DAPA

Privacy-Native Blockchain Currency

PRIVACY & COMPLIANCE POSITION PAPER

Version 1.0 | April 2026

Executive Summary

DAPA is a privacy-native blockchain currency built on a blockDAG architecture, utilising Twisted ElGamal homomorphic encryption. This document sets out DAPA's position on the relationship between financial privacy and regulatory compliance — and demonstrates that these two objectives are not in conflict.

DAPA provides financial privacy by default, in the same way that a bank account is private by default. Privacy is not the same as anonymity, and DAPA does not provide anonymity from legal process. Users of DAPA retain the full ability to disclose their transaction history to tax authorities, auditors, legal counsel, or any other authorised party at their discretion.

Core Position:
DAPA provides financial privacy to ordinary people and businesses. It is not designed to facilitate criminal activity. Users can comply fully with their legal and tax obligations while using DAPA, and the protocol includes native audit capability for authorised disclosure.

1. The Case for Financial Privacy

1.1 Privacy is a Fundamental Right

Financial privacy is a well-established legal concept recognised across democratic jurisdictions worldwide. The European Union's General Data Protection Regulation (GDPR), the United Kingdom's Data Protection Act 2018, and equivalent legislation in dozens of countries recognise that individuals have a legitimate right to control who can access their personal financial information.

Ordinary financial instruments already provide this privacy by default. A bank account is not publicly readable. A salary payment is not announced to neighbours. A business invoice is not broadcast to competitors. DAPA applies this same expectation of privacy to blockchain-based currency — nothing more.

1.2 The Distinction Between Privacy and Anonymity

The most important distinction in any discussion of privacy coins is the difference between privacy and anonymity:

Concept	What it means for DAPA
Financial Privacy	Transactions are not publicly visible on an open ledger. Balances are encrypted. Third parties cannot see your financial activity without authorisation.
Financial Anonymity	No party can ever determine the identity behind transactions, even under legal compulsion. DAPA does NOT provide this.
Selective Disclosure	The account holder can choose to reveal transaction history to any authorised party — tax authority, auditor, regulator, legal counsel — using cryptographic proof.

DAPA is a privacy system, not an anonymity system. The distinction matters enormously from a regulatory perspective.

1.3 Why Transparent Blockchains Create Harm

Fully transparent blockchains such as Bitcoin create privacy risks that are not present in traditional banking. On a transparent blockchain:

- Every transaction is permanently and publicly visible to anyone in the world.
- Wallet balances are exposed to any party who knows an address.
- Transaction graphs can be analysed to profile individuals' spending, income, and business relationships.
- Businesses expose their commercial relationships and revenue to competitors simply by transacting on-chain.
- Individuals in high-risk jurisdictions may face physical danger if wealth is publicly visible.

These are not hypothetical risks. Chain analysis companies sell services specifically designed to profile individuals from transparent blockchain data. DAPA addresses these harms by encrypting balances and transaction amounts by default.

2. How DAPA's Technology Works

2.1 Twisted ElGamal Homomorphic Encryption

DAPA uses Twisted ElGamal encryption — a modern cryptographic scheme that allows transaction amounts and account balances to be encrypted while still permitting the network to verify that transactions are mathematically valid, without revealing the underlying amounts.

This is a meaningful technical advance over earlier privacy coin approaches. The encryption is:

- Mathematically proven — not security through obscurity, but cryptographically sound.
- Efficient — transactions can be verified quickly without decrypting the underlying amounts.
- Auditable — the account holder holds keys that permit selective decryption and disclosure.

2.2 blockDAG Architecture

DAPA is built on a blockDAG (Directed Acyclic Graph) architecture rather than a traditional linear blockchain. This allows multiple blocks to be processed in parallel, providing higher throughput and more resilient network performance. The privacy encryption operates at the protocol level across this architecture.

2.3 Native Audit Capability — View Keys

This is the most important feature from a compliance perspective.

DAPA's cryptographic structure gives every account two distinct access levels:

Key Type	Capability
Private Spend Key	Full control — can send funds, decrypt balances. Held only by the account owner.
Public Key / View Key	Read-only access — can verify transaction history and prove balances to authorised parties. Can be shared without any risk of fund loss.

This means a DAPA account holder can provide their accountant, tax authority, or legal counsel with a view key that allows complete verification of their transaction history — without that party ever gaining the ability to move funds.

Practical Example:
A business using DAPA for payments gives its accountant a view key at year end. The accountant can verify every payment received and sent, confirm balances, and produce accurate tax filings — all without the business having to surrender control of funds or expose itself to the public blockchain.

This capability is native to the DAPA protocol. It is not a workaround or a compromise — it is built into the cryptographic design from the ground up.

3. Compliance Framework

3.1 Tax Reporting

DAPA users are responsible for their own tax obligations in their respective jurisdictions. DAPA does not prevent, hinder, or make more difficult the reporting of taxable income or capital gains arising from cryptocurrency transactions.

Using the view key mechanism, users can:

- Produce a complete record of all transactions for any time period.
- Verify the DAPA value of transactions at the time they occurred.
- Share this record with tax authorities or accountants in a verifiable, cryptographically proven format.
- Comply fully with Self Assessment, HMRC, IRS, or equivalent reporting requirements.

3.2 Anti-Money Laundering (AML) Considerations

DAPA's privacy protections apply to balances and transaction amounts on the public ledger. They do not prevent law enforcement or regulators from:

- Obtaining transaction records through lawful legal process directed at the account holder.
- Requesting voluntary disclosure from account holders under investigation.
- Working with regulated exchanges and payment processors who operate KYC/AML programmes.

DAPA does not operate as a mixer, tumbler, or anonymisation service. It is a currency with private balances — the equivalent of a private bank account rather than an untraceable cash dispensing machine.

