IntentEX: Protocol Engineering Whitepaper
Author: Steven Alber
Date: June 22, 2025
Version: Technical v1.0

Foreword

The digital economy is standing at the edge of reinvention.

For decades, our thoughts — the most intimate signals of economic desire — have been harvested, profiled, and monetized without our consent or compensation. We believe this era is ending. And something radically new is beginning.

IntentEX is the first protocol designed to capture *subconscious, real-time intent* and transform it into a new asset class: live, ephemeral, user-licensed signals.

This document is not theory. It is a buildable, verifiable, and execution-ready architecture. It is written for engineers, cryptographers, product architects, and visionary builders who want to help reshape how value moves in the cognitive era.

If you've been waiting for a moment to contribute to something that is both technically challenging and philosophically meaningful — this is it.

We are assembling a global team of developers, protocol designers, and zero-knowledge specialists to bring IntentEX into reality. Your fingerprints could shape the future of this system — and with it, the next phase of participatory economics.

I invite you to read, fork, question, and build.

Your thoughts deserve more. Let's tokenize them.

— Steven Alber
Founder, IntentEX Protocol

1 Overview

1.1 System Scope

IntentEX is a real-time, end-to-end protocol that transforms ephemeral, on-device human micro-intents into cryptographically licensed assets that can be traded on an open on-chain order book. It solves three coupled problems:

Legacy Data Economy	IntentEX Solution
Third-party cookies, fingerprinting and stale brokered profiles	100 % on-device parsing; only a ZK-attested intent hash leaves the device ntEX_ Marketplace.pdf.pdf](file-service://file-3iEszdnTcdx3VDkLsPJa4N)
Guess-based ad bidding with 500 ms–seconds latency	<50 ms parse → <200 ms proof → <200 ms bid clearing
Users earn $0 while intermediaries capture the entire margin	95 % of licence proceeds paid to the user in stablecoins in < 5 s ntEX_ Marketplace.pdf.pdf](file-service://file-3iEszdnTcdx3VDkLsPJa4N)

1.2 Intent ≠ Conventional Data

Intent is defined as a high-entropy, short-lived behavioural vector (“I am about to buy noise-cancelling headphones <$200”) detected at the moment of cognitive formation. It differs from clickstreams or demographic profiles in that it:

- expires in minutes, not months;
- has far higher predictive power per byte;
- is licensable without ever revealing the raw stimulus that generated it.

2 Component Stack

Layer	Key Tech Choices	Engineering Notes
Edge-LLM	3 B-parameter transformer, 4-bit QLoRA, int8 matrix multiply fallback. Runs on iOS Neural Engine, Android NNAPI, Apple M-series, desktop Apple Silicon. Target ≤ 50 ms inference for 256-token window. ntEX_ Marketplace.pdf.pdf](file-service://file-3 iEszdnTcdx3VDkLsPJa4N)	
ZK Proof Engine	Primary: Halo 2 (Plonkish) for succinctness; backup: Risc-Zero STARK for transparent setup. Circuits written in	

	Noir; compiled to WASM prover.
Intent Tokenizer	LicensePacket = {intent_id, category, confidence, price_floor, expiry_ts, revocation_root}. Serialized with CBOR; SHA-256 hash committed on-chain.
On-chain Order Book	Move smart-contracts (Sui) using shared object model. Bids stored as “cancellable offers” to enable atomic match-and-settle. 50 k TPS capacity with ≤ 400 ms finality (Sui v1.13 benchmark).
Intent Vault UX / Wallet	React-Native + Rust FFI SDK; one-device-one-wallet enforced via Ed25519 hardware-bound key + confidential device fingerprint.
Post-Quantum Revocation	Each licence embeds a XMSS hash-based one-time signature. Upon expiry the

	revocation Merkle root is rotated; buyers must present a still-valid signature each API poll.
Federated Learning Loop	FedAvg w/ Secure Aggregation over TLS + HPKE. Global model checkpoints signed and streamed via IPFS; devices update in background when idle ∧ battery > 40 %.

3 Data Lifecycle

(1) Activity → Edge-LLM → JSON intent_summary
(2) intent_summary → ZK Prover → π (proof) , vk (verification key hash)
(3) Device signs {π, licence_meta} → sends to Relay
(4) Relay → Order-Book.create_offer() on-chain
(5) Buyer bid matched → escrow USDC
(6) Buyer receives {intent_summary, π} via gRPC stream
(7) Licence expires (t+120 min) → Order-Book.revoke() emits RevocationEvent
(8) Off-chain revocation root update invalidates any late API pulls

4 ZKP System

Item	Spec

Statement	“Device D whose public key is in allow-set parsed raw input R and produced category C, confidence ≥ τ, at timestamp t.”
Inputs	Poseidon hash of R, device key, model weights hash, category index, confidence score.
Outputs	Proof π, public signals {category, confidence_range, time_slice_id}.
Circuit Size	≈ 1.3 M constraints (Poseidon + affine ReLU). Halo 2 prover ~140 ms on A17 Bionic; verifier gas ~220 k on Sui.
Libraries	Noir (DSL), halo2-ecc, risc-0-zkvm fallback, Circom compat layer for custom gadgets.
Zero-Leakage	No raw R or device UID in public signals; model weights hashed inside the circuit, preventing model inversion.

