TOKENISED VIRTUAL VIDEO DELIVERY SYSTEM AND METHOD

TECHNICAL FIELD

[0001] The present disclosure relates to the field of digital video virtualization. Specifically, the present invention relates to a system and method for controlling the resolution authority of virtualized video containers using cryptographic tokens to enable secure, non-rendered, and programmable video assembly.

BACKGROUND

[0002] The current digital landscape is characterized by a fundamental disconnect between advanced computational intelligence and the structural limitations of digital video formats.

[0003] Digital video represents approximately 82 percent of global internet traffic, forming the largest repository of human knowledge and creativity ever assembled. Despite its dominance, video remains largely trapped within static, rendered file formats designed primarily for distribution rather than intelligent manipulation.

[0004] Traditional video systems rely on these rendered files to deliver content, which forces platforms to maintain vast libraries of finished, immutable objects. Even the most advanced Artificial Intelligence (AI) platforms, while capable of indexing data and understanding context, are severely limited when interacting with these files.

[0005] While Artificial Intelligence can analyze video to identify specific moments or identify timestamps, it cannot yet compose video with the same fluidity that it composes text.

[0006] To act on intelligence extracted from a video, existing systems are forced to edit and render entirely new video files. This dependency on re-rendering introduces significant global inefficiencies across storage, workflow complexity, and Rights Management.

[0007] For consumers, this translates to measurable friction; up to 30% of viewing time on social platforms is spent searching for content within static libraries rather than receiving content shaped around individual intent.

[0008] Earlier technological advancements established that video could be separated from its physical file. They cover the virtualization of rendered video into reference-based containers that contain no actual video or audio sample data, allowing video to be indexed, linked, and reassembled dynamically without re-rendering.

[0009] However, these systems focused primarily on the mechanics of assembly rather than the governance of access.

[0010] US Patent No 9918134 B2 recites of a method and system for providing video content on a data network connected device having a display and a device display controller including a player. T It focuses on the mechanics of assembly via reference files and linking data and does not disclose a cryptographic video token that binds container identity with dynamic user consent parameters, licensing constraints, and transaction metadata.

[0011] The document is silent and does not teach a separate control layer that governs whether reference resolution is permitted at all at the moment of execution.

[0012] A critical gap exists in the control layer of virtualized video: specifically, the governance of whether reference resolution, the act of connecting a reference to its underlying media sample is

permitted at all at runtime. In a virtualized environment where the container holds no sample data, the true value of the asset shifts from the file itself to the specific right to resolve those references.

[0013] Currently, there is no standardized, method to package, enforce, or monetize this resolution rights.

[0014] Traditional Digital Rights Management (DRM) and streaming access tokens are insufficient for this purpose, as they focus on protecting the delivery of entire files or streams rather than binding authorization logic directly to individual virtualized video elements.

[0015] Further, the lack of fine-grained control prevents content owners from maintaining sovereignty over their assets while still allowing third-party AI systems to innovate. Without a dedicated control layer, the transition of video from a static distribution object to an intelligent, data-driven object remains restricted by the inability to decouple authorization from the delivery layer.

[0016] Moreover, the exiting systems lack the necessary consent mechanisms required for modern privacy and compliance standards.

[0017] The rise of AI agents further highlights this structural problem. These agents require the ability to orchestrate personalized video experiences on behalf of users by drawing from disparate indexed data streams.

[0018] The exiting models, such orchestration requires constant re-rendering and duplication of media assets, leading to unsustainable storage and processing costs.

[0019] A structural gap remains between AI systems that excel at understanding context and digital video systems that remain locked in distribution-only formats.

[0020] In view of the above drawbacks, there exists a need for a system that can instantly stop the resolution of specific video moments if user permission is revoked.

[0021] A new infrastructure layer is required to turn resolution rights into cryptographic artifacts. These artifacts must be capable of being managed within digital wallets, ensuring that only authorized binary samples ever leave a content owner's environment. By replacing rendering with token-governed resolution, video can be assembled dynamically at runtime under explicit, enforceable control.

[0022] Any discussion of the prior art throughout the specification should in no way be considered as an admission that such prior art is widely known or forms part of common general knowledge in the field.

