ENTERTAINMENT TECHNOLOGY CENTER

Consortium Shared Identity (CSI) over an Enterprise Blockchain

A Technical White Paper

ETC Adaptive Production Blockchain Working Group

October 2019

Abstract

The current onboarding and offboarding processes for production crews involve a set of often inconsistent and manual activities, which are repetitive and inefficient, leading to various issues such as longer delays in bringing people on to a production project, inconsistent permission enforcement when a project is over, and higher overall cost. Consortium Shared Identify (CSI) is intended to leverage a cryptographically protected private blockchain network to create a secure, shared, and decentralized identity system for all consortium members to onboard and offboard production crew. The identity owners (contract users) maintain full control of their own identity and decide what information to share, with whom to share with, and for how long to share their identities with the network. They have the right to revoke any and all sharing of their identities. CSI provides governance and full audit capabilities for all identity-related transactions

through blockchain smart contracts. CSI will enhance efficiencies of the identity checking and accelerate the crew onboarding and offboarding processes.

Contents

Executive Summary

The current crew onboarding process used by various production companies is often laborious and sometimes lengthy as it involves many manual touchpoints and inconsistent processes. Because the onboarding is done independently, some of the work results in duplication of effort. Additionally, there is no validation of the crew list performed by the studios— or, at times, the production already has their own admin-level access, thus bypassing the HR entirely. The offboarding process can also be described as inconsistent, and there is very little validation that access to sensitive tools and assets is properly terminated once a production is complete.

Consortium Shared Identity (CSI) is a novel solution to address inefficiencies and risks in the current onboarding and offboarding of contract workers in the entertainment industry. CSI leverages the unique features brought by blockchain to create a single source of truth for contract worker identity that is shared by the consortium. A private and enterprise-grade blockchain will be used to protect the network and data. Because of the tamper-proof, decentralized, and distributed features, the blockchain provides CSI the capability of immutable tracking, consortium consensus, efficiency, and reliability. Blockchain smart contracts are software code instantiated on the blockchain to allow controlled interactions with the identity attributes. Every such interaction or transaction is tracked immutably.

Privacy protection is paramount for any identity systems. CSI distinguishes two types of identity attributes: internal identity attributes (IIA) and external identity attributes (EIA). IIAs are inherent identity attributes belonging to an identity owner, such as name, birthday, or driver's license number. These attributes are fully under the control of the owner including when to share, who to share with, and for how long will they be shared. The owner can revoke sharing of the IIAs at any time. EIAs are attributes assigned by the consortium member entities to track external evidence for onboarding and offboarding, including identity attestation results. Consortium members control these attributes and can share them on the blockchain. Identity attestation is done using the approach of

