BitGo



Australia's Digital Asset Transition: Turning Regulatory Clarity into Business Value

Six practical questions for business leaders delivering services that customers value, meeting institutional standards and generating sustainable returns.

Last updated: 2026 November

From Regulatory Direction to Commercial Decisions

An industry perspective from Angela Ang, BitGo's APAC Managing Director

Australia has reached a watershed moment for regulatory clarity in digital assets. A legislative framework for digital asset platforms is in place, and work beyond Project Acacia is underway. Institutions have a firmer basis for deciding where and how to participate.

The questions for institutional leaders are now practical. How should businesses turn these developments into services customers value? And how can they deliver those services to institutional standards while generating sustainable commercial returns?

Regulatory clarity helps institutions commit resources. Sustainable returns depend on how those resources are deployed: the balance between building and partnering, the integration of governance and customer protection, and the ongoing cost of reliable execution and settlement.

Leaders can begin that assessment while regulatory standards are being finalised. Drawing on my experience implementing digital asset regulation in Singapore and BitGo's work with global institutions, this briefing brings an international perspective to six practical questions for Australian leaders. They cover the operating decisions, supporting evidence and preparations worth considering.

About Angela Ang

Angela leads BitGo's regional operations and serves as resident executive director of its Singapore-regulated entity. She previously spent over a decade at the Monetary Authority of Singapore (MAS), where she led the team responsible for building and operationalising Singapore's payments and crypto-licensing framework.



About BitGo

BitGo (NYSE: BTGO) is the digital asset infrastructure company, delivering custody, wallets, staking, trading, financing, and settlement services from regulated cold storage. Since our founding in 2013, we have been focused on accelerating the transition of the financial system to a digital asset economy. With a global presence and multiple regulated entities, BitGo serves thousands of institutions, including many of the industry's top brands, exchanges, and platforms, and millions of retail investors worldwide.

REGULATORY CONTEXT

As of November 2026

The Corporations Amendment (Digital Assets Framework) Act 2026 ("DAF Act") establishes the new regulatory framework for digital asset platforms and tokenised custody platforms. ASIC's CP 392 (published October 2026) proposes implementing guidance and standards; these are not yet final.

Key Dates
27 November 2026: CP 392 feedback due.
March 2027: ASIC publishes finalised instruments and regulatory guidance
9 April 2027: The DAF Act commences and licence applications open
7 October 2027: Close of transition window for existing firms to make a licence application (new application or variation)

Six Questions for Australia's Digital Asset Transition

Use these six questions to focus leadership discussions and turn regulatory readiness into a practical operating plan:

1. **Can Customers Recover Their Assets When Something Goes Wrong?**
   Customer protection must work when normal operations stop.

2. **Who Is Accountable Across the Service Chain?**
   Every critical responsibility needs a clear owner, especially when several providers deliver the service.

3. **Which Operating Model Will Make the Business Viable?**
   Choose the model the business can sustain as customers, costs and requirements change.

4. **Can Assets Move Reliably When Customers Need Them?**
   Custody, liquidity and settlement must work as one service, including under pressure.

5. **What Can Australia Adopt from International Experience?**
   Adapt proven approaches to Australian customers, laws and market economics.

6. **What Should Leaders Do Now?**
   Build readiness now and preserve flexibility around requirements still being finalised.

1 Can Customers Recover Their Assets When Something Goes Wrong?

Customer protection must work when normal operations stop.

INSIGHTS

Customer protection depends on legal rights, transaction controls and practical access working together. Assess the full arrangement, including whether those protections hold when a provider or process fails.

Protecting digital assets requires institutions to understand three distinct matters: the customer's legal rights, who can technically authorise transactions and whether assets can be accessed or recovered when something goes wrong.

A customer may have a legal entitlement to assets without directly controlling the cryptographic keys used to move them. A platform may maintain accurate ownership records while relying on separate systems or providers to process withdrawals. Those differences matter during outages, financial distress and transaction failures.

Technical safeguards alone do not establish adequate customer protection. Cold storage keeps the private keys used to authorise transactions offline, reducing exposure to certain online attacks. Multiple approvals can provide additional protection, but only when they involve meaningful, independent checks.

