The Cantillon Institute

Working Paper Series: The Protocol Layer

Working Paper No. 1

K.R. Black 2026

The Finality Illusion: Settlement Architecture, Probabilistic Consensus, and the GENIUS Act's Foundational Assumption

Abstract

The GENIUS Act defines payment stablecoins by economic function: a dollar-denominated instrument redeemable at par, backed by high-quality liquid assets, operated by a licensed issuer. The definition is silent on technical architecture. That silence is not neutral. Every redemption obligation in the Act, every requirement for par settlement, every assumption about the operational integrity of the payment rail beneath the instrument, depends on a condition the Act does not define and the underlying systems do not guarantee: transaction finality. Blockchain networks do not produce deterministic finality. They produce probabilistic finality; a statistical condition in which the irreversibility of a settled transaction is a function of elapsed time, block depth, validator participation, and network conditions, not a binary state that legislation can mandate. This paper maps the gap between the finality the GENIUS Act assumes and the finality blockchain consensus mechanisms actually provide. It examines the redemption mechanics the Act requires, the settlement architecture the underlying networks produce, and the failure mode that emerges when legislative obligation meets probabilistic reality at scale. The gap is not

theoretical. The conditions that reveal it have occurred on every major public blockchain. The GENIUS Act has no mechanism to address them.

Introduction

I have been building on-chain infrastructure since 2016. In that time I have watched the DAO hack, two DeFi summers, three algorithmic stablecoin collapses, and more bridge exploits than I can list without a spreadsheet. I have also watched legislators produce framework after framework that describes what these systems do in economic terms while remaining systematically agnostic about how they do it.

The GENIUS Act is the most consequential iteration of that pattern. It establishes a federal licensing framework for payment stablecoin issuers, mandates 1:1 reserve backing in high-quality liquid assets, and requires that licensed issuers honor redemption requests at par (Guiding and Establishing National Innovation for U.S. Stablecoins Act, 2025, §4(a)). The Act defines a payment stablecoin as a digital asset designed to be used as a means of payment or settlement that the issuer represents will maintain a stable value relative to a fixed monetary value. The definition covers the economic promise. It says nothing about the technical substrate on which that promise must be kept.

This is the GENIUS Act's foundational error; not its most visible one, but its deepest. Every other architectural failure I intend to document in this series sits on top of it. The Act assumes that when a payment stablecoin transaction is recorded on a blockchain, that transaction has settled. In the sense the Act requires, settled means final, irreversible, and legally discharged. Blockchain networks do not produce that state. They produce a probabilistic approximation of it that improves over time and degrades under specific conditions. The Act's authors did not account for those conditions because the Act's authors did not model the underlying system. They modeled the economic outcome the system is supposed to produce.

The distinction matters in normal conditions. It matters catastrophically in abnormal ones.

I. What Finality Means: The Technical Condition the Act Does Not Define

In traditional payment systems, settlement finality is a defined legal and operational state. The Bank for International Settlements describes settlement finality as the irrevocable and unconditional transfer of an asset or financial instrument, or the discharge of an obligation by the infrastructure or its participants, in accordance with the terms of the underlying contract (BIS Committee on Payment and Settlement Systems, 2003, p. 1). Under Fedwire, a funds transfer is final and irrevocable at the moment the Federal Reserve credits the receiving institution's account. The legal condition is instantaneous and deterministic. No subsequent network event can reverse it.

Blockchain networks operate differently. In a proof-of-work system, transactions are included in blocks, and blocks are appended to a chain. A transaction is not final at inclusion. It is final when the probability of a competing chain of equal or greater length superseding the chain on which the transaction appears becomes negligible. Nakamoto (2008) demonstrated that this probability decreases exponentially with the number of subsequent blocks. At six confirmations on Bitcoin's network, the probability of a successful double-spend attack by an adversary controlling 10% of hash power falls below 0.1% (Nakamoto, 2008, §11). The transaction is not irreversible. It is irreversible enough.

"Irreversible enough" is not a legal standard. It is an engineering tolerance. The gap between those two descriptions is where the GENIUS Act breaks.

