The Legalities of New Money

Regulating Blockchain, DeFi, and Buy Now, Pay Later

Ivan

September 2026

[Influenced by Claude, Fable 5.1]

Table of Contents

I. Introduction..... 3
II. Blockchain and Cryptoassets: What the Law Is Actually Looking At..... 4
III. Who Regulates a Token? The Jurisdictional Divide..... 5
IV. Stablecoins: Where Crypto Meets the Banking System..... 7
V. Decentralized Finance: Regulating Code Without a Company..... 9
VI. Case Studies in Crypto Failure..... 11
VII. Buy Now, Pay Later: Old Credit in New Packaging..... 13
VIII. The Regulatory Catch-Up: BNPL Around the World..... 14
IX. The Common Thread: Regulatory Arbitrage as a Business Model..... 16
X. Consumer Protection at the Margins..... 17
XI. Systemic Risk: When Fintech Meets Macroprudential Policy..... 18
XII. Toward Coherent Regulation..... 19
XIII. Conclusion..... 20
Bibliography..... 21

I. Introduction

In the space of fifteen years, three separate innovations have each tried to answer the same question from a different direction: what counts as money, who gets to move it, and who is responsible when it disappears. Blockchain networks proposed that value could be recorded and transferred without a bank in the middle. Decentralized finance (DeFi) proposed that lending, trading, and insurance could run on that same infrastructure without a company in the middle either. And buy now, pay later (BNPL) proposed something quieter but just as disruptive: that consumer credit could be issued at the point of sale, instantly, without looking much like a loan at all. None of these three began as a legal category. Regulators built the rules for banks, broker-dealers, and credit card issuers long before any of them existed, and each has spent the years since trying to fit itself into, or slip around, a rulebook that was never written with it in mind.

This essay treats those three innovations as a single legal problem rather than three unrelated ones, because the pattern connecting them is the same in each case: a product grows quickly by occupying a gap between existing categories, causes visible harm once it reaches enough people, and forces regulators to decide, after the fact, which of the old rules should apply, whether new rules are needed, or whether the activity should simply be left alone. Cryptoassets spent a decade being alternately ignored, litigated against, and finally, as of 2026, subjected to the first genuinely comprehensive rulebooks on both sides of the Atlantic. Decentralized finance is still mostly unregulated in any direct sense, precisely because it was built to remove the kind of intermediary that regulation usually targets. Buy now, pay later has followed almost the opposite path: a familiar product, consumer credit, wrapped in unfamiliar packaging that let it avoid consumer credit law for the better part of a decade, before the United Kingdom, Australia, and the European Union each closed that gap within roughly eighteen months of one another.

What follows is organized in three movements. The first examines cryptoassets and stablecoins, tracing how the United States, the European Union, and the United Kingdom have each drawn the line between a security, a commodity, and something else entirely, and what happened when several of the largest platforms in the space collapsed anyway. The second turns to decentralized finance specifically, where the legal difficulty is not classification but the absence of a defendant. The third turns to buy now, pay later, a product that looks nothing like crypto on the surface but raises the identical legal question underneath: when a service performs the economic function of credit, should it be regulated as credit, regardless of what its terms of service call it. A closing section draws the three threads together around a single organizing idea, sometimes called functional regulation, that has quietly become the dominant approach across every jurisdiction discussed here.

A note on scope. This is a general educational overview, not legal advice, and international and comparative financial regulation is a fast-moving and genuinely unsettled field: several of

the frameworks described below, including the FCA's regulation of buy now, pay later and the European Union's second Consumer Credit Directive, take effect only in the second half of 2026, and their practical operation will not be clear for some time after that. Figures on market size, adoption, and enforcement outcomes are current as of September 2026 and are cited to their sources throughout.

II. Blockchain and Cryptoassets: What the Law Is Actually Looking At

A. Blockchain as Infrastructure, Not Asset

It is worth separating, at the outset, two things that public discussion routinely collapses into one: blockchain the technology, and cryptoassets the financial products built on top of it. A blockchain is a distributed ledger, a way of recording transactions across many computers so that no single party controls or can quietly rewrite the record. That is an infrastructure choice, comparable in kind (though not in effect) to choosing a database architecture. It is not, by itself, a financial instrument, and it is not what regulators regulate. What regulators regulate are the assets, contracts, and services built on top of that infrastructure: a token that represents a claim on a company's future profits, a stablecoin that promises to be redeemable for a dollar, a lending pool that pays interest to depositors. The legal questions in this essay are almost entirely about those layers, not about the ledger technology underneath them, which is itself legally unremarkable.

That distinction matters because it explains why blockchain-based systems have proven so difficult to regulate coherently. A single piece of infrastructure can host a payment network, a securities exchange, a lending market, and a casino, sometimes within the same protocol, and regulators organized around institutional categories, a banking regulator, a securities regulator, a consumer credit regulator, each see only the slice that falls within their own jurisdiction. The result, for most of the technology's first decade, was not so much bad regulation as an absence of any regulation that treated the whole picture as one system.

B. A Taxonomy of Cryptoassets

Most regulatory frameworks now sort cryptoassets into a small number of functional categories, even though the underlying technology does not enforce any such distinction. Payment tokens are designed primarily to be used or held as a medium of exchange or store of value, the category Bitcoin is generally placed in. Utility tokens grant access to a specific product or service on a platform, functioning more like a prepaid voucher than an investment, at least in their idealized form. Security tokens represent a claim on the profits, assets, or governance of an enterprise and are treated, functionally, the same way a share of stock or a bond would be treated. Stablecoins, a fourth and increasingly important category, are designed to hold a stable value by reference to a fiat currency or basket of assets, and occupy a distinct regulatory lane of their own, discussed in Part IV below.

This taxonomy sounds tidy in the abstract and is frequently not tidy in practice. A token can be marketed as a utility token, function economically as a security during its initial sale, and trade on secondary markets as something closer to a payment token, all within the life of a single project. The next section examines how the two principal American regulators, and their European and British counterparts, have tried to draw usable lines through that ambiguity.

