INFORMATIONAL HEARING
ASSEMBLY BANKING AND FINANCE COMMITTEE

Government Use Cases of Digital Financial Assets
Wednesday, February 18, 2026
2:00 P.M., State Capitol Room 447

PURPOSE AND OVERVIEW OF HEARING

Today's hearing will provide a primer on digital financial assets and blockchain technology. Speakers will discuss government use cases related to digital financial assets in the context of 1) recently enacted state unclaimed property law, and 2) the prospect of a digital financial asset reserve fund in the state of California.

BASIC TERMS

Blockchain is the term used to describe a cryptographically secured ledger. There is no single blockchain. The three dimensions of blockchain are function, structure, and accessibility.[1] The **function** of a blockchain involves the recording and validating of transactions. The **application** is wide; each block on a blockchain contains the information of a transaction that is linked chronologically to create a chain. The **structure** of a blockchain is decentralized; there is no single authority or owner, but rather a community of independent blockchain computer participants called *nodes*. All of the nodes are constantly syncing information between each other about transactions on the ledger and checked against the ledger's history to ensure that they are valid. Once enough nodes have verified a new transaction, the transaction is confirmed and becomes final. The network will bundle a certain number of finalized transactions and seal them into a block using cryptography. The block encrypts the details of the block into a long hexadecimal number called a **hash**. The next block will use the previous block's hash as a starting point thus connecting the entire history of the ledger in a chain of blocks. **Access** to a blockchain can be public or private. A private blockchain is only visible to authorized viewers, while a public blockchain is visible to anyone.

Digital financial assets are electronically issued, stored, and transferred items of value using blockchain that are secured with cryptography. There are two broad categories of digital financial assets: currency and tokens. **Currency** includes: 1) cryptocurrencies, which are currencies that are native to a blockchain for use within that blockchain; 2) stablecoin, a type of cryptocurrency designed to maintain a stable value by pegging its value to a reserve asset like the U.S. dollar; and 3) central bank digital currencies (CBDCs), an exploratory currency that would represent a nation's fiat currency that is a direct liability of that country's central bank. **Tokens** include

[1] Friel v. Dapper Labs, Inc., 657 F. Supp. 3d 422 (2023)

nonfungible tokens (NFTs), a unique digital representation of ownership of a specific singular item, commonly art; and tokenized assets (security tokens), digital representations of traditional financial instruments such as stocks and real estate. Conceptually, currencies are more narrowly limited to the traditional concept of an exchange of value, while tokens can be broadly applied to digitizing rights of the holder (functionality), and tangible and intangible goods.

Users can exchange their digital financial assets through a centralized exchange or decentralized exchange. A **centralized exchange**[2] works as a third party intermediary platform similar to an escrow; the exchange holds users' private keys to access the funds itself. This is also known as a **custodial wallet**. A **decentralized exchange** is a peer-to-peer transaction where the platform does not hold the funds. In this case, the user maintains a **non-custodial wallet** which can be held offline with hardware (**cold storage)**, or online in a **hot wallet**. Non-custodial wallets provide greater security because they are not subject to exchange breaches; however, there are still vulnerabilities to user error (misplacing hardware or recovery phrases) and phishing scams. Regardless of the selected method of exchange, the user's transaction is recorded to the appropriate blockchain.

Smart contracts are automated programs made to perform specific functions on the blockchain once a predetermined condition occurs. Smart contracts are tamper-proof once created and deployed to the blockchain.[3] To use the example from its inception, a vending machine is a physical example of a smart contract; the user deposits money and makes their selection, the machine dispenses the item from the selected location. Digitally, in the decentralized exchange discussed above, a self-executing smart contract is used in the peer-to-peer transaction to facilitate the exchange without the platform ever holding the funds while still maintaining confidence in the transaction.

A **zero knowledge proof** is a cryptographic method that allows a party to prove the validity of a statement or claim without revealing the underlying information. This concept is essential for privacy, regulatory compliance, financial transactions, government use, and beyond. There are three primary types of zero-knowledge proofs: interactive zero-knowledge proofs, non-interactive zero-knowledge proofs, and zero-knowledge succinct non-interactive argument of knowledge. Each relies on complicated mathematical algorithms and cryptography to verify the transaction without revealing the information.

