May 5, 2021, 3:28 PM), https://www.vox.com/policy-and-politics/22356339/free-speech-facebook-twitter-big-tech-first-amendment [https://perma.cc/E8NW-KAYW].

97 The economic costs of compliance would present a meaningful disincentive for technology corporations to undertake AML obligations voluntarily, absent a system that holds them liable for AML violations. *See* Anna Bleazard, *The High Costs and Low Returns of AML Compliance for Banks: Is There a Better Way?*, FTI CONSULTING (Mar. 25, 2022), https://www.fticonsulting.com/emea/insights/fti-journal/high-costs-low-returns-aml-compliance-banks-better-way [https://perma.cc/6Y5E-H2NB].

firms are not subject to at the federal level."[98] These prudential regulations stem from systemic stability concerns[99] which may be jeopardized if regulators designate banks to be gatekeepers in the metaverse. Such a designation would require banks to increase their activity on the platform, which could unnecessarily expose banks to nefarious activity. Because history has shown that bank failures have far-reaching systemic impacts, it would be imprudent for regulators to risk compromising financial stability by designating banks to be gatekeepers.

2. Enforcement Mechanisms

In order to ensure that gatekeepers comply with their AML obligations, regulators should evaluate which modes of enforcement are most likely to induce compliance. Leveraging traditional AML tools offers a helpful starting point. Therefore, the core feature of this proposed gatekeeper liability scheme should be modeled on current reporting requirements. Just like banks are required to report suspicious activity to regulators in the status quo, technology companies should be required to report suspicious activity to regulators. Under the BSA/AML framework, banks, bank holding companies, and their subsidiaries are required to file a SAR with respect to: "criminal violations involving insider abuse in any amount"; "criminal violations aggregating $5,000 or more when a suspect can be identified"; "criminal violations aggregating $25,000 or more regardless of a potential suspect"; "transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction . . . [m]ay involve potential money laundering or other illegal activity[,] . . . [i]s designed to evade the BSA[,] . . . [or h]as no business or apparent lawful purpose or is not the type of transaction that the particular customer would

[98] MARK LABONTE, CONG. RSCH. SERV., R44918, WHO REGULATES WHOM? AN OVERVIEW OF THE U.S. FINANCIAL REGULATORY FRAMEWORK 14 (2023).

[99] *Id.*

normally be expected to engage in."[100] Consequences of noncompliance include "civil and criminal penalties, [such as] substantial fines, regulatory restrictions, loss of banking charter, and even imprisonment."[101] However, a safe harbor from civil liability applies to a bank and its directors, officers, employees, and agents who file a SAR.[102]

Notably, the BSA/AML SARs affirmative obligations are currently limited to financial institutions. Congress should begin by amending the statute in order to expand the statutory mandate to technology corporations. Next, Congress should address technology companies' ability to comply with new obligations. Because technology companies lack the requisite expertise to build AML compliance systems from scratch and financial institutions already utilize robust AML systems, legislation should incentivize partnerships in which the technology industry can utilize banks' existing AML infrastructure.[103] These partnerships would reduce implementation costs for technology companies, but they may still face significant hiring costs since human-led check remains the primary method of detecting money laundering.[104] Alternatively, technology companies could adopt fintech solutions

100 *BSA/AML Manual: Assessing Compliance with BSA Regulatory Requirements: Suspicious Activity Reporting*, FED. FIN. INSTS. EXAMINATION COUNCIL, https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/04 [https://perma.cc/FC7Z-Z2XS] (last visited Apr. 12, 2024).

101 *What is a Suspicious Activity Report?*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/what-is-a-suspicious-activity-report [https://perma.cc/TM4P-9Q3A] (last visited Mar. 5, 2024).

102 *See* 31 U.S.C. § 5318(g)(3).

103 There is a distinction between financial institutions providing their services to technology companies in their role as gatekeepers versus the financial institutions themselves being designated as gatekeepers. In the former case, prudential concerns are not as meaningfully implicated because banks are not the entities who bear the exclusive responsibility of effectuating the AML regime, nor do they risk liability for violating AML obligations. In other words, banks have less skin in the game, which minimizes systemic concerns.

