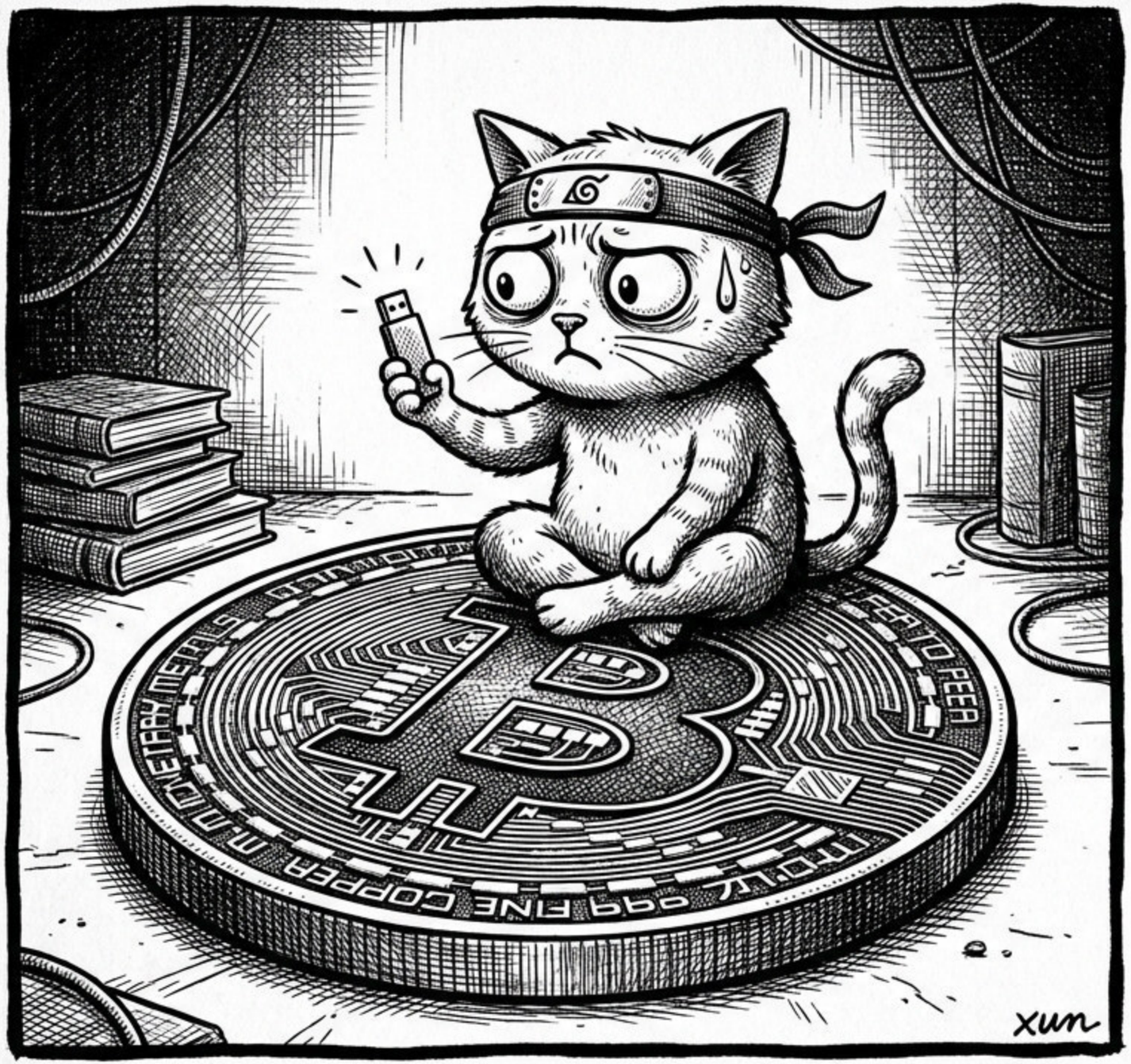
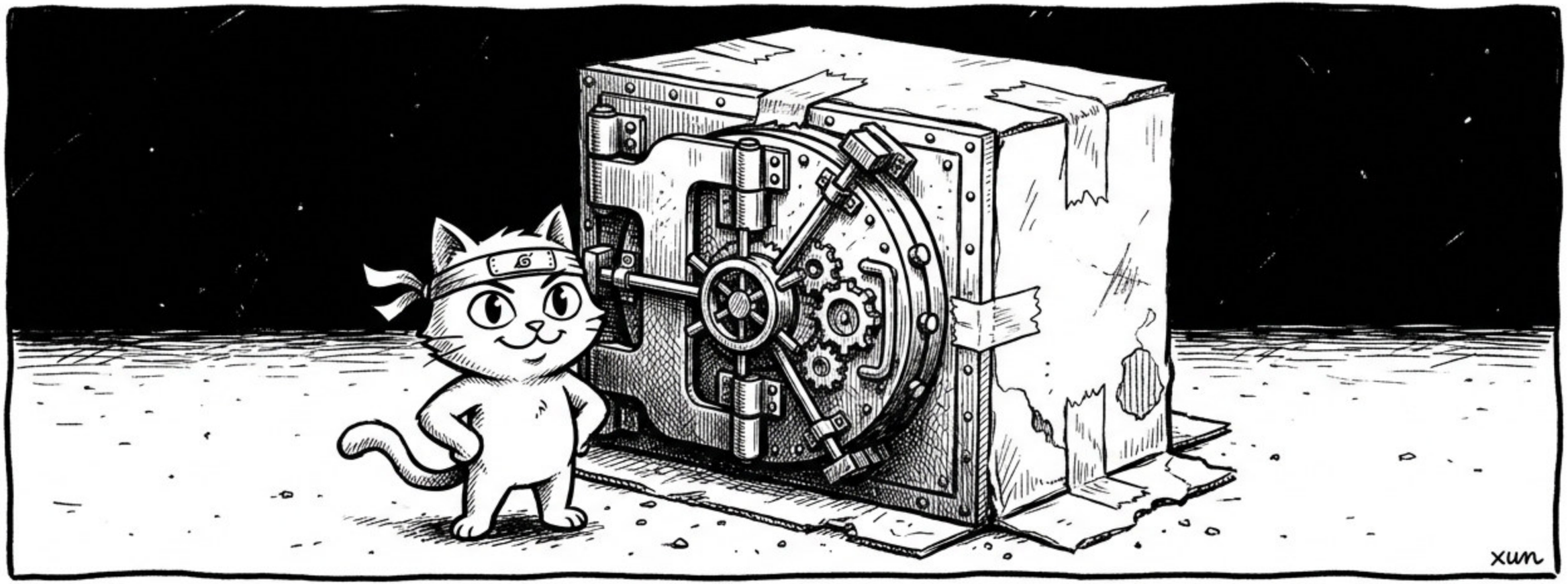



