

In-Depth Analysis: Privacy Coins, Between Technological Sovereignty and Regulatory Constraint

I - Executive Summary and The Monetization of Geopolitical Fear

The **privacy coin** sector, which includes cryptocurrencies focused on anonymizing transaction tracking, has entered a phase of exponential valuation. The spectacular surge of these assets has shaken the crypto ecosystem in recent days, notably **ZCash (ZEC)**, **Monero (XMR)**, and **Dash**. This trend shows astounding performance, with ZCash recording a gain of more than **1400%** since August (with a peak of 1800% increase over 90 days), and this is happening right in the middle of an unprecedented regulatory wave.

ZCash has been the speculative engine of this surge, but the sector shows over 205% performance year-to-date, crushing Bitcoin and Ethereum. The central analytical thesis of this trend stipulates that this performance is not the result of a simple bubble, but the monetization of a **financial sovereignty premium**, where prohibition by states validates the technological necessity of these tools.

This change in market dynamics is the direct result of a paradox: **prohibition fuels demand**. Every regulatory attack only serves to feed their explosive growth. The October explosion of ZCash and the stable growth of Monero since 2024 are not speculative anomalies. Instead, they are symptoms of **collective anxiety** in the face of totalizing financial surveillance. A detailed analysis of the drivers of this rise reveals a complex intertwining of speculation led by Key Opinion Leaders (KOLs), institutional access (like the launch of the Grayscale ZCash Trust), and the European legal framework.

Before examining these mechanisms, it is imperative to stress that **this is not investment advice; conduct your own research**. The privacy coin sector is highly volatile and remains exposed to legal risks and extreme volatility. Finally, trading cryptocurrency carries a risk of partial or total loss of capital.

II - The European Regulatory Constraint and the Validation Factor

The European Union has unintentionally served as a catalyst for the price surge by adopting regulations that directly target anonymity, thereby creating a paradox in the market. The conflict is led by the **Anti-Money Laundering Regulation (AMLR)**, which, along with the **MiCA** framework, establishes the formal **prohibition of privacy coins**. This legislation mandates rigorous identification for transactions exceeding **€1,000**, even between individuals via a hosted service, with the implementation of these measures planned for **July 2027**.

The Insoluble Conflict: Traceability vs. Compliance

The legal objective of these regulations is to ensure LCB-FT compliance (Fight against Money Laundering and the Financing of Terrorism), which requires platforms to be able to verify transactions both upstream (*pre-trade*) and downstream (*post-trade*).

However, the very nature of the confidentiality protocols (such as Monero's **Ring Signatures** or ZCash's **shielded** transactions) renders the cryptocurrency **totally untraceable**. Regulated exchange platforms (such as Binance, Kraken, or OKX) are thus constrained to **delist these tokens**, because the impossibility of analyzing the blockchain structurally prevents them from

meeting their regulatory obligations. The massive delisting by 73 centralized exchanges has also forced 40% of the volume onto less-regulated platforms.

The Streisand Effect: Validation of the Anti-Surveillance Thesis

The prohibition has had the opposite effect of what was intended, acting as a "**Streisand Effect**" that validates the utility of **privacy coins**. By explicitly targeting these technologies, regulators confirm that confidentiality "bothers the system."

For users, this legislative act transforms these assets into an **essential insurance against state financial surveillance**. These are symptoms of a collective anxiety in the face of total surveillance and the arrival of Central Bank Digital Currencies (**CBDC**).

The result is clear: instead of eliminating the market, the regulatory threat accelerates the collective awareness that it is urgent to secure financial liberty. This is why: **the tighter the regulation, the more demand explodes for these "anti-censorship" tokens**, as users seek to secure their financial freedom before legal access points close definitively on the continent.

III - ZCash: The Speculative Amplifier and New Drivers

ZCash (ZEC) has been the true speculative engine of the **privacy coins** rally, largely surpassing the more organic growth observed in Monero. This surge was not triggered by a revolutionary technical update, but by a powerful convergence of media, speculative, and access factors, creating a massive **FOMO** (Fear Of Missing Out) phenomenon. The rally was widely amplified by the endorsement of major influencers in the crypto ecosystem, transforming speculation into a frantic race. The prediction by BitMex co-founder, **Arthur Hayes**, of a **\$10,000** price target for ZEC fueled the frenzy, especially after he tweeted that ZCash was the second-largest position in his investment fund. Simultaneously, the narrative was cemented by figures like **Naval**, who positioned ZEC as the "insurance against Bitcoin," which itself is considered an assurance against fiat currencies. This narrative positioned the asset as a logical evolution in the face of BTC's traceability.

