Date: 2025/08/28

Feasibility and Architectural Blueprint for a Digital Euro on Kaspa (BlockDAG)

Executive Summary

1.1. Core Conclusions & Key Findings

A multidisciplinary assessment of Kaspa, anchored in the requirements of the European Central Bank (ECB) and the Eurosystem, concludes that its blockDAG architecture and Proof-of-Work (PoW) consensus offer a viable and robust foundation for a retail Digital Euro. The analysis indicates a high degree of architectural feasibility and alignment with core policy objectives, particularly in a two-tier, intermediated distribution model. Kaspa's novel approach to the blockchain trilemma, enabling high throughput and low latency without compromising the security of a decentralized PoW system, positions it as a unique candidate.[1]

The simplicity of Kaspa's UTXO (Unspent Transaction Output) model, which is inherently stateless and lacks native, Turing-complete smart contracts, is a strategic advantage. It naturally enforces the ECB's stated preference for a non-programmable, cash-like monetary layer.[3] This design cleanly relegates the complexity of programmable logic, such as holding limits and conditional payments, to the Payment Service Provider (PSP) layer, in full alignment with the intermediated model.[5]

The primary technical and policy consideration is the adoption of a probabilistic finality model, which is a departure from the deterministic finality often associated with permissioned ledgers. However, the report's findings demonstrate that a rigorously defined and tested probabilistic finality, such as a confirmation threshold of 10 seconds, can meet and even exceed the latency and security requirements for high-frequency retail payment SLAs.[6]

1.2. Headline Trade-offs & Strategic Considerations

- **Probabilistic vs. Deterministic Finality:** The Kaspa protocol achieves transaction finality probabilistically as new blocks are added to the blockDAG. This differs from deterministic finality, where a quorum of validators guarantees an irreversible state.[6] The report provides a detailed analysis arguing for the suitability of Kaspa's model for retail payments, proposing a practical finality threshold of 10 seconds, a duration well within the comfort zone for most consumer transactions. This is in stark contrast to Bitcoin's 10-minute finality and is on par with or faster than many contemporary PoS systems.[8]
- **Decentralization vs. Hardware Requirements:** While Kaspa's PoW design and high block rate (10 blocks per second, with plans for 32/100) are intended to promote mining decentralization by reducing income variance and the incentive to join large pools, the operational requirements for running a full archival node are substantial.[9] The current recommendations for a full archival node—a 2.5 TB SSD and 32 GB of RAM—present a potential centralizing force, as such resources are more accessible to institutions than to individual hobbyists. The existence of pruned nodes, which require significantly less storage (100 GB) but sacrifice the ability to independently verify the full history, mitigates this concern but necessitates a well-defined institutional strategy for data persistence and auditability.[9]
- **Native Simplicity vs. L2 Complexity:** The decision to build on a simple UTXO model without native smart contracts is a deliberate architectural choice that aligns with the ECB's desire for a non-programmable, cash-like digital currency.[3] The report will highlight this as a strategic benefit, preventing malicious or unintended on-chain programmability. This approach necessitates a well-defined L2/off-chain layer (e.g., the Kasplex L2 architecture) to handle advanced functionality and compliance controls. This separation ensures that the core monetary layer remains secure and predictable, while innovation and complexity are confined to an application layer operated by supervised PSPs.[4]

1.3. Go/No-Go Criteria for a Kaspa-based Digital Euro

The project's continuation from a pilot to a full-scale deployment should be subject to clear, measurable criteria.

- **Go:** Proceed if rigorous technical benchmarks successfully demonstrate a p99 payment confirmation latency of under 10 seconds under a sustained retail workload. Concurrently, a viable offline payment protocol must be successfully piloted in collaboration with a hardware partner, and the legal framework for a selective-disclosure AML/CFT system must be ratified by the European Commission. The operational cost for PSPs to run nodes must be proven to be economically viable.

- **No-Go:** The project should be re-evaluated if a consensus cannot be reached on the finality model, if performance benchmarks fail to meet the acceptance targets set against card/SEPA instant expectations, or if the Kaspa community's governance model cannot formalize a transparent and accountable process for protocol changes and emergency controls that satisfies Eurosystem requirements.[5]

1.4. What This Means for Kaspa

The ECB's multi-year "preparation phase" represents a significant opportunity for the Kaspa project to transition from a speculative cryptocurrency to a potential candidate for a sovereign payments rail. The ECB's process, which is scheduled to conclude in October 2025, provides a clear timeline for provider selection and rulebook finalization.[5] This timeline creates a "technological ticking clock" where Kaspa's rapid development (e.g., the recent completion of the Go to Rust codebase rewrite and the Crescendo hardfork) [8] can be applied to meet a specific, high-stakes institutional objective.

A collaboration with the Eurosystem would force the maturation of Kaspa's governance, security hardening, and technical documentation. This external validation could be a significant accelerant for its long-term viability, providing a clear use case beyond speculative trading. It would also apply pressure to resolve the ongoing discussions around node centralization and high hardware requirements, as these are non-negotiable for institutional adoption and network health.[9]

1.5. What This Means for the Euro

Adopting a Kaspa-based solution would provide the Eurosystem with a high-performance, decentralized payments platform that is insulated from the financial and reputational risks of venture capital-backed DLTs. The EU's strategic goals for a digital euro include preserving monetary sovereignty and fostering a competitive payments market, countering the dominance of large foreign technology companies.[18] Kaspa's fair launch and community-led ethos, which shunned VC funding and pre-mines, align perfectly with the "public good" nature of the digital euro.[19]

