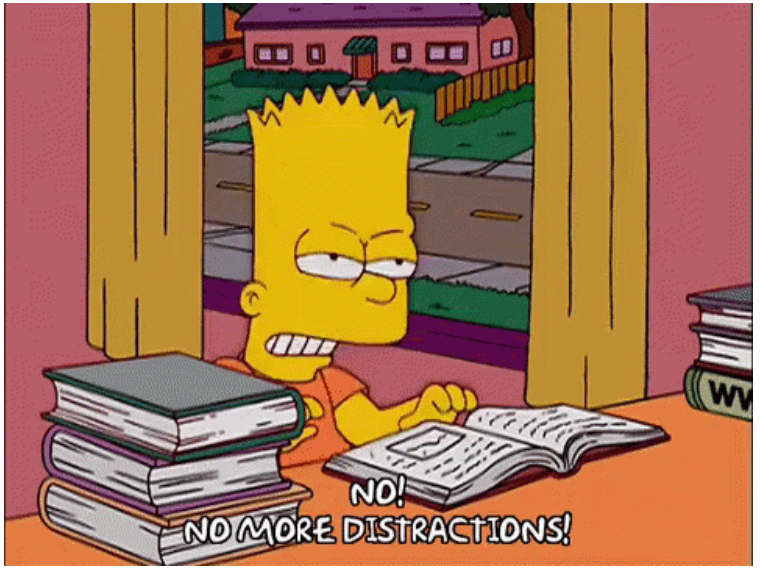
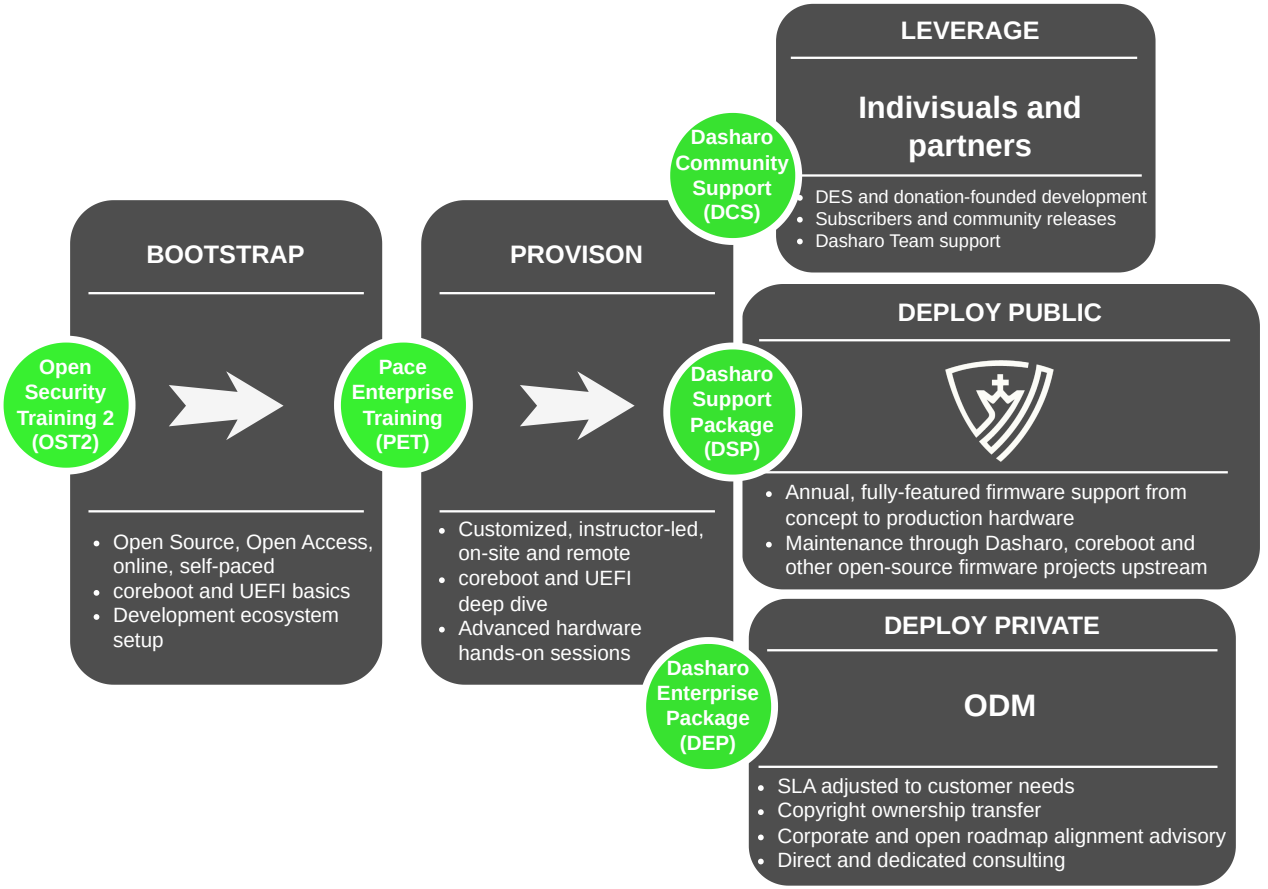
Dasharo Roadmap

Dasharo Roadmap Disclaimer

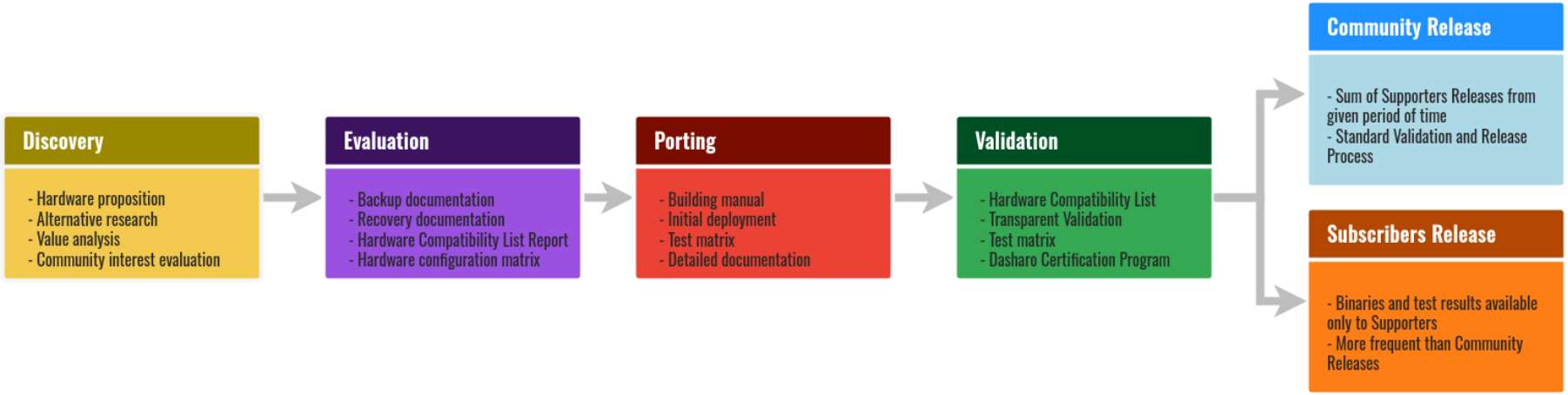


Please note that the roadmap for the Dasharo Community Support Program is subject to change and may not represent final release candidates or end of support dates. This roadmap is intended to provide guidance and direction for the program's development, but is not a guarantee of specific timelines or outcomes. For more information on release candidates or release dates, please contact the Dasharo Team directly.