# Cómo NO confiar en tu Hardware Wallet

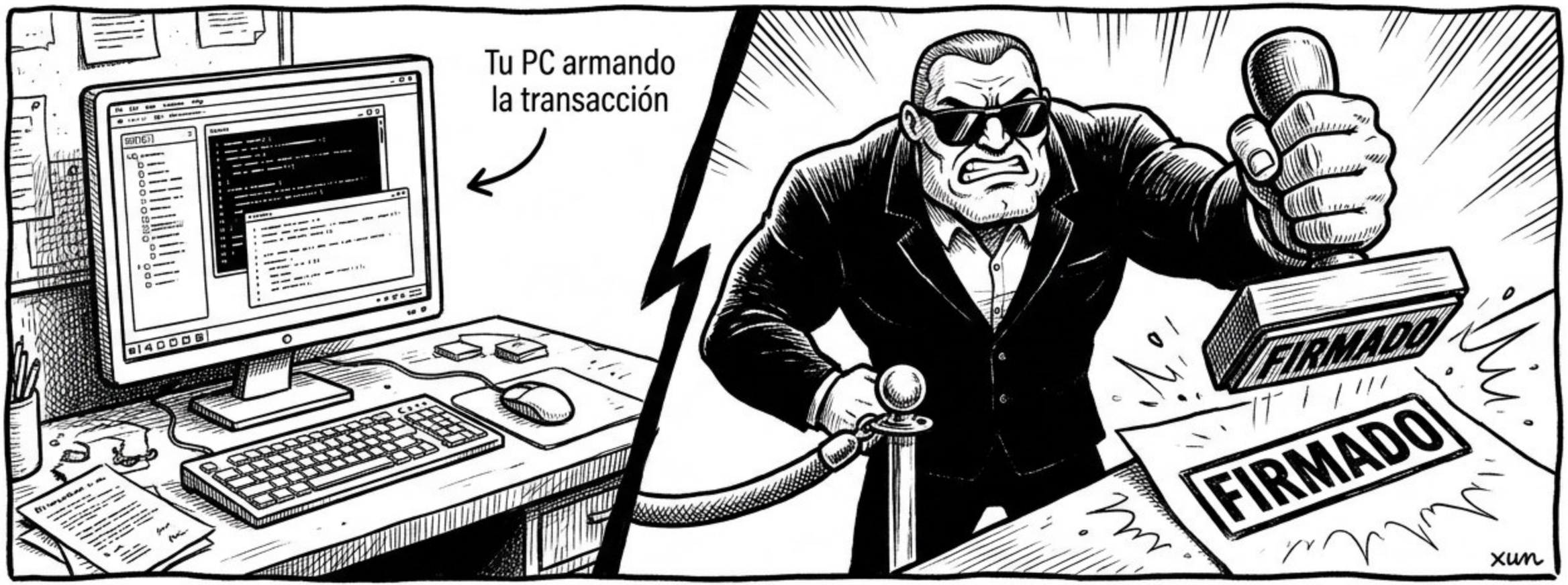
Un manual clandestino para principiantes sobre la verdadera entropía.




