LEAN ETHEREUM — Resumen Ejecutivo

Casper FFG + LMD-GHOST → Lean Consensus, Lean Data, Lean Execution

Basado en: "*lean Ethereum*" — Justin Drake, Ethereum Foundation, 31 de julio de 2025 **Fecha:** Febrero 2026

---

1. ¿Qué es Lean Ethereum?

El 31 de julio de 2025 — un día después del 10.° aniversario de Ethereum — **Justin Drake** (Ethereum Foundation) presentó **Lean Ethereum**: una visión para la próxima década que reimagina las tres capas de Ethereum L1 desde primeros principios.

> "*We stand at the dawn of a new era. Millions of TPS. Quantum adversaries. How does Ethereum marry extreme performance with uncompromising security and decentralization?*"

La respuesta es un protocolo **más simple, más rápido y resistente a computadoras cuánticas**, unificado por **criptografía basada en hashes**.

---

2. El Protocolo Actual: Gasper (Casper FFG + LMD-GHOST)

Ethereum usa **Gasper** como protocolo de consenso desde The Merge (septiembre 2022). Combina dos componentes:

LMD-GHOST — Fork Choice Rule (Vivacidad)

- Determina cuál es la cadena canónica en cada momento.
- En cada bifurcación, elige el **subárbol con mayor peso** de attestaciones.
- Solo cuenta el **último voto** de cada validador (*Latest Message Driven*).
- Inicia desde el último checkpoint justificado por Casper FFG.
- **Garantiza que la cadena siempre avanza**, pero no ofrece finalidad por sí solo.

Casper FFG — Finality Gadget (Seguridad)

- Añade **finalidad económica determinista** sobre LMD-GHOST.
- Opera sobre **checkpoints** (primer bloque de cada época, cada ~6.4 min).
- Los validadores votan con pares `(source, target)` en cada attestación.
- Un checkpoint se **justifica** cuando ≥2/3 del stake vota por él.
- Un checkpoint se **finaliza** cuando el siguiente también es justificado.
- **Tiempo de finalidad actual: ~12.8 minutos (2 épocas).**

Condiciones de Slashing

Dos reglas inviolables que protegen la integridad del consenso:

1. **No Double Vote:** No emitir dos votos para la misma época target.
2. **No Surround Vote:** No emitir un voto que envuelva a otro previo.

Teorema de Seguridad Responsable: Si dos checkpoints conflictivos son finalizados, al menos **1/3 del stake total** violó una condición de slashing y puede ser identificado y penalizado (~$44 mil millones USD al 2025).

Limitaciones de Gasper

Problema	Impacto
Finalidad ~12.8 min	UX pobre para bridges, pagos, DeFi
Firmas BLS12-381	Vulnerables a computadoras cuánticas
Compromisos KZG	Vulnerables a computadoras cuánticas

Complejidad dual GHOST+Casper	Vectores de ataque sutiles
EVM 256-bit	Ineficiente para pruebas ZK
Mínimo 32 ETH para validar	Barrera a la descentralización

---

3. Los Dos Modos de Lean Ethereum

Fort Mode (Defensa)

Preparar a Ethereum para sobrevivir a **estados-nación y computadoras cuánticas**:

- Reemplazar **toda** la criptografía vulnerable (BLS, KZG, ECDSA) con primitivas basadas en hashes.
- Los hashes son inherentemente resistentes a ataques cuánticos.
- Mantener 100% uptime, diversidad de clientes y $130B+ en seguridad económica.

Beast Mode (Ofensiva)

Escalar a rendimiento extremo:

- **L1: 1 gigagas/segundo** → ~10,000 TPS (vs. ~15-30 actuales).
- **L2: 1 teragas/segundo** → ~10,000,000 TPS vía rollups.
- Habilitado por zkVMs en tiempo real y Data Availability Sampling.

---

4. Los Tres Pilares de Lean Ethereum

4.1 Lean Consensus — Beacon Chain 2.0

Anteriormente conocido como **Beam Chain** (propuesta de Drake, noviembre 2024).

Aspecto	Gasper (Hoy)	Lean Consensus
Finalidad	~12.8 minutos	**~12 segundos** (3-Slot Finality)
Block time	12 segundos	**~4 segundos**
Firmas	BLS12-381	**Hash-based aggregate**
Min. staking	32 ETH	**1 ETH**
Builder separation	MEV-Boost (off-protocol)	**ePBS (nativo)**
Anti-censura	Limitada	**FOCIL (inclusion lists)**
Aleatoriedad	RANDAO (manipulable)	**RANDAO + VDFs**

3-Slot Finality (3SF) reemplaza a Gasper con un protocolo BFT unificado:

```
Slot 1 (~4s): Propuesta del bloque
Slot 2 (~4s): Votación (≥2/3 → bloque LOCKED)
Slot 3 (~4s): Confirmación (≥2/3 → bloque FINALIZADO)
Total: ~12 segundos (vs. ~12.8 minutos actual = 64x más rápido)
```

4.2 Lean Data — Blobs 2.0

Evolución de Proto-Danksharding (EIP-4844, marzo 2024):

- **Blobs post-cuánticos:** Reemplazar compromisos KZG (vulnerables) con **compromisos DAS basados en hashes**.
- **Granularidad flexible:** Blobs de tamaño variable (vs. ~125 KB fijo actual).
- **Developer experience tipo calldata:** Más intuitivo para desarrolladores L2.
- **Escalado:** De 6 blobs/bloque máximo hacia 32+ (Full Danksharding con DAS).