SUMMARY OF THE INVENTION

PROBLEMS TO BE SOLVED

[0023] It may be an advantage to develop a to system and method for controlling the resolution authority of virtualized video containers using cryptographic tokens

[0024] It may be an advantage to develop a control layer for virtualized video that governs the specific right to resolve references into playable media, rather than merely protecting access to a static file container.

[0025] It may be an advantage to develop a method to remove the necessity for re-rendering entire video files when performing contextual edits or personalization, reducing global storage and computational overhead.

[0026] It may be an advantage to develop an infrastructure that allows Artificial Intelligence (AI) systems to treat video as dynamic, modular data, similar to text, rather than immutable rendered objects.

[0027] It may be an advantage to develop a content wallet environment that manages resolution authority via cryptographic tokens

[0028] It may be an advantage to develop an enforceable consent mechanism that is checked at the moment of reference resolution, ensuring that if a user revokes consent, access to specific video moments is terminated instantly at runtime.

[0029] It may be an advantage to develop an auditable transaction layer that logs individual dereferences events, enabling precise monetisation of specific video moments or edits

[0030] It may be an advantage to develop a secure resolution service that can be restricted to trusted execution environments (TEE) or hardware-attested states, ensuring that high-value media references are only resolved on authorized devices.

[0031] It may be an advantage to develop a system that reduces the search friction experienced by consumers by allowing AI agents to dynamically assemble programs shaped around individual intent.

[0032] It may be an advantage to develop a cryptographic video token that binds container identity, transaction data, and execution constraints into a single machine-readable artifact to prevent unauthorized dereferencing of virtualized assets.

[0033] It may be an advantage to develop a method for AI systems to analyze and modify video sequencing instructions within a virtual container without ever requiring access to the raw, underlying media sample data.

[0034] It may be an advantage to develop a technical solution to the structural gap between the context-indexing capabilities of AI and the rigid distribution formats of modern digital video systems.

[0035] It may be an advantage to develop a system that is fully compatible with existing ISO base media file format structures while introducing non-rendered, programmable assembly layers.

[0036] It may be an advantage to develop a platform where content owners can package resolution rights as licensed, revokable, and monetizable assets independent of the original video distribution platform.

MEANS FOR SOLVING THE PROBLEM

[0037] The present invention is directed to a computer-implemented method for tokenized virtual video delivery and system for programmable video assembly using cryptographic tokens.

[0038] In an aspect of the present invention, a system for programmable video assembly is disclosed. The system includes a virtualization engine configured to convert rendered video files into reference containers; token issuance service integrated into the system to generate cryptographic video tokens; a secure resolution service configured to dereference media data only upon successful validation of the cryptographic video tokens; a playback environment to assemble a video stream from the dereferenced media data in real time.

[0039] In another aspect of the present invention, a computer-implemented method for tokenized virtual video delivery is provided. The method comprises the steps of accessing a digital video file and interrogating its structure to identify media sample tables and timing metadata; generating a virtual video container by removing the 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 token against one or more authorization policies; resolving the referenced media data and facilitating the dynamic assembly of a playable video stream without the creation of a new rendered video file.

[0040] In a further aspect of the present invention, a cryptographic video token is provided as a distinct technical artifact, serving as a gatekeeper for resolution authority. The token comprises a reference container identifier, one or more user consent attributes, and one or more licensing attributes.

[0041] Preferably, the system separates the video into three layers namely, a cybersecurity layer for content owners, a consent and compliance layer for personalised and AI shaped video, and a transaction layer where moments that matter can be monetised without needing to edit the video.

[0042] Preferably, token includes transaction metadata, a session-specific unique identifier or nonce, and execution constraints that limit the scope of the resolution.

[0043] Preferably, the cryptographic video token is configured to authorize the dereferencing of remote media data referenced by a virtual video container only when defined conditions are met.

[0044] Preferably, the token binds authorization and transaction logic directly to the virtualized video layer, allowing the right to resolve references to be packaged, enforced, and monetized independently of the underlying media samples.

[0045] Preferably, the cryptographic video token may include a hardware attestation component for proving execution within a trusted environment.

[0046] Preferably, the user consent attributes specify permitted content classes, personalisation logic, and data usage scope.