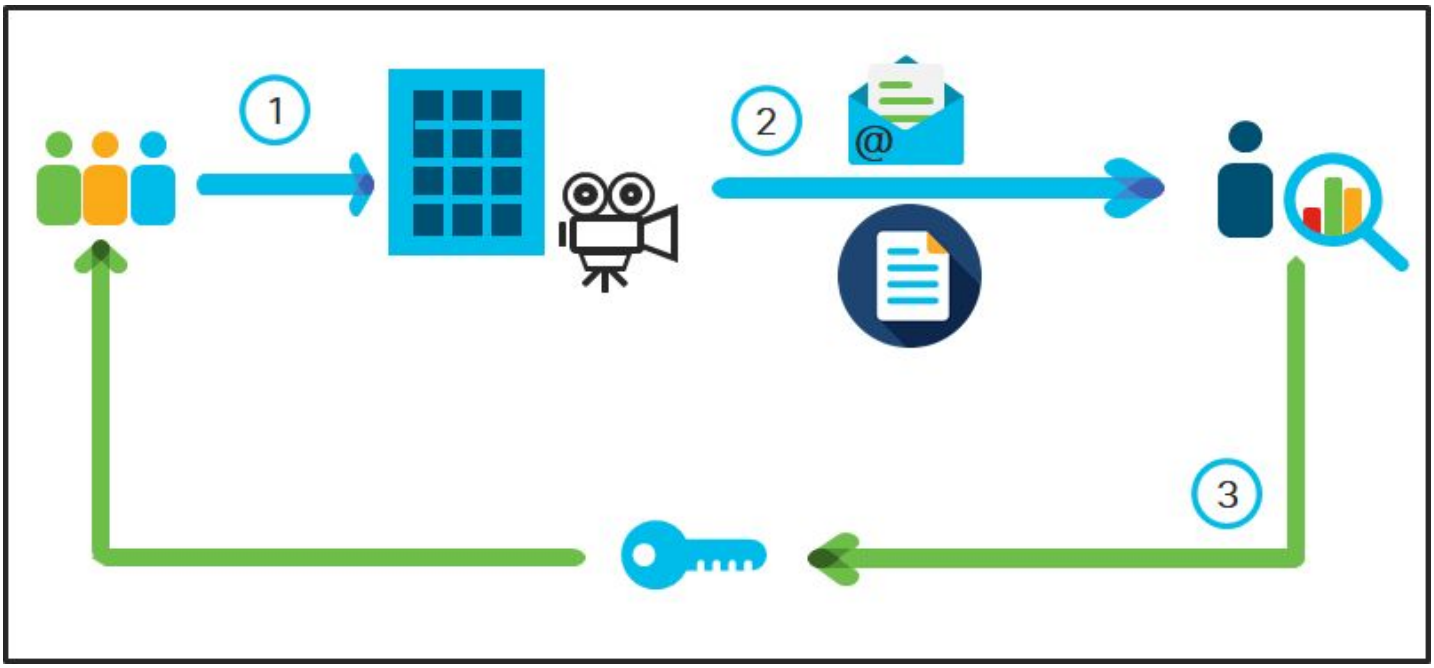
zero-knowledge proof, where only the outcome of the attestation is recorded as part of the EIA on the blockchain and not the actual identity attribute that is being attested,

CSI provides the consortium members a common and reliable database to track onboarding and offboarding of contract workers with data privacy and governance. It will result in improved efficiency, data longevity and consistency across productions and studios.

Problem Statement

The challenges with regards to production crew identity are demonstrated in both the onboarding and offboarding processes. The current onboarding workflow is as shown in Figure 1.

Figure 1. The current crew onboarding process



(1) Production companies interview and hire crew independently of the studio
(2) Crew lists are generally provided to the studio as a spreadsheet, a text document or an email.
(3) Studios do not generally validate the crew in the list they are provided before providing access to studio tools such as email, collaboration, or shared storage. In some instances, a production company has admin access to required studio tools or their own provisioned system bypassing studios tools altogether.

On the offboarding side, there is no consistent and widely accepted process. It typically relies on the system expiration set up during the onboarding process to remove the content access for contractors.

