DEBITMYDATA / DMD

Proof-of-Work, Cyclical Issuance & Agentic Payments

DebitMyData (DMD) Whitepaper

Version 2.0 • October 14, 2026

A long-term SHA-256 Proof-of-Work blockchain with a proposed application-layer integration for autonomous-agent payments, decentralized identity registration, and approved multi-asset settlement.

DOCUMENT STATUS

Public-facing technical review draft. Existing protocol behavior and production deployment statuses must be confirmed against the current DMD Core release, source code, and service tests before publication. Roadmap features are not representations of live services.

debitmydata.io | github.com/DebitMyData-PoW/DebitMyData-PoW-Core

Document Overview

This edition retains the original Whitepaper's emphasis on long-term Proof-of-Work incentives and broadens it to describe DebitMyData's planned Agentics payment infrastructure. The application layer enables payment requests, settlement verification, decentralized identity issuance, and authorized services without changing the underlying consensus rules merely by deploying a gateway.

Item	Details
Document	DebitMyData PoW Whitepaper
Version / date	2.0 / October 14, 2026
Primary topic	Cyclical Proof-of-Work issuance and autonomous-agent payment interoperability
Protocol and service status	Core PoW network: operational; Agent Gateway and new payment services: planned / under development
Prepared from	Original DMD Whitepaper and Preska Thomas's September 18, 2026 payment directive

Contents

Abstract 3
1 Introduction 3
2 Design Goals 3
3 Blockchain Overview 4
4 Monetary Policy and Supply Epochs 4
5 Mining, Network Security and Difficulty 5
6 Transactions, Scaling and Accessibility 6
7 Wallets and Network Infrastructure 6
8 Digital Artifacts and Data Anchoring 7
9 The Agentic Economy and DMD 7
10 Agent Gateway and Payment Architecture 8
11 DID Registration and Payment Lifecycle 9
12 MCP, x402 and Service Discovery 10
13 Security, Privacy and Operational Controls 10
14 Economic and Technical Risks 11
15 Development Roadmap 11
16 Conclusion 12
Appendix A Frequently Asked Questions 12
Appendix B References and Editorial Verification 13

Abstract

DebitMyData (DMD) is a Proof-of-Work blockchain designed to examine the long-term sustainability of mining incentives across generations. It uses SHA-256 mining, a target block interval of 150 seconds, and an issuance model organized around recurring supply epochs rather than a one-time, permanently exhausted subsidy schedule.

The network's core proposition is that continued, predictable miner rewards can remain part of decentralized security over long periods. This is an economic design choice, not a guarantee of mining profitability, decentralization, hashrate, or price stability.

DMD is also being developed as a native payment and participation rail within the broader DebitMyData Agentics ecosystem. A proposed Agent Gateway will allow eligible autonomous agents and other participants to discover approved services, request price quotes, pay through supported wallets and assets, demonstrate control of the relevant identity key, and receive a decentralized identifier (DID) or other service entitlement after independently verified settlement.

Agentic payments and DID issuance are application-layer capabilities. They do not, by themselves, require a change to DMD's block validation, mining algorithm, or monetary policy. Integration will be phased, with native DMD payments and compatible x402-based USDC payments prioritized, followed by carefully approved additional assets and networks.

1. Introduction

Most Proof-of-Work blockchains begin with a high mining subsidy and reduce it through scheduled halvings. Over time, their security budgets can become more dependent on transaction fees. DebitMyData explores an alternative approach in which predictable subsidy cycles are intended to preserve an ongoing incentive for miners far into the future.

DMD combines this long-term settlement infrastructure with an emerging practical use case: machine-to-machine payments. Autonomous agents may need verifiable identities and controlled access to paid digital resources without requiring every payer to adopt one wallet or blockchain.

The DebitMyData Agent Gateway is designed to connect these services to approved payment networks, including the native DMD chain. Independent validation of incoming payments, explicit pricing, and controller-key proof are intended to provide a consistent entitlement-issuance process across supported payment rails.