Proof-of-stake systems introduce a different finality model. Ethereum's post-Merge consensus mechanism, Casper FFG, achieves finality when a checkpoint block receives justification and finalization votes from validators representing at least two-thirds of total staked ETH (Buterin & Griffith, 2017, §4). Once finalized, a block cannot be reverted without the attacking party burning at least one-third of total staked ETH through the slashing mechanism. As of April 2026, the total staked ETH supply exceeded 34 million ETH, placing the cost of finality reversal above $60 billion at prevailing prices. That is a meaningful economic deterrent. It is not a legal guarantee. The finality condition depends on validator participation rates, client software integrity, and the absence of coordinated validator failure. None of those conditions can be guaranteed in the way Fedwire guarantees settlement.

Ethereum's finality timeline under normal conditions is approximately two epochs, or 12.8 minutes. The GENIUS Act's redemption framework does not specify a blockchain confirmation threshold. It does not specify an acceptable finality latency. It does not distinguish between a payment stablecoin settled on a network with 12.8-minute probabilistic finality and one settled on a network with 60-minute probabilistic finality. The Act is agnostic. That agnosticism is itself a decision with structural consequences.

II. The Consensus Landscape: Finality Across the Architecture the Act Does Not Name

The GENIUS Act does not specify which blockchain networks a licensed payment stablecoin may use. This means the finality conditions applicable to a GENIUS Act-licensed instrument range across every major public blockchain network, from the relatively robust to the demonstrably fragile.

Bitcoin's proof-of-work consensus produces probabilistic finality with a six-confirmation standard of approximately 60 minutes. The economic cost of reorganizing the chain grows with each subsequent block. As of April 2026, Bitcoin's hash rate exceeded 800 exahashes per second (EH/s), placing the capital cost of a sustained 51% attack beyond the reach of any non-state actor and above the deterrence threshold for most state actors under most conditions (Cambridge Centre for Alternative Finance, 2026). Bitcoin's finality model is slow. It is also the most battle-tested in production. The network has operated continuously since January 2009 and has never experienced a successful double-spend on the main chain beyond one block depth.

Ethereum's proof-of-stake consensus, operating under the Gasper protocol combining Casper FFG and LMD-GHOST, targets finality within two epochs under normal validator participation (Buterin & Griffith, 2017). The system is newer than Bitcoin's. Its finality assumptions depend on sustained participation above two-thirds of active validators and the absence of coordinated client failure. On May 11, 2023, Ethereum mainnet experienced a finality delay lasting approximately 25 minutes when a surge in attestation load triggered a cascading issue in minority client implementations, causing the network

to fail to finalize blocks across multiple consecutive epochs (Ethereum Foundation, 2023). The network recovered. The GENIUS Act's framework contains no provision for what a licensed issuer's redemption obligations are during a period in which the settlement network is not finalizing transactions.

Solana operates under a tower BFT consensus variant and claims slot times of approximately 400 milliseconds, with theoretical finality within seconds under optimal conditions (Yakovenko, 2018). In practice, Solana has experienced at least six major network outages between 2021 and 2024, including a 17-hour outage in September 2021 and a second major halt in May 2022 (Solana Foundation, 2022). During these outages, transaction finality was not delayed. It was unavailable. A payment stablecoin issuer licensed under the GENIUS Act and operating on Solana would face redemption obligations on a network that had periodically ceased producing finality altogether.

Smaller proof-of-work chains present a different failure mode. Ethereum Classic suffered 51% attacks in August 2020 in which attackers reorganized 3,693 blocks in the first incident and 4,000 blocks in the second, reversing transactions that had received standard confirmation thresholds (Messari Research, 2020). These were not theoretical attacks. They were executed, confirmed, and documented. Bitcoin SV experienced a 51% attack in August 2021 in which attackers sustained a reorganization for several hours before being detected (Coin Metrics, 2021). The affected transactions were not settled in any sense the GENIUS Act's redemption architecture can accommodate.

The GENIUS Act's architecture permits a licensed payment stablecoin issuer to operate on any of these networks. It distinguishes between them on no technical criterion relevant to settlement finality. The legal obligation to redeem at par is identical regardless of whether the underlying network is Bitcoin, Solana, or Ethereum Classic. The finality conditions are not.