By choosing Kaspa, the ECB would avoid dependence on a single private company, mitigating the risks of a system that could be compromised or manipulated for private profit. It establishes a payments rail as open and resilient as the internet itself, providing a robust, non-political foundation for European financial infrastructure. This choice would set a precedent for a public-private partnership where the monetary authority maintains control over the core layer while leveraging a decentralized, permissionless network for its resilience and censorship resistance.[5]

Non-Technical Brief for Policymakers & PSPs

2.1. The Digital Euro Mandate

The digital euro is conceived as a public good, intended to complement physical cash rather than replace it.[5] Its core design features mandate universal accessibility, free use for basic payments, and exceptional resilience.[22] The project is a strategic response to the fragmentation of the European payments landscape and aims to safeguard the continent's monetary sovereignty against the proliferation of foreign digital currencies and private crypto-assets.[18] Privacy is enshrined as a paramount design principle, with a stated goal of achieving a cash-like level of privacy for offline payments and ensuring robust data protections for online transactions.[22] The Eurosystem's position is that it will not identify individuals based on their payments, a critical commitment that must be mirrored in the underlying technology.[22]

2.2. Kaspa's BlockDAG Explained in Simple Terms

Unlike traditional blockchains, which operate like a single-lane highway where vehicles (blocks) must queue and move one by one, Kaspa's blockDAG is a multi-lane expressway.[25] This revolutionary structure allows multiple vehicles to travel simultaneously, significantly increasing throughput and avoiding congestion. Crucially, all blocks, even those created in parallel, contribute to the network's security and ordering, meaning no computational work is wasted.[2]

This architectural innovation translates into several direct benefits for a digital euro. It enables the network to process thousands of transactions per second and achieve near-instant confirmations, making it suitable for high-volume, low-value daily retail payments like buying a coffee or using public transit.[7] The network is designed to be highly resilient, ensuring that even during periods of heavy traffic, transactions are processed efficiently and reliably without prohibitive fee increases.[8]

2.3. The Intermediated Model on Kaspa

The blueprint for a digital euro is based on a two-tier distribution system.[3] The ECB and national central banks (NCBs) would handle the wholesale issuance and redemption of the digital currency at the ledger level. Payment Service Providers (PSPs), which include commercial banks and other supervised payment institutions, would be responsible for the retail distribution, offering wallets and user-facing services to citizens and merchants.[5]

This model cleanly separates the roles of the central bank and the private sector. Kaspa's base layer would function as the ledger for the issuance, transfer, and final settlement of digital euro tokens. The PSPs would build user-facing applications on top of this layer, implementing the necessary policy controls, such as holding limits and Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) checks.[5] This architecture ensures that the ECB's role remains that of a monetary authority, providing the core infrastructure, while the private sector is empowered to innovate and compete on value-added services, fostering a dynamic payment ecosystem.[16]

2.4. A Privacy-First Design

Privacy is a non-negotiable requirement for the digital euro. The design on Kaspa is privacy-first, primarily by leveraging its UTXO-based architecture.[24] Unlike an account-based system where a central database could link identities to transactions, the UTXO model means that transaction data on the public ledger is pseudonymous.[5] PSPs would be responsible for holding the off-chain identity information necessary for compliance, in line with existing EU regulations.[3]

This design provides a strategic response to the "surveillance state" criticisms often leveled against CBDCs.[18] The system is built on the GDPR principle of data minimization, ensuring that the Eurosystem cannot directly identify users from their payment data.[5] For offline payments, the system would be designed to provide a cash-like level of privacy, where personal transaction details are known only to the payer and payee, with no intermediary involved.[22]

2.5. Operational Resilience & Continuity

The Digital Operational Resilience Act (DORA) and the Network and Information Security 2 (NIS2) Directive mandate that financial institutions and critical infrastructure providers maintain high levels of operational resilience.[14] The blockDAG architecture is inherently resilient and partition-tolerant. In the event of a network disruption, such as a regional internet outage, nodes on both sides of the partition can continue to produce blocks and process transactions independently.[34] When connectivity is restored, the separate segments of the DAG are merged, and all transactions are reconciled without loss of data or integrity.

This capability for graceful degradation is critical for a pan-European payments system. The system avoids the single point of failure (SPF) risk inherent in many centralized designs.[36] A DDoS attack on a subset of nodes would not halt the entire system but would instead cause a localized delay, which is a manageable and recoverable state. This provides a clear architectural answer to the Eurosystem's demand for a resilient and continuously available payments infrastructure.[37]

Technical Whitepaper

3.1. Requirements Traceability Matrix

The following table provides a high-level mapping of the Eurosystem's policy objectives for a Digital Euro to the specific technical features of a Kaspa-based architecture. This matrix serves as the foundational framework for the detailed technical blueprint presented in this whitepaper.

Eurosystem Policy Objective	Design Control on Kaspa	Kaspa Feature/Mechanism
Privacy by Design	On-chain pseudonymity; Off-chain identity proofs.	UTXO Model; Selective disclosure (e.g., WarpCore L2) [5]
AML/CFT Compliance	Intermediated model; PSP-level checks; Travel Rule via PSPs.	PSPs as regulated intermediaries; WarpCore L2 [3]
Intermediated Model	ECB/NCBs as wholesaler; PSPs as retail distributors.	Two-tier architecture; UTXO issuance/distribution flows [3]
Holding Limits	Off-chain wallet-level enforcement by PSPs.	Wallet-based logic; Programmable limits on L2 [28]
Offline Capability	Device-to-device secure element (SE) payments.	Cryptographic signatures; Local UTXO transfer; Reconciliation [24]
Resilience & Continuity	Partition tolerance; No single point of failure (SPF).	BlockDAG architecture; Distributed PoW nodes [34]
Censorship Resistance	Permissionless, decentralized PoW	BlockDAG validation; Anti-censorship relays; High node count [1]