2. Design Goals

- Preserve an open SHA-256 Proof-of-Work network with transparent, deterministic consensus rules.
- Maintain a predictable mining-incentive schedule over multiple generations.
- Provide stable target block intervals and difficulty responsiveness as hashrate changes.
- Keep private keys with users of non-custodial wallets and isolate sensitive node administration from public services.
- Make native DMD available as a payment rail for autonomous agents, organizations, and individuals.
- Support approved multi-asset payments through explicit quotes and independent settlement verification.
- Offer DID registration and service entitlements without compromising blockchain consensus or treasury controls.
- Disclose implementation status and technical risks rather than presenting future work as completed.

3. Blockchain Overview

Parameter	DMD design / current stated value
Name and ticker	DebitMyData Proof-of-Work (DMD)
Consensus / mining	Proof-of-Work / SHA-256

Target block interval	150 seconds
Initial block subsidy	35 DMD
Subsidy halving interval	300,000 blocks
Coinbase maturity	250 blocks
Difficulty algorithm	LWMA-3, 60-block averaging window; activation documented at height 120
Issuance objective	Approximately 21 million DMD per supply epoch; not a permanent lifetime 21M cap
Nominal epoch duration	Approximately 45.66 years at target block interval
Core generation	DMD Core 1.3.x, rebased on Bitcoin Core 31.0 (project release context)
Transport	BIP324 v2 encrypted transport capability
Light-wallet connectivity	Electrum-based infrastructure and non-custodial applications
P2P Port	18556
RPC Port	18557

4. Monetary Policy and Supply Epochs

4.1. The cyclical issuance model

DebitMyData describes a recurring issuance design. Within an epoch, rewards begin at the defined starting subsidy and halve every 300,000 blocks. When an epoch ends, the monetary design calls for a new issuance cycle according to the prescribed consensus schedule.

The figure of approximately 21 million DMD is a per-epoch issuance objective, not a permanently fixed lifetime cap. Coins already in circulation do not disappear merely because an issuance epoch completes. Aggregate supply can therefore grow across successive epochs, according to the actual implemented rules.

4.2. Approximate schedule and transparency

At a target of 150 seconds per block, 300,000 blocks correspond to roughly 521 days (1.43 years). An approximately 46-year epoch is consistent with a halving sequence spanning roughly 32 such intervals, subject to actual block timing, subsidy rounding, and the exact epoch-reset logic in the node implementation.

The intended benefit is rule-based predictability: users and miners can inspect an objective, code-defined reward schedule rather than rely on discretionary monetary decisions. This predictability does not prevent dilution of a holder’s share of all outstanding units in later epochs.

4.3. Economic tradeoffs

Continuing subsidy issuance offers a possible long-run supplement to transaction fees. It also creates ongoing monetary expansion and requires users to evaluate long-run supply, demand, and purchasing-power risk. Security depends on incentives and competitive mining behavior, not merely on the existence of new rewards.

CONSENSUS VERIFICATION REQUIRED

Prior to treating this Whitepaper as an authoritative consensus specification, verify the precise subsidy, epoch-boundary, rounding, and supply behavior directly in the current DMD Core code and on-chain tests. This revision retains the original paper’s stated policy; it is not an independent consensus audit.

5. Mining, Network Security and Difficulty

5.1. SHA-256 as mining infrastructure

DMD uses SHA-256 Proof-of-Work, benefiting from mature mining hardware, software tools, and operational experience. Participating miners secure transaction history by producing valid blocks and competing for block subsidies and fees. Hardware cost, electricity costs, pooled mining concentration, and hashrate migration remain important security considerations.

5.2. LWMA-3 difficulty adjustment

DMD uses a 60-block Linear Weighted Moving Average (LWMA-3) adjustment intended to respond to changing hashrate while targeting 150-second blocks. Difficulty adjustment improves responsiveness but cannot guarantee a fixed confirmation time or eliminate temporary pauses under sudden hashrate fluctuations.

5.3. Encrypted peer-to-peer transport

The project supports Bitcoin-style BIP324 v2 peer transport. Encrypted peer connections can reduce passive observability of network traffic; protection depends on the negotiated connection and configuration. It does not make transaction broadcast anonymous or provide end-to-end confidentiality for public blockchain contents.

5.4. Stratum v2 and mining decentralization — planned

Stratum v2 is a roadmap target for improving mining protocol efficiency and potentially increasing miner participation in block-template construction through compatible infrastructure. Job Negotiation and practical decentralization benefits depend on deploying and validating the relevant pool, miner, and node components.

