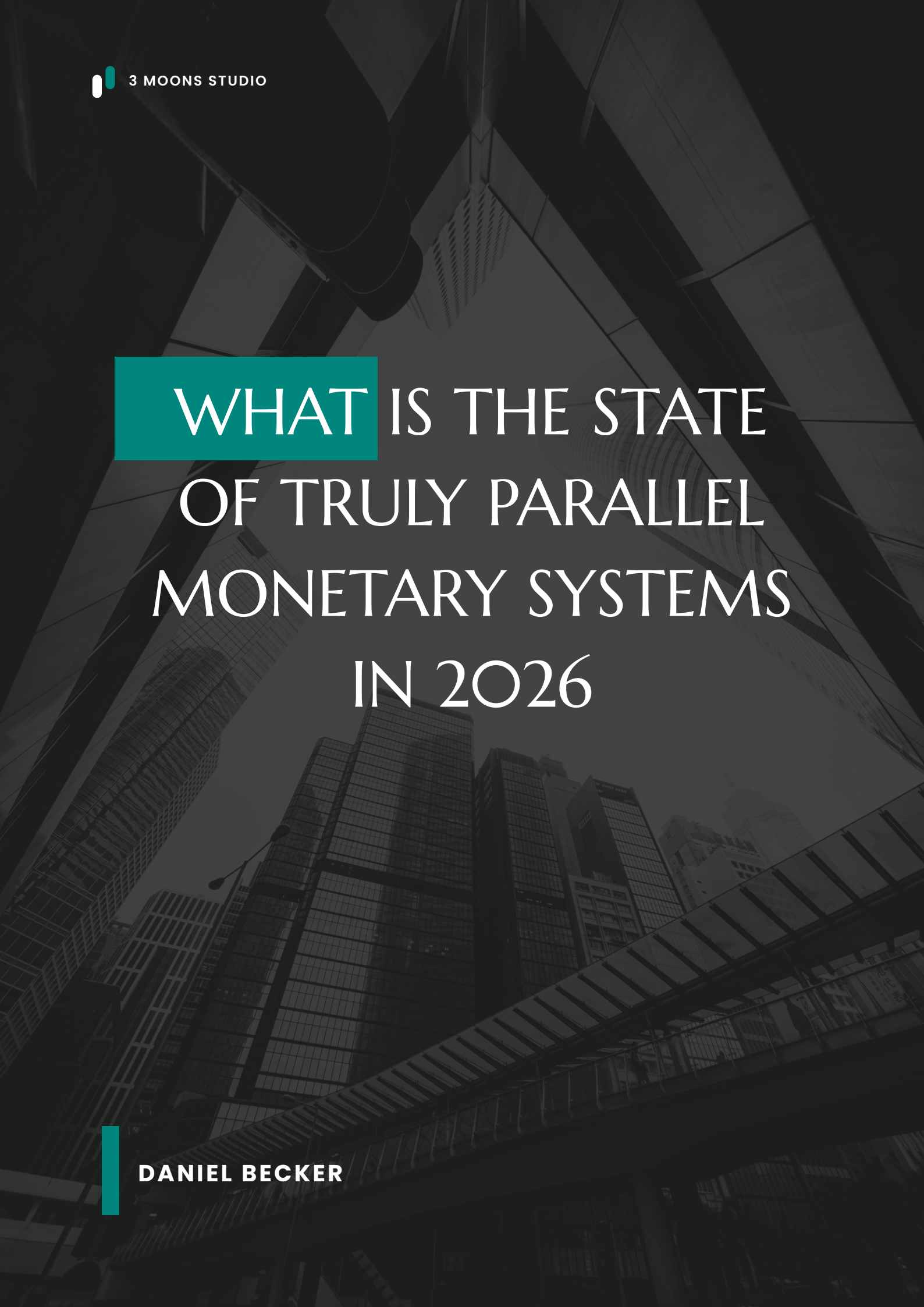
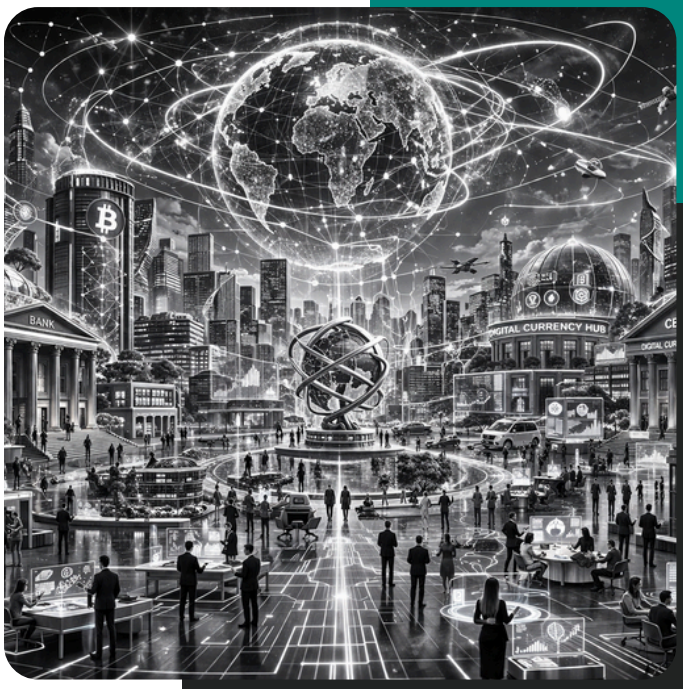