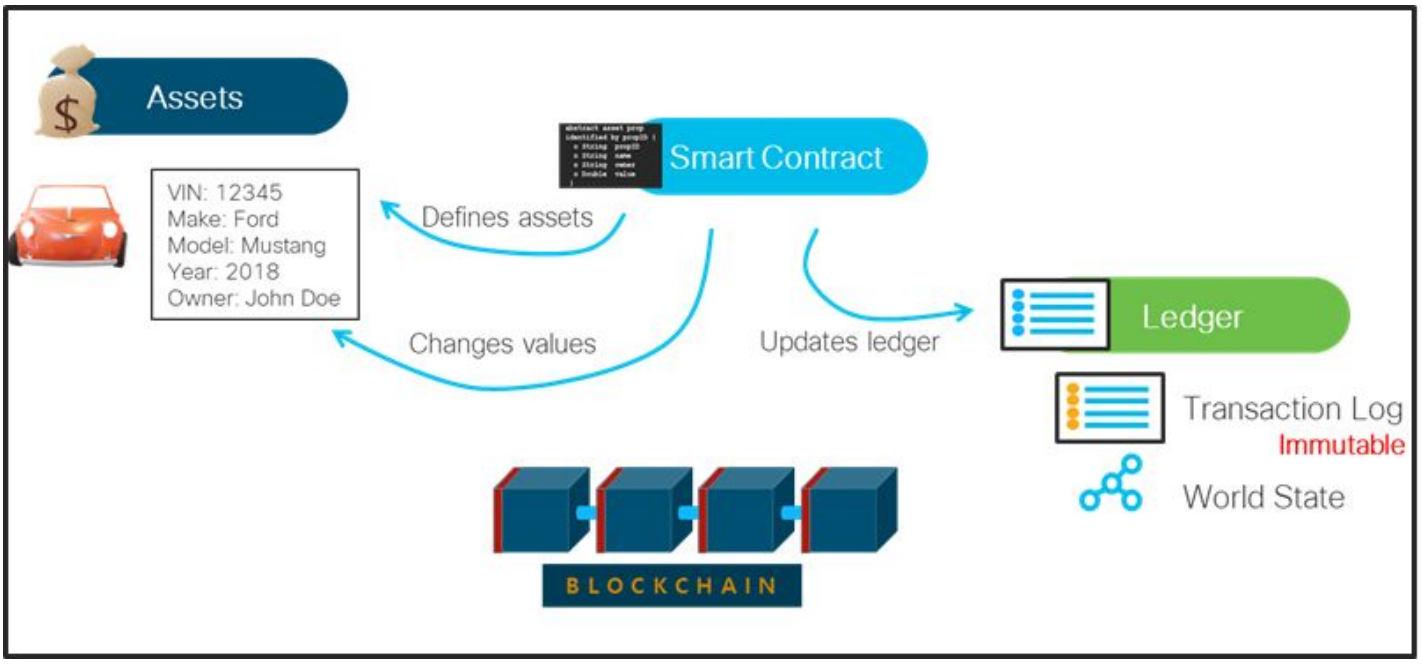
In summary, the challenges facing the current onboarding and offboarding processes are:

- Repetitive work: if a contractor is employed on one production and moves on to another production, the onboarding process starts anew each time
- Onboarding time: each contractor requires an onboarding time even if they have a good history of project delivery in other productions
- Onboarding cost: the cost of onboarding is anew each time
- Inconsistent and unreliable offboarding process, this leads to times when contractors may maintain their access even after the production is over. Also, there is a chance of miscommunication between the production and studio regarding when and what users are terminated. Finally, it is often difficult to track and verify when access has been properly terminated.

Consortium Shared Identity (CSI)

Blockchain is a decentralized and distributed ledger construct that provides an immutable record of transactions. A smart contract is a piece of code that lives on the blockchain with a set of predefined logic and can be controlled by transactions to update the ledger. Figure 2 shows an example of how a smart contract is used to control the asset states and how the ledger is updated.

Figure 2. An example of how blockchain smart contract updates asset and ledger



By leveraging a tamper-proof decentralized database with blockchain, a consortium-based identity system can be created that allows all members to share the same contractor database thus significantly reducing the obstacles and cost to production crew onboarding and offboarding.

Blockchain provides a cryptographically secured single source of truth that is distributed among all members. The consortium identity system is based on an enterprise-grade permissioned blockchain that is privately owned and operated by the consortium with an approved governance model.

