Independent Claim 6 (System – Zero-Trust OTP Ledger for RWA Digital Twins)
A zero-trust ledger system for tokenized banking, comprising: a live non-repeating random number sequence for OTP encryption of any RWA digital twin or token record; a timestamp-based distributed ledger that stores encrypted packets; and banking functionality for deposit tokens, payments, transfers, and collateral while ensuring server-side key destruction and perfect secrecy.

Dependent Claims for Independent Claim 6
The following is a complete set of dependent claims (Claims 2–17) that further specify and narrow the zero-trust ledger system of Independent Claim 6. Each dependent claim is fully supported by the disclosures in the attached document (Parisii™ Filings 041518 & 052018 Tokenization and Banking Highlights - Q2 2026.docx), including the detailed OTP zero-trust ledger designs, live non-repeating random number sequences sourced from IoT or secure generators, timestamp-based distributed ledger mechanics for encrypted packets, server-side key destruction, perfect secrecy (information-theoretic and quantum-resistant), account balance and transaction record options, TEE integration, privacy-preserving features, applicability to any RWA/digital twin or token record, integration with deposit token issuance, payments, transfers, collateral, and the overall cryptocurrency/financial system business model.

Full Claim Set in Formal USPTO-Style Format

1. A zero-trust ledger system for tokenized banking, comprising: a live non-repeating random number sequence for OTP encryption of any RWA digital twin or token record; a timestamp-based distributed ledger that stores encrypted packets; and banking functionality for deposit tokens, payments, transfers, and collateral while ensuring server-side key destruction and perfect secrecy.
2. The zero-trust ledger system of claim 6, wherein the live non-repeating random number sequence is derived from Internet of Things (IoT) devices or other secure random number generators to provide information-theoretic perfect secrecy.
3. The zero-trust ledger system of claim 6, wherein the timestamp-based distributed ledger stores encrypted packets using only account balance records by default and does not record individual transaction details unless activated by a legal requirement such as a subpoena or warrant.
4. The zero-trust ledger system of claim 6, wherein the timestamp-based distributed ledger is further configured to store both account balance records and transaction records related to deposit tokens, payments, transfers, and collateral.
5. The zero-trust ledger system of claim 6, wherein the account record on the distributed ledger contains a unique user identifier, a timestamp for sequencing and lookup, and the account balance itself.
6. The zero-trust ledger system of claim 6, wherein the banking functionality for deposit tokens further comprises issuance after user verification via Know Your Customer/Anti-Money Laundering (KYC/AML) processes, with the resulting deposit token secured as an encrypted packet on the ledger.
7. The zero-trust ledger system of claim 6, wherein the banking functionality for payments and transfers comprises encrypting a payment data packet using the OTP encryption,

recording the encrypted packet on the timestamp-based distributed ledger, and providing the recipient with a timestamp and size lookup for decryption and redemption.

8. The zero-trust ledger system of claim 6, wherein the banking functionality for collateral comprises using one or more value tokens or deposit tokens as collateral to secure a fiat-based financial arrangement with a bank, financial institution, or other financial services company, with the collateral contract recorded as an encrypted packet on the distributed ledger.
9. The zero-trust ledger system of claim 6, further comprising a Trusted Execution Environment (TEE) for executing secure wallet applications and payment applications on computing devices in connection with the zero-trust ledger operations.
10. The zero-trust ledger system of claim 6, wherein server-side key destruction of the OTP decryption key or key segments occurs immediately after secure delivery of the key or key segments to the token owner or recipient.
11. The zero-trust ledger system of claim 6, wherein the system provides full anonymity to users during daily operations involving deposit tokens, payments, transfers, and collateral, with activation of full transaction history occurring only upon a legal requirement.
12. The zero-trust ledger system of claim 6, wherein the OTP encryption and non-repeating random number sequence provide quantum-resistant security for all RWA digital twin tokens, deposit tokens, and encrypted packets stored on the distributed ledger.
13. The zero-trust ledger system of claim 6, wherein the system supports tokenization of any physical asset or commodity as a digital twin, with the resulting digital twin token or record secured as an encrypted packet using the OTP encryption on the timestamp-based distributed ledger.
14. The zero-trust ledger system of claim 6, wherein the banking functionality further includes automated monetization, settlement, and reinvestment of tokenized reserves using the value tokens or deposit tokens recorded on the distributed ledger.
15. The zero-trust ledger system of claim 6, wherein the timestamp-based distributed ledger ensures proper sequencing and lookup of encrypted packets without exposing plaintext data outside the TEE or owner possession.
16. The zero-trust ledger system of claim 6, wherein the system merges existing asset instruments with cryptocurrency instruments on the same zero-trust OTP ledger to introduce new financial markets while maintaining server-side key destruction and perfect secrecy.
17. The zero-trust ledger system of claim 6, wherein the system integrates regulatory compliance mechanisms during user onboarding while preserving the zero-trust OTP architecture and privacy-preserving design for all ledger operations.

These claims form a self-contained, commercially robust claim family that directly maps to the zero-trust OTP ledger system, live non-repeating random number sequence, timestamp-based encrypted packet storage, server-side key destruction, perfect secrecy, RWA/digital twin coverage, and full tokenized banking functionality (deposit tokens, payments, transfers, and collateral) described in the provisionals. The full set can be incorporated into a non-provisional

or continuation application (alone or in combination with the claim families of Independent Claims 1–5) to further strengthen the Parisii patent portfolio for tokenized banking and RWA infrastructure.