

Inseguridad en procesadores



Agenda



- Presentarme
- ¿Hardware libre?
- Spectre & Meltdown
- Port Slackware riscv64
- ¿Que sigue?

¿Quién dice?



- Álvaro Figueroa
- ¿Informático? No, polímata
- Colaborador en GULCR y RCSL
- Tuve distro, basada en Slackware para Sparc
- Solo uso software libre
- Cofundador y Gerente técnico en Greencore Solutions

¿Cazador de pescadores ilegales?



Telf/Fax: 2257 1015
Greencore Solutions SRL, San José, Costa Rica
cursos@greencore.co.cr | www.greencore.co.cr



Búsqueme en:
alvaro@greencore.co.cr

<https://github.com/fede2cr>
https://twitter.com/fede2_cr

¿Grin que dijo?



- Greencore Solutions, desde 2005, asistencia técnica en software libre y GNU/Linux
- ~10 años de dar cursos y certificaciones en: GNU/Linux, Robótica (con hardware abierto), Seguridad (white hat), Python, Socios de Red Hat, LinuxFoundation, etc
- Todo el contenido de los cursos es Creative Commons, usa software libre, en varios cursos no se entrega libro sino una Raspberry Pi

¿Porqué la charla?



- Es común desconfiar en software
 - Cisco lleva 5 hardcoded passwords en 5 meses
 - Open/libre software
 - 2FA para prevenir keyloggers
 - Distribuciones aceptan solo código fuente
- ¿y el hardware? Lo dejamos en pocas manos, y con pésima historia de seguridad
- Impulsar arquitectura RiscV en la región

¿Hardware libre?

