Night Coin

A next-generation privacy cryptocurrency

Legal Disclaimer

This document is provided for informational purposes only and does not constitute financial, investment, or legal advice. Night Coin (XNT) is an experimental decentralized protocol under active development. Participation involves risks, including but not limited to software defects, economic attacks, and regulatory changes. Nothing in this paper constitutes an offer to sell or the solicitation of an offer to buy any tokens or securities. Prospective participants should conduct their own due diligence and comply with all applicable laws in their jurisdictions.

Context & Motivation

Bitcoin is not anonymous. In the early Silk Road era, Bitcoin's pseudonymous design was widely misinterpreted as anonymity. However, open-ledger analysis and off-chain records enabled investigators to trace flows from Silk Road to real-world identities, demonstrating that Bitcoin transactions are traceable without additional privacy layers. This historical lesson highlights the need for privacy-preserving protocols at the base layer.

Why Monero for peer-to-peer privacy. Monero introduced ring signatures, stealth addresses, and RingCT to conceal senders, receivers, and amounts by default. It remains the go-to choice for individuals seeking robust on-chain privacy in everyday P2P transfers.

From Grin to Tari: making Mimblewimble practical. Mimblewimble (MW) achieves confidentiality and scalability via cut-through and aggregated transactions. Grin proved MW's lightweight design, but its interactive transactions hindered commerce since both parties needed to be online. Tari advances MW with an addressing layer for non-interactive payments, retaining MW's compactness while improving usability for merchants and services.

Threat model update: 2025 Monero hashrate crisis. In 2025, a well-resourced competitor, Qubic, organized miners and subsidies to capture a dominant share of Monero's hashrate, prompting exchanges to take precautions and exposing how economic coordination can endanger PoW networks. This episode motivates Night Coin's phased **PoW → PoS** design: bootstrap with ASIC-resistant PoW, then migrate to stake-weighted finality where attacks require acquiring and risking stake.

Vision

NightCoin’s vision is to deliver private-by-default payments that are usable in the real world, hard to capture, and sustainable for decades. We focus on five pillars: privacy, resilience, scalability, accessibility, and sustainability.

Privacy

Design goal. Privacy in digital payments must balance individual confidentiality with practical usability. Night Coin adopts a Tari-style, address-enabled Mimblewimble base layer to combine compact chain state with non-interactive transactions.

Bitcoin. Transparent UTXOs and permanent public records enable forensic clustering and flow analysis. While transparency supports auditability, it exposes spending patterns and counterparties, as shown in the Silk Road investigations. Bitcoin users must rely on external tools (mixers, CoinJoin, or off-chain paths) for privacy, each with trade-offs and surveillance risk.

Monero. Default privacy via ring signatures (plausible-deniability inputs), stealth addresses (unlinkable outputs), and RingCT (confidential amounts). Monero demonstrates strong resistance to routine tracing, though higher resource usage and regulatory friction can impact adoption in certain jurisdictions.

Grin (MW). Mimblewimble reduces on-chain data via cut-through, removing spent transaction links and aggregating transactions, yielding a lightweight chain. However, its interactive transaction model complicates asynchronous commerce and custodial flows.

Tari-style MW with addresses (adopted by Night Coin). By introducing long-lived recipient identifiers and one-time stealth addresses for non-interactive payments, Tari preserves MW's confidentiality and scalability while enabling practical UX for wallets, merchants, and cold storage. Benefits include: (1) non-interactive sends to offline recipients; (2) unlinkability via one-time outputs; (3) compact chain state from MW cut-through; and (4) business compatibility through stable addressing and invoice workflows.

Consensus Mechanism

Phase1 —Proof-of-Work Bootstrapping (≈3 months). Night Coin starts with CPU-friendly, ASIC-resistant RandomX to maximize miner diversity at launch. Blocks target 5-minute intervals (≈105,120 blocks/year) with a constant 500 XNT reward. To harden security during the small-cap phase, Night Coin supports optional auxiliary merge-mining with compatible PoW networks where practical.

Economic Transition Trigger. The network transitions to PoS when the cost of capturing a supermajority of stake (including slashing risk) exceeds the cost of achieving a 51% PoW hashrate for a sustained period. This aligns attack costs with the asset's market value and deters rent-a-hash or subsidy-driven takeovers.

Phase 2 — Proof-of-Stake (LMD-GHOST). Night Coin adopts an LMD-GHOST fork-choice with finality. Staking yields 10% APY for the first two years to decentralize stake, then stabilizes at 6%. A baseline 3% inflation funds staking rewards with zero transaction fees, prioritizing UX. Empty blocks still mint rewards to preserve liveness. Security features include slashing for equivocation, inactivity leak recovery, and stake-weighted finality that resists hashrate manipulation.

References

• Poelstra,A. (2016).Mimblewimble (PDF).

• Tari Labs University. Mimblewimble transactions explained; addressing & stealth addresses updates.

• Monero Research Lab (2015). Ring Confidential Transactions (MRL■0005).

• Silk Road & Bitcoin traceability: U.S. DOJ court filings; WIRED trial coverage.

• Ethereum Beacon Chain & LMD■GHOST explainers (ethos.dev; Ethereum Research).

• 2025 Monero hashrate / Qubic event: exchange notices and security analysis (e.g., Kraken pause, Halborn blog, Cointelegraph).