DAPA

Privacy-Native Blockchain Currency

WHITEPAPER

Version 2.0 | April 2026

Abstract

DAPA is a privacy-native digital currency operating on a standalone blockDAG blockchain.
It uses Twisted ElGamal homomorphic encryption to provide confidential balances and
transaction amounts by default, while supporting selective disclosure for compliance purposes.
Built in Rust on an open-source protocol base, DAPA extends the foundation with additional privacy infrastructure, a multi-platform wallet ecosystem, and a regulated genesis distribution. This paper describes the technical architecture, economic model, compliance approach, and development roadmap of the DAPA protocol.

1. Introduction

1.1 The Problem with Transparent Blockchains

Bitcoin introduced the concept of decentralised digital currency in 2009. Its blockchain is fully transparent — every transaction, every balance, every address is permanently recorded on a public ledger accessible to anyone. While this transparency was a deliberate design choice aimed at achieving trustless consensus, it created a fundamental problem: public blockchains provide less financial privacy than traditional banking.

When a person makes a bank transfer, the transaction is visible to the sending bank, the receiving bank, and to regulators with appropriate legal authority. It is not visible to the person's employer, their neighbours, their competitors, or any other party without a legal basis for access. This is the normal expectation of financial privacy that people have always had.

On a transparent blockchain, none of these protections exist. A single known address exposes the complete transaction history and current balance of that account to any party in the world. Chain analysis firms have built multi-million dollar businesses specifically exploiting this transparency to profile individuals, track funds, and sell intelligence on blockchain users' financial behaviour.

The core problem:

Transparent blockchains provide less financial privacy than cash, less than traditional banking, and less than the legal standard in most democratic jurisdictions. A technology intended to give individuals financial sovereignty instead exposed their financial lives to the world.

1.2 Existing Privacy Solutions and Their Limitations

Several projects have attempted to address the privacy problem in blockchain:

Project	Approach & Limitation
Monero (XMR)	Ring signatures and RingCT provide strong privacy but offer no selective disclosure mechanism. Users cannot prove transaction history to an auditor or tax authority. Increasingly delisted from regulated exchanges. Written in legacy C++.
Zcash (ZEC)	zk-SNARKs with optional shielded pools and view keys. Privacy is opt-in — the majority of ZEC transactions are fully transparent. The shielded pool has seen limited adoption despite technical capability.
Ethereum L2 Privacy	Various Layer 2 solutions attempt to add privacy to Ethereum. These inherit the complexity and gas costs of the base layer and require trust in additional smart contract infrastructure.
Grin / Beam	MimbleWimble protocol provides transaction graph privacy but balances are not fully hidden. Limited ecosystem and wallet support.
DAPA	Twisted ElGamal homomorphic encryption with privacy by default. Native view key mechanism for selective disclosure. blockDAG architecture. Modern Rust codebase. Regulated genesis distribution.

1.3 The DAPA Approach

DAPA takes a different position: privacy should be the default, not the exception. Every DAPA account has an encrypted balance. Every DAPA transaction has a confidential amount. The network can verify that transactions are mathematically valid without ever seeing the underlying values.

Critically, DAPA does not sacrifice auditability for privacy. The protocol includes a native view key mechanism that allows an account holder to grant read-only access to their transaction history to any authorised party. This resolves the tension between privacy and compliance that has hampered other privacy coins.

2. Technical Architecture

2.1 blockDAG Consensus

DAPA operates on a blockDAG (Directed Acyclic Graph) architecture rather than a traditional linear blockchain. In a conventional blockchain, blocks are produced sequentially — each block references exactly one parent. This creates a bottleneck: only one block can be added at a time, and blocks produced simultaneously compete to be included, with the loser discarded as an orphan.

In a blockDAG, multiple blocks can be produced and referenced simultaneously. Rather than one block referencing one parent, each new block can reference multiple recent blocks as its parents. This has several important properties:

- Higher throughput — the network is not serialised to a single block producer at a time.
- Reduced orphan rate — blocks produced simultaneously are incorporated rather than discarded.
- Better latency tolerance — the network handles variable propagation delays more gracefully.
- More decentralised mining — smaller miners have better odds of contributing blocks that count.