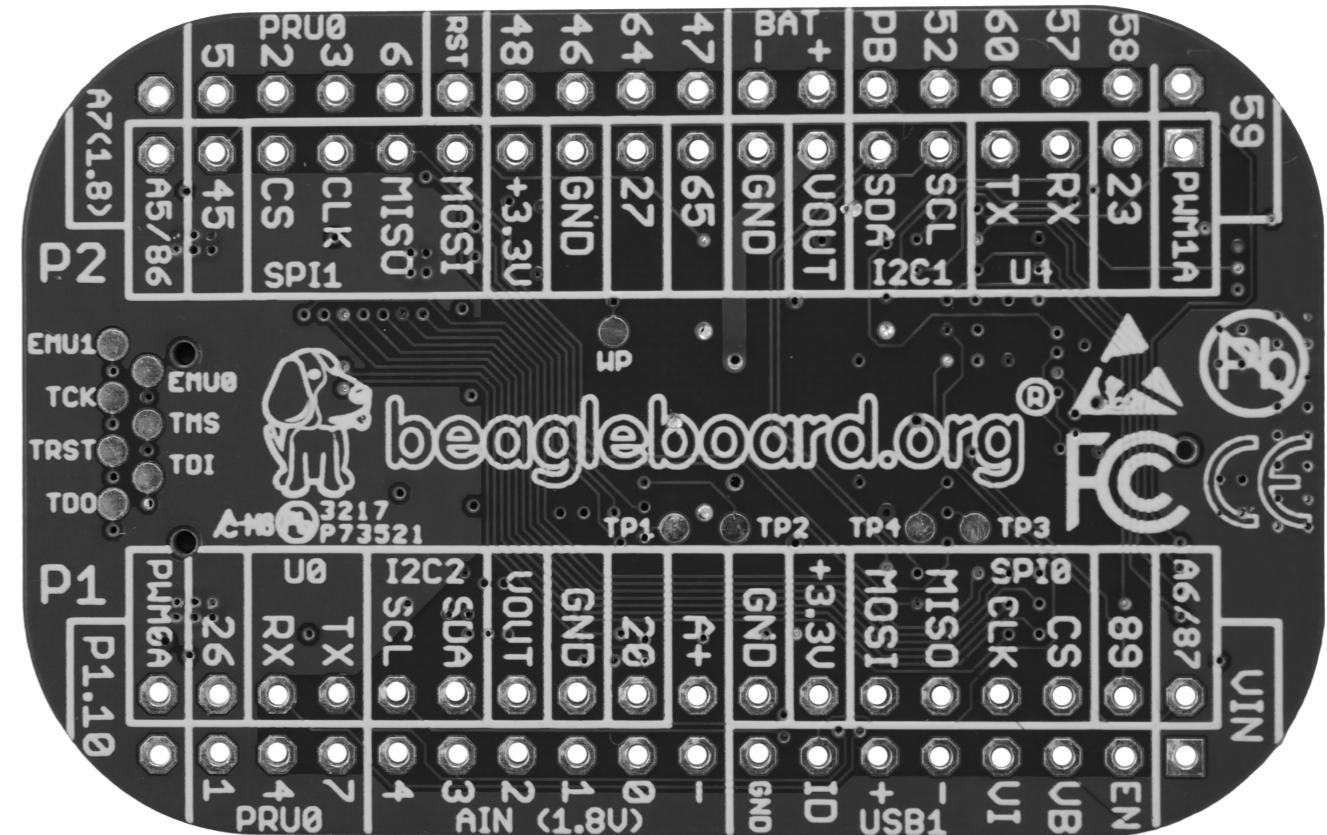
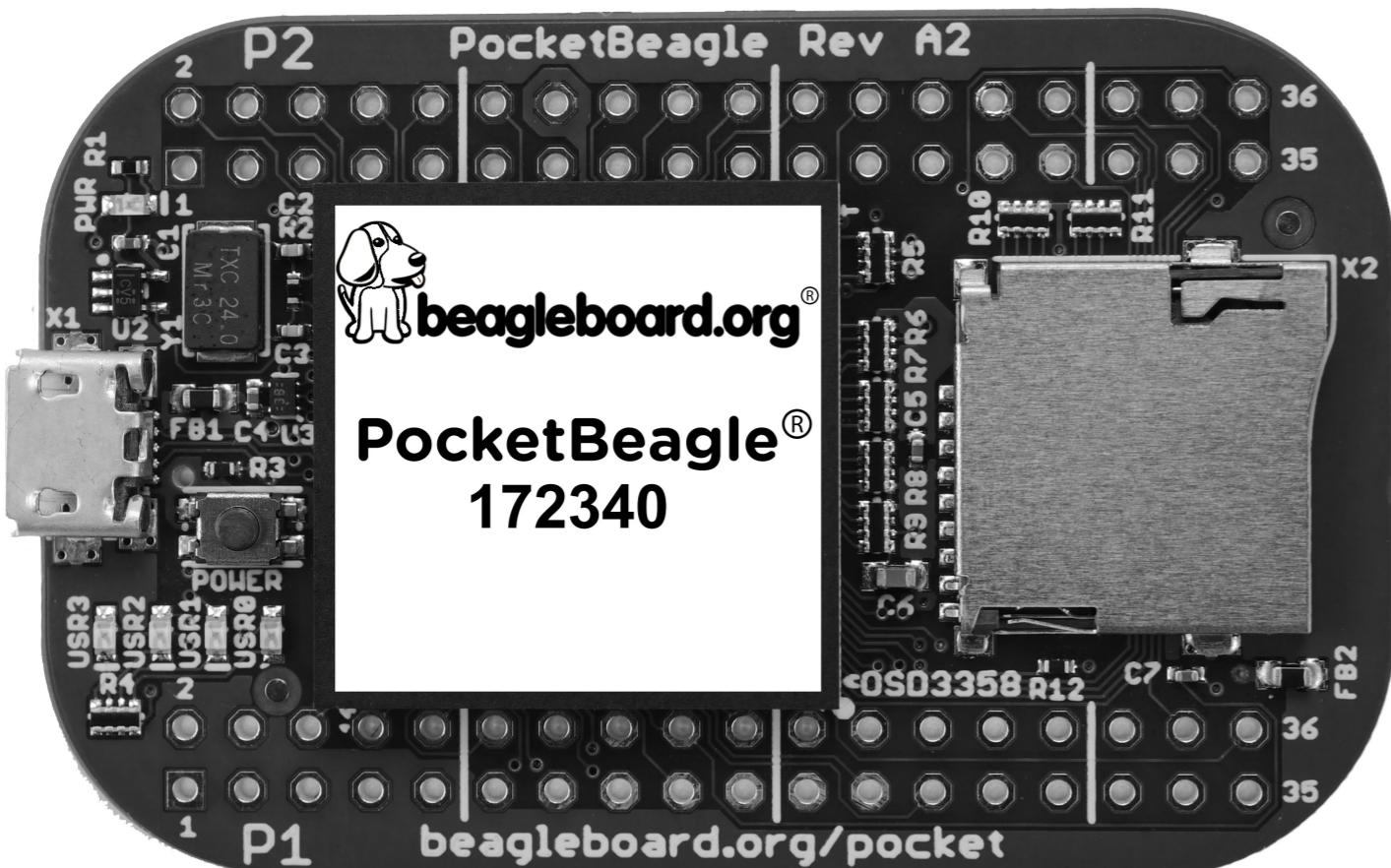


- Son muchos componentes, y definir libertad es complicado.
- Libre como Adafruit: Publican fuente de PCBs, crean comunidad, y entregan productos en desarrollo.
 - El software es EagleCAD que no es libre
- Libre como Raspberry Pi: Raspberry no es libre...

Pocket Beagle



- Diseño de PCB disponible en KiCAD, Bill-of-Materials (BOM).
 - OSHPark tiene su versión, sencillo de ordenar
 - Procesadores OCTAVO, System-on-a-Chip