III. Who Regulates a Token? The Jurisdictional Divide

A. The United States: Securities, Commodities, and the Howey Test

American financial regulation is organized around a jurisdictional split that predates cryptoassets by decades: the Securities and Exchange Commission (SEC) regulates securities, the Commodity Futures Trading Commission (CFTC) regulates commodities and their derivatives, and for most of crypto's history neither agency had clear, uncontested authority over the assets themselves. Whether a given token is a security turns, under long-standing case law, on the Howey test, which asks whether an arrangement involves an investment of money in a common enterprise with an expectation of profit derived from the efforts of others. Tokens sold to fund a company's development, with the expectation that the company's efforts would make the token valuable, have generally been treated as securities at the point of that initial sale. Tokens that, once a network is sufficiently decentralized, no longer depend on any single promoter's efforts have a stronger claim to falling outside that definition, though exactly when a network crosses that threshold has never been reduced to a bright-line rule.

For most of the 2010s and early 2020s, this ambiguity was resolved mainly through enforcement actions rather than rulemaking, which left the industry litigating its legal status case by case, against a backdrop of genuine disagreement between the SEC and CFTC about which of them had jurisdiction over which tokens. That period effectively ended in 2026.

B. The 2026 SEC-CFTC Joint Interpretation

In March 2026, the SEC and CFTC issued a joint interpretive release setting out, for the first time, a shared analytical framework for classifying digital assets as securities, commodities, or neither. The release did not abandon Howey, but it applied it with more precision to the lifecycle of a token: an asset sold as part of an investment contract can be a security at issuance while the asset itself, once a network is functionally decentralized and no longer dependent on a central promoter, is not necessarily a security in secondary trading. That distinction between the transaction and the asset had been argued by industry participants for years and had occasionally been accepted by individual courts, but the joint release was the first time both agencies endorsed it in a single, coordinated document rather than through separate and sometimes conflicting enforcement positions.

The practical effect has been to give exchanges and custodians a clearer basis for deciding which tokens can be listed and traded under commodities-style rules, administered by the CFTC, and which remain subject to full securities regulation by the SEC. It has not eliminated the line-drawing problem, since a newly launched token still has to be assessed for how decentralized its governance and development actually are, a factual question rather than a formal one, but it replaced years of case-by-case litigation with a standing interpretive framework that market participants can apply prospectively. Congress has separately been considering more permanent market-structure legislation that would codify a version of this split into statute, which would settle the question more durably than an interpretive release, which either agency could in principle revise.

C. The European Union: MiCA's Comprehensive Framework

The European Union took a different approach from the outset: rather than fitting cryptoassets into pre-existing securities and banking law, it wrote a dedicated statute, the Markets in Crypto-Assets Regulation (MiCA), covering the asset classes crypto law in the United States has spent years litigating one at a time. MiCA applies across all twenty-seven member states directly, without needing separate national implementing legislation for most of its provisions, and it creates a single licensing category, the Crypto-Asset Service Provider (CASP), that covers exchanges, custodians, and trading platforms. A CASP authorized in one member state can passport that authorization across the entire bloc, which was intended to prevent the kind of fragmented, country-by-country licensing regime that has slowed institutional adoption elsewhere.

CASP authorization is not a light-touch registration. Firms must meet minimum capital requirements (roughly €125,000 for the base license tier), maintain anti-money-laundering and counter-terrorist-financing controls, safeguard client assets in segregated custody, comply with cybersecurity standards under the EU's Digital Operational Resilience Act, and operate systems to detect and prevent market abuse, including insider dealing and market manipulation applied, for the first time, to crypto markets specifically rather than borrowed awkwardly from securities law. MiCA also directly addresses stablecoins through two dedicated categories, discussed in Part IV, which is arguably the area where its practical bite has been felt earliest and hardest.

D. The United Kingdom's Phased Approach

The UK, having left the EU before MiCA was finalized, opted for its own framework rather than mirroring it, administered by the Financial Conduct Authority (FCA) through a phased rollout rather than a single statute taking effect all at once. Stablecoins and custody arrangements were prioritized in the FCA's early phases, on the view that these pose the most direct risk to ordinary consumers and to the stability of the payments system, with broader trading and lending activities brought into scope in later phases. The practical result, as of 2026, is that a

firm operating across the UK and the EU faces two licensing regimes built on similar principles, protecting consumers, preventing market abuse, requiring capital and custody safeguards, but with different registration processes, different timelines, and different specific obligations, adding a compliance cost that a single, larger jurisdiction would not impose on its own.

IV. Stablecoins: Where Crypto Meets the Banking System

A. Asset-Referenced Tokens and E-Money Tokens Under MiCA

MiCA treats stablecoins as a fundamentally different risk category from other cryptoassets, and splits them into two types. An asset-referenced token (ART) maintains its value by reference to a basket of assets, which might include multiple currencies, commodities, or other cryptoassets. An e-money token (EMT) is simpler and more tightly regulated: it references a single fiat currency, typically the euro or the dollar, and is meant to function as a direct digital substitute for that currency. Both categories require reserves equal to at least one hundred percent of the tokens in circulation, regular independent audits, and public transparency reporting, and EMT issuers additionally need authorization as an electronic money institution under the EU's separate Payment Services Directive, layering two licensing regimes on top of one another for what looks, to an end user, like a single product.