A **consensus mechanism** is the set of rules that governs the manner of adding, changing, or deleting information to or from a blockchain that is agreed upon by all its members. All blockchains must maintain accurate records to function correctly. Unlike banks, blockchains

[2] Under the Digital Financial Asset Businesses Law, the term "digital financial asset administrator" (DFAA) is used to describe a central exchange. Section 3102 (h) of the Financial Code states that "digital financial asset administrator" means 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. DFAA are required to obtain a license from the Department of Financial Protection and Innovation for digital financial asset business activity in California by July 1, 2026.

[3] Once a smart contract is deployed to the blockchain, it is distributed, making the code immutable by anyone including the creator. Still, a smart contract can contain bugs or vulnerabilities that can allow for hostile attacks.

don't have any central authority to keep all the records. By contrast, all peers are equal in a decentralized network. Different blocks are broadcast simultaneously, and the network must decide which chain to follow. A mechanism that determines which chain to follow is called consensus. A consensus mechanism is what keeps decentralized networks secure. Nodes must agree on the current state before updating the blockchain. This automated process prevents errors and secures the network against threats where malicious actors can manipulate the network with fake nodes.[4]

Web3 is the umbrella term given to a collective ecosystem of decentralized applications (*dapps*), decentralized gaming, decentralized finance (*DeFi*), digital assets (which in addition to financial assets, includes non-fungible tokens and governance tokens). Often, Web3 is referred to as the third phase of the internet centered around ownership.

A SHORT HISTORY OF CRYPTOCURRENCY

Two of the current leading cryptocurrencies, bitcoin (BTC) and ether (ETH) share the foundational principles of operating on decentralized blockchain technology, but diverge on nearly all other aspects. Stripped down, bitcoin is a store of value, while Ethereum is a functional platform, **Ethereum Virtual Machine** (EVM), upon which other applications and smart contracts can be built (see *Web3* above). For illustrative purposes Bitcoin and Ethereum will be used as examples, however, these concepts apply to different blockchains for different cryptocurrencies to varying degrees as well.

Understanding the Origins to Understand the Current State

In 1989, a company called DigiCash came to market to offer digital payments, similar to a debit card, but with the ability for the banks to verify the digital money *without knowing the identity of the person* using the money.[5] Despite interest from large technology companies and a financial institution, a lack of user demand, even with the rise of the internet, ultimately led to the company's bankruptcy in 1997. In 1992, a group of coders inspired by DigiCash's transformative proposition of privacy protected e-money expanded the idea to remove the intermediary bank, a centralized entity. The group wanted the anonymity of cash without the physical inconvenience of carrying paper and coin money. Based on their personal ideologies, the group wanted a type of digital money that did not require them to trust anyone at all–they only wanted to trust the money itself.[6] However, removing the centralized entity, which normally acts as a verifier for the funds, creates an issue of potentially double-spending the digital money.[7]

[4] https://hacken.io/discover/consensus-mechanisms/
[5] "*Money the True Story of a Made up Thing*" by Jacob Goldstein (2020) at page 189 citing "Security Without Identification: Transaction Systems to Make Big Brother Obsolete" by David Chaum in *Communications of the ACM*.
[6] *Id.* at page 194
[7] Normally, double-spending is prevented by maintaining a ledger to follow the money.

In 1998, a coder named Wei Dai suggested an upside-down solution; instead of a single intermediary to maintain the ledger, make everyone maintain the ledger.[8] In this proposal, all participants maintain a separate database containing the ledger and record of reconciliation for all pseudonymous accounts and transactions. In this proposal, transactions are calculated and validated across the network of computers. For example if user A wants to pay user B $5, it would broadcast the transactions across the network, the network would first verify that user A has $5 in their account, if there isn't, the request is ignored. If there is, every computer on the network deducts $5 from user A's account and adds $5 to user B's account. But, the biggest flaw in the early concept was that it would impractically require synchronicity among users; the requirement that all participants would have to be online all the time, communicating without interruption.[9] A foreseeable lack of incentive for the heavily burdensome responsibility made the proposal unscalable.

In 2008, Dai received an email from a stranger commenting on the similarities of Dai's idea and the proposal attached to the email called, "Electronic Cash without a Trusted Third Party", later published as "Bitcoin: A Peer-to-Peer Electronic Cash System." In this white paper, Satoshi Nakamoto proposed an incentive for the network described by Dai; payment in newly created bitcoin for doing the work, as well as a proposal to create a network based on a chain of blocks, better known now as blockchain, to address the problem of double spending.[10] The result was Bitcoin.

