CONF42

SECURING HFT AT SCALE

Event-Driven Architectures & Real-World Practices

Janardhan Reddy Chejarla, Calypso Technology

The HFT "Iron Triangle"

Speed vs. Security

The core conflict of HFT security is the **latency tax**. Every security control introduces delay.

- **Latency:** Microsecond requirements leave no room for traditional firewall inspections or heavy TLS handshakes.
- **Scale:** Processing millions of messages/sec makes "security by obscurity" fragile; automated controls are mandatory.
- **Monoliths:** Traditional Order Management Systems (OMS) cap out at 10k-50k orders/sec.

EVENT-DRIVEN & CLOUD-NATIVE

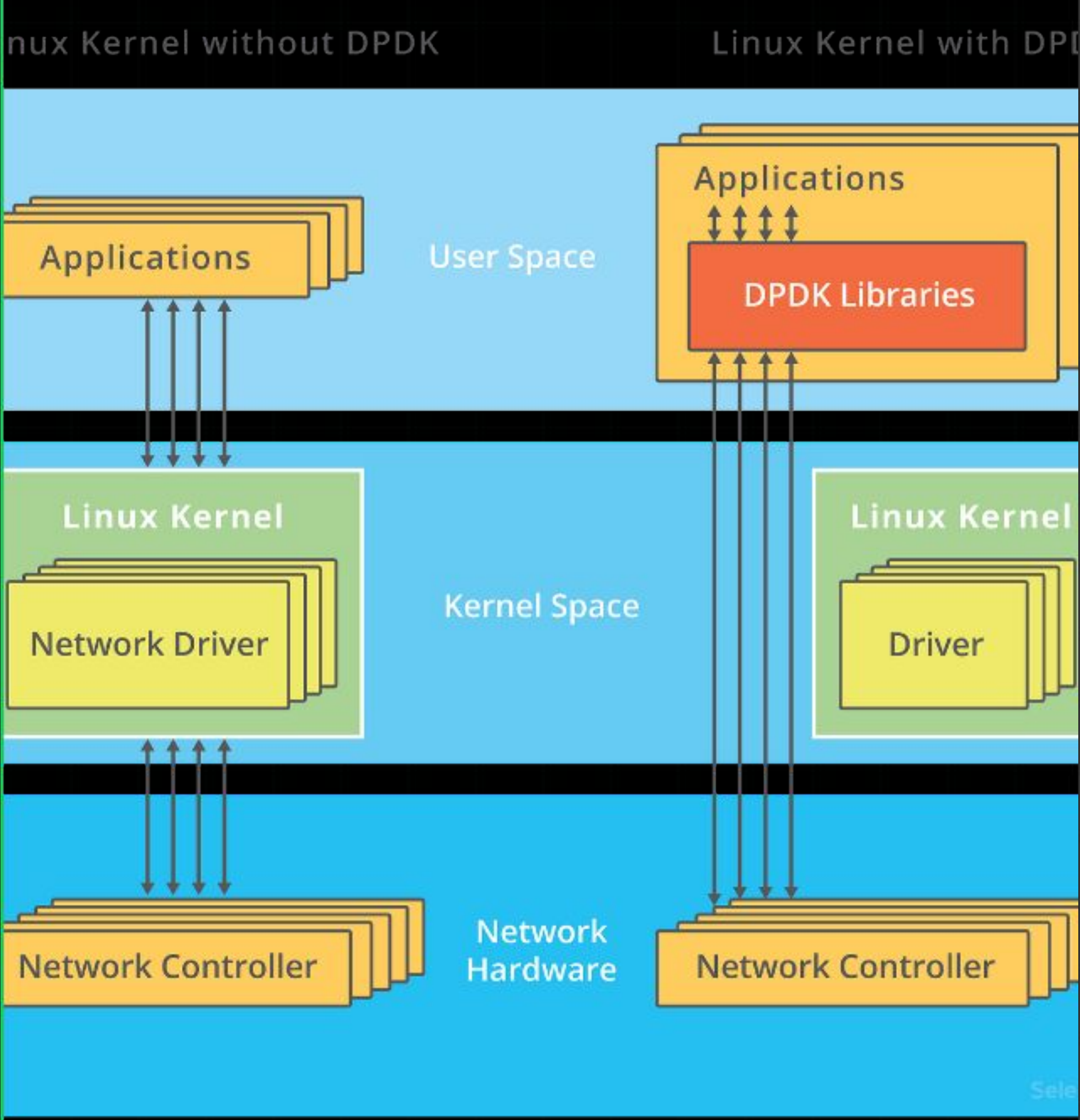
Microservices, Kafka, and Micro-Latency Services

The Latency Killer: Kernel Bypass

Avoiding the OS Tax

Standard OS networking stacks involve multiple memory copies and context switches, adding unacceptable latency (10-20µs).