DAPA's blockDAG consensus resolves conflicts through a deterministic ordering algorithm that produces a consistent total ordering of all transactions across the DAG, enabling UTXO-like balance tracking despite the parallel block structure.

2.2 Twisted ElGamal Homomorphic Encryption

The core cryptographic innovation in DAPA is the use of Twisted ElGamal encryption for account balances and transaction amounts.

2.2.1 Standard ElGamal Encryption

ElGamal encryption is a public-key cryptographic system based on the Diffie-Hellman key exchange. In its standard form, it encrypts a value m as a pair (rG, mG + rPK) where G is the

elliptic curve generator point, r is a random nonce, and PK is the recipient's public key. The recipient can decrypt by computing mG = (mG + rPK) - r·PK using their private key.

2.2.2 The Twisted Variant

Twisted ElGamal modifies this scheme to enable efficient homomorphic addition. In the twisted variant, a value m is encrypted as (rG, m·G + r·PK). This modification means that two ciphertexts can be added together to produce the encryption of the sum of their plaintexts — without decryption. This property is essential for blockchain validation:

Homomorphic property:

Enc(a) + Enc(b) = Enc(a + b)

The network can verify that inputs equal outputs in a transaction without knowing the values of either. Transaction validity can be proven cryptographically without revealing amounts.

2.2.3 Balance Decryption — ECDLP

Encrypted balances are stored as elliptic curve points. Decrypting a balance requires solving the Elliptic Curve Discrete Logarithm Problem (ECDLP) — finding the scalar m such that the stored point equals m·G. This is computationally infeasible in general, but practical within the range of valid balances using precomputed lookup tables.

DAPA wallets generate or download precomputed tables (approximately 333MB at the L1_FULL level) that enable balance decryption within seconds for any value in the valid range. These tables are specific to DAPA's elliptic curve parameters and cannot be reused to attack other systems.

2.3 Account Model

DAPA uses an account-based model rather than UTXO. Each address maintains a single encrypted balance for each asset. Transactions update balances using homomorphic operations, allowing the network to verify balance changes without decrypting them.

Key properties of the account model:

- Balances are stored as ElGamal ciphertexts — commitment and handle pairs.
- Stable balances are confirmed after a configurable number of blocks (~28 block lag).
- Nonces prevent double-spend without requiring UTXO tracking.
- The asset system supports multiple asset types on the same chain.

2.4 View Keys and Selective Disclosure

Every DAPA account has two asymmetric key pairs:

Key	Properties
Private Spend Key	Derived from the account seed phrase. Required to authorise outgoing transactions. Must be kept secret. Cannot be derived from any other key.
Public Key	Derived from the private spend key via elliptic curve multiplication. Used as the account's public identifier. Can be shared freely.
View Key (derived)	A read-only key derived from the account's cryptographic material. Allows verification of incoming and outgoing transactions and decryption of balance history. Cannot authorise spending. Safe to share with auditors, accountants, or tax authorities.

The view key mechanism resolves the primary regulatory objection to privacy coins. Users of DAPA can provide full transaction transparency to any authorised party without surrendering control of funds and without exposing themselves to the entire world.

2.5 Cryptographic Foundations

DAPA's cryptography is built on the Ristretto255 group — a prime-order group constructed from Curve25519. Ristretto255 provides:

- A prime-order group free from cofactor-related vulnerabilities.
- Efficient 32-byte point encoding with strong uniformity properties.
- Wide adoption — the same curve family underlies Ed25519 signatures used across the industry.

The Twisted ElGamal scheme operates on this group, with security resting on the hardness of the Decisional Diffie-Hellman problem in Ristretto255 — a well-studied assumption with strong academic consensus.

2.6 Transaction Construction

A DAPA transaction is constructed as follows:

1. The sender's wallet fetches their current stable balance ciphertext and nonce from the network.
2. The sender specifies recipient addresses and amounts.
3. The wallet constructs encrypted transfer ciphertexts for each recipient using the recipient's public key.
4. A range proof (or equivalent validity proof) is generated demonstrating that amounts are non-negative and within valid range, without revealing the amounts.

5. The transaction is signed with the sender's private key and broadcast to the network.
6. Nodes verify the cryptographic proofs, update encrypted balances homomorphically, and record the transaction.