For example, several approvers may independently authorise a transaction but rely on the same compromised interface to verify its destination. Multiple approvals would then reproduce the same error rather than prevent it. Effective controls must include independent transaction verification.

ASIC's CP 392 reflects the importance of evaluating outcomes rather than prescribing every technical arrangement. Paragraph 66 describes a preference for principles-based, technology-neutral requirements instead of detailed rules governing hot and cold wallet allocations or key-management processes.

This flexibility accommodates different custody models and allows security practices to evolve. It also places greater importance on understanding whether individual controls deliver the intended protections.

Practical access and reporting also matter. For a self-managed superannuation fund (SMSF), a custody arrangement must work with the fund's administration and reporting processes. Trustees, administrators and auditors need access to information required for their respective responsibilities.

Institutions should assess legal holding arrangements, transaction authority, recordkeeping and recovery together. The question is whether customers' interests remain protected when normal processes fail.

Lucas Dobbins, CEO of BTC Markets, connects asset protection with broader institutional participation: **“Institutional adoption in Australia has always come down to asset safety and trust. CP392 would make licensed custody the standard, creating the confidence needed for broader institutional participation.”**

→ **Action: Trace a digital asset withdrawal across the full provider chain under normal conditions and during an outage. Check the ownership evidence, transaction authority, independent verification and access to records needed at each step.**

> **Outcome: A documented assessment of the withdrawal and recovery process, identifying control gaps, required evidence and accountable owners.**

2 Who Is Accountable Across the Service Chain?

Every critical responsibility needs a clear owner, especially when several providers deliver the service.

INSIGHTS

Appointing external providers changes the allocation of responsibilities; it also requires continuing oversight. Moomoo Singapore's approach illustrates the importance of due diligence and regular counterparty assessments alongside clear contractual responsibilities.

Digital asset services often involve several organisations. A platform may manage the customer relationship, a specialist provider may safeguard assets and another business may supply wallet software or transaction infrastructure.

One important distinction is between purchasing custody technology and appointing a custodian.

A business can purchase sophisticated wallet software while remaining responsible for safeguarding the assets itself. Appointing a custodian is different: the provider assumes specified safeguarding responsibilities under the applicable service agreement and legal arrangements.

This distinction affects who controls assets, authorises transfers and responds when something goes wrong. Insurance arrangements, where relevant, may also depend on the particular service and holding structure.

Consider a withdrawal failure involving a platform, custody provider and technology partner. Each may have established procedures, but customers can still experience delays if responsibility for investigating and resolving the problem is unclear.

Contracts and operating procedures should establish who safeguards assets, maintains records, approves transfers and handles incidents. Effective oversight requires access to operational records, clear escalation procedures and the ability to establish what happened when a process fails.

Appointing an external provider does not necessarily remove the institution's own obligations. Due diligence, monitoring and governance remain important, with responsibilities determined by the applicable Australian requirements and services involved.

Jeyson Ng, CEO of Moomoo Singapore, outlines the importance of this oversight: "As a wealth-tech and trading platform serving over 2 million users in Singapore and regulated by the MAS, Moomoo is well-positioned to bridge traditional finance and digital assets for our users. That makes us highly selective about where we custody their assets. Ensuring customer assets are safe and supported by institutional-grade infrastructure is critical, which is why we conduct rigorous due diligence and annual counterparty assessments on all our providers, including BitGo."

Andrea Yuen, CEO of Swyftx, agrees: **"Accountability stays with you, even when a partner delivers part of the service. Customers see one brand, so before we launch anything, we map who holds the assets, who fixes it if something breaks, and who tells the customer."**

→ **Action: Map responsibilities across providers, such as who leads the response to a failed withdrawal, which records each party must supply and how the issue is escalated.**

Outcome: An agreed responsibility map across the service chain.

3 Which Operating Model Will Make the Business Viable?

Choose the model the business can sustain as customers, costs and requirements change.

INSIGHTS

The build-versus-partner decision becomes clearer when institutions compare the full operating commitment: people, controls, integration, assurance and the ability to change course. The key question is which capabilities differentiate the business and which are better obtained from a specialist.

The choice between developing infrastructure internally and engaging specialist providers is both an operational and commercial decision. It determines which services a business can deliver, how quickly it can adapt and what resources it must commit over time.