104 FACCIA ET AL., *supra* note 82, at 32.

that use machine learning to analyze data and detect suspicious activity.[105]

Yet even if technology gatekeepers are equipped to comply with their affirmative obligations, they may flout the law if sufficient enforcement mechanisms do not exist. Historically, fines imposed on banks for AML deficiencies have failed to remedy compliance shortcomings; major banks have frequently been liable for repeat AML violations.[106] Moreover, there is a lack of streamlined coordination among the various financial regulators,[107] which may further undercut the effectiveness of enforcement actions. In order to prevent the same issues from plaguing this new gatekeeper regime, regulators should impose penalties that have more teeth, such as more punitive monetary fines (e.g., setting fines at a percent of profitability) or more severe criminal liability.

Another foundational feature of this gatekeeper system involves ensuring that regulators actually bring enforcement actions. The BSA/AML regime has traditionally suffered from weak enforcement, which leads to the law being under-inclusive. Even though the statutes articulate clear standards for enforcement, they are often watered down at best, or enforcement simply does not occur at worst.[108] That said, an effective AML framework does not necessarily need to detect and

105 COELHO, DE SIMONI & PRENIO, *supra* note 85.

106 *See* Laura Noonan & Alan Smith, *Global Anti-Money Laundering Fines Surge 50%*, FIN. TIMES (Jan. 19, 2023), https://www.ft.com/content/7a4821e6-96f1-475c-ae55-6401e402061f [https://perma.cc/TJ6Q-QQGA] ("There's a lot of evidence, particularly in the UK and the US, in terms of recidivism . . . repeat offending by the big firms after they've been fined for things.").

107 *See* Valentina Pasquali, *Enforcement Actions Against Capital One Raise Timing, Oversight Questions*, ASS'N OF CERTIFIED ANTI-MONEY LAUNDERING SPECIALISTS (Jan. 20, 2021), https://www.moneylaundering.com/news/enforcement-actions-against-capital-one-raise-timing-oversight-questions/ [https://perma.cc/4V9U-WGC4].

108 *See The Panama Papers: A Torrential Leak*, THE ECONOMIST (Apr. 9, 2016), https://www.economist.com/international/2016/04/09/a-torrential-leak [https://perma.cc/PHC2-G67L] ("Panama has been praised for passing a strong anti-money laundering law last year, though it remains to be seen if this will be rigorously enforced.").

punish every violation that occurs. Such an idealistic strategy would even be unrealistic due to resource constraints, including under-funding and under-staffing at bureaus such as FinCEN.[109] Rather, a more pragmatic approach would rely on gatekeepers' probabilistic risk calculations to inform their compliance decisions. This risk-based strategy would allow regulators to target the AML violations that they determine to be the most critical threats to the financial system. Regulators could articulate a more transparent, rule-based set of criteria that guide their enforcement decisions, such as transactions that meet a certain dollar threshold or transactions that occur on platforms known to have higher rates of criminal activity. If gatekeepers clearly understand regulators' priorities, then they will be able to focus their efforts on a handful of key concerns rather than casting too wide of a net. This may result in an under-inclusivity issue too, but to a lesser degree. Rather than an underenforcement issue stemming from a lack of regulatory resources, this regime would be intentionally narrowed in order to account for the enforcement constraints that gatekeepers and regulators will realistically face.

B. Circumventing the Metaverse's Architectural Hurdles

To summarize, this Note's gatekeeper liability proposal is ultimately a legal design-based solution. Regulators can influence the structure of the metaverse by shifting the platform towards one that is functionally more centralized and interoperable, thereby creating an environment that is more regulable. In this way, the law can be used as a tool to overcome the metaverse's architectural challenges. Recall that a key hurdle associated with decentralization is regulators' limited oversight when control is diffused across countless private actors.

---

[109] *See* Pete Schroeder, *U.S. Policymakers Seize on FinCEN Leaks to Press for Stepped Up Money-Laundering Fight*, REUTERS (Sept. 21, 2020), https://www.reuters.com/article/global-banking-fincen-congress/u-s-policymakers-seize-on-fincen-leaks-to-press-for-stepped-up-money-laundering-fight-idUSKCN26D09W/ [https://perma.cc/C88G-68PQ] ("[T]he enforcement group is understaffed to handle the millions of SARs that need to be analyzed to determine whether a crime has been committed.").