5.5. Long-term cryptographic resilience — research

BIP360 proposes Pay-to-Merkle-Root (P2MR), a design that removes Taproot key-path spending and can reduce exposure to certain long-duration attacks against elliptic-curve keys. It does not provide comprehensive post-quantum protection by itself. DMD will evaluate the proposal and potential future post-quantum signatures only after technical review, compatibility analysis, and community consideration.

6. Transactions, Scaling and Accessibility

6.1. Base-layer payments

With a 150-second target interval, DMD is positioned as a native settlement layer for ordinary transfers and application payments. Actual transaction throughput and confirmation delays depend on policy, block construction, demand, and network conditions; neither zero fees nor immediate finality is guaranteed.

6.2. Lightning Network and TRUC — planned

The development roadmap includes research and integration work for Lightning-style channels and Topologically Restricted Until Confirmation (TRUC or v3) transaction policy. These tools can improve Layer-2 payment workflows when a complete compatible implementation exists. They should not be described as deployed or universally zero-fee at present.

6.3. AssumeUTXO — planned

AssumeUTXO-based snapshots may reduce the delay before a newly provisioned node becomes usable for selected operations while full historical validation continues. The feature requires suitable consensus assumptions, snapshot generation, chain-state validation, release engineering, and operational support. It is a roadmap objective, not a blanket guarantee of instant full validation.

7. Wallets and Network Infrastructure

The ecosystem includes desktop DMD Core software, Electrum-oriented infrastructure, a non-custodial web wallet, mobile wallet development, blockchain exploration services, and a public mining pool. These components provide user access to the network but remain distinct from the consensus layer.

Self-custody is an important design preference. In non-custodial wallets, recovery material and private keys remain under the user's control. Web and mobile interfaces should clearly identify their security assumptions, trusted services, network selection, and backup responsibilities.

A public Agent Gateway must not inherit privileged access to mining controls or unrestricted node RPC merely because a payment needs to be verified. Read-only settlement observation, separate receiving-address infrastructure, and narrow permissions are preferable to sharing a general administrative wallet.

8. Digital Artifacts and Data Anchoring

8.1. Taproot and inscription research

Taproot support in DMD Core provides a foundation for certain advanced spending patterns and applications. A complete Ordinals or inscription ecosystem additionally requires indexing rules, client behavior, and tooling. The roadmap lists Ordinals support as planned, rather than claiming that a production artifact service already exists.

8.2. Expanded OP_RETURN policy — planned / verify

The project has described an expanded OP_RETURN capacity target of up to 100,000 bytes for selected data-anchoring use cases. Such a change requires precise policy and block-usage analysis. Data embedded in transactions consumes network and storage resources even if the outputs are provably unspendable. Production limits and relay behavior must be confirmed in the running network before advertising native 100 kB support.

8.3. Intended applications

Potential applications include verifiable document fingerprints, metadata references, provenance records, and other compact commitments. Large documents and personal data should generally be kept off-chain, with access controls and appropriate privacy protections.

9. The Agentic Economy and DMD

Autonomous agents may request services, discover digital resources, purchase access, and manage digitally controlled identities. For such systems, a payment is useful only when it can be associated with an unambiguous offer, correct recipient, selected network, and confirmed fulfillment.

DebitMyData aims to support a broad ecosystem of autonomous agents, AI agents, bots, agentic bots (agenticbots), claws, digital twins, human users, and organizations. Through the planned DebitMyData Agent Gateway, eligible participants will be able to discover services, register decentralized identities (DIDs), and perform verified cryptocurrency payments using native DMD or other approved payment methods. This infrastructure is intended to enable autonomous economic interactions between AI-driven systems and human participants.

DebitMyData's proposed payment infrastructure aims to make its Agentics ecosystem usable by agents with different approved wallets while retaining native DMD as a direct payment option. A payer should not have to use DMD when its selected service explicitly supports another approved asset; likewise, users choosing DMD should be able to use the native PoW network rather than being forced onto a wrapped token.

