Crystal Intelligence



New York: crypto risk and regulation in 2026

CRYPTO CRIME LOSSES	CASH-FOR-CRYPTO	NEW YORK LISTINGS	CITIES WORLDWIDE
$593M	48	1,156	443

SERIES
Crystal Investigations

AUDIENCE
Regulators, compliance, law enforcement

PUBLISHED
June 2026

Contents

Key takeaways 03

New York at a glance 04

New York's crypto industry: can the Big Apple survive this many bites? 04

Why New York: the risk concentration 05

Crypto regulation in New York State 05

Live obligations and deadlines 06

Crypto adoption and trading infrastructure 07

New York's crypto crime profile 08

The anomaly explained 08

Cash-for-crypto services in New York 09

What the data reveals 10

Counter-asset availability 11

Privacy coins 12

Settlement methods 12

Global footprint 13

What this means for New York's crypto industry 14

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Key takeaways on crypto regulation and financial crime risk in New York State

- Beyond wealth concentration, New York's outsized share of institutional crypto activity makes it a high-value target.
- New York runs the most demanding state-level crypto framework in the country today.
- BitLicense obligations are continuous. The proposed 2026 CRYPTO Act would make unlicensed operation a criminal offense, with penalties up to a Class C felony.
- New York ranked fourth nationally in US crypto crime losses in 2025 at $593M. Complaints rose only 0.4% against a national 21.3% jump, but average loss per complaint surged 57.5% to $73,364.
- Crystal identified 48 cash-for-crypto services with 1,156 New York listings, most of them globally networked across 443 cities worldwide, and many are not registered locally.

New York crypto crime losses	Cash-for-crypto services identified	New York listings	Cities worldwide networked
$593M	48	1,156	443

"The BitLicense filters who serves New York. The CRYPTO Act would criminalize who serves it unlicensed. Together they raise the regulatory floor and the cost of operating beneath it."

Crystal Intelligence

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

New York at a glance

New York's economy, population, and financial infrastructure make it one of the most exposed states in the US to crypto-related financial crime.

Among US states for reported crypto crime losses in 2025.

NATIONALLY
Top 4

Behind only California and Texas, the third-largest state economy.

LARGEST ECONOMY
3rd

Statewide population, one of the largest consumer crypto markets in the US.

RESIDENTS
20M

Annual output at a scale that attracts institutional crypto activity.

GDP
$2.468T

New York's crypto industry: can the Big Apple survive this many bites?

New York's crypto framework faces pressure from three directions at once: a regulatory regime that is already the toughest in the country and about to get tougher, a crypto crime loss profile that sharply contradicts national trends, and a visibility gap where foreign-operated cash-for-crypto services operate beyond the reach of state licensing.

Regulators

Integrate incoming federal and state laws without disrupting New York's position as a global financial hub, on deadlines they did not set.

Compliance teams

Plan for an environment where the rules are tightening, the penalties are escalating (the CRYPTO Act introduces prison sentences), and the timeline keeps compressing.

Law enforcement

Protect citizens when they cannot identify, let alone investigate, crypto crimes which they cannot see.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Why New York: the risk concentration

New York's crypto risk profile is not simply a function of its size. It is a function of what concentrates here. The state accounts for approximately 8% of US GDP, but its share of institutional digital asset activity is disproportionately larger. New York hosts the densest concentration of hedge funds, private equity firms, family offices, and corporate treasuries in the country. When these entities are targeted, the losses are institutional-scale: a single compromised fund or fraudulently targeted executive can generate losses in the tens of millions without adding more than one complaint to the FBI's count.

This concentration also drives regulatory gravity. The state's stance on crypto does not just govern local businesses; it sets the de facto compliance floor for any financial institution that touches New York, which is most of them. That combination, institutional wealth density plus regulatory influence, is why gaps in New York's crypto framework carry national risk.

