Ndani: Trustless Privacy-Preserving Infrastructure for Machine Economies

Solomon Kembo [Affiliation]

Abstract

The Internet of Things generates extraordinary value, yet IoT devices capture none of it. Existing IoT-blockchain systems—IOTA, Helium, IoTeX—enable device *owners* to earn cryptocurrency for device services, but payments flow to human-controlled wallets. The device remains an instrument, not an economic agent. We present Ndani (Swahili: *inside*), a protocol enabling IoT devices to hold wallets, earn revenue, and transact autonomously, while preserving formal privacy guarantees against all observers.

The core technical insight is that **anonymity requires device-held keys**. If a human wallet pays for device transactions, the payment links device to human identity, destroying privacy guarantees. Device-held wallets are not a design preference; they are a *logical requirement* for anonymous device operation. The natural objection—"compromised devices lose funds"—is addressed via ZK-enforced spending policies: owners define bounds, devices operate autonomously within them, and zero-knowledge proofs (not trust) enforce compliance.

Critical architectural decision: Each device deployment includes a farmer-owned Raspberry Pi 5 running the Midnight proof server locally. This eliminates the gateway trust problem present in prior designs. The proof server—which must see device identity and raw data to generate ZK proofs—is controlled by the device owner, not a third party. Privacy guarantees hold against *all external observers*, not merely chain observers.

Phase 1 (Privacy Foundation) establishes anonymous device attestations. We introduce BRACE (Blind Registration via Anonymous Commitment Enrollment), enabling devices to register without revealing identity. **Phase 2 (Economic Agency)** transforms privacy infrastructure into economic infrastructure. We introduce IAR (Incentivized Anonymous Relay) and ACR (Anonymous Contribution Rewards), enabling payment for anonymous attestations via nullifier-based claim tickets.

To our knowledge, no production system currently enables devices to hold their own wallets and transact autonomously with trustless privacy guarantees. Ndani demonstrates this is achievable by combining established security patterns—HSMs, smart contracts, hardware wallets—with ZK-based policy enforcement and farmer-owned proof infrastructure. Implementation on Midnight Network with ~$160 hardware validates practicality.

Keywords: zero-knowledge proofs, machine economy, IoT privacy, autonomous agents, anonymous payments, trustless infrastructure

1. Introduction

The Internet of Things generates extraordinary value. Consider *cold-chain verification*—the process of proving that temperature-sensitive goods (vaccines, produce, pharmaceuticals) remained within required temperature ranges during transport. The World Health Organization estimates that 50% of vaccines are wasted due to cold-chain failures. A temperature sensor proving supply-chain compliance enables transactions worth thousands of dollars. The sensor itself receives nothing—it cannot be paid, cannot pay for services, and cannot participate in the markets its data creates.

This creates **misaligned incentives**. Device owners have limited motivation to maintain hardware, ensure data quality, or participate in network infrastructure (such as relaying messages for other devices). IoT systems depend on altruistic cooperation that fails at scale, in adversarial environments, or when participants have competing interests.

Recent IoT-blockchain projects address this partially. **IOTA** introduced a DAG-based ledger optimized for machine-to-machine micropayments, featuring feeless transactions suitable for IoT. **Helium** incentivizes wireless infrastructure deployment: hotspot owners earn HNT tokens for providing LoRaWAN coverage, successfully bootstrapping a network of 900,000+ hotspots. **IoTeX** provides IoT-focused blockchain with hardware-backed device identity via the "Pebble" tracker.

These systems share a common limitation: **payments flow to human-controlled wallets**. The device remains an instrument for human earnings, not an economic agent itself. When a Helium hotspot earns HNT, the tokens go to the owner's wallet—the hotspot cannot spend, save, or transact autonomously.

We propose Ndani, a protocol enabling devices to hold wallets, earn revenue, and transact autonomously with *trustless privacy guarantees*. The name—Swahili for *inside*—reflects both the protocol's African origins and its role as infrastructure for machine economies.

1.1 The Core Argument: Anonymity Requires Device-Held Keys

Device-held wallets may seem like an optional architectural choice. They are not. They are a **logical requirement for anonymity**.