[0047] Preferably, the token may expire after a defined temporal or transactional condition.

[0048] Preferably, media data is delivered via range requests defined by an ISO base media file format box.

[0049] Preferably, resolution events may be logged without exposing personally identifiable information.

[0050] Preferably, artificial intelligence systems may generate or modify virtual video containers without accessing underlying media sample data.

[0051] The foregoing general description of the illustrative embodiments and the following detailed description thereof are merely exemplary aspects of the teachings of this disclosure and are not restrictive.

BRIEF DESCRIPTION OF THE FIGURES

[0052] Embodiments of the present disclosure will be discussed with reference to the accompanying figures wherein:

FIG. 1 illustrates an architectural diagram showing token-governed resolution of virtual video;

FIG. 2 depicts the conversion process of a rendered video file into a reference-based virtual video container;

FIG. 3 illustrates the data structure of a cryptographic video token, highlighting its various governance attributes;

FIG. 4 is a flow diagram illustrating the runtime resolution process controlled by a cryptographic video token;

FIG. 5 illustrates a flow diagram that demonstrates the enforcement of user consent as a functional constraint during the reference resolution phase;

FIG. 6 illustrates the playback environment mechanism configured to function as a digital content wallet;

FIG. 7 illustrates the interaction between an artificial intelligence (AI) system and virtual video containers;

FIG. 8 illustrates a view of the system where token validation is restricted to a trusted execution environment (TEE);

FIG. 9 illustrates a transactional and monetization process featuring tokens with settlement attributes; and

FIG. 10 provides a view of the end-to-end lifecycle for token-governed virtual video execution.

DESCRIPTION OF THE INVENTION

[0053] The reference to any prior art in this specification is not, and should not be taken as, an acknowledgement or any form of suggestion that such prior art forms part of the common general knowledge.

[0054] It will be understood that the terms “comprise” and “include” and any of their derivatives (e.g. comprises, comprising, includes, including) as used in this specification, and the claims that follow,

is to be taken to be inclusive of features to which the term refers, and is not meant to exclude the presence of any additional features unless otherwise stated or implied.

[0055] In some cases, a single embodiment may, for succinctness and/or to assist in understanding the scope of the disclosure, combine multiple features. It is to be understood that in such a case, these multiple features may be provided separately (in separate embodiments), or in any other suitable combination. Alternatively, where separate features are described in separate embodiments, these separate features may be combined into a single embodiment unless otherwise stated or implied. This also applies to the claims which can be recombined in any combination. That is a claim may be amended to include a feature defined in any other claim. Further a phrase referring to "at least one of" a list of items refers to any combination of those items, including single members. As an example, "at least one of: a, b, or c" is intended to cover: a, b, c, a-b, a-c, b-c, and a-b-c.

[0056] As used herein, the term virtual video container is a reference-based video structure derived from a rendered video file, where all video and audio sample data has been removed.

[0057] As used herein, the term resolution authority is the explicit permission to turn a virtual video into something that can actually be played.

[0058] As used herein the term cryptographic video token is a machine readable, cryptographically protected object that explicitly grants resolution authority for a virtual video container under defined conditions.

[0059] The present invention relates to a computer-implemented method for tokenized virtual video delivery and system for programmable video assembly using cryptographic tokens.

[0060] The goal of the present invention is to establish a cryptographic control layer for virtualized video that governs the specific right to resolve references into playable media at runtime. By binding

resolution authority, user consent, and transaction logic into a secure video token, the invention enables AI agents to dynamically assemble personalized content within a content wallet environment. This shift from file-based access to token-governed resolution ensures content owner sovereignty while allowing video moments to be securely monetized and audited without re-rendering.

[0061] The present system and method offer a solution to the structural gap between the context-indexing capabilities of AI and the rigid distribution formats of modern digital video systems.

[0062] The computer-implemented method for tokenized virtual video delivery is provided. The method comprises the steps of accessing a digital video file and interrogating its structure to identify media sample tables and timing metadata; generating a virtual video container by removing the 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 token against one or more authorization policies; resolving the referenced media data and facilitating the dynamic assembly of a playable video stream without the creation of a new rendered video file.

