LEAN CONSENSUS: Ejemplo Práctico con 3-Slot Finality

¿Qué es LEAN Consensus?

LEAN Consensus (también conocido como Beam Chain o Beacon Chain 2.0) es la propuesta de Justin Drake para reimaginar el consenso de Ethereum. Reemplaza el sistema actual **Gasper** (Casper FFG + LMD-GHOST) con un protocolo BFT unificado llamado **3-Slot Finality (3SF)**.

Comparación Rápida

Aspecto	Gasper (Actual)	LEAN Consensus (3SF)
Finalidad	~12.8 minutos (2 épocas)	**~12 segundos (3 slots)**
Block time	12 segundos	**~4 segundos**
Firmas	BLS12-381 (vulnerable a quantum)	**Hash-based aggregate** (quantum-safe)
Protocolo	Dual (GHOST + Casper)	**Unificado (BFT)**
Complejidad	Alta (dos capas interactuando)	**Simplificada**

Configuración del Ejemplo

Tenemos **4 validadores** con sus stakes:

Validador	Stake	Color en diagramas
Alice	32 ETH	🔵
Bob	32 ETH	🟢
Carol	32 ETH	🟡
Dave	32 ETH	🔴

- **Total stake**: 128 ETH
- **Supermayoría (2/3)**: 85.33 ETH → necesitamos al menos **3 validadores**

Ejemplo 1: Operación Normal (Happy Path)

Bloque Génesis (Finalizado)

```
[Genesis] ✓ Finalizado
```

Este es nuestro punto de partida seguro.

Bloque 1: Propuesta → Votación → Confirmación

SLOT 1 (~4 segundos): PROPUESTA

Alice es seleccionada como proponente del slot 1.

```
t=0s: Alice propone bloque B1

      ┌─────────────────┐
      │  Bloque B1      │
      │  Proponente: 🔵 │
      │  Parent: Genesis│
      └─────────────────┘
```

Todos los validadores reciben B1.

SLOT 2 (~4 segundos): VOTACIÓN

Los validadores votan por el bloque B1:

```
t=4s: Votación por B1

🔵 Alice:  ✓ VOTA por B1
🟢 Bob:    ✓ VOTA por B1
🟡 Carol:  ✓ VOTA por B1
🔴 Dave:   ✓ VOTA por B1

Votos totales: 128 ETH (100%)
Supermayoría: 128 ETH ≥ 85.33 ETH → ✓ ALCANZADA
```

Resultado del Slot 2:

```
Estado de B1: LOCKED (bloqueado) 🔒
```

Un bloque **LOCKED** significa que los validadores se han comprometido a construir sobre él. No pueden votar por un fork conflictivo sin violar las reglas de slashing.

SLOT 3 (~4 segundos): CONFIRMACIÓN

Los validadores confirman el lock:

```
t=8s: Confirmación del lock de B1

🔵 Alice:  ✓ CONFIRMA
🟢 Bob:    ✓ CONFIRMA
🟡 Carol:  ✓ CONFIRMA
🔴 Dave:   ✓ CONFIRMA

Confirmaciones: 128 ETH (100%)
Supermayoría: 128 ETH ≥ 85.33 ETH → ✓ ALCANZADA
```

Resultado del Slot 3:

```
┌──────────────────────────────────┐
│  Estado de B1: FINALIZADO ✅      │
```

```
│  Tiempo total: ~12 segundos      │
└──────────────────────────────────┘
```

B1 es ahora irreversible. Ningún validador puede construir sobre una cadena que no incluya B1 sin perder su stake completo.

Resumen de la Finalización

```
Tiempo Total: ~12 segundos

Genesis ──→ [B1] FINALIZADO ✅
             ↑
             │
Slot 1: Propuesta (Alice)
Slot 2: Votación → LOCKED 🔒
Slot 3: Confirmación → FINALIZED ✅
```

Comparación con Gasper:

- Gasper: ~12.8 minutos (768 segundos)
- LEAN 3SF: ~12 segundos
- **Mejora: 64x más rápido**

Ejemplo 2: Fork Temporal y Resolución

¿Qué pasa si dos validadores proponen bloques simultáneamente?

Situación: Fork en Slot 4

```
          [B1] Finalizado ✅
           │
           ├──→ [B2] propuesto por 🔵 Alice
           │
           └──→ [B2'] propuesto por 🟢 Bob (mensaje tardío)
```

Ambos bloques llegan a diferentes validadores primero.