Crypto regulation in New York State

New York maintains the most established and demanding crypto regulatory framework in the United States. The 2015 BitLicense Regulation, issued under the New York Financial Services Law, established a specialized licensing regime for virtual currency businesses, administered by the New York State Department of Financial Services (NYDFS).

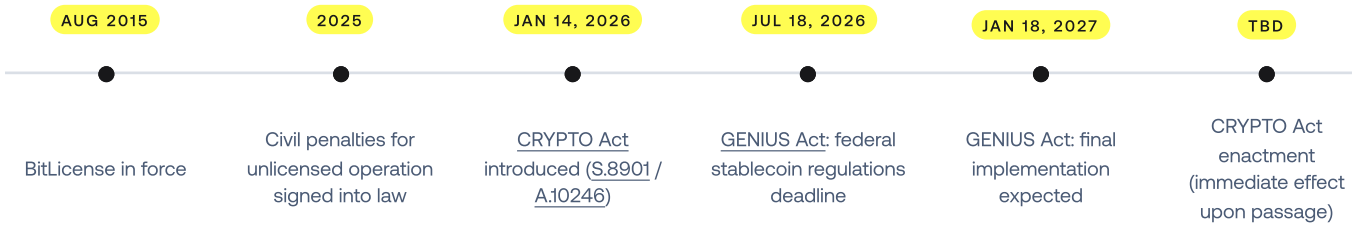
The BitLicense imposes ongoing obligations that go beyond initial registration. Licensees must maintain minimum capital reserves, implement AML and KYC programs, file suspicious activity reports, meet cybersecurity standards under 23 NYCRR 500, and submit to regular NYDFS examination. These requirements are substantively more demanding than the money transmitter licenses used by most other states, which is why several global exchanges, most notably Binance.US, have chosen not to serve New York residents rather than undergo the licensing process. The NYDFS is the primary regulatory authority, administering BitLicense, chartering limited-purpose trust companies and operating a dedicated virtual currency supervision unit, enhanced under its VOLT program.

Additionally, the Office of the New York State Attorney General (NYAG) has robust enforcement authority and has pursued multiple high-profile actions against unlicensed or fraudulent operators. These have resulted in settlements ranging from $18.5M to $2B for a range of offenses.

Meanwhile, Manhattan DA Alvin Bragg called for criminal penalties to address the “shadow financial system created by the explosion of crypto,” via the CRYPTO Act.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Live obligations and deadlines



The obligation to hold a BitLicense before conducting virtual currency business with New York residents is current and continuous.

The CRYPTO Act is the critical near-term development. If passed, operating without a license would become a criminal offense, with charges ranging from a Class A misdemeanor to a Class C felony depending on transaction volume. A Class C felony carries five to fifteen years. The bill takes effect immediately upon enactment.

The federal GENIUS Act adds a second layer of regulatory change. It requires final stablecoin implementing regulations by July 18, 2026, with full implementation by January 2027. For NYDFS-licensed stablecoin issuers, particularly Paxos Trust and Gemini Trust, this means updating existing compliance programs to align with federal requirements while continuing to meet state-level obligations.

The practical challenge is sequencing: state and federal rulemaking timelines overlap but are not coordinated.

Meanwhile, the CLARITY Act, which establishes regulatory frameworks for digital asset markets including disclosure requirements and DeFi protocol oversight, now sits before the Senate. New York officials have previously raised concerns about its scope. If enacted, it would add a third concurrent compliance workstream for New York's licensed operators.

Applications for new BitLicenses are submitted through the Nationwide Multistate Licensing System (NMLS) with a non-refundable $5,000 fee. Processing can take several years.

NMLS FEE

$5,000 fee

Non-refundable. Processing can take several years.

CLASS C FELONY

5-15 yrs

Under the proposed CRYPTO Act for unlicensed operation.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Identity verification under New York's compliance framework

New York has one of the world's most demanding regulatory environments for crypto businesses. The rules themselves are clear enough, yet executing them at scale is where crypto businesses come unstuck. Sumsub's crypto verification data shows a consistent pattern: most compliance failures trace back to legitimate customers getting caught in the controls built to stop fraudsters, not to companies skipping identity checks.