Consider the alternative: a device generates an anonymous attestation; a human wallet pays the transaction fee. The attestation is anonymous, but *the payment links device to human*. An adversary observing blockchain state sees: "anonymous attestation A was paid for by wallet W belonging to human H." Every privacy guarantee—blind registration, unlinkable nullifiers, zero-knowledge proofs—collapses.

For device anonymity to hold, the device must transact from keys that are not linked to human identity. This is not a design preference—it is a technical requirement of the threat model.

1.2 Trustless Architecture: Eliminating Gateway Trust

Prior designs for privacy-preserving IoT introduced a critical trust assumption: the *gateway problem*. Zero-knowledge proof generation requires access to the witness—the private inputs including device identity (pk, r) and raw sensor data. If proof generation occurs on a shared gateway operated by a third party, that operator sees everything the proof is meant to hide.

Ndani eliminates this trust assumption through a fundamental architectural decision: **each device deployment includes a farmer-owned Raspberry Pi 5 running the Midnight proof server locally**. The entity that sees device identity and raw data is the device owner—the same party who already has physical access to the device and its sensors.

This transforms the privacy model:

- **Prior design:** Privacy against chain observers only; gateway operator is trusted
- **Ndani:** Privacy against all external observers; no trusted third parties

The cost increase (~$110 for Pi 5 infrastructure) is justified by the elimination of trust assumptions. In adversarial environments—where government or corporate adversaries might compel gateway operators—trustless architecture is not optional.

1.3 Addressing the Objection: "Compromised Devices Lose Funds"

The natural concern: if devices hold value, compromised devices become attack targets. This objection assumes device autonomy requires device trust. Ndani decouples them.

We introduce **ZK-enforced spending policies**: owners define a policy P constraining device spending (maximum amounts, approved transaction types, daily limits). Every device transaction requires a zero-knowledge proof that P(tx) = true. The blockchain rejects non-compliant transactions, regardless of valid device signature.

An attacker who compromises device firmware cannot: drain the wallet (exceeds daily limit), send to arbitrary addresses (not in approved set), or bypass the policy (ZK proof required, policy embedded in cryptographic circuit). The device has autonomy—*bounded autonomy, enforced by mathematics, not trust*.

1.4 Contributions

1. **Trustless Architecture:** We demonstrate that farmer-owned proof servers eliminate gateway trust assumptions, achieving privacy against all external observers.
2. **Anonymity-Economic Correspondence:** We demonstrate that device-held wallets are required for anonymity (not merely convenient), and that ZK primitives enabling privacy simultaneously enable bounded economic agency.
3. **BRACE Protocol:** We introduce Blind Registration via Anonymous Commitment Enrollment—devices register without revealing identity to any external party (Section 4.2).
4. **ZK-Enforced Spending Policies:** We introduce device wallets with cryptographically-bounded autonomy—owners define rules, ZK proofs enforce them (Section 5.1).
5. **IAR and ACR Protocols:** We introduce Incentivized Anonymous Relay and Anonymous Contribution Rewards—economic incentives for mesh routing and payment for anonymous attestations (Sections 5.2, 5.3).

6. **Implementation:** Midnight Network deployment demonstrating ~$160 devices can participate in trustless anonymous machine economies (Section 6).

2. Background: Economy of Things

2.1 The Vision

The "Economy of Things" (EoT) describes a future where IoT devices participate directly in economic transactions—not merely as data sources, but as autonomous agents capable of negotiating, transacting, and holding value. Industry reports project EoT could generate trillions in value by enabling machine-to-machine commerce without human intermediation.

Concrete examples of what EoT could enable:

- **Sensors paying for connectivity:** A soil moisture sensor pays relay fees to mesh neighbors, sustaining network infrastructure without human coordination.
- **Attestation markets:** A cold-chain buyer posts: "I'll pay 0.01 tokens for proof that temperature stayed below 4°C during transit." Qualified sensors respond; payment settles; neither party knows the other's identity.
- **Self-sustaining devices:** An environmental monitor earns revenue from data attestations, automatically allocating 80% to owner and 20% to operational expenses (relay fees, gas costs).

