Date of Hearing:

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 2285 (Valencia) – As Amended March 16, 2026

SUBJECT: Digital Financial Asset Banking Act

SYNOPSIS

The rapid growth of digital assets like cryptocurrencies has outpaced existing financial regulations, leaving gaps in how banks safeguard customer assets, manage risks, and disclose key information. As traditional financial institutions begin offering digital asset services, a clear regulatory framework is needed to ensure consistent standards, accountability, and trust in these emerging markets.

This bill would establish a comprehensive regulatory framework governing how banks and credit unions in California can custody, manage, and transact in digital financial assets on behalf of customers. A coalition composed of California's Credit Unions, the California Bankers Association, and the California Community Banking Network take a "support in concept" position on the bill, mostly wishing to see the bill's requirements align with existing state and federal law. The bill has no formal opposition.

This committee's jurisdiction is limited to the cybersecurity provisions of this bill. The bill will be heard by the Banking and Finance Committee one day before it is heard by this committee.

EXISTING LAW:

1) Defines "digital financial asset administration" to mean issuing a digital financial asset with the authority to redeem the digital financial asset for legal tender, bank or credit union credit, or another digital financial asset. (Fin. Code § 3201(h).)

2) Defines "digital financial asset business activity" to mean any of the following:

    a. Exchanging, transferring, or storing a digital financial asset or engaging in digital financial asset administration, whether directly or through an agreement with a digital financial asset control services vendor.

    b. Holding electronic precious metals or electronic certificates representing interests in precious metals on behalf of another person or issuing shares or electronic certificates representing interests in precious metals.

    c. Exchanging one or more digital representations of value used within one or more online games, game platforms, or family of games for either of the following:

        i) A digital financial asset offered by or on behalf of the same publisher from which the original digital representation of value was received.

        ii) Legal tender or bank or credit union credit outside the online game, game platform, or family of games offered by or on behalf of the same publisher from which the original digital representation of value was received. (Fin. Code § 3102(i).)

3) Requires a person conducting digital financial business activity to obtain a license as a covered person. (Fin. Code § 3102.)

4) Requires a covered person to disclose specified business activity the covered person will undertake with a resident before engaging in digital financial asset business activity with the resident. (Fin. Code § 3501.)

THIS BILL:

1) Defines the following terms:

   a. "Active staking" means intentional participation in staking services resulting in inaccessibility to one's digital financial asset for an agreed-upon time in exchange for a staking reward minus a fee that is in a fixed amount or a percentage of the staking reward.

   b. "Customer" means a person for whom a financial institution provides digital asset services, including a digital asset account holder or a person on whose behalf the financial institution acts in a fiduciary capacity.

   c. "Department" means the Department of Financial Protection and Innovation.

   d. "Digital asset" means a digital representation of value recorded on a cryptographically secured, distributed ledger or similar technology, including, but not limited to, a digital financial asset.

   e. "Digital asset custody services" means the safekeeping or custody of a digital financial asset on behalf of a customer by a financial institution, including maintaining control over the digital financial asset and any associated key.

   f. "Digital asset transaction services" means to facilitate the execution of a digital asset purchase or sale on behalf of a customer for compensation.

   g. "Digital financial asset" means a digital representation of value that is used as a medium of exchange, unit of account, or store of value, and that is not legal tender, whether or not denominated in legal tender.

   h. "Digital financial asset business activity" means any of the following:

      i) Exchanging, transferring, or storing a digital financial asset or engaging in digital financial asset administration, whether directly or through an agreement with a digital financial asset control services vendor.

      ii) Holding electronic precious metals or electronic certificates representing interests in precious metals on behalf of another person or issuing shares or electronic certificates representing interests in precious metals.

      iii) Exchanging one or more digital representations of value used within one or more online games, game platforms, or family of games for either of the following:

(1) A digital financial asset offered by, or on behalf of, the same publisher from which the original digital representation of value was received.

