

State Leaders Briefing
The CLEAR Act
Consumer Ledger and Electronic
Asset Rights Act

Financial Transaction Freedom Briefing

September 10, 2026

2:00 - 4:00 PM Eastern

Our Panelists

Host

Elizabeth Murphy

Leading Solari's Financial Transaction
Freedom Legislative Initiatives



Our Panelists

Presenters

**Catherine Austin
Fitts**
President – Solari, Inc.



**David Liechty,
Esq.**
Attorney



**Carolyn Betts,
Esq.**
General Counsel – Solari, Inc.



Our Panelists

Representative Charles “Bud” Hulsey

Tennessee House of
Representatives



Tim Caban

Founder and President –
Copper Beech Advisors



Presentation Overview

the Solari Report 

I
What is the Automatic Third Lock?

II
Events Are Accelerating

III
CLEAR Act - Overview

IV
CLEAR Act - Guardrails

V
CLEAR Act – Substantive Sections

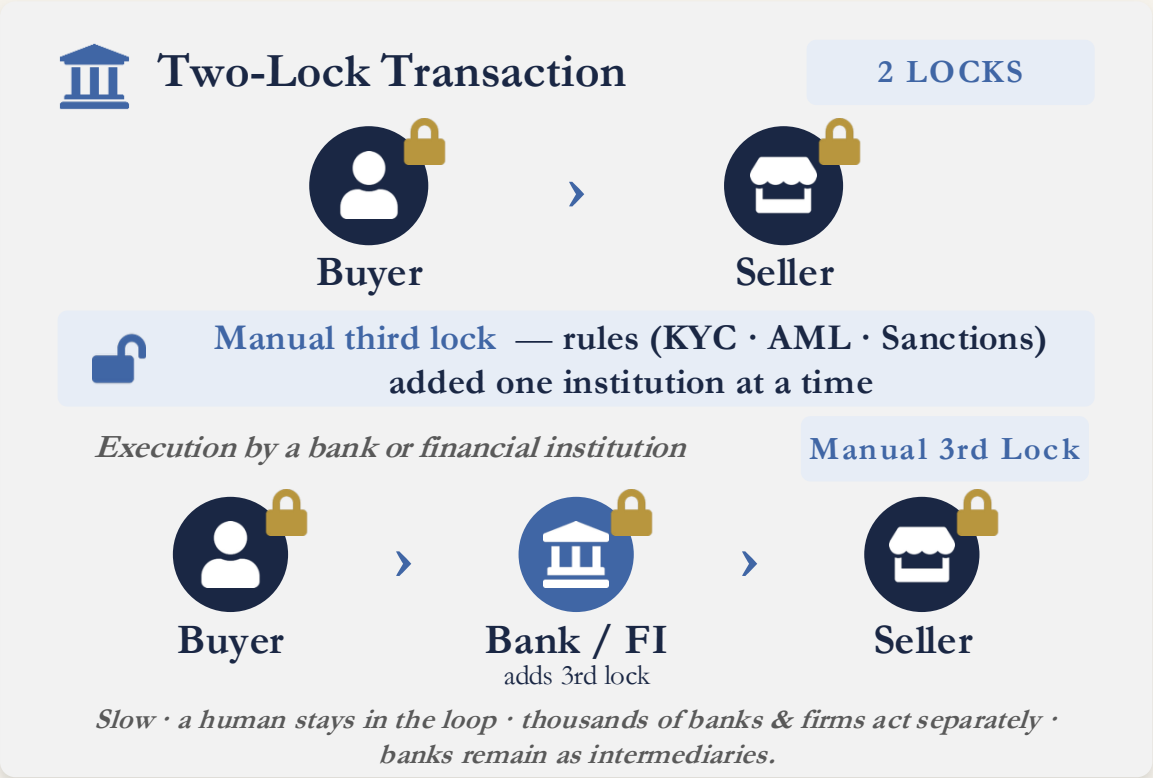
VI
Open Discussion

SECTION

I

What is the Automatic Third Lock?

