FEBRUARY 9, 2023 • BLOG • 1 MINUTE READ

Financial crime in the metaverse

Sentinels

The metaverse raises a number of legal and regulatory compliance issues, including data privacy, intellectual property, and consumer protection. Nevertheless, financial crime is becoming increasingly endemic in the metaverse as well.

Understanding the metaverse

The metaverse is a term applied to the technologies that aim to fuse the innovations of the digital age with the social connections of the real world. Web2.0 metaverses are considered to be the traditional use of apps under the control of a single entity. Conversely, web3.0 represents a more immersive metaverse in which ownership and control are decentralized.

The web3.0 metaverse is a 3D version of the internet - a parallel dimension to the physical world where one can lead a hyper-realistic, virtual life. This mixed reality universe blends physical and digital worlds in which real people with real-life behaviors and objectives engage with each other via a virtual identity.

As a virtual space, it allows people of all ages to have real-time interactions and experiences across distance using devices such as virtual reality headsets. Such interactions include the direct exchange of digital assets. Companies such as Facebook (now

But given that Meta alone has spent $36 billion on the metaverse this is a space that is set for further expansion in coming years.

How money works in the metaverse

Users can spend real money in the metaverse to buy virtual assets.

The metaverse operates both “open” and “closed” worlds. “Closed” represents a world where money can go in but it cannot come out, such as clothing or accessories for avatars (wearables) on the gaming platform Roblox, which have no value or transferability outside of the Roblox metaverse. “Open” refers to a world where digital assets can move in and out of the metaverse. Examples include Sandbox and Decentraland – these are blockchain-based metaverses which offer users the opportunity to explore the blockchain economy by buying and selling digital assets using cryptocurrencies or NFTs.

As an alternative reality, users can behave in the metaverse in ways that mirror the physical world, buying virtual property or in-world items, and possibly even setting up a business in the metaverse space itself. However, there is no centralized management of asset ownership in these worlds, rather they are recorded on a public blockchain.

The decentralized nature of the metaverse can lead to a number of dangers, including lack of regulation. Without a centralized authority to oversee and regulate activity in the metaverse, there is no inherent mechanism for addressing issues such as financial crime.

Financial crime in the metaverse

The metaverse is hailed as a key player in boosting the digital economy due to its high value projection. Given its value and popularity, as well as the high proportion of crypto-assets traded across the metaverse worlds, it’s an attractive target for financial crime. Unlike other risks, metaverse cybercrimes have more enduring and pervasive effects, representing a threat to the global financial system while slowing progress and technical innovation.

In addition, the metaverse is exposed to financial crime by virtue of its unregulated and largely unexplored territory. It also provides a platform for anonymous transactions and communication. These downfalls enable fraudsters to experiment with new strategies, employing sophisticated methods using NFTs and decentralized finance (DeFi) platforms to advance their corrupt activities, in an attempt to defraud users and businesses.

Phishing and scams

Fraudsters will employ conventional strategies, such as phishing attacks to gain access to accounts and extort money or NFTs a user holds.

By posing as legitimate metaverse projects and tricking users into clicking on a phishing link or sending money to the scammers' wallet, scammers attempt to gain users' trust.

This threat is further heightened as crypto transactions are practically irreversible due to the independent blockchain nodes, and can only be refunded by the receiving party.

Money laundering

Perpetrators are using the metaverse as a vehicle to launder illicit gains obtained from real world or crypto-based crimes using a number of techniques.

For instance, criminals may use multiple accounts and virtual currencies to move money through the metaverse without leaving a trace.

They can convert illicit funds into a digital asset, such as NFTs, land or wearables, and then sell it on a virtual marketplace for real-world currency. These marketplaces may be poorly regulated, making it easier to hide the proceeds of their illegal activities.

KYC checks are not typically required to purchase metaverse marketplace assets. In an environment where these marketplaces have facilitated multimillion-dollar transfers of virtual property, this poses a significant risk.

A fraudster would be able to purchase land and resell it to another user, be it through a secondary market or directly, as a way to legitimize their income.

Sanctions evasion and terrorist financing

Compliance inefficiencies along with the metaverse's decentralized nature allow sanctioned actors or nation states to abuse metaverse-related crypto assets in order to circumvent sanctions.

They can do this via pseudonyms or anonymity-enhancing technologies to conceal their identity, and by using decentralized platforms that are not under the jurisdiction of any particular government, making it easier to operate without detection.

Similarly, fraudsters may look to explore fundraising for sanctioned actors or those linked to terrorism via metaverse-related assets. By creating fake or fraudulent crypto assets they can solicit investments from unsuspecting individuals.

marketplaces to buy and sell illicit goods or services, such as drugs or weapons, and use the proceeds to fund their activities.

Compliance Solutions

Both businesses and individuals are left exposed to the metaverse's financial crime risks as illicit behavior is not as visible in this new and largely undiscovered dimension.

To address their own realities and unique situations, regulators and financial institutions must ensure they are employing the most recent and reliable procedures, systems and software to mitigate risks of financial crime through metaverse-related assets. Stakeholders can take a number of steps to combat fraud in the metaverse, for example:

1. Developing clear and enforceable regulations for the metaverse, including guidelines for what constitutes fraud and how it should be handled.

2. Screening metaverse-related assets, wallets and transactions for suspicious activities in order to defend against dangers of money laundering and sanctions. This will help determine any direct or indirect risk exposure. Mitigation steps can involve preventing withdrawals or notifying the appropriate authorities.

3. Educating users about the risks of fraud in the metaverse and providing them with guidance on how to protect themselves.

It's crucial to have a comprehensive understanding of the hazards associated with both a single metaverse and numerous metaverses, as nefarious actors frequently try to operate across a variety of assets via blockchain interoperability.

This can prevent the perpetrators from trying to "clean" money through one asset or metaverse while hiding it in another.

As a result, having access to the results across several blockchains and/or metaverses when screening assets or transactions related to metaverses can aid in uncovering these threats. These are just a few examples of the compliance limitations that the metaverse faces.

What's next for the metaverse?

As the technology continues to evolve, new issues are likely to arise, and regulators will need to keep pace with these developments in order to protect users and maintain a safe and fair digital space.

The metaverse's evolving financial ecosystem represents new and unexploited opportunities for banks to loan against these virtual assets, be it cryptocurrencies, NFTs or even virtual property.

Many of these issues fold into some of the fundamental problems that the crypto industry is facing. The lack of cohesive regulations and a lack of clarity around how to execute on regulations while still meeting the values of the crypto project.

But having effective transaction monitoring in place doesn't mean going against the mission underpinning various metaverses. In fact, by taking advantage of newer technologies, metaverse-focused companies and those that interact with them, can intervene against the problem of financial crime before it gets started in these digital worlds.