The CLARITY Act Built a Legal Wall Between Builders and the Government -- and Almost Nobody Noticed

Sections 309 and 409. Title VI. Section 604. The Roman Storm Precedent. 1inch Called It Very DeFi-Friendly. a16z Called It a Meaningful Win. -- Q2 2026

In August 2025, Roman Storm -- a software developer who co-created Tornado Cash, an open-source privacy protocol on Ethereum -- was convicted in federal court under 18 U.S.C. Section 1960, the federal criminal statute for operating an unlicensed money-transmitting business. Storm had written code. He had published that code as open source software. He had not held user funds. He had not executed user transactions. He had not maintained custody of anything. He had written software that other people chose to use, and for that act of software development, he was convicted of a federal crime carrying a maximum sentence of five years in federal prison. Storm is appealing. But his conviction established the legal precedent that the US government believes open-source blockchain software developers can be criminally liable for how other people use their code -- a precedent that sent a chill through the entire global blockchain development community and accelerated the migration of crypto development talent from the United States to jurisdictions with clearer legal frameworks. Sections 309 and 409 of the CLARITY Act -- along with Section 604, which folds in the Blockchain Regulatory Certainty Act, and Title VI, Protecting Software Developers and Software Innovation -- are the legislative response to the Roman Storm precedent. Together they create the first codified statutory protection for blockchain software developers, node operators, validators, oracle providers, and DeFi infrastructure builders in American legal history. The core principle, stated directly in the bill, is this: if you build software and never touch anyone's money, you should not be regulated like a bank. White House digital-assets adviser Patrick Witt described Section 1960 -- the statute that convicted Roman Storm -- as the final hurdle for the CLARITY Act. 1inch's chief legal officer called the CLARITY Act's DeFi provisions very DeFi-friendly. a16z crypto and the DeFi Education Fund described Sections 309 and 409 as meaningful wins. The CLARITY Act is a market structure bill for institutional investors. But its developer and validator protection provisions are the provisions that will determine whether blockchain innovation stays in America or moves permanently offshore.

01 -- THE ROMAN STORM PRECEDENT: WHY DEVELOPER PROTECTIONS ARE EXISTENTIALLY IMPORTANT

To understand why the CLARITY Act's developer and validator protection provisions matter, it is necessary to understand what happened to Roman Storm and why his case represents an existential threat to blockchain software development in the United States that the CLARITY Act's provisions are

specifically designed to address.

Tornado Cash is an Ethereum smart contract protocol that provides privacy for Ethereum transactions by mixing user deposits and withdrawals to obscure the on-chain transaction trail. The protocol was built as open-source software by Roman Storm, Roman Semenov, and Alexey Pertsev. The smart contracts are immutable -- once deployed to the Ethereum blockchain, they cannot be altered, updated, or shut down by their creators. The creators have no ongoing control over how the protocol operates, who uses it, or what purposes it serves.

In August 2022, the US Treasury's Office of Foreign Assets Control sanctioned Tornado Cash -- adding the protocol's smart contract addresses to the OFAC Specially Designated Nationals list. The OFAC action was legally controversial because it targeted immutable software code rather than a specific individual or entity with ongoing control over the protocol. In November 2024, a Fifth Circuit federal appeals court ruling confirmed that OFAC had exceeded its authority in sanctioning immutable smart contract code, holding that immutable software is not property within the meaning of the International Emergency Economic Powers Act.

Despite the Fifth Circuit's ruling that the OFAC sanction of the immutable smart contract code was unlawful, Roman Storm's criminal prosecution proceeded on different grounds: the government argued that Storm had operated an unlicensed money-transmitting business under 18 U.S.C. Section 1960 by creating and maintaining Tornado Cash as a developer. In August 2025, Storm was convicted. The conviction means that in the current US legal framework -- before the CLARITY Act is signed -- a developer who creates open-source financial software, retains no custody of user funds, executes no user transactions, and has no ongoing control over the deployed protocol can still be convicted of a federal crime for building the software in the first place.

The chilling effect of the Roman Storm conviction on blockchain software development in the United States was immediate and measurable. Developer surveys conducted in late 2025 showed that a significant percentage of US-based blockchain developers were considering relocating to jurisdictions with clearer legal frameworks for software developers. Token generation events began routing through non-US platforms and structures specifically to avoid US legal exposure. Coinbase's Echo platform -- a $375 million acquisition designed to bring token launches back onshore -- hosted Monad's $296 million raise, demonstrating that a compliant onshore alternative could work. But the underlying legal risk for developers writing code that interacts with financial systems remained unresolved until Section 604 of the CLARITY Act.