Fraud is now the bottleneck

In the first half of 2026, the average verification completion rate across crypto platforms reached 96%. The remaining 4% is a disproportionately expensive group: customers who need manual review, abandon onboarding, or trigger fraud investigations.

The leading reasons verification attempts fail:

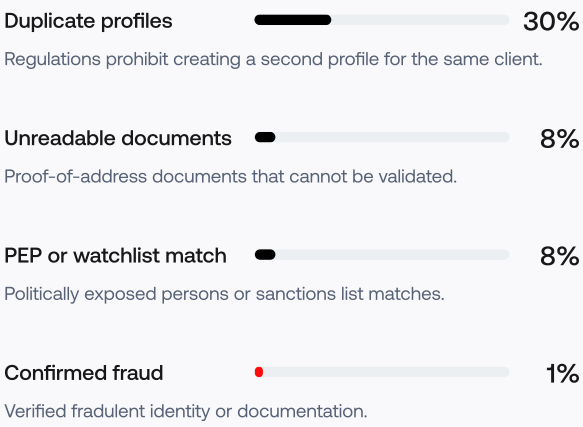
- 30% are duplicates, where a profile already exists for that client and the regulations prohibit creating another
- 8% come from unreadable proof-of-address documents
- 8% involve a Politically Exposed Persons or watchlist match
- 1% are confirmed fraud

Every missed fraud case creates regulatory and financial exposure.

The most mature compliance programs optimize for verification quality, treating the approval rate as one signal among several.

Why crypto verification attempts fail

Leading reasons for verification failure, H1 2026



Source: Sumsub crypto verification data, H1 2026

96%

average verification completion rate across crypto platforms in H1 2026. The remaining 4% drives disproportionate cost

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Cross-border users create the most operational complexity

Crypto businesses serving New York rarely onboard only New York residents. Many customers are international, holding passports, residence permits, or identity documents issued across dozens of jurisdictions.

That creates operational challenges regulation alone does not solve. Successful operators localize onboarding rather than applying one global ruleset. In practice, that means:

- Supporting jurisdiction-specific identity documents
- Validating names across multiple alphabets and transliteration standards
- Adapting verification flows to regional risk profiles
- Triggering Enhanced Due Diligence only when additional risk indicators are present

This reduces unnecessary friction while staying fully aligned with risk-based compliance expectations.

AI has changed the economics of identity fraud

Generative AI, more than any regulatory change, has reshaped crypto onboarding over the past two years. Fraudsters now produce identity documents, biometric spoofs, and synthetic identities at a scale that was previously impossible.

Across Sumsub's verification platform:

- AI-generated fraud attempts increased by 15% year-over-year.
- Deepfake-based biometric attacks grew by 20%

These attacks combine genuine stolen information with AI-generated imagery and increasingly sophisticated social engineering. As a result, identity verification has expanded well beyond document authentication. Effective onboarding now combines document verification, biometric Liveness, device intelligence, behavioral signals, and Fraud Prevention into a single decision.

Compliance doesn't end after onboarding

Identity verification is becoming a continuous process instead of a one-time event. Our data indicates that 76% of high-risk customer profiles surface only after onboarding, through ongoing monitoring, sanctions updates, or changes in customer behavior.

For regulated crypto businesses, continuous screening now carries as much weight as the initial verification decision. Firms that connect onboarding to ongoing monitoring detect emerging risks earlier, cut manual investigations by 90%, and hold a stronger audit trail for regulatory examinations.

For operators under New York's compliance framework, identity verification now means maintaining confidence in a customer's identity across the entire lifecycle, well past the moment they first prove who they are.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Crypto adoption and trading infrastructure

19% of New Yorkers own crypto (Coinbase, 2023) | 1.94% of households filed crypto tax returns (IRS/SmartAsset, 2022) | 18% of US crypto holders in the nine Northeastern states (NCA, 2026)

With 692 blockchain organizations and over 800 founders headquartered in the state (per Coinbase), New York is a national powerhouse of digital asset technology. Yet the state's institutional depth sits alongside a constrained retail landscape.