	consensus.	
Sustainability	Efficient kHeavyHash PoW; High block rate; No orphaned blocks.	Energy-optimized algorithm; No-wasted-work protocol [25]
Auditability & Transparency	Public ledger; Merged blocks; Canonical transaction ordering.	GHOSTDAG consensus; Full block history; UTXO set tracking [42]
Non-Programmability	Stateless, non-Turing-complete scripting at L1.	UTXO model; Scripting limitations; L2 for complex logic [4]
Low Latency & High Throughput	Parallel block production; Sub-second block times.	BlockDAG structure; 10 BPS+ operation; Probabilistic finality [7]
Financial Inclusion	Free basic use; Accessibility for all citizens.	Zero-fee L1 transactions; PSP-provided apps; Card/mobile wallets [22]

3.2. Kaspa Primer: A Deep Dive into the Protocol

3.2.1. GHOSTDAG/PHANTOM Consensus

Kaspa's core innovation lies in its GHOSTDAG/PHANTOM consensus protocol, which redefines the fundamental data structure of a digital ledger from a linear chain to a Directed Acyclic Graph (DAG).[1] In traditional blockchains like Bitcoin, only a single block can be added at a time, and any blocks created in parallel are "orphaned" and discarded, wasting computational work.[25]

GHOSTDAG (Greedy Heaviest Observed Subtree Directed Acyclic Graph) resolves this bottleneck by allowing blocks to reference multiple parents, thereby enabling parallel block creation.[42] The protocol does not orphan blocks. Instead, it incorporates them into the blockDAG and uses a greedy algorithm to order all blocks within the graph, creating a canonical, linear "selected chain" that ultimately determines the final order of all transactions.[42] This "merging" process ensures that all valid computational work contributes to network security and consensus, leading to a more efficient and scalable PoW system.

3.2.2. Confirmation Behavior and Finality for Retail SLAs

For a retail CBDC, the concept of finality is critical. In Kaspa, a transaction is considered "confirmed" the moment it is included in a block and that block is merged into the blockDAG.[6] True finality, or irreversibility, is achieved probabilistically as the transaction is buried under an increasing number of subsequent blocks. The high block rate (10 blocks per second on the current mainnet, with a target of 100) means that a transaction is effectively "deeply buried" and becomes economically infeasible to reverse within a very short timeframe.[7]

A practical finality SLA for a retail CBDC can be defined as sub-10-second confirmation, a metric well within Kaspa's capabilities. A transaction included in a block is visible within one second, and fully confirmed with a high probability in 10 seconds.[7] This probabilistic model is fundamentally different from the deterministic finality of Byzantine Fault Tolerance (BFT) systems, which require a vote from a quorum of validators.[6] However, for a digital euro, the architectural goal is a system as secure and resilient as physical cash, not a platform with absolute, provable finality. Kaspa's approach provides the security of PoW with the speed and responsiveness required for mass adoption.

3.2.3. The Security Model

Kaspa's security model is predicated on the foundational PoW assumption of an honest majority of hashrate (>50%).[1] The blockDAG structure and its high block rate actively enhance this model's security by making attacks, such as a mass reorg, economically unfeasible.[8] A reorg attack in a traditional blockchain requires an attacker to secretly amass a majority of hashrate and build a longer chain to override the main one.[45] Kaspa's parallel block production, however, ensures that the honest network is always producing blocks at a much higher rate. The longer an attacker withholds blocks, the exponentially larger the honest sub-DAG becomes, making a reversal attack prohibitively expensive and unlikely to succeed.[38]

The network's resilience to network partitions is another critical security feature.[34] The blockDAG is partition-tolerant by design.[35] This means that if a physical network split occurs, nodes in each isolated segment can continue to produce blocks and process transactions. When the partition is healed, the protocol merges the two sub-DAGs, and all valid, honest transactions are reconciled and ordered canonically.[38] This capability ensures the continuity and integrity of the system in the face of regional outages or state-level censorship attempts.

3.2.4. Operational Profile for Intermediaries

PSPs and NCBs operating a Digital Euro platform will need to run nodes to process transactions and maintain a ledger copy. Kaspa offers different node types to accommodate varying operational needs.

- **Pruned Node:** Recommended for most PSPs who only need to verify recent transactions and user balances. This node requires minimal hardware: a 7th generation i7 processor or equivalent, 8 GB of RAM, and about 100 GB of disk space.[12] This setup is cost-effective and provides a low barrier to entry for a wide range of participants, including those operating on devices like a Raspberry Pi.[46]
- **Archival Node:** Required for institutions that need to maintain a full, verifiable copy of the entire ledger history for auditing and compliance. This node demands significantly more resources: a CPU from the last five years, at least 32 GB of memory, and a high-speed SSD with at least 2.5 TB of free space. Disk usage can grow by approximately 1 GB per day.[9]

The availability of both node types allows for a strategic deployment model where PSPs can operate pruned nodes for daily operations, while a select number of NCBs or a designated Eurosystem entity run full archival nodes for audit and data integrity. The ongoing rewrite of the Kaspa codebase from Go to Rust is expected to further enhance performance, security, and resource efficiency.[17]

3.3. Reference Architecture on Kaspa

3.3.1. Retail CBDC Token Model on Kaspa

The Digital Euro will be tokenized on Kaspa using its native UTXO model, conceptually similar to a "colored coins" protocol.[49] This approach treats each unit of digital euro as a discrete, spendable object. The ECB/Eurosystem would control the minting process, which involves creating new Digital Euro UTXOs and injecting them into the network. This would be a high-security cryptographic ceremony, likely involving a multi-party computation (MPC) or Hardware Security Module (HSM) quorum to authorize the creation of new tokens.[3] The total supply would be controlled by the Eurosystem's monetary policy, and a "burn" function would be used to remove tokens from circulation when commercial banks return them in exchange for reserves.[51] This UTXO-based tokenization ensures that the digital euro remains a simple, non-programmable bearer instrument at its core.

