Independent Claim 1 (System – Tokenized Banking Platform)
A system for tokenized banking, comprising: an issuance process that mints value tokens or deposit tokens representing any physical asset, commodity, digital asset, security, contract, or RWA as a digital twin on a distributed ledger; OTP encryption using a non-repeating random number sequence to secure each token or record; and tokenized banking services including deposits, payments, transfers, and collateral for loans.

Dependent Claims for Independent Claim 1
The following is a complete set of dependent claims (Claims 2–16) that further specify and narrow the system of Independent Claim 1. Each dependent claim is fully supported by the disclosures in the April 15, 2018 and May 20, 2018 provisional applications (and the provisionals they incorporate by reference), including the detailed descriptions of KYC/AML processes, ledger designs, OTP zero-trust architecture, TEE integration, payment flows, collateral mechanisms, privacy-preserving features, primary-market issuance, and applicability to any physical asset or commodity tokenized as an RWA/digital twin.

Full Claim Set in Formal USPTO-Style Format

1. A system for tokenized banking, comprising: an issuance process that mints value tokens or deposit tokens representing any physical asset, commodity, digital asset, security, contract, or RWA as a digital twin on a distributed ledger; OTP encryption using a non-repeating random number sequence to secure each token or record; and tokenized banking services including deposits, payments, transfers, and collateral for loans.
2. The system of claim 1, wherein the issuance process further comprises performing a Know Your Customer/Anti-Money Laundering (KYC/AML) verification on a user prior to minting any value token or deposit token.
3. The system 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.
4. The system of claim 1, wherein the distributed ledger is configured to store only account balance records by default and does not record individual transactions unless activated by a legal requirement.
5. The system of claim 1, wherein the distributed ledger is further configured to store both account balance records and transaction records.
6. The system 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.
7. The system of claim 1, further comprising a Trusted Execution Environment (TEE) for executing secure wallet applications and payment applications on computing devices.
8. The system of claim 1, wherein the tokenized banking services further comprise payments and transfers 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 system of claim 1, wherein the tokenized banking services further comprise 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 distributed ledger.

10. The system of claim 1, wherein the system provides 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 system of claim 1, wherein the non-repeating random number sequence provides information-theoretic perfect secrecy and quantum-resistant security for all tokens, records, and transactions on the distributed ledger.
12. The system of claim 1, wherein the system supports 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 system of claim 1, further comprising 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 system of claim 1, wherein the issuance process treats 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 system of claim 1, wherein the tokenized banking services further include automated monetization, settlement, and reinvestment of tokenized reserves using the value tokens or deposit tokens on the distributed ledger.
16. The system of claim 1, wherein the system integrates 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 tokenization, deposit token, collateral, payment, OTP zero-trust ledger, TEE, privacy, and RWA/digital twin concepts described in the provisionals. The full set can be incorporated into a non-provisional or continuation application to strengthen the Parisii patent portfolio for tokenized banking and RWA infrastructure.