From OST2 to Dasharo Support Package

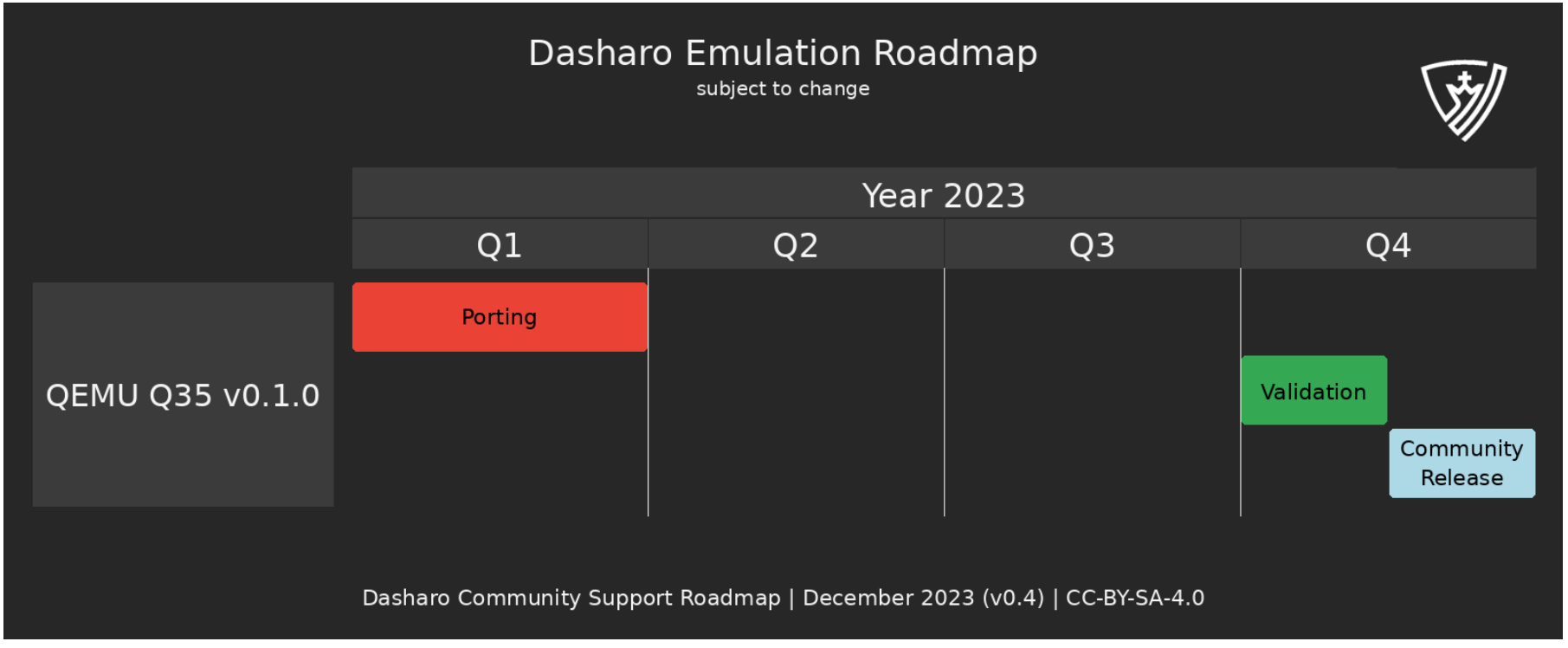


Dasharo Community Support Process



- How we qualify platforms for Dasharo Community Support?
- Business goals alignment with 3mdeb.
- Synergy with other projects e.g. TrenchBoot.
- Above stages very roughly map to real work/tasks performed by team.

Dasharo Emulation Roadmap



- Dasharo OSFV release provided infrastructure for validation.
- QEMU tests were proven to work and it is just matter to run set of tests defined by test matrix, prepare release notes and send newsletter.
- We will do that in Q4'23.

Dasharo Emulation Roadmap: Vision

- shift left firmware development
- new potential vendors/products: Intel Simics, AMD SimNow
- new potential release types to be supported for QEMU Q35 target
    - Dasharo (coreboot+UEFI)
    - Xen target (XCP-ng) although I'm not sure how how much firmware would be different, there is definitely stuff Xen-specific in OvmfPkg
- firmware will play role in Confidential VMs
- references:
    - MSFT talk about CVM
    - MSFT: DCasv5 and ECasv5
    - Edgeless Systems

Dasharo Emulation Roadmap: Features

Following features can be fully used:

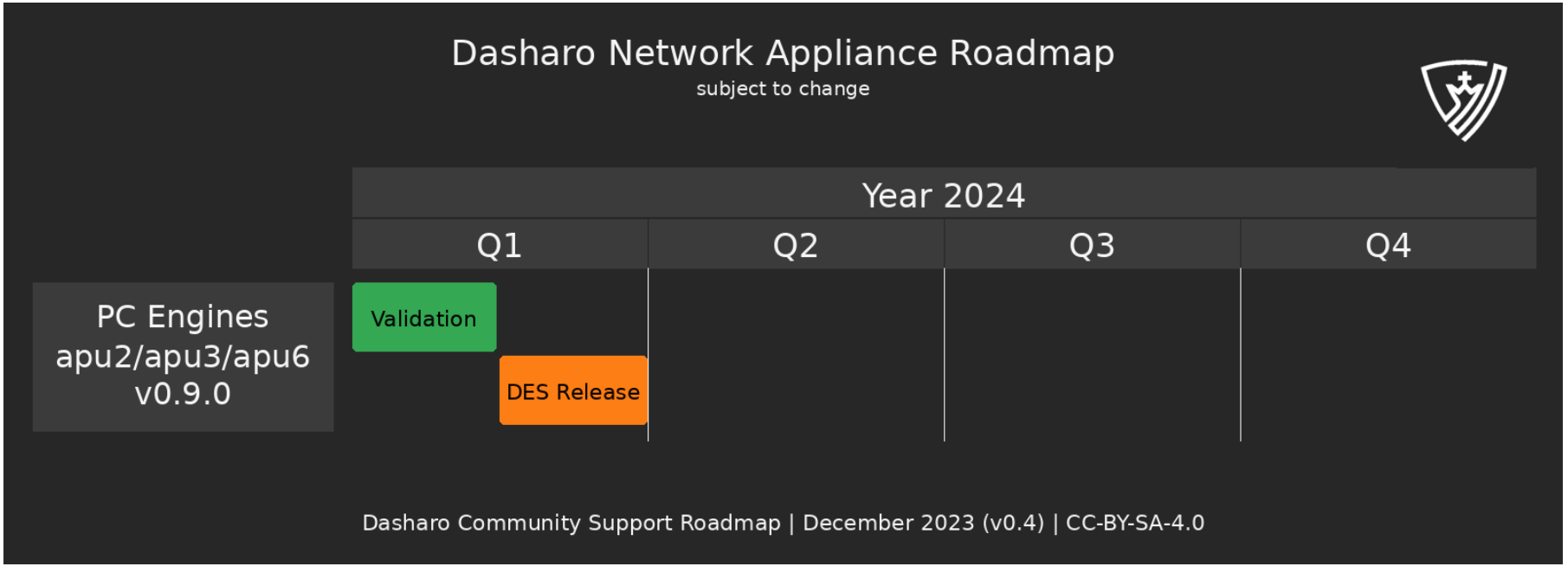
- Configurable boot order
- Configurable boot options
- Custom boot menu keys
- UEFI shell
- UEFI Secure Boot
- TPM Support
- Dasharo setup password
- Serial Port Configuration menu
- iPXE network boot
- ESP partition scanning in look for grubx64.efi or shimx64.efi or Windows bootmgr