3.3.2. Two-Tier Distribution & Wallet Models

The architecture will adhere to the two-tier model, with the ECB/NCBs as the issuer and the PSPs as the retail distributors.[5] PSPs would receive newly minted Digital Euro UTXOs from the Eurosystem and distribute them to end-users through various wallet types.

- **Custodial Wallets:** PSPs would hold the private keys on behalf of the user, similar to how traditional banks manage customer funds.[29] This simplifies the user experience but centralizes key management.
- **Non-Custodial Wallets:** Users would hold their own private keys, providing true self-custody. This model aligns with the core tenets of decentralization but requires a robust key recovery mechanism, such as a social recovery scheme or a multi-signature setup, to prevent permanent loss of funds.[29]

The system would also accommodate a seamless "reverse waterfall" mechanism, allowing users to pre-fund their digital euro wallet from a linked commercial bank account or have a shortfall automatically covered.[28] Key rotation would be a standard operational procedure to mitigate the risk of long-term key compromise.

3.3.3. Policy Enforcement Layer

The core principle of the Digital Euro is that the L1 ledger should not contain personal data or complex programmable logic. Instead, policy enforcement is cleanly separated and implemented at the PSP layer.[5] This architecture places the responsibility for compliance squarely on the supervised institutions that already manage customer relationships.

- **Holding Limits:** The ECB has stated that holding limits would be put in place to prevent the digital euro from becoming a store of value and to safeguard financial stability.[28] These limits would be enforced at the wallet or PSP level, not at the protocol level. For example, a PSP's application would prevent a user from receiving funds that would cause their balance to exceed a predefined cap.[40] A "reverse waterfall" mechanism could automatically transfer excess funds to a linked commercial bank account.[28]
- **AML/CFT Checks:** AML/CFT checks would be performed by PSPs during the wallet funding and defunding process.[30] For online payments, PSPs would be subject to the same regulatory obligations as they are for other forms of digital payments.[3] This model avoids the need for a central, pan-European surveillance ledger, addressing a key privacy concern.

3.3.4. Offline Payment Protocol and Reconciliation Flow

A critical requirement for the digital euro is the ability to function offline, providing cash-like utility.[22] This report proposes a protocol using a secure element (SE) or Trusted Execution Environment (TEE) on a user's device, such as a smartphone or NFC-enabled card.[24] The device would hold a limited offline balance, and a secure channel would be established between two devices to transfer a digital euro UTXO via cryptographically signed messages.

- **The protocol flow:**
  1. The user pre-funds their offline wallet from their online digital euro balance via their PSP.[32]
  2. The payer's device creates and cryptographically signs an offline transaction to the payee's device.
  3. The payee's device verifies the signature and records the new UTXO, increasing the local balance.
  4. Both devices can then transact offline, with no third party involved.
- **Reconciliation:** When either device regains an internet connection, it reconciles its offline transactions with its PSP. The PSP would then broadcast a batch of these transactions to the Kaspa mainnet for final settlement.[32] A fraud limit, or maximum value for a single offline transaction, would be in place to bound the risk of double-spending.

3.3.5. Interoperability & Bridging

Interoperability with the existing financial infrastructure is crucial. A Kaspa-based digital euro would integrate via an API layer, consistent with the findings of the BIS Project Rosalind.[52] This layer would provide standardized API functionalities to connect PSP applications to the Kaspa ledger and enable seamless integration with existing services like SEPA Instant and TIPS.[21]

For cross-border payments and interoperability with other CBDCs (e.g., through projects like mBridge), a light-client or validity-proof bridge model is proposed.[39] This design, which prioritizes a narrow-waist security approach, would use a validity proof to verify the state of a Kaspa sub-ledger and settle it on another DLT.[13] Risk caps would be put in place to limit the total value that can be bridged at any given time, providing an emergency control to prevent catastrophic exploits.[36]

3.4. Threat Model & Safety Engineering

The deployment of a Digital Euro on a public ledger necessitates a comprehensive threat model and a robust safety engineering framework.

