SMSF Crypto Assets

Why SMSFs Fail To Hold Crypto Assets Securely

May 2026 | Version 1.0

Executive Summary

SMSF auditors are required to verify that a fund's crypto assets are held securely and separately from personal assets, in line with ATO requirements. While trustees carry primary responsibility for digital asset security, auditors must be satisfied that these standards are being appropriately met.

Crypto security has evolved into two distinct tiers. The key point for SMSF auditors is that the standard retail-grade security used across most Australian exchanges does not adequately mitigate known risks associated with crypto-assets held within an SMSF. In contrast, institutional-grade security has become the global benchmark adopted by financial institutions, and it is this framework that informs the approach outlined in this document for the SMSF context.

Accordingly, the central concern for auditors is whether SMSFs holding crypto are meeting a level of security that would satisfy an informed interpretation of the ATO's requirements for assets to be held securely.

Contents

01. The Compliance Question

Under ATO regulations and superannuation legislation, SMSF trustees are responsible for the security of their fund's digital assets. Those assets must be held securely and kept separate from personal holdings. Auditors are required to obtain evidence that this standard is being met or they must report that the fund is in breach.

Crypto-asset security has developed significantly recently resulting in two distinct security grades. The question auditors need to be able to answer is not whether a fund's assets are held securely to mitigate the primary theft and loss vectors present with crypto.

---

02. What "Held Securely" Means

The ATO expects that SMSF assets be, what is known as, 'held securely'. Applied to crypto assets, the reasonable interpretation of that requirement is that there is **no credible risk of theft or permanent loss.**

With the arrival of financial institutions into the space, crypto-asset security has evolved into two grades. Financial institutions that allocate to crypto have established their own requirements through procurement decisions, and those requirements define what the upper grade looks like in practice.

Institutional-Grade Security has emerged as the minimum standard applied by financial institutions where:

- assets are held with a licensed digital asset custodian such as Zodia or Bitgo
- crypto withdrawals from the account are blocked so that a compromised account cannot result in stolen assets, and

- fiat withdrawals are whitelisted to verified accounts only.

Retail-Grade Security is, by definition, what falls outside that standard. With custody, individuals are recommended to store assets either in ‘exchange custody’ or ‘self-custody’.

---

03. Security Features That Do Not Hold Up

SMSF auditors currently request a range of security evidence from crypto platforms, including Audit Reports and Proof of Reserves. The following assessment covers the most commonly cited features and what they actually demonstrate in the context of SMSF compliance.

Audit Reports. An exchange Audit Report is an independent assessment verifying that a platform's systems, security protocols, and financial safeguards are designed and operating effectively. Most credible exchanges already operate to SOC (System and Organisation Controls) standards developed by AICPA. However, an Audit Report does not confirm that assets held in a specific account are protected from theft. It is not relevant evidence for this purpose.

Proof of Reserves. Following the FTX collapse, publicly presenting exchange-held crypto balances with blockchain addresses became a common market confidence signal. Unless reserves are compared against total client holdings, they demonstrate nothing and are simply a marketing trick. Holding $2 billion in assets is not evidence of security if the exchange was meant to hold $3 billion in client accounts.

Other commonly cited features:

- **Two-factor authentication.** All exchanges offer 2FA, and it is increasingly compulsory. It provides a baseline layer of login security. However, 2FA

can be bypassed, typically through account holder error or social engineering, and it does not prevent asset removal once account access is obtained.

- **AUSTRAC registration.** A compliance requirement to confirm that a platform has met its anti-money-laundering registration obligations. It provides no protection for client assets.
- **Fireblocks integration.** Several Australian exchanges cite 'We use Fireblocks' as evidence of strong security. In reality, Fireblocks is an Israeli digital asset infrastructure company used by exchanges to manage their own internal custody operations. It is not a licensed custodian in Australia, and its sole custody licence covers US markets only. It is not a client asset security measure.
- **Chainalysis.** Chainalysis analyses crypto transfers for links to criminal activity. It provides no security for individual account assets.
- **ISO 27001 certification.** Relevant to claim professional privacy and operational standards. It does not address whether client assets can be stolen from an account by an unauthorised party.
- **1:1 Reserves.** Without independent, ongoing verification, this claim is unverifiable. Balances change daily and a point-in-time assertion does not confirm ongoing security.
- **Australian owned and operated.** Relevant context for some regulatory considerations. Not a security standard.
- **Penetration testing and related measures.** Professional and worthwhile practices. They do not confirm that assets are held to the standard required for SMSF compliance.

---

04. The Three Risk Areas

Crypto-asset security for SMSF purposes should be assessed across three areas. Each must be adequately addressed for assets to be considered securely held.

- **Risk Area 01: Asset Custody.** The risk that assets are lost or stolen due to how private keys are held and managed.
- **Risk Area 02: Account Security.** The risk that assets are stolen or lost through account compromise, user error, or platform-level hacking.
- **Risk Area 03: Platform Security.** The risk that assets become inaccessible or are lost in the event of platform failure.

---

05. Asset Custody Risk

Custody of crypto assets refers to control of the private keys. That control can rest with three parties: a regulated digital asset custodian, the exchange itself, or the account holder through self-custody.

