CLAIMS:

1. A system comprising,

a data store comprising data describing a plurality of internet of things (IoT) devices and a corresponding plurality of firmware versions; and

at least one computing device in communication with the data store, the at least one computing device being configured to at least:

receive a request to change firmware of a particular IoT device of the plurality of IoT devices from a first version to a second version over a particular network, the first version being specified in a corresponding one of the plurality of firmware versions;

identify a particular IoT device family for the particular IoT device;

determine a firmware change profile corresponding to the particular IoT device family; and

initiate changing a firmware image of the particular IoT device to the second version over the network based on the firmware change profile.

2. The system of claim 1, wherein the at least one computing device is further configured to:

subsequent to changing the firmware image, interrogate the particular IoT device over the network according to an interrogation profile corresponding to the particular IoT device family to determine a current firmware version;

in response to the current firmware version matching the second version, update the corresponding one of the plurality of firmware versions.

3. The system of claim 1, wherein the at least one computing device is further configured to:

perform an interrogation the particular IoT device over the network according to an interrogation profile; and

determine that the first version of the firmware is currently installed based at least in part on a formatting of responses to the interrogation.

4. The system of claim 1, wherein the at least one computing device is further configured to:

generate a signature of firmware image; and

verify the signature against the data describing the plurality of IoT devices and the corresponding plurality of firmware versions.

5. The system of claim 1, wherein the request is received via at least one of: a web page or a scheduled process.

6. The system of claim 1, wherein the at least one computing device is further configured to:

determine an upgrade path for the particular IoT device based on the first version, the second version, and the firmware change profile; and

prior to initiate changing of the firmware image to the second version, initiate changing the
firmware image of the particular IoT device to at least one intermediary version based on the upgrade path.

7. The system of claim 1, wherein the firmware image is stored in a blockchain ledger store and the at least one computing device is further configured to verify a hash associated with the firmware image in the blockchain ledger store prior to initiating changing of the firmware image.

8. A method comprising,

receiving, via at least one computing device, a request to change firmware of a particular IoT device of a plurality of IoT devices from a first version to a second version over a particular network, the first version being specified in a corresponding one of a plurality of firmware versions;

identifying, via the at least one computing device, a particular IoT device family for the particular IoT device;

determining, via the at least one computing device, a firmware change profile corresponding to the particular IoT device family; and

initiating, via the at least one computing device, changing a firmware image of the particular IoT device to the second version over the network based on the firmware change profile.

9. The method of claim 8, further comprising:

interrogating, via the at least one computing device, the particular IoT device over the network according to an interrogation profile corresponding to the particular IoT device family to determine a current firmware version;

in response to the current firmware version matching the second version, updating, via the at least one computing device, a corresponding firmware version for the particular IoT device in a data store.

10. The method of claim 8, wherein the request is received via at least one of: a web page or a scheduled process.

11. The method of claim 8, further comprising:

determining, via the at least one computing device, an upgrade path for the particular IoT device based on the first version, the second version, and the firmware change profile; and

initiating, via the at least one computing device, changing the firmware image of the particular IoT device to at least one intermediary version based on the upgrade path.

12. The method of claim 8, further comprising:

performing, via the at least one computing device, an interrogation the particular IoT device over the network according to an interrogation profile; and

determining, via the at least one computing device, that the first version of the firmware is currently installed based at least in part on features available on the particular IoT device.

13. The method of claim 8, wherein the firmware image is stored in a blockchain ledger store and the at least one computing device is further configured to verify a hash associated with the firmware image in the blockchain ledger store prior to initiating changing of the firmware image.

14. A non-transitory computer-readable medium embodying a program that, when executed by at least one computing device, causes the at least one computing device to at least:

receive a request to change firmware of a particular IoT device of a plurality of IoT devices from a first version over a particular network, the first version being specified in a

corresponding one of a plurality of firmware versions;

identify a particular IoT device family for the particular IoT device;

determine a firmware change profile corresponding to the particular IoT device family; and

initiate changing a firmware image of the particular IoT device to a second version over the network based on the firmware change profile.

15. The non-transitory computer-readable medium of claim 14, wherein the at least one computing device is further configured to:

apply a policy to the particular IoT device in response to the request to change firmware; and

identify the second version for installation according to the policy.

16. The non-transitory computer-readable medium of claim 14, wherein the at least one computing device is further configured to:

subsequent to changing the firmware image, interrogate the particular IoT device over the network according to an interrogation profile corresponding to the particular IoT device family to determine a current firmware version;

in response to the current firmware version matching the second version, update the a corresponding version for the particular IoT device in a data store.

17. The non-transitory computer-readable medium of claim 14, wherein the request is received via at least one of: a web page or a scheduled process.

18. The non-transitory computer-readable medium of claim 14, wherein the program further causes the at least one computing device to:

determine an upgrade path for the particular IoT device based on the first version, the second version, and the firmware change profile; and

prior to initiate changing of the firmware image the second version, initiate changing the firmware image of the particular IoT device to at least one intermediary version based on the upgrade path.

19. The non-transitory computer-readable medium of claim 14, wherein the firmware image is stored in a blockchain ledger store and the program further causes the at least one computing device to verify a hash associated with the firmware image in the blockchain ledger store prior to initiating changing of the firmware image.

20. The non-transitory computer-readable medium of claim 14, wherein the program further causes the at least one computing device to:

perform an interrogation the particular IoT device over the network according to an interrogation profile; and

determine that an expected version of firmware is not currently installed based at least in part on the interrogation.