CLAIMS

1. A system for programmable video assembly, comprising:

- a virtualization engine, wherein the engine is configured to convert a rendered video file into a reference container by extracting metadata and removing media sample data;

- a token issuance service, wherein the service configured to generate a cryptographic video token binding transaction, consent, and licensing information;

- a secure resolution service, wherein the service dereferences remote media data upon successful validation of the cryptographic video token; and

- a playback environment, wherein the playback environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references.

2. The system of claim 1, wherein the playback environment is configured to manage independent tokens from multiple content owners within a single session.

3. The system of claim 1, wherein the playback environment may function as a content wallet capable of managing multiple tokens from independent content owners.

4. The system of claim 1, further comprising an artificial intelligence orchestration layer configured to modify the sequencing instructions of the reference container without accessing raw media samples.

5. The system of claim 1, wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment.

6. The system of claim 1, wherein the token issuance service includes a unique session nonce in each generated token to prevent unauthorized resolution reuse.

7. The system of claim 1, wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.

8. A computer-implemented method for tokenized virtual video delivery, comprising the steps of;

- accessing a rendered digital video file and interrogating its structure to identify media sample tables and timing metadata;
- generating a virtual video container by removing media sample data and replacing it with encrypted reference links to remote media data sources;
- generating a cryptographic video token at the time of an access request, comprising a virtual video container identifier, user consent parameters, licensing terms, and specific execution constraints
- validating the cryptographic video token against at least one authorisation policy;
- resolving referenced media data only upon successful validation of the token; and
- assembling a playable video stream dynamically in volatile memory without creating a persistent rendered video file.

9. The method of claim 8, wherein user consent parameters define specific permitted content classes and personalization branches that may be resolved during runtime assembly.

10. The method of claim 8, wherein the cryptographic video token further comprises a hardware attestation component configured to prove execution within a verified trusted environment.

11. The method of claim 8, further comprising logging each individual media dereference event to an auditable transaction layer.

12. The method of claim 11, wherein the logged dereference events trigger a commercial action selected from a group consisting of billing, royalty allocation, and advertising insertion.

13. The method of claim 8, wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data.

14. The method of claim 8, wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources.

15. A cryptographic video token for governing virtual media resolution, comprising:

- a reference container identifier, wherein the identifier binds bind the cryptographic video token to a virtual video container;
- plurality of consent attributes, wherein the attributes define permitted purposes and functional constraints for content assembly;
- plurality of licensing attributes, wherein the attributes establish rights-based parameters and ownership constraints for the associated media;
- transaction metadata including settlement instructions for recording resolution-based commercial events; and
- at least one session-specific unique identifier, wherein the identifier prevent unauthorized reuse of the resolution authority.

16. The token of claim 15, wherein the transaction metadata includes instructions for micro-payments triggered by individual segment resolution events.

17. The token of claim 15, wherein the user consent attributes are configured to be interrogated at the moment of each media reference resolution.

18. The token of claim 15, wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the necessary cryptographic permissions and binds governance logic to the resolution event.