Independent Claim 7 (Method – Hybrid TEE + OTP Banking Security)
A computer-implemented method for secure tokenized banking, comprising: executing wallet and payment applications in a Trusted Execution Environment (TEE); combining TEE hardware keys with OTP encryption from a non-repeating sequence to secure value tokens and deposit tokens; and performing deposits, payments, and collateral transactions without exposing sensitive data outside the TEE or owner possession.

Dependent Claims for Independent Claim 7
The following is a complete set of dependent claims (Claims 2–17) that further specify and narrow the computer-implemented method of Independent Claim 7. 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 TEE-based implementation of the Blockchain Secure Wallet and Mining App, hybrid OTP + TEE encryption architecture, secure execution of wallet and payment applications on computing devices, no-exposure of sensitive data (plaintext tokens, keys, or transaction details) outside the TEE or owner possession, integration with deposit tokens/payments/collateral, zero-trust key handling, privacy-preserving designs, quantum-resistant security, and the overall cryptocurrency/financial system business model described in the provisionals.

Full Claim Set in Formal USPTO-Style Format (Reordered to Start with Claim 1)

1. A computer-implemented method for secure tokenized banking, comprising: executing wallet and payment applications in a Trusted Execution Environment (TEE); combining TEE hardware keys with OTP encryption from a non-repeating sequence to secure value tokens and deposit tokens; and performing deposits, payments, and collateral transactions without exposing sensitive data outside the TEE or owner possession.
2. The method of claim 1, wherein the wallet and payment applications are executed on a computing device of a user in the tokenized banking system.
3. The method of claim 1, wherein the Trusted Execution Environment (TEE) complies with a Trusted Execution Environment specification for implementing the Blockchain Secure Wallet and Mining App.
4. The method of claim 1, wherein combining TEE hardware keys with OTP encryption comprises using TEE-derived hardware keys to wrap, protect, or augment OTP key segments derived from the non-repeating sequence.
5. The method of claim 1, wherein performing deposits, payments, and collateral transactions includes issuing, updating, or transferring value tokens and deposit tokens secured by the hybrid TEE-OTP encryption.
6. The method of claim 1, wherein no sensitive data—including plaintext value tokens, deposit tokens, OTP keys, or transaction details—is exposed outside the TEE or the owner's possession during any step of the method.
7. The method of claim 1, further comprising encrypting a payment data packet within the TEE using the combined TEE hardware keys and OTP encryption prior to transmission or recording on a distributed ledger.
8. The method of claim 1, wherein decryption and redemption of any payment packet or tokenized record occurs within the TEE on the recipient's computing device.

9. The method of claim 1, further comprising integrating the hybrid TEE-OTP method with a timestamp-based distributed ledger for immutable recording of all deposits, payments, and collateral transactions while maintaining no exposure of sensitive data.
10. The method of claim 1, wherein the non-repeating random number sequence, when combined with TEE hardware keys, provides information-theoretic perfect secrecy and quantum-resistant security for all value tokens and deposit tokens.
11. The method of claim 1, wherein the value tokens and deposit tokens represent any physical asset, commodity, digital asset, security, contract, or RWA as a digital twin secured by the hybrid TEE-OTP encryption.
12. The method of claim 1, further comprising server-side destruction of OTP decryption key segments immediately after secure delivery to the owner, while all owner-side operations remain within the TEE.
13. 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 such as a subpoena or warrant.
14. The method of claim 1, further comprising performing upstream Know Your Customer/Anti-Money Laundering (KYC/AML) verification while preserving the hybrid TEE-OTP security and privacy-preserving design for all subsequent tokenized banking activities.
15. The method of claim 1, wherein the wallet and payment applications further support secure key distribution mechanisms consistent with the zero-trust architecture of the tokenized banking system.
16. The method of claim 1, wherein the hybrid TEE-OTP method enables the creation and use of new financial instruments based on tokenized assets without exposing sensitive data outside the TEE or owner possession.
17. The method of claim 1, wherein the method merges existing asset instruments with cryptocurrency instruments on the same distributed ledger while executing all secure operations under the hybrid TEE-OTP architecture.

These claims form a self-contained, commercially robust claim family that directly maps to the hybrid TEE + OTP secure tokenized banking method, TEE wallet/payment application execution, key-combination mechanisms, no-data-exposure guarantees, and integration with deposits, payments, collateral, and RWA/digital twin coverage 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 1–6) to further strengthen the Parisii patent portfolio for tokenized banking and RWA infrastructure.