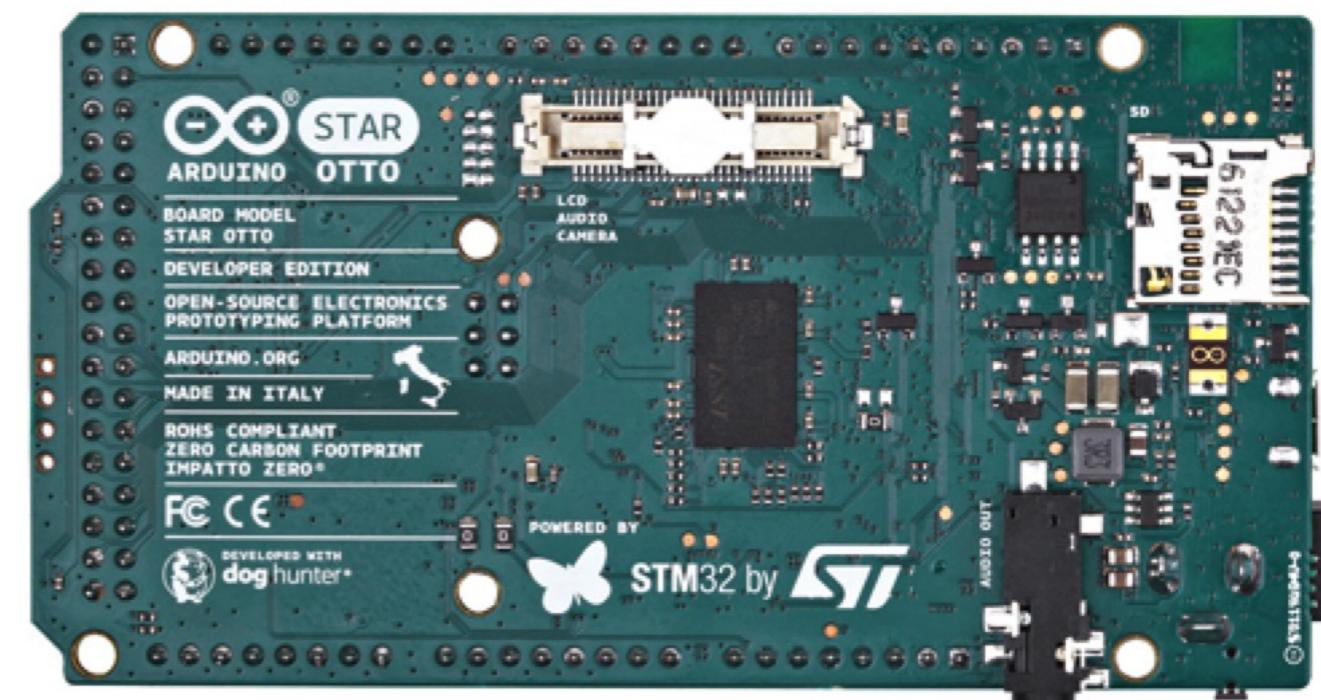
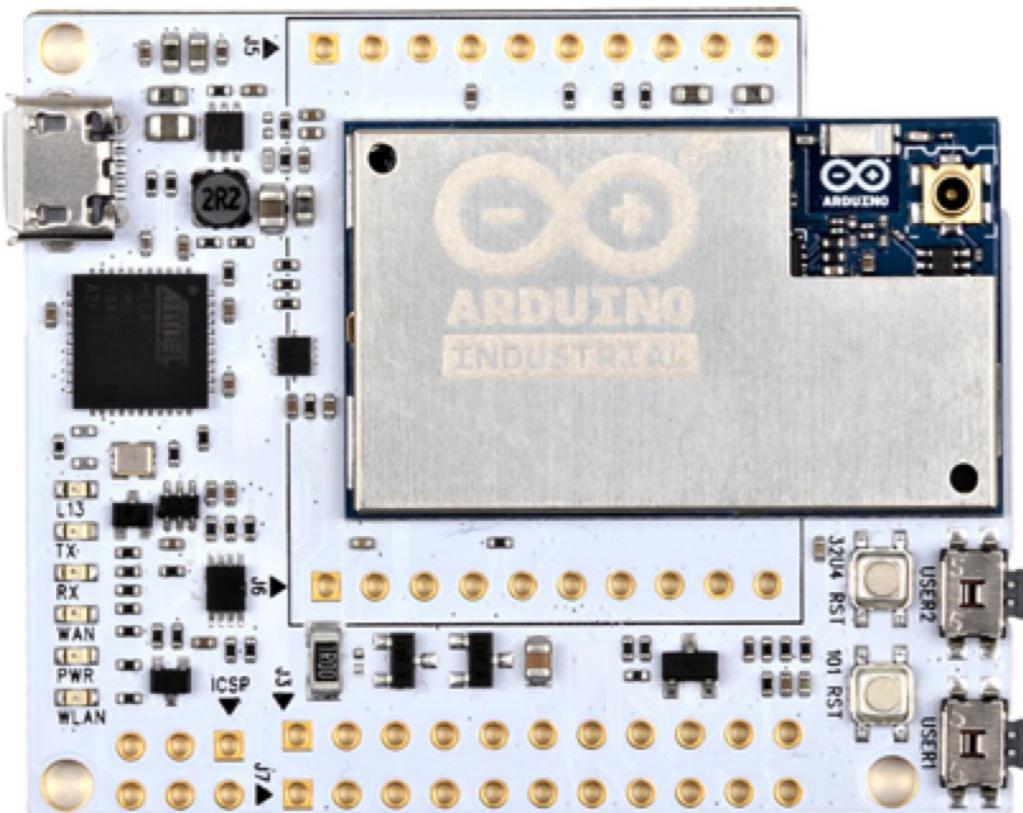


<https://github.com/beagleboard/pocketbeagle/wiki/FAQ>

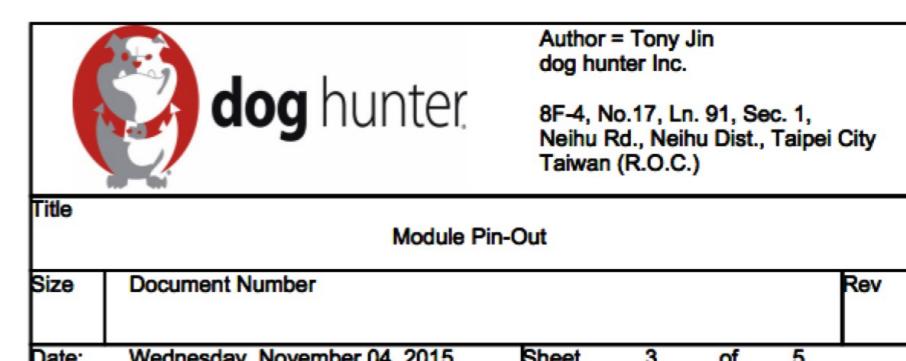
¿Hardware libre? #FreeArduino



- ¿Libre como Arduino?