The Three-Lock Paradigm



SECTION

II

Events are
Accelerating

Stablecoins & Crypto: A Small but Fast-Growing Share of the Pie



Outstanding Stablecoins & Crypto

DefiLlama live tracker: \$311 billion (7/26)

Projected issuance after the GENIUS Act: \$3–\$3.7T by 2030

\$2.6T

Crypto — total global market
(7/5/26)

\$183T

US household & nonprofit net
worth — Fed, Q1 2026



US Crypto Ownership Estimates

Federal Reserve: 10% of adults owned or used crypto at end-2025
(up from 7% in 2024; below the 12% peak in 2022, pre-FTX)

Motley Fool: 22% own crypto or hold via ETF — 16% direct, 6%
via ETF

< 0.5%

of total US household assets held in distributed-ledger
stablecoins & crypto



Conclusion

Critical to put up guardrails now — before
programmable-money volume grows from a
negligible share of household assets into a
structurally significant one.

Sources: DefiLlama; Federal Reserve (SHED survey, Z.1 Financial Accounts); Motley Fool Money 2026 Crypto Investor Trends Survey; State Street (Aug 2025); Scott Bessent (X, June 17 2025); Forbes.

DTCC Advances Its New Tokenization Service

**DTCC**

Press Release · July 15, 2026

DTCC Turns Tokenization into Reality: U.S. Trades Successfully Processed Using DTC-Tokenized Assets

DTCC began initial, limited production trades of securities tokenized via DTC's tokenization service on July 15, 2026, with plans to launch the service in October 2026.

The Depository Trust & Clearing Corporation (DTCC), the premier post-trade market infrastructure for global financial services, announced successful conversion of assets held at The Depository Trust Company (DTC) into tokens that were then used in real production trades. DTC's tokenization service is designed with feedback and collaboration from more than 50 financial industry firms, including BlackRock, Citi, J.P. Morgan, Morgan Stanley, Goldman Sachs, Charles Schwab, Robinhood, and Nasdaq. As DTCC noted, "today, DTC custodies assets valued at over \$114 trillion."

<https://www.dtcc.com/news/2026/july/15/dtcc-turns-tokenization-into-reality>



Key Facts

\$114T

in assets custodied by DTC today

- Limited production trades began July 15, 2026
- Broader service launch targeted October 2026
- 50+ collaborating financial firms
- BlackRock · Citi · JPMorgan · Morgan Stanley
· Goldman Sachs · Schwab · Robinhood · Nasdaq

Banks Plan a Shared Tokenized Deposit Network for 2027

**Blockhead**

Industry News · June 5, 2026

JP Morgan, Citi, US Banks Plan Shared Tokenized Deposit Network for 2027

The Clearing House — owned by the banks themselves — will run the network as a direct counter to stablecoins, keeping deposits on blockchain rails while inside the regulated banking system.

JPMorgan Chase, Citigroup, Bank of America, Wells Fargo, and other major US banks are building a shared tokenized deposit network through The Clearing House, targeting a launch in the first half of 2027, per a Wall Street Journal report. The system would let member banks move tokenized versions of customer deposits across blockchain infrastructure 24/7, with instant settlement. Clearing House CEO David Watson called it “a big move for the banks,” noting the industry faces a “radically different” future around on-chain payments and finance.

Source: blockhead.co/2026/06/05/jp-morgan-citi-us-banks-plan-shared-tokenized-deposit-network-for-2027



Key Facts

H1 2027

targeted network launch

- Run by The Clearing House — owned by the banks
- 24/7 movement with instant settlement
- A direct counter to stablecoins
- Deposits stay inside the regulated banking system
- JPMorgan · Citi · Bank of America · Wells Fargo

Tokenized Stocks Could Open Markets to 4 Billion People

**Benzinga**

Industry News · June 28, 2026

Coinbase CEO Brian Armstrong Says Tokenized Stocks Could Open US Markets To 4 Billion Unbrokered People

Coinbase CEO Brian Armstrong says tokenized stocks could fundamentally reshape global investing, pointing to a single striking metric to make his case.

Coinbase CEO Brian Armstrong said the shift to tokenized equities on modern financial rails is “going to totally change the world,” opening investment access for the roughly “four billion people in the world who are unbrokered” and “can’t get access to any high-quality U.S. companies to invest in.” Unlike earlier tokenized-equity products — which Armstrong described as “a derivative or a synthetic” that don’t convey true ownership — Coinbase’s offering is backed one-to-one by the underlying stock. Recent data also shows tokenized-stock trading volumes reaching record levels.