The minimum transaction fee is 0.00125000 DAPA (125,000 atomic units). Fees are publicly visible as they must be paid in the native asset.

3. Wallet Ecosystem

DAPA is committed to providing a complete, high-quality wallet experience across all major platforms. Privacy technology is only valuable if it is accessible.

Wallet	Status & Description
Zodiac Mobile (Android)	Production — v1.0.0. Flutter/Rust cross-platform wallet with full transaction support, QR scan-to-pay, backup PDF generation, and precomputed table bundling for instant balance decryption.
DAPA Web Wallet	Production — webwallet.dapahe.com. React/WASM browser wallet with full send/receive, transaction history, and address book. No installation required.
CLI Wallet	Production — included with node distribution. Full-featured command-line wallet for advanced users, miners, and server environments.
Zodiac iOS	Roadmap — Flutter codebase enables iOS build with minimal additional work.
Desktop Wallet	Roadmap — native desktop application for Windows, macOS, and Linux.
DapaPay	In development — payment platform enabling merchants to accept DAPA, with view key integration for accounting and compliance.

4. Economic Model

4.1 Supply

DAPA has a maximum supply of 800,000,000 coins with a decreasing emission curve designed for long-term sustainability. A genesis premine of 52,000,000 DAPA was allocated at launch to fund development, exchange listings, ecosystem grants, and operations. Early miners who supported the chain during its launch phase received an elevated block reward of

19 DAPA per block — a deliberate incentive to bootstrap the network and reward those who took the earliest risk on the project.

Parameter	Value
Maximum Supply	800,000,000 DAPA
Genesis Premine	52,000,000 DAPA — development, listings, ecosystem, operations
Early Miner Reward	19 DAPA per block — rewarded to miners who supported the chain at launch
Atomic Unit	1 DAPA = 100,000,000 atomic units (8 decimal places)
Block Reward	Decreasing emission curve — current reward approximately 9.49 DAPA per block
Minimum Fee	0.00125000 DAPA (125,000 atomic units)
Mining Algorithm	XelisHash v3 — ASIC-resistant PoW, egalitarian design, CPU and GPU compatible

4.2 Genesis Sale

The DAPA Genesis Sale distributed coins to early supporters at a price of $0.12 USD per DAPA, with a 50% bonus allocation in Tier 1. The sale was conducted exclusively through regulated payment processors:

- PayPal — full buyer protection and chargeback rights
- Stripe — regulated card processing with KYC/AML compliance
- Payoneer — international business payment processing

The use of regulated processors was a deliberate choice providing accountability, buyer protection, and compliance with financial regulations. It also serves as independent verification of the project's legitimacy — regulated processors conduct their own due diligence before onboarding merchants.

4.3 Premine — Transparency Statement

The 52,000,000 DAPA genesis premine is one of the most scrutinised aspects of any new blockchain project, and DAPA addresses it directly rather than minimising it. Premines exist to fund the real costs of building, launching, and growing a blockchain ecosystem. Without development funding, security audits, infrastructure, and exchange listing fees, no project reaches sustainability.

The DAPA premine is allocated across the following purposes:

- Development fund — ongoing protocol development, security audits, infrastructure costs
- Exchange listing reserve — fees and liquidity requirements for exchange integrations
- Ecosystem grants — incentives for developers building applications on DAPA
- Marketing and community — promotion, events, forum presence, media relations
- Operational reserve — server infrastructure, legal counsel, compliance costs

Early miners who supported the chain during its genesis period received 19 DAPA per block — a higher reward than the current emission rate. This was intentional: bootstrapping a new blockchain requires incentivising early participants to commit hashrate when the network and its value are unproven. Those early miners took a real risk and were compensated for it.

DAPA believes that transparency about these decisions is more valuable than hiding them. The premine and early miner rewards are documented facts. The project's long-term credibility rests on delivering on its roadmap, not on obscuring its launch structure.

5. Compliance and Regulatory Position

DAPA's approach to compliance is covered in detail in the separately published Privacy & Compliance Position Paper. A summary of key positions:

- **DAPA provides financial privacy, not criminal anonymity. These are meaningfully different.**
- Users retain full ability to disclose transaction history via view keys for tax and legal compliance.
- DAPA does not prevent, hinder, or complicate the meeting of legal obligations.
- VASPs (exchanges, custodians) can implement Travel Rule and KYC/AML requirements at the platform level.
- DAPA commits to engaging constructively with regulators rather than opposing regulatory oversight.
- Third-party security audits will be commissioned and results published publicly.