Value of Currency

Fiat currency is government issued money that is not backed by any physical commodity, but rather the "full faith and credit" of the issuing government. The U.S. dollar, Japanese yen, and British pound are examples of fiat currency. Because the currency is not backed by a tangible commodity, fiat currency has no intrinsic value. Instead, the value of the currency is based on several factors including supply and demand, public trust, and stability of the issuing government.

Cryptocurrency, with the exception of commodity-collateralized stablecoin, is similar to fiat currency in the sense that neither are backed by a physical commodity, and the value of the currency is heavily influenced by public trust and supply and demand. One major difference affecting the value of cryptocurrencies is the lack of government origination.

Value for bitcoin comes from supply and demand. Bitcoin is finite with a cap of 21 million coins. These coins are released incrementally on a halflife basis determined by the amount of mined bitcoin, thus the limited amount and increasing demand creates value.

---

[8] Goldstein, supra note 5, at 196.
[9] Goldstein, supra note 5, at 197.
[10] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

Creating New Blocks

Adding new blocks to a blockchain happens when a transaction is initiated by a user and the transaction is validated. The network structure of decentralization requires consensus from the nodes in order to validate the transaction. The reliance on community participation does open a blockchain to attacks by malicious actors who can impersonate or fake user identities[11] in order to gain disproportionate influence or degrade the security of blockchain and its users. This is known as a Sybil attack. The risk of a Sybil attack is one primary consideration when adopting a consensus mechanism. There are several different types of consensus mechanisms with more being developed. For the purpose of this analysis, only PoW and PoS will be considered.

Proof of work (PoW) is a consensus mechanism based on game theory. The Bitcoin blockchain is an example that utilizes a PoW consensus mechanism. *Miners* are participating nodes in the blockchain who participate in a complex mathematical puzzle tournament wherein solving the puzzle results in adding a new transaction to the blockchain. The first to solve wins the game and is rewarded with a small portion of uncirculated BTC. This process is better known as **bitcoin mining**. An overview of the process is:

- A Bitcoin transaction is created when a user sends bitcoins from one address to another. The transaction includes the sender's address, the recipient's address, the amount to be sent, and a digital signature.
- The digital signature is generated using the sender's private key, ensuring the authenticity of the transaction, which is then broadcast to the Bitcoin network, where it is picked up by nodes, which verify the transaction.
- Nodes verify that the transaction is signed by the rightful owner of the bitcoins being spent, confirm the bitcoins have not been previously spent, and ensure the transaction follows the protocol rules and data structure.
- Verified transactions are grouped into a block by miners competing to solve a complex mathematical problem based on a cryptographic hash function.
- The solution involves finding a *nonce* (a random number) that, when hashed with the block's data, produces a hash value with a certain number of leading zeros.
- Once a miner finds the correct nonce, they broadcast the new block to the network, where other nodes verify the PoW and validity of all transactions in the block. If the block is valid, it is added to the blockchain, and the network updates to reflect this new state.[12]

Bitcoin mining is an energy- and time-intensive process. There is a lot of trial and error to find a valid nonce. Even with specialised hardware used to make mining more efficient, the massive

[11] Fake nodes referenced in "consensus mechanism" paragraph.
[12] https://crypto.com/us/university/bitcoin-mining

computational effort consumes a significant amount of electricity. Average block time and transaction finality is measured in minutes, which is relatively slow. In terms of security, PoW relies on the huge effort required. A bad actor's computer needs to surpass 51% of the network's computational power.

Once the idea of using blockchain technology to decentralize currency solidified, the cryptocurrency community began to recognize the other potential uses for blockchain unrelated to currency, like a decentralized domain name system. However, the issue with the existing technology was that it would require building a new blockchain for one or more set functions. Thus, the release of another blockchain with the same functions plus more would render the previous blockchain less appealing. In 2013, Vitalik Buterin proposed **Ethereum**, a single blockchain upon which many different applications and smart contracts can be operated. Ether (ETH) is the native currency used on Ethereum, and its smaller denomination, gwei, can be used to pay for services or transaction fees (also known as gas fees) on the network. As a result of this framework, other cryptocurrencies (as well as gaming, NFTs, apps, and smart contracts) are built on the Ethereum blockchain.

