Also, most of the ARM-based SoC's implement a so called TrustZone (TZ) extension. Of course, as with most technologies on ARM, TZ is just a specification and not malicious in itself. However, it opens a possibility for the vendors who produce TZ-compatible SoCs (which most do) to lock down their processor so that their TZ implementation will not differ significantly from Intel ME.

Also, there is nothing special in ARM-based architecture that could prevent a vendor from introducing backdoors into the SoCs they produce.

FPGA-based, true open source processors and platforms?

There are also efforts to create a fully open processor design ([1], [2]). This surely is the proper way to go for our civilization, long term. The important question is how much time it would take for such processors to become performant enough for typical desktop workflows (e.g. watching HD movies, running modern Web browsers or an office suite)?

But performance is only part of the story – another question relates to security technologies these processors should be offering? Technologies such as e.g. IOMMU and potentially also CPU and memory virtualization?[1]

Sadly, it seems like we're at least years away from having consumer-grade laptops based on such processors, and perhaps more than a decade from having these systems offering isolation technologies on par with what the current Intel processors offer.

[1] Arguably virtualization technologies might not be needed for such new processors. On the other hand, it might turn out more practical to port e.g. the existing Linux kernel and recompile many of the currently used POSIX applications for these new processors, than to write everything from scratch. In that case we would need virtualization in order to implement reasonably strong compartmentalization.