Independent Claim 2 (Method – Issuance of OTP-Secured RWA Digital Twin Token)
A computer-implemented method for issuing a tokenized digital twin or representation of any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset (RWA) on a non-repeatable digital ledger, comprising: collecting real-time data via IoT sensors to produce a continuous non-repeating random number sequence; encrypting the asset data or RWA certificate using a unique segment of the sequence as a one-time pad key; minting a value token on a timestamp-based distributed ledger by recording the OTP-encrypted digital twin or representation with its encryption-start timestamp; returning the exact one-time pad key segment securely to the owner while destroying it server-side; and registering the token for subsequent transfers or redemptions using only the owner-provided key and timestamp.

Dependent Claims for Independent Claim 2
The following is a complete set of dependent claims (Claims 2–22) 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 US20210019429A1.docx), including the detailed descriptions of IoT edge hardware generating a continuous live non-repeating random number sequence from physical measurements, real-time data collection and transmission, automated validation/certification, OTP encryption using unique segments of the non-repeating sequence, timestamp-based distributed ledger recording, secure key delivery with server-side destruction, device/user registration, primary-market issuance, quantum-resistant perfect secrecy, and applicability to any tokenized RWA/digital twin or physical/commodity asset as of the January 15, 2018 priority date.

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

1. A computer-implemented method for issuing a tokenized digital twin or representation of any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset (RWA) on a non-repeatable digital ledger, comprising: collecting real-time data via IoT sensors to produce a continuous non-repeating random number sequence; encrypting the asset data or RWA certificate using a unique segment of the sequence as a one-time pad key; minting a value token on a timestamp-based distributed ledger by recording the OTP-encrypted digital twin or representation with its encryption-start timestamp; returning the exact one-time pad key segment securely to the owner while destroying it server-side; and registering the token for subsequent transfers or redemptions using only the owner-provided key and timestamp.
2. The method of claim 1, wherein collecting real-time 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 real-time data is performed continuously from physical facilities, infrastructure, renewable resources, or efficiency systems instrumented with the IoT sensors.
4. The method of claim 1, wherein the continuous non-repeating random number sequence is generated from fluctuating physical measurements including voltage fluctuations from solar panels or electrical grids, electromagnetic fields, thermal events, or barometric pressure.
5. The method of claim 1, wherein encrypting the asset data or RWA certificate further comprises normalizing the non-repeating random number sequence to a system clock at microsecond or finer granularity so that each encryption uses a unique timestamp-aligned one-time pad segment.

6. The method of claim 1, wherein minting the value token further comprises creating the value token as a primary market activity based on the validated digital RWA certificate generated from the IoT-sourced data.
7. The method of claim 1, wherein minting the value token further comprises recording the OTP-encrypted digital twin or representation as an immutable digital asset on the timestamp-based distributed ledger that includes one or more of public-key addresses, cryptographic block linking (where applicable), timestamps, transaction data, user identifiers, equipment identifiers, validation reports, and verification statements.
8. The method of claim 1, wherein registering the token further comprises registering unique identifiers for IoT sensors, routers, and gateways on the distributed ledger to cryptographically bind device provenance to the tokenized digital twin or representation.
9. The method of claim 1, wherein returning the exact one-time pad key segment securely to the owner comprises one or more of digital channels, physical media, or split-key distribution mechanisms, with immediate server-side destruction of the used key segment.
10. The method of claim 1, wherein the method provides information-theoretic perfect secrecy and quantum-resistant security for the tokenized digital twin or representation through the one-time pad encryption and non-repeatable ledger architecture.
11. The method of claim 1, further comprising integrating the minted value token with a trading platform that enables secure transfer, swapping, or exchange of the OTP-secured token while maintaining perfect secrecy.
12. The method of claim 1, wherein the timestamp-based distributed ledger records each OTP-encrypted digital twin or representation identified exclusively by its encryption-start timestamp without traditional hash-chain linking between records.
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 minted value token.
14. The method of claim 1, wherein the method operates in real time or near real time to enable continuous measurement, OTP encryption, ledger recording, and registration of the tokenized digital twin or representation.
15. The method of claim 1, wherein the value token represents an immutable digital twin or representation of any commodity, security, physical asset, financial instrument, or other verifiable Real World Asset that is verifiable and cannot be double-spent due to the one-time pad encryption and non-repeatable ledger architecture.
16. The method of claim 1, wherein the method eliminates intermediaries by performing end-to-end automated issuance of the tokenized digital twin or representation directly from IoT-sourced data to the non-repeatable digital ledger.
17. The method of claim 1, wherein the non-repeating random number sequence is generated from IoT sensor measurements in a manner that is non-reproducible with earth-bound technology.
18. The method of claim 1, further comprising automated preparation for monetization by associating the minted value token with mechanisms for ownership transfer and payment upon future trading execution on an integrated trading platform.
19. The method of claim 1, wherein the method supports scalable, industrial-scale issuance of tokenized digital twins or representations of any physical asset or commodity by combining real-time IoT data acquisition with automated OTP encryption and timestamp-based ledger minting.
20. The method of claim 1, wherein registering the token for subsequent transfers or redemptions further comprises enabling owner-initiated transfer or redemption solely by presentation of the matching timestamp and one-time pad key segment.

21. 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 issuance and registration of the tokenized digital twin or representation.
22. The method of claim 1, wherein the method provides Encryption as a Service for any RWA data or value token, enabling real-time OTP encryption, timestamp-based ledger storage, and secure key delivery for subsequent transfers or redemptions of the tokenized digital twin or representation.

These claims form a self-contained, commercially robust claim family that directly maps to the computer-implemented method for issuing a tokenized digital twin or representation of any physical asset, commodity, or verifiable Real World Asset (RWA) on a non-repeatable digital ledger using IoT-generated OTP encryption, timestamp-based recording, secure key delivery with server-side destruction, and device/user registration 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 and subsequent claims) to further strengthen the Parisii patent portfolio for quantum-tolerant Web4 W4S security, tokenized Real World Assets, and blockchain-based RWA/digital twin infrastructure.