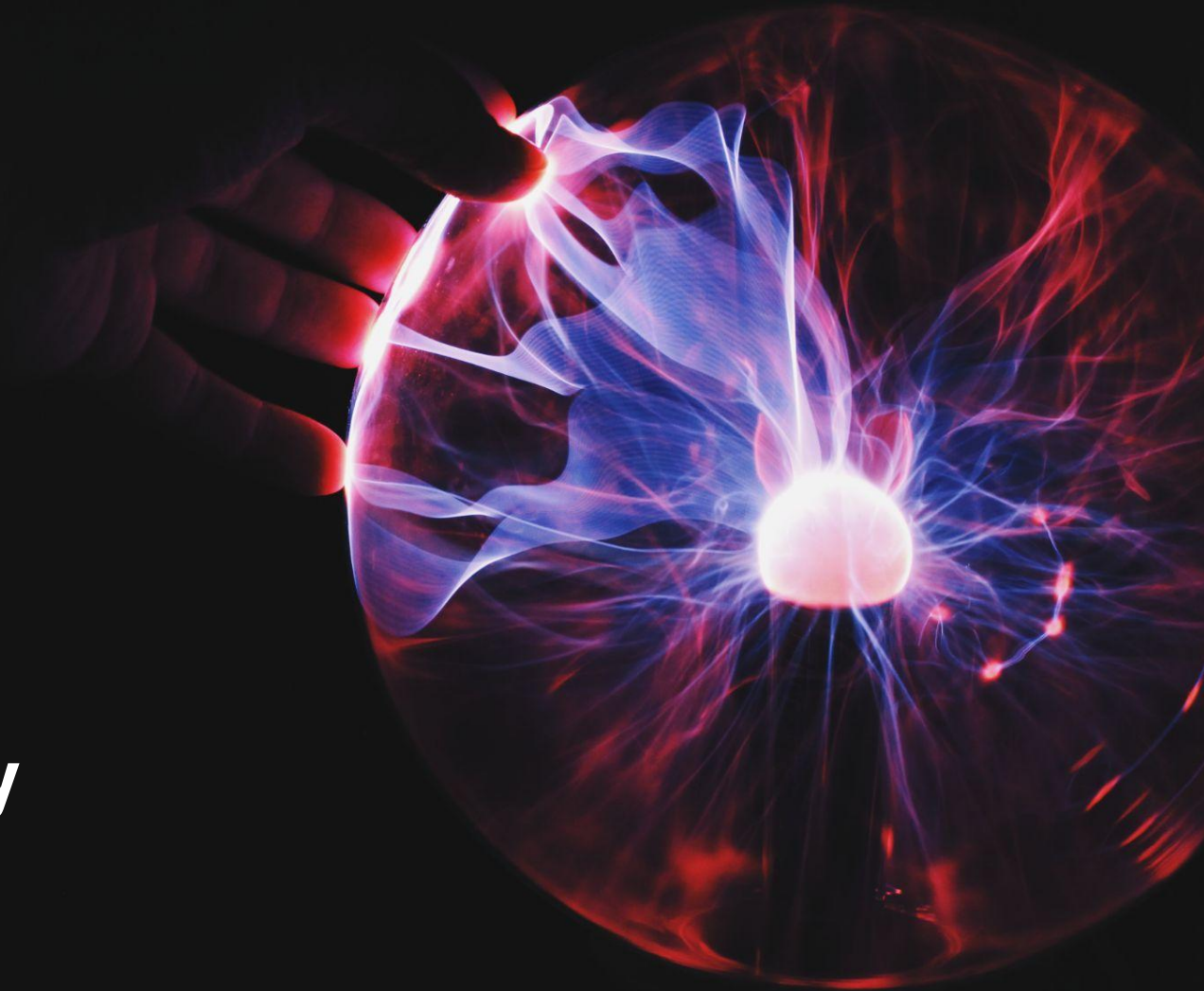


INPUT | OUTPUT

Determinismo y Tiempo



Determinismo y Tiempo: Qué significa que Tx sean determinísticas?

