

The Essential Role of Independent Attestation in Digital Asset Self-Custody and Decentralised Finance

By Peter Christo
December 2023

In the evolving landscape of digital finance, particularly within the domain of decentralised finance (DeFi) and digital assets, independent verification of proof of digital asset holdings (attestation) could become the cornerstone for establishing trust and integrity in the new digital economy. In this essay, I explore the critical role of independent attestation for digital assets not held by custodial services and exchanges but in self-custody by the owner and hardware wallets (non-custodial wallets).

At the heart of understanding independent attestation of digital assets is a comparison with the validation of physical assets like gold or art. Consider the traditional scenario where an individual owns gold bars securely stored in a vault. This vault's physical or digital key to the vault lies solely with the owner, ensuring control and restricted access. Periodically, an independent expert verifies the vault's contents, assessing the authenticity of the gold and confirming the owner's control over it. They provide a certificate attesting to these assets' genuine and secure possession. This process assures the owner and any potential stakeholders of the legitimacy and safety of the assets. This attestation can be used for insurance, tax, accounting and other commercial reasons.

With digital assets, such as Bitcoin, a similar process of attestation is equally pivotal. Here, attestation involves verifying the control and access to these assets without revealing specific details on the blockchain and without the private keys required to move digital assets. This verification form plays a vital role in ensuring the integrity and ownership of digital assets in a trustless environment. Just as the independent expert in our traditional example assures physical assets, digital asset attestation confirms digital assets' genuine, controlled, and secure holding.

This is, however, only part of the challenge. For example, auditing Self-Managed Superannuation Funds (SMSFs) or private 401Ks incorporating cryptocurrencies opting to capitalise on DeFi offerings like lending, staking and other offerings offering yield present new challenges to attestation. These include accurately valuing highly volatile

digital assets like Bitcoin, verifying transactions on decentralised ledgers cum exchanges (DEX), and comprehensively understanding the tax implications per ATO guidelines.

The intricacies of DeFi, with its reliance on blockchain technology and smart contracts, demand a high level of technological proficiency and financial acumen from auditors to ensure accurate, compliant, and secure management of SMSF investments in this innovative yet intricate financial sector. Moreover, the high trading speed, its global nature (and thus financial jurisdictions and, ultimately, regulations) and the 24-hour nature of DeFi make the audit job remarkably challenging.

Decentralised Finance by its very nature, means the absence of central authorities to validate transactions introduces unique challenges and opportunities in the emerging decentralised economy. As such, independent attestation becomes essential for verifying ownership and ensuring the integrity of these decentralised holdings. Cryptographic methods are employed to confirm transactions on the blockchain, a public and secure ledger, thereby mitigating fraud, maintaining transparency, and adhering to regulatory compliance. This aspect is particularly crucial in digital finance, where transactions are irreversible, and assets can quickly transfer globally.

Independent attestation provides an impartial and unbiased verification of asset ownership and integrity, which builds confidence within the DeFi ecosystem and enables users to engage with the assurance of their assets' safety and legitimacy. As a neutral arbiter, independent attestation services validate transactions and holdings in this decentralised context, free from conflicts of interest, allowing parties to enter into commercial agreements, comply with tax and regulatory obligations with a level of confidence due to an ability to see the ultimate source of truth within the context of their specific holdings and commercial situation.

With the growing interest of institutional investors in DeFi, there is an increased demand for risk management and compliance solutions. Regulatory agencies increasingly recognise the need to implement regulations that ensure consumer protection, prevent money laundering, and maintain financial stability while fostering innovation in the DeFi space.

As such, independent attestation is fundamental in the growth and broader adoption of DeFi. It is critical in establishing a secure, transparent, and compliant digital financial

ecosystem. The future of finance, heavily reliant on self-custody and decentralised mechanisms, hinges on establishing and maintaining trust. Independent attestation is not merely a service but a foundational aspect in realising the principles of decentralised finance. As the digital financial landscape continues to evolve, independent attestation will undoubtedly become more prominent, reinforcing its status as a linchpin in the secure and trustworthy management of digital assets.

This essay is protected under the DMCA (Digital Millennium Copyright Act), a legal framework established to safeguard digital content and the rights of content creators—inquiries to peter.christo@dacs.io.

Digital Asset Custody Solutions Pty Ltd.

Digital Asset Custody Solutions Pty Ltd (DACS) offers a specialised Cryptocurrency Attestation Service, ideal for various clients including individuals and businesses, to verify cryptocurrency holdings for financial purposes like tax reporting and investment analysis. DACS ensures client information is handled with utmost discretion, employing robust measures like double encryption. Please visit www.dacs.io for more information.

peter@dacs.io
www.dacs.io
WhatsApp: +61412133363