[0063] Step 1: Rendered Video Virtualization. The method commences with the ingestion of a conventional rendered digital video file. The system interrogates the file's internal structure, specifically identifying and extracting ISO Base Media File atoms, including but not limited to moov, trak, stbl, and mdat. During this stage, media sample data blocks are removed while the sample tables are retained and rewritten to reference secure external storage locations. The resulting output is a virtual video container that contains the necessary structural instructions but is devoid of actual video or audio sample data.

[0064] Step 2: Transaction Initiation. A token requestor initiates a request to access the virtualized video content. The requestor may be a user device, an Artificial Intelligence (AI) agent, a platform

service, an enterprise system, or a dedicated personal content wallet. This request triggers the verification of the requestor’s identity and the intended use case for the content.

[0065] Step 3: Video Token Issuance. Upon approval of the request, a token service generates a cryptographic video token. This token serves as a technical artifact that binds the virtual video container ID with specific licensing terms, user consent parameters, transaction data, and a unique session identifier (UUID) or nonce. Critically, the token contains neither media data nor direct URLs; it represents the resolution authority required to bridge the virtual container to the physical media payload.

[0066] Step 4: Token Validation and Decryption. The token is submitted by the playback or assembly environment to a policy engine for validation. This engine evaluates the token against real-time constraints, including user consent, licensing validity, jurisdictional restrictions, and the specific execution context. Upon successful validation, the token is decrypted to expose the resolution permissions required for the next phase.

[0067] Step 5: Virtual Video Exposure. Once authorized, the virtual video container is exposed to the playback engine. The rewritten sample tables begin to resolve through a process of token-governed dereferencing. The system issues dynamic MDAT range requests to retrieve the authorized sample ranges from external storage. This media data is streamed directly into the system's volatile memory for immediate processing.

[0068] Step 6: Runtime Assembly. The video is assembled in real time within the playback environment. Because the process occurs dynamically, no permanent rendered output file is created on the device. Personalization logic may be applied at this stage to select alternative references based on user intent, and AI systems may adjust the sequencing of scenes without requiring modifications to the underlying source media.

[0069] Step 7: Audit and Settlement. To ensure accountability and compliance, every individual dereference event is logged. Based on these logs, settlement tokens may be generated for automated billing, royalty distribution, or granular analytics. Continuous consent enforcement is maintained throughout this stage, ensuring that resolution ceases immediately if the governing token expires or permissions are withdrawn.

[0070] The system includes a virtualization engine configured to convert rendered video files into reference containers; token issuance service integrated into the system to generate cryptographic video tokens; a secure resolution service configured to dereference media data only upon successful validation of the cryptographic video tokens; a playback environment to assemble a video stream from the dereferenced media data in real time.

[0071] In the system , there includes cryptographic video token provided as a distinct technical artifact, comprises a reference container identifier, one or more user consent attributes, and one or more licensing attributes.

[0072] The system separates the video into three layers namely, a cybersecurity layer for content owners, a consent and compliance layer for personalised and AI shaped video, and a transaction layer where moments that matter can be monetised without needing to edit the video.

[0073] FIG. 1 illustrates a system architecture designed for the token-governed resolution of virtual video.

[0074] The architecture is anchored by a virtual video container 100 which acts as a reference-based structure containing no actual media sample data, but instead utilizing reference pointers 102 to identify media sample locations stored externally to the container. When an access attempt is initiated via a reference request, the cryptographic video token issuance service 120 generates a secure technical artifact that binds the identity of the container with granular governance data, such as

licensing and user consent. This token is then processed by a suite of policy and validation engines, which evaluate the request against specific authorization policies and execution constraints to ensure the validity of the session.

[0075] Upon successful verification by these engines, a token validation signal is transmitted to the resolution service 140.

[0076] The resolution service 140 functions as a secure gatekeeper that permits the dereferencing of media sample locations only when a valid token is presented. Once the token is validated, the service facilitates a resolved stream by connecting the virtual references to the underlying media payload, which is then delivered to one of several playback environments 150, such as a user device or a media platform.

[0077] Within these playback environments 150, the video is dynamically assembled in volatile memory using the authorized media samples, ensuring that a complete rendered video file is never stored locally or duplicated.