- **The Fix:** Technologies like **DPDK** (Data Plane Development Kit) and **RDMA(**Remote Direct Memory Access) allow apps to talk directly to the NIC.
- **The Risk:** You bypass the kernel firewall (iptables). The application is now directly exposed to the wire.
- **The Mitigation:** Security must move upstream (network ACLs) or onto the hardware (SmartNICs).

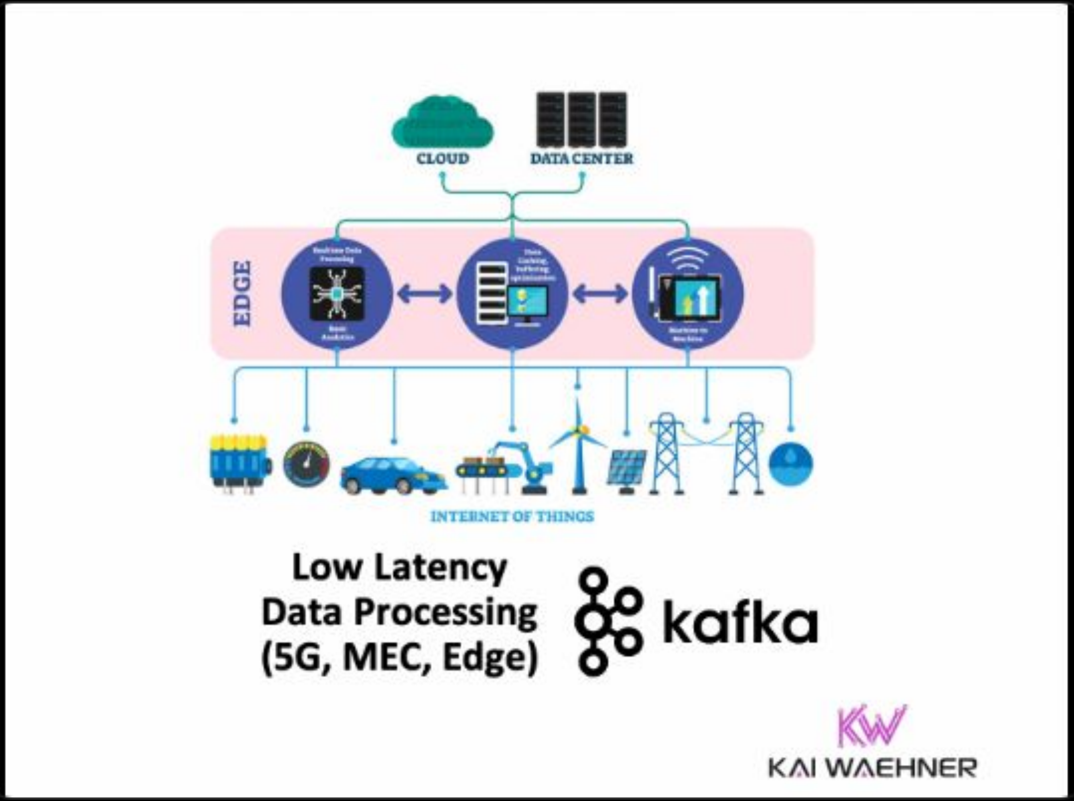


The Backbone: Aeron (Sub-µs)

Reliable UDP & IPC

Aeron is the industry standard for high-throughput, low-latency messaging, typically used for the matching engine core.

- **Transport:** Uses UDP unicast/multicast with kernel bypass support for raw speed.
- **Cluster:** Provides Raft consensus for fault tolerance, ensuring trading state is replicated safely.
- **Security (ATS):** Aeron Transport Security adds encryption (AES-GCM) securing the stream "on the wire."

