Independent Claim 13 (Method – Privacy-Preserving RWA Digital Twin Trading)
A computer-implemented method for privacy-preserving trading of tokenized digital twins of any physical asset or RWA, comprising: minting value tokens on a blockchain that store only cryptographic hashes and public-key ownership; sharing transaction details only with trade parties via point-to-point validation; and enabling regulatory observer nodes to verify provenance and prevent double-spending without exposing underlying physical asset details.

Dependent Claims for Independent Claim 13
The following is a complete set of dependent claims (Claims 2–22) that further specify and narrow the computer-implemented method of Independent Claim 13. Each dependent claim is fully supported by the disclosures in the attached document (Patent Filing Highlights US20220180374A1.pdf), 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, immutable ledger recording, and the overall tokenized RWA/digital twin trading architecture as of the December 26, 2017 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 of any physical asset or RWA, comprising: minting value tokens on a blockchain that store only cryptographic hashes and public-key ownership; sharing transaction details only with trade parties via point-to-point validation; and enabling regulatory observer nodes to verify provenance and prevent double-spending without exposing underlying physical asset details.
2. The method of claim 1, wherein minting the value tokens further comprises collecting real-time data associated with any physical asset or RWA using IoT sensors, routers, and gateways, transmitting the data to an IoT cloud platform, validating the data, and generating a digital RWA certificate prior to minting.
3. The method of claim 1, wherein the blockchain stores only cryptographic hashes and public-key ownership for the value tokens, with no underlying physical asset details or transaction metadata recorded by default.
4. The method of claim 1, wherein sharing transaction details only with trade parties 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.
6. The method of claim 1, wherein the method provides full anonymity to users during daily operations involving the tokenized digital twins, with activation of full transaction history occurring only upon a legal requirement such as a subpoena or warrant.

7. The method of claim 1, wherein the blockchain ledger is configured to store only minimal metadata by default and does not record individual transaction details unless activated by a legal requirement.
8. The method of claim 1, wherein the blockchain ledger is further configured to store both account balance records and transaction records, but transaction records remain inactive and inaccessible until activated by a legal requirement.
9. The method of claim 1, wherein the value tokens represent immutable digital twins of any commodity, security, physical asset, financial instrument, or other RWA that are verifiable and cannot be double-spent due to the cryptographic hashes and public-key ownership stored on the blockchain.
10. 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.
11. 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.
12. 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.
13. The method of claim 1, wherein the non-repeating or cryptographic mechanisms provide information-theoretic perfect secrecy or quantum-resistant security for the tokenized digital twins and all associated privacy-preserving records.
14. 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.
15. The method of claim 1, wherein the blockchain 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.
16. 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.
17. 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.
18. The method of claim 1, wherein the method supports high-frequency, derivative, and institutional trading of tokenized digital twins while maintaining the privacy-preserving architecture throughout all trading, swapping, and collateral activities.
19. 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.
20. 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.

21. 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.
22. 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.

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 of any physical asset or RWA, including minting with only cryptographic hashes and public-key ownership, point-to-point validation for trade parties, and regulatory observer nodes for provenance and double-spending prevention without exposing underlying details as described in the December 26, 2017 provisional disclosure (and the incorporated earlier provisionals). 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 1–12) to further strengthen the Parisii patent portfolio for tokenized Real World Assets and blockchain-based RWA/digital twin infrastructure.