3.3 FATF Travel Rule

The Financial Action Task Force Travel Rule requires Virtual Asset Service Providers (VASPs) — exchanges, custodians, and payment processors — to share originator and beneficiary information for transactions above threshold values. This obligation sits with the VASPs, not with individual users of a currency.

DAPA is compatible with VASP-level Travel Rule compliance. Exchanges and custodians listing DAPA can implement Travel Rule requirements at their platform level, in the same way they do for Bitcoin, Ethereum, or any other cryptocurrency.

3.4 Regulated Payment Processing — Genesis Sale

The DAPA Genesis Sale was conducted exclusively through regulated payment processors: PayPal, Stripe, and Payoneer. Each of these companies operates under strict financial services regulations and conducts its own KYC and AML due diligence before onboarding any merchant.

> **Verification of Legitimacy:**
> *PayPal, Stripe, and Payoneer are regulated financial institutions. They do not process payments for projects they determine to be fraudulent or non-compliant with financial regulations. The fact that these processors onboarded and processed payments for the DAPA Genesis Sale is independent third-party evidence of the project's legitimacy.*

Furthermore, these processors provide buyer protection and chargeback mechanisms. Anonymous or fraudulent projects avoid regulated processors precisely because chargebacks and regulatory oversight create accountability. DAPA's choice to use regulated processors was a deliberate signal of good faith.

4. Comparison with Other Privacy Approaches

DAPA's privacy model can be understood in context of other approaches in the cryptocurrency space:

Project	Privacy Approach & Compliance Position
Bitcoin / Ethereum	Fully transparent — no balance or transaction privacy. All data publicly visible. No compliance advantage for privacy.
Monero (XMR)	Ring signatures and stealth addresses. Strong privacy

	but no selective disclosure mechanism. No view key for authorised audit. Increasingly delisted by exchanges under regulatory pressure.
Zcash (ZEC)	zk-SNARKs with optional shielded pools. View keys available but privacy is opt-in, not default. Strong academic backing and regulatory engagement.
DAPA	Twisted ElGamal homomorphic encryption with privacy by default. Native view key / selective disclosure mechanism. blockDAG architecture. Genesis Sale through regulated processors. Modern Rust codebase.

DAPA occupies a distinct position: privacy by default (stronger than Zcash's opt-in model) combined with native audit capability (absent from Monero) built on more modern cryptographic foundations than either.

5. DAPA's Public Commitments

DAPA makes the following public commitments with respect to privacy and compliance:

5.1 We will not position DAPA as a tool for illegal activity.

DAPA is designed for ordinary people and businesses who have a legitimate interest in financial privacy. It is not marketed to, and we actively do not support, any use of DAPA to facilitate crime, tax evasion, sanctions evasion, or money laundering.

5.2 We support user compliance with legal obligations.

We will maintain documentation and tooling that helps DAPA users understand and meet their tax and reporting obligations in their respective jurisdictions. The view key mechanism will be made accessible through all official DAPA wallets.

5.3 We will engage proactively with regulators.

DAPA commits to constructive engagement with regulators and exchange compliance teams. We will respond to reasonable requests for information and will not obstruct legitimate regulatory enquiries.

5.4 We will pursue third-party security audits.

DAPA commits to commissioning independent cryptographic and security audits of the protocol. Audit results will be published publicly. This is a standard of transparency that exceeds many projects in the cryptocurrency space.

5.5 We will maintain regulated payment processing.

DAPA will continue to use regulated payment processors for any fiat currency transactions related to the project, maintaining the accountability and buyer protection that regulated processors provide.

6. Conclusion

Financial privacy is a legitimate and important right for individuals and businesses. DAPA provides this privacy through technically advanced cryptography — Twisted ElGamal homomorphic encryption on a blockDAG architecture — while maintaining the full ability for users to comply with their legal obligations.

The key distinction that regulators and exchanges should understand is this: DAPA is private, not anonymous. The account holder retains control over disclosure. Privacy does not mean hiding from the law — it means that your financial life is your own business, shared with whom you choose, on your terms.

DAPA has demonstrated good faith through its use of regulated payment processors, its commitment to audit capability, and its willingness to engage openly with compliance requirements. We believe DAPA represents what modern private currency can and should look like — responsible, technically sound, and fully compatible with a lawful financial system.

For compliance enquiries, exchange listing applications, or regulatory engagement:

Website: dapahe.com | dapacurrency.com

This document may be freely shared with regulators, exchange compliance teams, legal counsel, and media.

Appendix — Glossary of Terms

Term	Definition
blockDAG	Directed Acyclic Graph blockchain architecture allowing parallel block processing for higher throughput than traditional linear chains.
Twisted ElGamal Encryption	A homomorphic encryption scheme allowing mathematical operations on encrypted values —

	enabling transaction verification without revealing amounts.
Homomorphic Encryption	Encryption that allows computation on ciphertext, producing an encrypted result that matches the result of operations on the plaintext.
View Key	A cryptographic key that permits read-only access to an account's transaction history. Cannot be used to move funds. Shareable with auditors and tax authorities.
VASP	Virtual Asset Service Provider. An exchange, custodian, or payment processor regulated under financial services law.
FATF Travel Rule	Financial Action Task Force requirement for VASPs to share originator and beneficiary information on qualifying transactions.
KYC / AML	Know Your Customer / Anti-Money Laundering. Regulatory requirements for financial services providers to verify customer identities and monitor for suspicious activity.
ECDLP	Elliptic Curve Discrete Logarithm Problem. The mathematical foundation of DAPA's cryptographic security.
Genesis Sale	DAPA's initial coin distribution event, conducted through regulated payment processors PayPal, Stripe, and Payoneer.