Dasharo Emulation Roadmap: Features

Following features are visible in setup menu and can be used for testing the menus, but have no actual backend hooked up:

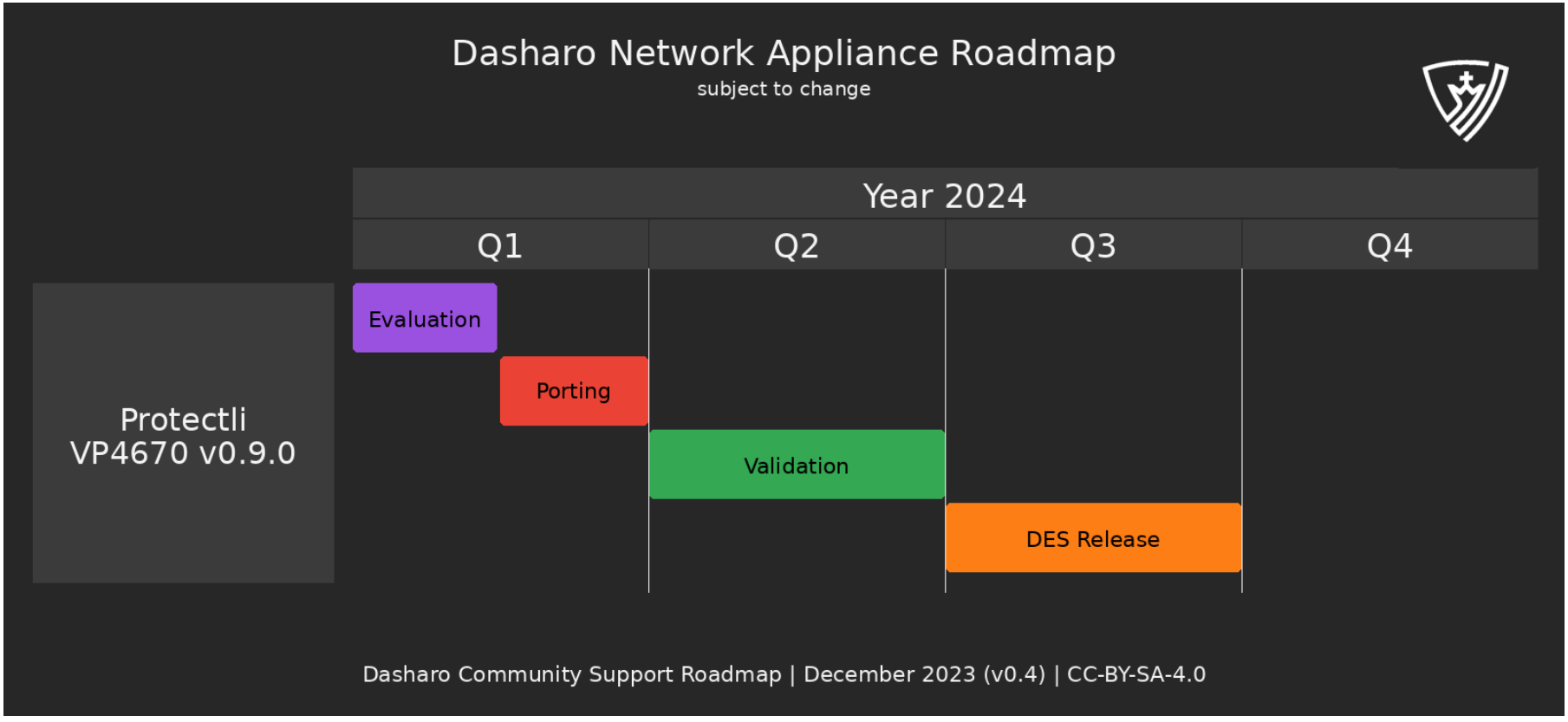
- PS/2 Controller enable/disable option
- Watchdog configuration menu
- Early boot DMA protection menu option
- Intel ME disable support and menu options
- SED/OPAL disk password support
- SATA disk password support
- SMM BIOS Write Protection support and enable/disable option
- USB stack and mass storage enable/disable option
- Firmware Update Mode feature
- One of the two fan profiles can now be selected in Setup Menu
- Setup menu option for switching between S0ix and S3 suspend mode
- Wi-Fi / Bluetooth module disable option in setup menu
- ...