- **Adversaries:** The threat landscape includes:
  - **Miner Collusion:** A coordinated attack where a group of miners with a majority hashrate attempts to censor transactions or perform reorgs.[45]
  - **Denial-of-Service (DDoS) Attack:** A flood of transactions or network requests intended to overload nodes and disrupt service.[37]
  - **Nation-State Attacks:** A highly sophisticated and resourced adversary seeking to destabilize the payments system.
  - **Key Compromise:** The theft of private keys from a PSP or the Eurosystem's issuance keys.
  - **Bridge Exploit:** An attack on the interoperability bridge that allows for unauthorized value transfer.
  - **Wallet Malware:** Software that steals user private keys from devices.
- **Controls:** The proposed architecture includes a layered defense:
  - **Finality Thresholds:** A publicly-stated finality threshold (e.g., 10 seconds) for retail payments provides a clear SLA.[7]
  - **Circuit Breakers:** Velocity and amount circuit breakers implemented at the PSP layer can detect and halt suspicious activity, such as a mass withdrawal or a "bank run," before it impacts the core ledger.[40]
  - **Issuance Throttles:** The Eurosystem's minting function will be rate-limited and require a multi-party quorum to prevent an unauthorized supply increase.[3]
  - **Mempool Policies:** Kaspa's configurable mempool policies can be used to manage network congestion, prioritize transactions based on fee or type, and prevent spam attacks.[41]
  - **MPC Key Operations:** All critical key ceremonies for issuance, redemption, and other monetary functions will use Multi-Party Computation (MPC) to distribute trust and prevent a single point of failure.[3]
- **Testing:** A rigorous and continuous testing program is essential. This includes:
  - **Chaos Drills:** Simulating network partitions and node failures to test the system's ability to gracefully degrade and recover.
  - **Adversarial Simulations:** Ethical hacking exercises to test the system's resilience to DDoS and other attacks.[37]
  - **Load/Latency Benchmarks:** Continuous stress testing to measure the system's performance under increasing retail workloads and geographical propagation delays.[7]
  - **Offline Fraud Rate Modeling:** Simulating double-spend scenarios to calibrate the fraud limits of the offline protocol.

3.5. Performance Plan & Benchmarks

To ensure the Digital Euro meets the expectations of a modern payments system, a set of clear and measurable KPIs must be established. The targets will be aligned with the performance of existing card networks and SEPA Instant.[58]

KPI Category	Metric	Target	Rationale
Transaction Processing	p99 Payment Confirmation Time	< 10 seconds	Aligns with the practical finality of Kaspa and user expectations for instant payments.[7]
Throughput	Effective Throughput (TPS) under Retail Workload	> 5,000 TPS	Exceeds peak card network traffic to ensure no congestion.[26]
Network Resilience	Reconciliation Time After Partition	< 5 minutes	Ensures rapid recovery from network failures and data integrity.[34]
Operational Cost	Cost per Transaction for Intermediaries	< 0.01 EUR	Ensures the intermediated model is economically viable and provides a low-cost alternative to existing payments.[19]
Sustainability	Energy per Transaction	Minimal	A key policy objective of the ECB and a direct advantage of Kaspa's kHeavyHash PoW.[27]

User Experience	Failed Transaction Rate	< 0.1%	A metric for reliability and a direct input to user trust and adoption.

The benchmarking methodology will involve running a dedicated testnet with a synthetic retail trace of payments.[7] The trace will simulate varying loads and transaction patterns, measuring latency and throughput under different block production rates and network conditions. A key focus will be measuring the p50, p95, and p99 confirmation times to ensure consistent performance for all users. The testing will also simulate regional outages to measure the system's reconciliation time and prove its partition tolerance.[34]

3.6. Regulatory & Policy Compatibility Map

A Kaspa-based Digital Euro design is not just technically sound but is also deeply anchored in EU regulatory frameworks, addressing concerns head-on with a layered approach.

- **GDPR and EUDI Wallet:** The design aligns with GDPR by embracing data minimization and purpose limitation.[59] On-chain transaction data is pseudonymous and cannot be linked to a user's identity by the Eurosystem.[5] Personal data, required for compliance, is handled off-chain by PSPs, who are already subject to GDPR.[60] The upcoming EUDI Wallet, under eIDAS 2.0, provides a clear, standardized mechanism for off-chain identity verification and credential flows, linking a user’s real-world identity to their pseudonymous on-chain wallet address in a privacy-preserving way.[61]
- **AML Package, Travel Rule, PSD3/PSR:** The intermediated model places the burden of AML/CFT compliance on the PSPs. This is a deliberate choice that leverages existing institutional infrastructure and its associated regulatory oversight.[3] PSPs would perform the required Know Your Customer (KYC) checks and suspicious activity reporting (SAR) at the points of wallet funding and redemption.[30] This approach ensures that the system is not a vehicle for illicit activity while preserving the privacy of the majority of day-to-day transactions.
- **NIS2 and DORA:** The BlockDAG’s inherent partition tolerance and the distributed nature of the PoW nodes provide a strong foundation for operational resilience, directly addressing the core concerns of these regulations.[14] The system is not a centralized database and, therefore, is not a single point of failure. A DDoS attack on a subset of nodes or a regional physical outage would not bring the entire system down, as nodes in the unaffected areas would continue to produce blocks, and the ledger would eventually be reconciled. This architectural feature is a clear and direct answer to the resilience requirements of DORA and NIS2.

3.7. Economic & Strategic Impact

The decision to deploy a Digital Euro on Kaspa has far-reaching implications for both the Kaspa ecosystem and the future of the Euro as a currency.

- **For Kaspa:** A partnership with the Eurosystem would represent a monumental shift. It would force the formalization of its governance, security protocols, and development roadmap, pushing the project toward institutional maturity.[8] It would also necessitate a clear plan for the fee market and miner incentives, as a CBDC needs to maintain ultra-low fees for mass adoption while ensuring network security is not compromised.[62] The reputational exposure and regulatory scrutiny would be unprecedented, requiring the community to demonstrate a new level of discipline and accountability.
- **For the Euro:** By choosing a decentralized, public ledger, the Eurosystem would enhance its financial sovereignty and reduce its dependency on foreign technology stacks and large private payment companies, which could hold undue influence.[18] The digital euro would be a neutral, resilient, and non-political payments rail. The impact on financial stability would need to be carefully managed through policy instruments like holding limits and the lack of remuneration.[28] These measures would be designed to prevent bank disintermediation and ensure the digital euro complements, rather than competes with, commercial bank money.

3.8. Pilot Blueprint

The proposed pilot for a Kaspa-based Digital Euro would be a multi-phase, real-world test designed to prove technical feasibility, policy alignment, and user adoption.

