Independent Claim 2 (Method – Deposit Token Issuance)
A computer-implemented method for issuing deposit tokens in a tokenized banking system, comprising: verifying a user; receiving a deposit of value associated with any physical asset, commodity, digital asset, security, contract, or RWA; minting a deposit token on a distributed ledger using OTP encryption with a unique non-repeating key segment; storing the token as an account balance; and delivering the OTP key securely to the owner while destroying it server-side.

Dependent Claims for Independent Claim 2
The following is a complete set of dependent claims (Claims 2–16) that further specify and narrow the computer-implemented method of Independent Claim 2. 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 KYC/AML verification, deposit issuance and ledger storage processes, OTP zero-trust encryption and key-handling mechanisms, account record formats, primary-market issuance logic, privacy-preserving designs, RWA/digital twin applicability, TEE integration, and secure key distribution features described in the attached document.

Full Claim Set in Formal USPTO-Style Format

1. A computer-implemented method for issuing deposit tokens in a tokenized banking system, comprising: verifying a user; receiving a deposit of value associated with any physical asset, commodity, digital asset, security, contract, or RWA; minting a deposit token on a distributed ledger using OTP encryption with a unique non-repeating key segment; storing the token as an account balance; and delivering the OTP key securely to the owner while destroying it server-side.
2. The method of claim 2, wherein the verifying a user comprises performing a Know Your Customer/Anti-Money Laundering (KYC/AML) verification on the user prior to minting the deposit token.
3. The method of claim 2, 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 method of claim 2, wherein storing the token as an account balance further comprises creating an account record that includes a unique user identifier, a timestamp for sequencing or lookup, and the account balance itself.
5. The method of claim 2, 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 such as a subpoena or warrant.
6. The method of claim 2, wherein the distributed ledger is further configured to store both account balance records and transaction records.
7. The method of claim 2, 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.
8. The method of claim 2, wherein the minting step or the storing step is executed at least in part within a Trusted Execution Environment (TEE) on a computing device.

9. The method of claim 2, wherein delivering the OTP key securely to the owner comprises distributing the key or key segments via one or more of digital channels, physical media, or split-key distribution mechanisms consistent with the zero-trust architecture.
10. The method of claim 2, further comprising destroying the OTP decryption key or key segments on the server side immediately after secure delivery of the key or key segments to the token owner.
11. The method of claim 2, wherein receiving the deposit of value and minting the deposit token are performed as a primary market activity based on validated asset performance, deposit of value, or other asset-backed issuance associated with any physical asset, commodity, digital asset, security, contract, or RWA.
12. The method of claim 2, wherein the deposit token represents a digital twin of any physical asset or commodity and is secured by the OTP encryption using the non-repeating key segment on the distributed ledger.
13. The method of claim 2, further comprising providing full anonymity to the user during daily operations after issuance of the deposit token, with activation of full transaction history occurring only upon a legal requirement.
14. The method of claim 2, wherein the non-repeating random number sequence provides information-theoretic perfect secrecy and quantum-resistant security for the deposit token, the account balance, and all associated records on the distributed ledger.
15. The method of claim 2, further comprising integrating the issued deposit token with tokenized banking services selected from the group consisting of payments, transfers, and use as collateral for loans or other financial arrangements, wherein the integration is recorded on the distributed ledger.
16. The method of claim 2, wherein the method maintains regulatory compliance mechanisms during the user verification step while preserving a privacy-preserving design for all subsequent operations involving the deposit token on the distributed ledger.

These claims form a self-contained, commercially robust claim family that directly maps to the deposit token issuance process, OTP-secured ledger mechanics, privacy features, primary-market token creation, RWA/digital twin coverage, and tokenized banking integration described in the provisionals. The full set can be incorporated into a non-provisional or continuation application (alone or in combination with the claim family of Independent Claim 1) to further strengthen the Parisii patent portfolio for tokenized banking and RWA infrastructure.