Independent Claim 10 (Article of Manufacture – Firmware for IoT OTP Random Sequence)
A non-transitory computer-readable medium embodied in IoT edge hardware firmware that causes sensors, routers, and gateways to: continuously sample fluctuating physical measurements to produce a non-repeating random number sequence; transmit the sequence securely for use as one-time pad material; and participate in registration on a timestamp-based non-repeatable DLT for OTP encryption of tokenized digital twins or representations of any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset (RWA).

Dependent Claims for Independent Claim 10
The following is a complete set of dependent claims (Claims 2–22) that further specify and narrow the non-transitory computer-readable medium of Independent Claim 10. Each dependent claim is fully supported by the disclosures in the attached document (Patent Filing Highlights US20210019429A1.docx), including the detailed descriptions of IoT edge hardware firmware for sensors, routers, and gateways; real-time/continuous measurement of data associated with any physical asset or RWA; encryption and transmission to the IoT cloud platform; supply of unique device identifiers and measurement provenance; wireless protocols; tamper-proof registration; OTP encryption using non-repeating random number sequences; timestamp-based ledger integration; and the enablement of verifiable value token minting as tokenized digital twins as of the January 15, 2018 priority date.

Full Claim Set in Formal USPTO-Style Format (Reordered to Start with Claim 1)

1. A non-transitory computer-readable medium embodied in IoT edge hardware firmware that causes sensors, routers, and gateways to: measure data associated with any physical asset or RWA; encrypt and transmit the data to an IoT cloud platform; and supply unique device identifiers and measurement provenance to enable minting of verifiable value tokens representing tokenized digital twins.
2. The non-transitory computer-readable medium of claim 1, wherein the firmware causes the sensors, routers, and gateways to communicate using one or more wireless protocols selected from the group consisting of Bluetooth, Zigbee, WiFi, Z-Wave, Sub-Gigahertz, Cellular, Satellite, LoRaWAN, Sigfox, and combinations thereof.
3. The non-transitory computer-readable medium of claim 1, wherein the firmware causes continuous or real-time measurement of data associated with any physical asset or RWA from physical facilities, infrastructure, renewable resources, or efficiency systems.
4. The non-transitory computer-readable medium of claim 1, wherein the firmware causes encryption of the measured data using one-time pad encryption with a unique segment of a live non-repeating random number sequence generated from IoT sensor measurements.
5. The non-transitory computer-readable medium of claim 1, wherein the firmware causes transmission of the measured data and unique device identifiers to the IoT cloud platform in real time or near real time.
6. The non-transitory computer-readable medium of claim 1, wherein the firmware causes supply of unique device identifiers that are cryptographically bound to the measured data to establish tamper-proof provenance for the tokenized digital twin.

7. The non-transitory computer-readable medium of claim 1, wherein the firmware causes the sensors, routers, and gateways to register their unique identifiers on the blockchain ledger prior to or in conjunction with data transmission to enable verifiable minting of the value token.
8. The non-transitory computer-readable medium of claim 1, wherein the firmware causes the measured data and unique device identifiers to be formatted such that the IoT cloud platform can automatically validate the data and generate a digital RWA certificate for minting the value token.
9. The non-transitory computer-readable medium of claim 1, wherein the firmware causes the IoT edge hardware to operate with battery backup and low-power modes while maintaining continuous measurement, encryption, and provenance supply capabilities.
10. The non-transitory computer-readable medium of claim 1, wherein the firmware causes the sensors, routers, and gateways to supply measurement provenance that includes timestamps, transaction data, or validation metadata to support immutable recording on the blockchain ledger.
11. The non-transitory computer-readable medium of claim 1, wherein the firmware causes the value token minted from the supplied data and identifiers to represent an immutable digital twin of any commodity, security, physical asset, financial instrument, or other verifiable Real World Asset.
12. The non-transitory computer-readable medium of claim 1, wherein the firmware enables the IoT edge hardware to integrate with a blockchain trading platform for subsequent listing and trading of the tokenized digital twin.
13. The non-transitory computer-readable medium of claim 1, wherein the firmware causes the measured data to be processed locally on the edge hardware prior to encryption and transmission to reduce bandwidth requirements and enable real-time exception-based reporting.
14. The non-transitory computer-readable medium of claim 1, wherein the firmware causes the unique device identifiers and measurement provenance to be cryptographically signed to prevent tampering and ensure authentic physical asset origin for the minted value token.
15. The non-transitory computer-readable medium of claim 1, wherein the firmware supports execution within a Trusted Execution Environment (TEE) on the IoT edge hardware for secure measurement, encryption, and provenance supply.
16. The non-transitory computer-readable medium of claim 1, wherein the firmware causes the IoT edge hardware to maintain multiple redundant communication paths for reliable transmission of measured data, unique device identifiers, and measurement provenance to the IoT cloud platform.
17. The non-transitory computer-readable medium of claim 1, wherein the firmware enables scalable, industrial-scale operation by allowing simultaneous measurement and provenance supply from multiple sensors, routers, and gateways for a single physical asset or RWA.
18. The non-transitory computer-readable medium of claim 1, wherein the firmware causes the supplied data and identifiers to support primary-market minting of the value token as an immutable digital twin on the blockchain ledger.

19. The non-transitory computer-readable medium of claim 1, wherein the firmware causes the IoT edge hardware to supply provenance information that is directly incorporated into the immutable digital asset record created during value token minting.
20. The non-transitory computer-readable medium of claim 1, wherein the firmware operates in a closed-loop automated process from measurement and encryption through transmission and provenance supply to enable end-to-end tokenized digital twin creation.
21. The non-transitory computer-readable medium of claim 1, wherein the firmware causes the sensors, routers, and gateways to support bidirectional communication for receiving commands or updates from the IoT cloud platform or blockchain ledger while maintaining secure measurement and provenance supply.
22. The non-transitory computer-readable medium of claim 1, wherein the firmware eliminates intermediaries by enabling direct, cryptographically verifiable contribution of measured data and unique device identifiers from the IoT edge hardware to the minting of tokenized digital twins on the blockchain.

These claims form a self-contained, commercially robust claim family that directly maps to the article-of-manufacture embodiments of the IoT edge hardware firmware for enabling measurement, encryption, transmission, unique device identification, and provenance supply to support minting of verifiable tokenized digital twins of any physical asset or RWA as described in the January 15, 2018 provisional disclosure. The full set (renumbered to begin with Claim 1) can be incorporated into a non-provisional, continuation, or continuation-in-part application (alone or in combination with the claim families of Independent Claims 1–9) to further strengthen the Parisii patent portfolio for quantum-tolerant Web4 W4S security, tokenized Real World Assets, and blockchain-based RWA/digital twin infrastructure.