[0078] FIG. 2 illustrates the technical process for converting a conventional rendered video 200 file into a specialized virtual video container 205. The virtualization engine performs a destructive extraction whereby the underlying media sample data, consisting of the actual binary video and audio sample is removed from the original file. This separation ensures that the physical payload is decoupled from the control logic, leaving the original rendered file as a lightweight shell.

[0079] While the sample data is discarded, the system retains and incorporates critical structural elements into the virtual video container 205, timing metadata, sequencing instructions, and reference pointers.

[0080] The timing metadata and sequencing instructions provide the temporal framework necessary for reassembly, while the reference pointers identify the secure external storage locations where the media samples now reside. Because all playable media data has been removed, the resulting virtual video container 205 is an inert reference-based structure that cannot produce video output independently of the token-governed resolution process.

[0081] FIG. 3 illustrates the exemplary structure of a cryptographic video token 300, which serves as the primary authorization artifact for governing access to virtualized media.

[0082] The cryptographic video token 300 acts as a secure container that binds several critical governance elements together, including a virtual video container identifier, user consent parameters, licensing constraints, transaction metadata, session identifiers or a nonce, and specific execution constraints.

[0083] The architecture of the cryptographic video token 300 is designed for security and privacy; it explicitly does not contain media sample data or direct access paths or URLs to the underlying storage.

[0084] By isolating these sensitive resolution elements from the token itself, the system ensures that the token functions solely as a gatekeeper of resolution authority rather than a direct delivery vehicle for content.

[0085] FIG. 4 illustrates a runtime resolution flow managed by the cryptographic video token to control access to virtualized media.

[0086] The process initiates when a request to access is issued from a virtual video container 400 toward the cryptographic video token which may be provided by a cryptographic video token

issuance service 420. This request triggers a token validation check to determine if the presented token is valid.

[0087] If the validation engine returns a YES , it indicates the token validity period is active and session constraint success has been achieved, which results in a permit for media dereference.

[0088] Conversely, if the result is NO the token is considered invalid or expired, leading to a consent constraint failure where media access is denied.

[0089] Only upon successful validation does the system permit resolution, allowing the reference to be resolved and the subsequent media dereference 440 to occur.

[0090] FIG. 5 illustrates the flow digaram for consent enforced at reference resolution, wherein user consent acts as a primary functional constraint on the assembly of virtualized content.

[0091] The process is governed by a cryptographic video token 500, which carries or is associated with specific consent parameters 510 that define the operational boundaries for the session. These parameters 510 specifically define permissible reference classes, authorized personalized branches, and the application of data-driven logic during the resolution phase.

[0092] The figure demonstrates how these parameters 510)dictate the availability of different media components:

[0093] Segment A and Segment B are designated as unconditionally capable, meaning they are resolved without additional logic gates once the primary token is validated.

[0094] Complex resolution paths are managed via logic tags; for instance, TAG 1 and TAG 2 act as conditional checkpoints to authorize specific content paths such as Branch B2, which is designated as personalization capable.

[0095] The final output of this governed process results in resolved virtual video containers 540, which may consist of a sequence of authorized elements such as Segment A, Branch B1, and Segment C.

[0096] By embedding these constraints within the cryptographic video token 500, the system ensures that the assembly of the final video stream is strictly aligned with the user's current consent state at the moment of runtime resolution.

[0097] FIG. 6 illusrates the playback environment mechanism configured to operate as a content wallet.

[0098] The process begins externally when a request to access virtual video is submitted to the playback environment. This request must be accompanied by a cryptographic video token, which acts as the machine-readable "key" containing the necessary resolution authority.

[0099] Within the content wallet playback environment, the system directs the incoming token to an internal module containing tokens and a validation engine. This engine interprets the cryptographic attributes of the token, such as user consent, licensing, and execution constraint to determine if the requested resolution is permitted in the current context. Upon successful validation, the environment initiates the process of handling dereferenced media samples. The system utilizes reference pointers to identify the specific locations of remote media data. It is a critical feature of this embodiment that the virtual container contains no sample data itself, relying entirely on these pointers to locate the payload.

