Identity & Protocols for Digital Securities

The financial sector is currently in a race against time to integrate emerging technology that can scale operations within capital markets and drive global liquidity but there is an increasing lag time between technology used in the traditional financial world

and the new technology that is constantly emerging from the blockchain sector. Access to capital markets is expanding and traditional established services will have to adapt large amounts of infrastructure in order to maintain pace with this change.

A growing demand for hybrid models of financial services has surfaced that utilizes current infrastructure by leveraging Blockchain Technology, Digital Securities and Digital Identity. There are many applications for all three of these technologies such as trustless systems, automated processes and minimizing time spent on human analysis. Counterparty risk, poor on-ramping mechanisms, unclear regulation and lack of awareness towards cryptographic tokens (like NFT's) are hindering the financial world from entering the Digital Asset realm. This is now being resolved by the rise of security token issuance and transfer platforms that can accommodate institutions and provide a foundation for accredited investors to access the market. A large obstacle to this is fragmented regulation and varied identity compliance, through KYC/AML procedures and a lack of common protocol standards.

One specific case in all of these happenings that plays a crucial role in the expansion of global liquidity is the development of interoperable identity systems and protocols for Digital Securities. As time progresses, financial services and communities of all sizes will adopt or develop different Digital Security protocols themselves, either internally or as part of a consortium of partners on top of existing technologies. A current example of this includes the ERC-1400 library of standards for security tokens built on the Ethereum protocol. The challenge in the coming years will be understanding how identity can then be verified across multiple Digital Security protocols simultaneously, utilizing Blockchain, Digital Securities and Digital Identity with regulatory compliance and thus opening up a new accelerated era of digital finance.

There are currently many technologically dated intermediaries that lie between many forms of financial transactions. Current entities that handle financial exchange such as clearing, settlement and custody services are centralised, regulated and already carry trusted positions of stability in the financial markets. This is important, as the role of trust these entities play

in our ecosystem can potentially still remain in place. A key hurdle to verification of Identity in decentralized networks is the selection of trusted third parties to verify identity. The idea that previously established trusted parties could remain in that trusted position as “nodes” within this digital finance framework is a possibility and a role that many financial institutions like investment banks may take in the future. Interoperable identity systems and Digital Security protocols can be key to unlocking the full potential of this new digitized financial ecosystem and may also help legitimize and absorb Identity & protocol development that would otherwise be segregated due to lack of access to capital.

Digital Securities can be divided into sub-categories representing different instruments be it equity, debt, commodities or tokenized derivatives. An identity system that is constructed on top of blockchain-powered Digital Security protocols must allow information to be verified at an extremely high frequency in order to allow a multi trillion-dollar market to operate at full capacity.

A Digital Security identity profile may contain differentiating smart contracts and multiple tiers of programmable information

that need to be reviewed and authenticated in a customized order by authorized parties. Examples of what these identity profiles may include are the following: Digital Security Type (Token Standard) — Price History — Voting rights — Governance Models — Legal Ownership — Exchange Records — Jurisdictional Metadata and any other contractual obligation or future utility information attached to the Digital Security. This information will then need to be analyzed and authenticated across multiple protocols at a sufficient speed, which is where Digital Identity can increase efficiency of data analysis and reduce labor-intensive costs. Furthermore the use of localized KYC and AML procedures will be tested as the electronic identity industry matures. From here, all this verifiable data can then be relayed over an immutable blockchain that can connect and record the entire verification process and ultimately be compatible with other authorized chains and digital security protocols.

The idea of a blockchain world, Digital Identity and Digital Securities all connected on an interoperable network in such a rigid ecosystem at this time is somewhat hard to imagine but will inevitably develop in the future, as businesses want to digitalize,

enhance their current systems and adopt a technologically driven approach to the markets. The infrastructure for identity and Digital Securities that is built to accommodate Digital Asset adoption will hopefully advance the financial sector forward, allowing for a network of interconnected markets and automated regulatory oversight.