Independent Claim 7 (Method – Timestamp-Based Non-Repeatable Ledger)
A computer-implemented method for operating a non-repeatable digital ledger technology for any tokenized asset, comprising: synchronizing a live IoT-generated non-repeating random number sequence to a system clock at microsecond or finer granularity; encrypting each RWA token or digital twin or representation of any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset using a unique timestamp-aligned one-time pad segment; writing the ciphertext to the ledger identified exclusively by the encryption-start timestamp; destroying the used key segment immediately after commit; and permitting owner retrieval or transfer only upon presentation of the matching timestamp and key.

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 US20210019429A1.docx), including the detailed descriptions of synchronizing the live IoT-generated non-repeating random number sequence to a system clock, timestamp-aligned one-time pad segments, writing ciphertext to the ledger identified exclusively by encryption-start timestamp, immediate server-side key destruction, owner retrieval/transfer only upon presentation of matching timestamp and key, quantum-resistant perfect secrecy, device/user registration, primary-market issuance, and the overall non-repeatable DLT architecture 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 operating a non-repeatable digital ledger technology for any tokenized asset, comprising: synchronizing a live IoT-generated non-repeating random number sequence to a system clock at microsecond or finer granularity; encrypting each RWA token or digital twin or representation of any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset (RWA) using a unique timestamp-aligned one-time pad segment; writing the ciphertext to the ledger identified exclusively by the encryption-start timestamp; destroying the used key segment immediately after commit; and permitting owner retrieval or transfer only upon presentation of the matching timestamp and key.
2. The method of claim 1, wherein synchronizing the live IoT-generated non-repeating random number sequence further comprises generating the sequence from fluctuating physical measurements of IoT sensors, edge routers, and edge gateways including voltage fluctuations from solar panels or electrical grids, electromagnetic fields, thermal events, or barometric pressure.
3. The method of claim 1, wherein synchronizing the live IoT-generated non-repeating random number sequence further comprises normalizing the sequence to a system clock at microsecond or finer granularity so that each encryption uses a unique timestamp-aligned one-time pad segment.
4. The method of claim 1, wherein encrypting each RWA token or digital twin or representation further comprises receiving the token record from an IoT edge hardware layout comprising 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.

5. The method of claim 1, wherein writing the ciphertext to the ledger further comprises recording the OTP-encrypted digital twin or representation identified exclusively by its encryption-start timestamp without traditional hash-chain linking between records.
6. The method of claim 1, wherein destroying the used key segment immediately after commit occurs server-side immediately after the ciphertext is written to the timestamp-based distributed ledger.
7. The method of claim 1, wherein permitting owner retrieval or transfer further comprises decrypting the ciphertext using the owner-provided matching timestamp and one-time pad key segment and updating the ledger to reflect new ownership or redemption.
8. 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.
9. The method of claim 1, further comprising 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.
10. The method of claim 1, wherein the timestamp-based distributed ledger maintains multiple redundant copies across cloud environments to provide fault tolerance and Byzantine fault tolerance.
11. The method of claim 1, further comprising integrating the method with a trading platform that enables secure transfer, swapping, or exchange of the OTP-secured tokenized digital twin or representation while maintaining perfect secrecy.
12. The method of claim 1, wherein the trading platform supports market orders, limit orders, options, forwards, futures, swaps, or pre-market contracts.
13. The method of claim 1, wherein the trading platform further supports advanced order types selected from the group consisting of short selling, trailing stop orders, conditional orders, One-Triggers-the-Other (OTO) orders, One-Cancels-the-Other (OCO) orders, One-Triggers-a-One-Cancels-the-Other (OTOCO) orders, and combinations thereof.
14. The method of claim 1, wherein the trading platform applies time-in-force rules to orders, the time-in-force rules selected from the group consisting of day orders, good-’til-canceled orders (up to 180 days), fill-or-kill orders, immediate-or-cancel orders, on-the-open orders, on-the-close orders, and combinations thereof.
15. The method of claim 1, wherein the method operates in real time or near real time to enable continuous synchronization of the non-repeating random number sequence, OTP encryption, ledger recording, and owner-initiated retrieval or transfer.
16. The method of claim 1, wherein the value token or digital twin represents an immutable 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.
17. The method of claim 1, wherein the method eliminates intermediaries by performing end-to-end operation of the non-repeatable digital ledger technology directly from IoT-

sourced data to timestamp-based recording and authorized-key-holder retrieval or transfer.

18. 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.
19. The method of claim 1, further comprising automated preparation for monetization by associating the OTP-secured tokenized digital twin or representation with mechanisms for ownership transfer and payment upon future trading execution.
20. The method of claim 1, wherein the method supports scalable, industrial-scale operation of a non-repeatable digital ledger technology for tokenized digital twins or representations of any physical asset or commodity.
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 decryption and ledger update during owner-initiated retrieval or transfer.
22. The method of claim 1, wherein the method provides Encryption as a Service for any RWA data or value token, enabling real-time synchronization of the non-repeating random number sequence, timestamp-aligned OTP encryption, ledger storage identified by encryption-start timestamp, and secure owner-initiated retrieval or transfer.

These claims form a self-contained, commercially robust claim family that directly maps to the computer-implemented method for operating a non-repeatable digital ledger technology for any tokenized asset using live IoT-generated non-repeating random number sequence synchronization to a system clock, timestamp-aligned one-time pad encryption, timestamp-based ledger recording, immediate key destruction, and owner retrieval/transfer by matching timestamp and key 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 1–6) to further strengthen the Parisii patent portfolio for quantum-tolerant Web4 W4S security, tokenized Real World Assets, and blockchain-based RWA/digital twin infrastructure.