(2) Legal tender or bank or credit union credit outside of the online game, game platform, or family of games offered by, or on behalf of, the same publisher from which the original digital representation of value was received.

i. "Digital wallet" means a digital interface or physical device that stores a digital asset or a private key in a manner that enables the owner to securely manage, transfer, and maintain independent control over the owner's digital asset.

j. "Fiduciary capacity" means a capacity in which a financial institution possesses investment, management, or administration discretion of a digital financial asset on behalf of a customer that creates for the financial institution a strict duty to act in the best financial interest of the customer, including against its own interest.

k. "Financial institution" means a bank or credit union operating under the examination authority of the Department of Financial Protection and Innovation (DFPI).

l. "Key" means a pair of cryptographic codes associated with a digital asset wallet that consists of a public key and a private key that meets both of the following criteria:

i) The public key of the pair enables the receipt of a digital financial asset and the verification of a digital signature.

ii) The private key of the pair enables the control, transfer, or management of a digital asset within the digital asset wallet.

m. "Material cybersecurity incident" means a cybersecurity breach or event that materially compromises the security, confidentiality, or integrity of a financial institution's information system or a digital asset under the financial institution's control.

n. "Nonfiduciary capacity" means providing digital asset custody services solely for safekeeping without discretionary authority to manage or transfer a digital financial asset and with respect to which legal title and control of the assets remain with the customer.

o. "Passive staking" means staking pooled assets by, or on behalf of, the financial institution wherein the customer may receive the customer's digital financial asset upon demand in exchange for a staking reward minus an agreed-upon fee, in a fixed amount or a percentage of the staking reward, from the financial institution staking service provider.

p. "Pooled custody" means the collective holding of fungible digital financial assets of like kind belonging to different customers in a shared account or digital asset wallet.

q. "Segregated custody" means the holding separately from the digital financial assets of other customers of the fungible digital financial assets of an individual customer in an account or digital asset wallet.

r. "Slashing" means a penalty imposed by a blockchain protocol that results in the forfeiture or reduction of staked digital assets or staking rewards due to validator misconduct or failure.

s. "Staking" means committing fungible digital financial assets to a blockchain network to participate in the network's operations by validating transactions, proposing and attesting to blocks, and securing the network.

t. "Staking reward" means any interest, yield, or other compensation earned by a customer from staking a digital financial asset on a blockchain network.

u. "Subcustodian" means a third party that a financial institution uses to hold a digital financial asset on the financial institution's behalf as part of providing digital asset custody services to a customer.

2) Permits state-chartered financial institutions to offer digital financial asset (DFA) retail services under specified requirements.

3) Requires annual auditing of custodial services by way of independent audit or review and signed attestation of the DI's Board of Directors.

4) Requires consumer disclosures, as specified.

5) Provides a framework for the payment of fees or commissions for staking services.

6) Requires financial institutions adopt anti-money laundering measures, as specified.

7) Requires a financial institution and any of its subcustodians to maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of the financial institution's information systems, digital asset custody, and staking software and hardware that is based on the financial institution's risk assessment and designed to perform all of the following functions:

a. Identifying and assessing internal and external cybersecurity risks that threaten the security or integrity of nonpublic information stored on the financial institution's information systems as it relates to the digital financial assets of its customers.

b. Using defensive infrastructure and the implementation of policies and procedures to protect the financial institution's information systems, and the nonpublic information stored on those information systems, from unauthorized access, use, or other malicious acts.

c. Detecting cybersecurity events.

d. Responding to identified or detected cybersecurity events to mitigate any negative effects.

e. Recovering from cybersecurity events and restoring normal operations and services.

f. Fulfilling applicable regulatory reporting obligations.

8) Requires that any information relevant to the financial institution's cybersecurity program, including the relevant and applicable provisions of a cybersecurity program maintained by any subcustodian, be made available to the department upon request.

9) Requires that the cybersecurity program for a financial institution and any of its subcustodians align with applicable federal cybersecurity standards for financial institutions, including, but not limited to, the guidelines of the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook, the framework established by the National Institute of Standards and Technology (NIST), and any other standard deemed applicable by the department and shall comply with applicable federal financial privacy and data security requirements, as determined by the department.

10) Requires a financial institution to notify the department within 72 hours after discovering any material cybersecurity incident that impacts the financial institution or its subcustodian's digital asset custody or staking software or hardware or any digital financial asset held or managed through those systems. Requires the notice to include a description of the incident and its likely impact on the financial institution and its customers, as prescribed by the department.

11) Requires a financial institution to maintain, for at least seven years, detailed records of its cybersecurity compliance efforts, including any policy, procedure, risk assessment, audit report, or training material related to its cybersecurity program. Requires the financial institution to make those records available for inspection by the department upon request or during any examination.

