Banking in the metaverse and the question of identity

In global terms, the banking sector is one of the leading industries where Web 3.0 technologies are implemented. Ultimately, with utility in the real world, Web 3.0 is also the foundation of a banking system in the metaverse.

One of the principal challenges for banks and regulators will be how individuals will interact with such banking platforms in the metaverse. For example, how banks will verify an individual's virtual identity, or avatar, with their real-world identity. The capability to prove the provenance of a virtual identity will touch every fundamental aspect of banking; without it there is little possibility of tracking identity theft from impersonation or preventing fraud.

In broad terms, there are three basic approaches to managing identity in the metaverse.

The first is to allow individuals to have multiple identities for different purposes and in different sub-domains within the Metaverse, with each of these identities verified by individual monetary system administrators. This approach would maintain an individual's privacy and security but could add complexity, and involve multiple intermediaries (and would therefore be more prone to vulnerabilities and fraud), and would be difficult to regulate.

The second is to create a decentralized identity system. For this to work, the system would have to be what's termed 'trustless', meaning it would have to be trustworthy as a standalone system distributed among many different nodes on a blockchain. With this option, a person's real-world identity could, say, be embodied within a non-fungible token (NFT) that would aggregate unique identifying components of information such as, for example, government-backed identity verification, social media attestations, biometric data, and personal attributes. No intermediaries would be involved, instead third parties, including banks, would decrypt the token to establish that someone is who they claim to be.

> **Proof of identity, identifiability, provenance, and trust. Without these, banking in the metaverse will not materialize.**

The third is to create a global identity system, an approach that offers optimal security and privacy controls. The system would generate a real-world unique identifier that could be linked to an individual's virtual identity or identities. However, such a system would need to be universally adopted and would have to interface with the disparate array of existing identification systems used by individual nations across the world. A centralized global system would also run up against geopolitical resistance (who would govern it?) and could take decades to formulate and ratify. In which case, individual nations or consortia may resort to developing and implementing their own systems, leading to a fragmentation of monetary systems, and taking us back, full circle, to multiple identities approach.

Countries that have centralized, sophisticated identity systems in place – like Saudi Arabia – will find themselves in a favorable position to either establish their own proprietary identity system with a distributed monetary system, or they may wish to integrate into a global identity system that will either be based on a distributed, decentralized, or mixed monetary system.

Another level of complexity is the way identity will be integrated within a monetary system which may need to support a variety of fiat, digital, and crypto currencies

Technical and operational banking framework level

Web 3.0 is the process framework that will support banking in the metaverse.

- **Transactions and fiat/crypto integration**
  The systems that facilitate the transaction of value in exchange for digital assets. In the metaverse, banking transactions may involve cryptocurrencies fiat currencies or both. Exchange mechanisms between dimensions will be required.
- **Digital assets**
  A class of intangible assets that are verifiable and ownable and include cryptocurrencies, non-fungible tokens (NFTs), native tokens, stable coins and real-world assets
- **Smart contracts**
  The use of verifiable contracts on the blockchain will enable contracts, agreements, and terms to be executed or enforced. An example is a payment to a commissioning agent on the sale of an NFT.
- **Distributed ledger (blockchain)**
  The integration of a digital, decentralized, distributed ledger that facilitate the recording of transactions, yet coexists with a proprietary banking model.

and that can be used by a payments transaction system that will operate across both real and virtual worlds. Banking in the real world uses a distributed system and intermediaries and entities that are vetted and trusted, identifiable and identified and have various rights and responsibilities. This enables one of the most fundamental aspects of banking – reversibility – which allows for transactions to be undone and is a mainstay of managing fraud and resolving, for a limited time, any issues with transactions.

Cryptocurrencies, on the other hand, use decentralized systems (although not all the time), typically on blockchain, which forgo identifying and restricting who can participate. Unlike a conventional payments transaction system, the participants in a transaction are identified only by cryptographic keys (a key is a long-string random number). A private cryptographic key allows for the creation of a public key (another random number) both of which are then used by the participants to create a public key signature which is used to action the transaction. At no time during the transaction is any participant's identity revealed which means at no point is a real-world identity associated to the transaction. How cryptocurrencies will integrate with conventional banking is not apparent; with no single identifiable third party, and no way of identifying the participants involved in the transaction, there is no way to reverse or block disallowed transactions.