Source: benzinga.com/crypto/26/06/coinbase-ceo-brian-armstrong-says-tokenized-stocks-could-open-us-markets-to-4-billion-unbrokered-people



Key Facts

4 billion

“unbrokered” people who could gain access

- Backed one-to-one by the underlying stock
- Not a derivative or synthetic — true ownership
- Tokenized-stock volumes at record levels
- Coinbase — Brian Armstrong, CEO
- Framed as global, unbrokered market access

The Rest of the Balance Sheet: Deposits, Securities & Custody



Bank Deposits

\$19.37T

Total deposits, all US commercial banks — Fed (6/26)

\$103T

Customer deposits, world's 1,000 largest banks — TAB Global (FY2024)



Global Stocks & Bonds

Global equity: \$126.7 trillion

Global bonds / fixed income: \$145.1 trillion

Combined: roughly \$271.8 trillion



Depository Trust Company (DTC): \$114 trillion in custodied assets — as of the 7/26 tokenization pilot announcement.



US Household Net Worth

Rough composition — Federal Reserve Z.1 Financial Accounts (Q4 2025)



Securities (equities, bonds, funds)

40–55%



Real estate

23%



Bank deposits

5%

Sources: Federal Reserve (H.8, Z.1 Financial Accounts); TAB Global 1000 (2025); SIFMA Capital Markets Fact Book; DTCC.

SECTION

III

**CLEAR Act -
Overview**

A Rights Framework for Programmable Money

Residents increasingly hold value in programmable digital assets — stablecoins, tokenized deposits and securities, and other tokens — each of which can be frozen, restricted, surveilled, or conditioned through code, administrative keys, or external data feeds. The CLEAR Act protects the rights and financial freedom of residents across all such **covered digital assets**.

1

It does not ban the technology

Programmable money stays legal and useful. The Act regulates conduct, not instruments — it does not touch the issuance, registration, or qualification of any asset.

2

It binds who can pull the levers

Guardrails govern who may freeze, block, or alter your digital money, i.e., under what circumstances and with what accountability to the people affected.

3

It gives you enforceable rights

Disclosure, due process, data privacy, and a guaranteed non-programmable option — backed by the Attorney General and a private right of action.

A consumer-protection (UDAP) law built to sit alongside federal law — not to override it.

How the Act Is Built: Six Coordinated Parts

I

Short Title, Findings & Definitions

Sections 1–4

II

Non-Discrimination & Due Process

Sections 5–9

III

Financial Data Privacy

Sections 10–13

IV

Code & Control Transparency

Sections 14–18

V

Financial Freedom & State Operations

Sections 19–23

VI

**Coordination, Enforcement &
General Provisions**

Sections 24–29

Each Part is severable and independently enforceable — a distinct exercise of state authority. A court’s treatment of one Part does not govern another. (Section 28)

Key Concepts — and How It Fits Federal Law

Controlling person — a functional test

Duties fall on whoever actually holds the power to freeze, block, or alter your money: an issuer, custodian, exchange, payment processor, smart-contract administrator, or oracle / compliance-data provider. Whoever can pull the lever is on the hook.

Section 3

Covered digital asset vs. programmable money

Broad duties — disclosure, transparency, non-discrimination — reach any covered digital asset: stablecoins, tokenized deposits and securities, NFTs, governance tokens. The narrower cash-option guarantee applies to programmable money used as a medium of exchange.

Section 3

Built to sit alongside federal law

The Act does not regulate issuance or registration of any instrument, and steps back wherever a valid federal statute or regulation specifically requires otherwise, through general federal-compliance and anti-preemption language rather than naming any one federal regime.

Sections 8, 9, 24

Targets over-application of AML/KYC — not the rules

Bank Secrecy Act and AML/KYC duties stay fully in place. What the Act curbs is over-broad, automated dragnets that sweep in far more people than the law requires: comply with what is actually required, in the least restrictive manner it allows.