III. The Redemption Obligation Against the Probabilistic Record

The GENIUS Act's redemption requirements establish a clear legal standard. Licensed issuers must honor redemption requests at par value, meaning one payment stablecoin redeems for one dollar of reserve assets (GENIUS Act, 2025, §4(a)(1)(A)). The Act's redemption timeline provisions require issuers to process redemptions in a commercially reasonable time, with regulatory guidance expected to operationalize this as a T+1 standard, consistent with existing money market fund redemption frameworks.

The T+1 standard assumes that the transaction triggering the redemption request has settled. A user submits a redemption request. The issuer receives the payment stablecoin. The issuer returns one dollar from reserves. The transaction is discharged. This sequence requires that the payment stablecoin transfer to the issuer is final at the point the issuer processes it; otherwise the issuer is exposed to a double-spend in which the user receives reserve dollars while the original stablecoin transfer is reversed on-chain.

This is not a novel vulnerability. It is the oldest attack vector in public blockchain transaction processing, first described formally by Nakamoto (2008) and operationalized in practice on virtually every major proof-of-work chain. The defense in traditional blockchain payment processing is to wait for sufficient confirmations before releasing funds. A merchant accepting Bitcoin waits for six confirmations. An exchange processing a large withdrawal may wait twelve. The waiting period is the finality buffer; the time required for the probabilistic guarantee to become commercially adequate.

The GENIUS Act's T+1 redemption framework does not accommodate a finality buffer of any duration. It establishes a maximum processing window, not a minimum confirmation threshold. An issuer processing a redemption under T+1 constraints faces a direct conflict with the finality requirements of the underlying network: accepting the stablecoin transfer after two confirmations to meet the redemption timeline, or waiting for six confirmations and potentially violating the T+1 standard for transactions submitted late in the business day. The Act does not resolve this conflict. The Act does not acknowledge it exists.

The exposure is not symmetric. In normal conditions, on well-capitalized networks, the probability of a successful double-spend after two or three confirmations is low enough to

be commercially acceptable for small transactions. For large-denomination redemptions, the economics change. Karame, Androulaki, and Capkun (2012) demonstrated that double-spend attacks on Bitcoin requiring only one confirmation are feasible with modest computational resources. A $10 million redemption request processed after two confirmations presents a materially different risk profile than a $50 transaction. The GENIUS Act's redemption obligations are denomination-agnostic. The finality risk is not.

IV. The Failure Mode the Framework Cannot See

The GENIUS Act's finality problem is structurally invisible in normal operating conditions. When networks are healthy, validator participation is high, and transaction volume is within normal range, probabilistic finality converges to practical finality quickly enough that the distinction is operationally irrelevant. A payment stablecoin transferred on Ethereum under normal conditions will reach effective finality within 15 minutes. A T+1 redemption processed against that transfer carries minimal double-spend exposure.

The failure mode appears when conditions are not normal. And the conditions that produce abnormal finality events are precisely the conditions most likely to accompany a stress event in the stablecoin market.

Consider the mechanism. A stablecoin issuer faces a reserve adequacy concern. A regulatory announcement, a counterparty failure, or a market event triggers redemption demand. Users submit large-denomination redemption requests simultaneously. Transaction volume on the underlying network spikes. Mempool congestion increases. Gas fees rise sharply. Block inclusion times lengthen. Network finality slows because attestation loads increase and minority client implementations may fall behind. Simultaneously, the issuer is processing high-value redemptions against transactions that have not reached full probabilistic finality, because the T+1 window is closing and the network is congested.

This is not a hypothetical scenario assembled for rhetorical effect. It is a description of the conditions present during every significant stablecoin stress event on record. In March 2023, USDC lost its dollar peg following the disclosure of $3.3 billion in reserve deposits held at Silicon Valley Bank (Circle Internet Financial, 2023). USDC traded as low as $0.877

on secondary markets. Redemption volume spiked. The Ethereum network, which carries the majority of USDC supply, experienced elevated gas prices and extended block times during the peak redemption period. The GENIUS Act's regulatory framework, had it been in force, would have required par redemptions processed within commercially reasonable time against a network operating under precisely the conditions that degrade finality.