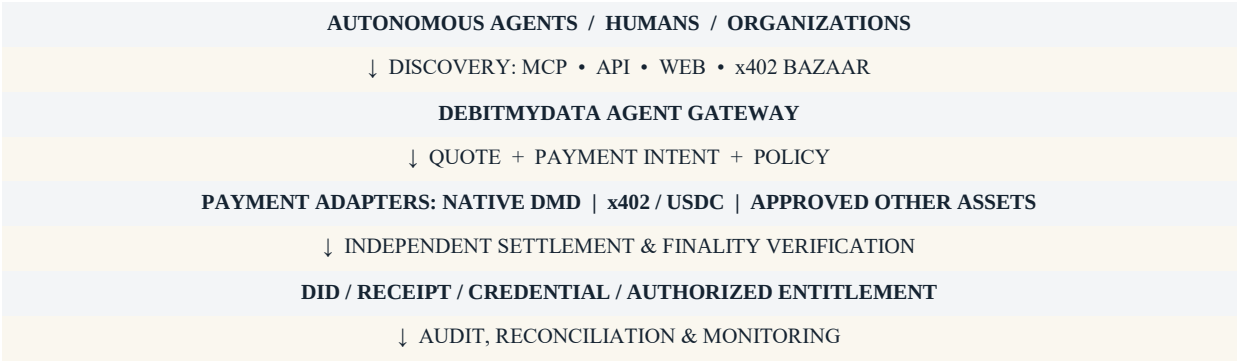
Use cases can include DID registration, authorized service access, licenses, marketplace activities, and other approved products. Commercial availability must follow successful implementation, security review, and relevant policy or legal checks.

10. Agent Gateway and Payment Architecture

10.1. One public-facing integration layer

The DebitMyData Agent Gateway is intended to be the controlled public integration surface. It will manage discovery, payment selection, quotes, payment-intent creation, settlement verification, proof of identity-controller authority, and delivery of receipts or entitlements. Internal nodes, private keys, signing functions, and treasury operations remain isolated.

10.2. Architectural overview



10.3. Modular, approved payment rails

Payment rail	Intended role	Rollout stance
Native DMD PoW	Direct on-chain DMD settlement	Initial priority; integration in development
x402 / USDC	Compatible autonomous-agent payments on an approved supported network	Initial interoperability priority
Additional EVM assets	Approved ERC-20 assets with chain and contract validation	Later, controlled enablement
Solana assets	Approved Solana-compatible payment flows	Later, controlled enablement
Wrapped or bridged DMD	Potential DMD representation outside its native PoW chain	Optional; requires formal approval and audit
Other chains / assets	Future approved adapters	Case-by-case validation

10.4. Gateway integration is not a token bridge

A gateway that checks DMD transfers and issues a DID is an application service, not an automatic cross-chain bridge. A separate bridge or wrapped-DMD mechanism could introduce custody, mint/burn, solvency, and contract risks and must not be implied or announced as delivered without its own approved design and independent review.

11. DID Registration and Payment Lifecycle

11.1. Fixed commercial fee, asset-specific settlement

The planned DebitMyData Agentic DID Registration service has a commercial fee fixed at USD 25.00. The cryptocurrency amount is not fixed for volatile assets: a payer receives a time-limited quote with a precise asset amount and destination under an approved pricing policy. This does not imply that 25 DMD equals USD 25.

11.2. Required quote fields

- Commercial fee: USD 25.00; the selected payment rail, asset, and network; and token contract when applicable.

- Exact amount in the chosen asset; destination address or payment endpoint; and payment-intent identifier.
- Required confirmations or finality standard; creation and expiry times; and current payment status.
- Approved price source and timestamp for non-USD-denominated assets.
- Applicable DID, marketplace, terms, refund, and privacy policies; and controller-proof requirements.

11.3. Expected registration sequence

- An eligible agent discovers supported payment methods through MCP, API, web, or applicable Bazaar metadata.
- The agent submits the desired DID information, controller key, and chosen supported payment method.
- The quote service returns an exact, time-limited amount, network, destination, and intent ID.
- The payer authorizes or broadcasts the payment through the selected wallet or payment protocol.
- The adapter independently verifies the correct asset, chain, destination, amount, uniqueness, and settlement finality.
- The agent proves control of the DID controller key or qualifying wallet using an appropriate challenge.
- Only after settled payment and valid proof does the DID service issue the credential, receipt, and authorized entitlements.