The uptake has been lopsided in a way that is itself informative about where the real regulatory friction lies. By March 2026, nineteen issuers across eleven EU member states had been authorized to issue twenty-nine separate e-money tokens, seventeen referencing the euro and nine referencing the dollar, with France alone accounting for roughly a quarter of all authorized issuers. Asset-referenced tokens, by contrast, had produced zero authorizations by the same date, nearly two years into MiCA's implementation, suggesting that the more open-ended, multi-asset ART structure is either commercially less attractive or operationally harder to get licensed than the simpler, single-currency EMT model. Perhaps more strikingly, among the fifty largest stablecoins by market capitalization globally, only three were MiCA-compliant as of early 2026. Tether, the largest stablecoin issuer in the world by a wide margin, had not obtained MiCA authorization, which as a practical matter restricts its use by regulated EU financial institutions even though it continues to trade freely on many exchanges accessible to EU residents.

B. The GENIUS Act: America's Federal Stablecoin Regime

The United States addressed stablecoins through dedicated federal legislation, the GENIUS Act, signed into law on 18 July 2025. Unlike MiCA, which folds stablecoins into a broader cryptoasset statute, the GENIUS Act is a stand-alone stablecoin law, and it takes a more restrictive approach to who may issue one at all: only federally or state-approved entities may issue a payment stablecoin, a category that includes subsidiaries of insured depository

institutions, nonbanks supervised by the Office of the Comptroller of the Currency, and state-chartered entities meeting standards the statute deems equivalent to the federal ones. Ordinary non-financial public companies are generally barred from issuing stablecoins directly unless they obtain unanimous approval from a newly created Stablecoin Certification Review Committee, chaired by the Treasury Secretary and including the heads of the Federal Reserve and the FDIC, a deliberately high bar aimed at preventing large technology or retail companies from issuing their own private currencies without close supervision.

Substantively, the reserve requirements mirror the strictest end of the international spectrum: issuers must back outstanding stablecoins one-to-one with cash, US Treasury securities, or equivalent short-term instruments, held in segregated accounts that cannot be rehypothecated or lent out, and must certify reserve adequacy on a monthly basis in addition to whatever capital and liquidity standards their federal or state supervisor separately imposes. States retain a limited regulatory role: an issuer with under ten billion dollars in outstanding stablecoins may be supervised at the state level instead of federally, but only if that state's regulatory framework has been certified by the review committee as substantially similar to the federal standard, which in practice pulls state regimes toward convergence with the federal one rather than allowing meaningful divergence. The statute takes full effect at the earlier of eighteen months after enactment or one hundred twenty days after final implementing regulations are issued, meaning the regime was still being phased in through 2026 and 2027 even though the underlying law had already passed.

C. The Compliance Gap: Why Most Stablecoins Are Not Actually Compliant

Read together, MiCA and the GENIUS Act point toward the same underlying judgment: a stablecoin is, functionally, a payment instrument and a form of narrow banking, and should be regulated with something close to banking-grade reserve and disclosure requirements rather than left to the lighter-touch rules applied to other cryptoassets. What the MiCA authorization numbers make visible, though, is the gap between that regulatory ambition and where the market actually sits. The largest stablecoin by circulation in the world remains outside the EU's compliant perimeter, and a comparable compliance gap exists in the United States, where issuers have until the GENIUS Act's full phase-in to restructure, obtain federal or certified state approval, and bring existing reserve practices up to the new statutory standard. For a category of asset whose entire value proposition rests on the promise of being redeemable at par, the persistence of large, non-compliant issuers operating alongside a newly built compliant perimeter is the single clearest sign that stablecoin regulation, as of 2026, is still in its early implementation phase rather than its steady state.

V. Decentralized Finance: Regulating Code Without a Company

A. What DeFi Automates, and What It Doesn't

Decentralized finance refers to financial services, lending, borrowing, trading, and increasingly insurance and derivatives, built as self-executing software (smart contracts) running on a blockchain rather than operated by a licensed intermediary. A DeFi lending protocol like Aave, currently the second-largest by assets locked, does not employ loan officers or maintain a balance sheet in the way a bank does; instead, it runs code that accepts deposits into a shared pool, sets interest rates algorithmically based on supply and demand within that pool, and allows borrowers to draw against collateral they lock into the same protocol, all without any human counterparty approving individual transactions. As of mid-2026, roughly seventy-two billion dollars was locked across DeFi protocols globally, concentrated overwhelmingly on the Ethereum network, which alone accounts for just over half of all value locked in the sector, with Aave and the liquid-staking protocol Lido together representing a substantial share of that total. That figure had fallen sharply over the preceding year, down more than a third from where it started 2026, a decline that tracks the broader contraction in cryptoasset valuations over the same period rather than any single regulatory event.

What DeFi automates, in other words, is the operational middle of a financial transaction: matching, pricing, and settlement. What it generally does not automate, and cannot automate through code alone, is the underlying legal relationship: whose money is actually at risk if the protocol is exploited, who bears the loss if a smart contract has a bug, and who, if anyone, is accountable to a regulator or a court when something goes wrong. That gap between what the software does and what the law needs to know is the central legal problem DeFi presents, and it is different in kind from the classification problem discussed in Part III.

B. Smart Contracts as (Almost) Legal Instruments

A smart contract is code that executes automatically once its programmed conditions are met, and the early cypherpunk slogan for this idea, "code is law," captured a genuine appeal: an agreement that enforces itself removes the need to trust a counterparty, or a court, to honor its terms. In practice, courts and regulators have been unwilling to treat smart contract code as a complete substitute for a legal contract, for reasons that go beyond mere institutional conservatism. Code can only execute the logic it was written with; it cannot interpret ambiguous intent, cannot account for fraud or duress in how a party was induced to interact with it, and cannot adapt to circumstances its authors failed to anticipate, all things ordinary contract law does routinely. When a smart contract's code contains a bug that lets an attacker drain a lending pool, the code has, in one sense, executed exactly as written, and in another sense has produced an outcome no reasonable party could have intended, a tension that

traditional contract doctrine, built around the parties' actual intent rather than the literal text alone, is generally better equipped to resolve than the code itself.