Industrial 101, Otto y FPGA



<https://blog.adafruit.com/2017/06/26/arduino-industrial-101-arduinoorg-freearduino-is-it-open-source/comment-page-1/>

https://blog.adafruit.com/2017/07/02/is-the-arduino-star-otto-open-source-st_world-arduinoorg-st_news-arduino/

Spectre+Meltdown



Variant	Description	CVE	Codename	Affected CPUs	More info
Variant 1	Bounds check bypass	CVE-2017-5753	Spectre v1	Intel, AMD, ARM	Website
Variant 1.1	Bounds check bypass on stores	CVE-2018-3693	Spectre 1.1	Intel, AMD, ARM	Paper
Variant 1.2	Read-only protection bypass	CVE unknown	Spectre 1.2	Intel, AMD, ARM	Paper
Variant 2	Branch target injection	CVE-2017-5715	Spectre v2	Intel, AMD, ARM	Website
Variant 3	Rogue data cache load	CVE-2017-5754	Meltdown	Intel, ARM	Website
Variant 3a	Rogue system register read	CVE-2018-3640	-	Intel, AMD, ARM, IBM	Mitre
Variant 4	Speculative store bypass	CVE-2018-3639	SpectreNG	Intel, AMD, ARM, IBM	Microsoft blog post
-	Return mispredict	-	SpectreRSB	Intel, AMD, ARM	Paper
-	Access-driven remote Evict+Reload cache attack	-	NetSpectre	Intel, AMD, ARM	Paper

Spectre+Meltdown



- ¿Como caímos en esto?
 - Muere ley de Moore
- ¿Tantos ataques juntos? Sandsifter
- ¿Como mitigar?
 - OpenBSD deshabilita HT
 - No Virtualizar ni contenedores: Muerte a “la nube”
- ¿Siguen peores?
 - Faltan secretos: Rootkits invisibles, Minix y FPGAs
 - Variante TLBleed: Conferencia Blackhat (4-9 Agosto)

Chips libres



- RISC es una forma de diseñar procesadores, usando simplicidad para alcanzar diseño.
- Se han venido usando en UCB, varias generaciones de procesadores académicos, RISC-V sería la 5ta versión
- Podemos correr varias implementaciones de procesadores RISC-V en FPGAs
- Algunos miembros: NVidia, Espressif, Microsemi, Lattice, MediaTek, Qualcomm, Esperanto.ai

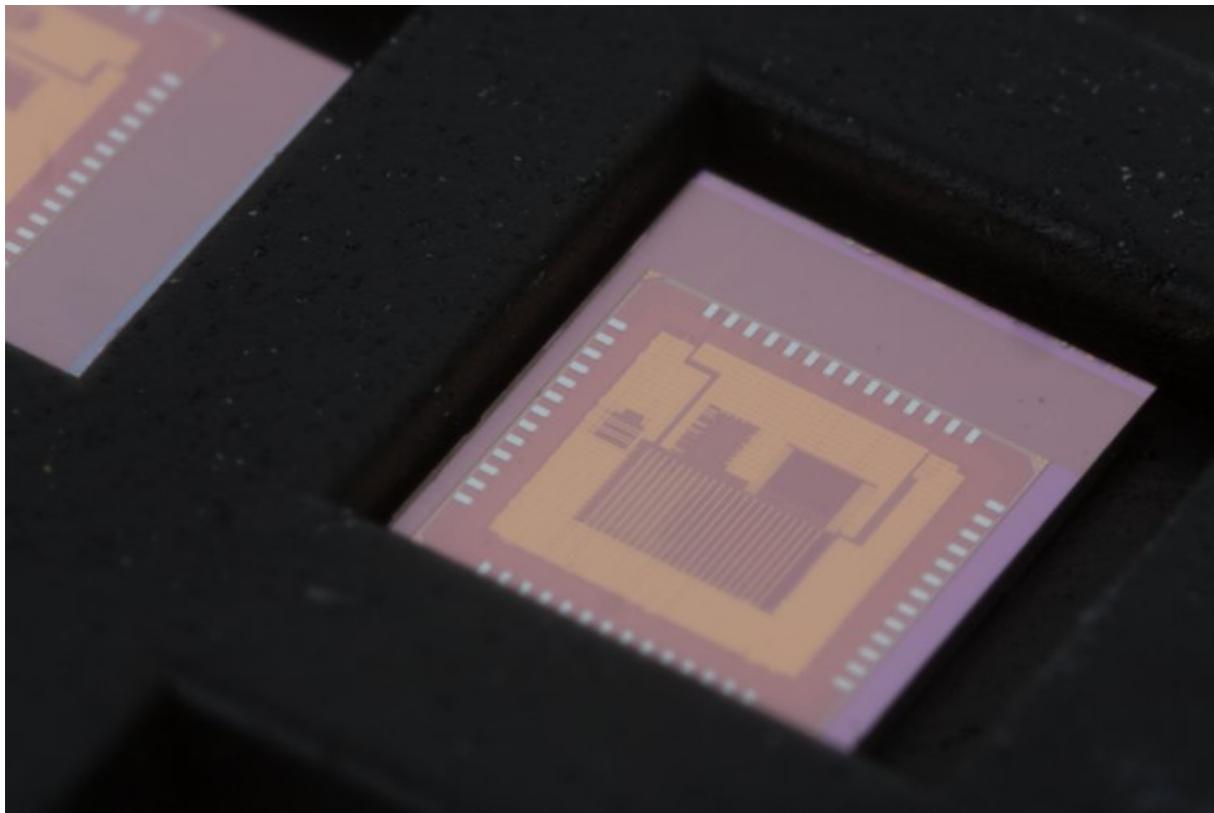
Chips libres



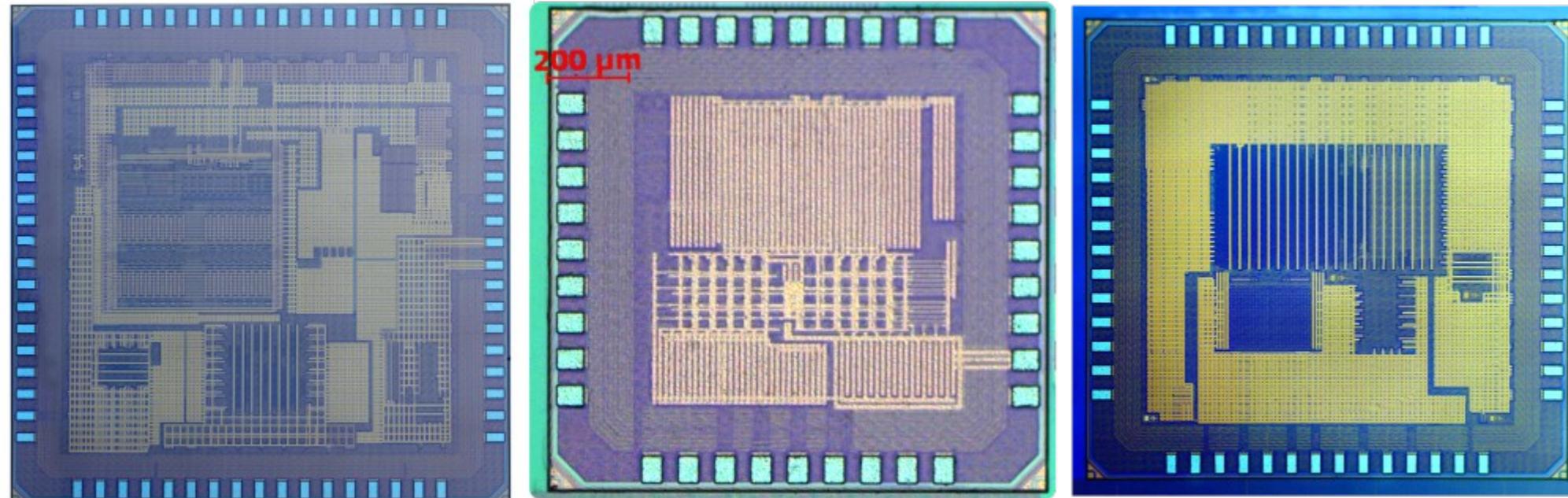
RISC-V Foundation: 65+ Members



OnChip



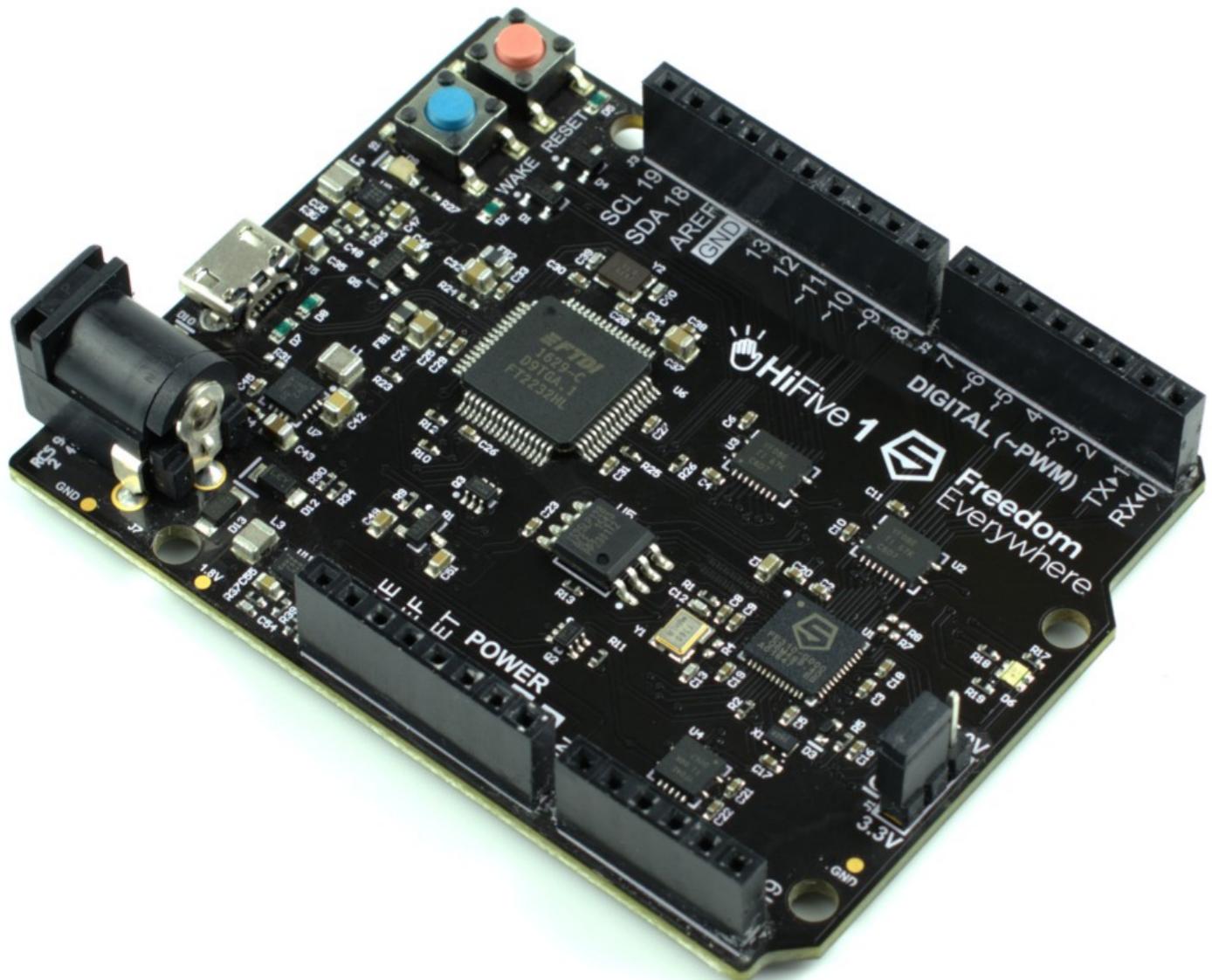