# El espejismo de la bóveda perfecta.

Bitcoin exige que custodies tu propio dinero. Los Hardware Wallets se venden como bóvedas físicas, aisladas de internet ('air-gapped').

**La caja fuerte parece inquebrantable,** pero **¿quién fabricó la cerradura** y **quién** la copia de **la llave maestra?**




# El único trabajo real del dispositivo.

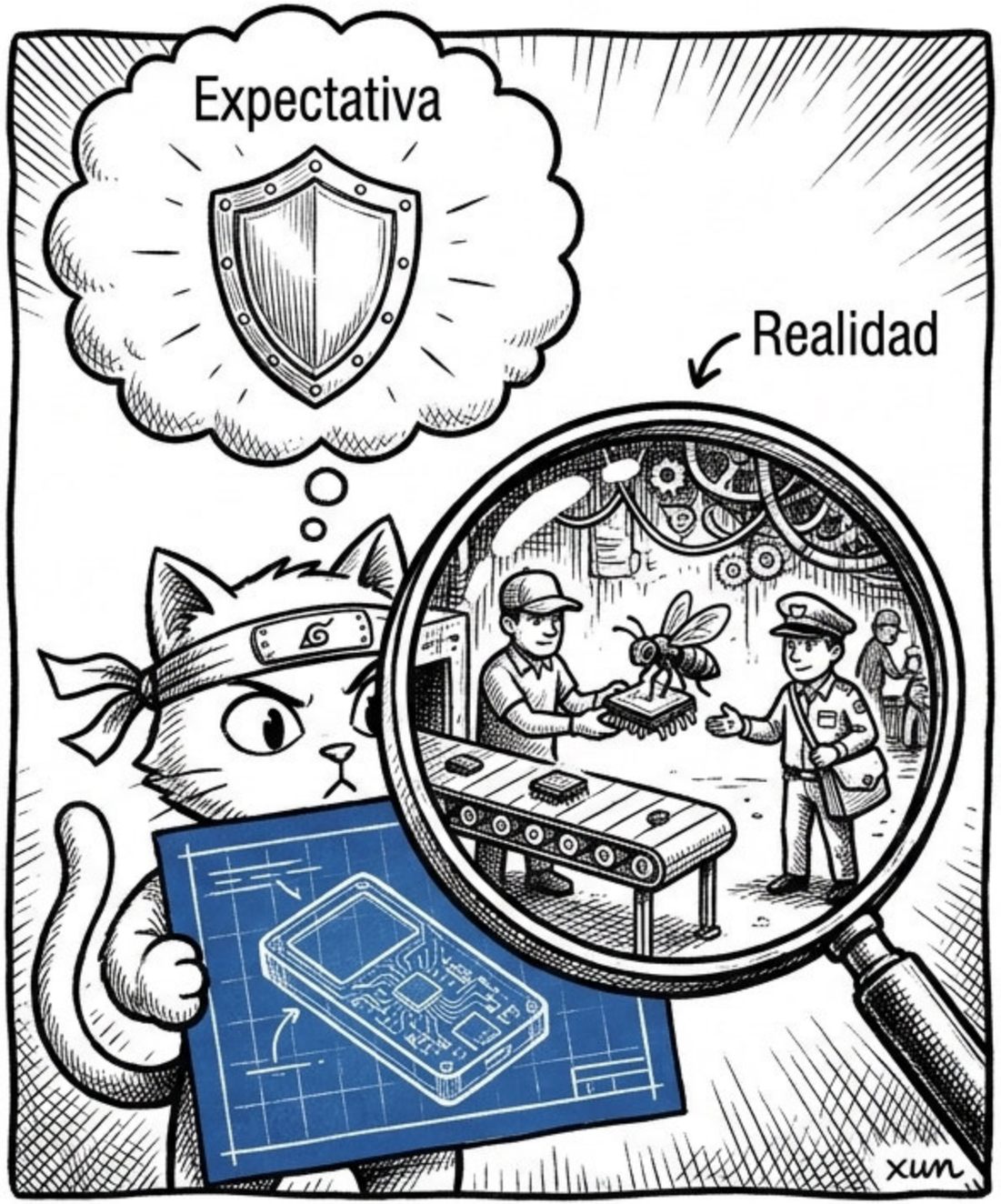
**Paso A** (Cero Riesgo):
Tu computadora ensambla la transacción.