The more workable position, and the one most regulators and scholars have converged on, treats smart contracts as an enforcement mechanism layered on top of an underlying legal agreement rather than as a replacement for one. The code executes the routine, undisputed cases automatically, while genuinely contested questions, was there fraud, was the protocol's governance process itself compromised, who is liable for a bug, still get resolved through ordinary legal process, when a court or regulator can identify a party to resolve them against.

C. The Missing Defendant Problem

This is where DeFi's regulatory difficulty becomes distinct from anything discussed so far in this essay. Securities regulation, banking regulation, and consumer credit regulation are all built around the assumption that there is an identifiable regulated entity, a company, a bank, a licensed lender, that can be required to register, file disclosures, maintain capital, and answer to a supervisor or a court. A sufficiently decentralized DeFi protocol may have no such entity at all: its code may be immutable or governed by a decentralized autonomous organization (DAO) whose token holders are anonymous and dispersed across dozens of jurisdictions, with no office, no employees in the traditional sense, and no single party who can meaningfully be said to control it once it is deployed.

Regulators have responded in three overlapping ways. The first targets the people who write and deploy the code, on the theory that even a decentralized protocol had human developers who can be identified and held responsible for the system they built, an approach that raises its own fairness questions when a developer has genuinely relinquished control. The second targets the points where DeFi touches the regulated financial system, the fiat on-ramps and off-ramps, the centralized exchanges that list DeFi tokens, on the theory that a chokepoint regulator can control does not need to reach the unreachable protocol directly to meaningfully constrain how much economic activity flows into it. The third, reflected in the Congressional Research Service's 2026 overview of the sector, is simply to acknowledge that a meaningful share of DeFi activity currently falls into a genuine regulatory gap, neither clearly permitted nor clearly prohibited under existing statute, and to treat that gap as an open policy question for legislators rather than something existing agencies can resolve through interpretation alone.

VI. Case Studies in Crypto Failure

Abstract regulatory frameworks are easiest to evaluate against concrete failures, and the three collapses below, each among the largest in the industry's history, illustrate three different legal problems: an algorithmic stablecoin that could not maintain its peg, a centralized exchange that commingled customer funds with its own trading arm, and a lending platform that promised bank-like yields without bank-like capital.

A. Terra/Luna: An Algorithmic Stablecoin's Death Spiral

TerraUSD (UST) was an algorithmic stablecoin, meaning it maintained its dollar peg not through a reserve of actual dollars but through a coded arbitrage mechanism tied to a second, freely traded token, Luna. In May 2022, that mechanism failed under stress: as holders began redeeming UST for Luna faster than the protocol could absorb, the arbitrage loop that was supposed to restore the peg instead accelerated its collapse, wiping out approximately fifty billion dollars in combined value across the Terra ecosystem over the course of about three days. The collapse is now generally treated as the clearest cautionary case for why regulators, in both the MiCA and GENIUS Act frameworks discussed above, insist on full reserve backing with real assets rather than allowing an algorithmic peg to substitute for one; UST's failure mode, a self-reinforcing spiral once confidence broke, is structurally very close to a traditional bank run, except that it happened in a system with no deposit insurance, no lender of last resort, and no circuit breaker.

Terraform Labs' founder, Do Kwon, fled after the collapse, traveling on false passports through Serbia before being apprehended in Montenegro, where he spent roughly seventeen months in custody before being extradited to the United States in January 2026. He pleaded guilty in August 2025 to one count of conspiracy to commit commodities, securities, and wire fraud and one count of wire fraud, and was sentenced on 11 December 2025 to fifteen years in prison, with a requirement to serve at least half that term before becoming eligible for transfer to South Korea. At sentencing, the presiding judge described Kwon's conduct as a knowing scheme to defraud UST purchasers, pointing in particular to evidence that Kwon had publicly urged retail investors to hold their positions through the collapse while privately moving to exit his own.

B. FTX: Custody, Commingling, and the Limits of "Crypto-Native" Trust

FTX, once the third-largest cryptocurrency exchange in the world, collapsed in November 2022 after reporting revealed that customer deposits held on the exchange had been transferred to and used by Alameda Research, a trading firm under common ownership with FTX, to cover Alameda's own losses and fund a range of other expenditures, in direct contradiction to FTX's public representations that customer assets were held separately and were not being used for proprietary trading. The core legal failure was not novel or crypto-specific: commingling customer funds with a firm's own assets is precisely what custody and segregation rules in traditional finance, and the equivalent custody provisions now built into MiCA's CASP licensing regime, are designed to prevent. What made FTX distinctive was scale and the extent of the fraud, not the underlying legal category of the wrongdoing.

Sam Bankman-Fried was convicted in November 2023 on seven counts of fraud, conspiracy, and money laundering, and was sentenced to twenty-five years in prison along with a forfeiture order of eleven billion dollars. As of September 2026, he was pursuing a petition for

the Supreme Court to review his conviction, arguing principally that he was improperly prevented at trial from presenting evidence that FTX and Alameda, while temporarily illiquid at the time of the collapse, held assets sufficient to eventually make customers and investors whole, and separately arguing that the eleven-billion-dollar forfeiture order violates the Eighth Amendment's prohibition on excessive fines. The petition also directly challenges a 2025 Supreme Court precedent, Kousisis v. United States, which held that a fraud conviction does not require the prosecution to prove the victims suffered net economic harm, a doctrinal question with implications well beyond crypto cases. Whatever the Supreme Court ultimately decides, the underlying regulatory lesson, that a firm calling itself an exchange must actually segregate customer assets rather than merely promise to, has already been substantially codified into the custody requirements of both MiCA and comparable American proposals.

