Unsplash © Minh Pham

# Multiple identities, security, and the growth of the metaverse

## Mark Zuckerberg's announcement in late 2021 that Facebook, Inc. was to be renamed 'Meta' triggered a seismic shift in the public's perception of the metaverse.

---

Previously, the term ‘metaverse’ had largely been the preserve of academics, theorists, media artists and tech-savvy industry insiders, who, with the rapidly innovating developments in virtual & augmented reality (VR & AR), and decentralised technologies such as blockchain, had envisaged a new dimension of digital interaction – and with it a potential revenue source worth billions of dollars.

Zuckerberg changed that. He released a video exploring his utopic vision for how the metaverse – or, more aptly, *his* metaverse – could look, and committed Facebook’s future (and resources) to the vision.

Everything from commerce, to work, to social interactions could be undertaken in his metaverse, and not only that but it would be *better* than those experiences in the physical world. *Anyone could be anything*, and individual expression was a key selling point for the user experience.

Zuckerberg’s vision is just one iteration in a raft of competing metaverses, with other popular versions such as The Sandbox and Decentraland already established before the rechristening of Meta. Part of these worlds’ appeal is that users can dictate their appearance. An avatar might be a facsimile of their real-life appearance, or it might have hooves. Or, six arms. Or, a brick instead

of a head. Or, all three, in totally separate avatars. In short, the possibilities could be limitless.

The issue is, there must be limits within any infrastructure, no matter how limitless it aims to be. There is a reason we have laws in society: to create order and propriety. This too must be the case within the metaverse.

The possibility of creating multiple avatars raises issues with authenticity and accountability. In order to limit fraud and malicious metaverse identities, there must be a system in place to ensure the identification of the person behind the avatar. This will stymy the inevitable influx of bad actors hiding behind multiple anonymous false identities, including bots, which could otherwise take the form of counterfeit avatars spreading malware throughout the digital world. Secure, verifiable identity is the only option where complex financial transactions take place that will be necessary for the metaverse to become a truly transformative virtual ecosystem.

For example, metaverses such as the aforementioned Decentraland offer users the option of buying virtual property (prices vary hugely at the moment, but recent estimations put the average value for a plot at $3,000. And – although this is a discussion for another article – the selling of 'land' within metaverses is paradoxical because one of the great values of the digital universe is that there, unlike in the real world, physical space is not a rare and precious resource; it is theoretically infinite).

This, naturally, creates the opportunity for a reality-mirrored system of property mortgages and loans, which could be carried out by existing banks. When dealing with complex financial instruments such as this, transparent authentication becomes a necessity.

At *Tintra,* we're developing an infrastructure that will allow such transparency. Though our own vision for the metaverse is not bound by the parameters set by existing companies, we are making sure that our software is completely interoperable between ecosystems, allowing universal access to the features we are developing.

*Read also*

Meet Improbable, developing the technologies powering interconnected metaverse experiences

However, the public nature of blockchain creates problems for retaining multiple identities while keeping one's real identity private and secure. In other words, not every user will want their real identity to be known, yet must be held accountable for their actions and transactions within the metaverse. Therefore, a system must be implemented whereby people can create multiple identities which could potentially remain (partially) anonymous in a range of circumstances, but which can also be securely verified when called into question.

This is also something that Tintra is addressing. We believe that security and anonymity can – and must – coexist across metaverses, where currently they do not. Our software is designed to run in parallel with these ecosystems, creating a frictionless experience that does not interfere with the userface.

Our wider mission as a company has always been to reduce unnecessary mechanisms within existing (and often outdated infrastructures), and this is something that we're carrying over into the metaverse. It is often easier to create new solutions than it is to fix existing problems, which is why the tabula rasa of the metaverse presents such a unique and exciting opportunity.

Connectivity is at the heart of the metaverse, and we are simply facilitating that. Safeguarding must exist both for both the consumer-focussed aspects of the metaverse, and also for the corporate. If the vast potential of these environments is to be unlocked, the proper regulatory systems must be in place.

Davy Smith, Chief Innovation Officer at *Tintra.*

---

Article by DAVY SMITH