⇒

**Paso B (Riesgo Crítico):** El HW tiene un solo trabajo sensible: **Firmar con tu clave privada** en su interior, sin dejar que toque internet.

⇒

**Paso C** (Cero Riesgo):
La transacción firmada se transmite al mundo.




# La trampa de la confianza ciega.

| | |
|---|---|
| **Promesa:** Es Open Source. | **Realidad:** El software sí, pero es imposible verificar qué hace realmente el chip de silicio físico (STM32/ESP32). |
| **Promesa:** Viene de fábrica sellado. | **Realidad:** Intervenciones en la cadena de suministro, carteros comprometidos y backdoors de fábrica. |

**Eres un blanco de alto valor que concentra su riqueza en una caja de plástico.**




# El Manifiesto Clandestino.

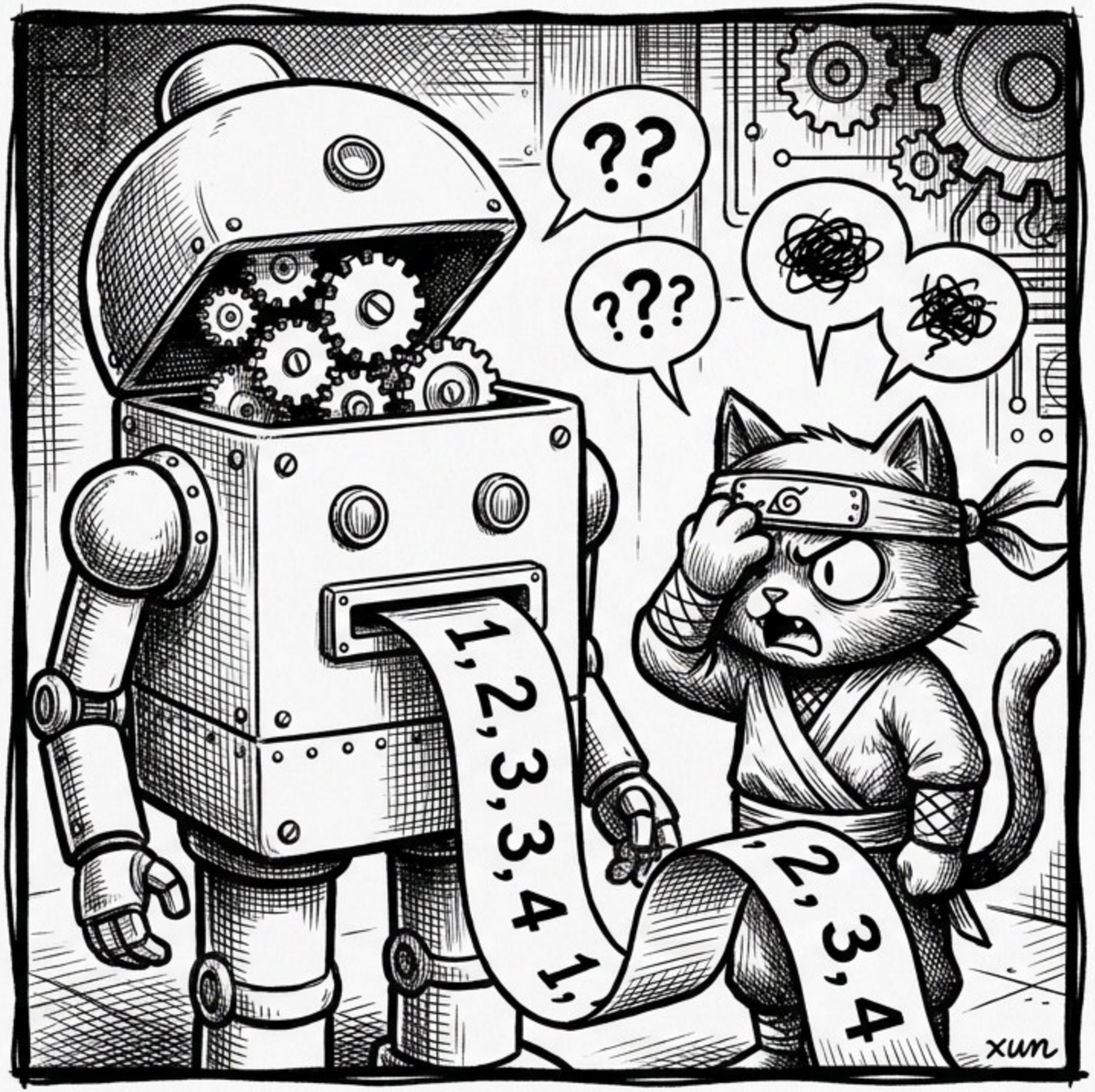
1. Do not say you own a HW. (Nunca reveles que tienes uno).
2. Do not buy a HW. (No lo compres... al menos no ciegamente).
3. Do not trust a HW... DIY? (No confíes en él... ¿Hazlo tú mismo?).