5 Smart-Contract Architecture

```
module intentex::order_book {
    struct Offer has key { id: u64, seller: address, ipfs_cid:
vector<u8>,
```

```
                            price_floor: u64, expiry: u64, filled:
bool }
    public fun create_offer(o: Offer, sig: vector<u8>) { /* sig =
Ed25519 */ }
    public fun bid(offer_id: u64, amount: u64, buyer: address) { /*
escrow */ }
    public fun settle(offer_id: u64) { /* atomic transfer + emit
LicenceMinted */ }
    public fun revoke(offer_id: u64) { /* called by off-chain
relayer at expiry */ }
}
```

- Auction model: sealed-bid Vickrey variant to reduce bid shading.
- Escrow: USDC (Sui native) via fungible_asset::transfer_locked.
- Price-floor enforcement: contract rejects bids < price_floor.
- Cross-VM ports: lightweight adapters to EVM (ERC-20 escrow) and Cosmos SDK via IBC.

6 User Sovereignty & Control

- Intent Vault GUI
    - Price Curves: log-slider per category or flat minimum.
    - Blocklists: Bloom-filter of buyer IDs stored locally, hashed list committed on-chain for MEV-safe enforcement.
    - Sleep Mode: toggles parse_loop off; contract automatically pauses licence creation.
- Wallet Binding: Hardware-attested Ed25519 + local PIN/Biometrics; rotation revokes earning rights until

re-verification.

- $INTENT Utility (optional)
    - Stake to unlock premium categories.
    - Governance: parameter votes (max licence duration, protocol fee).
    - Market-making rewards for providing USDC/$INTENT liquidity.

7 Network Performance Targets

Stage	Latency Budget
Edge-LLM parse	≤ 50 ms
ZK proof generation	≤ 200 ms
Relay → on-chain inclusion	≤ 100 ms (Sui fast-path)
Bid-match + settlement	≤ 200 ms
End-to-end “click-to-cash”	≤ 550 ms

- Relay Layer: Anycast QUIC relays in us-east-1, eu-central-1, ap-se-1.

- Mempool protection: encrypted gossipsub until inclusion to thwart front-running.

8 Security Model

- Data-Minimisation Axiom: raw behavioural bytes never leave the secure enclave.
- Threats & Mitigations
    - Device compromise → local SE policy, OS Health attestation, remote wipe of key.
    - Front-running bids → in-contract commit-reveal salt + MEV-protected relays.
    - Licence replay → post-quantum XMSS signatures + revocation root rotation.
- Bug-Bounty: tiered payouts up to $250 k; mandatory audit by Trail of Bits.

9 Compliance & Ethics

- GDPR / CCPA: lawful basis = explicit, granular opt-in via Vault; right-to-be-forgotten implemented by key-pair burn (renders user’s proofs unverifiable).
- EU AI Act (2024/882): classified “minimal-risk” because inference is fully on-device; no biometrics, no profiling across users.

- Ethical Guardrails: licence categories tagged; health-related intents default-off, political-targeting blocked at protocol level unless DAO majority whitelists via governance.

10 Deployment Plan (Engineering-Ready)

Phase	Stack & Deliverables	Duration
MVP (Weeks 0–6)	Mobile SDK (Swift/Kotlin) with: quantised MiniLM-6B, Halo 2 prover (WASM), CBOR serializer; Sui-testnet contracts; gRPC relay. Test harness: criterion-bench + zk-bench.	6 wks
Alpha (Weeks 7–10)	Integrate Brave browser extension; 5 000 invited users; Sentry-style telemetry (only proof latency & gas, no PII). Benchmark: goal median Δt parse→settle < 700 ms.	4 wks
Beta (Weeks 11–14)	OEM preload POC with Oppo (ColorOS 15); federated learning	4 wks

	server on Fly.io; > 500 k DAU. Run zk-STARK vs SNARK shoot-out and publish.	
Prod v1 (Weeks 15–18)	Main-net launch, USDC payouts via Circle CCTP; ISO/IEC 27701 audit sign-off; Intent categories v1: Retail-Electronics, Travel-Booking, Gaming-In-App, Financial-Products.	4 wks
Tooling	zk-bench (Rust) – circuit time/size profiler; intent-sim (Go) – synthetic interaction generator; orderbook-fuzzer (Move) – invariant fuzz tests.	–

Integration Partners (signed / target): Brave, Arc Browser, Apple Shortcut plug-ins; future: Android Private Compute Core API, iOS App Intents.

Ready for Monday

All interfaces are specified, latency SLOs defined, and cryptographic primitives selected with post-quantum headroom. Engineering teams can begin parallel work on:

1. Edge SDK → parse/prove pipeline.
2. Order-book contracts → Move + cross-VM adapters.
3. Relay & Revocation services → Rust + QUIC.
4. Intent Vault UX → React-Native + Rust WASM bindings.

Detailed circuit definitions, API protobufs, and Move ABIs can now be committed to the mono-repo for immediate implementation.