The licensing requirement means a significant number of global and smaller US exchanges have chosen not to serve New York, most notably Binance.US. New Yorkers who want access to tokens or platforms unavailable through licensed channels face a choice: go without, or seek alternatives outside the regulated perimeter. This dynamic is central to the crime and cash-for-crypto findings later in this report.

The exchanges that do serve New York include Coinbase, Gemini (New York-founded), Kraken, Robinhood Crypto, Bitstamp USA, bitFlyer USA, and eToro USA. Peer-to-peer marketplaces, OTC desks (Galaxy Digital, Cumberland, Coinbase Prime, Fidelity Digital Assets), and NYDFS-chartered trust companies (Paxos Trust, Gemini Trust) provide additional trading and custody infrastructure.

New York has a constrained crypto ATM footprint (243 as of May 2026, according to Bytescraper), owing to the compliance burden on operators.
All kiosk operators serving New York residents must hold a BitLicense and comply with transaction monitoring and KYC requirements at the point of sale.

Applications for new BitLicenses are submitted through the Nationwide Multistate Licensing System (NMLS) with a non-refundable $5,000 fee. Processing can take several years.

Exchanges that serve New York

Licensed channels available to residents

- Coinbase
- Gemini (New York-founded)
- Kraken
- Robinhood Crypto
- Bitstamp USA
- bitFlyer USA
- eToro USA

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

New York's crypto crime profile

According to the FBI Internet Crime Report 2025, New York ranked fourth in the US in both criminal complaints with a crypto nexus (8,088) and reported losses ($593M, up 58.2% from $375M in 2024). New York retained the same ranking as in 2024. New York's complaint numbers barely moved from 2024 to 2025, rising just 0.4% against a nationwide jump of 21.3%. But average loss per complaint tells the opposite story: New York's surged 57.5% to $73,364, while the national average rose just 0.52%.



Sources: FBI Internet Crime Report 2025, FBI Internet Crime Report 2024.

The anomaly explained

01 Investment fraud targeting high-net-worth individuals

New York's concentration of finance professionals, executives, and high-wealth retirees makes it a natural hunting ground for sophisticated long-duration investment scams.

02 The BitLicense paradox

The strict licensing regime means fewer crypto businesses operate in the state, which may push users toward unregulated platforms, precisely where investment fraud flourishes. A New Yorker unable to access a given exchange through normal channels may be more susceptible to a fraudulent "platform."

03 Institutional exposure

New York's financial infrastructure means a single incident, one family office, one fund, one corporate treasury, can substantially increase the average loss figure without adding complaint volume.

THE SIGNAL IN THE DATA

New York isn't seeing more crypto crime. The flat complaint line with a surging loss line likely indicates precision targeting, not mass fraud.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Cash-for-crypto services in New York

Crystal Intelligence analysis of BestChange, a cash-for-crypto aggregator popular with Russian speakers, identified 48 distinct exchanger services listing cash-handling options in New York, across 1,156 trading-pair listings. These are services where a "cash" listing denotes an in-person or cash-by-courier exchange of physical currency against crypto.

