Independent Claim 3 (Method – Tokenized Payments and Transfers)
A computer-implemented method for tokenized payments and transfers in a banking system, comprising: encrypting a payment packet containing a value token or deposit token using OTP with a non-repeating key segment; recording the encrypted packet on a timestamp-based distributed ledger; notifying the recipient with the timestamp and key; and allowing decryption and redemption with immutable ledger update of ownership.

Dependent Claims for Independent Claim 3
The following is a complete set of dependent claims (Claims 2–16) that further specify and narrow the computer-implemented method of Independent Claim 3. 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 payment flows using OTP-encrypted "payment data packet[s]", timestamp-based ledger recording and lookup, recipient notification with timestamp and key information, TEE-based decryption and redemption, immutable ownership/balance updates, zero-trust key handling, privacy-preserving designs, integration with previously issued value tokens or deposit tokens, and applicability to any physical asset, commodity, digital asset, security, contract, or RWA as a digital twin.

Full Claim Set in Formal USPTO-Style Format

1. A computer-implemented method for tokenized payments and transfers in a banking system, comprising: encrypting a payment packet containing a value token or deposit token using OTP with a non-repeating key segment; recording the encrypted packet on a timestamp-based distributed ledger; notifying the recipient with the timestamp and key; and allowing decryption and redemption with immutable ledger update of ownership.
2. The method of claim 3, wherein the payment packet is created from a value token or deposit token previously issued via the tokenized banking system's issuance process after user verification.
3. The method of claim 3, wherein encrypting the payment packet is performed within a Trusted Execution Environment (TEE) on the sender's computing device.
4. The method of claim 3, wherein the recipient decrypts and redeems the payment packet within a Trusted Execution Environment (TEE) on the recipient's computing device.
5. The method of claim 3, wherein notifying the recipient further comprises providing a timestamp and size lookup for locating the encrypted packet on the distributed ledger.
6. The method of claim 3, further comprising destroying the OTP decryption key or key segments on the server side immediately after notification to the recipient.
7. The method of claim 3, wherein the immutable ledger update of ownership comprises updating account balance records for both the sender and the recipient on the distributed ledger.
8. The method of claim 3, wherein the distributed ledger is configured to store only account balance records by default and does not record individual transaction details unless activated by a legal requirement such as a subpoena or warrant.

9. The method of claim 3, wherein the distributed ledger is further configured to store both account balance records and transaction records.
10. The method of claim 3, 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.
11. The method of claim 3, wherein the method provides full anonymity to the sender and recipient during the payment and transfer process, with activation of full transaction history occurring only upon a legal requirement.
12. The method of claim 3, wherein the non-repeating random number sequence provides information-theoretic perfect secrecy and quantum-resistant security for the payment packet and the corresponding ledger record.
13. The method of claim 3, wherein the payment packet contains data representing any physical asset, commodity, digital asset, security, contract, or RWA as a digital twin secured by the OTP encryption.
14. The method of claim 3, further comprising integrating the tokenized payment or transfer with other tokenized banking services selected from the group consisting of collateralization for loans, settlements, and reinvestment of reserves, wherein the integration is recorded on the distributed ledger.
15. The method of claim 3, wherein the timestamp-based distributed ledger ensures proper sequencing and lookup of the encrypted payment packet without exposing plaintext data outside the TEE or owner possession.
16. The method of claim 3, wherein the method maintains regulatory compliance mechanisms through upstream user verification while preserving privacy-preserving end-to-end OTP encryption for the entire payment and transfer flow.

These claims form a self-contained, commercially robust claim family that directly maps to the tokenized payment and transfer processes, OTP-secured “payment data packet” handling, timestamp-based ledger mechanics, TEE integration, privacy features, and RWA/digital twin coverage 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 and 2) to further strengthen the Parisii patent portfolio for tokenized banking and RWA infrastructure.