Core compliance statement:

DAPA is private, not anonymous. The account holder controls disclosure. Privacy does not mean hiding from legitimate legal process — it means your financial life is your own business, shared with whom you choose, on your terms.

6. Node Infrastructure

The DAPA network currently operates across multiple geographically distributed nodes providing redundancy and decentralisation:

- node.paymetc.com — primary public RPC node
- node.dapahe.com — secondary public RPC node
- index.dapahe.com — transaction indexer for wallet history queries
- Block explorer — real-time network state, transaction lookup, peer map

Node software is written in Rust and distributed as precompiled binaries for Linux. The daemon exposes a JSON-RPC API for wallet integration, block querying, and transaction submission. WebSocket connections are supported for real-time event streaming.

The network supports both P2P peer discovery and static peer configuration. Nodes communicate on port 20100 (P2P) and expose RPC on port 20101.

7. Development Roadmap

Phase 1 — Foundation (Complete)

- Mainnet blockchain launch with genesis block and premine
- CLI wallet with full transaction support
- Web wallet (webwallet.dapahe.com) with WASM cryptography
- Zodiac mobile wallet v1.0.0 (Android)
- Block explorer
- Public node infrastructure (2+ nodes)
- Transaction indexer (index.dapahe.com)
- Genesis Sale via regulated processors (PayPal, Stripe, Payoneer)
- Privacy & Compliance Position Paper

Phase 2 — Ecosystem Growth (Active)

- Exchange listings — Tier 2 and Tier 3 exchanges
- Zodiac iOS wallet
- DapaPay merchant payment platform
- View key interface in all official wallets
- Third-party cryptographic security audit
- Developer documentation and SDK
- Community grant programme

Phase 3 — Maturity

- Tier 1 exchange listings
- Desktop wallet (Windows, macOS, Linux)
- Smart contract or token issuance capability
- Decentralised exchange (DEX) integration
- Additional asset support
- Hardware wallet integration (Ledger / Trezor)
- Regulator engagement — UK FCA, EU MiCA framework

---

8. Team and Transparency

DAPA is developed by a core team with deep expertise in Rust systems programming, blockchain architecture, cryptography, and full-stack application development. The project maintains transparency through:

- Open source protocol code available for review
- Public node infrastructure with visible network statistics
- Published position papers and documentation
- Active community presence on established forums
- Genesis Sale conducted through regulated processors providing third-party accountability
- Commitment to third-party security audits with public results

For team enquiries, technical questions, and partnership discussions: support@dapahe.com

---

9. Conclusion

DAPA addresses a genuine and important problem: the absence of financial privacy on public blockchains. It does so with modern cryptographic tools — Twisted ElGamal homomorphic encryption on a blockDAG architecture — that provide privacy by default without sacrificing the auditability that compliance requires.

The design choices in DAPA reflect a considered position on the relationship between privacy and compliance. Privacy and accountability are not opposites. A private bank account is still accountable. A DAPA account is still auditable, by the people its holder chooses to share it with, on the holder's terms.

DAPA is not the first privacy coin. It is, however, the most modern — built on better cryptography, in a safer programming language, with a more complete wallet ecosystem, and with a compliance posture that positions it for long-term acceptance rather than regulatory conflict.

Your money. Your business. Built to last.

dapahe.com | dapacurrency.com

DAPA Whitepaper v2.0 — April 2026

References & Further Reading

Base Protocol — The open-source protocol from which DAPA is built and extended.

Twisted ElGamal Encryption — Cramer, R., Shoup, V. (2003). Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack.

Ristretto255 — Decaf/Ristretto group construction. ristretto.group

blockDAG Consensus — PHANTOM / GHOSTDAG protocols for blockDAG ordering.

FATF Travel Rule — FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (2019, updated 2021).

DAPA Privacy & Compliance Position Paper — Published separately. Available at dapahe.com.

DAPA Brand Manifesto — Published separately. Available at dapahe.com.