Proof of stake (PoS) is a consensus algorithm of security that incentives behavior through rewards and penalties against secured capital supplied by the validators. Validators are the PoS equivalent of miners for PoW. Proof of stake networks rely on validators who are chosen based on the amount of cryptocurrency they hold and are willing to "stake." **Staking** is the act of locking away a portion of currency, like a good-will security deposit, to gain and maintain eligibility to participate in the selection process for securing the network and creating more blocks in exchange for payment. The more coins a validator stakes, the higher their chances of being selected and thus to earn payment. Since the value of the payments fluctuate, and PoS is based on a behavioral incentivization, these payments for services are characterized as "rewards". This "skin-in-the-game" model encourages participants to perform accurately–good behavior results in payment, malicious[13] or undesirable[14] behavior results in penalization against the participants personal stake or slashing of the entire amount. Slashing results in prevention from participation and forcible exit.

Because PoS does not rely on solving computational puzzles, it requires significantly less energy than PoW. With a PoS mechanism, average block time and transaction finality is measured in seconds. An overview of the process is:

- A validator stakes no less than a minimum amount of ETH. (32 at the time of this writing.) Generally, the more ETH staked the more likely the validator node will be selected.

[13] Malicious behavior amounts to a dishonest proposal or attestation. There are three ways a validator can be slashed (all the stake taken): 1) By proposing and signing two different blocks for the same slot; 2) By attesting to a block that "surrounds" another one (effectively changing history); 3)By "double voting" by attesting to two candidates for the same block. https://ethereum.org/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/#slashing Last visited 1/30/2026

[14] Undesirable behavior is action that can result in unreliability in the protocol, such as being offline for consistent intervals or long periods of time. This results in a penalty taken against the validator's stake.

- The protocol selects multiple validators, each with a unique position, to create a new block.
- Validators must use specialized hardware and software, as well as stay online 24 hours to perform the validation services for a global market. Going offline for a number of days with regularity results in penalization against the validator's stake.
    - Minimum required software includes:
        - **Validator client**– the software that acts on behalf of the validator by holding and using its private key to make attestations about the state of the chain. A single validator client can hold many key pairs, controlling many validators.
        - **Consensus clients**–the software used to run Ethereum's PoS consensus algorithm allowing the network to reach agreement. Consensus clients do not participate in validating/broadcasting transactions or executing state transitions.
        - **Execution clients**–the software used for processing and broadcasting transactions and managing Ethereum's state. This runs the computations for each transaction using the EVM to ensure that the rules of the protocol are followed.
    - Minimum required hardware includes:
        - A computer with large storage and processing capabilities with a recommended 4TB SSD and 64 GB of RAM.
        - Reliable internet as close to 24/7 without interruption as possible and no throttling or capping bandwidth (minimum 1.3 GB download and 1 GB upload per hour; *this estimate is likely to increase*).
- Validators are rewarded for correctly validating transactions. However, if a validator acts against the network's interests, a portion or all of their staked ETH may be forfeited — a process known as *slashing*.

Ether has a dynamic supply. New ETH is issued to reward validators, while a portion is burned in a gas fee with every transaction. This is not a 1:1 ratio. The issuance rate is limited by how much ETH is staked. As more ETH is staked, individual rewards decrease, thus creating a natural balance. This design ensures a sustainable security budget into the future, without relying solely on transaction fees.[15]

[15] https://ethereum.org/what-is-ethereum/ Last visited 1/15/2026

USE CASES

Government Use Case Example 1: Unclaimed Property

In 2025, SB 822 was signed into law allowing the State Controller to take custody of unclaimed digital financial assets. California's unclaimed property law (UPL) governs the process by which unclaimed personal property escheats to the state. The UPL framework is one based on custodial possession instead of ownership. The state assumes possession and holds the property in perpetuity as a trustee for the rightful owner.[16] This custodial model was designed to preserve individual property rights while permitting the state to benefit from the use of dormant funds.[17]

UPL involves three distinct parties: the owner, or the person/entity with the rightful claim to the property; the holder, who is typically the business or financial institution that is in possession of the property that becomes abandoned; and the state Controller who assumes custody of the unclaimed property from the holder and then administers claims and manages the unclaimed property fund on behalf of the state. The holder acts as a fiduciary and must report and remit property to the state when it is presumed abandoned.[18] The Controller can retain custody of tangible and intangible property. Once in the Controller's custody, the property is either retained (in the case of tangible property) or liquidated (in the case of securities) and deposited in the Unclaimed Property Fund. Any interest, dividends, or other benefits accrued before or at liquidation of unclaimed property is credited to the owner's account. Any interest or income derived from the investment of money deposited in the Unclaimed Property Fund is transferable to the General Fund.[19]