C. Celsius Network: Yield Without a Balance Sheet

Celsius Network marketed itself as a crypto lending and yield platform, accepting customer deposits and promising returns often well above what any bank offered, funded by lending those deposits out and by proprietary trading and staking activity that customers had limited visibility into. When crypto markets fell sharply in 2022, Celsius froze customer withdrawals and filed for bankruptcy, in a case that ultimately concluded with findings that the firm had operated, in substance, an unsecured and inadequately capitalized lending business dressed in the language of a savings product, resulting in losses to customers estimated at roughly 4.7 billion dollars. Celsius founder Alex Mashinsky was sentenced in May 2025 to twelve years in prison for fraud, a sentence prosecutors and the court both framed around the gap between what Celsius told depositors about the safety and liquidity of their funds and what the firm's actual balance sheet and risk exposure looked like at the time.

The three collapses in this section, taken together, do not really describe three different kinds of fraud so much as one recurring pattern applied to three different products: a promise of stability or yield that depended on conditions the promoter did not disclose, control over customer assets, and a failure that became visible only once external market stress removed the slack that had been concealing the underlying insolvency. It is worth noting how much of that pattern, custody without segregation, yield without adequate capital, opacity about what backs a promised peg, maps directly onto the specific requirements MiCA and the GENIUS Act now impose. These statutes were, in a real sense, written in response to exactly these failures.

VII. Buy Now, Pay Later: Old Credit in New Packaging

A. How BNPL Products Work

Buy now, pay later products let a consumer split the cost of a purchase, typically made online at the point of checkout, into a small number of installments, most commonly four payments spread over six weeks, with the first payment due immediately and no interest charged if all

payments are made on time. The provider (Klarna, Affirm, Afterpay, and PayPal's own BNPL product are the largest in most Western markets) pays the merchant close to the full purchase price up front, taking on the credit risk of the buyer itself and earning revenue primarily from merchant fees rather than from interest charged to the consumer, at least for the standard short-term, no-interest product; longer-term BNPL installment loans, increasingly offered by the same providers, do carry interest and function much closer to a traditional installment loan.

The application process is deliberately minimal by design: rather than the multi-day underwriting process associated with a credit card application, most BNPL providers perform a rapid, often automated affordability check at checkout and can approve a purchase in seconds, a design choice core to the product's appeal and, as later sections discuss, core to the regulatory concern about it as well.

B. Why It Grew So Fast

BNPL's growth over the past several years has been rapid by almost any measure. Global gross merchandise volume transacted through BNPL reached approximately 560 billion dollars in 2025, and in the United States alone total BNPL issuance reached 156.7 billion dollars the same year, split across Afterpay (roughly 34 percent of US volume), Affirm (26 percent), PayPal's BNPL product (17 percent), and Klarna (15 percent). Globally, an estimated 380 million consumers used a BNPL product in 2024, a figure projected to approach 670 million by 2028, with US usage alone expected to reach roughly 96 million people in 2026.

Several forces explain that growth. E-commerce checkout friction is a well-documented driver of abandoned purchases, and BNPL reduces that friction more effectively than a traditional credit application. Many BNPL users, particularly younger consumers, report using it specifically because they are wary of or have limited access to traditional credit cards, whether from limited credit history, general debt aversion, or the psychological framing of BNPL as "not really debt" given that the standard product carries no interest. That last point of framing, that a BNPL installment plan does not feel like borrowing even though it functionally is borrowing, is precisely what allowed the product to grow for years largely outside the reach of consumer credit regulation, and it is the thread connecting BNPL back to the classification problem this essay opened with in the cryptoasset context: a product's legal treatment has tended to follow its label rather than its economic substance, until regulators specifically intervened to correct that gap.

VIII. The Regulatory Catch-Up: BNPL Around the World

A. United Kingdom: The FCA's July 2026 Regime

The UK moved first among major jurisdictions to bring BNPL, formally termed deferred payment credit, fully within the Financial Conduct Authority's regulatory perimeter, following

legislation passed in 2025 with a one-year transition period ending on the regime's effective date of 15 July 2026. From that date, lenders must conduct a creditworthiness assessment before every transaction, regardless of amount, including purchases as small as fifty pounds, considering both the risk that a loan will not be affordable and the risk that the customer cannot realistically repay it, and taking into account existing indicators of financial difficulty or vulnerability rather than assessing each purchase in isolation. Key product information, the applicable rate structure, repayment schedule, and complaint rights, must be presented clearly and immediately at the point of sale, without requiring the customer to click through additional screens to find it, and customers must be given a durable copy of the completed agreement.

The regime also imposes specific obligations once a payment is missed: firms must contact the customer promptly, provide clear and tailored communication including signposting to free debt advice, and give reasonable notice before pursuing enforcement action, obligations that mirror, deliberately, the protections that have applied to mainstream consumer credit for years. Existing BNPL providers were given a temporary permissions regime allowing a further six months from the July 2026 start date to obtain full FCA authorization, a transitional accommodation intended to prevent an abrupt market disruption while still bringing the sector definitively inside the regulatory perimeter.

B. United States: A Federal Vacuum After the CFPB's Retreat

The United States has moved in the opposite direction. In May 2024, the Consumer Financial Protection Bureau (CFPB) issued an interpretive rule treating certain BNPL products as functionally equivalent to credit cards, which would have required BNPL lenders to comply with Regulation Z disclosure and dispute-resolution obligations that apply to credit card issuers. That rule faced an immediate legal challenge from the industry, and the CFPB's posture shifted sharply following a change in the Bureau's leadership: by May 2025 the agency announced it would not prioritize enforcement of the interpretive rule while it considered rescinding it outright, and by June 2025 it confirmed that it would not reissue the rule at all, concluding that credit-card-style requirements were, in the Bureau's own words, ill-suited for BNPL products, which it characterized as short-term, closed-end installment products typically carrying no finance charge, rather than the revolving, open-end credit that Regulation Z's card provisions were designed around.

The practical result, as of 2026, is that BNPL providers in the United States operate under no dedicated federal regulatory regime specific to the product, though general consumer protection statutes, state lending laws, and (for the minority of BNPL products structured as interest-bearing installment loans rather than the standard no-interest, four-payment product) existing installment lending regulation continue to apply in the background. Individual states, New York prominent among them, have moved to fill part of that gap with their own BNPL-specific statutes, producing a patchwork rather than a uniform national

standard, a pattern that echoes, in miniature, the fragmented state-by-state cryptoasset regulation that existed in the US before the 2026 SEC-CFTC interpretation discussed in Part III.

