

Not a PGPZ member? Sign up here:



Weekly Policy Memo: Week of September 21, 2026

<https://community.pgpz.org/updates/2026-09-21-weekly-policy-memo>

Key Takeaways

- SEC Commissioner Hester Peirce argued that federal financial regulation should move away from indiscriminate data collection and toward more targeted, privacy-preserving methods of verification. She questioned whether existing customer identification, transaction monitoring, and reporting requirements create large repositories of personal information without proportionate enforcement benefits, while increasing cybersecurity and confidentiality risks.

Action Items

- No action items.

X Post of the Week:



Cypherpunk 🟡 @cypherpunk · 22h



The "Shielded Bitcoin" paper is a great step forward. More privacy on Bitcoin is good for everyone.

Fun fact: Zerocoin, the paper behind **Zcash**, was first proposed for Bitcoin in 2013. The Bitcoin community passed on it, as zero-knowledge proofs were still immature.

But the solution the paper presents is not competition for Zcash:

- It uses a trusted setup
- There's no consensus enforcement
- No trustless light clients
- Its bridge, usually the most hacked part of these designs, isn't specified yet
- Bitcoin L1 transaction fees
- It doesn't have a >\$7B shielded pool with millions of transactions to hide in
- It's a paper. Zcash has ~10 years in production, pioneered ZK proofs in production, and has the wallets, audits, and hardware support.

More broadly: privacy works best when built into the base layer. Not requiring Bitcoin changing is this design's biggest selling point, and also its biggest drawback.

We're rooting for more privacy on Bitcoin. Financial privacy isn't zero-sum.

💬 36

↻ 95

❤️ 535

📊 30K



Commissioner Peirce Calls for Data Minimization and Zero-Knowledge Verification in Financial Regulation

In remarks at SIFMA's Digital Assets Conference, SEC Commissioner Hester Peirce argued that federal financial regulation should move away from indiscriminate data collection and toward more targeted, privacy-preserving methods of verification. She questioned whether existing customer identification, transaction monitoring, and reporting requirements create large repositories of personal information without proportionate enforcement benefits, while increasing cybersecurity and confidentiality risks. As alternatives, Commissioner Peirce identified attribute-

based credentials, third-party identity verification, and zero-knowledge proofs. She also cautioned against introducing intermediaries into permissionless systems principally to create a point of data collection.

Why it matters for Zcash:

The remarks provide direct support for zero-knowledge proofs, reduced duplication of identity records, and data minimization and supports the proposition that regulatory compliance does not require universal disclosure of identity or transaction history. These concepts may strengthen the public policy case for use of selective disclosure and privacy-preserving credentials instead of routine demands for full viewing keys or permanent public surveillance.

Action Item:

No action item.

Relevant Posts:

