

### **Independent Claim 2 (Method Claim – Token Creation)**

A computer-implemented method for creating a value token representing a verified Real World Asset (RWA), the method comprising:

collecting data associated with any commodity, security, physical asset, financial instrument, or other RWA using IoT sensors, edge routers, and gateways;  
sending the data to an IoT cloud platform;  
validating the data and generating a digital RWA certificate; and  
recording the certificate as a value token on a blockchain ledger, with the token linked to a public-key address and protected by cryptographic blocks to ensure it is verifiable and cannot be double-spent.

### **Dependent Claims for Independent Claim 2**

The following is a complete set of dependent claims (Claims 2–20) that further specify and narrow the computer-implemented method of Independent Claim 2. Each dependent claim is fully supported by the disclosures in the attached document (Patent Filing Highlights US20200027096A1.docx), including the detailed descriptions of IoT data collection via sensor devices, edge routers, and gateways; real-time/continuous transmission to the IoT cloud platform; automated validation and verification processes; digital RWA certificate generation; blockchain token recording with public-key linking and cryptographic protection; user/equipment registration to prevent double-spending; primary-market issuance; immutable ledger recording for verification and auditability; and the overall IoT-to-blockchain tokenized RWA creation architecture as of the November 7, 2017 priority date.

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

1. A computer-implemented method for creating a value token representing a verified Real World Asset (RWA), the method comprising: collecting data associated with any commodity, security, physical asset, financial instrument, or other RWA using IoT sensors, edge routers, and gateways; sending the data to an IoT cloud platform; validating the data and generating a digital RWA certificate; and recording the certificate as a value token on a blockchain ledger, with the token linked to a public-key address and protected by cryptographic blocks to ensure it is verifiable and cannot be double-spent.
2. The method of claim 1, wherein collecting the data further comprises using an IoT edge hardware layout with sensor devices, 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 the data is performed continuously or in real time from physical facilities or infrastructure instrumented with the IoT sensors, edge routers, and gateways.
4. The method of claim 1, wherein sending the data to the IoT cloud platform comprises transmitting the measured data in real time or near real time for automated processing.

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 digital RWA certificate is performed automatically by the IoT cloud platform upon successful validation of the received data.
7. The method of claim 1, wherein recording the certificate as a value token further comprises creating an immutable digital asset record 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.
8. The method of claim 1, wherein the blockchain ledger registers all participants and equipment associated with the RWA to prevent double-spending or fraud in the tokenized asset.
9. The method of claim 1, wherein the value token is created and recorded as a primary market activity based on the validated digital RWA certificate generated from the IoT-sourced data.
10. The method of claim 1, wherein the cryptographic blocks protecting the value token employ cryptographic hashing of each new block to prior blocks to ensure immutability and permanent verifiability of the tokenized RWA.
11. The method of claim 1, wherein the method further comprises a secure registration process that cryptographically binds the IoT sensors, edge routers, gateways, the digital RWA certificate, and the value token on the distributed ledger.
12. The method of claim 1, wherein the value token represents a digital representation of any commodity, security, physical asset, financial instrument, or other RWA that is verifiable and cannot be double-spent due to the immutable nature of the blockchain ledger.
13. 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 value token record.
14. The method of claim 1, further comprising integrating the created value token with a blockchain-based trading platform that enables subsequent trading of the tokenized RWA on a commodity, crypto, security, or financial exchange.
15. The method of claim 1, wherein the method eliminates intermediaries by performing end-to-end automated data collection, validation, certificate generation, and token creation directly from IoT-sourced data to the blockchain ledger.
16. The method of claim 1, wherein the IoT cloud platform and blockchain ledger operate in a closed-loop automated process to enable continuous measurement, validation, and minting of the value token representing the verified RWA.
17. The method of claim 1, wherein recording the certificate as a value token further includes automated monetization preparation by associating the token with mechanisms for ownership transfer and payment upon future trading execution.
18. The method of claim 1, wherein the method provides permanent auditability of the tokenized RWA through immutable recording of all validation data, certificate generation steps, and token creation on the blockchain ledger.

19. The method of claim 1, wherein the value token is protected against double-spending through cryptographic linkage to the public-key address and registration of associated IoT equipment and users on the distributed ledger.
20. The method of claim 1, wherein the method supports scalable, fraud-resistant creation of tokenized RWAs at industrial scale by combining real-time IoT data acquisition with blockchain-native token minting.

These claims form a self-contained, commercially robust claim family that directly maps to the computer-implemented method for IoT-driven RWA data collection, cloud validation, digital certificate generation, and blockchain value token creation described in the November 7, 2017 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 Claim 1 and subsequent claims) to further strengthen the Parisii patent portfolio for tokenized Real World Assets and blockchain-based RWA infrastructure.