3 MOONS STUDIO

WHAT IS THE STATE OF TRULY PARALLEL MONETARY SYSTEMS IN 2026

DANIEL BECKER

In 2026, truly parallel monetary systems still exist, but they operate under pressure and mostly outside the regulated financial core. The original idea behind crypto was to create money capable of functioning independently of banks, payment processors, and state controlled financial rails. That vision has not disappeared, but its architecture has evolved. Bitcoin increasingly functions as a macro asset integrated into traditional finance through ETFs, custodial platforms, and regulated exchanges. Stablecoins, meanwhile, have become a dominant transactional layer for cross-border payments and digital asset markets, but their degree of monetary independence is structurally limited by partially centralized governance mechanisms.



Major fiat-backed stablecoins are issued by identifiable entities that control minting and redemption processes, maintain reserve assets within the traditional financial system, and retain technical capabilities to restrict transactions through smart contract functions such as address blacklisting or token freezing. These features demonstrate that while stablecoins provide parallel settlement efficiency, elements of custody control, liquidity access, and balance usability remain influenced by centralized actors, including issuers, custodians, and regulated exchanges.

As a result, the strongest fully parallel monetary functions are increasingly concentrated in systems where control over assets and transactions does not depend on permission from regulated intermediaries. These include privacy-oriented cryptocurrencies that reduce transaction traceability, self-custodial wallet architectures that preserve direct control over private keys, bearer-style digital cash models that allow transfer without reliance on account-based identity systems, and community-validated networks where transaction inclusion is determined by distributed consensus rather than centralized payment processors. In these systems, core monetary functions such as custody, transaction validation, and network access remain materially independent from institutional gatekeepers.

If Bitcoin continues evolving primarily into an institutional reserve asset, the parallel monetary function does not disappear; rather, its components become distributed across different technological layers. Monetary parallelism depends on whether users retain credible alternatives for holding assets without custodial intermediation, transferring value without centralized payment authorization, and accessing liquidity without exclusive reliance on regulated banking infrastructure.

In this sense, the parallel system becomes modular: certain layers, such as price reference and liquidity pools, may increasingly interact with traditional finance, while other layers, particularly custody and transaction authorization, remain capable of operating independently. The persistence of parallel monetary capacity therefore depends not on the existence of any single cryptocurrency, but on whether the combined ecosystem continues to provide functional alternatives to centralized custody, permissioned payment routing, and state-dependent settlement infrastructure.

WHAT SATOSHI ACTUALLY PROPOSED

The foundation remains the ideas described in Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi described a system allowing payments to move directly between users without relying on financial institutions.

The purpose was to remove trusted intermediaries and replace them with cryptographic verification. Control of funds was meant to come from control of private keys, not from holding an account with a regulated entity.

The whitepaper does not discuss ETFs, custodians, or institutional wrappers. It describes digital bearer money, meaning ownership depends on possession of cryptographic keys. In that model, a user can store and transfer value without relying on a bank, payment company, or centralized ledger operator.

This is the core benchmark for evaluating whether a system is truly parallel.

If BTC is co-opted, what changes?

Co-optation does not mean Bitcoin stops working. It means that most users interact with Bitcoin through intermediaries. Examples include:

- ***ETFs***
- ***custodial exchanges***
- ***broker platforms***
- ***hosted wallets***
- ***regulated payment providers***

In these structures, users gain price exposure to BTC but lose direct control over the asset. The system begins to resemble traditional finance, where intermediaries manage custody and compliance obligations.

This creates a split; 1. Bitcoin as asset continues growing 2. Bitcoin as independent payment system becomes less central. As this happens, the parallel industry shifts toward tools designed to preserve direct control and transaction privacy.