The May 2022 Terra/LUNA collapse presents the outer bound of the failure mode. UST, an algorithmic stablecoin not backed by reserves in the GENIUS Act sense, de-pegged catastrophically. $40 billion in notional value was destroyed within 72 hours (Chainalysis, 2022). Transaction volumes on the Terra network overwhelmed block production capacity. The network halted twice during the collapse. This is not a scenario directly analogous to a GENIUS Act-licensed issuer, whose reserves would provide a meaningful buffer. But the network behavior, the congestion, the finality degradation, the halts, is entirely analogous. Reserve-backed issuers operating on networks under stress do not receive special network priority. The blockchain is indifferent to their regulatory obligations.

The GENIUS Act contains no provisions for network outage scenarios. It contains no finality standard. It contains no mechanism by which a licensed issuer can suspend or delay redemptions pending restoration of network finality. The only analogous provision in existing financial regulation is the money market fund redemption gate, permitted under SEC Rule 2a-7, which allows funds to suspend redemptions for up to 10 business days during periods of market stress (Securities and Exchange Commission, 2023). The GENIUS Act does not extend an equivalent mechanism to payment stablecoin issuers facing network-level settlement failure.

V. The Regulatory Architecture's Structural Blind Spot

The GENIUS Act's silence on finality is not an oversight that can be corrected by guidance. It reflects a structural feature of how the Act was drafted: by defining payment stablecoins through economic function while remaining agnostic about technical architecture, the Act made finality impossible to regulate within its own framework.

To mandate a finality standard, the Act would need to specify either a minimum confirmation threshold on each permitted network or a maximum acceptable finality

latency. Either approach requires naming the networks and characterizing their consensus mechanisms. The Act does not do this. The Office of the Comptroller of the Currency and the Federal Reserve, as the primary regulatory bodies under the Act's framework, have authority to issue guidance on reserve requirements, capital adequacy, and redemption processes. Neither agency has published any indication that it intends to address on-chain settlement finality in implementing regulations (OCC, 2025; Federal Reserve Board, 2025).

The prudential regulators are not equipped to address it. The Fed's payment system oversight framework was built for Fedwire, ACH, and CHIPS; deterministic settlement systems operating under known rules with defined finality conditions. The Fed has developed a conceptual framework for stablecoin oversight that focuses on reserve adequacy and issuer solvency (Federal Reserve Board, 2022). It has not developed a framework for probabilistic settlement risk, because the systems the Fed has historically overseen do not exhibit it.

There is a deeper problem. Even if regulators attempted to mandate a finality standard, enforcement would require monitoring on-chain confirmation depths for every transaction processed by every licensed issuer. No regulatory body currently has this capability at production scale. The OCC examines bank holding companies. It does not operate blockchain node infrastructure or run real-time mempool surveillance. The gap between the regulatory obligation the Act creates and the supervisory infrastructure required to enforce it is not a resourcing problem. It is an architectural one.

Goodhart (1975) observed that any statistical regularity used as a control target tends to collapse once pressure is placed upon it. The principle has been extended broadly across financial regulatory contexts, but its original formulation describes precisely the problem here. The finality guarantee that makes T+1 redemption operationally feasible in normal conditions is the same guarantee that degrades under the stress conditions that would trigger large-scale redemptions. The Act's regulatory architecture is calibrated for the normal condition and blind to the failure mode.

Conclusion

The GENIUS Act is enacted. The licensed payment stablecoin market it creates is growing. Issuers operate on multiple networks with materially different finality characteristics. The regulatory framework is agnostic about those differences because the framework was designed to govern economic outcomes, not technical mechanisms.

The failure mode I have described is not continuous. It is episodic. In the intervals between stress events, the probabilistic finality of major public blockchain networks is adequate for commercial payment processing. The T+1 redemption standard is meetable. The double-spend exposure on large-denomination transactions is manageable. The legislative framework functions well enough that no one is required to look at what it assumes.

The stress event changes this. The stress event is not a tail risk. The stablecoin market has experienced material reserve concerns, de-peg events, and network congestion in 2019, 2020, 2021, 2022, and 2023. The market has existed for approximately seven years. It has experienced significant stress events in five of them. This is not a market with an obscure tail risk. It is a market with a recurring stress pattern that the GENIUS Act's finality assumptions cannot accommodate.