SB 822 requires the Controller to accept digital financial assets in their native form, holding them as such for no less than 18 months, but no longer than 20 months from the actual date of reporting as required under the statute.[20] If digital financial assets delivered to the Controller remain in the custody of the Controller, a person making a valid claim for those assets under this chapter shall be entitled to receive the digital financial assets from the Controller. If the digital financial assets have been converted, the owner shall be entitled to receive the net proceeds received by the Controller from its sale.[21] The Controller may select one or more custodians for the management and safekeeping of digital financial assets that have escheated to the state.[22]

When making a selection for custodian of escheated digital financial assets, the controller must consider the following criteria:

---

[16] *Harris v. Westly* (2004) 116 Cal.App.4th 214, 219 (internal quotations omitted), *Bank of America v. Cory* (1985) 164 Cal.App.3d 66, 75.
[17] *Azure Limited v. I-Flow Corp.* (2009) 46 Cal.4th 1323, 1328 (internal quotations omitted).)
[18] Cal. Code Civil Proc. Section 1530-1532
[19] Cal. Code Civil Proc. Section 1562
[20] Cal. Code of Civil Proc. Section 1563(c)
[21] *Id.*
[22] Cal. Code of Civil Proc. Section 1568

1. Storage security to ensure the safekeeping of digital financial assets, including robust cybersecurity measures to prevent unauthorized access.
2. Capability to manage private keys associated with digital financial assets and ensure the ability to transfer or transact with the assets when required.
3. Proven experience in handling digital financial assets.
4. Compliance with all applicable federal and state regulations related to digital financial asset custody.
5. Regular reporting mechanisms to the Controller regarding the status and value of the digital financial assets in their custody.
6. Processes to reunite owners with their digital financial assets, including maintaining updated contact records and issuing timely notifications.
7. Qualifying as a "financial institution" under Chapter X of Title 31 of the Code of Federal Regulations, which subjects the qualified custodian to the anti-money laundering obligations of the federal Bank Secrecy Act (31 U.S.C. Sec. 5311 et seq.), in addition to any state-imposed anti-money laundering obligations.
8. Any other factor that the Controller deems relevant.

Government Use Case Example 2: Digital Financial Asset Reserve Fund

What is an Asset Reserve Fund?

The California constitution requires the Legislature to pass a balanced budget.[23] In some years, the state will collect more revenue than its costs, and in other years, it will collect less; reserves smooth out the difference. State reserves ensure stable funding for the state's services over time, even when revenue fluctuates unpredictably. Using reserves during years of shortfall helps avoid increasing taxes or cutting core programs. State investments are conducted through the Office of the Treasurer with Government Code Section 16430 providing the rules for eligible securities for the investment of surplus. Examples of eligible securities are conservative interest bearing U.S. Treasury bonds and shares of money market mutual funds that meet specific conditions.[24]

Currently Enacted Digital Financial Asset Reserves

On March 6, 2025, Executive Order 14233 was signed by President Donbald Trump establishing the Strategic Bitcoin Reserve and United States Digital Asset Stockpile. The order directed the secretary of the Treasury to do several tasks; 1) establish an office to administer and maintain control of custodial accounts collectively known as the "Strategic Bitcoin Reserve"; 2) establish an office to administer and maintain control of accounts collectively known as the "United States Digital Asset Stockpile," capitalized with all digital assets owned by the Department of the Treasury, other than BTC, that were finally forfeited as part of criminal or civil asset forfeiture proceedings; and 3) with the secretary of Commerce, develop strategies for acquiring additional

[23] California Constitution Article IV, Section 12
[24] Cal. Government Code Section 16430 (p)

government BTC provided that such strategies are budget neutral and do not impose incremental costs on United States taxpayers.[25] The Order cites the scarcity of bitcoin and the fact that the Bitcoin protocol has never been hacked as reasons for a "strategic advantage" against other nations to create a bitcoin reserve. The federal government holds a significant amount of bitcoin from criminal forfeiture and civil penalties, but until the Order, there was no established policy to maximize BTC's position as currency in the global market.