[00100] Once the references are resolved, the system performs a temporary assembly of the virtual video stream. Unlike traditional players that download a whole file, this environment ensures that the

video is dynamically assembled in memory. This means media samples are fetched and sequenced on-the-fly, existing only in the device's volatile memory during the playback session.

[00101] The final video stream playback is then output to the user's hardware. The figure illustrates that a single content wallet can manage and deliver these dynamic streams to a variety of interconnected devices, including smart televisions, mobile phones, and wearable technology.

[00102] FIG. 7 illustrates the interaction between an Artificial Intelligence (AI) system (700) and a virtual video container 710, highlighting a modular architecture where analysis is decoupled from content resolution.

[00103] The AI system 700 which may function as an orchestration agent or metadata processor interacts with the virtual video container 710 by accessing only reference data.

[00104] A critical technical distinction is that this interaction involves no sample data, as the AI system 700 performs its analysis and sequencing tasks solely on the reference pointers and timing & sequence data contained within the container.

[00105] Firstly, the AI system 700 analyzes the virtual structure to identify in-scene events or to generate new personalized sequencing instructions. While the AI can manipulate these virtual instructions within an execution environment 730, it remains unable to resolve the references into playable media independently.

[00106] Secondly, to facilitate actual video assembly or playback, the AI system 700 must issue a request for a cryptographic video token. This ensures that resolution authority is governed independently of the AI's analysis layer, requiring a validated token to bridge the gap between virtual instructions and the physical media payload.

[00107] This architecture allows AI to treat video as malleable data while strictly maintaining the content owner’s security and sovereignty.

[00108] FIG. 8 illustrates a flow diagram of the hardware or trusted execution enforcement, wherein the validation of a cryptographic video token is coupled with a verified hardware state.

[00109] In this configuration, the security of the resolution authority is elevated from a software-only check to a hardware-rooted requirement, ensuring that high-value or sensitive media references are only resolved on authorized and secure devices.

[00110] The process initiates when a cryptographic video token is submitted as a token validation request to a Trusted Execution Environment (TEE) 810. This request serves as the trigger for the system to verify that both the token and the physical environment meet the required security standards.

[00111] The TEE 810 functions as a secure, isolated area within a processor that performs hardware-level checks, including hardware attestation and secure execution verification.

[00112] For the validation to succeed, the system must confirm that specific hardware requirements are met and that the associated validation services are certified as genuine and untampered.

[00113] Once the TEE 810 completes its interrogation of the hardware and the token, it issues a token validation response to the playback/resolution environment. If the attestation is successful, resolution authority is granted, allowing the device to begin dereferencing the media samples for dynamic assembly.

[00114] Next is the restricted resolution that ensures that if the playback environment fails to satisfy the hardware attestation or secure execution requirements, resolution is denied, and no video data is accessed, even if the user possesses a virtual video container.

[00115] FIG. 9 illustrates the transactional and monetization of the wherein cryptographic video tokens 900 that are utilized to drive commercial actions and financial settlements based on discrete resolution events.

[00116] This shifts monetization away from traditional coarse playback metrics (such as total view time) toward a more granular, event-driven system tied to the specific assembly of virtualized video elements.

[00117] The process is triggered when a cryptographic video token 900 is presented to authorize the assembly of a virtual video container. As the system resolves references into playable media, it generates specific resolution events. These events represent the precise moment a media sample is authorized and retrieved for assembly.

[00118] These resolution events are captured and processed by a content wallet, which functions as a resolver and a compliance enforcement fence.

[00119] The content wallet acts as a trusted reporting environment that logs each dereference event, ensuring that the commercial data derived from these events is accurate and authorized by the governing token.

[00120] The captured resolution events trigger a variety of automated commercial actions. These include billing or payment settlement for the end-user or requestor, the calculation of royalty or revenue allocation for multiple content owners, and specific advertising attribution or insertion based on which references were resolved.

[00121] The last stage of the process is the creation of a settlement disbursement data record. This record serves as an auditable, machine-readable log of all transactions and commercial actions triggered during the session. It allows for complex financial settlements, such as micro-payments for individual video moment to be processed without the need for manual reporting or traditional file-level tracking.

[00122] By integrating settlement attributes directly into the cryptographic video token 900, the system enables content owners to package and monetize the right to resolve their content as a liquid, programmable asset.