Dasharo Network Appliance Roadmap



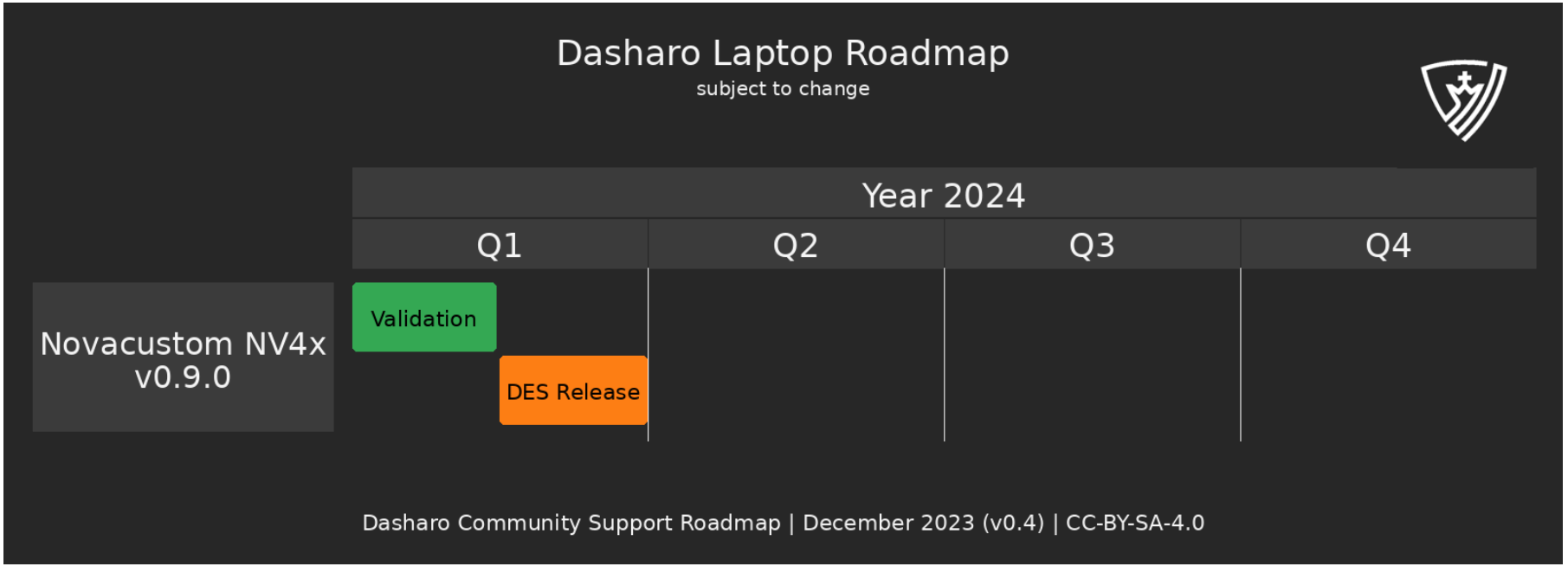
- We will prioretize Dasharo(coreboot+UEFI) for PC Engines in Q1'24
- There should be two options for buying DES
- We would like to enable as many Dasharo features as possible, especially important for us are security features (measured boot, TPM2.0 support, verified boot, UEFI Secure Boot).

Dasharo Network Appliance Roadmap



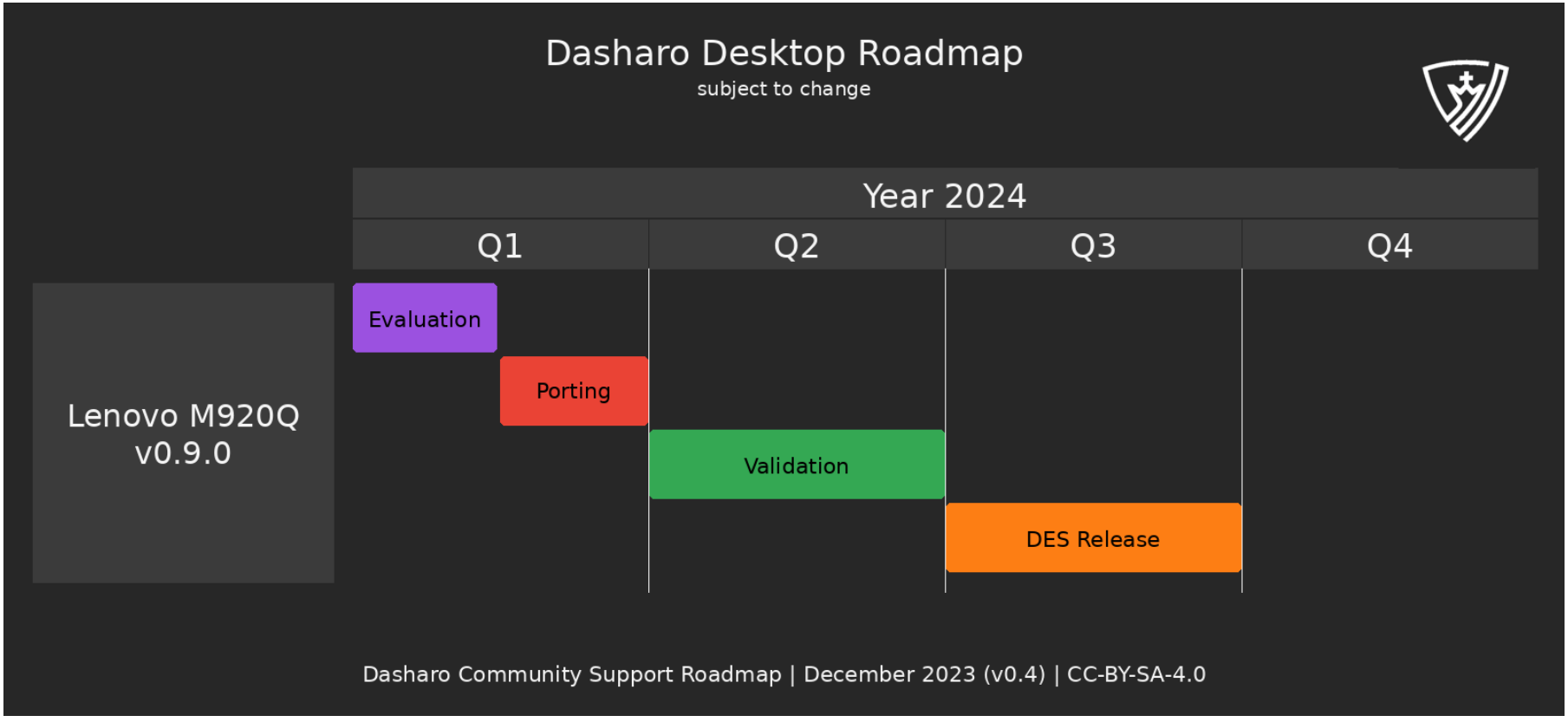
- Does Dasharo(coreboot+SeaBIOS) with TrenchBoot/D-RTM make sense on 10th Gen?