COMMENTS:

1) **Author's statement.** According to the author:

> As federal regulations continue to evolve, California banks need the tools to responsibly integrate this technology into their existing systems, while ensuring consumers are protected from potential mismanagement of digital assets.
>
> Blockchain technology is increasingly shaping the future, with new applications emerging across everyday use cases. By providing our state-chartered banks and credit unions, the go-to choice for many residents, a responsible framework for offering this technology, we give our state financial institutions a reputational advantage from the start."
>
> AB 2285 provides an innovative and modern framework for California banks seeking to offer digital asset services, positioning California to lead in balancing strong consumer protections with continued innovation in the digital asset space

2) **Background.** The Assembly Banking and Finance Committee explains recent developments related to financial institutions managing digital financial assets in their bill analysis:

> In May, 2025, the Office of the Comptroller of the Currency (OCC) which oversees nearly 4,000 federal institutions across the country, issued guidance to clarify that national banks and federal savings associations can buy and sell digital financial assets held in custody at its customer's direction if they follow the practices they use for traditional assets. This

clarification also included the permissibility of the use of third-party sub-custodians. Since this guideline was issued, five applications to either newly charter or convert existing institutions into national trust banks that will engage in digital financial asset activity have been conditionally approved.

On July 30, 2025, JP Morgan Chase issued an announcement regarding its partnership with Coinbase to offer seamless bank to exchange access. "We're excited to partner with JP Morgan Chase to onboard the next generation of consumers into crypto. Together, we are expanding choice and lowering barriers to entry for consumers to participate in the future of financial services onchain," said Max Branzburg, Head of Consumer & Business Products at Coinbase.

As of August, 2025, more than half of the 25 largest banks in the United States are now either considering or actively rolling out crypto-related products. Digital financial assets (DFA) afford financial institutions the opportunity to establish novel revenue streams and expand market presence by facilitating cryptocurrency access without geographical constraints. Institutions integrating digital asset services can have significant advantages in financial inclusion and benefit from the enhanced transaction speed, settlement finality, and automation inherent in smart contracts. Additionally, the adoption of blockchain technology promotes heightened security and substantial operational efficiencies within the existing financial framework.

State chartered banks and credit unions are regulated by the Department of Financial Protection and Innovation, not the OCC. Despite progress on the Digital Financial Asset Law (DFAL), there is no pathway for banks and credit unions to participate in an emerging and global market.

[…]

This bill comes at a time when it appears that federal DFA regulation is on the precipice of passage. Congress has been at an impasse on the CLARITY Act, a bill aimed at establishing a comprehensive regulatory framework for digital assets, dividing oversight between the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC).

3) **What this bill would do.** This bill would establish a comprehensive regulatory framework governing how banks and credit unions in California manage digital financial assets on behalf of customers. The bill requires financial institutions to clearly define whether they are acting in a fiduciary or nonfiduciary capacity, obtain customer consent through written agreements, and provide key disclosures about risks, insurance status, and control of assets. The bill also imposes strict requirements around safeguarding customer assets, including maintaining full one-to-one reserves, keeping accurate ownership records, and ensuring that customer assets remain the property of the customer. The bill regulates emerging practices like staking and subcustody by requiring transparency, limiting fees, mandating timely payment of rewards, and ensuring that institutions retain responsibility even when using third parties. The bill also establishes robust compliance obligations, including annual audits, anti-money laundering programs, and cybersecurity standards aligned with federal frameworks, along with rapid breach notification requirements. Finally, the bill grants enforcement authority to the Department of Financial Protection and Innovation, including the ability to issue orders, impose penalties, and suspend or

revoke a financial institution's authority to engage in digital asset activities.

This committee's jurisdiction is limited to the cybersecurity provisions of this bill. Taking what they describe as a "support in concept" position, a coalition that includes California's Credit Unions, the California Bankers Association, and the California Community Banking Network request that the bill avoid creating duplicative cybersecurity requirements:

> State-chartered federally insured financial institutions are already subject to oversight by Department of Financial Protection and Innovation (DFPI), the California Department of Justice (DOJ) and federal prudential regulators for cybersecurity incidents. AB 2285 should not add new, duplicative requirements.

The author may wish to consider working with DFPI, DOJ, and federal regulators to align this bill with existing frameworks.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file.

Opposition

None on file.

Analysis Prepared by: Slater Sharp / P. & C.P. / (916) 319-2200