For Australian businesses, the comparison must reflect the market they can realistically serve. Infrastructure that is economical for a global institution may be difficult to sustain with a smaller domestic customer base.

Building custody capabilities internally can provide direct control over technology and processes, but the initial investment represents only part of the commitment. Secure operations require continuing expenditure on specialist personnel, infrastructure maintenance, governance, recovery procedures and independent assurance.

Controls must remain effective as systems change, staff leave and new threats emerge. Records and reporting must also support reconciliation, audits and oversight, regardless of whether customer adoption meets expectations.

BTC Markets' Lucas Dobbins emphasises that these commitments shape the business from inception: **"Operating responsibly in digital assets costs real money. Compliance, capital, and custody are not overheads to add later; they shape the business from the start. Treating them as core infrastructure is what builds trust with institutions."**

Working with a specialist custodian may allow an institution to rely on established capabilities and concentrate resources on its core business. However, the commercial comparison must also account for integration, reporting and the cost of potentially changing providers.

Raagulan Pathy, Co-founder of KAST, described the practical value of using established infrastructure: **"Many of the operational and security features KAST needed, like fund sweeping, balance checks, and access controls were already built into BitGo's infrastructure, saving us significant time in development and compliance."**

A hybrid model can distribute functions between internal teams and external partners, but the institution must understand the dependencies created by that division.

CP 392's proposed financial requirements could also affect commercial viability, depending on the final standards and activities performed. Outsourcing should not be assumed to remove those obligations.

Consider an Australian exchange reviewing custody infrastructure developed several years ago. Its leadership must compare the continuing cost of internal systems and staff with the expense of engaging a specialist provider, including migration, integration and operational disruption.

That decision should also account for the services the exchange intends to offer. A custody arrangement that meets existing requirements may not provide the capabilities needed for new trading, liquidity or settlement workflows. Equally, expanding infrastructure before establishing customer demand can create costs the business cannot recover.

An operating model that made commercial sense when a business was established may no longer be appropriate as its customers, costs and regulatory obligations change.

→ **Action: Compare the full cost, retained responsibilities and exit options of at least two viable operating models against a realistic customer base. Identify the customer demand, revenue and cost assumptions required for sustainable returns.**

> **Outcome: A preferred operating model, with retained responsibilities, assumptions and commercial thresholds.**

4 Can Assets Move Reliably When Customers Need Them?

Custody, liquidity and settlement must work as one service, including under pressure.

INSIGHTS

Custody, trading and settlement need to work together, whether delivered through an integrated service or several providers. Institutions should assess where assets sit, how liquidity is accessed and who bears exposure at each stage.

Custody cannot be evaluated in isolation from the transactions an institution intends to support. Secure asset holding is foundational, but institutions also need to understand how customers can use those assets, access liquidity and complete transactions.

A customer instruction may lead to trade execution, asset movement and settlement of cash and asset obligations. Different stages can involve separate providers, counterparties and sources of liquidity, creating operational dependencies and potential exposure.

Some trading arrangements require institutions to transfer assets to an exchange or trading counterparty before executing transactions. This is known as pre-funding. It makes assets available for trading but requires the institution to understand who holds them, what happens if the counterparty fails and how they can be recovered.

Other arrangements allow trades to take place while assets remain with a separate custodian, with payment and asset obligations settled afterwards. This can reduce the need to transfer assets to trading counterparties in advance, but institutions must still manage settlement obligations, credit exposure and failed delivery.

Leon Marshall, Chief Executive of Europe at Galaxy, described the institutional rationale for this model: **“The bifurcation of qualified custody and global exchange access offers investors greater risk mitigation, capital efficiency, and liquidity, helping to deepen access to the digital asset market.”**

The choice affects more than counterparty exposure. Institutions must consider the liquidity available through each arrangement, the timing of asset movements and the operational requirements of their trading activity. An arrangement that reduces one form of exposure may introduce additional settlement dependencies or constraints.

Institutions also need to distinguish execution from settlement and settlement from withdrawal availability. A trade may execute while its obligations remain unsettled. Assets may be recorded as transferred within one system while an external withdrawal requires additional processing.