4.3 Lean Execution — EVM 2.0

Reemplazo de la EVM actual con un entorno SNARK-friendly:

- **RISC-V** como candidato de instruction set: open-source, simple, cada instrucción genera constraints ZK predecibles.
- **zkVMs en tiempo real:** Un prover ejecuta y genera una prueba ZK; los nodos solo verifican la prueba (vs. re-ejecutar cada transacción).
- **Preserva compatibilidad EVM:** Contratos existentes y herramientas (Solidity, Vyper) siguen funcionando vía compilación/interpretación sobre RISC-V.

---

5. Lean Cryptography — La Base Unificadora

La observación central de Drake: la **criptografía basada en hashes** resuelve dos megatendencias simultáneamente:

1. **SNARKs:** Los hashes son la primitiva más eficiente dentro de circuitos ZK.
2. **Amenaza cuántica:** Los hashes son inherentemente quantum-safe.

Transformación criptográfica completa

Capa	Actual (Vulnerable)	Lean (Post-Quantum)
Consenso	Firmas BLS12-381	Hash-based aggregate signatures
Datos	Compromisos KZG	Hash-based DAS commitments
Ejecución	Re-ejecución EVM	Hash-based real-time zkVMs

---

6. Ataques que Lean Resuelve

Ataque	En Gasper	En Lean
Balancing attack	Mitigado parcialmente (Proposer Boost)	**Eliminado** (3SF sin fork choice separado)
Bouncing attack	Mitigado	**Eliminado** (sin rebotes entre épocas)
Avalanche attack	Mitigado	**Eliminado** (sin epoch boundaries)
Ex-ante reorg	Parcialmente mitigado	**Reducido** (ventana de reorg de ~12s)
Quantum attack	**Sin mitigación**	**Eliminado** (criptografía hash-based)
RANDAO bias	Aceptado (bajo impacto)	**Eliminado** (VDFs)
MEV censura	Solo off-protocol	**Mitigado** (ePBS + FOCIL)

La clave: los ataques de Gasper explotan la **brecha temporal** entre LMD-GHOST (12s/slot) y Casper FFG (384s/época). 3SF elimina esa brecha al unificar selección de cadena y finalidad en ~12 segundos.

---

7. Lean Craft — Filosofía de Diseño

Drake articula seis principios bajo "*Lean Craft*" (analogía: "*Dreams of Sushi*"):

- **Minimalismo:** Cada componente justifica su existencia.
- **Modularidad:** Consenso, datos y ejecución evolucionan independientemente.
- **Complejidad encapsulada:** La complejidad inevitable se aísla con interfaces simples.
- **Verificación formal:** Propiedades demostrables matemáticamente.
- **Seguridad demostrable:** Reducciones formales a supuestos bien estudiados.
- **Optimalidad demostrable:** Diseño óptimo o cercano al óptimo en su clase.

---

8. Roadmap

```
2022  The Merge (PoW → PoS)
2023  Shanghai/Capella (retiros habilitados)
2024  Dencun (proto-danksharding) · Beam Chain propuesta
2025  Pectra (MaxEB 2048 ETH) · Lean Ethereum publicado (Jul 31)
2026  Desarrollo e implementación en clientes · PeerDAS
2027  Testing en devnets y testnets
2028+ Deploys graduales de Lean Consensus, Data, Execution
2029+ Protocolo Lean operacional
```

Recursos:

- Blog post: https://blog.ethereum.org/2025/07/31/lean-ethereum
- Roadmap tracker: https://leanroadmap.org
- Contacto: lean@ethereum.org

---

9. Síntesis Final

```
GASPER (Hoy)                          LEAN ETHEREUM (Futuro)
────────────                          ──────────────────────
Casper FFG + LMD-GHOST          →     Protocolo 3SF unificado
Finalidad ~12.8 min             →     Finalidad ~12 seg
Firmas BLS (quantum-vulnerable) →     Firmas hash-based (quantum-safe)
KZG commits (quantum-vulnerable)→     Hash-based DAS commits
EVM re-ejecución (~15 TPS)      →     RISC-V zkVM (~10,000 TPS)
Min. 32 ETH para validar        →     Min. 1 ETH
Proto-danksharding (6 blobs)    →     Full DAS (32+ blobs)
MEV-Boost (trusted relays)      →     ePBS nativo + FOCIL
```

Lean Ethereum es un **"juramento generacional"** (*generational oath*): mantener la continuidad operacional de Ethereum, escalar sin compromisos, y construir un protocolo digno de asegurar el internet del valor durante décadas o siglos.

> *"If the world is online, the world is onchain." — Justin Drake*

Referencias clave:

1. Drake, J. (2025). *lean Ethereum*. Ethereum Foundation Blog.
2. Buterin et al. (2020). *Combining GHOST and Casper*. arXiv:2003.03052.
3. Buterin & Griffith (2017). *Casper the Friendly Finality Gadget*. arXiv:1710.09437.
4. Sompolinsky & Zohar (2013). *GHOST Protocol*.
5. D'Amato & Zanolini (2023). *A Simple Single Slot Finality Protocol*.