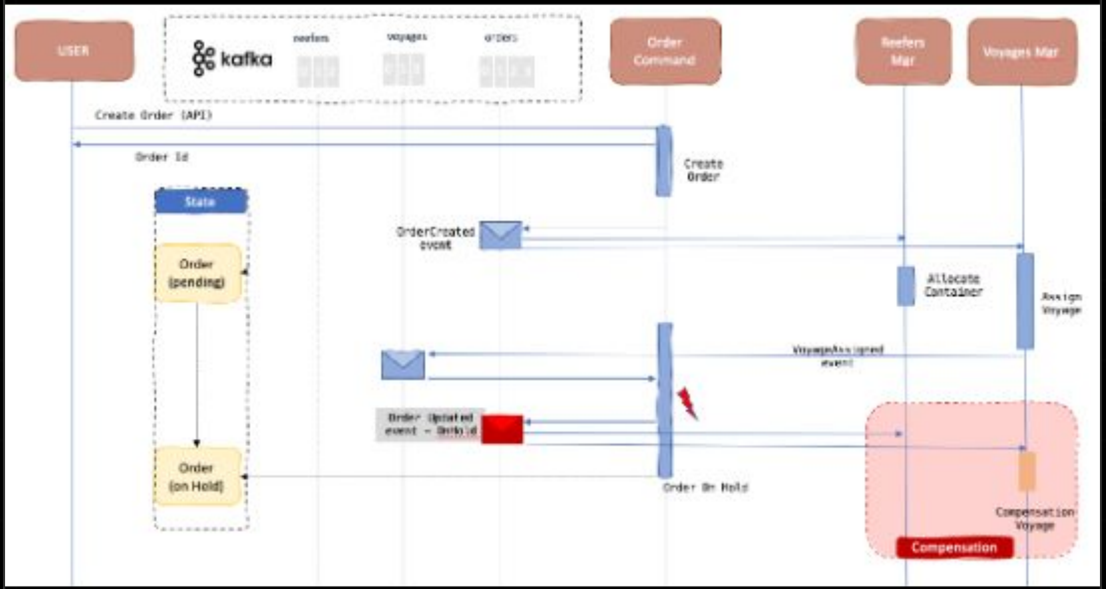


Cloud-Native Event Bus & Orchestration

Kafka, CQRS, & Saga Patterns

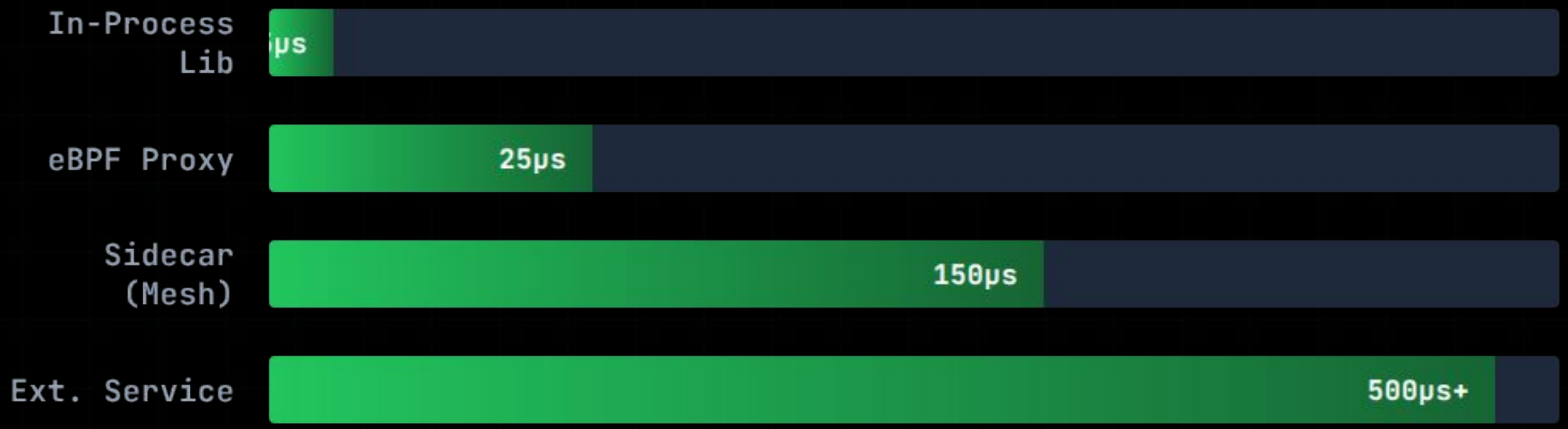
For high-throughput, non-latency-critical components (market data ingestion, risk, settlement), we leverage standard cloud-native tools.

- **Event Streaming:** Apache Kafka / RabbitMQ handle 1M+ messages/sec for decoupled services.
- **Patterns:** CQRS and Event Sourcing simplify data integrity and separate command (write) from query (read).
- **Saga:** Orchestrates complex, distributed transactions (e.g., cross-exchange settlement) with guaranteed consistency.



The Latency Tax: Security Patterns

Comparison of security implementation patterns in microservices.