C. Australia: Licensing Under the National Credit Code

Australia closed its own BNPL gap through the Treasury Laws Amendment (Responsible Buy Now Pay Later and Other Measures) Act 2024, which extended the National Credit Code, Australia's core consumer lending statute, to cover BNPL contracts directly. From 10 June 2025, any entity carrying on BNPL credit activities has been required to hold an Australian credit licence with the appropriate authorizations, and to become a member of the Australian Financial Complaints Authority, giving BNPL customers access to the same external dispute-resolution body available to customers of banks and traditional lenders. For contracts that qualify as "low cost credit contracts", broadly, the smaller, shorter-term products that dominate the standard BNPL model, providers may apply a modified, proportionate version of the responsible lending obligations that otherwise apply under the Code, an attempt to preserve BNPL's low-friction checkout experience while still requiring some baseline affordability check, rather than importing the full, more elaborate responsible lending assessment used for larger and longer-term consumer loans.

D. European Union: CCD2's November 2026 Deadline

The European Union's approach runs through its second Consumer Credit Directive (CCD2), which expressly brings BNPL products within the scope of EU consumer credit law for the first time, alongside other credit products the original 2008 directive did not anticipate. Member states were required to transpose CCD2 into national law by 20 November 2025, with the directive's substantive obligations applying from 20 November 2026, giving a full year between transposition and application, though reporting through 2026 suggested a number of member states were behind schedule on meeting even the earlier transposition deadline. Once fully in force, CCD2 will require BNPL lenders operating in the EU to conduct creditworthiness assessments, provide standardized pre-contractual information, and comply with the directive's advertising and early-repayment provisions, bringing the EU into broad substantive alignment with the UK's FCA regime and Australia's amended National Credit Code, even though each jurisdiction reached that alignment through a differently structured piece of legislation and on its own separate timeline.

IX. The Common Thread: Regulatory Arbitrage as a Business Model

A. "Not a Security," "Not a Loan": The Categorization Game

Reading Parts III through VIII together, a single pattern recurs across cryptoassets, stablecoins, DeFi, and BNPL alike: each grew fastest in the years when its own promoters could plausibly argue it fell outside an existing regulatory category, a token that was "not a security," a

lending pool that was "not a bank," an installment plan that was "not a loan." That argument was not always made in bad faith; in each case there were genuine, non-trivial legal questions about whether the old categories actually fit the new product. But in each case, the period of genuine ambiguity was also a period of rapid, largely unsupervised growth, and in each case, the eventual regulatory response arrived only after that ambiguity had already produced visible consumer or systemic harm, whether the Terra/Luna and FTX collapses in crypto, or the debt-stacking concerns discussed in Part X below for BNPL.

This is not, on its own, evidence that regulators moved too slowly, and it would be equally wrong to read it as evidence that faster regulation would necessarily have been better regulation; premature rules written before a technology's actual risks are understood can just as easily entrench the wrong protections or foreclose beneficial innovation. What the pattern does show, fairly clearly, is that the gap between a product's legal label and its economic function is where regulatory arbitrage consistently concentrates, and that closing that gap has, across every jurisdiction and every product examined in this essay, eventually required regulators to look past the label to the function underneath it.

B. Same Risk, Same Rules: The Functional Regulation Principle

The organizing principle that has emerged from this pattern, across securities regulators, banking regulators, and consumer credit regulators alike, is sometimes summarized as "same activity, same risk, same rules": if a product performs the economic function of a security, it should face securities-style disclosure obligations, whatever it is called; if it performs the function of a bank deposit or a stablecoin promising redemption at par, it should face reserve and custody requirements resembling banking regulation; if it performs the function of consumer credit, it should face consumer credit protections, regardless of whether its provider prefers to describe itself as a payments company rather than a lender. Every major framework surveyed in this essay, MiCA's asset taxonomy, the GENIUS Act's stablecoin reserve rules, the SEC-CFTC joint interpretation's transaction-versus-asset distinction, and the UK, Australian, and EU BNPL regimes, is, at bottom, an application of that same functional principle to a different product.

The principle is easier to state than to apply consistently, and its application has generally lagged well behind the growth of the product it is meant to govern, sometimes by the better part of a decade, as the BNPL and early cryptoasset examples in this essay both illustrate. But as a description of where financial regulation across every jurisdiction discussed here has actually converged by 2026, it is a more accurate account than any framework organized around fixed institutional categories, bank, broker-dealer, payments company, that assumes new financial products will continue to sort themselves neatly into the boxes regulators built for an earlier generation of institutions.

X. Consumer Protection at the Margins

A. Phantom Debt and the BNPL Stacking Problem

The single most consistent concern raised about BNPL, across every jurisdiction discussed in Part VIII, is what regulators have taken to calling phantom debt: because most BNPL loans have historically not been reported to mainstream credit bureaus, a lender assessing a consumer's overall debt burden for a mortgage, car loan, or credit card application typically cannot see how many BNPL obligations that consumer is currently carrying. The scale of the underlying behavior is significant enough to make that invisibility a real prudential concern rather than a hypothetical one: available data suggests that around 63 percent of BNPL users hold multiple BNPL loans simultaneously, with roughly a third of users spreading those loans across more than one provider, a pattern of "loan stacking" that is difficult for any single lender to detect precisely because no individual provider can see what a consumer owes to its competitors. Default rates on individual BNPL loans remain relatively low, around 1.8 to 2 percent, but the share of users who report making at least one late payment is far higher, somewhere between 34 and 41 percent, suggesting that BNPL debt, even where it does not default outright, is a meaningfully more frequent source of short-term financial strain than the low headline default rate alone would suggest.