Secondly, ZCash benefited from a seal of legitimacy and improved accessibility. The launch of the **Grayscale Zcash Trust** offered accredited institutional investors regulated exposure to ZEC, which is not the case for Monero. This perceived legitimacy attracted institutional investors.

Furthermore, on the user experience front, the launch of the new **Zashi** wallet helped to simplify the activation of **shielded** (anonymized) transactions. The improvement in ease of use indirectly helped reinforce this narrative.

Finally, rumors concerning a **halving** or a similar mechanism aimed at reducing the number of new ZEC issued into circulation created a powerful scarcity effect. This mechanism, familiar to Bitcoin, increases the difficulty of obtaining the asset for miners and fed the buying pressure, contributing to the extreme volatility observed. Increased access to liquidity on leveraged trading platforms (like Hyperliquid) also amplified this speculative rush.

IV - Differential Technical Analysis: Auditability vs. Absolute Anonymity

The rivalry between Monero and ZCash is less a simple technical competition than an ideological confrontation over how to ensure confidentiality, a choice that directly impacts their relationship with regulators. These two projects represent two radically different approaches to anonymity.

Monero embodies pure resistance, prioritizing **Absolute and Mandatory** confidentiality. Its protocol relies primarily on **Ring Signatures** and **Stealth Addresses**. Ring Signatures create a group of possible signers, making it impossible to know who actually issued the transaction. Stealth addresses generate a unique and temporary address for each payment, preventing any link between a single person's transactions.

The underlying philosophy is the **Refusal of any compromise with regulators**. Since anonymity is integrated and non-optional, Monero ensures maximum fungibility, but this intransigence has a direct consequence: it is **difficult to list on regulated exchanges (often delisted)**. The regulatory attack reinforces the idea that it is the anti-censorship money *par excellence*.

ZCash, in contrast, prioritizes flexibility. Its protocol uses **ZK-Snarks (Zero-Knowledge Proofs)**, a technology allowing transaction validity to be verified without ever revealing the amounts or addresses. Anonymity is left to the **User's Choice (ZK-Snarks)**, via so-called shielded transactions.

This technical approach allows for **Flexibility, allowing for selective disclosure***. This function means that, thanks to **Viewing Keys**, the user can prove compliance to an auditor or authority without sacrificing their privacy. This strategic compromise has the consequence of being **Retained by certain exchanges and institutional investors (e.g., Grayscale Trust)**. ZCash thus seeks a path between the necessity of confidentiality and the reality of the regulatory framework.

V - Market Implications, Existential Risks

The explosion in the price of **privacy coins** must be analyzed in light of their fundamental utility compared to their market capitalization. Despite the speculative surge, the sector remains comparatively undervalued when considering the volume of real transactions it generates. **Monero**, in particular, historically shows a higher proportion of real and useful transactions (more than half of transactions are real exchanges between users) than Bitcoin, where the majority of movements are linked to speculation.

This organic utility, contrasting with the low market capitalization of the sector (less than 1% of the global crypto market), suggests that the market is still far from having integrated the potential of these assets into a privacy-conscious economy. The adoption of these tokens is a symptom of collective anxiety and becomes a logical hedge.

However, the opportunity for return is accompanied by major risks. The **regulatory execution risk** is predominant and existential. If regulations like the **AMLR** manage to target access via decentralized protocols (**DEX**), the liquidity and the ability to exchange (*off-ramp*) these tokens would be severely compromised. Furthermore, history has shown that ease of use prevails over all other advantages: protocols based on **Proof-of-Work (PoW)** face potential obsolescence compared to the scalability and reduced costs offered by ZK solutions based on Ethereum's L2s.

The sector is therefore subject to **extreme volatility**. The price is largely dictated by influencer narratives and liquidity access (like Hyperliquid), exposing the investor to the fear of missing out

(**FOMO**) and brutal corrections. In 2024 and 2025, ZCash experienced no less than 12 drops of at least 25%.

Analytical Conclusion

The explosion of **privacy coins** is the **monetization of a financial sovereignty premium**. It is a reflection of growing defiance against state control. The value of these tokens will increase proportionally to the expansion of surveillance.