*Sidecars are great for OMS, but fatal for Matching Engines.

eBPF: Observability w/o Penalty

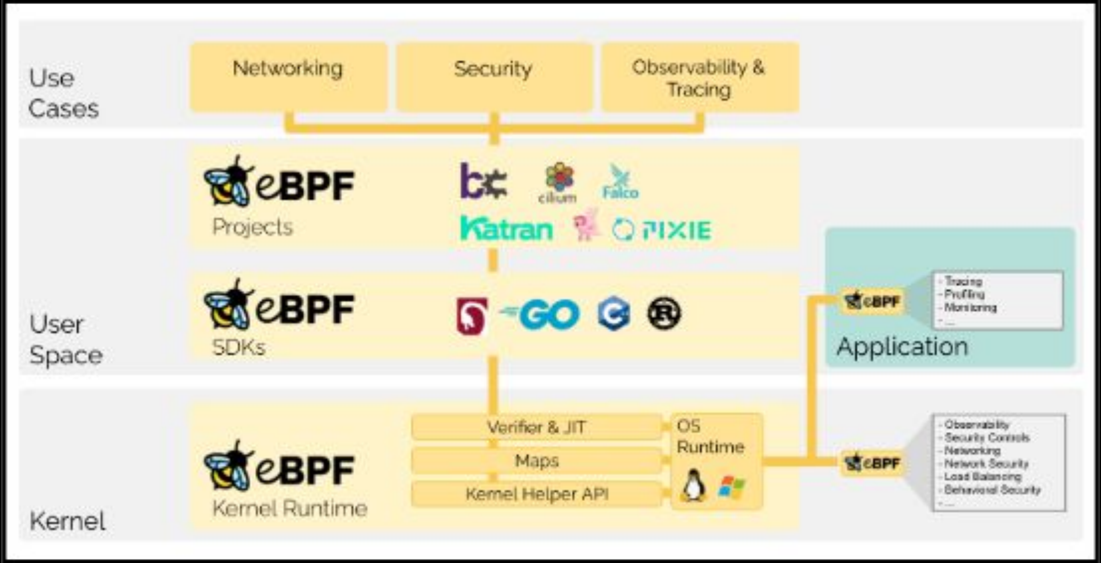
The "Magic" Hook

eBPF (Extended Berkeley Packet Filter) allows running sandboxed programs directly in the Linux kernel. It is a key tool for Service Mesh observability in cloud-native HFT.

> **No Sidecars Needed:** Observe traffic and enforce security policies (like mTLS) at the kernel level.

> **Zero-Copy Visibility:** Inspect packets without copying them to user space, maintaining the low-latency requirement.

> **Audit:** Trace every syscall and network event for compliance without degrading application performance.



Determinism is Security

Event Sourcing

Capture every state change as an immutable event. If you can't replay it, you can't prove it happened.

Forensics

Post-mortem analysis of "flash crashes" requires bit-perfect deterministic replay of the trading sequence.

Compliance

Regulators demand proof of "Best Execution." Deterministic logs provide irrefutable evidence of system behavior.

Compliance as Code & Real-World Scale

Actionable Case Studies

Compliance is embedded in the architecture, not bolted on. This drives tangible results:

- **LSE Throughput:** Systems designed to handle 15 million messages per second.
- **GS Risk:** 14 billion daily risk calculations, automated and verified.
- **DevSecOps Speed:** Deployment times cut from 6 hours to 15 minutes.
- **Availability:** Reduced annual downtime from 40 hours to just 2.5 hours.

Resilience & Chaos Engineering

> "In HFT, a system that cannot recover in milliseconds is a system that has already failed."