The Consortium Shared Identity (CSI) is different from the popular Self Sovereign Identity (SSI) in a couple of significant ways:

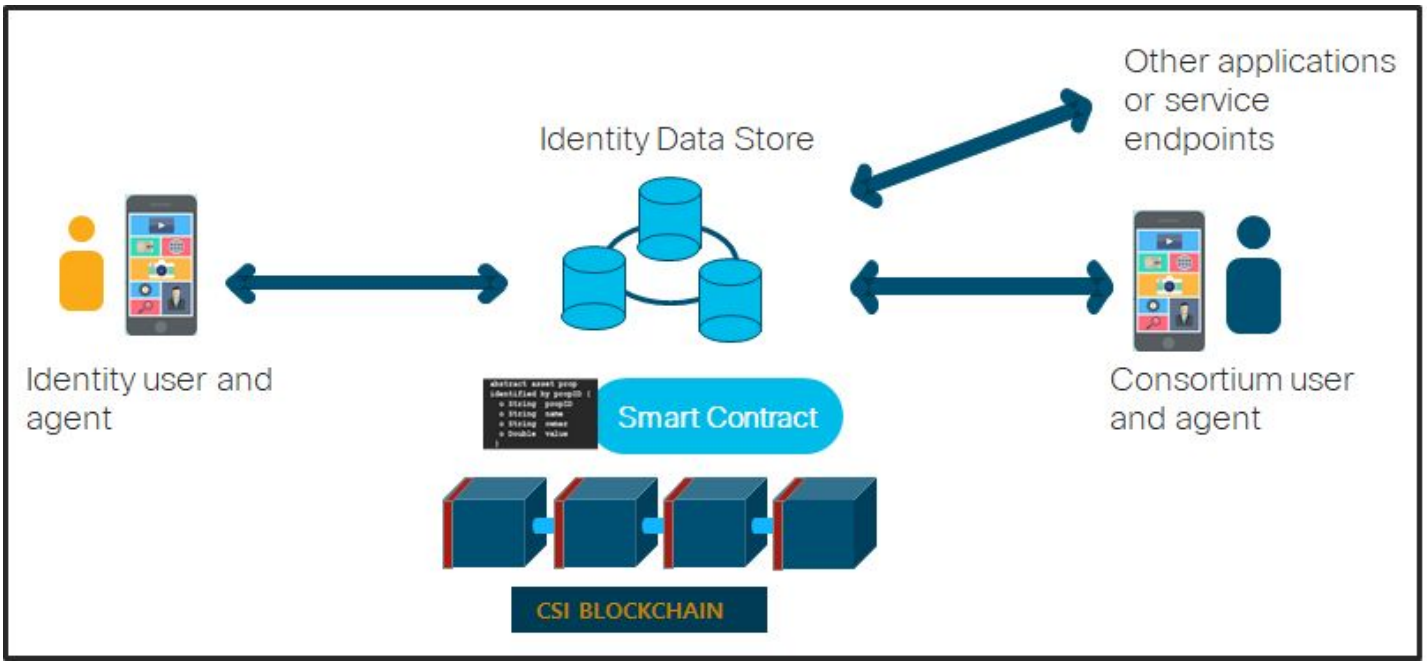
- The blockchain network along its database is private and permissioned
- The identity of users is a shared property between the identity owner and the consortium.

Because of these differences, the CSI design contains some key unique characteristics:

- Identity attributes of an identity owner user are stored on the blockchain with role-based access control (RBAC) that allows users to grant or revoke certain level of access, or no access. The access provides CRUD (Create, Read, Update, Delete) level granular access to specified roles
- Identity owner user controls the access through a private key, which is residing only on the user device
- Consortium member users are assigned roles that controls the identity attribute access
- Identity attributes are divided into Internal Attributes and External Attributes.
- Internal Identity Attributes are inherent to the identity owner and form the core of the identity. Internal Identity Attributes are controlled by the identity owner users who can grant and deny access as needed for individual access and the type of access.
- External attributes are attached to the identity and are imposed by consortium members and other authorities external to the identity owner. External Attributes are controlled by consortium member users or other authorities. Examples of External Attributes are onboarding, offboarding, and attestation.