SLOT 4: Propuesta con Fork

```
t=12s: Dos propuestas compiten

🔵 Alice ve primero: B2
🟢 Bob ve primero:   B2'
🟡 Carol ve primero: B2
🔴 Dave ve primero:  B2
```

SLOT 5: Votación

Los validadores votan por el bloque que vieron primero:

```
t=16s: Votación dividida

Por B2:
  🔵 Alice:   ✓ VOTA B2
  🟡 Carol:   ✓ VOTA B2
  🔴 Dave:    ✓ VOTA B2
  Subtotal: 96 ETH

Por B2':
  🟢 Bob:     ✓ VOTA B2'
  Subtotal: 32 ETH
```

Cálculo de supermayoría:

- B2: 96 ETH ≥ 85.33 ETH → ✓ SUPERMAYORÍA
- B2': 32 ETH < 85.33 ETH → ✕ Sin supermayoría

Resultado:

```
B2  → LOCKED 🔒 (tiene supermayoría)
B2' → DESCARTADO ❌ (sin supermayoría)
```

SLOT 6: Confirmación

```
t=20s: Confirmación

🔵 Alice:   ✓ CONFIRMA B2
🟢 Bob:     ✓ CONFIRMA B2 (abandona B2')
🟡 Carol:   ✓ CONFIRMA B2
🔴 Dave:    ✓ CONFIRMA B2

Confirmaciones: 128 ETH → ✓ SUPERMAYORÍA
```

Resultado:

```
┌──────────────────────────────────┐
│  B2 es FINALIZADO ✅              │
│  B2' es descartado               │
└──────────────────────────────────┘
```

Diagrama final:

```
[B1] Finalizado ✅
  │
  └──→ [B2] Finalizado ✅

       [B2'] ❌ (huérfano)
```

Ejemplo 3: Ataque Bizantino Detectado

Dave intenta atacar el sistema mediante doble voto.

Escenario: Dave intenta revertir

```
Cadena honesta:
[Genesis] → [B1] → [B2] → [B3]
                           ↑
                         Todos finalizados ✅
```

Dave crea una cadena alternativa:

```
Cadena de ataque de Dave:
[Genesis] → [B1] → [X2] → [X3]
                    ↑
                  Bloque malicioso
```

SLOT 7-9: Dave intenta doble voto

Voto 1 (legítimo):

```
SLOT 7: Dave vota por B3 (voto honesto)
  Source: B2 (locked)
  Target: B3
```

Voto 2 (malicioso):

```
SLOT 8: Dave intenta votar por X3 (voto conflictivo)
  Source: B1
  Target: X3
```

Detección Inmediata

El protocolo detecta la violación:

```
┌─────────────────────────────────────────────┐
│  SLASHING DETECTADO                         │
├─────────────────────────────────────────────┤
│  Validador: 🔴 Dave                         │
│  Violación: SURROUND VOTE                   │
│                                             │
│  Voto 1: B2 → B3                            │
│  Voto 2: B1 → X3                            │
│          └─ Conflicto detectado             │
│                                             │
│  Penalización:                              │
│  • Pérdida inmediata: 1 ETH                 │
│  • Penalización correlacionada: 31 ETH      │
│  • TOTAL: 32 ETH (100% del stake)           │
│  • Expulsión de la red                      │
└─────────────────────────────────────────────┘
```

Proof de violación:

```
Condición de slashing #2 (No Surround Vote):

Voto antiguo (epoch 1 → 2): Source B1, Target B2
Voto nuevo   (epoch 1 → 3): Source B1, Target X3

B1.epoch < B2.epoch < X3.epoch
→ SURROUND VOTE DETECTADO ⚠️
→ SLASHING AUTOMÁTICO
```

Resultado

```
Estado de la red:
✅ Cadena honesta [B1]→[B2]→[B3] continúa finalizada
❌ Cadena de ataque descartada
🔴 Dave pierde sus 32 ETH y es expulsado

Validadores restantes:
🔵 Alice:  32 ETH
🟢 Bob:    32 ETH
🟡 Carol:  32 ETH
──────────────────
Total: 96 ETH (2/3 de 96 = 64 ETH para supermayoría)
```

La red continúa operando normalmente con los validadores honestos.

