Independent Claim 9 (Method – Encryption as a Service for OTP-Secured Tokens)
A computer-implemented method for providing Encryption as a Service to tokenize and secure any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset (RWA) as a digital twin or representation on non-repeatable DLT, comprising: receiving RWA data or token records; allocating a unique segment of a live IoT-derived non-repeating random number sequence as a one-time pad key; encrypting the record and returning the key to the owner while writing the ciphertext to a timestamp-based ledger; and enabling subsequent decryption, transfer, or exchange exclusively by the key holder.

Dependent Claims for Independent Claim 9
The following is a complete set of dependent claims (Claims 2–22) that further specify and narrow the computer-implemented method of Independent Claim 9. Each dependent claim is fully supported by the disclosures in the attached document (Patent Filing Highlights US20210019429A1.docx), including the detailed descriptions of Encryption as a Service, receipt of RWA data or token records, allocation of unique segments from the live IoT-derived non-repeating random number sequence as one-time pad keys, real-time encryption, writing ciphertext to a timestamp-based ledger, secure key return to the owner with immediate server-side destruction, enabling subsequent decryption/transfer/exchange exclusively by the key holder, quantum-resistant perfect secrecy, device/user registration, primary-market issuance, 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 computer-implemented method for providing Encryption as a Service to tokenize and secure any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset (RWA) as a digital twin or representation on non-repeatable DLT, comprising: receiving RWA data or token records; allocating a unique segment of a live IoT-derived non-repeating random number sequence as a one-time pad key; encrypting the record and returning the key to the owner while writing the ciphertext to a timestamp-based ledger; and enabling subsequent decryption, transfer, or exchange exclusively by the key holder.
2. The method of claim 1, wherein receiving RWA data or token records further comprises receiving data collected in real time or near real time from an IoT edge hardware layout with sensor devices, edge routers, and edge gateways.
3. The method of claim 1, wherein the live IoT-derived non-repeating random number sequence is generated from fluctuating physical measurements of IoT sensors including voltage fluctuations from solar panels or electrical grids, electromagnetic fields, thermal events, or barometric pressure.
4. The method of claim 1, wherein allocating a unique segment 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.

5. The method of claim 1, wherein encrypting the record further comprises performing modular addition or XOR encryption using the allocated one-time pad key segment on the RWA data or token record.
6. The method of claim 1, wherein writing the ciphertext to the timestamp-based ledger further comprises identifying the record exclusively by its encryption-start timestamp without traditional hash-chain linking between records.
7. The method of claim 1, wherein returning the key 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 one-time pad key segment.
8. The method of claim 1, wherein enabling subsequent decryption, transfer, or exchange further comprises permitting owner-initiated actions solely by presentation of the matching timestamp and one-time pad key segment for decryption and ledger update.
9. 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.
10. 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.
11. The method of claim 1, wherein the timestamp-based ledger maintains multiple redundant copies across cloud environments to provide fault tolerance and Byzantine fault tolerance.
12. The method of claim 1, further comprising integrating the Encryption as a Service 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.
13. The method of claim 1, wherein the trading platform supports market orders, limit orders, options, forwards, futures, swaps, or pre-market contracts.
14. 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.
15. 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.
16. The method of claim 1, wherein the method operates in real time or near real time to enable continuous receipt of RWA data, allocation of one-time pad segments, encryption, key return, ledger recording, and owner-initiated decryption/transfer/exchange.
17. 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.

18. The method of claim 1, wherein the method eliminates intermediaries by providing end-to-end Encryption as a Service directly from receipt of RWA data or token records to OTP-secured ledger storage and authorized-key-holder decryption/transfer/exchange.
19. 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.
20. 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.
21. The method of claim 1, wherein the method supports scalable, industrial-scale Encryption as a Service for tokenized digital twins or representations of any physical asset or commodity by combining real-time IoT data receipt with automated OTP encryption and timestamp-based ledger operations.
22. 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 transfer or exchange.

These claims form a self-contained, commercially robust claim family that directly maps to the computer-implemented method for providing Encryption as a Service to tokenize and secure any physical asset, commodity, or verifiable Real World Asset (RWA) as a digital twin or representation on non-repeatable DLT, including receipt of RWA data/token records, allocation of live IoT-derived one-time pad segments, encryption, timestamp-based ledger recording, secure key return with server-side destruction, and enabling owner-initiated decryption/transfer/exchange 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 1–8) to further strengthen the Parisii patent portfolio for quantum-tolerant Web4 W4S security, tokenized Real World Assets, and blockchain-based RWA/digital twin infrastructure.