**OpenV - micro 32 bits
Crowdsupply fallido**



**Módulos de Itsy-Chip
Aprox \$100**

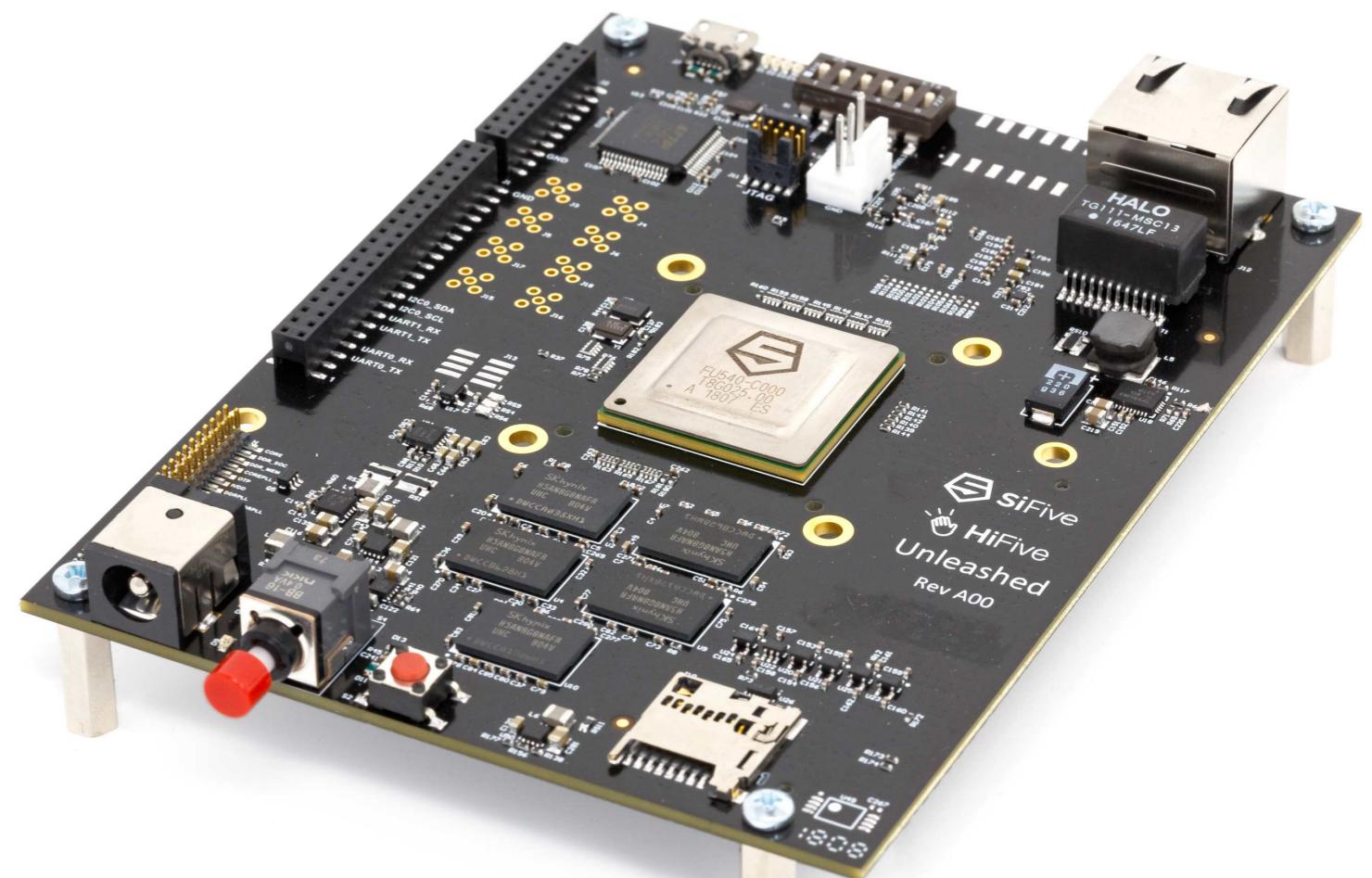
<https://hackaday.io/project/152709-itsy-chipsy-make-your-own-100-chip>