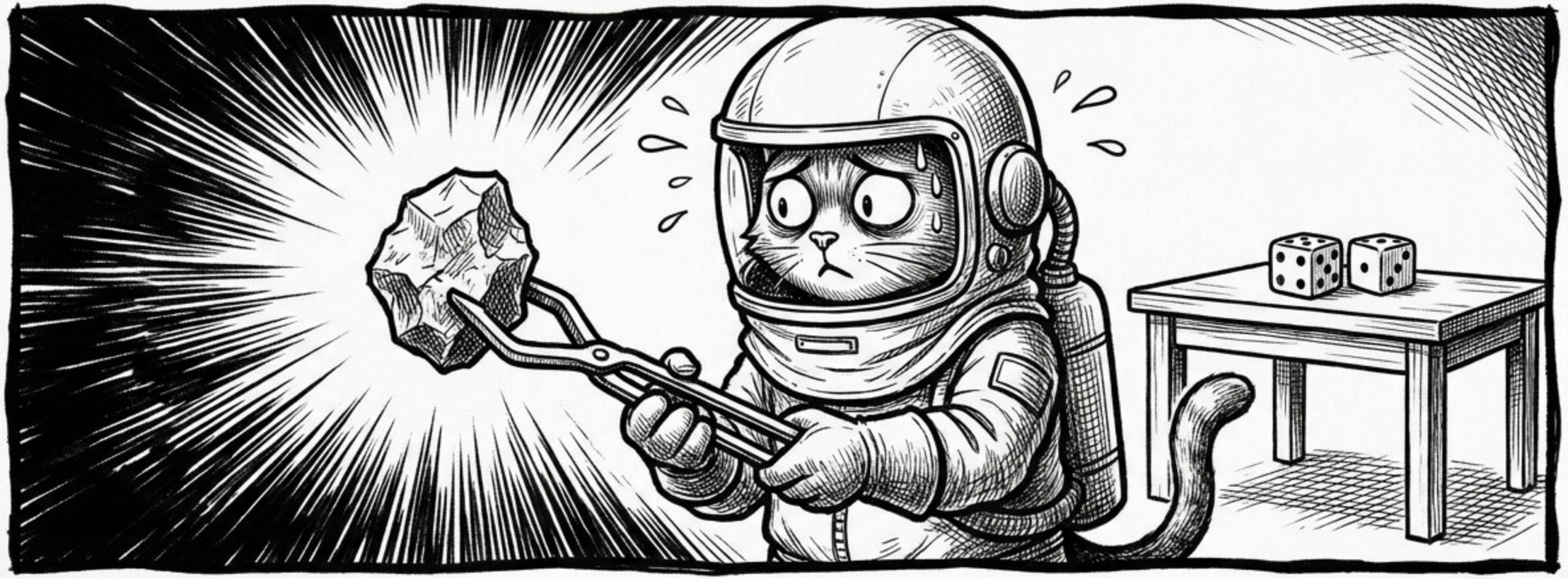
# El enemigo oculto: La Entropía.