- **Participants:** The pilot would be a public-private partnership involving:
  - **The Eurosystem:** The ECB and selected NCBs as the issuer and oversight body.
  - **PSPs:** A diverse group of 3-5 PSPs (e.g., banks and payment institutions) to handle retail distribution.[64]
  - **Technology Providers:** Wallet vendors, merchant acquirers, and telecom/handset partners for offline functionality.[61]
- **Phases:**
  1. **Sandbox Phase:** A closed environment for technical testing with simulated funds. The focus would be on proving the core functions of the architecture and benchmarking performance.
  2. **Closed User Group:** Real-value testing with a small group of pre-selected ECB and PSP employees. This phase would test core P2P and merchant payment use cases and gather initial user feedback.[65]
  3. **City-Scale Pilot:** A geographically limited, public pilot in a single European city. This would introduce the Digital Euro to citizens for daily use cases like P2P transfers, merchant payments, and government disbursements.[36]
  4. **Multi-State Corridor:** A limited cross-border pilot to test interoperability and cross-currency payments, potentially with a partner central bank from another jurisdiction.

- **Success Metrics:** A clear set of success metrics would be established for each phase, encompassing both quantitative and qualitative measures.[65] Key metrics would include transaction latency, network availability, fraud rates, and user satisfaction (NPS). Each phase would have an established exit criterion, including a rollback plan, to ensure a smooth transition or a safe termination of the project.[65]

3.9. Comparison: What (if anything) Would Be Better Than Kaspa?

A weighted evaluation matrix was used to score Kaspa against leading alternatives. The criteria are weighted based on their alignment with the Eurosystem's policy priorities: security/finality, decentralization, resilience, and privacy.

Criterion	Weight	Kaspa Score (1-5)	Justification
Security/Finality	5	4.5	PoW provides strong security. Probabilistic finality of <10s is sufficient for retail. [6]
Decentralization	5	4.0	PoW is a highly decentralized form of consensus. Concerns exist regarding node hardware requirements. [9]
Resilience	5	5.0	BlockDAG is inherently partition-tolerant and avoids single points of failure. [34]
Throughput & Scalability	4	5.0	Parallel block production enables high TPS and low latency without sharding or L2s. [7]

Privacy Tooling	4	3.5	L1 is pseudonymous. L2/off-chain solutions (e.g., WarpCore) are required for full compliance. [5]
Programmability	3	2.0	L1 is not Turing-complete. L2 solutions (e.g., Kasplex) are required, which is a deliberate design choice. [4]
Energy Profile	3	4.5	kHeavyHash is a highly efficient PoW algorithm that also reduces wasted work. [25]
Regulatory Comfort	2	2.5	As a public, permissionless chain, it is new to regulators. The intermediated model helps mitigate this. [3]
Maturity/Tooling	2	3.0	Growing ecosystem with Go/Rust clients but lacks the institutional maturity of other platforms. [17]
TCO/Ops	1	3.5	Pruned nodes are cheap to run, but archival nodes are expensive. The overall model is low-cost. [9]

Interoperability	1	2.5	No native interoperability. Requires L2 solutions and bridges, which introduce complexity. [39]
Total Weighted Score	-	**41.0**	-

- **Ethereum/L2s:** Ethereum excels in native programmability due to its EVM, but this comes at the cost of higher L1 latency, gas fee unpredictability, and a more complex security model.[13] Its move to PoS and L2s introduces trust assumptions that are not present in a pure PoW system. For the Digital Euro, which is designed to be a simple, non-programmable monetary layer, this native complexity is a drawback, not an advantage. An L2 solution built on Ethereum could be a contender for the private-sector-led policy layer, but the L1 itself is not a superior fit for the core monetary protocol.
- **Solana:** Solana offers high throughput and low latency, but its design comes at a significant cost to decentralization and stability.[11] Its high hardware requirements for running a validator node and its history of frequent outages make it an unsuitable choice for a core payments rail that must be resilient and continuously available.
- **Permissioned DLTs (Hyperledger, Corda):** These DLTs offer deterministic finality and a high degree of regulatory comfort.[36] However, they completely sacrifice the public-good nature, censorship resistance, and decentralized resilience that are core to the Digital Euro's mandate.[18] This would be a superior choice only if the ECB discards its stated goals for a public, cash-like digital currency.

The lack of native smart contracts on Kaspa is a potential gap, but it is a gap that can be filled by an L2 control plane (e.g., Kasplex) anchored to the L1.[4] This approach provides a mitigation that ensures the core protocol remains simple and non-programmable, while allowing PSPs to build a rich ecosystem of services on a trustless L2. The analysis concludes that, even with this mitigation, Kaspa remains a superior architectural choice, as its foundational layer is fundamentally more aligned with the non-negotiable requirements of the digital euro than any of the alternatives.

Conclusions & Go/No-Go Criteria

This comprehensive assessment concludes that a Kaspa-based retail Digital Euro is technically feasible and highly aligned with the Eurosystem's policy objectives. The blockDAG architecture provides a novel and powerful solution to the scalability challenges of a public, decentralized ledger, offering high throughput and low latency without compromising the foundational security of Proof-of-Work. The system's layered design—with a simple, non-programmable L1 and an off-chain/L2 policy enforcement layer—is a deliberate and strategic choice that directly addresses the core requirements for privacy, financial stability, and the intermediated model.

The primary trade-off is the adoption of a probabilistic finality model. However, the analysis demonstrates that a rigorously defined and tested finality threshold can meet and even exceed the performance demands of a modern payments system. While the operational requirements for running a full archival node present a potential centralizing force, the availability of lightweight pruned nodes and a clear separation of institutional roles mitigates this concern.