Dasharo Laptops Roadmap



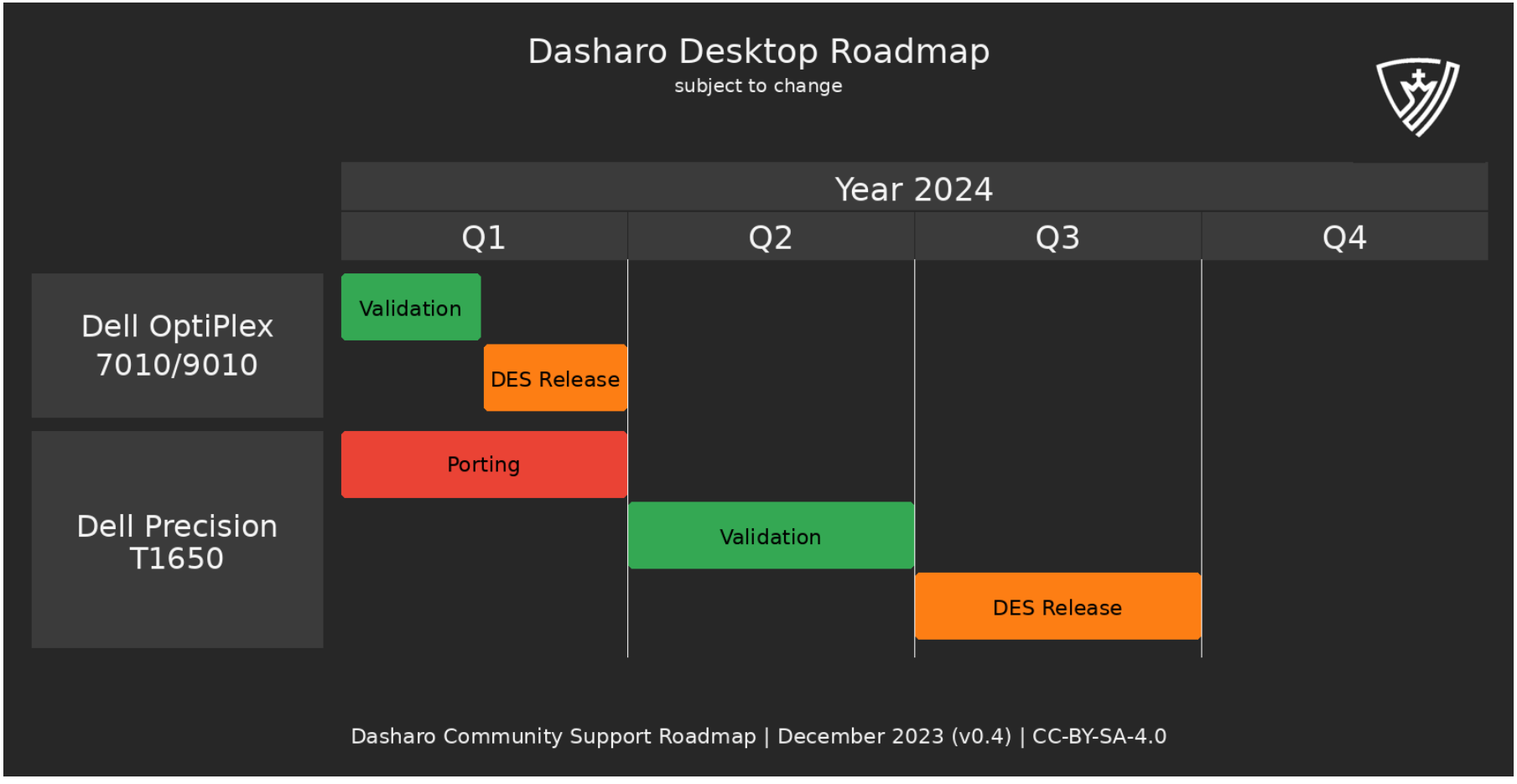
- Dasharo(coreboot+Heads) v0.9.0
- Shifted because of our engagement in NV4x/NS5x/7x 11th Gen v1.5.x and NV4x/NS5x/7x 12th Gen v1.7.x release series
- High priority release for Q1'24

Dasharo Desktop Lenovo Roadmap

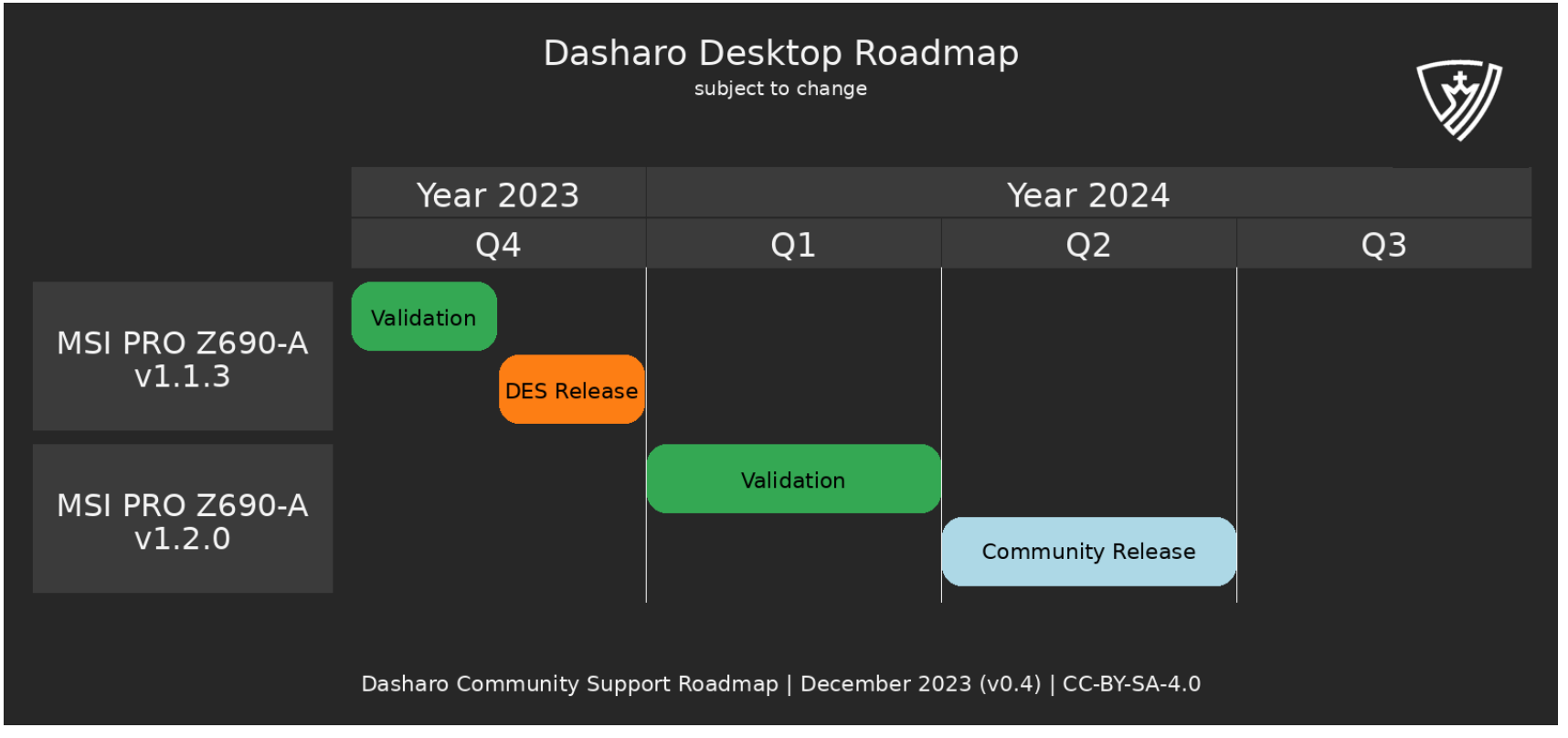


System is Intel Boot Guard Ready, verified boot disabled, ME not in Manufacturing Mode - Dasharo Porting Ready.