La seguridad de tus fondos depende de la Entropía (aleatoriedad pura). Si el número de tu clave es predecible, tu dinero desaparece.

Los microchips son calculadoras **deterministas**. Son pésimos siendo 'aleatorios'.

**Core Insight:** Muchos fallos históricos de seguridad provienen de generadores de hardware defectuosos.






# Física cuántica vs. El mundo real.

**La Teoría:** Alex Waltz demostró que la verdadera aleatoriedad requiere eventos físicos impredecibles, usando desintegración nuclear para generar claves.

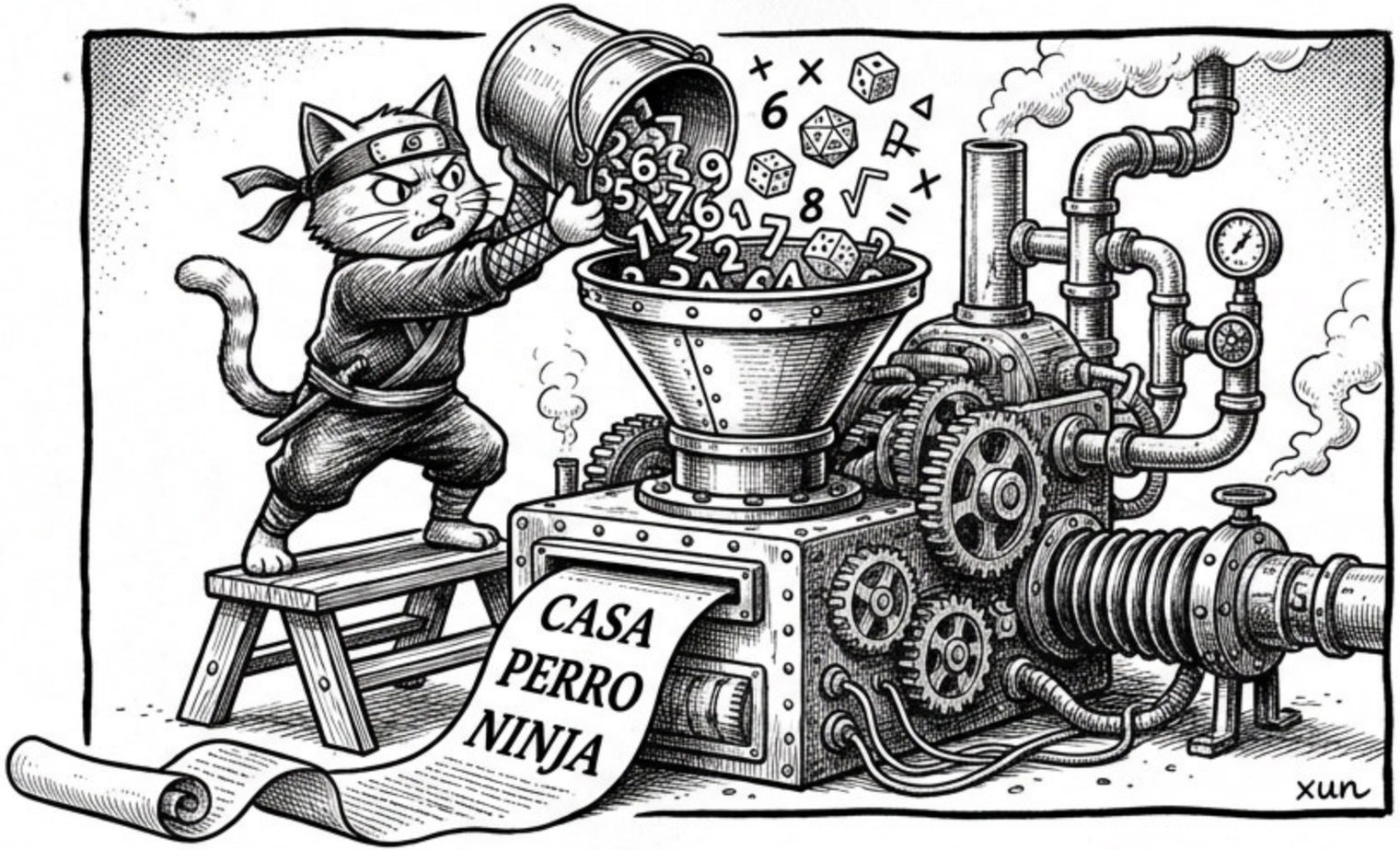
**La Práctica:** Como no guardas plutonio en la alacena, asume que el generador interno de tu HW es débil. La solución es analógica.