For the investor, the bet is clear: the performance of these assets is a reliable indicator that the state will not stop in its quest for surveillance. **Privacy coins** now occupy a permanent role in the crypto ecosystem, not as criminal tools, but as an **existential insurance** against totalizing financial control. Investing in this sector is betting on freedom, even if the regulatory risks and volatility demand maximum prudence.

— VILLEMAN Emile | TradFi, M&A, DeFi & Crypto Research

© 2025 – Please respect this content. Any reproduction must be credited.

Analyse Approfondie : Les Privacy Coins, Entre Souveraineté Technologique et Contrainte Réglementaire

I - Synthèse Exécutive et La Monétisation de la Peur Géopolitique

Le secteur des *Privacy Coins*, ces cryptomonnaies axées sur l'anonymisation du suivi des transactions, est entré dans une phase de valorisation exponentielle. L'envolée spectaculaire de ces actifs a secoué l'écosystème crypto ces derniers jours, notamment ZCash (ZEC), Monero (XMR) et Dash. Cette tendance affiche des performances ahurissantes, ZCash marquant un gain de plus de **1400 %** depuis le mois d'août (avec une pointe à 1800% de hausse sur 90 jours), et ce, en plein cœur d'une vague réglementaire sans précédent.

ZCash a été le moteur spéculatif de cette envolée, mais le secteur dans son ensemble affiche plus 205 % de performance sur l'année, pulvérisant Bitcoin et Ethereum. La thèse analytique centrale de cette tendance stipule que cette performance n'est pas le fruit d'une simple bulle, mais la monétisation d'une **prime de souveraineté financière**, où l'interdiction par les États valide la nécessité technologique de ces outils.

Ce changement de dynamique de marché est le résultat direct d'un paradoxe : l'interdiction alimente la demande. Chaque attaque réglementaire ne fait qu'alimenter leur croissance explosive. L'explosion d'octobre de ZCash et la croissance stable de Monero depuis 2024 ne sont pas des anomalies spéculatives. Au lieu de cela, ce sont des symptômes d'une anxiété collective face à la surveillance financière totalisante. L'analyse détaillée des moteurs de cette hausse révèle une imbrication complexe entre la spéculation menée par les Key Opinion Leaders (KOLs), l'accès institutionnel (comme le lancement du Grayscale ZCash Trust) et le cadre légal européen.

Avant d'examiner ces mécanismes, il est impératif de souligner que ceci n'est pas un conseil en investissement ; menez vos propres recherches. Le secteur des Privacy Coin est très volatile et reste exposé à des risques juridiques. Pour finir, le trading de cryptomonnaie possède un risque de perte partiel ou total de capital.

II - La Contrainte Réglementaire Européenne et le Facteur de Validation

L'Union Européenne a involontairement servi de catalyseur à la flambée des prix en adoptant des réglementations qui ciblent directement l'anonymat, créant ainsi le paradoxe du marché. Le conflit est mené par l'**Anti-Money Laundering Regulation (AMLR)**, qui, avec le cadre **MiCA**, établit l'interdiction formelle des *Privacy Coins*. Cette législation impose l'identification rigoureuse des transactions excédant **1 000 €**, même entre particuliers via un service hôte, l'application de ces mesures étant prévue pour **juillet 2027**.

Le Conflit Insoluble : Traçabilité vs. Conformité

L'objectif légal de ces réglementations est d'assurer la conformité LCB-FT (Lutte contre le Blanchiment des Capitaux et le Financement du Terrorisme), ce qui exige des plateformes de pouvoir vérifier les transactions tant en amont (*pré-trade*) qu'en aval (*post-trade*).

Cependant, la nature même des protocoles de confidentialité (comme le *Ring Signatures* de Monero ou les transactions *shielded* de ZCash) rend la cryptomonnaie **totalement intraçable**. Les plateformes d'échange régulées (telles que Binance, Kraken, ou OKX) sont ainsi contraintes de **délistier ces jetons**, car l'impossibilité d'analyser la blockchain les empêche structurellement de satisfaire à leurs obligations réglementaires. Le délistage massif par 73 exchanges centralisés a d'ailleurs forcé 40 % du volume vers des plateformes moins régulées.

L'Effet Streisand : Validation de la Thèse Anti-Surveillance

L'interdiction a eu l'effet inverse de celui escompté, agissant comme un « **Effet Streisand** » qui valide l'utilité des *Privacy Coins*. En ciblant explicitement ces technologies, les régulateurs confirment que la confidentialité « dérange le système ».