Sections 7(c), 8, 16

SECTION

IV

**CLEAR Act -
Guardrails**

Code Can Freeze Your Money — the Law Says Where That Power Stops

Programmable money can be written to automatically block, freeze, restrict, or expire a transaction. The CLEAR Act does ***not*** ban that technology — it puts guardrails around who may use those powers, under what circumstances, and with what accountability to the people affected.



Code can block a
transaction
automatically.



Code can freeze a
transaction
automatically.



Code can restrict a
transaction
automatically.

Guardrails don't ban the power. They bind it. Section 2 — Findings & Purpose

You Can't Be Frozen Out for Who You Are — or What You Believe

A controlling person may not deny a transaction, let it fail, or restrict or terminate service based, in whole or in part, on any of these factors:

- Sex, race, ethnicity, sexual orientation
- Religious belief, exercise, or affiliation
- Purchase or browsing history
- Trade, profession, or industry
- Political opinion, affiliation, or speech
- Medical history, incl. vaccination status
- Geographic location or residence
- A “social credit score” rating

Carve-out: a transaction that is itself a criminal act — and even then, due-process protections still apply. (§5(b))

You Get to Know Why

If your money is frozen or your account is restricted, the law turns a silent “no” into an accountable, on-the-record decision.

1

Contact information required

The controlling person must publish a phone number, physical address, and email address so a real person can be reached about the action.

Section 6(a)–(b)

2

A written explanation within 30 days

On request, they must provide a written statement that cites the specific rule relied on and attaches the term of service — no vague “policy violation.”

Section 6(c)

No Blanket Freezes — Only Individual, Specific Orders

NOT ALLOWED

A standing, automated algorithm that freezes accounts based on broad categories, e.g., an industry, a region, or a type of transaction, without a specific order naming the person.

Section 7(c)

REQUIRED INSTEAD

A particularized order that names the person, e.g., by name, account number, or other specific designation, together with prompt notice of the restriction and its basis.

Section 7(a)–(b)

Narrow exception: federal law or regulation may specifically require an action, but it must be applied in the least restrictive manner possible. (§8)

Your State Government Needs a Warrant

A note on “government”: this Act binds only this state’s own agencies. It cannot — and does not attempt to — restrict federal agencies (FBI, IRS, NSA) or another state’s government.

Warrant + notice

No access to your transaction-graph data without a probable-cause warrant. A subpoena or national-security letter is not enough, and you are notified within 90 days.

Section 10(a)–(b)

No purchase loophole

State government can’t buy its way around the warrant by purchasing your ledger-analytics data from a broker or other vendor.

Section 10(c)

No fishing expeditions

No bulk or reverse searches for “everyone who transacted with X” without a warrant tied to a specific, described crime and narrowly scoped.

Section 10(d)

Your Data Is Protected — and So Are Privacy Tools

Data duties, by default

- Collect only what is needed to complete the transaction
- Don't sell or share your data without informed consent
- Delete or de-identify it when no longer needed
- Notify you, and the Attorney General, of any breach
- No conditioning service on non-essential data collection

Section 12(a)(1)–(5)

Privacy tools protected — not “suspicious”

The controlling person must offer privacy-protective options where feasible (§13(a)). And the lawful use of encryption or self-custody cannot, standing alone, be treated as “suspicious activity” or a basis to deny or cut off service.

Section 13(b) — Safe Harbor

The Fine Print Is Public. So Is the Kill Switch.

Every capability must be disclosed

In plain, machine-readable language, the controlling person must publicly disclose everything the code can do — freeze, expire, reverse, restrict, burn. Code is a binding disclosure: an undisclosed restriction can't be enforced, and you can be compensated if one is used to erase or reverse your assets.

Section 14(a)–(c)

Whoever holds the “kill switch” is named

The specific people or key-holders who can alter, freeze, or upgrade the asset must be publicly identified — not just a company name. And at least 30 days' notice is required before any material change to that authority.

Section 15(a)–(b)

The “Compliance Blocklist” System Is Disclosed

Screening and blocklists shape who can transact. This guardrail makes the system visible — with a two-tier structure that still protects legitimate screening logic.

PUBLIC TIER

The public must be told that screening happens, and who provides the compliance data — the oracle or compliance-data provider behind the blocklist, by legal name.