The project should proceed with a multi-phase pilot plan to validate the technical assumptions and prove the model's viability in a real-world setting. The go/no-go decision should be based on the following criteria:

- **Go:** Proceed to a city-scale pilot if the technical benchmarks prove a p99 confirmation latency of under 10 seconds, if the offline payment protocol with a hardware partner is successful, and if the legal and regulatory frameworks for selective disclosure and the intermediated model are ratified.
- **No-Go:** The project should be re-evaluated if a consensus cannot be reached on the finality model's suitability for retail payments, if performance benchmarks fail to meet the established SLAs, or if a transparent, accountable governance framework for the Kaspa protocol cannot be formalized to the Eurosystem's satisfaction.

A successful pilot would not only provide a robust blueprint for a Digital Euro but would also set a new global standard for how a central bank can leverage a decentralized, public ledger to serve the public interest, providing a resilient, open, and sovereign payments infrastructure for the digital age.

Works cited

1. Kaspa WIKI: HOME, , https://wiki.kaspa.org/
2. About Kaspa, , https://kaspa.org/about-kaspa/
3. WHAT DOES THE EUROPEAN COMMISSION'S ... - Clifford Chance, , https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/07/what-does-the-european-commissions-digital-euro-proposal-mean-for-the-future-of-money-in-the-eu.pdf
4. Kasplex L2: A Light-Weight Based Rollup Solution on Kaspa (APR 2025) - Medium, , https://medium.com/@KaspaKEF/kasplex-l2-a-light-weight-based-rollup-solution-on-kaspa-33a5939bdf61
5. Digital euro | Legislative Train Schedule - Carriages preview ..., , https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-digital-euro
6. The race to finality: How Kaspa changes the game | by JC | Aug ..., , https://medium.com/@jcroger/the-race-to-finality-how-kaspa-changes-the-game-51ee52e91133
7. Kaspa: Home, , https://kaspa.org/
8. Kaspa (KAS): The High-Speed Proof-of-Work Blockchain Revolution - InsiderFinance Wire, , https://wire.insiderfinance.io/kaspa-kas-the-high-speed-proof-of-work-blockchain-revolution-ea0495a059d4
9. Node - Kaspa WIKI, , https://wiki.kaspa.org/node
10. Kaspa — Decentralization and Mining Pools, , https://kaspa.org/kaspa-decentralization-and-mining-pools/
11. What TECHNICAL or ECONOMICAL concerns do you have in regards to KASPA? Can these concerns be overcome with time? : r/CryptoTechnology - Reddit, , https://www.reddit.com/r/CryptoTechnology/comments/1h5cw8q/what_technical_or_economical_concerns_do_you_have/
12. docs/Getting Started/Full Node Installation.md at main · kaspanet/docs - GitHub, , https://github.com/kaspanet/docs/blob/main/Getting%20Started/Full%20Node%20Installation.md
13. Kasplex L2: A lightweight Rollup solution based on Kaspa - PANews, , https://www.panewslab.com/en/articles/a546pscqwgj8
14. Digital Operational Resilience Act (DORA), , https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
15. Third Progress Report on the Digital Euro Preparation Phase - Banca d'Italia, , https://www.bancaditalia.it/media/notizia/third-progress-report-on-the-digital-euro-preparation-phase/
16. Digital Euro Nears Reality: Key Takeaways from the ECB's Third Progress Report, , https://digital-euro-association.de/blog/takeaways-from-the-ecbs-third-progress-report
17. Kaspa on Rust — Improving Performance, , https://kaspa.org/kaspa-on-rust-improving-performance/

18. Digital euro - Wikipedia, , https://en.wikipedia.org/wiki/Digital_euro
19. How to Launch a Low-Fee Token Like Kaspa (KAS) - Blockchain App Factory, , https://www.blockchainappfactory.com/blog/how-to-launch-low-fee-token-like-kaspa/
20. What is Kaspa (KAS): A Beginner's Guide - 99Bitcoins, , https://99bitcoins.com/cryptocurrency/kaspa-review/
21. The ECB's case for central bank digital currencies - European Union, , https://www.ecb.europa.eu/press/blog/date/2021/html/ecb.blog211119~fda94a3f84.en.html
22. FAQs on a digital euro - European Central Bank, , https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.html
23. A Digital Euro | Central Bank of Ireland, , https://www.centralbank.ie/financial-system/a-digital-euro
24. ECB Advances Digital Euro: Privacy, Offline Functionality, and Future Plans - FTF, , https://fintechfrontiers.live/ecb-advances-digital-euro-privacy-offline-functionality-and-future-plans/
25. Kaspa Crypto: Speed, Scalability, and Future Potential Explained - Ulam Labs, , https://www.ulam.io/blog/kaspa-crypto-understanding-speed-scalability-and-potential
26. Kaspa Blockchain: Better Speed and Scalability with BlockDAG - TheHolyCoins, , https://theholycoins.com/news/kaspa-blockchain-solving-scalability-and-speed-challenges-with-blockdag-innovation
27. Kaspa Blockchain: Revolutionizing Speed and Scalability with GHOSTDAG Technology, , https://www.okx.com/learn/kaspa-blockchain-speed-scalability
28. The digital euro after the investigation phase: Demystifying fears about bank disintermediation | CEPR, , https://cepr.org/voxeu/columns/digital-euro-after-investigation-phase-demystifying-fears-about-bank
29. Cryptocurrency: Selected Policy Issues - Congress.gov, , https://www.congress.gov/crs-product/R47425
30. Anti-Money Laundering and Blockchain Technology - Projects at Harvard, , https://projects.iq.harvard.edu/files/financialregulation/files/aml_case_study_0.pdf
31. Central bank digital currency - Wikipedia, , https://en.wikipedia.org/wiki/Central_bank_digital_currency
32. ECB provides offline digital euro progress report - Ledger Insights - blockchain for enterprise, , https://www.ledgerinsights.com/ecb-provides-offline-digital-euro-progress-report/
33. DORA vs NIS2: Key Differences and Similarities | House of Control, , https://www.houseofcontrol.com/blog/dora-vs-nis2
34. What is partition tolerance in the CAP Theorem? - Milvus, , https://milvus.io/ai-quick-reference/what-is-partition-tolerance-in-the-cap-theorem
35. CAP theorem - Wikipedia, , https://en.wikipedia.org/wiki/CAP_theorem
36. Central Bank Digital Currencies: A Survey - arXiv, , https://arxiv.org/html/2507.08880v1