Retail-grade security places assets in exchange custody or self-custody. Australian exchanges apply strong operational security and have solid records relative to global peers. The limitation is structural: no exchange holds sufficient financial reserves to compensate clients for losses from a significant breach, and global exchange hack losses have continued to rise annually. This risk is widely acknowledged within the industry so experts always recommend self-custody.

Self-custody places private key control with the account holder, typically via a hardware wallet such as a Trezor or Ledger. Assets held this way have been permanently lost due to lost or damaged devices, forgotten passwords, the death or incapacity of the keyholder, and the absence of workable recovery procedures. For a superannuation fund with a legal obligation to preserve member assets over time, self-custody introduces risks that are difficult to manage within a compliant fund structure.

Institutional-Grade Security requires assets to be held with a regulated, insured digital asset custodian. In Australia, Bitgo and Zodia are established providers operating in this space. Assets are held independently of the exchange and the custodian is regulated and insured. Licensed custody involves a monthly fee based on asset value, which is standard in institutional settings.

> *Wealth99 has stored client assets with a regulated independent custody for five years. What must be understood is that assets are stored in the same account so there is no possibility of verification of individual client account balances.*

---

06. Account Security Risk

Crypto exchange retail accounts are designed to serve multiple purposes: trading, payments, and transfers between platforms. Crypto withdrawals are enabled by default. This creates a structural risk for accounts holding superannuation assets: an attacker who gains access to an account can permanently transfer assets to an external wallet, and that transaction cannot be reversed.

Account-level loss can occur in two ways: direct crypto withdrawal to an attacker-controlled wallet, which is irreversible; or liquidation of holdings to fiat and transfer to an external bank account, potentially overseas.

No combination of standard security features fully eliminates the first risk. Two-factor authentication, device verification, and login monitoring reduce the likelihood of unauthorised access but do not prevent asset removal once access is obtained. **The only control that eliminates this risk is blocking crypto withdrawals at the account level.**

A crypto account structured for wealth holding operates differently from a trading account. Clients can deposit crypto and fiat but can only withdraw capital in fiat. Crypto remains on the platform. Fiat withdrawals are restricted to whitelisted bank accounts in the account holder's name. This structure removes the primary account-level theft vector and is the defining difference between a retail trading account and a wealth account designed for holding superannuation assets.

---

07. Platform Security Risk

It is not possible to determine the financial strength of a private company with certainty. The relevant concern for SMSF purposes is whether, in the event of platform financial difficulty, assets can be independently accessed and recovered.

There are currently no regulatory controls or industry standards that provide investors with structured assurance on this point yet the requirement to own an Australian Financial Services License [AFSL] is being introduced in mid 2026. Wealth99 was one of the first exchanges to work with an AFSL through its CAR with its sister company, RWA in 2025. The risk is compounded with international platforms, where assets may be held offshore. Every platform should have a clearly documented policy for asset recovery in the event of financial difficulty.

End-of-year balance statements provided by the platform are not a substitute for independent verification. They reflect a single point in time, can be manipulated, and cannot be independently confirmed after the fact. The appropriate standard is auditor read-only access to SMSF accounts at any time, not only at year end.

---

08. What Auditors Should Require

The following three requirements reflect the framework applied by financial institutions when allocating to crypto assets. They represent current institutional practice, not an aspirational benchmark. A platform that cannot meet all three is operating at retail-grade security.

Requirement 1: Licensed Custody. Assets must be held with a regulated, insured digital asset custodian holding a relevant licence in their jurisdiction of operation. Established custodians operating in this space include Zodia and Bitgo. Digital asset infrastructure providers such as Fireblocks are not custodians and do not satisfy this requirement.

Requirement 2: Blocked Crypto Withdrawals with Whitelisted Fiat. The SMSF account must be structured so that crypto cannot be withdrawn to external wallets. Fiat withdrawals must be restricted to whitelisted Australian bank accounts held in the account holder's name. This is the control that eliminates the primary account-level theft vector.

Requirement 3: Independent Auditor Access. Auditors must have read-only access to the SMSF account at any time, independent of the platform's cooperation. Year-end balance statements do not satisfy this requirement.

---

09. Wealth99's Approach

Wealth99 has been a pioneer in the crypto-wealth sector since 2018. The platform was among the first in Australia to apply Institutional-Grade Security controls to retail SMSF accounts.

In 2021, client assets were moved to a licensed digital asset custodian. In August 2023, crypto withdrawals were blocked across all accounts and fiat withdrawals were

restricted to whitelisted Australian bank accounts in the account holder's name. These are the same structural controls that financial institutions require.

The practical outcome has been that the account structure itself has functioned as the primary security layer. Since those controls were implemented, no Wealth99 account has been successfully compromised. In two separate cases, clients experienced theft from personal bank accounts held at other institutions. Their Wealth99 accounts were unaffected, as the structural controls prevented any unauthorised access from resulting in asset loss.

Wealth99 has engaged directly with the ATO on the matters covered in this report. The retail-focused crypto exchange market has historically been designed around trading functionality and accessibility, rather than the custody and security standards required in regulated financial environments. As a result, the distinction between retail-grade and institutional-grade security has not been consistently reflected in SMSF auditing practice. As ATO guidance in this area develops, the three requirements outlined in Section 08 represent the standard that auditors will need to apply.

This document has been prepared by Wealth99 and reflects our analysis of crypto-asset security standards in the context of Australian superannuation law. It does not constitute legal advice. Readers should verify requirements with the ATO and assess each fund's circumstances independently.