Independent Claim 7 (Method – IoT Device Registration and Tamper-Proof RWA Provenance)
A computer-implemented method for creating tamper-proof tokenized digital twins of any physical asset or RWA on blockchain, comprising: registering unique identifiers for IoT sensors, routers, and gateways on a blockchain ledger; collecting RWA data from the registered devices; validating the data and generating a certified digital twin certificate; and minting a value token that cryptographically incorporates the device identifiers and validation metadata to prove authentic physical asset origin.

Dependent Claims for Independent Claim 7
The following is a complete set of dependent claims (Claims 2–22) that further specify and narrow the computer-implemented method of Independent Claim 7. Each dependent claim is fully supported by the disclosures in the attached document (Patent Filing Highlights US20220180374A1.pdf), including the detailed descriptions of IoT device registration on the blockchain ledger, real-time data collection from registered sensors/routers/gateways, automated validation/certification processes, certified digital twin certificate generation, value token minting that cryptographically incorporates device identifiers and validation metadata, tamper-proof provenance, primary-market issuance, cryptographic hashing/linking, redundant ledger copies, closed-loop automation, and the overall IoT-sourced tokenized digital twin architecture for any physical asset or RWA as of the December 26, 2017 priority date.

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

1. A computer-implemented method for creating tamper-proof tokenized digital twins of any physical asset or RWA on blockchain, comprising: registering unique identifiers for IoT sensors, routers, and gateways on a blockchain ledger; collecting RWA data from the registered devices; validating the data and generating a certified digital twin certificate; and minting a value token that cryptographically incorporates the device identifiers and validation metadata to prove authentic physical asset origin.
2. The method of claim 1, wherein registering unique identifiers further comprises registering IoT sensors, edge routers, and edge gateways configured 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 method of claim 1, wherein collecting RWA data from the registered devices is performed continuously or in real time from physical facilities, infrastructure, renewable resources, or efficiency systems instrumented with the registered IoT devices.
4. The method of claim 1, wherein collecting RWA data from the registered devices further comprises transmitting the data in real time or near real time to an IoT cloud platform.
5. The method of claim 1, wherein validating the data comprises performing automated processes for accuracy, sampling design, internal controls, and verification consistent with established standards for real-world asset certification.
6. The method of claim 1, wherein generating the certified digital twin certificate is performed automatically by the IoT cloud platform upon successful validation of the data collected from the registered devices.

7. The method of claim 1, wherein minting the value token further comprises creating the value token as a primary market activity based on the certified digital twin certificate generated from the IoT-sourced data collected from the registered devices.
8. The method of claim 1, wherein minting the value token further comprises recording the certified digital twin certificate as an immutable digital asset on the blockchain ledger that includes one or more of public-key addresses, cryptographic block linking, timestamps, transaction data, user identifiers, equipment identifiers, validation reports, and verification statements.
9. The method of claim 1, wherein the cryptographic incorporation of device identifiers and validation metadata creates a tamper-proof linkage that proves the authentic physical asset origin of the digital twin.
10. The method of claim 1, wherein the blockchain ledger maintains multiple redundant copies across cloud environments to provide fault tolerance and Byzantine fault tolerance for the minted value token and associated metadata.
11. The method of claim 1, wherein the immutable record employs cryptographic hashing of each new block to prior blocks to ensure permanent verifiability of ownership, provenance, and tamper-proof status of the tokenized digital twin.
12. The method of claim 1, wherein the method provides permanent auditability and fraud reduction through the immutable record of the entire registration, data collection, validation, certificate generation, and minting process on the blockchain ledger.
13. The method of claim 1, further comprising integrating the minted value token with a blockchain-based trading platform that enables subsequent listing and trading of the tamper-proof tokenized digital twin on a commodity, crypto, security, or financial exchange.
14. The method of claim 1, wherein the method operates in a closed-loop automated process from device registration and data collection through validation, certificate generation, and automatic minting of the tamper-proof value token representing the digital twin.
15. The method of claim 1, wherein the value token represents an immutable digital twin of any commodity, security, physical asset, financial instrument, or other RWA that is verifiable and cannot be double-spent due to the cryptographic incorporation of device identifiers and validation metadata on the distributed ledger.
16. The method of claim 1, wherein the method eliminates intermediaries by performing end-to-end automated creation of the tamper-proof tokenized digital twin directly from registered IoT device data to the blockchain ledger.
17. The method of claim 1, wherein registering unique identifiers for IoT sensors, routers, and gateways further comprises a secure registration process that cryptographically links the device identifiers to the certified digital twin certificate and the minted value token on the distributed ledger.
18. The method of claim 1, wherein the blockchain ledger records the minted value token with timestamps and transaction data to ensure real-time or near real-time provenance tracking and tamper-proof verification of the digital twin.
19. The method of claim 1, wherein the method supports scalable, industrial-scale creation of tamper-proof tokenized digital twins by combining real-time IoT data acquisition from

registered devices with automated blockchain minting that incorporates device identifiers and validation metadata.

20. The method of claim 1, further comprising automated preparation for monetization by associating the minted tamper-proof value token with mechanisms for ownership transfer and payment upon future trading execution on an integrated blockchain-based exchange.
21. The method of claim 1, wherein the certified digital twin certificate and the value token are cryptographically bound with device identifiers such that any participant in the network can permanently verify authentic physical asset origin and tamper-proof status without reliance on off-chain records.
22. The method of claim 1, wherein the method further comprises executing wallet or payment applications within a Trusted Execution Environment (TEE) in connection with the registration of IoT devices and the automatic minting of the tamper-proof value token representing the digital twin on the blockchain ledger.

These claims form a self-contained, commercially robust claim family that directly maps to the computer-implemented method for creating tamper-proof tokenized digital twins of any physical asset or RWA on blockchain, including unique device registration, IoT data collection from registered devices, validation, certificate generation, and cryptographic minting with device identifiers and validation metadata as described in the December 26, 2017 provisional disclosure (and the incorporated earlier provisionals). 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 1–6) to further strengthen the Parisii patent portfolio for tokenized Real World Assets and blockchain-based RWA/digital twin infrastructure.