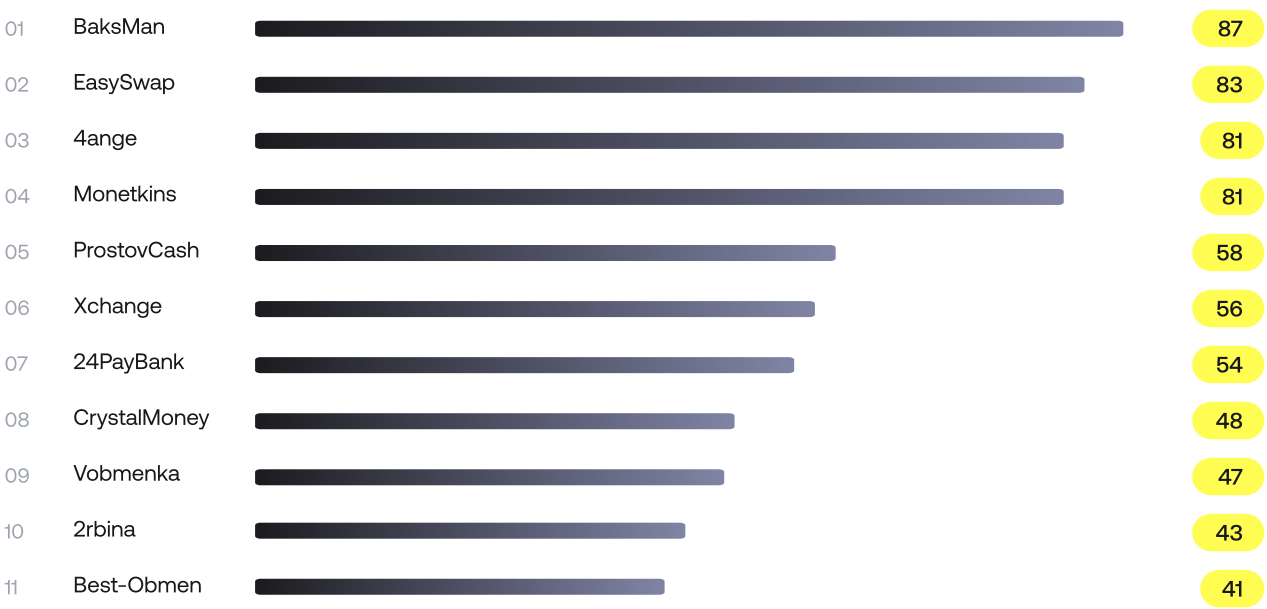
The market is concentrated: just 11 services account for 59% of cash-handling listings monitored statewide. BaksMan leads with 87 listings, followed by EasySwap (83), 4ange (81), and Monetkins (81).

This analysis draws on BestChange, one of several cash-for-crypto aggregator platforms. The findings reflect the services, listings, and settlement methods visible through this source and should not be read as a complete picture of New York's cash-for-crypto market. They do, however, provide a structured and replicable view of a segment that is otherwise difficult to observe.

The services moving cash into crypto

Cash-handling exchangers ranked by trading-pair listings

1,156
listings monitored statewide



Source: Crystal Intelligence. Top 11 services: 679 of 1156 listings (59%).

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

What the data reveals

The 48 services identified in New York share a distinct operational profile that separates them from licensed exchanges and registered money services businesses.

Settlement is physical

Within the dataset, nearly all New York listings (1,154 of 1,156) involve physical cash settlement. Electronic settlement options appear only twice. No traditional bank transfers are tagged to New York. This is a cash business operating alongside, but entirely outside, the banking system.

The operator base appears predominantly CIS-origin

The aggregator platform, service naming conventions, and bank rails recorded in the broader dataset point to a Russian-speaking operator community. Where remote settlement options appear, they reference Sberbank, T-Bank, Alfa-Bank, and Gazprombank (27, 27, 25, and 23 services respectively), alongside Kazakhstan's Kaspi, Halyk, and Forte banks. Several of these institutions are under international sanctions.

Privacy coins are disproportionately represented

Monero holds roughly 0.3% of total crypto market capitalization. Yet 56% of these services offer it, making it the sixth most available counter-asset, ahead of USDC. Dash (42%) and Zcash (33%) follow. This level of adoption relative to market share indicates deliberate selection for traceability resistance.

For an investigator, a Monero off-ramp paired with physical cash settlement represents the point where on-chain tracing ends and traditional investigative methods must begin.