[00123] FIG. 10 illustrates the end-to-end lifecycle of token-governed virtual video execution, tracing the technical progression from initial asset virtualization to final transactional recording.

[00124] The operational lifecycle depicted in FIG. 10 comprises the following sequential steps

[00125] Step 1: The process begins with a conventional rendered video 100 which is ingested for virtualization. In this phase, the system separates the media payload from its structural metadata, resulting in a virtualized container that contains only references and instructions.

[00126] Step 2: Following virtualization, the system performs the issuance of token phase. This generates the cryptographic video token 300, which acts as the session-specific gatekeeper. This token binds the virtualized asset to specific licensing, consent, and execution parameters.

[00127] Step 3: The cryptographic video token 300 is then submitted to a validation service for the validation of authority. During this stage, the system ensures all conditions defined within the token are met before permitting access to the underlying media references.

[00128] Step 4: Upon successful validation, the system enters the resolution of media phase. Here, the "resolution of" command is executed, allowing the virtual references to point toward physical media samples stored in secure, remote locations.

[00129] Step 5: This phase facilitates the runtime dereference of media 440. Media samples are retrieved in real-time and dynamically assembled in volatile memory to create the final video stream for playback on an end-user device.

[00130] Step 6: The final phase involves the audit/settlement event recording. Every resolution event is captured and stored as audit/settlement records 950. These records enable granular billing, royalty distribution, and compliance tracking, closing the loop on the transactional lifecycle.

[00131] In one or more embodiments, the cryptographic video token functions as a machine-readable artifact comprising a plurality of governing attributes. These attributes include, but are not limited to, a virtual video container identifier, user consent parameters defining permitted purposes, licensing and rights constraints, and transaction metadata associated with the specific access request.

[00132] Additionally, the token incorporates session-specific identifiers or nonces and execution constraints such as temporal limits, device specifications, geographic location, or environmental requirements.

[00133] Notably, the token is characterized by the absence of media sample data, direct URLs, or file paths, as it represents a specific grant of resolution authority rather than a permission to download or copy a static file.

[00134] In the present system, user consent is implemented as a primary constraint enforced at the moment video data is utilized, rather than merely at the initiation of playback. While a virtual video

container may exist independently, consent parameters determine whether its internal references are permitted to connect to actual media data during execution.

[00135] These settings govern the specific parts of the video allowed for use, the authorization of personalized assembly, the inclusion of commercial elements, and the degree to which Artificial Intelligence (AI) systems may influence assembly. Should consent be withdrawn, the system immediately ceases reference resolution, ensuring that no further video data can be accessed or assembled even if the container remains on the device.

[00136] Rather than loading and playing monolithic video files, the content wallet manages multiple cryptographic video tokens to determine if video data is authorized for access and assembly.

[00137] Specifically, the wallet stores and reads tokens, verifies resolution authority prior to media access, and dynamically assembles video from authorized references in real-time.

[00138] In some embodiments, the transactional framework enables advanced forms of monetization and validation that are driven by cryptographically validated resolution events rather than coarse playback metrics. This approach allows for billing models based on the individual video moments or segments that are actually resolved and assembled during a session. Furthermore, the system can enable or restrict advertising insertion at specific reference points and trigger dynamic commercial or branded overlays during authorized execution. Content owners can also utilize the system for allocating royalties or revenue shares based on the specific references resolved at runtime. Finally, where user consent permits, the platform facilitates the validation of audience engagement or behavioral signals to drive high-fidelity personalization.

[00139] It will be appreciated by those skilled in the art that the disclosure is not restricted in its use to the particular application or applications described. Neither is the present disclosure restricted in

its preferred embodiment with regard to the particular elements and/or features described or depicted herein. It will be appreciated that the disclosure is not limited to the embodiment or embodiments disclosed, but is capable of numerous rearrangements, modifications and substitutions without departing from the scope as set forth and defined by the following claims.

[00140] Please note that the following claims are provisional claims only, and are provided as examples of possible claims and are not intended to limit the scope of what may be claimed in any future patent applications based on the present application. Integers may be added to or omitted from the example claims at a later date so as to further define or re-define the scope.