New Hampshire, Texas, and Arizona have recently passed legislation to create digital financial asset reserve funds in their respective states. Enacted in May 2025, New Hampshire established a strategic reserve that encompasses exchange-traded products[26], precious metals, and digital financial assets. The new law allows the state treasurer to invest no more than a total of five percent of public funds in precious metals and any digital assets with a market capitalization of over $500 billion averaged over the previous calendar year from the general fund, the revenue stabilization fund, and any other funds as authorized by the legislature.[27]

Soon after New Hampshire, Texas enacted its Strategic Bitcoin Reserve; a special fund operating outside of the state's treasury under the state's comptroller. The fund is used to purchase bitcoin and other digital financial currency.[28] The Texas statute empowers the comptroller to administer and manage the reserve, including maintaining custody of digital financial assets and the power to purchase, exchange, and sell assets with reasonable care on par with a prudent investor. The state's legislature may appropriate funds for deposit 1) to the credit of the reserve to invest in bitcoin or other cryptocurrency and 2) administering and managing the reserve.[29]

Around the same time, Arizona enacted a statute creating the Bitcoin and Digital Asset Reserve Fund.[30] This model is a budget-neutral approach to funding its reserve. This reserve fund is administered and operated through the state treasurer. Unlike the Texas and New Hampshire statutes, Arizona's statute does not provide for the purchase of bitcoin and other cryptocurrencies. In matters of unclaimed property, the state of Arizona assumes custody and control of unclaimed property, not an ownership interest; a framework similar to California's. To fund its digital asset reserve fund, it uses the state's unclaimed digital financial assets to generate rewards from staking and ***airdrops*** (a marketing or engagement strategy used to build awareness or encourage early adoption of a new blockchain project by distributing free tokens or coins to wallet holders who may need to complete certain tasks like sharing the information on social media or making a video). If after three years from the date of transfer the property remains unclaimed, any staking rewards and airdrops may be transferred to the reserve fund.[31]

---

[25] Executive Order 14233 Section 3 (a), (b), and (c).
[26] Exchange-traded products means any financial instrument that is approved by the Securities and Exchange Commission, the Commodities Future Trading Commission or the state securities commissioner that is traded on a United States-regulated exchange and derives its value from an underlying pool of assets, such as stocks, bonds, commodities, or indexes. NH Rev. Stat §6:8-d (I)(a).
[27] NH Rev. Stat §6:8-d(II) and (III).
[28] TX Government Code Section 403.701-403.709, effective June 2025.
[29] TX Government Code Section 403.703(c).
[30] AZ Rev Stat § 41-180 (2025)
[31] AZ Rev Stat § 44-308(d)

Proposed Legislation in Other States

Massachusetts has three bill proposals regarding digital financial asset reserve funds.

The first, SB 1967, establishes a strategic reserve to be managed by the state treasurer. The bill authorizes investment of unexpended state funds, up to 10% of annual Stabilization Fund deposits, into bitcoin or other digital assets, and also allows the reserve to hold digital assets seized by the state. Assets may be held directly by the treasurer, through qualified custodians, or through regulated exchange-traded products. The treasurer is also permitted to loan bitcoin or digital assets, if it can be done without increasing financial risk, in order to generate additional returns for the state.

Similarly, SB 2008 and House Bill 3279 authorize the state treasurer and public pension funds to invest in bitcoin and other "stable digital financial assets" as a hedge against inflation and to enhance fiscal resilience. The bills allow for a maximum of 10% of specific state financial reserves—such as the general fund, stabilization fund, and the retiree benefits trust—to be invested in bitcoin. The measures establish a 5% excise tax on digital currency revenues. Furthermore, it permits the state to lend its digital assets to earn returns. The revenue generated from these activities will be deposited into the general fund, with provisions for reimbursement and strict oversight to ensure financial security.

Michigan's proposed legislation, HB 4087, is very similar to Massachusetts' proposed legislation, nearly combining the three proposals. The Michigan proposal limits available funds from the general fund and economic stabilization fund to 10% for the state to invest in cryptocurrency, it allows the treasurer to hold cryptocurrency through secure custody solutions, qualified custodians, or exchange-traded products, and to loan the cryptocurrency if it does not increase financial risk.

In Ohio, two measures, HB 18 and SB 57, also reflect the same terms seen in the Massachusetts proposals: the authority to invest in cryptocurrency and the establishment of a digital asset reserve fund. HB 18 permits the treasurer to invest up to 10% of interim funds from the general fund and budget stabilization fund, along with other specific funds. However the investments are restricted to exchange-traded products with a minimum average market capitalization of $750 billion over the preceding twelve months. The bill also amends several existing sections of the statute to explicitly allow state retirement boards to invest in these exchange-traded products, while maintaining their fiduciary responsibilities to prioritize financial returns. SB 57 enacts a bitcoin reserve fund in the state treasury. Additionally, the bill allows law enforcement agencies to transfer forfeited bitcoin to the state's bitcoin reserve fund.