CURRENT STATE OF PARALLEL CASH

Monero

Monero remains the clearest example of parallel digital cash in 2026. Its system hides transaction history, sender, receiver, and amounts. This protects fungibility, meaning each unit is interchangeable and cannot be blacklisted based on transaction history. Parallel money requires fungibility. If each coin can be traced and evaluated differently, the asset behaves more like a surveilled token than cash.

Monero's main challenge is liquidity pressure from regulation. Several exchanges have removed it in certain jurisdictions, limiting access through compliant platforms.

However, the protocol itself continues functioning and maintains active use.

Because Monero is a privacy coin, many regulated exchanges have delisted it due to AML/KYC compliance pressure. However, XMR is still actively traded, mainly on crypto native platforms and peer-to-peer markets: Kraken (availability depends on jurisdiction), KuCoin, Gate.io, MEXC, HTX. Binance officially delisted Monero on 20 February 2024, removing trading pairs such as XMR/USDT, XMR/BTC and XMR/ETH.

CURRENT STATE OF PARALLEL CASH

Zcash and Zodl

Zcash remains an important privacy protocol using zero-knowledge cryptography. The ecosystem is currently emphasizing shielded transactions through the Zodl wallet, which focuses on private payments and self-custody. Zcash demonstrates that strong privacy technology still exists, although adoption depends heavily on usability and exchange support.

Cashu

Cashu is one of the most important developments in recent years. It creates digital bearer tokens backed by Bitcoin using Chaumian ecash cryptography. These tokens behave more like physical cash:

- instant transfer
- low cost
- strong privacy
- held directly by the user

Cashu shows how Bitcoin liquidity can support parallel cash layers even if the base chain becomes more institutionalized.

CURRENT STATE OF PARALLEL CUSTODY

Fedimint

Fedimint is not a coin and not a company. It is a protocol for federated custody of Bitcoin, combined with a privacy-preserving payment system based on Chaumian e-cash.

Instead of trusting one custodian (exchange, bank, fintech wallet), users trust a group of guardians ("federation" - examples of guardians are: community organizations, NGO's, local finance cooperatives, fintech groups, trusted social networks) who jointly control the Bitcoin backing the system. Trust is therefore distributed, not eliminated.

Fedimint currently uses Bitcoin as the reserve asset.

Users typically obtain BTC through:

- crypto exchanges
- peer-to-peer markets
- existing wallets

Example flow: user buys BTC → transfers BTC to Fedimint federation. After deposit, the system issues Fedimint e-cash tokens representing claims on the pooled BTC.

Important distinction:

Asset	Nature
BTC	base settlement asset
Fediminttokens	private bearer instrument

These tokens:

- can be transferred privately
- do not reveal transaction history publicly
- can be redeemed for BTC later

Transactions between users occur off-chain, using Chaumian blind signatures.

Implications:

- transactions are not publicly traceable on blockchain
- balances are not visible to external observers
- payments are fast and low cost

At any time, users can redeem tokens for BTC. The federation collectively signs the withdrawal transaction. But withdrawal of the underlying Bitcoin reserve requires a predefined threshold of federation members to authorize transactions. If a sufficient number of guardians refuse or fail to validate redemption requests, users may be unable to convert federation-issued tokens back into Bitcoin. The model therefore replaces unilateral control risk typical of centralized custodians with a distributed governance risk, in which intervention requires coordination among multiple independent operators rather than reliance on a single institutional intermediary.

Privacy infrastructure beyond simple payments

RAILGUN

RAILGUN provides zero-knowledge privacy for smart contract transactions on public blockchains such as Ethereum. It functions as a smart contract layer that allows users to interact with decentralized finance applications without publicly exposing wallet balances, transaction amounts, or counterparties. Instead of changing Ethereum itself, RAILGUN acts as an additional privacy layer that users can choose when making transactions.

In practical terms, a user first acquires assets such as ETH or stablecoins (for example USDC or DAI) in a standard wallet. The user then deposits these assets into the RAILGUN smart contract. After the deposit, transactions can be conducted inside the RAILGUN privacy pool using zero-knowledge proofs that confirm the validity of transfers without revealing transaction details on the public blockchain.

For example, when a user trades tokens on Uniswap using a normal wallet, observers can see the wallet address, trade size, token balances, and transaction history. Blockchain analytics companies such as Chainalysis or TRM Labs can analyse these transaction graphs and cluster related addresses. When the same activity is performed through RAILGUN, the trade can still be executed, but the publicly visible data does not reveal the user's balance or transaction relationships.

Earlier privacy tools often required users to convert assets into separate privacy-focused cryptocurrencies, reducing liquidity and limiting compatibility with decentralized finance applications. RAILGUN instead allows users to continue using common Ethereum-based assets while applying privacy protections to transaction data. This allows users to access decentralized exchanges, lending protocols, and liquidity pools without publicly exposing full transaction histories.

