Independent Claim 5 (Article of Manufacture – Medium for OTP Tokenized Banking)
A non-transitory computer-readable medium storing instructions that, when executed, cause a distributed ledger and banking platform to: issue deposit tokens and value tokens representing any physical asset, commodity, digital asset, security, contract, or RWA; secure all records and transactions with OTP encryption using non-repeating sequences; and provide tokenized banking services including payments, collateralized loans, and transfers.

Dependent Claims for Independent Claim 5
The following is a complete set of dependent claims (Claims 2–17) that further specify and narrow the non-transitory computer-readable medium of Independent Claim 5. 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 descriptions of the cryptocurrency/financial system business model, KYC/AML processes, OTP zero-trust ledger designs (account-balance-only and full transaction records), TEE-based wallet and payment applications, payment data packet encryption and redemption flows, collateral mechanisms, privacy-preserving features, primary-market issuance, digital twin/RWA tokenization for any physical asset or commodity, server-side key destruction, timestamp-based sequencing, quantum-resistant security, and integration of tokenized banking services on the distributed ledger.

Full Claim Set in Formal USPTO-Style Format

1. A non-transitory computer-readable medium storing instructions that, when executed, cause a distributed ledger and banking platform to: issue deposit tokens and value tokens representing any physical asset, commodity, digital asset, security, contract, or RWA as a digital twin; secure all records and transactions with OTP encryption using non-repeating sequences; and provide tokenized banking services including payments, collateralized loans, and transfers.
2. The non-transitory computer-readable medium of claim 5, wherein the instructions further cause the issuance process to perform a Know Your Customer/Anti-Money Laundering (KYC/AML) verification on a user prior to minting any value token or deposit token.
3. The non-transitory computer-readable medium of claim 5, wherein the instructions cause user identifying information to not be permanently recorded on the distributed ledger and to instead be stored offline or with only minimal metadata to provide privacy protection after initial verification.
4. The non-transitory computer-readable medium of claim 5, wherein the instructions cause the distributed ledger to store only account balance records by default and to not record individual transactions unless activated by a legal requirement.
5. The non-transitory computer-readable medium of claim 5, wherein the instructions cause the distributed ledger to store both account balance records and transaction records.
6. The non-transitory computer-readable medium of claim 5, wherein the instructions cause the OTP encryption to utilize key segments derived from a live non-repeating

random number sequence sourced from Internet of Things (IoT) devices or other secure random number generators.

7. The non-transitory computer-readable medium of claim 5, wherein the instructions further cause execution of secure wallet applications and payment applications within a Trusted Execution Environment (TEE) on computing devices.
8. The non-transitory computer-readable medium of claim 5, wherein the instructions for tokenized banking services further cause payments and transfers to be performed by encrypting a payment data packet using the OTP encryption, recording the encrypted packet on the distributed ledger, and providing the recipient with a timestamp and size lookup for decryption and redemption in a TEE.
9. The non-transitory computer-readable medium of claim 5, wherein the instructions for tokenized banking services further cause one or more value tokens or deposit 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 distributed ledger.
10. The non-transitory computer-readable medium of claim 5, wherein the instructions cause the system to provide full anonymity to the user during daily operations, with full transaction history activation occurring only upon a legal requirement such as a subpoena or warrant.
11. The non-transitory computer-readable medium of claim 5, wherein the instructions cause the non-repeating random number sequence to provide information-theoretic perfect secrecy and quantum-resistant security for all tokens, records, and transactions on the distributed ledger.
12. The non-transitory computer-readable medium of claim 5, wherein the instructions cause the system to support tokenization of any physical asset or commodity as a digital twin, with the resulting digital twin token secured by the OTP encryption on the distributed ledger.
13. The non-transitory computer-readable medium of claim 5, 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.
14. The non-transitory computer-readable medium of claim 5, wherein the instructions cause the issuance process to treat the creation of value tokens or deposit 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 5, wherein the instructions for tokenized banking services further cause automated monetization, settlement, and reinvestment of tokenized reserves using the value tokens or deposit tokens on the distributed ledger.
16. The non-transitory computer-readable medium of claim 5, wherein the instructions cause the account record on the distributed ledger to contain a unique user identifier, a timestamp for sequencing and lookup, and the account balance itself.
17. The non-transitory computer-readable medium of claim 5, wherein the instructions cause the system to integrate regulatory compliance mechanisms during user onboarding while maintaining privacy-preserving design for end-user daily operations.

These claims form a self-contained, commercially robust claim family that directly maps to the article-of-manufacture embodiments of the tokenized banking platform, OTP-secured ledger mechanics, TEE integration, privacy features, primary-market token creation, RWA/digital twin coverage, and full tokenized banking services 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 1–4) to further strengthen the Parisii patent portfolio for tokenized banking and RWA infrastructure.