Deploying gatekeepers would address this shortcoming because the existence of gatekeepers would functionally centralize the scope of regulators' supervision. Regulators would no longer need to identify and directly regulate each individual actor. Instead, regulators could focus their efforts on inducing gatekeepers' compliance—a pool that is meaningfully smaller than all metaverse users—and gatekeepers in turn would be responsible for preventing money laundering among their respective users. A benefit of this legal design-based approach is that even if the metaverse remains decentralized from a formalistic perspective, creating gatekeepers alters the metaverse's architecture so that it is functionally more centralized and thus more conducive to regulation.

Next, a metaverse that lacks interoperability would present a similar scope-based challenge. If users are forced to transact in a different virtual currency on each distinct platform, then criminals may exploit this design feature by carrying out complex layering techniques. Once again, a legal design-based solution can functionally circumvent this challenge even if the metaverse remains minimally interoperable. The crux of the interoperability challenge stems from incomplete information flows; regulators must piece together disparate strands of information in order to create a comprehensive account of the crime. If gatekeepers like Meta, Google, and Microsoft have affirmative obligations to share detailed information with the government, then regulators will benefit from receiving data about each gatekeeper's respective platform. These gatekeepers can therefore be "envisioned as acting interdependently and thus as forming an interlocking and interacting web of protection against corporate wrongdoing"[110] because the distinct information that each gatekeeper provides

110 Tuch, *supra* note 90, at 625. *See also* DELOITTE & INST. OF INT'L FIN., THE GLOBAL FRAMEWORK FOR FIGHTING FINANCIAL CRIME: ENHANCING EFFECTIVENESS & IMPROVING OUTCOMES 2 (2019), https://www.iif.com/portals/0/Files/content/Regulatory/Financial%20Crime%20Report.pdf [https://perma.cc/FE4Y-DGY4] ("Different financial institutions each may hold information on the same customer which may overlap, but which may also be inconsistent and incomplete, a weakness which criminals can navigate in order to exploit the financial system.").

will fill in gaps and bolster other gatekeepers' information streams. By creating a system that requires technology companies to report suspicious activity to FinCEN, regulators are more likely to have the necessary information at their disposal to combat money laundering.

Finally, this proposed gatekeeper regime would allow regulators to work around anonymity challenges. Cryptocurrency is central to financial transactions in the metaverse, but it raises identity-verification challenges because it bypasses a financial intermediary. Regulators can technically trace cryptocurrency transactions through ledgers because the currency is pseudonymous, but the practical limitations on assembling piecemeal strands of information together impede effective identification. In fact, cross-chain bridges, which are software applications "used to send digital assets across blockchains, bypassing a centralized service that can trace transactions," exploit this precise loophole, so they are a tool of choice for criminals.[111] In order to address these information gaps, regulators should leverage each gatekeeper's "distinct spheres of influence and expertise."[112] This is especially critical if each gatekeeper can provide unique information about the specific transactions carried out using the digital currencies on their respective platforms. This information will improve regulators' ability to trace the chronology of financial transactions and identify money launderers.

V. CONCLUSION

Due to the metaverse's rapid growth and its potential to transform the digital economy, regulators should modify the existing BSA/AML framework in order to improve its efficacy on the platform. Legislative action would be prudent sooner rather than later in order to minimize the influence of regulatory capture and to ensure maximal focus on safeguarding the

111 MacKenzie Sigalos, *Crypto Criminals Laundered $540 Million by Using a Service Called RenBridge, New Report Shows*, CNBC (Aug. 10, 2022), https://www.cnbc.com/2022/08/10/crypto-criminals-laundered-540-million-using-renbridge-elliptic-says.html [https://perma.cc/L5L8-75L5].

112 Tuch, *supra* note 90, at 625.

financial system from abuse. To achieve this aim, regulators can create a gatekeeper liability regime that relies on technology corporations. This framework, based on principles of legal design, would circumvent the metaverse's architectural challenges and shape the platform into one that is more regulable. Ideally, the resulting metaverse would close the gates on money laundering by building in robust guardrails against illicit activity.