The networks are global but the operators are concentrated

Eighty-five percent of the services active in New York also operate in London. The top ten operators span 281 cities. Yet the market is not fragmented: 11 services account for 59% of all New York listings. This concentration means targeted investigation is operationally feasible in a way that pursuing hundreds of small operators would not be.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

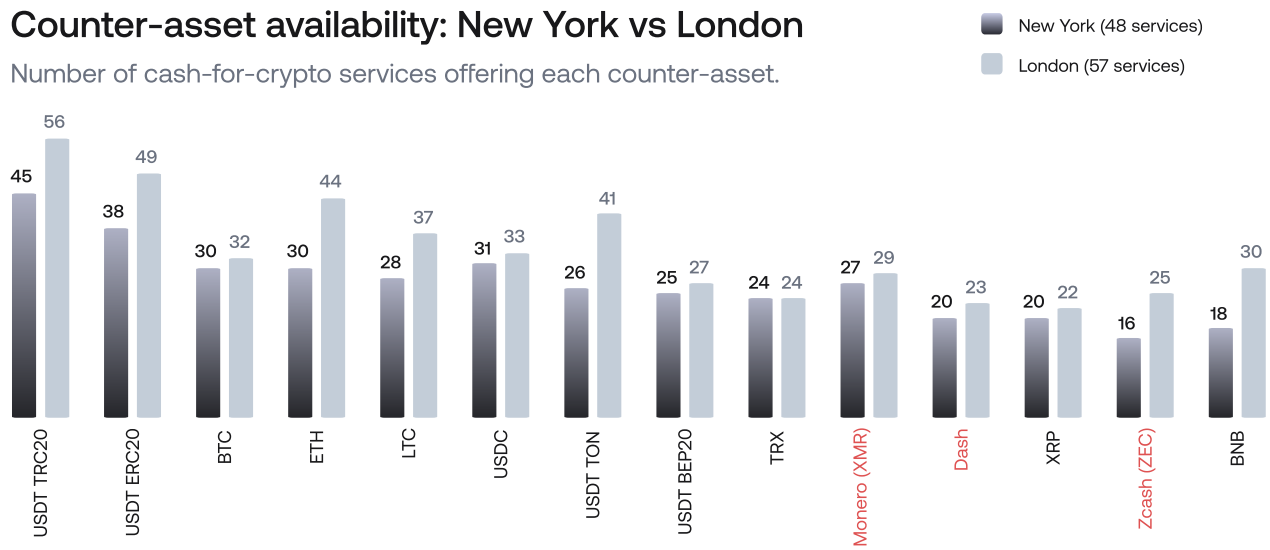
Counter-asset availability

LISTING TYPE	NEW YORK	LONDON
Cash services	48	57
Cash listings	1,156	2,131
Dominant cash currency	USD (99.8%)	EUR (then GBP, USD)
Leading counter-asset	USDT TRC20 (45 svc)	USDT TRC20 (56 svc)
Monero prevalence	56% of services	56% of services
Shared operators	—	41 of NY's 48 (85%)

Source: Crystal Intelligence analysis of BestChange data.

Counter-asset availability: New York vs London

Number of cash-for-crypto services offering each counter-asset.



Source: Crystal Intelligence analysis of BestChange data.

For comparative purposes, London illustrates key differences between these markets. On the fiat side, New York activity is almost entirely denominated in US Dollars: 1,154 of the 1,156 listings involve USD cash, compared to London's three-currency mix. On the crypto side, Tether on the Tron network (USDT TRC20) is the most widely listed counter-asset in both cities, offered by 45 of New York's 48 services and 56 of London's 57.

