Independent Claim 3 (Method – Transfer and Storage of OTP-Secured Tokens)
A computer-implemented method for transfer and storage of tokenized value tokens or digital twins or representations of any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset (RWA) on a non-repeatable digital ledger using one-time pad encryption, comprising: receiving a token record for encryption; allocating a unique non-repeating random number sequence segment from an IoT-derived live stream as a one-time pad key; encrypting the record and writing the ciphertext to a timestamp-based distributed ledger identified by the encryption-start timestamp; securely delivering the one-time pad key segment to the owner while destroying it server-side; and enabling owner-initiated transfer or redemption by providing the timestamp and key for decryption and ledger update.

Dependent Claims for Independent Claim 3
The following is a complete set of dependent claims (Claims 2–22) that further specify and narrow the computer-implemented method of Independent Claim 3. Each dependent claim is fully supported by the disclosures in the attached document (Patent Filing Highlights US20210019429A1.docx), including the detailed descriptions of OTP encryption using unique segments of the IoT-derived live non-repeating random number sequence, timestamp-based distributed ledger recording identified solely by encryption-start timestamp, secure key delivery with immediate server-side destruction, owner-initiated transfer/redemption using timestamp + key, quantum-resistant perfect secrecy, applicability to any tokenized RWA/digital twin or physical/commodity asset, 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 transfer and storage of tokenized value tokens or digital twins or representations of any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset (RWA) on a non-repeatable digital ledger using one-time pad encryption, comprising: receiving a token record for encryption; allocating a unique non-repeating random number sequence segment from an IoT-derived live stream as a one-time pad key; encrypting the record and writing the ciphertext to a timestamp-based distributed ledger identified by the encryption-start timestamp; securely delivering the one-time pad key segment to the owner while destroying it server-side; and enabling owner-initiated transfer or redemption by providing the timestamp and key for decryption and ledger update.
2. The method of claim 1, wherein receiving a token record for encryption further comprises receiving a value token previously minted as an immutable digital twin or representation from IoT-sourced validated data.
3. The method of claim 1, wherein allocating a unique non-repeating random number sequence segment further comprises generating the live non-repeating random number sequence from fluctuating physical measurements of IoT sensors, edge routers, and edge gateways.
4. The method of claim 1, wherein encrypting the record further comprises using the allocated one-time pad key segment to perform modular addition or XOR encryption on the token record.
5. The method of claim 1, wherein writing the ciphertext to the timestamp-based distributed ledger further comprises identifying the record solely by its encryption-start timestamp without traditional hash-chain linking between records.
6. The method of claim 1, wherein securely delivering the one-time pad key segment to the owner comprises one or more of digital channels, physical media, or split-key distribution mechanisms.
7. The method of claim 1, wherein destroying the one-time pad key segment server-side occurs immediately after secure delivery to the owner.

8. The method of claim 1, wherein enabling owner-initiated transfer or redemption further comprises decrypting the ciphertext using the owner-provided timestamp and one-time pad key segment and updating the ledger to reflect new ownership or redemption.
9. The method of claim 1, wherein the method provides information-theoretic perfect secrecy and quantum-resistant security for the tokenized value token or digital twin 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 value token or digital twin.
11. 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.
12. The method of claim 1, further comprising integrating the transfer and storage method with a trading platform that enables secure transfer, swapping, or exchange of the OTP-secured tokenized value token or digital twin while maintaining perfect secrecy.
13. 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.
14. The method of claim 1, wherein the method operates in real time or near real time to enable continuous encryption, ledger recording, key delivery, and owner-initiated transfer or redemption.
15. 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.
16. The method of claim 1, wherein the method eliminates intermediaries by performing end-to-end OTP-secured transfer and storage directly on the non-repeatable digital ledger technology.
17. The method of claim 1, wherein the timestamp-based distributed ledger records each OTP-encrypted record identified exclusively by its encryption-start timestamp.
18. The method of claim 1, further comprising automated preparation for monetization by associating the OTP-secured tokenized value token or digital twin with mechanisms for ownership transfer and payment upon future trading execution.
19. The method of claim 1, wherein the method supports scalable, industrial-scale transfer and storage 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 operations.
20. 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 redemption.
21. 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, secure key delivery, and owner-initiated transfer or redemption.
22. The method 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 value token or digital twin during transfer and storage.

These claims form a self-contained, commercially robust claim family that directly maps to the computer-implemented method for transfer and storage of tokenized value tokens or digital twins or representations of any physical asset, commodity, or verifiable Real World Asset (RWA) on a non-

repeatable digital ledger using one-time pad encryption, timestamp-based recording, secure key delivery with server-side destruction, and owner-initiated transfer/redemption 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 2) to further strengthen the Parisii patent portfolio for quantum-tolerant Web4 W4S security, tokenized Real World Assets, and blockchain-based RWA/digital twin infrastructure.