Section 16(a)

CONFIDENTIAL TIER

The specific criteria and thresholds are filed with regulators — not the public — protecting legitimate AML logic from being gamed, while remaining subject to audit and enforcement.

Section 16(b)–(d)

You Always Have a Cash / Non-Programmable Option

Anyone that requires programmable money for a transaction must also offer a non-programmable payment option — free of charge.

Large merchants

Businesses with annual revenue above \$5,000,000.

Government agencies

Any state agency paying, or being paid by, a resident.

Essential-service billers

Electricity, gas, water, telecom, and similar providers.

Non-programmable = cash, a non-electronic payment instrument, or a non-programmable electronic option.
(Section 21(a)–(b))

The State Restrains Itself

The Act does not only bind private controlling persons — it binds the state itself. No state agency may:

1

Impose a programmable restriction on payments to or from residents, or condition a payment on consent to financial surveillance

2

Condition any benefit, license, permit, or service on accepting financial or personal surveillance, or on using a particular payment instrument

3

Adopt, require, accept, or participate in a central bank digital currency (CBDC) arrangement without express legislative authorization

Applies to state agencies only — not to federal agencies. (Section 22(a)(1)–(3))

Real Teeth for Enforcement

The Attorney General

Can investigate, sue, fine, and force compliance from controlling persons — undefeated by any arbitration clause or class-action waiver.

Section 25(a)

You, directly

A private right of action: individuals harmed can sue and recover actual damages plus attorney's fees — and up to treble punitive damages for willful violations.

Section 25(b)

Suppression

Evidence gathered by state government in violation of the warrant rule is inadmissible in the courts of this state.

Section 25(f)

And for repeated, willful violations, the Secretary of State may revoke an entity's right to do business in the state. (§25(h))

Guardrails don't ban the power. They bind it.

The CLEAR Act keeps programmable money legal and useful — while making sure no issuer, custodian, or state agency can silently freeze, surveil, or restrict you without disclosure, due process, and a right to be heard.

SECTION

V

**CLEAR Act –
Substantive
Sections**

CLEAR Act Part II — Non-Discrimination and Due Process

Part II

CLEAR Act SECTIONS 5–9

THE PURPOSE

No one may be shut out of digital money for who they are or what they lawfully do — and if action is taken, they are owed reasons and due process.

WHAT IT INTENDS

- 1 No identity- or viewpoint-based denial**
A controlling person may not deny, fail, restrict, or terminate service based on politics, religion, speech, medical history, purchases, location, industry, any lawful activity, or a social-credit score. (§5)
- 2 A right to a statement of reasons**
Affected users can demand a written explanation within 30 days that cites the specific rule and the term of service relied on — no vague “policy violation.” (§6)
- 3 No blanket freezes**
Blocking requires a particularized order naming the person or account; standing, category-based automated freezes are barred. (§7)
- 4 Narrow, bounded exceptions**
A federal-compliance exception (least-restrictive, with notice) and a securities-law transfer carve-out are exceptions. (§§8–9)

CLEAR Act Part III — Financial Data Privacy

Part III

CLEAR Act SECTIONS 10–13

THE PURPOSE

Your on-chain financial life carries a reasonable expectation of privacy — against both the state and the firms that process your transactions.

WHAT IT INTENDS

- 1 A warrant to watch you**
State government needs a probable-cause warrant to reach your transaction-graph data; a subpoena or national-security letter is not enough, and you are notified within 90 days. (§10)
- 2 Loopholes closed**
No buying your data from brokers to sidestep the warrant, and no bulk or reverse “who-transacted-with-X” searches without a narrowly-tailored warrant. (§10)
- 3 Ledger data is not “public”**
The state formally recognizes a reasonable expectation of privacy in ledger data; evidence gathered in violation is suppressed. (§11, §25(f))
- 4 Private-sector data duties**
Collect only what is needed, don’t sell it, delete it when done, and disclose breaches — and privacy tools are protected, not treated as suspicious. (§§12–13)

CLEAR Act Part IV — Code and Control Transparency

Part IV

CLEAR Act SECTIONS 14–18

THE PURPOSE

If code can act on your money, the powers in that code — and the people who hold them — must be disclosed in plain, machine-readable form.