SiFive



**32 bits
Microcontroladora**

<https://www.sifive.com/products/hifive1/>



**64 bits
GNU/Linux**

<https://www.sifive.com/products/hifive-unleashed/>

RiscV



- Pocas instrucciones, sencillo de aprender, crear software para arquitectura. Elegante
- Para 32 bits (microcontroladoras), 64 bits (“Linux”) y en papel para 128 bits
- Evita SIMDs, para usar Vectores
- Sencillo de integrar múltiples tipos de cores

RiscV



- Core Modular:
 - M (multiplicar y dividir)
 - FD (punto flotante single/double)
 - A (Operaciones atómicas)
 - C (instruc. comprimidas)
 - V (Vector)
- Arquitectura de permisos y privilegios, ideal para aplicaciones de alta seguridad

Slackware riscv64



- Patrick Volkerding, creador de Slackware, la distro más vieja existente, base de Splack Linux

“(bug report from Alvaro Figueroa Cabezas)”
ChangeLog de Slack 9.1



slackware/slackware-9.1/ChangeLog.txt

Public Domain, <https://commons.wikimedia.org/w/index.php?curid=205333>

Slackware riscv64



https://github.com/fede2cr/slackware_riscv

- Port para riscv64 en progreso, 815 paquetes hasta el momento, “chroot” de +4.4GiB
- Paquetes de todas las series
- Por el momento usando base de Fedora (stage4), pero se ya se compiló Kernel, por lo que falta poco
- Usando qemu-riscv

Slackware riscv64



- Importante: Necesitamos hardware. Se ha contactado a Palmer Dabbelt de Sifive, pero me ha ignorado por +2 meses
- El hardware se ofrecerá a desarrolladores locales, sin importar el proyecto
- Patrick Volkerdi de Slackware también está solicitando donaciones por medio de su [PayPal](#)

¿Que sigue?