2.2 The Gap

Capability	IOTA	Helium	IoTeX	Ndani
Device identity on chain	✓	✓	✓	✓
Micropayments for IoT	✓	✓	✓	✓
Device-held wallet	✗	✗	✗	**✓**
Autonomous spending	✗	✗	✗	**✓**
ZK-enforced spending policy	✗	✗	✗	**✓**
Trustless privacy (no gateway)	✗	✗	✗	**✓**
Anonymous attestations	✗	✗	✗	**✓**

Table 1: Capability comparison of IoT-blockchain systems. Yellow rows = capabilities no existing system provides. Ndani's contributions in bold.

3. Threat Model

We define adversaries targeting both privacy and economic mechanisms. The trustless architecture means privacy adversaries have no gateway operator to compromise.

3.1 Privacy Adversaries

Government Adversary (A_gov): Compels ISP cooperation, accesses telecommunications metadata, pressures cooperative leadership, conducts long-term traffic analysis. Objective: identify specific individuals for targeting or surveillance. *Note: Cannot compel gateway cooperation because no trusted gateway exists.*

Corporate Adversary (A_corp): Purchases historical platform data, correlates with public records (land registries, satellite imagery), incentivizes insiders. Objective: competitive intelligence, differential pricing.

Network Observer (A_net): Observes LoRa transmissions, logs submissions, performs timing analysis. Limited by encryption and the fact that proof generation occurs locally—observer sees only encrypted traffic to chain.

3.2 Economic Adversaries

Freeloading Adversary (A_free): Attempts to receive relay services without payment, or claim rewards without valid attestations.

Griefing Adversary (A_grief): Disrupts economic mechanisms—drops relayed messages after accepting payment commitment, submits invalid attestations, spams network.

Sybil Adversary (A_sybil): Registers multiple fake devices to manipulate markets or dilute anonymity sets. Constrained by registration costs and hardware requirements (ATECC608A).

3.3 Security Assumptions

Standard cryptographic assumptions: discrete log hardness (Ed25519), collision resistance (SHA-256, BLAKE2), ZK soundness (Midnight/Halo2 proving system). ATECC608A physical security for key extraction resistance. Farmer controls their own proof server (no third-party trust required).

4. Phase 1: Privacy Foundation

Phase 1 establishes the cryptographic substrate: anonymous device registration, ZK attestations, and formal privacy guarantees against all external observers.

4.1 Architecture Overview

Two-layer trustless architecture:

- **Layer 1 (Device + Local Proof Server):** ESP32-S3 microcontroller + ATECC608A secure element + SX1276 LoRa transceiver + environmental sensors (~$50). Connected via local network to Raspberry Pi 5 running Midnight proof server (~$110). Keys generated in ATECC608A; proofs generated on farmer-owned Pi 5. Total: ~$160.
- **Layer 2 (Midnight Network):** Dual-ledger blockchain with private contract state. Stores device commitment Merkle tree in encrypted private state (adversaries cannot enumerate registered devices), verifies proofs publicly, maintains nullifier set.

Critical difference from prior designs: No trusted gateway. The proof server—which must see device identity and raw data—is owned and operated by the farmer. Privacy guarantees hold against all external parties.

4.2 BRACE: Blind Registration Protocol

We introduce **BRACE (Blind Registration via Anonymous Commitment Enrollment)**, enabling devices to register without revealing identity to any external party.

Protocol 1: BRACE

Setup: Device generates keypair (pk, sk) inside ATECC608A secure element. Private key sk never leaves the chip—all signing operations occur within the secure element.

Registration:

1. Device samples random blinding factor r
2. Device computes commitment C = H(pk || r)
3. Local proof server generates ZK proof of well-formed commitment
4. Proof server submits (C, proof) to chain; chain adds C to Merkle tree, publishes new root

Security: The hiding property of H ensures no external party can link commitment C to public key pk. The ZK property ensures on-chain verifiers learn only that a well-formed commitment was registered—not which device or who owns it.

4.3 Privacy Guarantees

We define six formal privacy guarantees. Let λ be the security parameter, negl(λ) a negligible function. **All guarantees hold against all external observers—no trusted third parties.**

PG1 (Device Anonymity): For anonymity set A of size N, an adversary cannot identify which device produced a given submission with probability greater than 1/N + negl(λ).