The FCA's rule requiring an affordability assessment on every transaction, the EU's CCD2 creditworthiness obligations, and Australia's extension of responsible lending duties to BNPL are all, in substance, direct responses to this phantom debt problem, and each depends for its effectiveness on lenders being able to see a fuller picture of a consumer's existing obligations, which in turn depends on BNPL data eventually being integrated into mainstream credit reporting in each jurisdiction, a process that, as of 2026, remains a work in progress everywhere it has been attempted.

B. DeFi's Irreversibility: No Chargebacks, No Ombudsman

Decentralized finance presents a different, in some ways more fundamental, version of the consumer protection problem. Traditional financial systems build in multiple layers of after-the-fact recourse: a credit card chargeback, a bank's fraud reversal process, a financial ombudsman scheme, a regulator with the power to order restitution. Blockchain transactions, by design, are irreversible once confirmed, and a genuinely decentralized protocol may have no operator empowered to freeze funds, reverse a transaction, or even respond to a complaint, however clearly a user was defrauded or however obvious a smart contract bug turns out to have been. A consumer who sends funds to a fraudulent DeFi protocol, or who loses assets to a smart contract exploit, frequently has no equivalent of the UK's Financial Ombudsman Service or the US CFPB's complaint process to turn to, because there is, in the strict sense, no regulated financial services provider on the other side of the transaction at all.

This is the most direct consumer-facing consequence of the missing defendant problem discussed in Part V.C, and it is also the area where the gap between traditional consumer protection law and decentralized financial infrastructure remains widest. Efforts to address it have mostly worked at the edges rather than the center: regulating the fiat on-ramps where consumers convert ordinary currency into cryptoassets, requiring centralized exchanges that list DeFi tokens to provide risk disclosures, and, in a small number of jurisdictions, exploring whether front-end interfaces, the websites and apps most ordinary users actually interact with, even when the underlying protocol itself is decentralized, can be held to consumer protection standards even where the protocol beneath them cannot.

XI. Systemic Risk: When Fintech Meets Macroprudential Policy

A. Crypto Contagion and Bank Exposure Limits

Beyond harm to individual consumers, regulators have increasingly worried about systemic risk, the possibility that stress in cryptoasset markets could transmit into the traditional banking system in ways that amplify rather than stay contained within crypto itself. The Terra/Luna and FTX collapses discussed in Part VI both produced contagion effects well beyond their own ecosystems, dragging down other crypto lenders and exchanges that had exposure to the failed firms, though in neither case did the contagion meaningfully spread into the regulated banking sector, in large part because banks' direct exposure to crypto remained relatively limited at the time. That containment was, to a significant degree, a matter of scale and timing rather than a structural guarantee, and it is precisely why MiCA and the GENIUS Act both impose capital, reserve, and custody requirements that mirror banking regulation: as stablecoins in particular become more integrated with the traditional payments system, the two 2026 authorization datasets discussed in Part IV suggest that integration is happening unevenly and only partially within the newly built compliant perimeter, the contagion channel between crypto markets and regulated banks grows correspondingly wider, and the case for treating stablecoin reserves with something close to banking-grade prudential seriousness becomes correspondingly stronger.

B. Household Debt You Can't See Coming

BNPL's systemic risk profile is smaller in absolute scale than a major stablecoin or exchange failure, but it raises an analogous visibility problem at the level of household finances rather than financial institutions. Because a meaningful share of BNPL debt has historically sat outside standard credit reporting, aggregate household debt figures compiled by central banks and statistical agencies have likely understated actual consumer indebtedness by an amount that is difficult to quantify precisely, which matters directly for monetary policy and macroprudential supervision: a central bank assessing how much room consumers have to absorb higher interest rates, or a banking regulator stress-testing card issuers' exposure to a downturn, is working from an incomplete picture if a meaningful slice of consumer obligations

simply is not visible in the data they rely on. The credit reporting integration efforts referenced in Part X.A are, from this angle, not just a consumer protection measure but a data quality measure, closing a blind spot in the statistics regulators use to judge how much stress the household sector can actually absorb.

XII. Toward Coherent Regulation

A. Principles-Based vs. Rules-Based Approaches

The frameworks surveyed in this essay split, broadly, between two regulatory styles. A rules-based approach, exemplified by the GENIUS Act's specific, numerically defined reserve and capital requirements, offers clarity and predictability: an issuer can check compliance against an explicit checklist, and a regulator can verify it the same way, but such rules can also become quickly outdated as products evolve, and can be gamed by structuring a product just outside the literal terms of the rule while still inside its intended purpose, the exact regulatory arbitrage problem discussed in Part IX.A. A principles-based approach, closer to how the FCA has historically regulated UK financial services generally and how it has approached BNPL specifically, asks firms to satisfy a broader standard, treat customers fairly, assess affordability meaningfully, rather than a fixed checklist, which adapts more readily to new product structures but sacrifices some of the predictability and ease of enforcement that a bright-line rule provides.

Most of the frameworks examined in this essay are, in practice, hybrids rather than pure examples of either style: MiCA combines detailed, rules-based reserve requirements for stablecoins with more open-ended, principles-based conduct obligations for CASPs generally, and the FCA's BNPL regime pairs a specific, non-negotiable point-of-sale affordability check with more general, principles-based obligations around vulnerable customer treatment. That hybrid pattern, detailed rules where the risk is quantifiable and can be gamed by omission, broader principles where the risk depends on context a rule cannot fully anticipate in advance, looks, as of 2026, like the direction financial regulation is converging on across every product discussed in this essay, rather than either pure style prevailing on its own.