WHAT IT INTENDS

- 1 Every capability disclosed**
All powers coded into the asset — freeze, expire, reverse, restrict, burn — must be publicly disclosed. Code is a binding disclosure. (§14)
- 2 Undisclosed control is unenforceable**
A restriction that wasn't disclosed can't be enforced, and its use can trigger compensation to the person harmed. (§14)
- 3 Name the “kill switch” holders**
The specific key-holders who can alter, freeze, or upgrade the asset must be identified, with 30 days' notice before major changes. (§15)
- 4 Tiered compliance-data disclosure**
The public learns that screening happens and who supplies it; the exact criteria are filed confidentially with regulators, subject to audit. (§§16–18)

CLEAR Act Part V — Financial Freedom and State Operations

V

CLEAR Act SECTIONS 19–23

THE PURPOSE

Guarantee the exits — self-custody, peer-to-peer, and cash — and bind the state so it cannot itself become the controller.

WHAT IT INTENDS

- 1 Right to self-custody & peer-to-peer**
Holding your own keys and transacting peer-to-peer is a protected right, not, by itself, money transmission requiring a license. (§19)
- 2 Right to run validation**
Operating a node or otherwise validating on a network cannot, by itself, trigger penalties or licensing. (§20)
- 3 A guaranteed cash option**
Large merchants, state agencies, and essential-service billers must offer a free non-programmable payment option. (§21)
- 4 The state restrains itself**
No programmable restrictions on payments, no surveillance conditions on benefits, and no CBDC without express legislative authorization. (§§22–23)

SECTION

VI

Open Discussion

Representative Charles “Bud” Hulsey



Career at a Glance

1972

B.A. in Education, Bob Jones University

Career

Retired Lieutenant, Kingsport Police Department

FBI NA

Post-graduate training, FBI National Academy (Univ. of Virginia)

2014

Elected to the Tennessee House, unseating a three-term incumbent

2025

Chair, House Appropriations & Oversight Committee



Retired Lieutenant, Kingsport Police



FBI National Academy Graduate



Tennessee House, District 2 (Sullivan Co.)



Born May 30, 1949



Served in the House from 2014-2026



Bob Jones University, B.A. (1972)



Why His Voice Matters Here



Law-enforcement veteran — A career in policing and FBI National Academy training bring a front-line grasp of surveillance, due process, and the limits of investigative power.



Main Street business owner — As founder and president of a Tri-Cities logistics company, he knows payment systems and the real cost of debanking on working businesses.



Senior legislator — A senior committee chairman with the standing to advance consumer-protection and financial-freedom legislation like the CLEAR Act.

Open Discussion

Catherine Austin Fitts

President - Solari, Inc.

David Liechty, Esq.

Attorney

Carolyn Betts, Esq.

General Counsel – Solari, Inc.

Charles “Bud” Hulse

Special Guest Panelist

Timothy Caban

Special Guest Panelist

Elizabeth Murphy

Host, Financial Transaction
Freedom Legislative Initiatives

Recommended Links & Resources

Solari Report Resources

- *Model Legislation: Solari Consumer Ledger and Electronic Asset Rights (CLEAR) Act* (<https://solari.com/ftf/model-legislation/clear-act/>)
- State Legislature Briefing on Programmable Money (Part 1) (<https://solari.com/briefing-for-state-leaders-a-legislators-guide-to-programmable-money/>)
- State Legislature Briefing on Programmable Money (Part 2) (<https://solari.com/briefing-for-state-leaders-a-legislators-guide-to-programmable-money-part-two-with-david-liechty/>)
- State Legislature Briefing on the GENIUS Act and Stablecoins (<https://solari.com/briefing-for-state-leaders-the-genius-act-and-stablecoins-video-presentation-now-available/>)
- The GENIUS Act and its Implications for Financial Transaction Freedom (<https://solari.com/the-genius-act-and-its-implications-for-financial-transaction-freedom/>)
- Financial Transaction Freedom Resources (<https://solari.com/ftf/>)
- Digital Money, Digital Control Series (<https://solari.com/digital-money-digital-control/>)