Independent Claim 10 (Method – Privacy-Preserving OTP Ledger in Tokenized Banking)
A computer-implemented method for privacy-preserving tokenized banking, comprising: storing tokenized RWA balances and deposit token records on an OTP-encrypted ledger with minimal metadata by default; activating full history only upon legal requirement; and enabling deposit tokens, payments, and collateral while maintaining quantum-resistant secrecy for daily operations.

Dependent Claims for Independent Claim 10
The following is a complete set of dependent claims (Claims 2–19) that further specify and narrow the computer-implemented method of Independent Claim 10. 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 privacy-preserving ledger designs that store only minimal metadata by default, activation of full transaction history solely upon legal requirement (subpoena, warrant, or probable cause), full anonymity during daily operations, OTP-encrypted account balance and transaction records, quantum-resistant/information-theoretic secrecy, integration with deposit tokens/payments/collateral, KYC/AML limited to onboarding, account record formats (unique user identifier, timestamp, balance), and the overall cryptocurrency/financial or document management system described in the provisionals.

Full Claim Set in Formal USPTO-Style Format (Reordered to Start with Claim 1)

1. A computer-implemented method for privacy-preserving tokenized banking, comprising: storing tokenized RWA balances and deposit token records on an OTP-encrypted ledger with minimal metadata by default; activating full history only upon legal requirement; and enabling deposit tokens, payments, and collateral while maintaining quantum-resistant secrecy for daily operations.
2. The method of claim 1, wherein the minimal metadata stored by default comprises only account balance records that do not include individual transaction details.
3. The method of claim 1, wherein the OTP-encrypted 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.
4. The method of claim 1, wherein activating full history occurs only upon a legal requirement such as a subpoena, warrant, or probable cause determination.
5. The method of claim 1, wherein the method provides full anonymity to the user during daily operations involving deposit tokens, payments, and collateral.
6. The method of claim 1, wherein user identifying information is not permanently recorded on the distributed ledger and is instead stored offline or with only minimal metadata to provide privacy protection after initial verification.
7. The method of claim 1, wherein the account record on the OTP-encrypted ledger contains a unique user identifier, a timestamp for sequencing and lookup, and the account balance itself, with no additional personal data stored by default.
8. The method of claim 1, wherein the OTP encryption utilizes key segments derived from a live non-repeating random number sequence sourced from Internet of Things (IoT)

devices or other secure random number generators to maintain quantum-resistant secrecy.

9. The method of claim 1, wherein the non-repeating random number sequence provides information-theoretic perfect secrecy for all tokenized RWA balances, deposit token records, and daily operations on the ledger.
10. The method of claim 1, wherein storing tokenized RWA balances and deposit token records further comprises performing a Know Your Customer/Anti-Money Laundering (KYC/AML) verification only during user onboarding, after which privacy-preserving design governs all subsequent operations.
11. The method of claim 1, further comprising executing one or more steps within a Trusted Execution Environment (TEE) on a computing device while preserving the privacy-preserving OTP-encrypted ledger design.
12. The method of claim 1, wherein enabling deposit tokens, payments, and collateral comprises encrypting all related data packets using OTP encryption prior to recording on the ledger, with server-side destruction of decryption keys immediately after secure delivery to the owner or recipient.
13. The method of claim 1, wherein the tokenized RWA balances represent a digital twin of any physical asset, commodity, digital asset, security, contract, or RWA secured by the OTP-encrypted ledger.
14. The method of claim 1, further comprising integrating the privacy-preserving method with timestamp-based sequencing on the distributed ledger for immutable storage while maintaining minimal metadata by default.
15. The method of claim 1, wherein the method merges existing asset instruments with cryptocurrency instruments on the same OTP-encrypted ledger to introduce new financial markets while preserving full anonymity during daily operations.
16. The method of claim 1, wherein the privacy-preserving tokenized banking further includes automated monetization, settlement, and reinvestment of tokenized reserves using the deposit tokens or RWA balances recorded on the ledger.
17. The method of claim 1, wherein the OTP-encrypted ledger applies to any other form of data in addition to tokenized RWA balances and deposit token records within a financial or document management system.
18. The method of claim 1, wherein the method maintains regulatory compliance mechanisms during user onboarding while ensuring that daily operations remain fully anonymous and quantum-resistant until activation of full history.
19. The method of claim 1, wherein the full history activation includes both account balance records and transaction records, with all prior privacy safeguards remaining in effect until the legal requirement is satisfied.

These claims form a self-contained, commercially robust claim family that directly maps to the privacy-preserving OTP ledger method in tokenized banking, minimal-metadata storage, conditional full-history activation, full anonymity during daily operations, quantum-resistant secrecy, and integration with deposit tokens, payments, and collateral as described in the provisionals. The full set (renumbered to begin with Claim 1) can be incorporated into a non-provisional or continuation application (alone or in combination with the claim families of

Independent Claims 1–9) to further strengthen the Parisii patent portfolio for tokenized banking and RWA infrastructure.