37. How to Ensure Resistance to DDoS Attacks? - StormWall, , https://stormwall.network/resources/blog/how-to-ensure-resistance-to-ddos-related-threats
38. An overview of PHANTOM: A blockDAG consensus protocol (part 3) | by Drew Stone, , https://medium.com/@drstone/an-overview-of-phantom-a-blockdag-consensus-protocol-part-3-f28fa5d76ef7
39. Warpcore – Kaspa Kii, , https://kaspa-kii.org/warpcore/
40. Central Bank Digital Currency and financial stability - European ..., , https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2783~0af3ad7576.en.pdf
41. mempool package - github.com/kaspanet/kaspad/mempool - Go Packages, , https://pkg.go.dev/github.com/kaspanet/kaspad/mempool
42. KASPA - Decentralized Finance - IQ.wiki, , https://iq.wiki/wiki/kaspa
43. Merging and Rewards | Kaspa WIKI, , https://wiki.kaspa.org/merging-and-rewards
44. THE GHOST-DAG PROTOCOL - Scaling Bitcoin, , https://tokyo2018.scalingbitcoin.org/files/Day2/the-ghost-dag-protocol.pdf
45. What Is a Blockchain Reorg and Why It Matters - Bitcoin.com News, , https://news.bitcoin.com/what-is-a-blockchain-reorg-and-why-it-matters/
46. nwbower/pi-docker-kaspad: Kaspa Node in Docker on a Raspberry Pi 4 Model B 8GB - arm64 - GitHub, , https://github.com/nwbower/pi-docker-kaspad
47. Setting Up a CLI Node | Kaspa WIKI, , https://wiki.kaspa.org/setting-up-a-cli-node
48. Rust vs Go in 2025 - Bitfield Consulting, , https://bitfieldconsulting.com/posts/rust-vs-go
49. en.wikipedia.org, , https://en.wikipedia.org/wiki/Colored_Coins#:~:text=Colored%20Coins%20is%20an%20open,used%20to%20establish%20asset%20ownership.
50. Colored Coins - Wikipedia, , https://en.wikipedia.org/wiki/Colored_Coins
51. Token Burning, explained - Trust Wallet, , https://trustwallet.com/blog/crypto-basics/token-burning-explained
52. Project Rosalind provides key lessons on retail CBDC system, , https://www.retailbankerinternational.com/news/project-rosalind-provides-lessons-on-key-aspects-of-retail-cbdc-system/
53. BIS, Bank of England complete CBDC trial using blockchain - Ledger Insights, , https://www.ledgerinsights.com/cbdc-bis-bank-of-england-blockchain-rosalind/
54. Frequently asked questions | ISO20022, , https://www.iso20022.org/faq
55. Miner Collusion and the Bitcoin Protocol - Cowles Foundation for Research in Economics, , https://cowles.yale.edu/sites/default/files/2022-11/parlour-miner-collusion-and-bitcoin-protocol.pdf
56. KASPA Live Price Data - KuCoin, , https://www.kucoin.com/price/KAS
57. How can I troubleshoot high target latency on an AWS DMS task?, , https://repost.aws/knowledge-center/dms-high-target-latency
58. Payments statistics: first half of 2024 - European Central Bank, , https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2024h1~5263055ced.en.html

59. Kaseya GDPR Resource Center - What, Why and Who of GDPR, , https://www.kaseya.com/gdpr/
60. Kaspa's Desserts Privacy Policy, , https://kaspas.co.uk/privacy-policy/
61. What are the Large Scale Pilot Projects - EU Digital Identity Wallet - - European Commission, , https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487808/What+are+the+Large+Scale+Pilot+Projects
62. Kaspa (KAS) Tokenomics Explained: Emission, Supply, and Incentives, , https://www.findas.org/tokenomics-review/coins/the-tokenomics-of-kaspa-kas/r/8xkQoBdciZj1cU6r3RtCgt
63. Retail CBDC: Implications for Banking and ... - Annual Reviews, , https://www.annualreviews.org/content/journals/10.1146/annurev-financial-082123-105958?crawler=true&mimetype=application/pdf
64. Members - Digital Euro Association, , https://digital-euro-association.de/members
65. Discover CBDCs: An IMF Roadmap for Central Banks - maseconomics, , https://maseconomics.com/discover-cbdcs-an-imf-roadmap-for-central-banks/
66. 8 Important Metrics for Retail Industry KPIs | Tableau, , https://www.tableau.com/learn/articles/retail-industry-metrics-kpis
67. kaspa-grpc-client — unregulated finances, in Rust // Lib.rs, , https://lib.rs/crates/kaspa-grpc-client