B. Regulatory Sandboxes and the Innovation Trade-Off

A recurring device across several of the jurisdictions discussed here is the regulatory sandbox, a supervised environment in which a firm can test a genuinely novel product against a limited customer base, under a regulator's direct observation, without needing to satisfy the full licensing regime that would apply to it at commercial scale. The FCA pioneered this approach for fintech generally well before BNPL or crypto became prominent policy issues, and it has informed the phased, sequenced rollouts both the UK's cryptoasset regime and its BNPL regime have followed, prioritizing the areas of clearest consumer risk, stablecoins and custody

in crypto, point-of-sale affordability in BNPL, before extending fuller obligations across the rest of the sector.

The trade-off a sandbox approach makes explicit, and which every framework in this essay ultimately has to make somewhere, is between protecting consumers from harm today and preserving enough space for a genuinely beneficial innovation to develop before it is regulated into a shape indistinguishable from the incumbent products it was meant to improve on. Cryptoassets, DeFi, and BNPL all, in their own way, promised to make some part of finance faster, cheaper, or more accessible than the traditional alternative, and each has delivered real versions of that promise to at least some users, even as each has also produced the harms this essay has documented. The regulatory task now, in every jurisdiction discussed here, is not to decide whether these products should exist at all, that question was effectively settled by their adoption at scale well before regulators caught up, but to decide how much of the old rulebook's substance, if not its exact form, should now apply to them.

XIII. Conclusion

Cryptoassets, decentralized finance, and buy now, pay later arrived through three different doors, a new payments and settlement infrastructure, a way of automating financial services without a company operating them, and a new packaging for an old consumer credit product, but they have converged, by 2026, on the same regulatory endpoint: a shift away from asking what a product calls itself and toward asking what it actually does. The Markets in Crypto-Assets Regulation, the GENIUS Act, the SEC-CFTC joint interpretation, and the UK, Australian, and EU BNPL regimes all reflect variations on that same functional principle, applied at different speeds, with different tools, and, in the case of DeFi specifically, still leaving a substantial and genuinely unresolved gap where no clearly identifiable regulated party exists at all.

None of this is finished. Stablecoin compliance under both MiCA and the GENIUS Act remains a work in progress rather than an achieved state, the UK's BNPL regime and the EU's CCD2 both take full effect only in the second half of 2026 and their practical operation is not yet tested, and DeFi's missing defendant problem has no clean resolution on the horizon in any jurisdiction surveyed here. What is reasonably clear, from the pattern traced across every product this essay has examined, is the direction of travel: financial regulation is converging, unevenly and often only after real harm has already occurred, on the idea that the economic substance of a product, not the label its promoters choose for it, should determine which rules apply. That is a genuinely old idea in financial regulation, arguably as old as financial regulation itself, and its re-application to blockchain, decentralized finance, and point-of-sale credit is less a story of law catching up to technology than of a familiar regulatory instinct being tested, once again, against a new set of products built, in part, specifically to see whether that instinct still holds.

Bibliography

Ballard Spahr. "SEC and CFTC Clarify When Digital Assets Are, and Are Not, Securities." March 2026.

Congress.gov, Library of Congress. "Stablecoin Legislation: An Overview of the GENIUS Act of 2025 (P.L. 119-27)." Congressional Research Service.

Congress.gov, Library of Congress. "An Overview of Decentralized Finance (DeFi)." Congressional Research Service, R48883, March 16, 2026.

Covington & Burling LLP. "The GENIUS Act Becomes Law: Key Provisions from the Federal Stablecoin Regulatory Framework." July 2025.

European Securities and Markets Authority (ESMA). "Markets in Crypto-Assets Regulation (MiCA)."

Financial Conduct Authority (FCA). "Regulating Buy Now Pay Later (BNPL)." fca.org.uk.

Skadden, Arps, Slate, Meagher & Flom LLP. "FCA Publishes New Proposals for Buy Now, Pay Later Regulation: One-Year Countdown to July 2026 Implementation." July 2025.

Holland & Knight LLP. "CFPB Provides Status Update Regarding Buy Now, Pay Later Interpretive Rule." May 2025.

Consumer Finance Monitor. "CFPB Will Not Issue Revised BNPL Rule." June 20, 2025.

Australian Securities and Investments Commission (ASIC). "Buy Now Pay Later Credit Contracts: Credit Licensing." asic.gov.au.

Karageorgiou & Associates. "Consumer Credit Directive (CCD2): Are We on Track for the 20 November 2025 Transposition Deadline?"

Hogan Lovells. "EU Second Consumer Credit Directive: Scope and Impact for Buy-Now Pay-Later (BNPL) Providers."

CoinDesk. "Terraform's Do Kwon Sentenced to 15 Years in Prison for Fraud." December 10, 2025.

CNBC. "TerraUSD Creator Do Kwon Sentenced to 15 Years Over $40 Billion Crypto Collapse." December 12, 2025.

U.S. Department of Justice, Southern District of New York. "Crypto-Enabled Fraudster Sentenced for Orchestrating $40 Billion Fraud." Press release.

The Block. "Sam Bankman-Fried Asks Supreme Court to Overturn Fraud Conviction and $11 Billion Forfeiture." September 11, 2026.

CNN. "Former Crypto Billionaire Sam Bankman-Fried Appeals Conviction to Supreme Court." September 10, 2026.

Forbes. "Disgraced FTX Founder Sam Bankman-Fried Loses Appeal of 25-Year Sentence." June 12, 2026.

CNBC. "Celsius CEO Alex Mashinsky Sentenced to 12 Years in Multi-Billion-Dollar Crypto Fraud Case." May 8, 2025.

CoinDesk. "Celsius Founder Alex Mashinsky Sentenced to 12 Years in Prison for Fraud." May 8, 2025.

Coinlaw.io. "Decentralized Finance Statistics 2026: TVL Drops to $71.77 Billion as Ethereum Tightens Its Grip."

Chargeflow. "$560B BNPL Market in 2026: Size, Growth & Provider Stats."

The Future of Money (Substack). "MiCA Q1 2026: EU Stablecoin Compliance, 19 EMT, 0 ARTs."