The 85% operator overlap between the two cities confirms that these are global networks with local listings, not locally originated services. Monero prevalence is identical at 56% in both markets, suggesting that the privacy coin offering is a standard feature of the operator model rather than a response to local demand. Zcash prevalence is higher in London (44%) than New York (33%), the only notable divergence in the counter-asset profiles.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Privacy coins

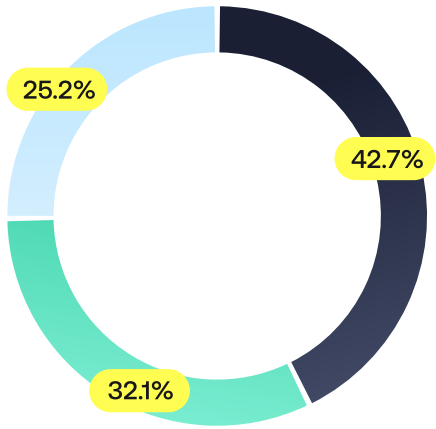
The privacy coin finding carries specific implications. A service offering Monero alongside physical cash creates a two-stage opacity barrier: the cash leg leaves no bank record, and the Monero leg resists blockchain tracing. Downstream conversion from Monero to a stablecoin or Bitcoin typically occurs on a separate platform, often in a different jurisdiction, breaking the chain of attribution.

Dash and Zcash offer weaker but still meaningful privacy features.

Their presence in 42% and 33% of services respectively suggests a market that systematically caters to users seeking reduced traceability.

For investigators, the counter-asset choice is itself intelligence. A cash-to-USDT transaction is traceable on-chain once the USDT address is known. A cash-to-Monero transaction is not. The 56% Monero prevalence among these services means that over half the market offers a path that conventional blockchain analytics cannot follow beyond the initial conversion point.

Privacy coin prevalence among New York cash-for-crypto services



Monero (XMR)	27 of 48 services
Zcash (ZEC)	20 of 48 services
Dash	16 of 48 services

Source: Crystal Intelligence analysis of BestChange data.

Settlement methods

On the settlement side, the USD monolith finding is itself significant. London's cash-for-crypto market operates across three currencies (EUR, GBP, USD). New York's operates in one. This is not simply a reflection of domestic currency preference.
It suggests a service model specifically built for the US dollar cash economy rather than one that incidentally touches it.

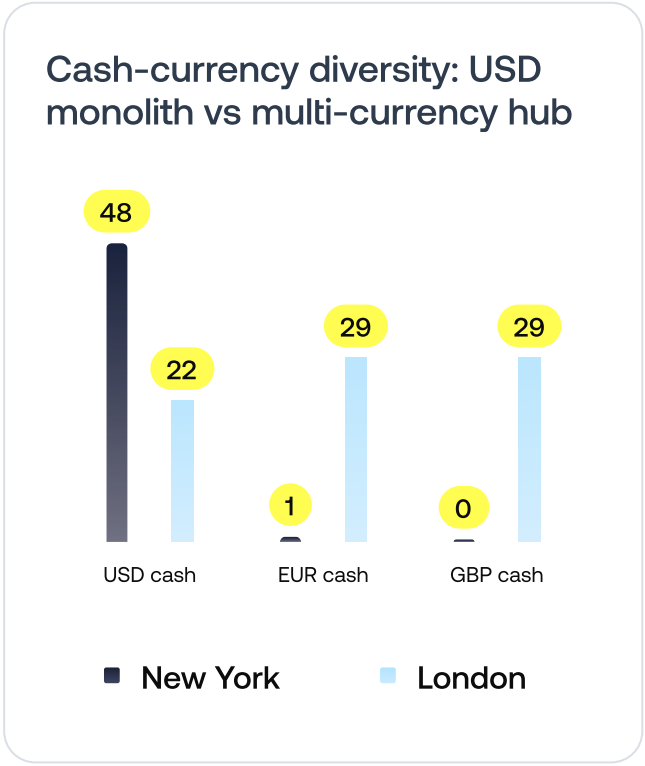
The near-total absence of electronic settlement in the New York listings reinforces this reading. Only two services (BTC2Pay and UAchanger) list any electronic-money options, each with a single listing. No traditional bank transfers are tagged to New York. The cash-only model eliminates the transaction records that bank settlement would create, making these services functionally invisible to the financial system's existing monitoring infrastructure.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

functionally invisible to the financial system's existing monitoring infrastructure.