11.4. Exactly-once issuance and settlement reversals

Payment-intent state must be idempotent. Duplicate requests or replayed transactions must not produce multiple paid entitlements. The system must record pending, confirming, settled, failed, expired, underpaid, overpaid, reorged, reversed, and refunded states as appropriate; any detected reorganization must be reflected in risk controls and fulfillment decisions.

12. MCP, x402 and Service Discovery

12.1. Model Context Protocol (MCP)

The proposed MCP service will allow compatible agents to discover supported assets, request registration offers or quotes, inspect payment status, prove controller-key ownership, complete qualified registrations, and retrieve authorized product catalog information. Exposing a tool does not grant it authority to override settlement or security policy.

12.2. x402 and Bazaar

The x402 path is intended to provide a recognized payment-gating pattern for compatible autonomous agents, while Bazaar metadata can make eligible paid routes discoverable. Each publicly advertised route must declare only the specific asset, network, contract, payment scheme, and recipient it can truly verify. A broad statement that “any crypto” is accepted would be misleading without corresponding adapters and policies.

12.3. Coinbase / AWS compatibility statements

Coinbase-compatible or AWS-hosted agentic systems may use the gateway only through supported integration and payment methods. Compatibility targets should not be presented as evidence of a completed Coinbase deployment, AWS infrastructure sponsorship, or commercial partnership unless separately confirmed.

13. Security, Privacy and Operational Controls

13.1. Segregation and least privilege

Public agent endpoints must not expose node administration, treasury movement, private-key material, unrestricted signing, or mining operations. Read-only DMD blockchain access should be behind network isolation and authenticated, method-restricted services. Payment destinations, operating funds, and refund workflows should be separated.

13.2. Independent verification

Payment adapters must enforce approved chain IDs, token-contract addresses, decimal precision, receiving destinations, intended amounts, transaction references, and finality policy. Systems must detect common replay and double-spend patterns, invalid or spoofed assets, wrong-network payments, and reorganizations.

13.3. Pricing and policy controls

Each volatile asset needs an approved market-data source, timestamp, maximum quote age, permitted price deviation, and fallback policy. Payment rails should be individually disabled if safety conditions are not met. Enabling a new asset, destination, or conversion rule should require documented change control and human approval where appropriate.

13.4. Privacy, auditability and identity

The audit trail should retain necessary payment-intent, settlement, receipt, and policy evidence without publishing credentials, controller secrets, or unrelated personal information. Blockchain payments are publicly observable; DID design must address metadata leakage, key rotation, revocation, recoverability, and appropriate privacy expectations.

14. Economic and Technical Risks

Risk	Implication / treatment
Cyclical issuance	Long-run supply increases across epochs; publish reproducible issuance analysis and on-chain behavior.
Mining concentration	Availability of SHA-256 hardware does not guarantee a decentralized hashrate distribution.
Reorganizations / volatility	Settlement finality, conversion prices, and quote expirations require explicit policies.
Gateway compromise	Use narrow permissions, independent verification, isolated secrets, monitoring, and rail kill switches.
External networks	Additional assets inherit token, bridge, validator, smart-contract, compliance, and operational risks.
Agentic misuse	Rate limiting, abuse controls, eligibility policies, controller proof, and audit trails remain essential.
Future protocol changes	Lightning, Stratum v2, OP_RETURN changes, AssumeUTXO, and BIP360 need tests and explicit activation decisions.

Any discussion of future liquidity, revenue, payment volume, or DMD value is an objective rather than a forecast or promise. This Whitepaper does not constitute an investment offer, a guaranteed-service commitment, or a claim that every third-party integration is already live.

15. Development Roadmap

The phases below mirror the revised DebitMyData PoW website roadmap. A feature’s presence here describes direction, not completion. Deployment status may change; maintained release notes and service documentation should identify current availability.