# Paso 1: Conviértete en el Caos.

## Genera tu propia entropía física.

Lanza dados reales decenas de veces y anota los resultados exactos. El caos de la física del mundo real es matemáticamente imposible de hackear, predecir o comprometer desde una fábrica.




# Paso 2: El traductor universal (BIP39).

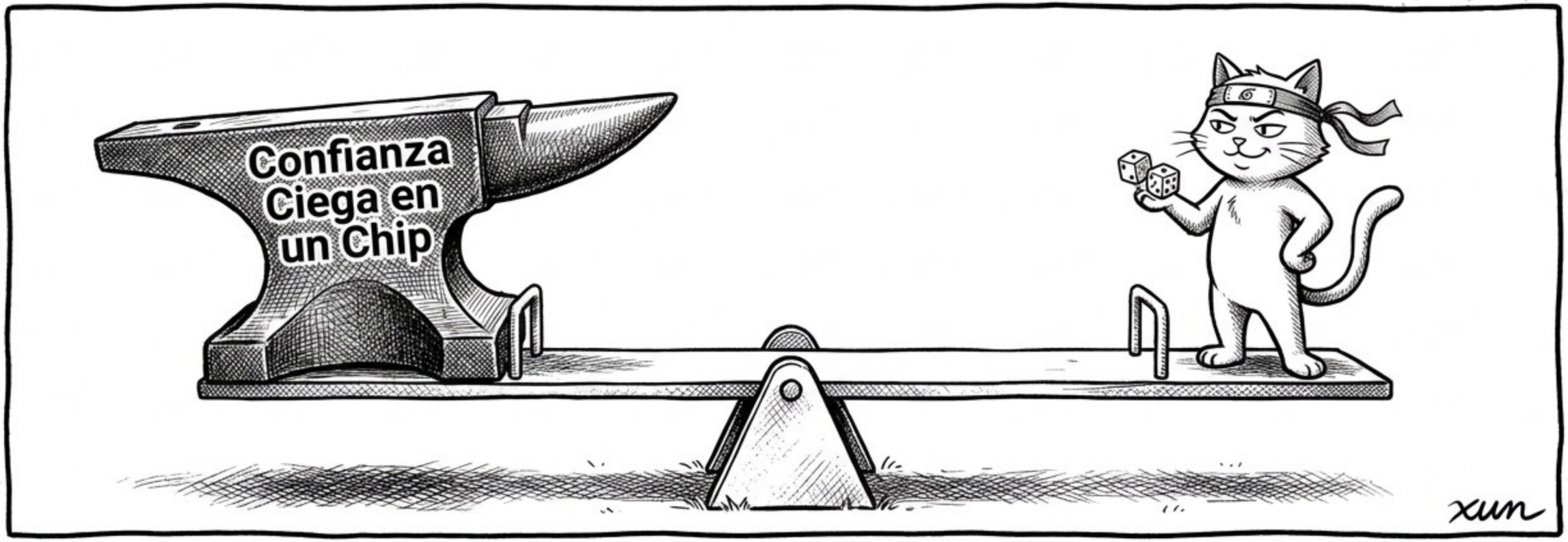
BIP39 es el estándar de Bitcoin que transforma tu caótica secuencia de números en una ‘frase semilla’ (seed phrase) de 12 o 24 palabras.

Elimina la necesidad de memorizar cadenas criptográficas, permitiéndote anotar palabras de un diccionario estándar.

# Paso 3: Aislamiento total (Modo Paranoico).

- [ ] Usa hardware de propósito general (una PC vieja que no uses).
- [ ] Descarga la herramienta BIP39 de Ian Coleman en un USB.
- [ ] Corta la conexión: Abre la herramienta en la PC vieja completamente desconectada de internet.
- [ ] Ingresa tus tiradas de dados y obtén tus 24 palabras en absoluto secreto.