Where bank rails do appear in the broader dataset, they are recorded as remote/online listings rather than tagged to New York. The banks involved, Sberbank and T-Bank (27 services each), Alfa-Bank (25), and Gazprombank (23), alongside Kazakhstan's Kaspi (25), Halyk (20), and Forte (18), reinforce the CIS-origin operator profile identified earlier in this report.

The cross-border platforms Wise and Revolut also appear in remote listings but not in New York-tagged entries. This separation between cash-only local listings and bank-rail remote listings suggests a deliberately segmented service model: physical cash for the New York client, electronic settlement for the operator's home jurisdiction.



Source: Crystal Intelligence analysis of BestChange data.

Global footprint

These services are not New York-specific: collectively they appear across 443 cities in the dataset. The widest-reaching operators (Clean-Exchange, ExLine, AbcObmen, Crybex, ProstovCash, BaksMan) each appear in between 216 and 255 cities.

Despite the state's regulatory rigors, some of these global services are sanctions-exposed and support privacy coins. Their presence in New York is not a local compliance failure; it is a structural limitation of a licensing regime designed for operators who present themselves for registration. These operators do not.

The geographic spread also has jurisdictional implications. An operator listed in 250 cities across dozens of countries is unlikely to be reached by any single state's enforcement action.

Effective intervention requires either federal coordination or international cooperation, neither of which the current BitLicense framework was designed to trigger.

443

cities worldwide

85%

of operators shared with London

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

What this means for New York's crypto industry

New York's regulatory framework was designed for operators who seek a license. The services identified in this analysis do not. That structural mismatch is the central finding: the state has the most demanding compliance regime in the country, and a parallel cash-for-crypto market operating entirely beneath it.

The incoming CRYPTO Act would close the legal gap by criminalizing unlicensed operation. But criminal penalties require detection, and detection requires visibility these services are specifically designed to avoid.

The gap is not statutory. New York has the legal authority to act. The gap is operational: the ability to see these services, attribute their transactions, and build cases that hold. The three audiences this report addresses each face a different version of that challenge.

For state law enforcement

The concentration of activity in 11 operators is an investigative advantage, not just a data point. Physical cash settlement means physical locations, and physical locations can be identified, surveilled, and evidenced. The priority is building blockchain forensic capability at case-officer level so that crypto-nexus cases do not stall waiting for specialist unit availability. Where Monero is involved, the conversion point itself resists chain analysis, but the transaction legs before and after it often do not.

If converted Monero re-enters a traceable blockchain as USDT or Bitcoin, as the counter-asset data in this report suggests is common, the off-ramp is visible. The investigative approach is to trace around the opaque segment, not through it.

For NYDFS and state regulators

The BitLicense framework assumes a licensee. These services have no presence in the NMLS, no compliance officer, and no obligation they recognize. The CRYPTO Act would give prosecutors a tool, but only if cases reach them. A common analytical baseline across the NYDFS, NYAG, Manhattan DA, and federal agencies would ensure that the intelligence gathered by one body is usable by the others without re-investigation. The sanctions exposure of the CIS bank rails in the dataset is a separate and immediate supervisory concern.

For compliance teams at licensed exchanges

The findings describe the environment your customers move through before and after they reach your platform. A New Yorker who cannot access a given exchange legitimately may interact with these services instead, and the funds arriving at your platform may carry that history. Exposure controls should screen for the transaction typologies this data suggests: physical cash conversion to USDT TRC20 or Monero, followed by transfer to a licensed exchange for fiat off-ramping.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Discuss a demonstration, an active investigation, or training for your team.

Crystal Intelligence's investigations, training and certification programs build the same capability inside state and local agencies.

Get a demo →

crystalintelligence.com

© 2026 Crystal Intelligence. All rights reserved.

This report is intended for informational purposes only. The data provided herein is based on information publicly available and analysis conducted by Crystal Intelligence. Crystal Intelligence accepts no liability for actions taken based on this information. Readers are advised to perform independent verification and seek professional advice where necessary.