Independent Claim 12 (Method – Privacy-Preserving OTP Ledger for Token Trading)
A computer-implemented method for privacy-preserving trading of tokenized digital twins or representations of any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset (RWA) on OTP-secured non-repeatable DLT, comprising: encrypting token records with unique non-repeating one-time pad segments derived from IoT sensors; storing only ciphertext and timestamps on the distributed ledger; sharing transaction details solely with trade counterparties via point-to-point key validation; and enabling regulatory verification of provenance without exposing underlying asset data.

Dependent Claims for Independent Claim 12
The following is a complete set of dependent claims (Claims 2–22) that further specify and narrow the computer-implemented method of Independent Claim 12. Each dependent claim is fully supported by the disclosures in the attached document (Patent Filing Highlights US20210019429A1.docx), including the detailed descriptions of privacy-preserving blockchain designs (storing only cryptographic hashes and public-key ownership), point-to-point validation for sharing transaction details exclusively with trade parties, regulatory observer nodes for verifying provenance and preventing double-spending without exposing underlying physical asset details, minimal metadata storage, full anonymity during daily operations, conditional activation of full history upon legal requirement, integration with IoT-sourced tokenized digital twins or representations, OTP-secured non-repeatable DLT, immutable ledger recording, and the overall tokenized RWA/digital twin trading 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 privacy-preserving trading of tokenized digital twins or representations of any physical asset, commodity, digital asset, security, contract, or other verifiable Real World Asset (RWA) on OTP-secured non-repeatable DLT, comprising: encrypting token records with unique non-repeating one-time pad segments derived from IoT sensors; storing only ciphertext and timestamps on the distributed ledger; sharing transaction details solely with trade counterparties via point-to-point key validation; and enabling regulatory observer nodes to verify provenance and prevent double-spending without exposing underlying asset data.
2. The method of claim 1, wherein encrypting token records further comprises using a live IoT-derived non-repeating random number sequence normalized to a system clock at microsecond or finer granularity so that each encryption uses a unique timestamp-aligned one-time pad segment.
3. The method of claim 1, wherein storing only ciphertext and timestamps on the distributed ledger further comprises storing only minimal metadata by default and not recording individual transaction details unless activated by a legal requirement such as a subpoena or warrant.
4. The method of claim 1, wherein sharing transaction details solely with trade counterparties further comprises using point-to-point validation between the involved parties without broadcasting full transaction details to the entire network.
5. The method of claim 1, wherein enabling regulatory observer nodes further comprises granting limited access to those nodes solely for verifying provenance and preventing

double-spending while prohibiting exposure of underlying physical asset details or full transaction history.

6. The method of claim 1, wherein the method provides full anonymity to users during daily operations involving the tokenized digital twins or representations, with activation of full transaction history occurring only upon a legal requirement.
7. The method of claim 1, wherein the distributed ledger is configured to store both account balance records and transaction records, but transaction records remain inactive and inaccessible until activated by a legal requirement.
8. The method 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 cryptographic hashes and public-key ownership stored on the OTP-secured non-repeatable ledger.
9. The method of claim 1, wherein the method operates in conjunction with a blockchain trading platform that lists the value tokens and supports market, limit, options, forwards, futures, swaps, or similar orders while maintaining the privacy-preserving design.
10. The method of claim 1, wherein the privacy-preserving design further comprises executing one or more steps within a Trusted Execution Environment (TEE) on computing devices to protect sensitive data during trading.
11. The method of claim 1, further comprising server-side destruction of any decryption keys or key segments immediately after secure delivery to the authorized trade parties.
12. The method of claim 1, wherein the non-repeating one-time pad segments provide information-theoretic perfect secrecy and quantum-resistant security for the tokenized digital twins or representations and all associated privacy-preserving records.
13. The method of claim 1, wherein the method integrates regulatory compliance mechanisms during user onboarding or device registration while preserving the privacy-preserving design for all subsequent trading operations.
14. The method of claim 1, wherein the distributed ledger maintains multiple redundant copies across cloud environments to provide fault tolerance and Byzantine fault tolerance while preserving privacy-preserving storage of only cryptographic hashes and public-key ownership.
15. The method of claim 1, wherein sharing transaction details via point-to-point validation further comprises cryptographic validation between trade parties without exposing the underlying physical asset details or full transaction history to non-participating nodes.
16. The method of claim 1, wherein enabling regulatory observer nodes further comprises allowing those nodes to verify provenance and prevent double-spending using only cryptographic proofs without granting access to the underlying physical asset measurements or details.
17. The method of claim 1, wherein the method supports high-frequency, derivative, and institutional trading of tokenized digital twins or representations while maintaining the privacy-preserving architecture throughout all trading, swapping, and collateral activities.

18. The method of claim 1, wherein the method operates in a closed-loop automated process from minting of privacy-preserving value tokens through point-to-point validated trading and regulatory observer verification.
19. The method of claim 1, wherein the immutable ledger record employs cryptographic hashing of each new block to prior blocks to ensure permanent verifiability of provenance without exposing underlying physical asset details.
20. The method of claim 1, wherein the method eliminates intermediaries by performing end-to-end privacy-preserving trading directly on the integrated blockchain ledger while restricting full details to trade parties and authorized regulatory observers.
21. The method of claim 1, wherein the privacy-preserving trading method further comprises automated monetization or settlement that directs proceeds without exposing underlying physical asset details to non-authorized parties.
22. The method of claim 1, wherein the method further comprises registering unique identifiers for IoT sensors, routers, and gateways on the distributed ledger to cryptographically bind device provenance to the privacy-preserving tokenized digital twins or representations.

These claims form a self-contained, commercially robust claim family that directly maps to the computer-implemented method for privacy-preserving trading of tokenized digital twins or representations of any physical asset, commodity, or verifiable Real World Asset (RWA) on OTP-secured non-repeatable DLT, including encryption with unique non-repeating one-time pad segments, minimal-metadata storage, point-to-point validation, and regulatory observer nodes 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 1–11) to further strengthen the Parisii patent portfolio for quantum-tolerant Web4 W4S security, tokenized Real World Assets, and blockchain-based RWA/digital twin infrastructure.