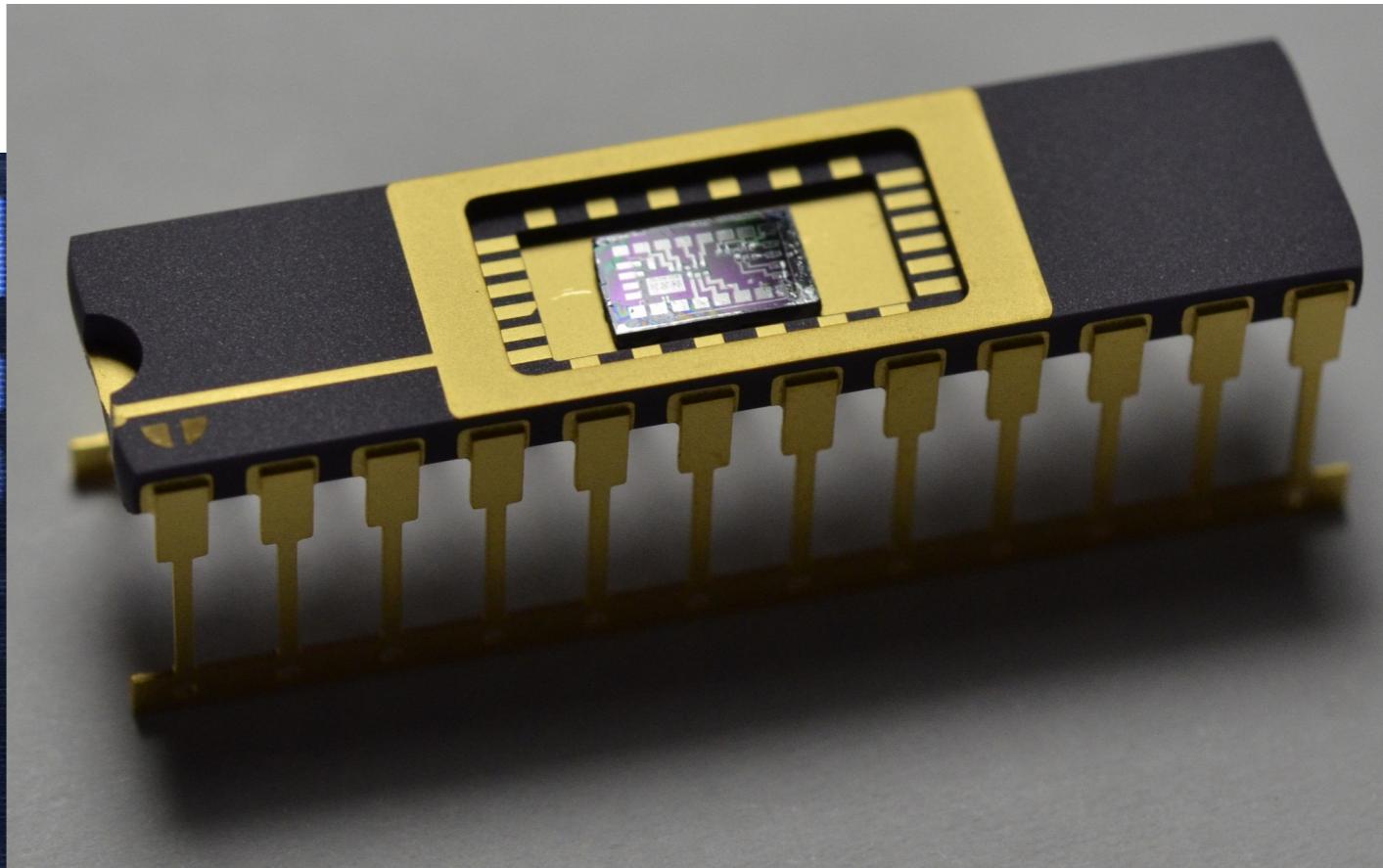
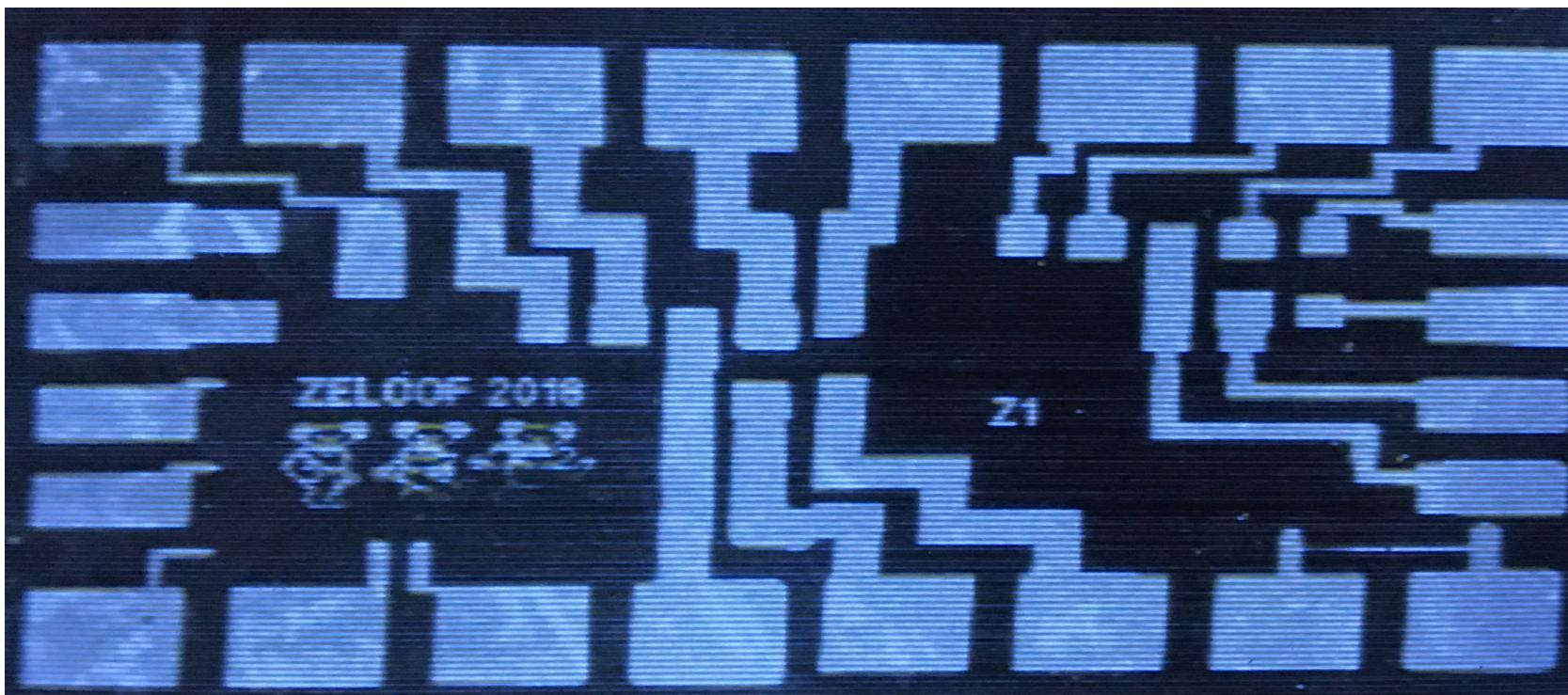
- Replicar la Pocket Beagle, pero con cores Riscv64
- Replicar una Beagle Board/Pi con Riscv64
- “Renovar” mi laptop preferida
- Riscv128
- Charla de **Bunnie Huang** sobre otros factores a tomar en cuenta



¿Que sigue?



- Sam Zelooft pudo crear primer circuito-integrado, con recursos maker/hobbie/garaje
- La comunidad quiere replicar, y Sam ya está creando la segunda versión del laboratorio para probar otras técnicas





¿Dudas o consultas?



Muchas gracias