Pour les utilisateurs, cet acte législatif transforme ces actifs en une **assurance essentielle** contre la surveillance financière étatique. Ce sont des symptômes d'une anxiété collective face à la surveillance totale et à l'arrivée des Monnaies Numériques de Banque Centrale (**CBDC**).

Le résultat est sans appel : au lieu d'éliminer le marché, la menace réglementaire accélère la prise de conscience collective qu'il est urgent de sécuriser sa liberté financière. C'est pourquoi : plus la réglementation se resserre, plus la demande pour ces jetons "anti-censure" explose, les utilisateurs cherchent à sécuriser leur liberté financière avant que les portes d'accès légales ne se ferment définitivement sur le continent.

III - ZCash : L'Amplificateur Spéculatif et les Nouveaux Moteurs

ZCash (ZEC) a été le véritable moteur spéculatif du rallye des *Privacy Coins*, surpassant largement la croissance plus organique observée chez Monero. Cette flambée n'a pas été déclenchée par une mise à jour technique révolutionnaire, mais par une convergence puissante de facteurs médiatiques, spéculatifs et d'accès, créant un phénomène de **FOMO** (Fear Of Missing Out) massif. Le rallye a été largement amplifié par l'endossement d'influenceurs majeurs dans l'écosystème crypto, transformant la spéculation en une course frénétique. La prédiction du cofondateur de BitMex, **Arthur Hayes**, d'un prix cible de **10 000 \$** pour ZEC a mis le feu aux poudres, surtout après qu'il ait tweeté que ZCash était la deuxième plus grosse position de son fond d'investissement. Simultanément, la narration a été cimentée par des figures comme **Naval**, qui a positionné ZEC comme l'**« assurance contre Bitcoin »**, lui-même étant considéré comme une assurance contre les monnaies *fiat*. Ce narratif a positionné l'actif comme une évolution logique face à la traçabilité de BTC.

Deuxièmement, ZCash a bénéficié d'un sceau de légitimité et d'une meilleure accessibilité. Le lancement du **Grayscale Zcash Trust** a offert aux investisseurs institutionnels accrédités une exposition réglementée à ZEC, ce qui n'est pas le cas pour Monero. Cette légitimité perçue a attiré les investisseurs institutionnels.

Par ailleurs, sur le plan de l'expérience utilisateur, le lancement du nouveau portefeuille **Zashi** a permis de simplifier l'activation des transactions *shielded* (anonymisées). L'amélioration de la simplicité d'utilisation a indirectement permis de raccrocher cette narration.

Enfin, des rumeurs concernant un **halving** ou un mécanisme similaire visant à réduire le nombre de nouveaux ZEC émis en circulation ont créé un puissant effet de rareté. Ce mécanisme, bien connu sur Bitcoin, augmente la difficulté d'obtention par les mineurs et a alimenté la pression acheteuse, contribuant à la volatilité extrême observée. L'accès accru à la liquidité sur des plateformes de *trading* à effet de levier (comme Hyperliquide) a également amplifié cette précipitation spéculative.

IV - Analyse Technique Différentielle : Auditabilité vs. Anonymat Absolu

La rivalité entre Monero et ZCash est moins une simple concurrence technique qu'une confrontation idéologique sur la manière d'assurer la confidentialité, un choix qui impacte directement leur relation avec les régulateurs. Ces deux projets représentent deux approches radicalement différentes de l'anonymat.

Monero incarne la résistance pure, privilégiant la confidentialité **Absolue et Obligatoire**. Son protocole s'appuie principalement sur les **Ring Signatures** et les **Stealth Addresses**. Les Ring Signatures créent un groupe de signataires possibles, rendant impossible de savoir qui a réellement émis la transaction. Les *stealth addresses* génèrent une adresse unique et temporaire pour chaque paiement, empêchant tout lien entre les transactions d'une même personne.

La philosophie sous-jacente est le **Refus de tout compromis avec les régulateurs**. Puisque l'anonymat est intégré et non optionnel, Monero assure une fongibilité maximale, mais cette intransigeance a une conséquence directe : il est **Plus difficile à lister sur les exchanges régulés (souvent délisté)**. L'attaque réglementaire renforce l'idée qu'il est l'argent résistant à la censure par excellence.

ZCash, en revanche, privilégie la flexibilité. Son protocole utilise les **ZK-Snarks** (Zero-Knowledge Proofs), une technologie permettant de vérifier la validité d'une transaction sans jamais révéler les montants ou les adresses. L'anonymat est laissé au **Choix de l'utilisateur (ZK-Snarks)**, via des transactions dites *shielded*.