Phase	Focus	Representative milestones
1 — Mainnet and access	Existing PoW network and user infrastructure	SHA-256 mainnet, Electrum, non-custodial wallets, public mining pool; iOS and exchange availability subject to release status.
2 — Agentics and payments	Priority application integration	Agent Gateway; native DMD payment adapter; DID quotes and issuance; MCP, x402/Bazaar; settlement controls; future approved multi-asset adapters.
3 — Blockchain	Protocol and application features	Taproot Assets, Ordinals tooling, expanded OP_RETURN research,

expansion		Stratum v2, AssumeUTXO, further listings.
4 — Scaling and security	Advanced transaction systems	Lightning integration, TRUC policies, Miniscript vault use cases, additional market access.
5 — Future resilience	Research and ecosystem	Silent Payments, Erlay, grants, post-quantum audit and BIP360/P2MR evaluation.

16. Conclusion

DebitMyData's long-term proposition rests on two complementary components. At the protocol layer, DMD explores sustained Proof-of-Work incentives through cyclical, deterministic issuance and SHA-256 mining. At the application layer, the Agentics initiative aims to make this native settlement network useful for decentralized identities, machine-initiated purchases, and approved digital services.

These layers should be evaluated separately. A functional payment gateway does not prove the security of a consensus design; a working blockchain does not establish that every agentic integration is ready for production. The project's development approach should emphasize explicit status reporting, independent settlement checks, transparent monetary rules, and carefully staged interoperability.

Appendix A — Frequently Asked Questions

Is DMD capped at 21 million units forever?

No. In the documented cyclical issuance model, approximately 21 million DMD is the issuance target for each epoch. A new epoch adds issuance rather than resetting balances or destroying existing coins.

Does the issuance model guarantee mining profitability?

No. Profitability depends on electricity, equipment, hashrate, coin value, fees, pool terms, and other changing conditions.

Does an autonomous agent need DMD to obtain a DID?

Not necessarily. The proposed service prioritizes native DMD payments while also planning approved x402/USDC and later other payment methods. Availability depends on the enabled routes.

What is the DID registration price?

The commercial registration fee is USD 25.00. For a non-USD asset, the payable cryptocurrency amount is calculated in a quote using an approved price source and expires after a specified time.

Is the Agent Gateway a DMD-to-EVM token bridge?

No. It is a policy, quote, settlement verification, and entitlement service. A wrapped token or cross-chain bridge is a separate, optional system requiring further approval.

Is x402 already deployed?

This revision describes x402 and Bazaar as an intended interoperability path. Live status must be verified through actual production endpoints and payment tests.

Do BIP360 or P2MR make DMD quantum-proof?

No. BIP360 is a proposal intended to address some long-exposure attack risks; it does not replace the need to study post-quantum signatures and broader migration concerns.

Can a public agent access DMD private keys or RPC administration?

No. The intended architecture deliberately separates public agent requests from privileged node functions, signing material, mining controls, and treasury operations.

Appendix B — References and Editorial Verification

Primary source documents

- DebitMyData (DMD) Whitepaper, original 14-page publication supplied for this revision (PDF).
- Preska Thomas, “Autonomous Agentic Payment / Multi-Wallet, Multi-Cryptocurrency Agentic Payment Deployment,” September 18, 2026 (implementation directive supplied for this revision).
- DebitMyData PoW website roadmap in the supplied index.php, October 14, 2026.

Technical references

- DebitMyData Core repository: https://github.com/DebitMyData-PoW/DebitMyData-PoW-Core
- Bitcoin Core 31.0 release notes: https://bitcoincore.org/en/releases/31.0/
- BIP360, Pay-to-Merkle-Root (draft): https://bitcoin.org/bip/360/
- Stratum v2 reference project: https://stratumprotocol.org/

Publication verification checklist

- Confirm the current DMD release lineage and active network parameters in the source code and build artifacts.
- Resolve P2P versus RPC port discrepancies between the old Whitepaper and website.
- Test and document precise supply-epoch transitions, halving behavior, rounding, and cumulative issuance.
- Confirm live availability of BIP324, 100 kB OP_RETURN policy, AssumeUTXO, inscriptions, Stratum v2, and Lightning integration before marking any item deployed.
- Confirm production readiness, security review, payment quote sources, operational controls, and eligible asset rails before advertising Agent Gateway services as live.
- Review legal, compliance, privacy, and refund terms before public payment activation.

REVISION SCOPE

v2.0 adds the Agentics application architecture and corrects internal inconsistencies visible in the supplied original Whitepaper. It does not constitute a third-party code audit, formal security certification, or production readiness assessment.