En este contexto, determinismo significa que una transacción tiene un **efecto fijo** en el estado del ledger:

- **Todas las blockchain tienen determinismo histórico:** El efecto de una transacción que ya fue agregada al ledger es fijo. Sino, se rompería el consenso al no poder revalidar Tx.
- **Pocas tienen determinismo prospectivo:** El efecto de una transacción que aún no se ha agregado al ledger es fijo (o no se agrega).

Una de las grandes ventajas de Cardano, es que **tiene determinismo prospectivo**.

Determinismo y Tiempo: Qué ventajas tiene el determinismo prospectivo?

- Los usuarios saben de antemano qué ocurrirá con una transacción, por lo que no hay sorpresas. Esto es particularmente relevante para los scripts porque los usuarios saben exactamente:
 - Cómo se van a comportar los validadores.
 - Cuánto presupuesto de ejecución (fees) hay que pagar.
- Las Tx propuestas se pueden procesar de forma segura en paralelo.
- Las fallas en los scripts pueden ser castigadas severamente (porque nunca les sucederán a usuarios no malintencionados).
- Hace que la interacción y la evolución de la blockchain sean más fáciles y predecibles.
- Simplifica desarrollar L2s como state channels y rollups porque pueden depender de este determinismo.

Determinismo y Tiempo: Cómo logra Cardano tener determinismo prospectivo?

El determinismo prospectivo requiere que **todas las partes** de la validación de la tx, incluida la ejecución del script, sean completamente deterministas.

Pero cómo puede ser que usemos tiempo si el tiempo cambia constantemente?!

En Cardano, lo logramos combinando estos ingredientes:

- (E)UTxO → Localidad
- Ouroboros
- Restringir la validez de una transacción a un rango de tiempo
- Separar la validación en 2 pasos

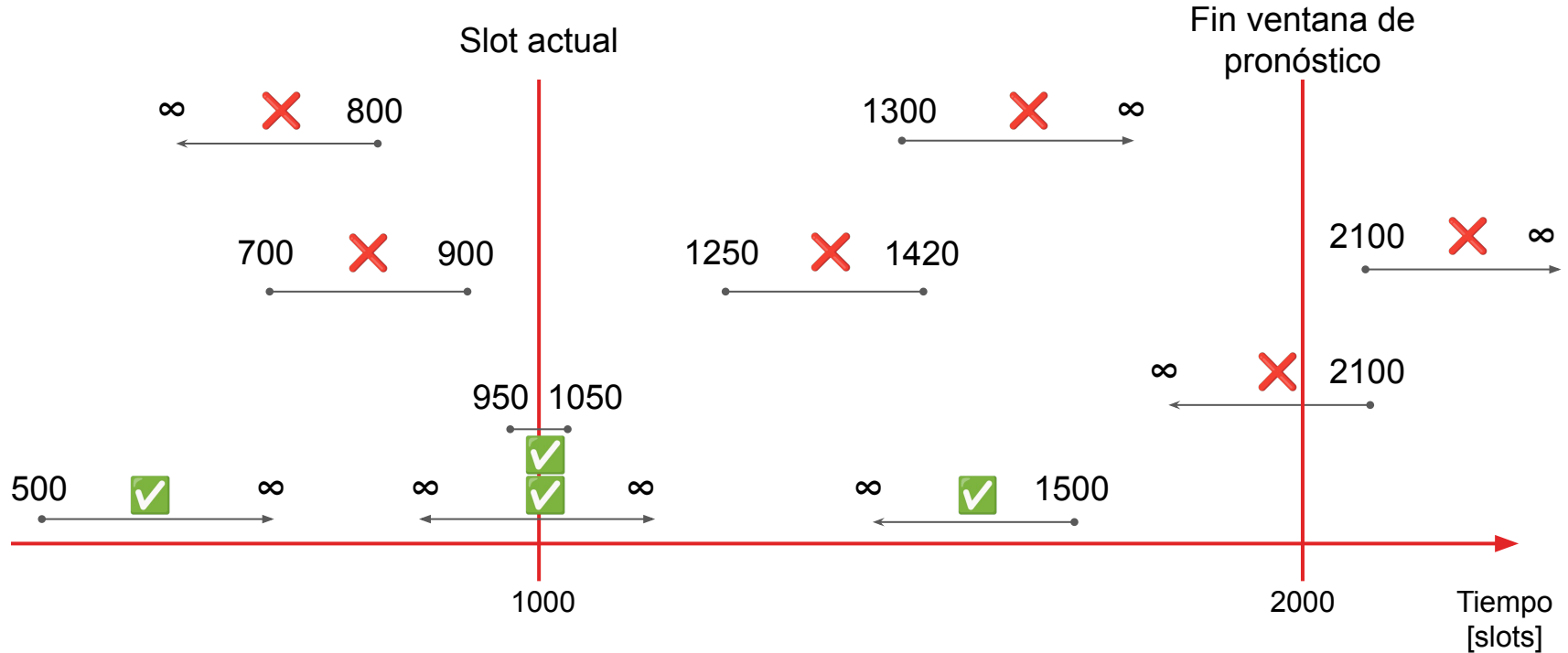
Tiempo en Validadores: Tiempo con Ouroboros