Some privacy systems also attempt to address regulatory concerns by allowing users to generate cryptographic proofs showing that deposited funds are not linked to publicly identified illicit addresses, without revealing the full transaction history. This differs from earlier tools such as Tornado Cash, which faced regulatory enforcement partly because transactions could not demonstrate separation from sanctioned funds.

These developments show that privacy infrastructure in the crypto ecosystem is changing in response to regulatory pressure. Instead of operating entirely outside financial oversight, newer tools attempt to reduce unnecessary exposure of transaction data while maintaining compatibility with existing blockchain networks. This indicates that privacy-oriented financial infrastructure is evolving toward models that allow users to retain transactional confidentiality while continuing to access widely used liquidity and payment systems.

Privacy infrastructure beyond simple payments

Aztec Network

Aztec is building infrastructure that allows users to perform programmable transactions on blockchain networks without publicly revealing sensitive data. It focuses on combining smart contracts with zero-knowledge proofs so that transaction logic can be verified without exposing underlying financial information such as balances, counterparties, or transaction conditions.

In practical terms, Aztec allows users to execute smart contract operations while keeping certain inputs private. For example, when interacting with decentralized finance protocols on Ethereum, wallet balances, borrowing positions, and trading strategies are normally visible to anyone analysing blockchain data. With Aztec-based infrastructure, parts of this information can remain confidential while the network can still verify that the transaction follows protocol rules.

One example involves lending protocols. Normally, if a user borrows cryptoassets through a smart contract, observers can see:

- collateral size
- liquidation thresholds
- wallet exposure
- financial strategy

Using Aztec infrastructure, the transaction can be validated without publicly revealing the exact size of collateral or position. The blockchain verifies correctness of the computation, but the detailed financial information remains shielded.

Another example involves payroll or business payments. If a company pays contractors directly using standard blockchain transfers, competitors or analytics firms can observe salary levels and business relationships. Privacy-preserving programmable transactions allow the payment logic to execute while limiting visibility of payment amounts and recipient relationships.

Aztec differs from earlier privacy tools because it focuses not only on private transfers but also on private computation. Earlier systems primarily attempted to hide transaction flows. Aztec extends this concept to programmable logic, allowing complex financial operations to occur without exposing detailed internal parameters on the public ledger.

Privacy infrastructure beyond simple payments

Aztec Network

This approach is still developing and not yet widely adopted compared to major public blockchain infrastructure. However, it demonstrates a direction in which privacy features are being integrated directly into smart contract environments rather than added only as external mixing tools. Instead of separating privacy from functionality, systems such as Aztec attempt to enable private execution of financial logic while maintaining compatibility with blockchain settlement layers.

The development of programmable privacy infrastructure illustrates that the parallel monetary ecosystem is continuing to evolve. Rather than abandoning transparency-based blockchains, new architectures attempt to reduce unnecessary disclosure of sensitive financial data while preserving the verifiability required for decentralized systems to function.

State of the attack on parallel systems.

Pressure on parallel monetary infrastructure continues mainly at the service-provider layer rather than the protocol layer.

Typical pressure points include:

- exchange delistings
- restrictions on hosted wallets
- compliance requirements for service providers
- enforcement actions against operators of privacy tools
- travel rule expansion
- AML obligations applied to crypto intermediaries

Recent regulatory developments in Europe restrict service providers from offering anonymous crypto accounts, especially where anonymity-enhancing assets are involved. This does not ban self-custody software itself, but it limits integration with regulated financial rails.

The practical result is fragmentation: 1. privacy tools still exist and 2. access through mainstream channels becomes harder.

Which systems currently deliver on the Original Promise?

Based on the criteria in the Bitcoin whitepaper, the strongest current examples are:

- Monero delivers private peer-to-peer cash.
- Cashu delivers bearer-style digital cash backed by Bitcoin.
- Fedimint delivers distributed custody outside large institutions.
- Zcash continues advancing zero-knowledge private payments.
- RAILGUN provides private transaction infrastructure for smart contract ecosystems.
- Aztec represents an emerging architecture for private computation and settlement.

No single system fully replaces Bitcoin's original ambition, but together they show that the parallel monetary sector continues evolving.

Overall,

Parallel monetary systems in 2026 are not dead, but they are no longer concentrated in one dominant protocol. Bitcoin increasingly functions as a global collateral asset integrated into regulated finance. Parallel monetary functionality is now distributed across privacy coins, ecash systems, and federated custody models.
The original idea described by Satoshi, peer-to-peer money independent of trusted intermediaries, is still being implemented, but through multiple specialized systems rather than one universal network.
The sector remains technically active, politically sensitive, and strategically relevant.