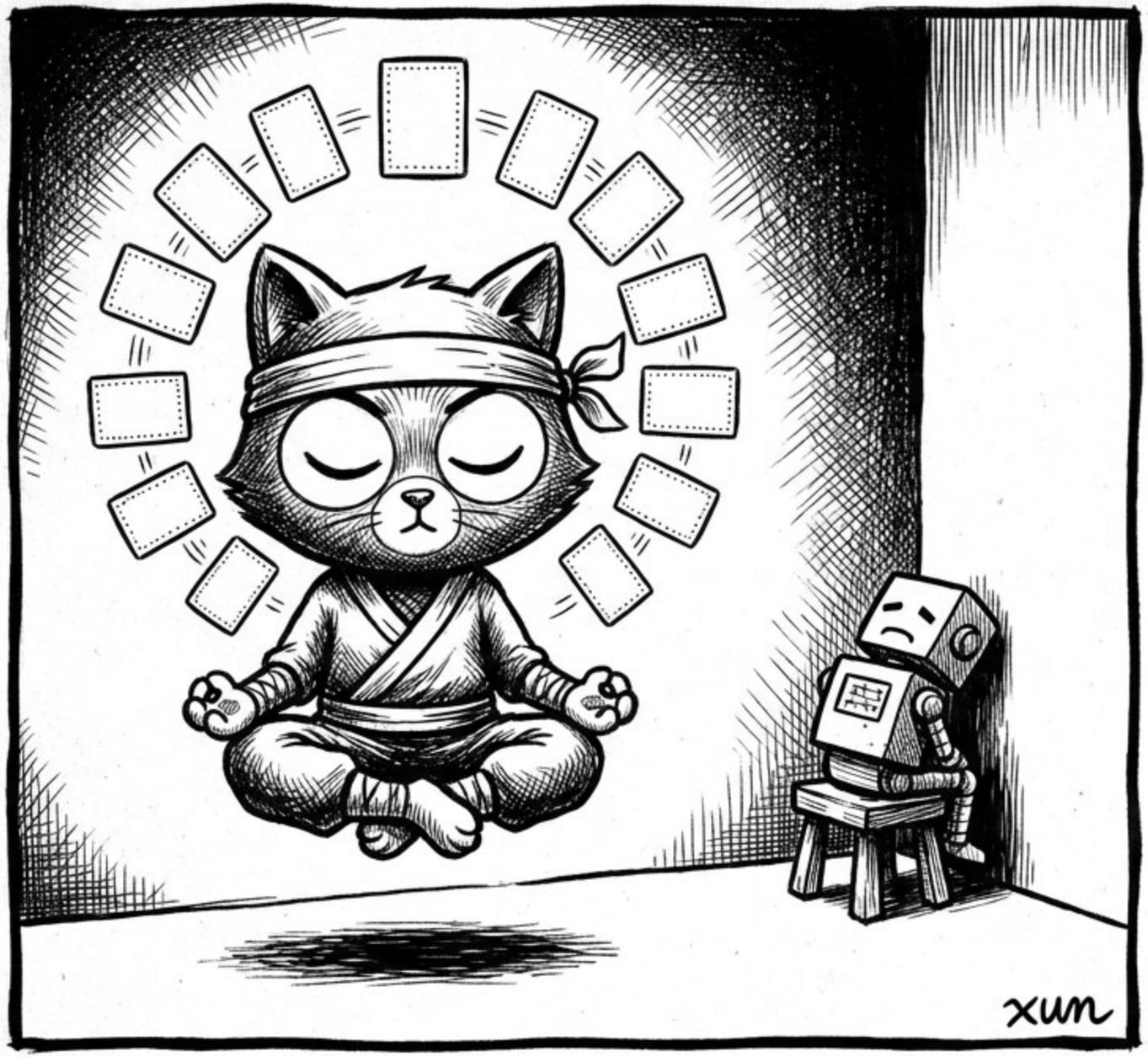

# El espectro de la custodia.

## Nivel Novato:

El HW genera la semilla.
(Riesgo: Bugs de firmware, generadores de aleatoriedad débiles, ataques de cadena de suministro).

## Nivel Ninja:

**Tú creas la semilla físicamente.**
El HW solo se utiliza como una calculadora tonta para firmar transacciones.
**(Minimiza drásticamente el residual de confianza).**




# El Zen de la Autocustodia.

**Verifica todo lo posible. Sé implacable con la generación de tus claves.**

La verdadera seguridad no se compra empaquetada en una caja de plástico; se construye asumiendo la responsabilidad de tu propia entropía.