Technical Disclosure Commons

Defensive Publications Series

March 06, 2019

CREATING A LEGAL COLLABORATIVE EXPERIENCE

Shankar Ramanathan

Muhilan Natarajan

Robert Barton

Jerome Henry

CREATING A LEGAL COLLABORATIVE EXPERIENCE

AUTHORS:
Shankar Ramanathan
Muhilan Natarajan
Robert Barton
Jerome Henry

ABSTRACT

Techniques are described for adding trust/reliability quotients to video conversation recordings by creating a secure ledger-based legal recording mechanism. The legal recording mechanism is tamper proof, faster than documenting the agreement, and legally binding.

DETAILED DESCRIPTION

Digital collaboration tools are used to store and record conversations, meetings, interviews, and Memoranda of Understanding (MOU) across representatives from the same or different organizations. Many of the agreements in these collaborative conversations involve a level of trust.

One example is an individual in an interview who verbally claims to have critical expertise, which is a condition to obtain access, a job, or other agreement between two sides. Another example involves the sharing of confidential information during a meeting, where the sharing is predicated on an agreement by the receiving party to keep the information confidential. For instance, a binding decision can be made by parties attending a virtual collaboration meeting.

In all these cases, recording consent is complicated. The only formal agreements lie in written communications (e.g., paper or digital signatures) and not via audio/video communications, which is where the consent is actually discussed and obtained.

Additionally, even when the meeting is recorded, locating the recording as well as the segment of the recording where consent was provided is cumbersome. For example, a standard project may include hundreds of meetings, throughout which a few agreements may have been discussed. Even when the correct meeting and segment is found, it is difficult to prove that the agreement was properly received (e.g., that the recording was not tampered with or edited, the consent was consciously given, etc.).

Accordingly, described herein are techniques to add trust/reliability quotients to video conversation recordings by creating a secure ledger-based legal recording mechanism. This mechanism is tamper-proof, faster than documenting the agreement, and legally binding.

A host-triggered blockchain ledger used as a storage space for audio/video transactions may create secure, legally binding audio/video agreements. This is more convenient than a traditional written agreement.

Each user or host has his/her own root blockchain node (or parent block) with respective identity details (e.g., name, social security number, address, etc.). This node is created, for example, when a user first registers in a company directory.

When a user A conducts a virtual meeting with user B (or users B and C) and realizes that the users are about to discuss a topic that requires a formal agreement (e.g., Non-Disclosure Agreement (NDA) at any level, a binding decision between parties, etc.), user A selects a "secure record" button option which causes the system to perform the following operations.

First, an option is presented to select which attendees are to be involved in the recorded agreement (e.g., only user B, users A and B, all attendees on the call, all attendees invited to the call including no-shows, etc.).

An option is presented to select the part of the meeting to be securely saved. In one example, that part of the meeting is defined from when the button was selected until a stop button is selected. Alternatively, that part of the meeting may be defined from the beginning of the call.

In a more elaborate example, bag of words speech recognition techniques may be used to label preceding segments of the meeting conversation and offer to record starting from a point in time or a specific marker (e.g., "start of slide 12," "when conversation moved to enterprise 1 – enterprise 2 cooperation," etc.).

Consent is requested from all attendees involved and categorizes the presence of the audience as either legal parties or witnesses. The consent can be a verbal question from the host, the presenter reading some text (e.g., NDA), or an automated question. In all cases, the answer is expected to be verbal (e.g., "Yes, I consent/agree").

In a more elaborate example, speech recognition techniques may be used to analyze the response and build a consent probability. For example, “Yes of course, I'll keep this information confidential” corresponds to a consent probability of 1, whereas “Yeah, I understand that I should likely not share that” corresponds to a consent probability of 0.64. The consent probability may be presented to the host or main speaker or computed automatically. Consent may be requested repeatedly until the consent probability reaches a satisfactory p level, or until consent is recorded as not fully granted.

For attendees that were invited to the call but did not join, a secondary consent process may be utilized. For example, the meeting tool may send an email/text/automated call to the required persons, with a message signifying that formal consent was required. The audio of the secure record is played before formal consent is requested. The process may then proceed as described above with reference to obtaining consent.

In one example, the segment with the verbal consent is sent to the consenter blockchain ledger and hashed before being returned to the main recording. This process can be used as a tamper-proof time mark of the consent time.

During the meeting, once the categorization and consents are received, the key section is recorded and the content of the conversation is attached directly into the blockchain ledger of the host (i.e., consent requester) as a child node to the existing root node or appends to the last known recording transaction.

The result is a meeting recording which has validated each consent in an unspoofable and undeniable manner. This recording can be kept for archive as with any other formal agreement.

Other elements may be adjoined to the recording (audio/video) in the requester ledger, such as meeting invite, attendee list, non-attending consenters and their consent timestamp, etc.

Additional traceability may also be implemented. For example, playing or sharing the recording may cause the receiver ledger signature to be added before returning the recording to the requester ledger, thereby recording in a tamperproof manner as to who accessed the recording and when.