Figure 3 shows a high-level view of components and interactions of CSI. Identity attributes are stored on the blockchain data store, which are modified by smart contract transactions. Users interact with the blockchain through a user agent. External applications and service endpoints can interact with the blockchain via API to receive notifications or offer services.

Figure 3. CSI components and interactions



With CSI, the future onboarding workflow is as follows:

The future onboarding workflow will allow for both internal and external attributes to be recorded to the blockchain depending on the earlier mentioned owners of the data.

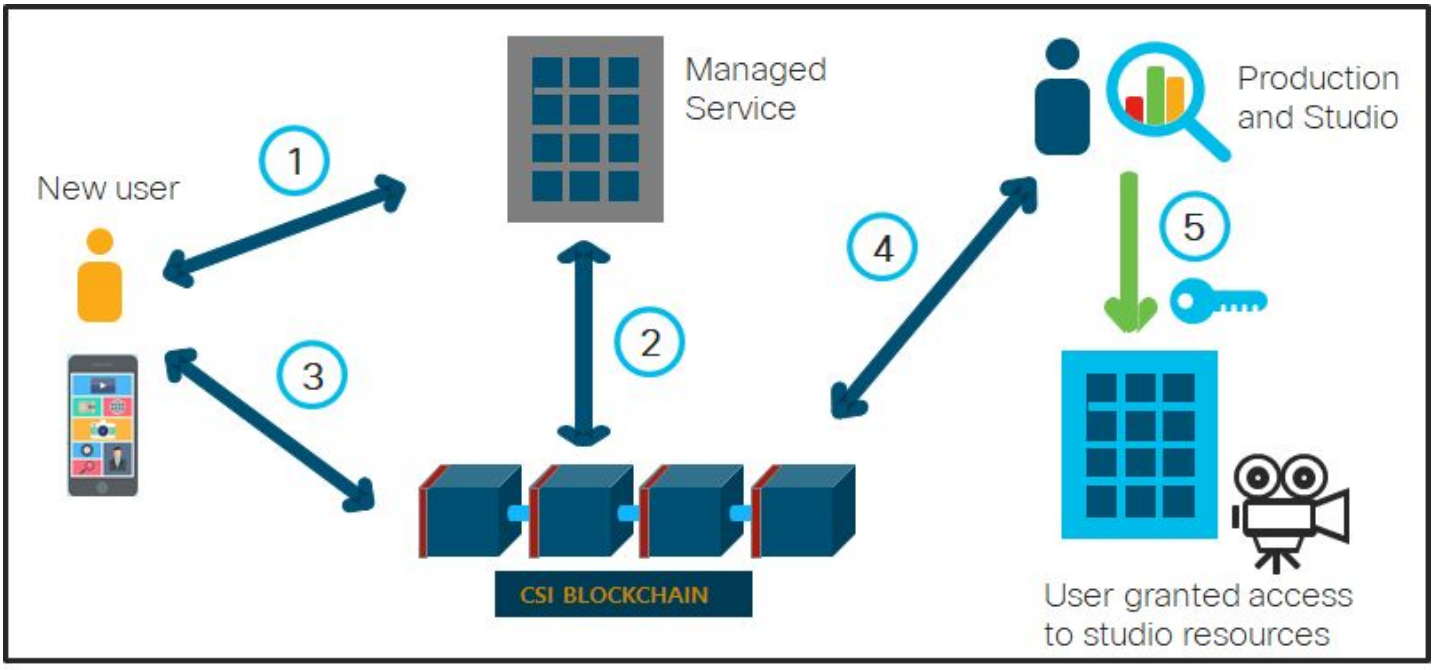
The first step of a new user being added to the private blockchain will be a validation step to verify that a user is who they say they are using industry accepted identity forms like passport, SSN, or driver's license number.

After validation of a user has been confirmed, likely by a 3rd party service, the blockchain consortium will add a user to the blockchain providing a means for the user to input their internal attributes and sharing preferences.

