Block 14 Review #2: IKP Accountable Wallet — Privacy Pools, Understanding as Key & Biometrics

Session summary: Three-part session covering Keegan Fukuda's Accountable Wallet / Privacy Pools work, the Relationship Proverb Protocol (Understanding as Key), and biometric key management. The throughline is wallet-level compliance, privacy, and recovery — all sitting at the IKP intersection of identity, key management, and privacy.

What landed:

Privacy Pools & Verifiable Compliance Affidavit (VCA): Keegan's core contribution is solving the centralized Association Set Provider (ASP) problem in Privacy Pools. The protocol has receivers check senders against crypto watchlists and record non-membership proofs on-chain as Verifiable Compliance Affidavits. These chain into provenance scores verified by "watchers" — third-party auditing entities that track compliance scores based on public information. The VCA paper is submitted to IEEE ICBC (under review). The semantic correction from VCR to VCA was accepted — important since VCR collides with Verifiable Credential Registry in the DID/VC ecosystem we work in.

Key open questions from the floor: who are the watchers practically, how do you establish watcher trust, and how do you get institutional recipients (Binance, Coinbase) to accept ZKP-based compliance proofs. The answer right now is: nobody accepts them yet. That's the gap the Ethereum Foundation RFP on Privacy Pools institutional integration is trying to close.

Understanding as Key / RPP: The proverb compression system was presented — using LLM-generated proverb summaries of documents as bilateral proof-of-understanding ceremonies, transmitted through Zcash's shielded memos and selectively disclosed on transparent chains. The visibility ratio concept (what proportion of each party's proverb is revealed) encodes the nature of the relationship. This is the methodology we've been using for meeting analysis and is now being formalized as a protocol.

Biometrics: Discussion on entropy vs. noise in biometric modalities (iris ~100 bits effective entropy, hand shape ~3 bits), fuzzy extractors for key recovery, and the persistent crypto community pushback against biometric approaches. Consensus: biometrics must be optional, backup is required, and perception remains a bigger barrier than the technology.

Overlap with active IKP work:

1. Taxonomy of Harms — directly connected. The session's closing note was "next topic: forensic analysis towards a common lexicon of harmful on-chain activities." The VCA/provenance scoring system is essentially a harm-prevention infrastructure — the watchlist non-membership proof is the forensics-analytics bridge we've been theorizing. The distinction between a watcher verifying public compliance data (analytics) and the VCA itself serving as evidence-grade proof of good faith (forensics) maps perfectly onto our forensics-analytics framework. The dusting attack problem Keegan raised (malicious actors sending dirty coins to damage honest users' provenance scores) is a harm category we need in the taxonomy.

2. Proof of Personhood & Agent Duality — convergent. The AI agent discussion was significant. The room explored using agents as privacy pool transaction transformers

(standardizing deposit patterns) and as high-frequency users that create adoption pressure on institutional recipients. This connects directly to our agent duality work: if AI agents are the primary users of privacy pools, then the association set becomes an agent verification mechanism. The “proof of honest trajectory” concept (proving a path through compliant states without revealing intermediate steps) is essentially agent provenance — and it’s a stronger formulation than point-in-time compliance checks.

The biometrics discussion feeds the PoP item directly: iris-based entropy (~100 bits) provides meaningful uniqueness, but the non-fixed entropy of living biology vs. fixed mathematical entropy is a framing our PoP document should adopt. World ID’s approach sits in this exact tension.

3. ZKP / SR 0011 — implementation context. The entire VCA system depends on ZK non-membership proofs. The scalability question (proving non-membership against 10,000+ sanctioned addresses) is a practical ZKP performance concern that our SR 0011 work contextualizes. Under PQC migration, these proofs need to transition to post-quantum ZK systems — connecting back to the crypto agility session.

4. Threat Intelligence / ISAC — watcher infrastructure. The watcher model (query-based vs. attestation-based) is essentially a threat intelligence sharing architecture. Watchers maintain real-time compliance databases, operate according to disclosed policies, and their scoring is publicly verifiable. This maps onto the STIX/TAXII-compatible sharing system we’re designing. The suggestion to use GliaNet data fiduciary pledges for watcher trust establishment is worth exploring as a governance model for our ISAC work.

5. RPP methodology. The Understanding as Key presentation formalizes what we’ve been doing with meeting reports — proverb compressions as bilateral proof-of-understanding ceremonies. The Zcash shielded ledger duality (private memo → selective transparent disclosure) provides the technical infrastructure for the discoverable-but-unlinkable relationship credentials we’ve been discussing.

Pending actions triggered:

- VCA acronym should be adopted in our documentation to avoid collision with Verifiable Credential Registry
- Dusting attacks need to be added to the Taxonomy of Harms as a provenance manipulation harm category
- “Proof of honest trajectory” should be explored as a formulation within the PoP + Agent Duality item — stronger than static compliance proofs for agent verification
- Watcher governance model should inform the ISAC threat intelligence sharing design — the query-based vs. attestation-based distinction maps onto our centralized vs. federated sharing architecture question
- The institutional adoption gap (no exchange accepting ZKP compliance proofs) is a governance problem BGIN can address through common language and evaluation frameworks — this could become a joint IKP-FASE deliverable

Compression seal: 🏛️🔍📋 — *The institution won’t accept the proof until the proof speaks the institution’s language.*