Since the root node for each ledger is host user based, subsequent legal secure recordings may be added as child node, creating a chain of nodes forming a legal ledger of

all recordings of the host user. The host user can reference or share a specific child node transaction for future use cases. A central safe may also be designed where each signed recording is stored (and its access traced).

Figure 1 below illustrates an example system at a point is time at which user A and user B are ready to undergo a mutual agreement.

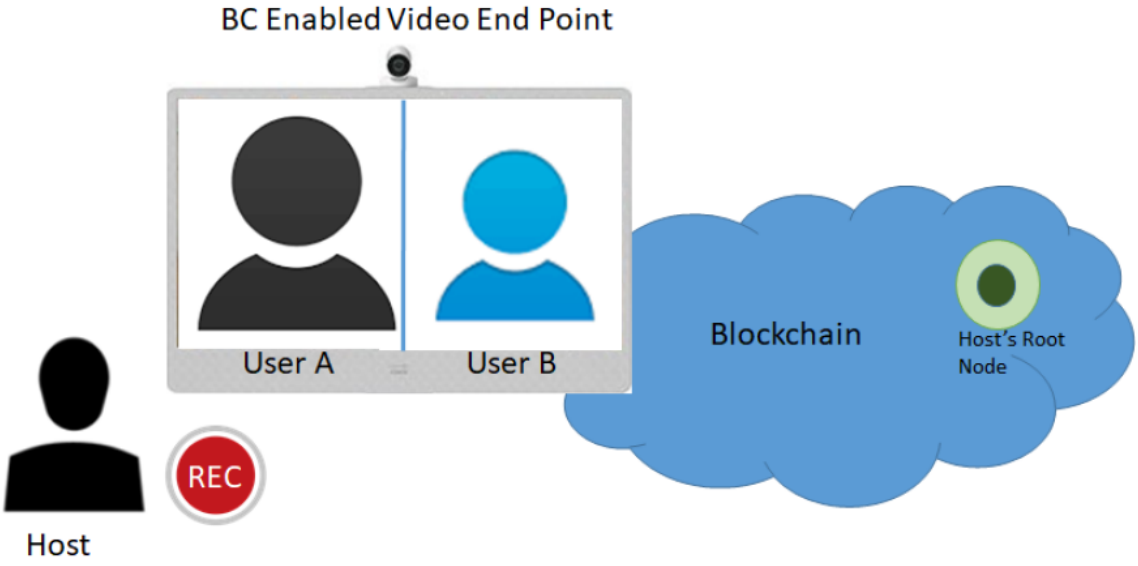

Figure 1

Figure 2 below illustrates the system of Figure 1 at a later point in time at which the users are presented with the consent option. Here, the video starts recording, and the consent and video recording is attached to the blockchain ledger of the host.

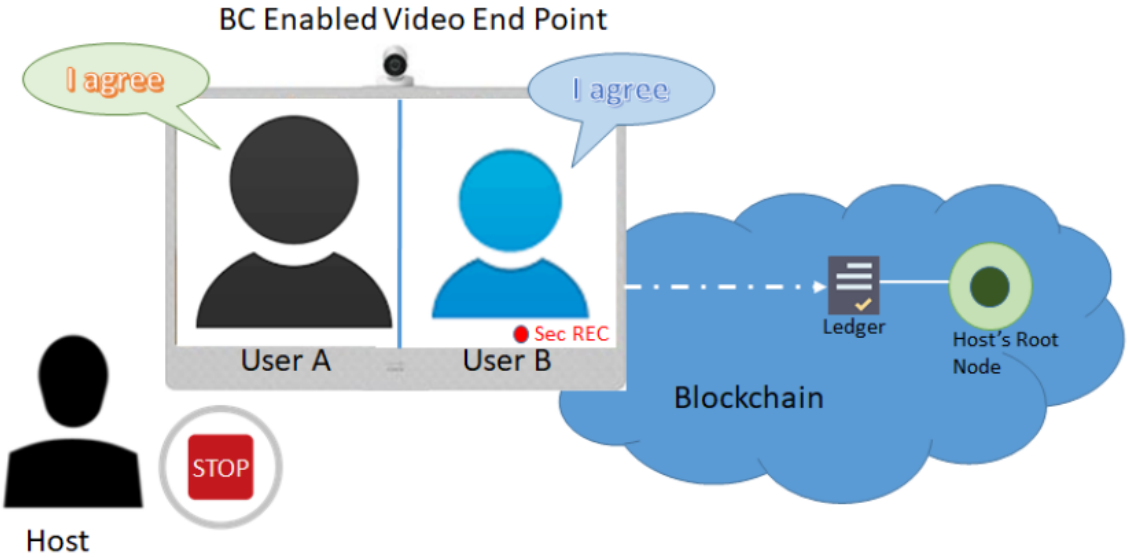

Figure 2

The solution presented herein avoids normal documentation and signing, which would be time consuming. Furthermore, the secure transaction may always be accessed and may not be tampered with.

In summary, techniques are described for adding trust/reliability quotients to video conversation recordings by creating a secure ledger-based legal recording mechanism. The legal recording mechanism is tamper proof, faster than documenting the agreement, and legally binding.