The Libre-SOC Hybrid CPU-VPU-GPU

and why Libre/Open is crucial
(even in a business context)
Practical gotchas for Silicon Transparency

Silicon Salon 2022

Sponsored by NLnet's PET Programme

May 24, 2022

What is the Libre-SOC Project

- An entirely Libre Vector-enhanced Power ISA compliant CPU with enough legs to tackle Supercomputing-class workloads.
- Working closely with the OpenPOWER Foundation: no rogue custom instructions. Both Long-term stability and open-ness is key.
- Huge reliance on Python OO and Software Engineering as applied to HDL. Not just traditional Verification: unit tests at every level, Formal Correctness Proofs as unit tests. "python3 setup.py test"
- Using Libre VLSI Tools: coriolis2 (by Sorbonne University) ultimate goal is to have the GDS-II Files publicly reproducible

What challenges does a Crypto-Wallet ASIC face?

- Industry-endemic paranoid 5-level-deep NDA Chain. Foundry NDAs themselves are under NDA. Sharing between teams inside the same company is prohibited! Cell Libraries: NDA'd. PDKs: NDA'd. HDL designs: NDA'd.
- Power-analysis attacks. Timing attacks. EMF attacks. Standards Verification (FIPS ain't it). Toolchain attacks. Cacheing is out: performance will suck.
- Achieving Full Transparency - a critical goal - is almost impossible to achieve. Ultimately, you need to buy (or build) your own Foundry.
- Production and Development costs (NREs) almost certainly dwarf the Sales costs.

Pragmatic solutions

- Use Formal Correctness Proofs at every step. Caveat: proofs are only as good as the mathematicians that write them!
- Work with Standards bodies (e.g. OpenPOWER Foundation ISA WG) and Members with similar interests. Custom Extension with zero public review == bad.
- Unstable PLLs to detect rogue EMF
- Develop a product that has a larger total market (an SoC)
- Accept that some levels of NDA are "out of reach" for now.
- Use E-Fabless "ChipIgnite" to at least get the NREs down.
- Ultimately: buy your own Foundry, make the PDK and Cell Library public. Only use Libre VLSI tools (limits to around 130 nm at the moment). Everything is "early days" in this space

The end

Thank you

Questions?

- Discussion: http://lists.libre-soc.org
- Libera.Chat IRC #libre-soc
- http://libre-soc.org/
- http://nlnet.nl/PET
- https://libre-soc.org/nlnet/#faq