Independent Claim 6 (System – IoT Random Stream as OTP Source for DLT)
A system for generating a quantum-resistant non-repeatable digital ledger for tokenized assets, comprising: IoT sensor devices that produce a continuous, non-repeating random number sequence from fluctuating physical measurements; a repository that normalizes the sequence to precise time intervals; an encryption service that allocates unique one-time pad segments from the sequence to encrypt any RWA data or digital twin or representation of any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset; and a distributed ledger that stores each OTP-encrypted record by its encryption-start timestamp, enabling retrieval and transfer solely by authorized key holders.

Dependent Claims for Independent Claim 6
The following is a complete set of dependent claims (Claims 2–22) that further specify and narrow the system of Independent Claim 6. Each dependent claim is fully supported by the disclosures in the attached document (Patent Filing Highlights US20210019429A1.docx), including the detailed descriptions of IoT sensor devices producing a continuous non-repeating random number sequence from fluctuating physical measurements, normalization to precise time intervals, encryption service allocation of unique one-time pad segments, distributed ledger storage by encryption-start timestamp, retrieval and transfer solely by authorized key holders, quantum-resistant perfect secrecy, device registration, multi-cloud redundancy, and applicability to any tokenized digital twin or representation of any physical asset, commodity, or verifiable Real World Asset (RWA) as of the January 15, 2018 priority date.

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

1. A system for generating a quantum-resistant non-repeatable digital ledger for tokenized assets, comprising: IoT sensor devices that produce a continuous, non-repeating random number sequence from fluctuating physical measurements; a repository that normalizes the sequence to precise time intervals; an encryption service that allocates unique one-time pad segments from the sequence to encrypt any RWA data or digital twin or representation of any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset; and a distributed ledger that stores each OTP-encrypted record by its encryption-start timestamp, enabling retrieval and transfer solely by authorized key holders.
2. The system of claim 1, wherein the IoT sensor devices comprise 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 system of claim 1, wherein the IoT sensor devices produce the continuous non-repeating random number sequence from fluctuating physical measurements including voltage fluctuations from solar panels or electrical grids, electromagnetic fields, thermal events, or barometric pressure.
4. The system of claim 1, wherein the repository normalizes 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.

5. The system of claim 1, wherein the encryption service allocates unique one-time pad segments in real time or near real time from the live IoT-generated non-repeating random number sequence.
6. The system of claim 1, wherein the distributed ledger stores each OTP-encrypted record identified exclusively by its encryption-start timestamp without traditional hash-chain linking between records.
7. The system of claim 1, wherein the distributed ledger enables retrieval and transfer solely by authorized key holders through owner-provided timestamp and corresponding one-time pad key segment.
8. The system of claim 1, wherein the system registers unique identifiers for IoT sensor devices on the distributed ledger to cryptographically bind device provenance to each OTP-encrypted digital twin or representation.
9. The system of claim 1, wherein the distributed ledger maintains multiple redundant copies across cloud environments to provide fault tolerance and Byzantine fault tolerance for the OTP-encrypted records.
10. The system of claim 1, wherein the system provides information-theoretic perfect secrecy and quantum-resistant security for all tokenized digital twins or representations through the one-time pad encryption and non-repeatable ledger architecture.
11. The system of claim 1, further comprising a trading platform integrated with the distributed ledger that enables secure transfer, swapping, or exchange of the OTP-secured tokenized digital twins or representations while maintaining perfect secrecy.
12. The system of claim 1, wherein the trading platform supports market orders, limit orders, options, forwards, futures, swaps, or pre-market contracts.
13. The system 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 system 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 system of claim 1, wherein the system operates in real time or near real time to enable continuous generation of the non-repeating random number sequence, OTP encryption, ledger storage, and retrieval/transfer of tokenized assets.
16. The system of claim 1, wherein the value tokens represent immutable digital twins or representations of any commodity, security, physical asset, financial instrument, or other verifiable Real World Asset that are verifiable and cannot be double-spent due to the one-time pad encryption and non-repeatable ledger architecture.
17. The system of claim 1, wherein the system eliminates intermediaries by performing end-to-end generation of the non-repeating random number sequence, OTP encryption, ledger storage, and authorized-key-holder retrieval/transfer directly on the quantum-resistant non-repeatable digital ledger.

18. The system 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 system of claim 1, further comprising automated monetization by transferring funds to the seller upon execution of a winning bid while simultaneously delivering the OTP-secured value token to the buyer.
20. The system of claim 1, wherein the system supports scalable, industrial-scale generation of a quantum-resistant non-repeatable digital ledger for tokenized digital twins or representations of any physical asset or commodity.
21. The system of claim 1, wherein the encryption service functions as Encryption as a Service for any RWA data or value token, enabling real-time allocation of one-time pad segments from the live IoT-generated non-repeating random number sequence.
22. The system of claim 1, wherein the distributed ledger employs the non-repeating one-time pad segments such that no key is ever reused, providing perfect forward secrecy for every tokenized digital twin or representation stored or transferred on the ledger.

These claims form a self-contained, commercially robust claim family that directly maps to the system for generating a quantum-resistant non-repeatable digital ledger for tokenized assets using IoT sensor devices to produce a continuous non-repeating random number sequence, normalization, OTP encryption service, timestamp-based distributed ledger storage, and authorized-key-holder retrieval/transfer 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 1–5) to further strengthen the Parisii patent portfolio for quantum-tolerant Web4 W4S security, tokenized Real World Assets, and blockchain-based RWA/digital twin infrastructure.