When the next stress event arrives, licensed issuers will face a convergence of conditions the Act did not anticipate: elevated redemption volume, network congestion, degraded finality, and a T+1 obligation that the settlement infrastructure beneath them cannot meet on its own terms. The issuers will be solvent. The reserves will exist. The dollar will be there. The blockchain will not cooperate on the timeline the law requires.

The gap between those two conditions is not a regulatory gap that prudential oversight can close after the fact. It is a structural gap embedded in the Act's foundational architecture at the point of drafting. This paper is the first in a series that maps that architecture precisely. The oracle problem, which governs how the dollar peg itself is determined within the technical system, is the next mechanism to examine. It shares the same foundational error.

References

Bank for International Settlements, Committee on Payment and Settlement Systems. (2003). *Recommendations for securities settlement systems*. BIS. https://www.bis.org/cpmi/publ/d46.pdf

Buterin, V., & Griffith, V. (2017). *Casper the friendly finality gadget*. arXiv preprint arXiv:1710.09437. https://arxiv.org/abs/1710.09437

Cambridge Centre for Alternative Finance. (2026). *Cambridge Bitcoin Electricity Consumption Index: Mining map and hash rate data*. University of Cambridge. https://ccaf.io/cbnsi/cbeci

Chainalysis. (2022, May 19). *The collapse of Terra: How the blockchain data tells the story*. Chainalysis Blog. https://blog.chainalysis.com/reports/terra-collapse/

Circle Internet Financial. (2023, March 11). *An update on USDC and Silicon Valley Bank*. Circle Blog. https://www.circle.com/blog/an-update-on-usdc-and-silicon-valley-bank

Coin Metrics. (2021, August 5). *BSV 51% attack post-mortem*. Coin Metrics State of the Network, Issue 113. https://coinmetrics.io/state-of-the-network-issue-113/

Ethereum Foundation. (2023, May 12). *Ethereum mainnet finality incident post-mortem*. Ethereum.org Blog. https://ethereum.org/en/blog/2023-05-12-finality-incident/

Federal Reserve Board. (2022, August 16). *Stablecoins: Growth potential and impact on banking*. FEDS Notes. https://www.federalreserve.gov/econres/notes/feds-notes/stablecoins-growth-potential-and-impact-on-banking-20220816.html

Federal Reserve Board. (2025). *Policy statement on bank engagement with crypto-asset activities*. Board of Governors of the Federal Reserve System. https://www.federalreserve.gov/

Goodhart, C. A. E. (1975). Problems of monetary management: The UK experience. In *Papers in monetary economics* (Vol. 1). Reserve Bank of Australia.

Guiding and Establishing National Innovation for U.S. Stablecoins Act, S. 1582, 119th Cong. Pub. L. 119-27 (2025).

Karame, G. O., Androulaki, E., & Capkun, S. (2012). Double-spending fast payments in Bitcoin. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security* (pp. 906–917). ACM. https://doi.org/10.1145/2382196.2382292

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, *4*(3), 382–401. https://doi.org/10.1145/357172.357176

Messari Research. (2020, August 10). *Ethereum Classic suffers third 51% attack in a month*. Messari. https://messari.io/report/ethereum-classic-51-attacks

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Office of the Comptroller of the Currency. (2025). *Interpretive letter on stablecoin activities of national banks*. OCC. https://www.occ.gov/

Securities and Exchange Commission. (2023). *Money market fund reforms; Form PF reporting requirements for large liquidity fund advisers* (Release No. IC-34959). SEC. https://www.sec.gov/rules/final/2023/ic-34959.pdf

Solana Foundation. (2022, June 1). *Mainnet beta outage report: May 2022*. Solana Foundation. https://solana.com/news/02-25-22-solana-mainnet-beta-outage-report

Yakovenko, A. (2018). *Solana: A new architecture for a high performance blockchain v0.8.13*. Solana Labs. https://solana.com/solana-whitepaper.pdf

---

power. Working papers represent the views of the named fellow and do not constitute investment advice or legal opinion.

The Protocol Layer series examines base infrastructure decisions embedded in stablecoin legislation. Working Paper No. 2 will address the oracle problem: how the dollar peg is technically determined within the stablecoin system and why the GENIUS Act's redemption architecture assumes a price feed mechanism that does not exist in the form the legislation requires.