

Independent Claim 11 (Article of Manufacture – Ledger Designs for Tokenized Banking)

A non-transitory computer-readable medium embodying OTP ledger designs for tokenized banking, the medium storing instructions for account balance records (deposit tokens) and transaction records, each secured by non-repeating OTP keys, and supporting payments, loans, collateral, and full banking functionality.

Dependent Claims for Independent Claim 11

The following is a complete set of dependent claims (Claims 2–20) that further specify and narrow the non-transitory computer-readable medium of Independent Claim 11. 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 two primary OTP ledger designs (account-balance-only and full transaction records), account record formats (unique user identifier, timestamp, balance), non-repeating OTP key segments from IoT or secure generators, timestamp-based sequencing/lookup, privacy-preserving minimal-metadata default with conditional full-history activation, server-side key destruction, TEE integration, support for deposit tokens/payments/transfers/collateral/loans, primary-market issuance, RWA/digital twin coverage, quantum-resistant perfect secrecy, 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 non-transitory computer-readable medium embodying OTP ledger designs for tokenized banking, the medium storing instructions for account balance records (deposit tokens) and transaction records, each secured by non-repeating OTP keys, and supporting payments, loans, collateral, and full banking functionality.
2. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the OTP ledger to store only account balance records by default and to not record individual transaction details unless activated by a legal requirement such as a subpoena or warrant.
3. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the OTP ledger to store both account balance records and transaction records.
4. The non-transitory computer-readable medium of claim 1, wherein the instructions cause each account record to contain a unique user identifier, a timestamp for sequencing and lookup, and the account balance itself.
5. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the non-repeating OTP keys to be derived from a live non-repeating random number sequence sourced from Internet of Things (IoT) devices or other secure random number generators.
6. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the OTP ledger to provide information-theoretic perfect secrecy and quantum-resistant security for all account balance records, transaction records, deposit tokens, and tokenized banking operations.
7. The non-transitory computer-readable medium of claim 1, wherein the instructions further cause server-side destruction of the OTP decryption key or key segments

immediately after secure delivery of the key or key segments to the token owner or recipient.

8. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the OTP ledger to support deposit token issuance after user verification via Know Your Customer/Anti-Money Laundering (KYC/AML) processes.
9. The non-transitory computer-readable medium of claim 1, wherein the instructions for payments and transfers cause encryption of a payment data packet using OTP encryption, recording of the encrypted packet on the ledger, and provision of a timestamp and size lookup for recipient decryption and redemption.
10. The non-transitory computer-readable medium of claim 1, wherein the instructions for loans and collateral cause one or more deposit tokens or value tokens to be used 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 OTP ledger.
11. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the OTP ledger to support tokenization of any physical asset, commodity, digital asset, security, contract, or RWA as a digital twin secured by non-repeating OTP keys.
12. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the system to provide full anonymity to users during daily operations, with activation of full transaction history occurring only upon a legal requirement.
13. The non-transitory computer-readable medium of claim 1, further comprising instructions for execution of secure wallet and payment applications within a Trusted Execution Environment (TEE) in connection with the OTP ledger designs.
14. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the OTP ledger to treat the creation of deposit tokens or value tokens as a primary market activity based on validated asset performance, deposit of value, or other asset-backed issuance.
15. The non-transitory computer-readable medium of claim 1, wherein the instructions further cause automated monetization, settlement, and reinvestment of tokenized reserves using the deposit tokens or value tokens recorded on the OTP ledger.
16. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the OTP ledger to maintain minimal metadata by default while preserving the ability to activate full history upon legal requirement without compromising quantum-resistant secrecy.
17. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the OTP ledger designs to apply to any other form of data in addition to account balance records and transaction records within a financial or document management system.
18. The non-transitory computer-readable medium of claim 1, wherein the instructions cause timestamp-based sequencing on the distributed ledger for immutable storage and lookup of all records secured by non-repeating OTP keys.
19. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the OTP ledger to integrate regulatory compliance mechanisms during user

onboarding while maintaining privacy-preserving design for all subsequent banking functionality.

20. The non-transitory computer-readable medium of claim 1, wherein the instructions cause the OTP ledger to merge existing asset instruments with cryptocurrency instruments on the same ledger to introduce new financial markets while supporting payments, loans, collateral, and full banking functionality.

These claims form a self-contained, commercially robust claim family that directly maps to the article-of-manufacture embodiments of the OTP ledger designs for tokenized banking, the two primary ledger configurations, account record structures, non-repeating OTP security, privacy-preserving features, and full support for deposit tokens, payments, loans, collateral, and RWA/digital twin functionality 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 1–10) to further strengthen the Parisii patent portfolio for tokenized banking and RWA infrastructure.