Dasharo Desktop Dell Roadmap

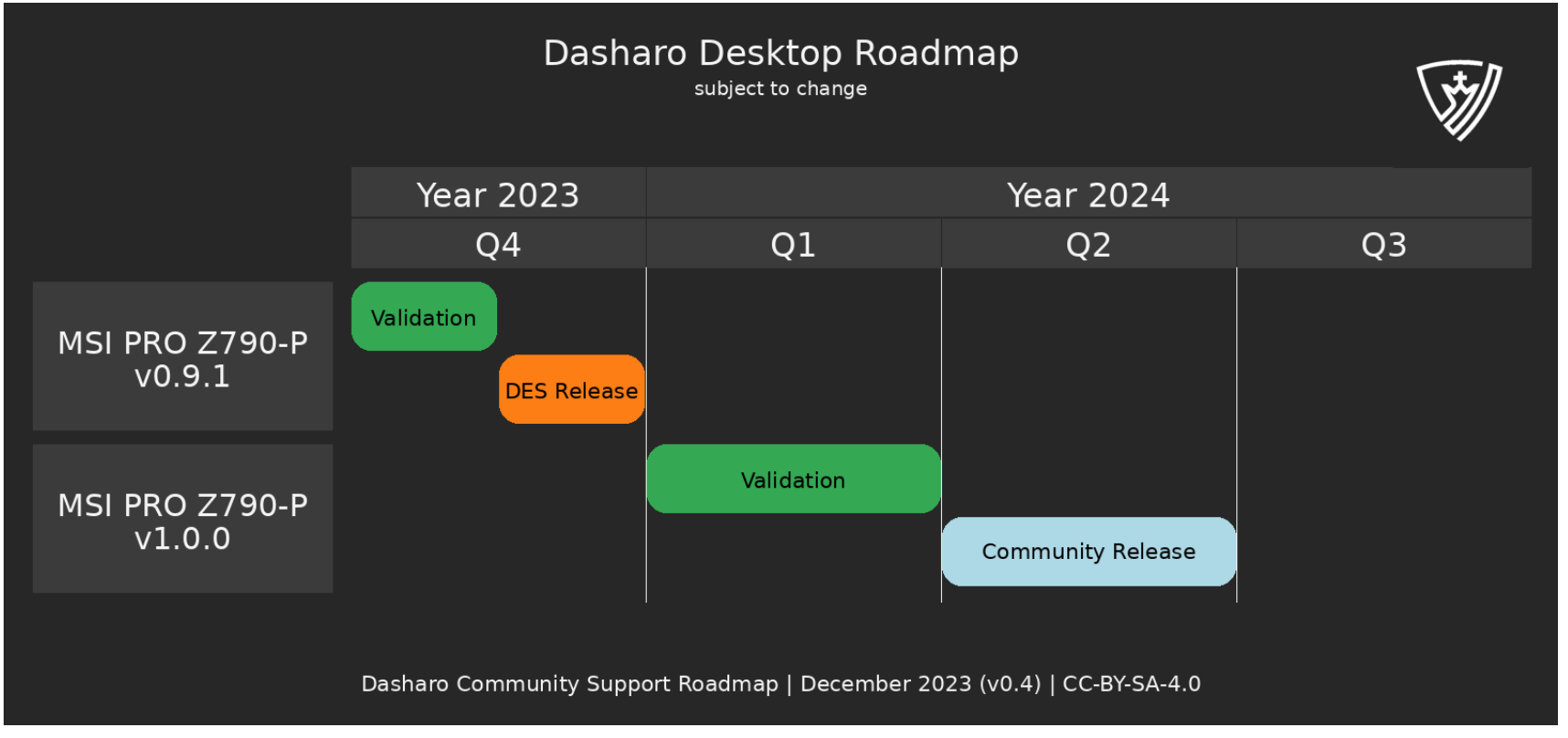


Dasharo Desktop MSI Roadmap



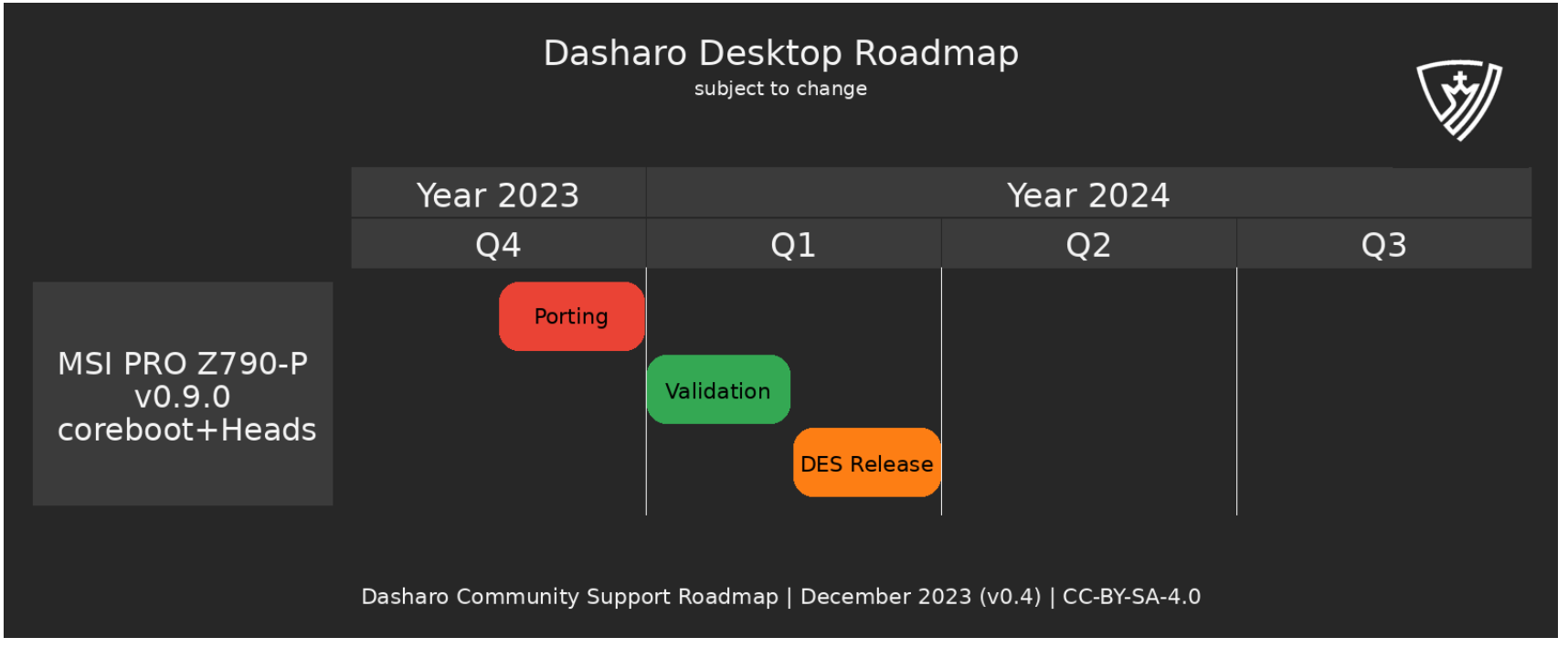
Community Release date changed because of PC Engines and NovaCustom.