Cette approche technique permet une **Flexibilité, permettant la selective disclosure***. Cette fonction signifie que, grâce aux *Viewing Keys*, l'utilisateur peut prouver la conformité à un auditeur ou une autorité sans sacrifier sa vie privée. Ce compromis stratégique a pour conséquence d'avoir été **Conservé par certains exchanges et institutionnels (e.g., Grayscale Trust)**. ZCash cherche ainsi une voie entre la nécessité de la confidentialité et la réalité du cadre réglementaire.

V - Implications de Marché, Risques Existentiels

L'explosion des prix des *Privacy Coins* doit être analysée à l'aune de leur utilité fondamentale par rapport à leur capitalisation boursière. Malgré la flambée spéculative, le secteur reste comparativement sous-évalué si l'on considère le volume de transactions réelles qu'il génère. Monero, en particulier, affiche historiquement une proportion plus élevée de transactions réelles et utiles (plus de la moitié des transactions sont de vrais échanges entre utilisateurs) que Bitcoin, dont la majorité des mouvements sont liés à la spéulation.

Cette utilité organique, contrastant avec la faible capitalisation boursière du secteur (moins de 1 % du marché crypto global), suggère que le marché est encore loin d'avoir intégré le potentiel de ces actifs dans une économie soucieuse de la confidentialité. L'adoption de ces jetons est un symptôme d'une anxiété collective et devient une couverture logique.

Toutefois, l'opportunité de rendement s'accompagne de risques majeurs. Le **risque d'exécution réglementaire** est prédominant et existentiel. Si les régulations comme l'AMLR parviennent à cibler l'accès via les protocoles décentralisés (DEX), la liquidité et la capacité d'échange (*off-ramp*) de ces jetons seraient gravement compromises. De plus, l'histoire a montré que la facilité d'utilisation prime sur tous les avantages : les protocoles basés sur le Proof-of-Work (PoW) font face à une obsolescence potentielle face à la *scalabilité* et aux coûts réduits offerts par les solutions ZK basées sur les L2 d'Ethereum.

Le secteur est donc sujet à une **volatilité extrême**. Le prix est largement dicté par la narration d'influenceurs et les accès de liquidité (comme Hyperliquide), exposant l'investisseur à la peur de rater le train (*FOMO*) et à des corrections brutales. En 2024 et 2025, ZCash a connu pas moins de 12 décrochages d'au moins 25 %.

Conclusion Analytique : Le Pari sur la Liberté

L'explosion des *Privacy Coins* est la monétisation d'une **prime de souveraineté financière**. Elle est le reflet d'une défiance croissante face au contrôle étatique. La valeur de ces jetons augmentera proportionnellement à l'expansion de la surveillance.

Pour l'investisseur, le pari est clair : la performance de ces actifs est un indicateur fiable que l'État ne s'arrêtera pas dans sa quête de surveillance. Les *Privacy Coins* occupent désormais un rôle permanent dans l'écosystème crypto, non pas comme des outils criminels, mais comme une **assurance existentielle** contre le contrôle financier totalisant. Investir dans ce secteur, c'est parier sur la liberté, même si les risques réglementaires et la volatilité exigent une prudence maximale.

Sources :

<https://finance.yahoo.com/news/arthur...>

<https://coingape.com/markets/zcash-pr...>

<https://tradingview.com/news/cointele...>

<https://cryptonews.net/news/analytics...>

<https://coinmarketcap.com/academy/art...>

<https://bitcoinist.com/bitcoin-1st-zc...>

<https://crypto.news/zcash-price-gains...>

<https://kucoin.com/news/flash/zcash-p...>

<https://ainvest.com/news/arthur-hayes...>

<https://x.com/naval/status/1973254136394293708>

<https://cointelegraph.com/news/eu-crypto-ban-anonymous-privacy-tokens-2027>

<https://decrypt.co/43451/irs-1-million-contracts-data-firms-crack-monero>

<https://www.coinspeaker.com/monero-xmr-zcash-zec-privacy-coins-delisting/>

<https://coinmarketcap.com/currencies/zcash/>

<https://www.grayscale.com/funds/grayscale-zcash-trust>

<https://x.com/MadarsV/status/1976027131516944856>

<https://x.com/CryptoHayes/status/1982371104082596248>

<https://bitinfocharts.com/comparison/monero-transactions.html#3y>