Ejemplo 4: Ataque del 51% (Imposible sin Pérdidas Masivas)

Supongamos que Dave y Carol se confabulan (2/4 = 50% del stake).

Intento de Ataque

```
Cadena honesta finalizada:
[Genesis] → [B1] ✅ → [B2] ✅ → [B3] ✅

Cadena de ataque:
[Genesis] → [B1] ✅ → [Y2]
```

¿Pueden Dave y Carol revertir B2?

NO, porque:

1. **B2 está FINALIZADO** (recibió >2/3 de votos)
2. Para revertirlo necesitarían:
    - Crear un fork desde B1
    - Hacer que Y2 reciba >2/3 de votos
    - Pero solo tienen 64 ETH (50%)
    - Necesitan 85.33 ETH (66%)

Resultado:

```
┌────────────────────────────────────────────┐
│  ATAQUE FALLIDO                            │
├────────────────────────────────────────────┤
│  Dave + Carol: 64 ETH (50%)                │
│  Necesario: 85.33 ETH (66%)                │
│                                            │
│  Conclusión: NO PUEDEN finalizar Y2        │
│  La cadena honesta continúa                │
└────────────────────────────────────────────┘
```

¿Y si controlan 67% (3 de 4 validadores)?

Si Dave, Carol y Bob se confabulan (96 ETH = 75%):

```
Escenario:
- Pueden crear fork desde B1
- Pueden finalizar bloques alternativos
```

PERO:

```
┌──────────────────────────────────────────────────┐
│  COSTO DEL ATAQUE                                │
├──────────────────────────────────────────────────┤
│  Para revertir B2 (ya finalizado):               │
│                                                  │
│  1. Necesitan votar conflictivamente             │
│  2. Esto viola condiciones de slashing           │
│  3. Penalización:                                │
│     • Detección: ≥1/3 del stake total            │
│     • Pérdida: 100% del stake de atacantes       │
│                                                  │
│  Costo:                                          │
│  96 ETH × $3,700 = $355,200 USD                  │
│                                                  │
│  En Ethereum real (~35.7M ETH):                  │
│  11.9M ETH × $3,700 = ~$44 BILLION USD           │
└──────────────────────────────────────────────────┘
```

Teorema de Accountable Safety:

> *Si dos bloques conflictivos son finalizados, entonces ≥1/3 del stake total ha violado condiciones de slashing y puede ser identificado y penalizado.*

Propiedades Clave de LEAN Consensus

1. Safety (Seguridad)

Los bloques finalizados son **irreversibles** sin que los atacantes pierdan >1/3 del stake total.

```
Garantía: Si B está finalizado, cualquier B' conflictivo
          requiere que ≥1/3 del stake sea slasheado.
```

2. Liveness (Vivacidad)

La cadena **siempre progresa** mientras >2/3 de validadores estén honestos y online.

```
Condición: Si ≥2/3 online y honestos
           → 1 bloque finalizado cada ~12 segundos
```

3. Finalidad Rápida

De ~12.8 minutos a ~12 segundos.

```
Gasper:  2 épocas × 32 slots × 12s = 768s (~12.8 min)
LEAN 3SF: 3 slots × 4s = 12s
Mejora: 64x más rápido
```

4. Quantum-Safe

Firmas basadas en hashes en lugar de BLS12-381.

```
BLS12-381 (actual):     Vulnerable a computadoras cuánticas ⚠️
Hash-based (LEAN):      Resistente a quantum ✅
```

5. Simplicidad

Un protocolo unificado vs. la dualidad GHOST + Casper.

```
Gasper:       Dos protocolos (LMD-GHOST + Casper FFG)
              → Interacciones complejas
              → Vectores de ataque (balancing, bouncing, avalanche)

LEAN 3SF:     Protocolo BFT unificado
              → Más simple
              → Elimina ataques de la brecha temporal
```

Comparación Final: Gasper vs LEAN

Timeline de Finalización

Gasper (actual):

```
Slot 1...32 (Época 1): Attestaciones se acumulan
  ↓
Checkpoint de Época 1 se justifica
  ↓
Slot 33...64 (Época 2): Más attestaciones
  ↓
Checkpoint de Época 2 se justifica
  ↓
Checkpoint de Época 1 se FINALIZA
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
Total: ~768 segundos (~12.8 minutos)
```