Dasharo Desktop MSI Roadmap



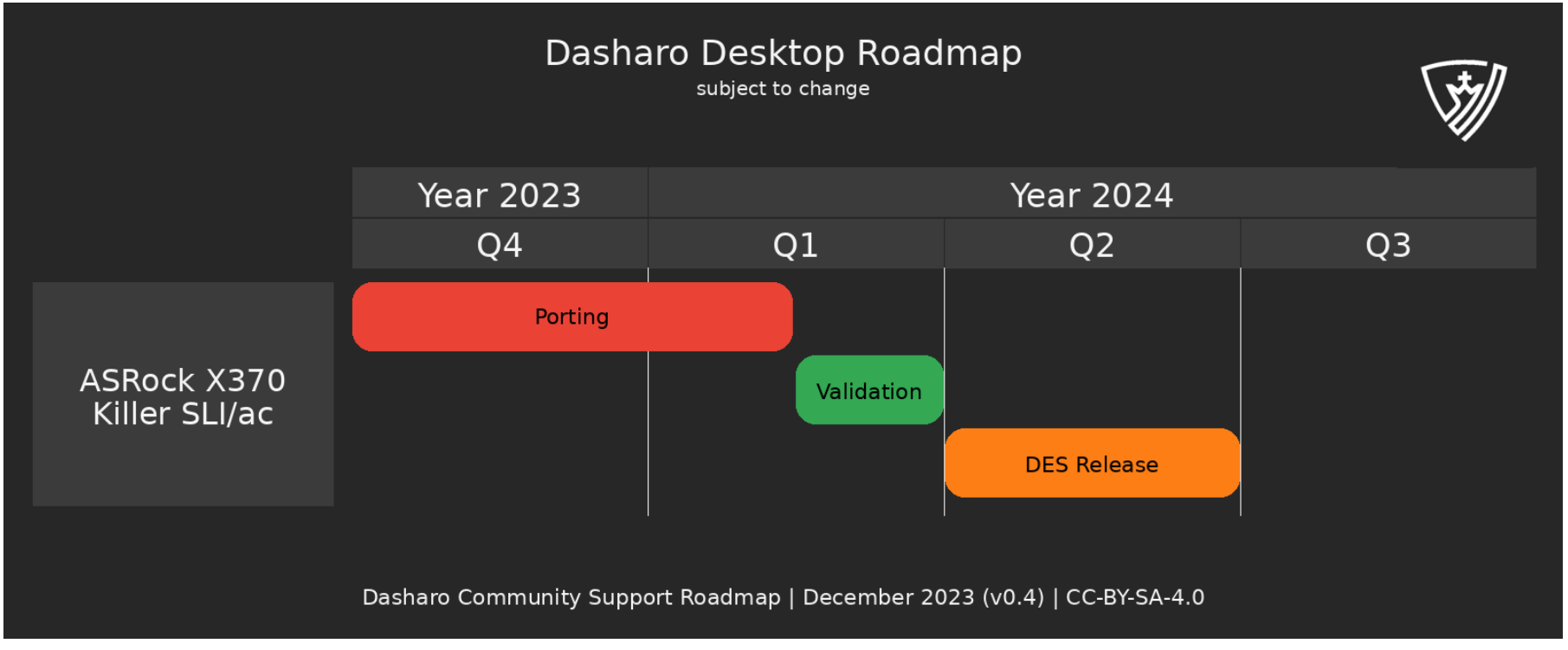
Community Release date changed because of PC Engines and NovaCustom.

Dasharo Desktop MSI Roadmap



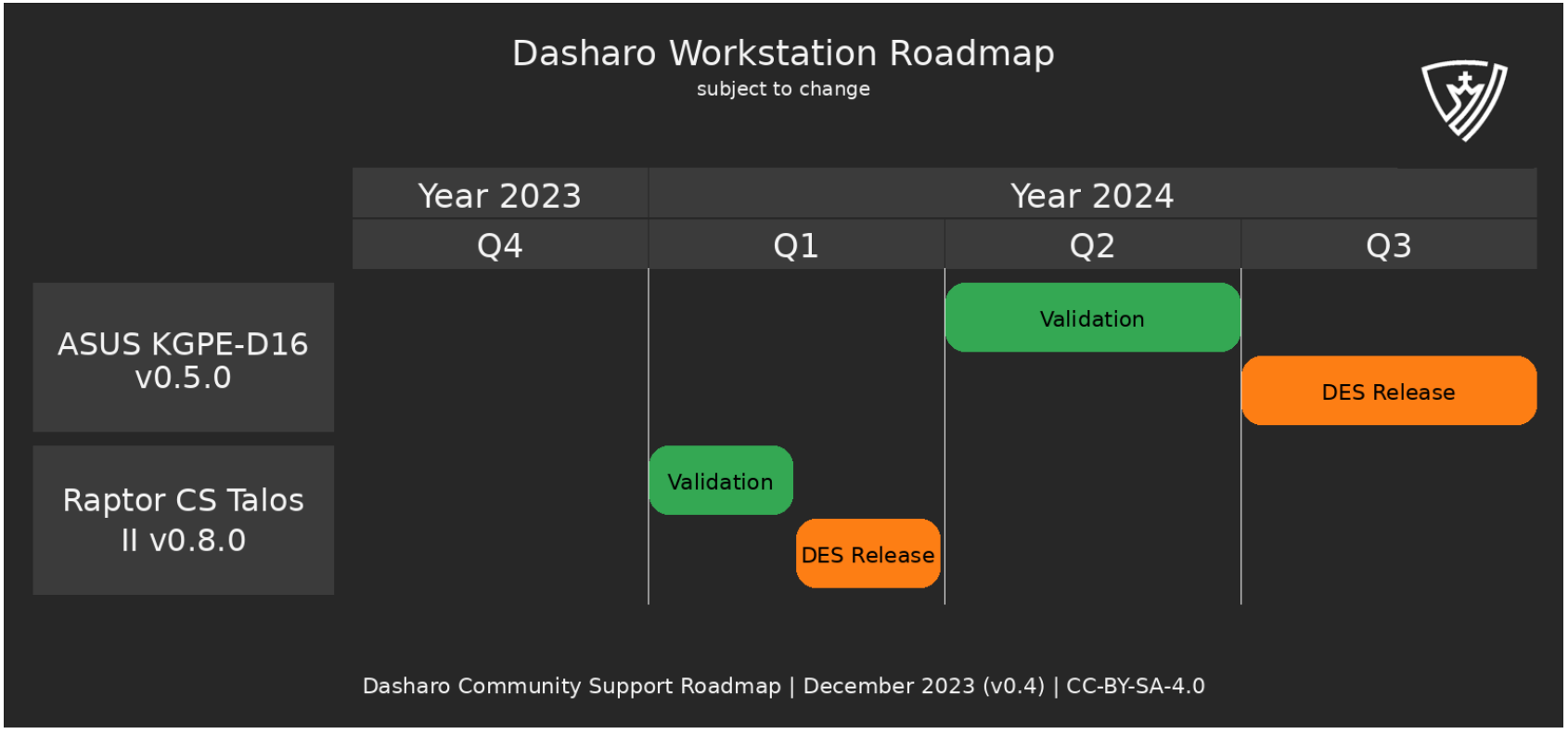
- We have to figure out better naming scheme.
- We plan to deliver this solution one quarter earlier.
- Status from call with ThePlexus.