> ***ROMAN STORM CONVICTION: Convicted under 18 USC 1960 for operating an unlicensed money-transmitting business. He wrote open-source code. He held no user funds. He executed no user transactions. He had no ongoing control over the deployed protocol. The CLARITY Act Section 604 carves out non-controlling developers from exactly this prosecution theory. Storm is appealing.***

02 -- SECTIONS 309 AND 409: THE BROKER-DEALER REGISTRATION EXEMPTIONS

Sections 309 and 409 of the CLARITY Act -- confirmed in the CCN analysis and the CryptoTimes breakdown of the 309-page bill text -- are the provisions that exclude validators, open-source developers, interface providers, and self-custodial wallet operators from the broker-dealer registration and compliance requirements that apply to centralized exchanges, brokers, and dealers.

Section 309 operates in the digital commodity market context -- the CFTC-regulated portion of the CLARITY Act that covers the 16 named digital commodities including Bitcoin, Ethereum, Solana, and XRP. It exempts participants in decentralized digital commodity networks from the dealer registration requirements that would otherwise apply to entities who regularly buy and sell digital commodities for their own account. A validator on the Ethereum network who processes transactions and receives transaction fees as compensation for that activity is, in a narrow technical sense, participating in transactions involving digital commodities. Without Section 309's exemption, the Gensler-era regulatory framework could theoretically have required such validators to register as commodity dealers with the CFTC.

Section 409 operates in the digital security context -- the SEC-regulated portion of the CLARITY Act that covers tokens that have not yet achieved sufficient decentralization to qualify as digital commodities. It creates parallel exemptions for interface providers, validators, and non-custodial infrastructure operators in the digital security market context. The combination of Sections 309 and 409 covers the full taxonomy of digital assets -- ensuring that infrastructure providers for both digital commodities and digital securities are protected from broker-dealer registration requirements based solely on their technical participation in blockchain network operations.

CCN's analysis confirmed that Sections 309 and 409 represent the first time US federal legislation has drawn a clear, codified line between regulated financial intermediaries and non-custodial, permissionless infrastructure. The exempted activities under Sections 309 and 409 include: relaying or validating transactions on distributed ledger networks, operating nodes, oracles, or bandwidth infrastructure, developing and publishing distributed ledger technology systems, creating or distributing self-custody tools like non-custodial wallets, and compiling network transactions or providing computational work as a network participant.

03 -- SECTION 604 AND TITLE VI: THE CRIMINAL LIABILITY PROTECTION

Section 604 of the CLARITY Act -- which folds in the Blockchain Regulatory Certainty Act -- is the provision that most directly addresses the Roman Storm prosecution theory. It creates a federal safe harbor from money-services-business registration under 31 U.S.C. Section 5330 and from criminal money-transmission prosecution under 18 U.S.C. Section 1960 -- the exact statute that convicted Roman Storm -- for non-controlling developers.

The Senate Banking Committee's version defines a non-controlling developer or provider as one who, in the regular course of operations, lacks the legal right or unilateral ability to control, initiate, or carry out transactions involving user assets without another party's approval. This definition is the critical boundary between protected and unprotected blockchain developers. A developer who writes open-source software that others use for financial transactions but who has no ability to unilaterally execute transactions involving user funds is a non-controlling developer protected by Section 604. A

developer who maintains admin keys that allow them to unilaterally upgrade a protocol in ways that affect user funds, or who maintains custody of user assets in any form, is not a non-controlling developer and does not receive Section 604's protection.

White House digital-assets adviser Patrick Witt described Section 1960 -- the criminal money-transmission statute that convicted Storm -- as the final hurdle for the CLARITY Act in early May 2026, predicting the bill would pass once the Section 1960 carveout for non-controlling developers was confirmed in the Senate floor vote language. Senate Judiciary Chairman Chuck Grassley and Senator Dick Durbin have objected to the Section 604 provision, arguing that the developer safe harbor could be used by bad actors to structure their activities to appear non-controlling while maintaining effective control through other means. The floor vote negotiation over the scope of Section 604 -- specifically how broadly or narrowly to define the non-controlling developer standard -- is the most legally consequential remaining legislative dispute in the CLARITY Act's path to passage.