A production will begin onboarding users by first asking for their production ID and then updating external attributes of the included production users (e.g. start date, title/job function, feature title, etc.).

Additionally, studios will be able to receive crew lists and provide their approval to studio provisioned tools like email and storage services. Production users will be required to have a production ID before being fully onboarded. Figure 4 shows a high level view of the future onboarding process.

Figure 4. Future onboarding process



Requirements

General Requirements

This section discusses general requirements and considerations for CSI.

At its core, the purpose of the CSI is to provide a verified work history trusted by identity owners and consortium members for its accuracy. To achieve this goal the CSI will only track factual and objective metadata from two main categories, production history and private information. CSI will track production IDs that an identity owner is associated

with and make available the metadata for that production ID. CSI will also securely store the identity owner's private information that needs to be trusted and accessible by consortium members, granted access by the identity owner. An identity owner's presence in the CSI blockchain is an assumption of their standing as a "good actor." Negative amendments to an identity owner's record on the CSI blockchain should be preceded by publicly available and verifiable documentation of the incident.

In order to comply with GDPR, identity owners must be able to control which of their identity metadata is public, be able to be removed from the CSI blockchain, and have a mechanism to dispute contested metadata. It is important that CSI be seen as a neutral purveyor of verifiable objective metadata. As such, suggestive or reputational metadata is out of scope for the CSI, and the CSI will not maintain opinions or assessments of an identity owner's work quality.

CSI will onboard new identity owners and issue new IDs based on the results of consortium members' verification processes, this means CSI will not be responsible for conducting background checks or verifying SSN, but merely storing such information privately and associating it with an identity owner on the CSI blockchain. The user identity will be verified by the managed services hired for CSI onboarding purposes. It will be the identity owner's responsibility to work with the managed services to resolve any issues of incorrect identity information used in the onboarding process.

There should be consortium-approved governance for general operations, including legal and ethical protections and dispute resolution. It is critical that CSI is able to make any required changes to an identity owner's record based on the dispute resolution process and indicate on an identity owner's record that the dispute resolution process has begun for a specific production ID.

CSI must ensure its service availability and consistency across geo locations. Measures should be taken to guard against any denial of service attacks or security hacks.

Technical Requirements

This section discusses the technical requirements for CSI.

The blockchain network is privately owned by the consortium and governed by the consortium board (CSI Board) for policy and regulations. The policy will stipulate that the network is distributed without single point of failure and the identity database is decentralized. The board may operate the network or choose an outside party to run the operations (authorized partners or managed services). All users who have access to the network are authenticated and authorized. The operator will ensure network availability, security and performance. For the stability of the network, the consortium policy needs to include a voting and approval mechanism for software and feature updates, tools to be allowed to have access, monitoring and auditing for proper use, and privacy protection. The consortium has the ultimate right, if allowable by laws, to completely destroy the network or rebuild the network.

The CSI blockchain network allows interactions with external applications through APIs or webhooks as appropriate. Identity User Agent (IUA) is such an application that it allows authenticated and authorized users to submit and query identity attributes. IUA should provide a web user interface that can be accessed via mobile phones or other computing platforms. Multi-factor authentication should be supported. The network should also allow other external applications to receive events and notifications, which can be used to trigger actions for additional events or actions in external systems. API throttling must be implemented to avoid denial of service attacks or application malfunctions.

The CSI network primarily supports three types of users: identity owners, consortium members, and super users such as auditors, operators, and admin users. Identity activities usually take place between identity owners and consortium members, who are also called regular users. For example, an identity user such as a contractor may be authorized to modify an identity on the network for the first project that the person is working with one of the members. Consortium member users, either directly or indirectly through an authorized partner, will ask for the access to the identity attributes of the user and perform attestation of the attributes. Results of attestation will be recorded on the network for the said identity, which may be accessed by other consortium members. All users are authenticated by board-approved cryptographic measures. A key recovery procedure must be implemented to help users recover their lost or forgotten keys.