- **Ouroboros** (el algoritmo de consenso de Cardano), mide el tiempo en **slots**.
- Actualmente, **1 slot = 1 segundo**.
- Debido a la posibilidad de **Hard Forks** (HF Combinator), no podemos convertir tiempo real a slots a futuro de la “**ventana de pronóstico**” de Ouroboros.
- Con los parámetros actuales, la ventana de pronóstico es de **36 horas**.

Tiempo en Validadores: Verificando el Tiempo de una Tx

- Al crear una transaccion, definimos un “**rango de validez**” que es un rango de tiempo en **slots**, donde la transacción es **válida**.
- En el caso que no se defina uno o ambos limites, se asume que es **infinito**.
- El nodo chequea en **fase 1** si la transacción está siendo validada dentro de ese rango de validez. Si no lo esta, la rechaza **sin costo**.
- En caso que pasen todos los chequeos de la **fase 1**, se convierte el rango de validez a **POSIX**, se provee al script dentro del **ScriptContext**, y se pasa a la **fase 2**.

Tiempo en Validadores: Verificando el Tiempo de una Tx

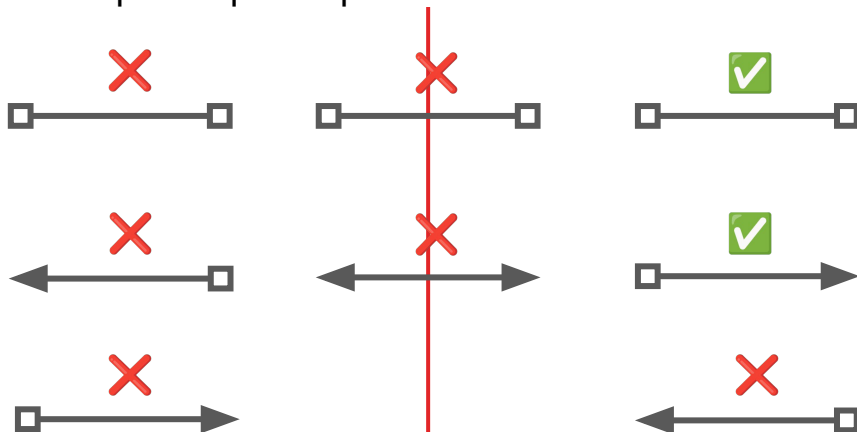


Tiempo en Validadores: Tiempo en el script

- El script **no tiene acceso al tiempo actual**, pero si **tiene acceso al rango de validación** y puede asumir que el tiempo actual está dentro de ese rango (de lo contrario, se habría rechazado la Tx en fase 1).
- Esto **garantiza el determinismo** ya que el script siempre verá **la misma información** por lo que el comportamiento será el mismo independientemente de cuándo se valide el script.
- Los límites del intervalo de validez para scripts se expresan en tiempo real **POSIX** (milisegundos desde 1 de Enero de 1970), en lugar de slots.
- Usar POSIX es importante porque el **tiempo por slot puede cambiar en un hard fork**. Suposiciones basadas en el conteo de slots generalmente no son confiables.

Tiempo en Validadores: Verificando el Tiempo en el Script

Fecha límite exacta **a partir** de la cual
quiero que se pueda consumir el UTxO



1722020987000

Viernes, 26 de Julio, 2024 7:09:47 PM (GMT)

Tiempo
[POSIX]

Fi

n Preguntas ?



INPUT | OUTPUT