DTCC's July 2026 limited-production event demonstrated how tokenised securities could move through institutional trading and settlement workflows. BitGo Bank & Trust supported the custody, delivery and settlement of tokenised securities collateral through repo and reverse repo transactions. In October 2026, DTCC launched its Tokenization Service, enabling eligible participants to convert securities entitlements held at DTC into tokenised representations and move them across supported blockchain networks. BitGo Bank & Trust is among the collaborators supporting the broader ecosystem. These developments illustrate how custody, asset movement, execution and settlement can connect within institutional workflows.

Before launching a service, institutions should test the complete transaction lifecycle, including constrained liquidity, counterparty failure, provider outages and settlement delays. The operating model must support the intended customer activity while maintaining appropriate protections throughout the service.

→ **Action: Trace one customer transaction from instruction to final settlement and withdrawal, then repeat the exercise for a provider outage or settlement failure.**

> **Outcome: An end-to-end transaction map showing failure points and fallback arrangements.**

5 What Can Australia Adopt from International Experience?

Adapt proven approaches to Australian customers, laws and market economics.

INSIGHTS

International experience shows how regulatory interpretation and operating practices develop through implementation. Continuing public-private dialogue helps resolve practical questions, while approaches to governance, resilience and provider oversight need to be assessed against Australian requirements and market conditions.

International experience can help Australian institutions understand how regulatory frameworks develop and what effective implementation requires. But lessons from other markets must be distinguished from the legal and commercial arrangements specific to each jurisdiction.

One key lesson Australia can take from international experience is that regulatory implementation does not end when legislation commences. Drawing on her experience implementing Singapore's Payment Services Act, Angela Ang explains: "New operating models continued to emerge after the Act commenced in January 2020, which my team at MAS had to evaluate against the Act's regulatory perimeter. Until today, MAS continues to update its frequently asked questions to clarify how particular activities fall within the framework. Businesses can contribute to ongoing dialogue by explaining how their arrangements operate, where uncertainty exists and how different interpretations would affect customer protection or service delivery."

Swyftx's Andrea Yuen notes that Australia's journey is just beginning: **"Australia's new laws bring legal certainty, but trust has a long memory. Institutions will commit once custody, settlement and accountability hold up under pressure. A licence isn't the finish line; it's the starting point."**

Operational lessons also travel across borders. Security practices, resilience planning and clear accountability can inform institutional arrangements in different markets. Licensing permissions, legal protections and customer requirements, however, must be assessed locally.

Australia's SMSF market illustrates the commercial side of that distinction. An overseas retirement market strategy may rely on relationships that do not translate directly to Australian trustees, administrators, advisers and software providers. Access to one participant does not necessarily provide authority to select custody arrangements or move assets on behalf of another.

An institution considering that market must identify the customer, the problem being solved and who can make the relevant decision. Applying an assumed percentage to Australia's total superannuation assets does not establish a credible business opportunity.

The same discipline applies when evaluating international service providers. An overseas licence or recognised institutional customer may demonstrate experience, but does not establish that a service satisfies Australian requirements.

In CP 392, ASIC proposes not to require domestic custody of underlying assets held by digital asset platform and tokenised custody platform operators. This "provides firms with added flexibility to manage their asset holding in the best way to protect consumers and provide efficient services." At the same time, ASIC proposes disclosure guidance covering custody locations and cross-border risk management arrangements, and is seeking feedback on emergency fallback arrangements. Institutions should assess those considerations alongside the contracting entity, permitted activities, customer protections, reporting arrangements and local support needs before adopting an international approach.

International experience is most valuable when it helps institutions understand what has worked elsewhere, why it worked and what would need to change for the same approach to succeed in Australia.

→ **Action: Assess one relevant international approach against Australian legal requirements, customer workflows and commercial scale. Identify the adaptations needed and any unresolved questions for providers or regulators.**

> **Outcome: A documented assessment of whether and how the approach could work in Australia, including required adaptations and outstanding questions.**

6 What Should Leaders Do Now?

Build readiness now and preserve flexibility around requirements still being finalised.

INSIGHTS

Singapore's experience illustrates that implementation continues after legislation commences. Teams can prepare by mapping services, assigning responsibility and testing controls while maintaining a clear list of decisions that depend on final guidance. This makes later changes easier to assess and implement.