The Future: Hardware Security

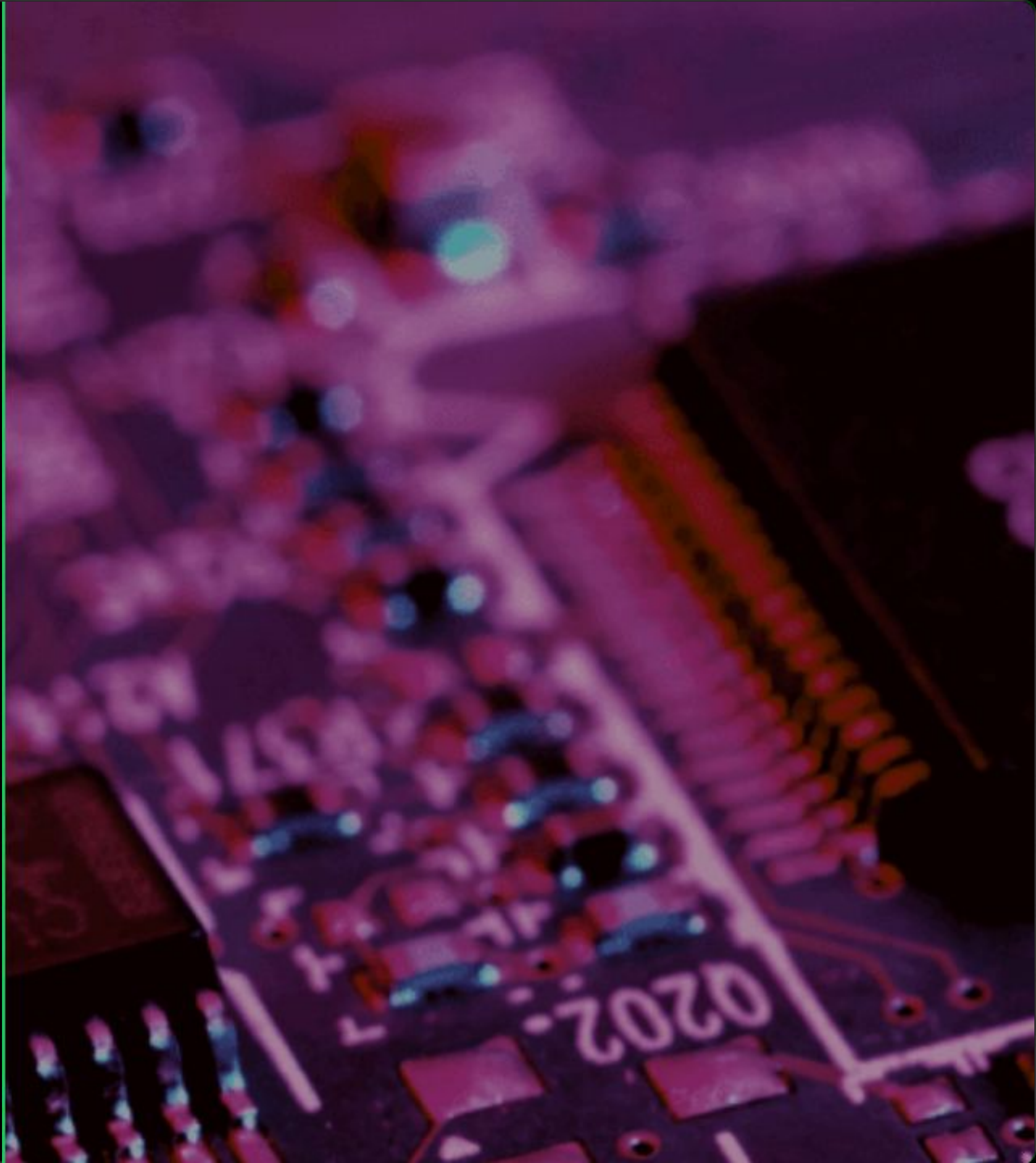
FPGA & SmartNICs

The next frontier is moving security logic directly onto the hardware.

> **Zero-CPU Overhead:** Implement firewalls, risk checks, and encryption directly on the FPGA gates.

> **Bump-in-the-Wire:** Bad packets are dropped at the NIC level, ensuring they never consume host CPU cycles or reach the trading engine.

> **Hybrid Cloud:** AWS F1 instances allow deploying these custom hardware circuits in the cloud.



Q & A

Thank you for attending.

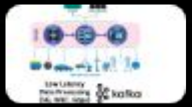
Image Sources

https://media.istockphoto.com/id/1465447344/vector/penrose-triangle-illustration-3d-with-neon-blue.jpg?s=1024×1024&w=is&k=20&c=V6D23qocOCZ0wWj7k77FpQoPjHSXImNZYEbCFWJnrJY=

Source: www.istockphoto.com

https://miro.medium.com/v2/resize:fit:1400/0*E6pvV9ebVYVCCC2L.png

Source: embedx.medium.com



https://www.kai-waehner.de/wp-content/uploads/2021/05/Low-Latency-Data-Processing-and-Edge-Computing-with-Apache-Kafka-5G-Telco-Network-and-AWS-Wavelength.png

Source: www.kai-waehner.de

https://ibm-cloud-architecture.github.io/eda-saga-choreography/images/saga-flow-2.png

Source: ibm-cloud-architecture.github.io

https://ebpf.io/static/e293240ecccb9d506587571007c36739/f2674/overview.png

Source: ebpf.io

https://cdn.dribbble.com/userupload/17839817/file/original-2aa68cd187f1190590a07e4d05b8e4d0.png?format=webp&resize=400×300&vertical=center

Source: dribbble.com

Image Sources

https://www.microchipusa.com/_next/image?url=%2Fmedia%2Fwhats-a-fpga-board-wordpress-768×402.png&w=3840&q=75

Source: www.microchipusa.com