LEAN 3SF:

```
Slot 1: Propuesta del bloque
  ↓
Slot 2: Votación → LOCKED (si ≥2/3 votan)
  ↓
Slot 3: Confirmación → FINALIZADO (si ≥2/3 confirman)
─────────────────────────────────
Total: ~12 segundos
```

Tabla Comparativa Completa

Característica	Gasper	LEAN Consensus
Finalidad	~12.8 min	~12 seg
Velocidad	1x	**64x más rápido**
Protocolo	Dual (GHOST+Casper)	Unificado (BFT)
Firmas	BLS12-381	Hash-based
Quantum-safe	❌ No	✅ Sí
Block time	12 seg	4 seg
Min. stake	32 ETH	1 ETH
Complejidad	Alta	Reducida
Ataques de timing	Susceptible	Eliminados

Flujo Completo: De Propuesta a Finalidad

```
┌─────────────────────────────────────────────────────────────┐
│                  LEAN CONSENSUS (3SF)                        │
│                                                             │
│  SLOT N (t=0s):   PROPUESTA                                 │
│  ┌────────────────────────────────────────────────┐         │
│  │ • Proponente seleccionado vía aleatoriedad     │         │
│  │   mejorada (RANDAO + VDF)                      │         │
│  │ • Propone bloque con tx + execution payload    │         │
│  │ • Broadcast a todos los validadores            │         │
│  └────────────────────────────────────────────────┘         │
│                        ↓                                    │
│  SLOT N+1 (t=4s):  VOTACIÓN                                 │
│  ┌────────────────────────────────────────────────┐         │
│  │ • Cada validador vota por el bloque            │         │
│  │ • Votos se agregan (hash-based signatures)     │         │
│  │ • Si ≥2/3 del stake vota → Bloque LOCKED 🔒    │         │
│  └────────────────────────────────────────────────┘         │
│                        ↓                                    │
│  SLOT N+2 (t=8s):  CONFIRMACIÓN                             │
```

```
│   ┌──────────────────────────────────────────────┐          │
│   │ • Validadores confirman el lock              │          │
│   │ • Si ≥2/3 confirman → Bloque FINALIZADO ✅   │          │
│   │ • Bloque es ahora irreversible               │          │
│   └──────────────────────────────────────────────┘          │
│                                                             │
│  TOTAL: ~12 segundos desde propuesta a finalidad            │
└─────────────────────────────────────────────────────────────┘
```

Parámetros de LEAN Ethereum

Consenso

- **Slot duration**: ~4 segundos (vs 12s actual)
- **Finalización**: 3 slots (~12s)
- **Min. stake**: 1 ETH (vs 32 ETH)
- **Firmas**: Hash-based aggregation (quantum-safe)
- **Aleatoriedad**: RANDAO + VDFs (sin bias)

Rendimiento

- **L1 target**: 1 gigagas/segundo (~10,000 TPS)
- **L2 target**: 1 teragas/segundo (~10,000,000 TPS)
- **Blobs**: 32+ por bloque (vs 6 actual)
- **Data availability**: Full DAS con hash-based commitments

Seguridad

- **Post-quantum**: Todas las primitivas criptográficas
- **Anti-censura**: FOCIL (inclusion lists)
- **MEV**: ePBS nativo (enshrined PBS)
- **Slashing**: Condiciones preservadas de Casper FFG

Conclusión

LEAN Consensus representa una **reimaginación completa** del consenso de Ethereum:

✅ **64x más rápido** (12s vs 12.8 min) ✅ **Quantum-safe** (hash-based crypto) ✅ **Más simple** (protocolo unificado) ✅ **Más descentralizado** (min. 1 ETH) ✅ **Misma seguridad** (accountable safety preservada)

La transición de Gasper (Casper FFG + LMD-GHOST) a LEAN 3SF mantiene las garantías fundamentales de seguridad mientras elimina la complejidad de la interacción dual entre protocolos, resultando en:

- Finalidad en segundos
- Eliminación de ataques de timing (balancing, bouncing, avalanche)
- Preparación para la era post-cuántica
- Rendimiento extremo vía zkVMs

Referencias:

- Drake, J. (2025). *lean Ethereum*. Ethereum Foundation Blog.
- D'Amato & Zanolini (2023). *A Simple Single Slot Finality Protocol*.
- Buterin et al. (2020). *Combining GHOST and Casper*.

- Roadmap: https://leanroadmap.org