Independent Claim 13 (Method – End-to-End Tokenized Bank with OTP Security)
A computer-implemented method for a tokenized bank, comprising: issuing deposit tokens via verification and OTP ledger storage; enabling payments, transfers, and collateralized loans using value tokens representing any physical asset, commodity, digital asset, security, contract, or RWA; and operating the entire system on a non-repeatable DLT that provides perfect secrecy for all tokenized activity.

Dependent Claims for Independent Claim 13
The following is a complete set of dependent claims (Claims 2–20) 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 (Parisii™ Filings 041518 & 052018 Tokenization and Banking Highlights - Q2 2026.docx), including the end-to-end tokenized bank model, deposit token issuance after verification, OTP ledger storage, payments/transfers/collateralized loans using value tokens or deposit tokens representing any physical asset/commodity/RWA as a digital twin, non-repeatable DLT operation with perfect secrecy, KYC/AML processes, ledger designs (account-balance-only and full transaction records), TEE integration, privacy-preserving features, primary-market issuance, server-side key destruction, timestamp-based sequencing, automated monetization/settlement/reinvestment, 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 a tokenized bank, comprising: issuing deposit tokens via verification and OTP ledger storage; enabling payments, transfers, and collateralized loans using value tokens representing any physical asset, commodity, digital asset, security, contract, or RWA; and operating the entire system on a non-repeatable DLT that provides perfect secrecy for all tokenized activity.
2. The method of claim 1, wherein issuing deposit tokens further comprises performing a Know Your Customer/Anti-Money Laundering (KYC/AML) verification prior to minting and storing any deposit token on the non-repeatable DLT.
3. The method of claim 1, wherein the verification step stores user identifying information offline or with only minimal metadata on the ledger to maintain privacy protection after initial onboarding.
4. The method of claim 1, wherein OTP ledger storage comprises encrypting deposit tokens and value tokens using non-repeating key segments derived from a live non-repeating random number sequence sourced from Internet of Things (IoT) devices or other secure random number generators.
5. The method of claim 1, wherein the non-repeatable DLT is configured to store 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.
6. The method of claim 1, wherein the non-repeatable DLT is further configured to store both account balance records and transaction records.

7. The method of claim 1, wherein an account record on the non-repeatable DLT contains a unique user identifier, a timestamp for sequencing and lookup, and the account balance itself.
8. The method of claim 1, wherein enabling payments and transfers further comprises encrypting a payment data packet containing a value token or deposit token using OTP encryption, recording the encrypted packet on the non-repeatable DLT, and providing the recipient with a timestamp and size lookup for decryption and redemption.
9. The method of claim 1, wherein enabling collateralized loans further 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 on the non-repeatable DLT.
10. The method of claim 1, wherein operating the entire system on the non-repeatable DLT further comprises executing wallet and payment applications within a Trusted Execution Environment (TEE) on computing devices while ensuring no sensitive data is exposed outside the TEE or owner possession.
11. The method of claim 1, further comprising server-side destruction of OTP decryption key or key segments immediately after secure delivery of the key or key segments to the token owner or recipient.
12. The method of claim 1, wherein the method provides full anonymity to the user during daily operations, with activation of full transaction history occurring only upon a legal requirement.
13. The method of claim 1, wherein the value tokens represent a digital twin of any physical asset or commodity secured by OTP encryption on the non-repeatable DLT.
14. The method of claim 1, wherein the non-repeatable DLT provides information-theoretic perfect secrecy and quantum-resistant security for all tokenized activity, including deposits, payments, transfers, and collateralized loans.
15. The method of claim 1, wherein issuing deposit tokens and enabling payments, transfers, and collateralized loans treats the creation and use of value tokens or deposit tokens as a primary market activity based on validated asset performance, deposit of value, or other asset-backed issuance.
16. The method of claim 1, further comprising automating monetization, settlement, and reinvestment of tokenized reserves using the value tokens or deposit tokens on the non-repeatable DLT to generate yield.
17. The method of claim 1, wherein the method merges existing asset instruments with cryptocurrency instruments on the same non-repeatable DLT to introduce new financial markets while maintaining perfect secrecy for all tokenized activity.
18. The method of claim 1, wherein the method maintains regulatory compliance mechanisms during verification while preserving the privacy-preserving and zero-trust design for all subsequent operations on the non-repeatable DLT.
19. The method of claim 1, wherein the non-repeatable DLT utilizes timestamp-based sequencing for immutable storage and lookup of all encrypted records related to deposit tokens, payments, transfers, and collateralized loans.

20. The method of claim 1, wherein the entire end-to-end tokenized bank operates as a zero-trust system in which decryption keys or key segments are never permanently stored on servers outside the TEE or owner possession.

These claims form a self-contained, commercially robust claim family that directly maps to the end-to-end tokenized bank method, deposit token issuance, payments/transfers/collateralized loans using RWA value tokens, and operation on a non-repeatable DLT with perfect secrecy 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 1–12) to further strengthen the Parisii patent portfolio for tokenized banking and RWA infrastructure.