Title VI of the CLARITY Act -- Protecting Software Developers and Software Innovation -- consolidates the developer protection provisions into a single statutory title that explicitly states software developers and network participants in DeFi are protected from federal and state securities laws for compiling network transactions, providing computational work, or other activities relating solely to software development. Title VI also creates an NFT safe harbor -- NFTs are exempt from securities laws unless they involve an investment contract -- and folds in both the Blockchain Regulatory Certainty Act and the Keep Your Coins Act into a unified developer and user rights framework.

> ***SECTION 604 DEFINITION: Non-controlling developer is one who lacks the legal right or unilateral ability to control, initiate, or carry out transactions involving user assets without another party's approval. If you write code and cannot unilaterally access user funds, you are protected from Section 1960 criminal prosecution. Roman Storm conviction specifically targeted by this carveout.***

04 -- THE 20 PERCENT DECENTRALIZATION THRESHOLD: WHO QUALIFIES AND WHO DOES NOT

The CLARITY Act's developer and validator protections are not available to all blockchain projects and protocols. They apply to genuinely decentralized networks and non-controlling developers. The bill's decentralization test -- which determines whether a network qualifies for the protections of Sections 309, 409, and 604 -- is the most technically specific provision in the entire legislation, and understanding it is essential for assessing which projects benefit from the developer protection framework and which do not.

The CLARITY Act supersedes the earlier FIT21 bill by tightening decentralization standards. A network or protocol satisfies the decentralization threshold when no single person or affiliated group controls more than 20% of the network's governance rights, token supply, or economic output. This 20% threshold is the bright line that distinguishes a genuinely decentralized network -- where the developer protections apply -- from a network with concentrated control -- where the developer protections do not apply and standard securities and financial services law requirements remain operative.

The practical effect of the 20% threshold is that protocols with large founder allocations, concentrated venture capital ownership, or foundation control over protocol governance may not qualify for the developer and validator protections at launch -- even if they are technically implemented as decentralized networks. This creates a specific compliance pathway for new blockchain projects: the graduation from concentrated control to decentralized governance over time, through token distribution, protocol upgrades that remove admin key capabilities, and governance transfer to token holders.

The CryptoTimes analysis identified the specific categories of losers under the Sections 309 and 409 framework: projects with concentrated governance that cannot clear the 20% control threshold, pseudo-DeFi platforms with custodial backstops -- protocols that present themselves as decentralized but maintain admin key control or custody user assets in any form -- and the Treasury enforcement wing that lost its push to restore DeFi sanctions authority. The clear losers from the decentralization threshold are projects that have been marketing themselves as DeFi while maintaining the control structures of centralized platforms.

05 -- WHY THIS BRINGS BLOCKCHAIN DEVELOPMENT BACK TO AMERICA

The immediate commercial implication of the CLARITY Act's developer and validator protection provisions is the return of blockchain development talent and capital to the United States -- a reversal of the offshore migration trend that the Roman Storm conviction and the Gensler-era regulatory enforcement approach had accelerated.

The geographic distribution of blockchain development talent is a direct function of legal risk. When writing financial software in the United States carried the risk of criminal prosecution under Section 1960, the rational response for developers building non-custodial financial protocols was to relocate to jurisdictions where that risk did not exist -- Switzerland, Singapore, the UK, the UAE, and other jurisdictions with clearer legal frameworks for non-custodial software development. The talent migration was documented in developer surveys, conference attendance patterns, and the geographic distribution of new protocol launches in 2024 and 2025.

Section 604's carveout for non-controlling developers from Section 1960 criminal liability removes the primary legal risk that drove the offshore migration. A developer in San Francisco who writes open-source DeFi protocol code, maintains no custody of user funds, and has no unilateral ability to execute user transactions will have statutory protection from criminal money-transmission prosecution once the CLARITY Act is signed. The risk profile of blockchain software development in the United States moves from criminally uncertain to statutorily protected -- a shift that is as significant for the US blockchain development ecosystem as the clarification of corporate liability rules was for the internet economy in the 1990s.

The DeFi Education Fund's statement that it was encouraged by the direction of negotiations and that core protections for developers and infrastructure providers remain in the bill -- despite the Grassley and Durbin objections to Section 1960 carveout scope -- reflects the crypto industry's assessment that the legislative outcome will be net positive for developers even if the final Section 604 language is narrower than the industry's preferred version. 1inch's chief legal officer calling the DeFi provisions very DeFi-friendly and a16z and the DeFi Education Fund describing Sections 309 and 409 as meaningful

wins are institutional-quality assessments from some of the most sophisticated legal and investment teams in the crypto industry.