Dasharo Desktop ASRock Roadmap



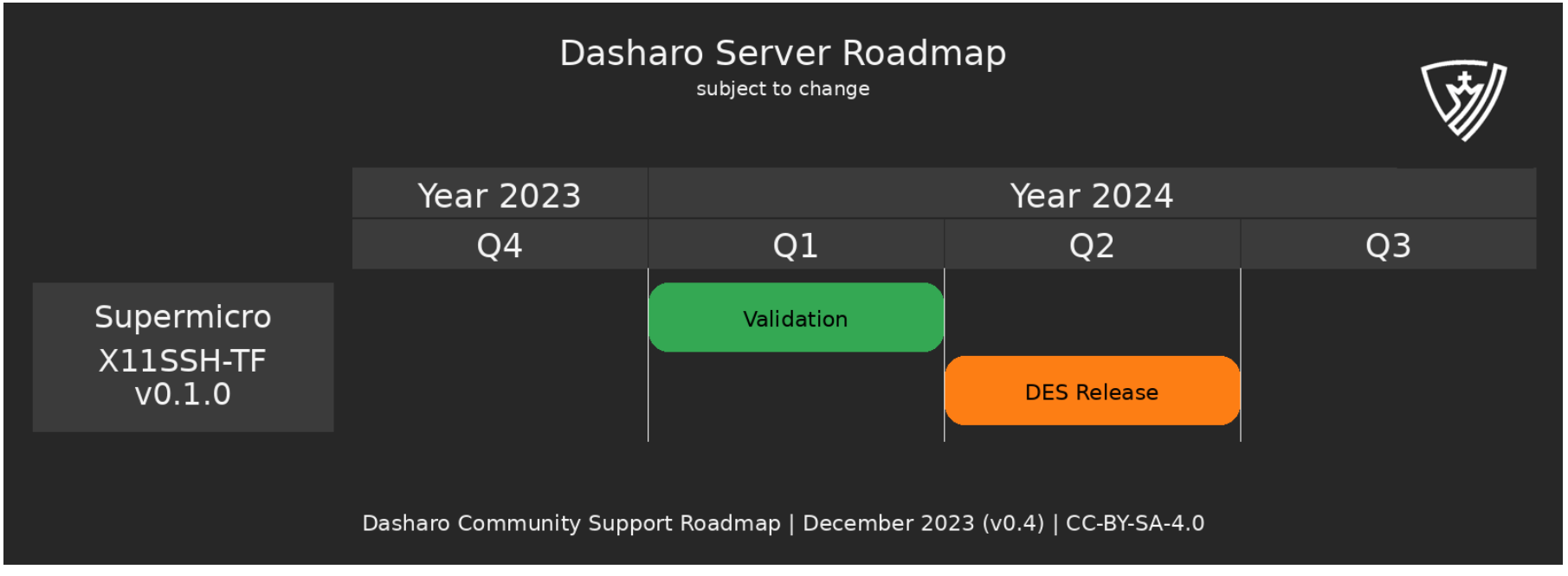
- Dasharo Supporting Partner discussion.
- Potential paths: AMD FSP or AGESA.

Dasharo Workstation Roadmap



- There is almost no hope for KGPE-D16
- New milestone for Dasharo(coreboot+Heads) v0.8.0 for Talos II

Dasharo Server Roadmap



- Low priority, but there is some market interest.

Q&A

CHANGELOG

Changelog DUG#1

- (NEW) QEMU Q35 v0.1.0 planned for Q3'23
- (NEW) Dell OptiPlex 7010/9010 v0.1.0 planned for Q2'23
- (NEW) Dell T1650 v0.1.0 planned for Q3'23
- (NEW) MSI Z690-A v1.1.2 planned for Q3'23
- (NEW) MSI Z690-A v1.2.0 planned for Q4'23
- (NEW) MSI Z790-A v1.0.0 planned for Q1'24
- (NEW) ASUS KGPE-D16 v0.5.0 planned for Q3'23
- (NEW) RCS Talos II v0.7.0 planned for Q3'23
- (NEW) Supermicro X11SSH-TF v0.1.0 planned for Q4'23
- Summary: 9 new

Changelog DUG#2

- (CHANGED) QEMU Q35 v0.1.0 planned for Q3'23
  - release date changed to Q4'23 (+1)
- (CHANGED) Dell OptiPlex 7010/9010 v0.1.0 planned for Q2'23
  - release date changed to Q4'23 (+2)
- (CHANGED) Dell T1650 v0.1.0 planned for Q3'23
  - release date changed to Q1'24 (+2)
- MSI Z690-A v1.1.2 planned for Q3'23
- (NEW) MSI Z690-A v1.1.3 release planned for Q4'23
- (CHANGED) MSI Z690-A v1.2.0 planned for Q4'23
  - release date changed to Q1'24 (+1)
- (NEW) MSI Z790-A v0.9.0 planned for Q3'23
- (NEW) MSI Z790-A v0.9.1 planned for Q4'23
- MSI Z790-A v1.0.0 planned for Q1'24
- (CHANGED) ASUS KGPE-D16 v0.5.0 planned for Q3'23
  - release date changed to Q1'24 (+2)

Changelog DUG#2

- RCS Talos II v0.7.0 planned for Q3'23
- (CHANGED) Supermicro X11SSH-TF v0.1.0 planned for Q4'23
    - release date changed to Q1'24 (+1)
- Summary: 3 new, 6 changed, 3 on track (total: 12)

Changelog DUG#3

- QEMU Q35 v0.1.0 planned for Q4'23
- (NEW) PC Engines apu3 v0.9.0 planned for Q4'23
- (NEW) Protectli VP4670 v0.9.0 planned for Q2'24
- (NEW) Novacustom NV4x Dasharo (coreboot+Heads) v0.9.0 planned for Q2'24
- (NEW) Lenovo M920Q v0.9.0 planned for Q2'24
- (CHANGED) Dell OptiPlex 7010/9010 v0.1.0 planned for Q4'23
    - release type changed to DES
- (CHANGED) Dell T1650 v0.1.0 planned for Q1'24
    - release type changed to DES
- (RELEASED) MSI Z690-A v1.1.2 planned for Q3'23
- MSI Z690-A v1.1.3 release planned for Q4'23
- MSI Z690-A v1.2.0 planned for Q1'24
- (RELEASED) MSI Z790-A v0.9.0 planned for Q3'23

Changelog DUG#3

- MSI Z790-A v0.9.1 planned for Q4'23
- MSI Z790-A v1.0.0 planned for Q1'24
- (NEW) MSI Z790-A Dasharo (coreboot+Heads) v1.0.1 planned for Q2'24
- (CHANGED) ASUS KGPE-D16 v0.5.0 planned for Q1'24
    - release type changed to DES
    - release date changed to Q2'24 (+1)
- (RELEASED) RCS Talos II v0.7.0 planned for Q3'23
- (CHANGED) Supermicro X11SSH-TF v0.1.0 planned for Q1'24
    - release date changed to Q2'24 (+1)
- Summary: 5 new, 4 changed, 5 on track, 3 released (total: 17)