Australian institutions can make meaningful progress while proposed standards are being finalised. The priority is to understand existing arrangements, identify potential gaps and preserve flexibility where requirements remain unresolved.

Asset holding is a useful starting point, given its importance in CP 392.

First, map where customer assets sit throughout the service.

Include custodians, trading partners and other providers. Document legal holding arrangements, transaction authority and how assets could be accessed or recovered during disruption.

Second, assess those arrangements against the proposed standards.

Review contracts, controls, records, provider oversight and internal expertise. Identify gaps, test recovery procedures and compare the cost and capabilities required under different operating models.

Third, engage with unresolved implementation questions.

Before the 27 November 2026 submission deadline, institutions can contribute to CP 392 consultation by presenting concrete examples of how their arrangements operate and how proposals could affect customers. After that deadline, monitor ASIC's response and any further consultation, and continue appropriate industry and regulatory dialogue.

These activities can proceed without assuming every proposal will be adopted unchanged.

Significant infrastructure investments, custody migrations or changes made solely to satisfy an unresolved provision may be costly to reverse. Institutions should identify which commitments depend on final requirements and prepare to act when those requirements become clearer.

For established operators, that may involve reassessing existing infrastructure and whether it can support future services. For new entrants, it may mean validating customer demand and identifying essential capabilities before choosing a provider or building internally.

→ **Action: Give each readiness task an owner and target date, and identify the evidence or regulatory decision needed before committing significant expenditure.**

> **Outcome: A prioritised action plan with owners, dates and decisions outstanding.**

Readiness Checklist

Institutions may use this checklist to capture the six outcomes from the suggested actions above, between now and the applicable commencement or licensing milestone. Assign a named owner and target date to each task, record the evidence and unresolved dependencies, and review progress at leadership meetings.

Section and Action	Outcome	Owner / target date	Status / dependency
1. **Customer protection** Test recovery	A documented assessment of the withdrawal and recovery process, identifying control gaps, required evidence and accountable owners.	Owner: Date:	Status: Dependency:
2. **Accountability** Agree responsibilities	An agreed responsibility map across the service chain.	Owner: Date:	Status: Dependency:
3. **Operating model** Compare and select	A preferred operating model, with retained responsibilities, assumptions and commercial thresholds.	Owner: Date:	Status: Dependency:
4. **Settlement** Trace and test transactions	An end-to-end transaction map showing failure points and fallback arrangements.	Owner: Date:	Status: Dependency:
5. **International experience** Adapt an approach	A documented assessment of whether and how the approach could work in Australia, including required adaptations and outstanding questions.	Owner: Date:	Status: Dependency:
6. **Readiness** Prioritise next steps	A prioritised action plan with owners, dates and decisions outstanding.	Owner: Date:	Status: Dependency:

Australia's next phase of digital asset growth will depend on institutions turning regulatory direction into services that work for customers. The opportunity is to combine local commercial judgement with international operating experience: choose a viable use case, establish clear accountability, test the complete service and build the evidence to move forward with confidence.

Important information

This report is published solely for general information purposes, to support a review of Australia's digital asset market and evolving regulatory framework.

References to BitGo, its affiliates, customers, services or international initiatives are provided as factual examples for discussion. This report does not represent, promote, market or imply an invitation or offer of services in Australia, confirmation of availability or eligibility, or endorsement by any regulator. Service availability depends on the relevant entity, jurisdiction, permissions and contractual arrangements.

Nothing in this report constitutes legal, regulatory, financial, investment, tax or accounting advice. Readers should obtain independent professional advice appropriate to their circumstances before acting on its contents. Digital assets are subject to a high degree of risk, including the loss of their value.

The report reflects information available as of the date of this report. CP 392 and its attachments contain consultation proposals that may change. Descriptions of proposed requirements should not be read as statements of final law or regulatory guidance.

Although reasonable care has been taken in preparing this report, BitGo does not warrant that its contents are complete, accurate or current and undertakes no obligation to update them. To the extent permitted by law, BitGo and its affiliates disclaim liability for loss arising from reliance on this report. Nothing in this disclaimer excludes liability that cannot lawfully be excluded.