PG2 (Unlinkability): Submissions from different epochs are computationally unlinkable. Achieved via epoch-based nullifiers: nullifier = H(device_secret || epoch).

PG3 (Data Confidentiality): ZK proofs reveal only predicate satisfaction (e.g., "temperature < 4°C"), not underlying values.

PG4 (Replay Resistance): On-chain nullifier set prevents duplicate submissions within an epoch.

PG5 (Network Metadata Protection): Network observers see only encrypted traffic; proof generation is local.

PG6 (Key Secrecy): ATECC608A secure element prevents key extraction even with physical device access.

5. Phase 2: Economic Agency

Phase 2 transforms privacy infrastructure into economic infrastructure. The same primitives—nullifiers, commitments, ZK proofs—gain economic interpretations.

5.1 Device Wallets with ZK-Enforced Policies

As established in Section 1.1, device-held wallets are required for anonymity. The ATECC608A already holds identity keys; extending to wallet keys is architecturally straightforward—the same secure element stores both.

Each device has an on-chain wallet in Midnight private state. The owner defines spending policy P; every transaction requires ZK proof that P(tx) = true.

Policy Components:

- Maximum per-transaction amount
- Approved transaction types (e.g., RELAY_FEE, GAS_PAYMENT, ATTESTATION_CLAIM)
- Daily/weekly spending limits
- Approved recipient addresses
- Revenue split ratios (e.g., 80% to owner, 20% retained for operations)

5.2 IAR: Incentivized Anonymous Relay

We introduce **IAR (Incentivized Anonymous Relay)**: economic incentives replace honest-majority trust assumptions for mesh routing between farms. Neither source nor relay learns the other's identity.

5.3 ACR: Anonymous Contribution Rewards

We introduce **ACR (Anonymous Contribution Rewards)**: payment for anonymous attestations via nullifier-based claim tickets. A buyer posts a bounty for attestations meeting a predicate; any qualifying device can respond; payment settles without either party knowing the other's identity.

5.4 Economic Security Properties

EG1 (Payment Integrity): Valid work receives payment; invalid work does not. Enforced by ZK verification before escrow release.

EG2 (Budget Compliance): Device spending cannot exceed policy bounds. Enforced by ZK proof of policy satisfaction.

EG3 (Relay Fairness): Relays are paid if and only if messages are delivered. Enforced by escrow release conditioned on confirmation.

EG4 (Sybil Resistance): Fake device registration is costly. Enforced by registration fees and hardware requirements (ATECC608A not trivially clonable).

6. Implementation

6.1 Hardware

Complete trustless deployment bill of materials:

Component	Function	Cost (USD)
Sensor Unit		
ESP32-S3	Microcontroller	$8.00
ATECC608A	Secure element (identity + wallet keys)	$2.50
SX1276 LoRa	Radio transceiver	$6.00
BME280 + soil sensor	Environmental sensing	$6.00
Solar panel + battery	Power	$16.00
Enclosure	Weather protection	$10.00
Subtotal (Sensor)		**~$48.50**

Component	Function	Cost (USD)
Local Proof Server		
Raspberry Pi 5 (8GB)	Midnight proof server	$80.00
Power supply + SD card	Pi infrastructure	$25.00
Enclosure	Protection	$10.00
Subtotal (Proof Server)		**~$115.00**
TOTAL	**Complete trustless deployment**	**~$163.50**

Table 2: Hardware bill of materials for trustless Ndani deployment.

6.2 Proof Server Performance (Pending Validation)

Critical research requirement: The Raspberry Pi 5 must be validated as performant for Midnight proof generation. Midnight uses the Halo2 proving system. Preliminary research indicates Halo2 can be memory-intensive (issues at ≥32KB input sizes on constrained hardware). The Pi 5's 8GB RAM and Cortex-A76 cores (2.4GHz) are expected to be sufficient for Ndani's circuits, but this requires empirical validation.

Validation targets:

- ARM64 compatibility of Midnight proof server Docker image
- Proof generation time for BRACE registration circuit
- Proof generation time for attestation circuit (Merkle membership + signature + predicate)
- Peak memory usage during proving
- Thermal stability under repeated proof generation

Acceptable thresholds: For agricultural use cases (daily or hourly attestations), proving times up to 5-10 minutes are acceptable. The farmer submits data, proof generates in background, transaction settles.