User identity is characterized by a set of identity attributes. For ease of access or organization, identity attributes may be combined into groups and hierarchies. Identity attributes are divided into two major categories: internal attributes and external attributes.

Internal attributes pertain to the core and inherent identity of the user, such as name, SSN, driver's license number, age, etc. The identity owner has full control of these attributes, such as granting access or revoking access. In an extreme case, an identity owner may choose to revoke access to all internal attributes. Consortium members do not have automatic access to internal attributes but may require the access of certain attributes as a condition for employment, for example. The attestation of an internal attribute may be performed by any of the consortium members or authorized partners. To protect the privacy of the internal attributes, CSI allows identity owners to control: with whom to share, what level of detail to share, and how long to share an identity attribute. An automatic sharing expiration must be implemented to revoke previous access when the timer expires. Additionally the identity owner must also be able to set an expiration timer other than the default for any internal identity attribute. If an internal attribute is verified by a managed service provider or a consortium member, only the

outcome of the verification is made available to the consortium members and not the actual identity attribute itself. This is the key point of the zero-knowledge proof.

External attributes are the ones that are created by consortium members or authorized partners, such as attestation results and onboarding and offboarding status. The member user who created the attribute may designate the access control for these attributes. The identity owner does not have control of these attributes.

Each identity attribute will have a role-based access control (RBAC) assigned to authorize access and actions that can be performed by the user on that particular attribute. The access control may indicate “read,” “update,” or “delete” for specific user roles. In general, the creator of the attribute sets the initial access and thus has all the access. In the case of managed service onboarding, the managed service partner will ensure only the identity owner has full control of his or her internal identity attributes. Subsequent access to internal attributes by consortium members or partners must be explicitly granted by the identity owner. Default access roles may be created by the system for attributes in order to provide ease of use based on consortium policy and regulations. The consortium policy and regulations may also define roles. For example, these roles may be created for contractors, consortium members, or super users. It is important to note that being a super user does not automatically grant the super user the permission to access all identity attributes unless they are permitted explicitly. The access is still controlled the same way by RBAC.

Each identity attribute will maintain version control for auditing purposes. Only the latest version will be made available to users. If not explicitly permitted to access the attributes, super users will only have access to the change logs for all the versions. Change logs are immutably maintained by the blockchain.

Appendix: Alternate Use Cases

The following use cases are examples that may leverage the CSI.

Use Case 1: Media Supply Chain Possession Tracking

Modern content production and distribution requires work of many hands. Content moving through modern supply chains may be touched by over a dozen suppliers, contractors, and subcontractors making it complicated to keep track of who is in possession of content at a given time. These concerns will become even more pressing as the industry moves to 4k standards and its accompanying complexity and volume of files that constitute a 4k package. This use case seeks to remedy this issue by utilizing blockchain technology to transparently track possession of assets in a studio's media supply chain. The focus of this use case will be on production suppliers rather than on distribution and possession by consumers.

Advantages of using blockchain to manage media supply chains:

- Source of truth for logging the receipt and distribution of assets in the media supply chain
- Track changes made to assets as they move between suppliers
- Automated asset revocation after a given supplier's task is complete
- Provide the ability to sanction or blacklist suppliers who violate rules

Monitoring media supply chains in this way has two key benefits:

- Reduced piracy from leaky supply chains
- Increased trust between studio and supplier

Use Case 2: Awards Screener Tracking

Screeners provide the ability to review and compare works in the comfort of a voter's own home prior to casting a vote. This time honored tradition is both fun and valuable, but it also lends itself to piracy. This use case seeks to reduce this risk by utilizing blockchain and anti-piracy watermarking to track possession of screeners and investigate the sources of piracy resulting from the distribution of screeners.