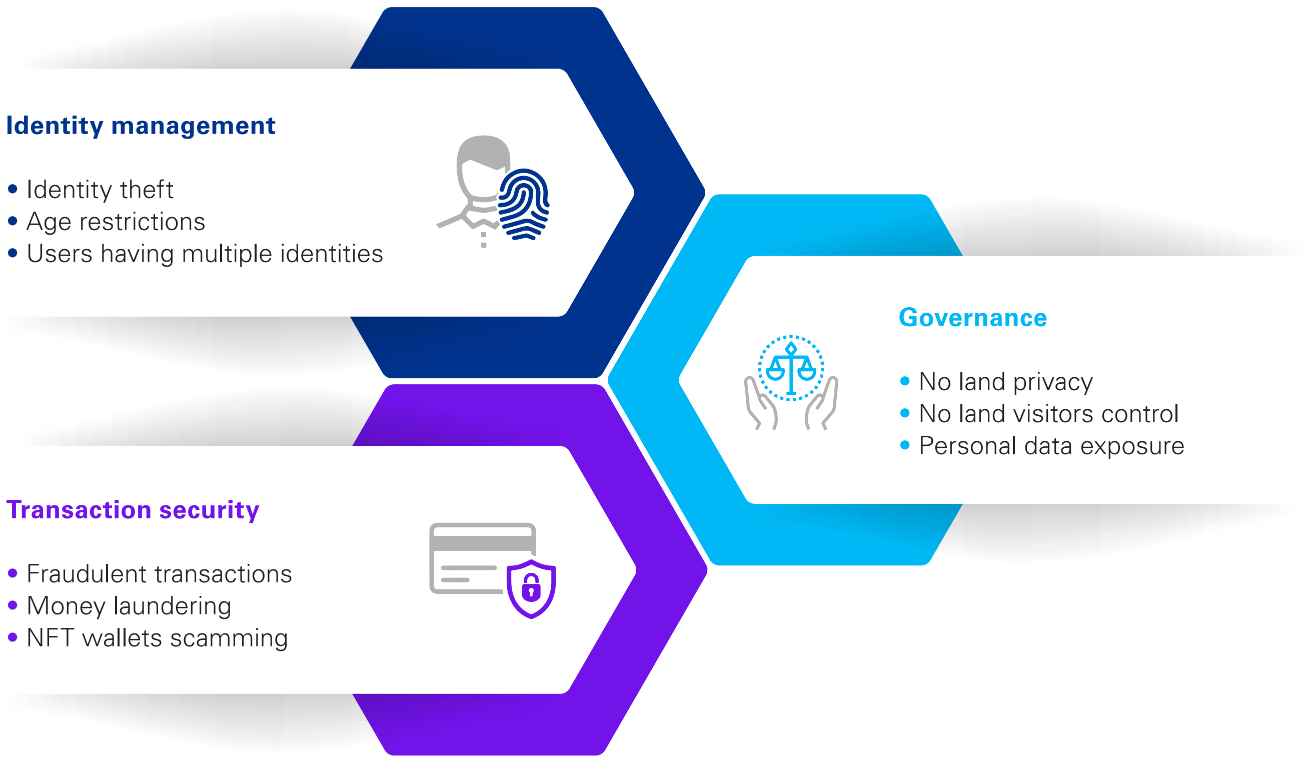
Identity management is the first of three pillars of a robust banking system in the metaverse; the other two are governance and transaction security and are at focus here. Progress is being made on all fronts and there are signs that banking in the virtual world will soon be a reality. Virtual bank branches are a next step for banks in metaverse, whereas insurance firms are expected to start providing services for digital currencies, such as NFTs, and virtual assets such as land and buildings.

What will a secure banking model look like in the metaverse?

Theoretically, there will be three tiers to the operational model. The first is the central bank which will set the regulatory framework and award licenses and certifications to operate within the virtual realm. In time, the central bank may set its own digital currency, although the preference will be to allow the market to decide for reasons that stronger, less volatile currencies, in whatever form they may take (NFT, token, stable coin), will eventually win through and dominate.

Identity management – one of three pillars facilitating a robust banking model

Financial services institutions are facing elevated operational risks with a spectrum of functions when they choose to exist in the metaverse.



Identity management

- Identity theft
- Age restrictions
- Users having multiple identities

Governance

- No land privacy
- No land visitors control
- Personal data exposure

Transaction security

- Fraudulent transactions
- Money laundering
- NFT wallets scamming

The next tier comprises the financial institutions that will establish an operating protocol that aligns with the central bank framework, typically this will be through, standardized smart contracts on the blockchain. Validity of each bank could be proven using land control verification, such as a soulbound token (a non-transferable NFT).

These help control identity management and increase the confidence that the user accessing the land is the same user who registered to it.

Once the bank is set up, a portfolio of services can be marketed and made available to avatars (customers) who have had their identities verified according to an accepted protocol. Any transfer of value will be processed by a transactional system that features strong multiple-factor authentication, the design of which will need to be determined and agreed on universally.

Lastly, the user – typically in the form of an avatar – will occupy the virtual world and interact with other avatars, retailers, and businesses as they go about their virtual lives. This will require a system of identity validation and verification between these various entities which will need to interface with the bank-owned transaction authentication system, much as it does in the real world. Finally, there will need to be some way of linking the virtual identity of the user and their transactions with the physical world, the simplest way being through a credit or debit card, or a more sophisticated way like integrating biometric authentication to digital wallets.

Setting up the identity validation, monetary and transactional systems that will enable banking in the metaverse will be a complex task with unique challenges. However, with global giants like JP Morgan and HSBC pioneering this space, banking in the metaverse isn't far away. A space to watch.

Maz Hussain
Head of Digital Lighthouse
Center of Excellence of Data Analytics, AI and Emerging Technologies
E: mazharhussain@kpmg.com