6.3 Midnight Contracts

Four Compact contracts totaling ~500 lines of code: Registry (device commitment Merkle tree), Attestation (ZK proof verification, nullifier tracking), Wallet (device balances, ZK-policy enforcement), Bounty (ACR escrow, reward payout).

7. Known Limitations

L1 (Sensor Integrity): ZK proofs verify cryptographic validity, not sensor accuracy. A device lying about temperature still produces valid proofs. This is a fundamental limit of attestation, not specific to Ndani. Mitigation requires orthogonal solutions (reputation systems, redundancy, physical audits).

L2 (Pi 5 Performance): Raspberry Pi 5 performance for Midnight proof generation requires empirical validation. If Pi 5 proves insufficient, alternative ARM64 hardware (e.g., Orange Pi 5, Odroid) or x86 mini-PCs may be required.

L3 (Testnet Only): Implementation validated on Midnight testnet. Mainnet economics, gas costs, and token volatility remain to be demonstrated.

L4 (Platform Dependency): Requires Midnight or equivalent private-state blockchain. Public chains allow enumeration attacks on the device registry.

8. Discussion

Cost-Trust Tradeoff. The ~$160 deployment cost is approximately 3x the $50 sensor-only cost. This premium buys trustless operation: no gateway operator to compromise, no third party seeing device identity or raw data. In adversarial environments—where government or corporate adversaries are realistic threats—this premium is justified. In benign environments with trusted community infrastructure, shared gateways may remain appropriate.

Novelty Acknowledgment. To our knowledge, no production system currently enables devices to hold wallets and transact autonomously with trustless privacy guarantees. The closest analogues are enterprise HSMs (which hold keys but lack blockchain integration and require trusted operators) and hardware wallets (which require human approval). Ndani's contribution is demonstrating this is achievable with ZK-enforced policy bounds and farmer-owned proof infrastructure.

Future Work. (1) Validate Pi 5 proof server performance empirically. (2) Explore lighter ZK schemes enabling on-device proving (eliminating proof server entirely). (3) Formal verification of Compact contracts. (4) Privacy-preserving reputation systems for sensor integrity. (5) Cross-chain bridges for token interoperability.

9. Conclusion

Ndani demonstrates that privacy-preserving IoT and autonomous machine economics are not separate problems—they are the same problem, addressed by the same cryptographic primitives. The core insight is that **anonymity requires device-held keys**, and ZK-enforced spending policies make device wallets safe.

The critical architectural decision—farmer-owned proof servers—eliminates the gateway trust problem that would otherwise undermine privacy guarantees. The additional cost (~$110 for Pi 5 infrastructure) buys trustless operation: privacy guarantees hold against all external observers, not merely chain observers.

The protocols introduced—BRACE for anonymous registration, IAR for incentivized relay, ACR for anonymous rewards—transform privacy infrastructure into economic infrastructure. Implementation on Midnight Network with ~$160 hardware demonstrates this is practical, not theoretical.

The Economy of Things will not emerge from centralized platforms treating devices as passive data sources. It requires infrastructure where devices can transact privately, earn for their contributions, and operate autonomously within owner-defined bounds—*without trusting any third party*. Ndani provides that foundation.

References

[1] S. Popov. "The Tangle." IOTA Whitepaper, 2018.

[2] Helium Systems. "Helium: A Decentralized Wireless Network." 2019.

[3] IoTeX. "IoTeX: A Decentralized Network for Internet of Things." 2018.

[4] World Health Organization. "Immunization Supply Chain and Logistics." 2021.

[5] Deloitte. "Economy of Things: Extracting New Value from IoT." 2018.

[6] IOTA Foundation. "Machine Economy." IOTA Research, 2021.

[7] E. Ben-Sasson et al. "Zerocash: Decentralized Anonymous Payments." IEEE S&P, 2014.

[8] Aztec Protocol. "AZTEC Protocol Whitepaper." 2018.

[9] Input Output Global. "Midnight: A Data Protection Blockchain." 2024.

[10] M. Wooldridge. "An Introduction to MultiAgent Systems." Wiley, 2009.