The BlackRock BUIDL integration with Uniswap in Q1 2026 -- the first regulated tokenized fund deployed on a decentralized exchange -- is the most commercially significant data point demonstrating that institutional capital is already integrating with DeFi protocols in anticipation of the CLARITY Act's passage. When BlackRock, which manages $10 trillion in assets, integrates its tokenized Treasury fund with a DeFi protocol before the CLARITY Act is signed, it is expressing institutional confidence that the CLARITY Act's DeFi protections will provide the legal clarity needed for that integration to become mainstream after passage.

06 -- THE NODE OPERATOR AND VALIDATOR INVESTMENT THESIS

The CLARITY Act's validator and node operator protections have a specific investment implication that extends beyond the developer community to the institutional investors who are considering or already running validator operations on Proof-of-Stake blockchain networks.

Ethereum's Proof-of-Stake consensus mechanism requires validators to stake a minimum of 32 ETH as collateral and run validator software that proposes and attests to blocks on the Ethereum network. Validators earn staking rewards -- approximately 3% to 4% annually at current network participation rates -- in exchange for their validation services. Under the pre-CLARITY Act regulatory framework, the SEC had argued that Ethereum staking services could constitute investment contracts under the Howey test, creating regulatory uncertainty about whether running a validator or offering staking-as-a-service could trigger SEC broker-dealer registration requirements.

Sections 309 and 409 explicitly exempt validators from broker-dealer registration requirements based solely on their validation activity. The Section 601 safe harbor for blockchain developers confirms that operating nodes, oracles, or bandwidth infrastructure does not subject a participant to Exchange Act registration requirements. The combination of these provisions means that institutional investors, family offices, and corporate treasury operations that want to run Ethereum validators to earn staking yields can do so without the SEC broker-dealer registration compliance burden that the Gensler-era regulatory posture had suggested might be required.

The commercial scale of the institutional staking market that the CLARITY Act's validator protections unlock is significant. Ethereum's current staking participation rate means approximately $120 billion in ETH is currently staked. Institutional staking services -- Coinbase Prime, Lido, Rocket Pool, and the institutional staking infrastructure documented across the DeFi ecosystem -- generate annual revenue proportional to the staking rewards on the ETH they manage. When institutional investors with hundreds of billions in AUM can allocate to ETH validator operations with statutory protection from securities law registration requirements, the addressable market for institutional staking services expands dramatically.

07 -- CONCLUSION: THE CLARITY ACT IS THE MAGNA CARTA OF BLOCKCHAIN DEVELOPMENT

The CLARITY Act's developer and validator protection provisions -- Sections 309, 409, and 604, Title VI, and the self-custody protections of Section 605 documented in Report 1 of this series -- collectively represent the most comprehensive statutory protection framework for blockchain builders, validators, and users that any national government has ever enacted. The CCN analysis described the combined impact as the first time US federal legislation has drawn a clear, codified line between regulated financial intermediaries and non-custodial, permissionless infrastructure.

The Roman Storm conviction is the starkest illustration of what the pre-CLARITY Act regulatory environment meant for blockchain developers in the United States: a developer who wrote open-source software and never held user funds was convicted of a federal crime. If that legal environment had persisted, the logical conclusion was the complete migration of blockchain development talent and capital from the United States to jurisdictions with clearer legal frameworks. The CLARITY Act's Section 604 carveout for non-controlling developers from Section 1960 criminal prosecution is the statutory answer to the Roman Storm precedent.

For investors in blockchain infrastructure -- Ethereum, Solana, Chainlink, and the DeFi protocols that run on public blockchain networks -- the CLARITY Act's developer and validator protections are the legislative foundation that makes long-term institutional investment in these networks viable. The legal uncertainty that has been a persistent risk factor in institutional DeFi allocation decisions is resolved by statute. The developer talent that has been migrating offshore returns when the legal risk is removed. The institutional capital that has been waiting for regulatory clarity allocates when the statutory framework is in place. The CLARITY Act is a market structure bill. But its developer provisions are the Magna Carta of blockchain development -- the first codified declaration that building on blockchain is a legally protected activity in America.

> ***Sections 309 and 409 exempt validators, node operators, and open-source developers from broker-dealer registration. Section 604 carves non-controlling developers out of Section 1960 criminal money-transmission prosecution -- the statute that convicted Roman Storm. Title VI makes it explicit: if you build software and never touch anyone's money, you are not a bank. The first time US law said this.***