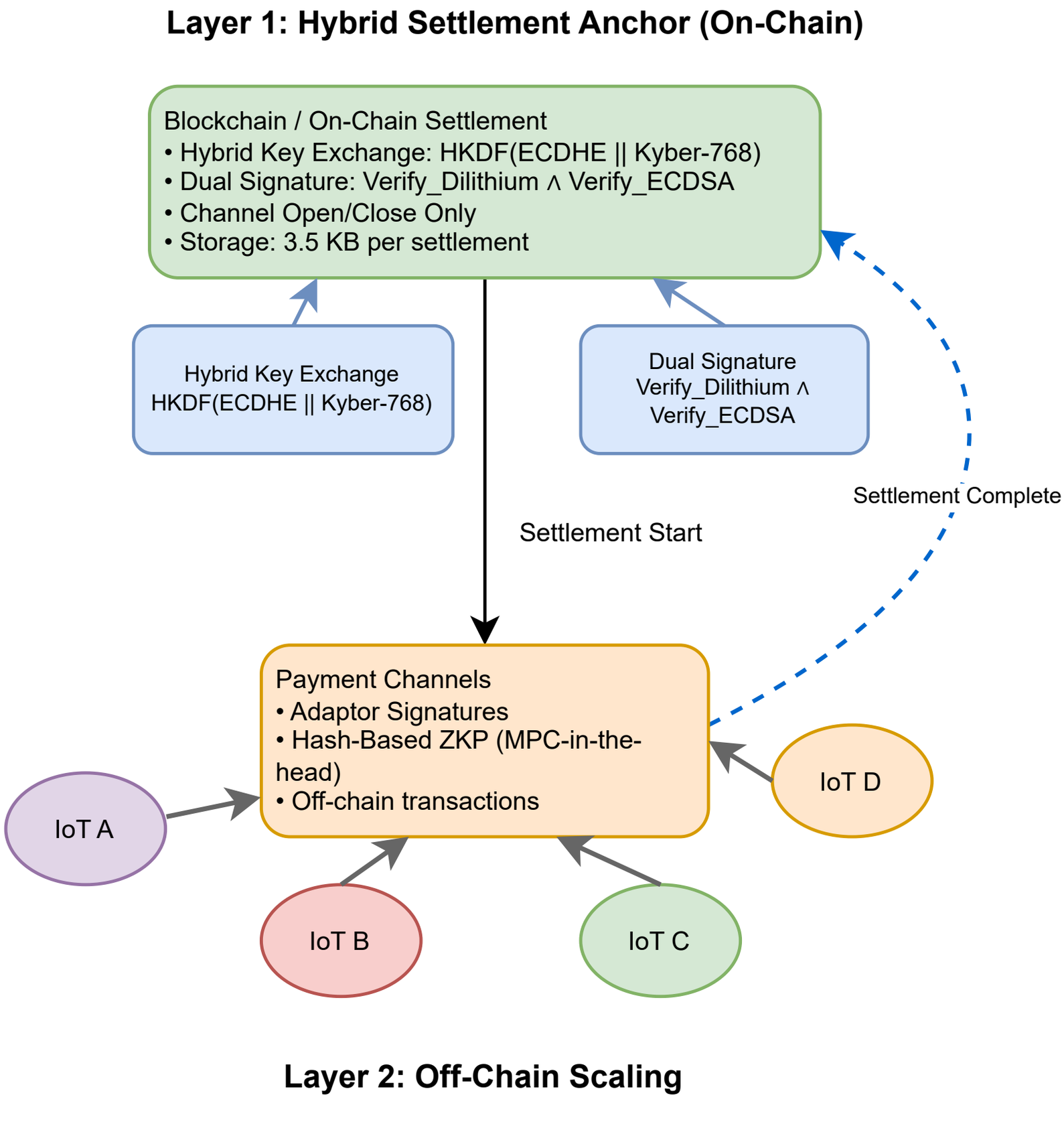
Layer 1: Hybrid Settlement Anchor (On-Chain)
Blockchain / On-Chain Settlement
• Hybrid Key Exchange: HKDF(ECDHE || Kyber-768)
• Dual Signature: Verify_Dilithium ∧ Verify_ECDSA
• Channel Open/Close Only
• Storage: 3.5 KB per settlement
Hybrid Key Exchange
HKDF(ECDHE || Kyber-768)
Dual Signature
Verify_Dilithium ∧
Verify_ECDSA
Settlement Start
Settlement Complete
Payment Channels
• Adaptor Signatures
• Hash-Based ZKP (MPC-in-the-head)
• Off-chain transactions
IoT A
IoT B
IoT C
IoT D
Layer 2: Off-Chain Scaling