This use case has three primary goals to address piracy:

- Assign a unique watermark to each screener distributed that will be associated with a recipient's ID on the blockchain
- Utilize watermark to determine individual sources of piracy
- Easily identify for sanctions or blacklisting, recipients whose content is pirated

Use Case 3: Identifying and Provisioning Access to Production Users

Utilize blockchain to assign a unique identity to individuals working on a production for the purposes of provisioning them access to content owner tools and resources. The identity record would be owned and managed by the production user and could be utilized as a single sign on type authentication independent from the production and/or content owner.

A few examples of tools a content owner would be able to dynamically provide access to:

- Content owner would setup access to secure file sharing platform (e.g. OneDrive, Dropbox, GDrive)
- Content owner would provide access to secure document storage platform (e.g. Scenechronize)
- Timecard tracking for use by payroll company (e.g. Cast & Crew, EP)
- Secure distribution of scripts using production's instance of ____ software

Additional benefits of tracking users involved in a production:

- Accurately tracking union residuals
- Verified resume - accurately tracking a production users TV and film work history
- Malicious user blacklist - troublesome users could be blacklisted from future productions

Managed Service

Trust is going to be an important factor from all users of the production ID use case. Ensuring a production user is who they say they are is necessary for content owners before they securely provision access to systems holding sensitive assets (e.g. scripts, set photos, etc.). Alternatively, production users need to be sure their timecards and "verified resumes" are not tampered with so they continue to get paid on time and can keep using their documented background experience to attain work on future productions.

Because of the trust that needs to be maintained in an ecosystem that requires verified identification, production IDs would likely need to leverage a managed service to maintain the integrity of the users data and provide a standard for onboarding new users made available to the blockchain. An example could be requiring a form of government issued identification (e.g. passport or driver's license) as a validation requirement. Another option could be to employ a background check similar to what is done by most major employers using personal details such as name, address, phone, SSN, picture, etc. Due to the obvious sensitivity of the information being collected, handling of this information in accordance with required privacy and data security laws and regulations will be an important factor for the managed service to offer.

Onboarding

The first step of onboarding a user would require the user to contact the managed service, described above, for a verification of their ID. Once this verification has been

completed, the user would be issued a new and unique 'production ID'. This production ID would then be made available to the blockchain as an available user. This users' production ID is now ready to be assigned to a current or upcoming production or potentially could be added to past productions as well.

Once a user's production ID has been added to a production, this can now serve as the main identifier for other companies systems to interact with the user -- similar to how SSO works in a corporate environment. Systems such as email, file sharing/collaboration suites, payroll, and timecard tracking could all be potential use-cases for this production ID. Also, because production ID is meant to be made available to other users and production integrations (e.g. email and file sharing), the ID itself does not need to be treated as sensitive data in the same way a users other forms of identification might (e.g. SSN).

Once assigned to a production, the production supervisor or a similar role would be expected to maintain a list of all production IDs assigned to the production and relate that with other job specific information such as show department, job description, direct supervisor, access rights. and onboarding/offboarding date.

As a content owner, provisioning access to studio tools would be made possible by supplying a list of production IDs from the production supervisor or similar. These IDs could be assigned rights to tools and systems as needed and removed after the show has wrapped.

Offboarding

At the conclusion of the production, tools owned by content owners, payroll systems, and all other systems needed during the production would remove access to the production IDs associated with that production.

Production users could then use their production ID as a way to show past experience to prospective shows and once hired could be onboarded to the new production using the same ID they used in the past.

Contributors

Working Group Chairs

Seth Levenson, Director, Adaptive Production, ETC@USC

Randy Zhang, Principal Architect, Cisco

Working Group Members

Anthony Anderson, Sr. Director, Film Security, Universal Pictures

Albhy Galuten, Vice President, Media Technology Strategy, Sony

Jim Helman, CTO, MovieLabs

Max Roessler, Consulting Metadata Architect, Disney

Joel Sloss, Sr. Program Manager, Microsoft

ETC@USC Member Companies