Independent Claim 4 (Article of Manufacture – Medium for OTP Non-Repeatable DLT)
A non-transitory computer-readable medium storing instructions that, when executed by processors of an IoT cloud platform or distributed ledger nodes, cause the system to: generate a continuous non-repeating random number sequence from IoT sensor measurements; apply one-time pad encryption using unique segments of the sequence to any RWA data or value tokens representing any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset; record each OTP-encrypted digital twin or representation on a timestamp-based non-repeatable ledger; destroy used key segments server-side; and support secure transfer or exchange of the OTP-secured tokens with perfect secrecy.

Dependent Claims for Independent Claim 4
The following is a complete set of dependent claims (Claims 2–22) that further specify and narrow the non-transitory computer-readable medium of Independent Claim 4. Each dependent claim is fully supported by the disclosures in the attached document (Patent Filing Highlights US20210019429A1.docx), including the detailed descriptions of the IoT cloud platform or distributed ledger nodes generating a continuous non-repeating random number sequence from IoT sensor measurements, applying one-time pad encryption using unique segments of the sequence to any RWA data or value tokens, recording each OTP-encrypted digital twin or representation on a timestamp-based non-repeatable ledger, server-side destruction of used key segments, support for secure transfer or exchange of the OTP-secured tokens with perfect secrecy, quantum-resistant security, device/user registration, primary-market issuance, and the overall Encryption as a Service model for tokenized RWAs/digital twins of any physical asset or commodity as of the January 15, 2018 priority date.

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

1. A non-transitory computer-readable medium storing instructions that, when executed by processors of an IoT cloud platform or distributed ledger nodes, cause the system to: generate a continuous non-repeating random number sequence from IoT sensor measurements; apply one-time pad encryption using unique segments of the sequence to any RWA data or value tokens representing any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset; record each OTP-encrypted digital twin or representation on a timestamp-based non-repeatable ledger; destroy used key segments server-side; and support secure transfer or exchange of the OTP-secured tokens with perfect secrecy.
2. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the IoT cloud platform or distributed ledger nodes to generate the continuous non-repeating random number 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 non-transitory computer-readable medium of claim 1, wherein the instructions cause normalization of 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.
4. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the system to receive RWA data or value tokens 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 non-transitory computer-readable medium of claim 1, wherein the instructions cause the one-time pad encryption to be performed in real time or near real time on any RWA data or value token representing a digital twin or representation of any physical asset or commodity.
6. The non-transitory computer-readable medium of claim 1, wherein the instructions cause each OTP-encrypted digital twin or representation to be recorded on the timestamp-based non-repeatable ledger identified exclusively by its encryption-start timestamp without traditional hash-chain linking between records.
7. The non-transitory computer-readable medium of claim 1, wherein the instructions cause immediate server-side destruction of each used one-time pad key segment after secure delivery of the key segment to the owner.
8. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the system to register unique identifiers for IoT sensors, routers, and gateways on the distributed ledger to cryptographically bind device provenance to the OTP-encrypted tokenized digital twin or representation.
9. The non-transitory computer-readable medium of claim 1, wherein the instructions cause support for secure transfer or exchange of the OTP-secured tokens using market orders, limit orders, options, forwards, futures, swaps, or pre-market contracts while maintaining perfect secrecy.
10. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the system to support 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.
11. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the system to apply 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.
12. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the distributed ledger to maintain multiple redundant copies across cloud environments to provide fault tolerance and Byzantine fault tolerance for the OTP-encrypted records.
13. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the system to provide 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.
14. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the system to operate as Encryption as a Service for any RWA data or value token, enabling real-time OTP encryption, timestamp-based ledger storage, and secure key delivery.
15. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the system to treat the minting of value tokens as a primary market activity based on validated IoT-sourced data representing any physical asset or commodity.
16. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the system to enable owner-initiated transfer or redemption solely by presentation of the matching timestamp and one-time pad key segment.
17. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the non-repeating random number sequence to be generated from IoT sensor measurements in a manner that is non-reproducible with earth-bound technology.
18. The non-transitory computer-readable medium of claim 1, wherein the instructions cause 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.

19. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the system to support scalable, industrial-scale tokenization and secure transfer of any physical asset, commodity, or other verifiable Real World Asset as a digital twin on the OTP-secured non-repeatable digital ledger technology.
20. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the system to execute wallet or payment applications within a Trusted Execution Environment (TEE) in connection with OTP encryption, key delivery, and ledger operations.
21. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the system to operate in real time or near real time to enable continuous measurement, OTP encryption, ledger recording, and trading of any physical asset or RWA as a digital twin.
22. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the distributed ledger to employ 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.

These claims form a self-contained, commercially robust claim family that directly maps to the article-of-manufacture embodiments of the non-transitory computer-readable medium for generating a continuous non-repeating random number sequence, applying OTP encryption, recording on a timestamp-based non-repeatable ledger, destroying used key segments server-side, and supporting secure transfer or exchange of OTP-secured tokenized digital twins or representations of any physical asset, commodity, or verifiable Real World Asset (RWA) 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 1–3) to further strengthen the Parisii patent portfolio for quantum-tolerant Web4 W4S security, tokenized Real World Assets, and blockchain-based RWA/digital twin infrastructure.