Enduring Net

Communication Organiser v.1

Use case: Modern Slavery Support Network

This version: 19 January 2020

1. Introduction

This document describes *Enduring Net Communication Organiser v.1* (ENCOv1) in the "Modern Slavery Support Network" use case. Section 2 below outlines the basic problems tackled by the proposed system underlies the prototype ENCOv1. Section 3 focuses on describing the basic technical outline of how this system operates. Section 4 presents functionalities offered in the user interface (UI) and explains the real world operations they correspond to. Section 5 presents a summary of the discussions regarding how well suited the system seemed to be to the practical needs of GMP and other practitioners.

A blockchain, as implemented here, is an audit trail of an immutable collection of time ordered records, called the "ledger", submitted by network participants. Each key participant (called a node) has an identical copy of the "ledger" that is updated in real time; hence the system is free from single-point failure. The blockchain is managed by consensus (being replaced here by the traditional roles in the modern slavery support network), so new participants can join the network based on their traditional roles and an agreed protocol among the network members.

In order to retain clarity and focus, we have purposefully chosen to omit the underlying technical details of how the blockchain itself might operate. These are being written up and presented elsewhere and can be made available on request.

2. The Use Case and Requirements

The basic use case centred on the Modern Slavery Support Network that consists of the following actors:

- Greater Manchester Police (GMP) HQ;
- Other regional police forces in the Greater Manchester area;
- Other specialist agencies such as the fire & rescue service;
- The national anti-Modern Slavery helpline;
- Indirectly, the victims and survivors of the crimes.

The remit of the system was to enhance the coordination of the communication and to permit more secured sharing of documents, and therefore more effective actions between disparate entities. The efficiency gain is the strongest when the system involves a heterogeneous group of organisations, NGOs and the peripheral support organisations. We envisage that, in the near future, this coordination will extend to include secure and privacy preserved victim identity matching capability.

The design of the prototype therefore focused on coordinating the early stages on the modern slavery investigation, and in particular, where multiple organisations were involved. Were the system to be adopted in practice it would be easily possible, if desired, to extend it in order to record how the investigations ultimately ended on the system, and the journey where the victims and survivors adjust to their new lives after the incidents.

In summary, we identified the following user *requirements*:

a) That the system should permit easy, secure communication between these organisations.

b) That it must involve only little deployment effort at each organisation.

c) That, while permitting each organisation to contribute, it must still allow the information stored to be fully trustworthy.

d) Minimum disruptions to each organisation own *standard operating procedures*.

e) Tamper proof, leaving a clear audit trail and reducing the chances for fraud.

f) As the situation called for, the system might be decentralised and guided by consensus or centralised for added efficiency and low maintenance.

These requirements were a natural fit for applying distributed ledger technology (DLT), allowing the control of the entries on a traditional ledger to be distributed to multiple organisations while retaining the trustworthiness of the data on that ledger. Such a system has three basic properties:

i) Each key organisation (node) connected to the distributed ledger has a full identical copy of the data on that ledger.

ii) Certain users are "authorised" (according to an agreed governance structure) can add new entries to the ledger.

iii) Once an entry has been added to the ledger, it *cannot* be changed.

This final property has a potentially very significant property in the current case – the combined set of entries in the system regarding the handling of a specific case is a fully reliable log of how this case was pursued by the different organisations. It is, in fact, even possible to envisage potential legal applications of this.

Requirement (b) is especially important. The difficulty of merging the databases, and systems, used by multiple public organisations is well known and enormous. Our proposed system is *not* envisaged as replacing any existing systems according to Requirement (d).

Rather it is meant to complement the existing systems. Namely:

- It aims to *replace* the use of informal communication, email and spreadsheets attachment with a more secure, organised system.
- It will provide auditable logs of these sequences of communication.
- Any data currently shared on databases within organisations will remain as shared on those databases, with encrypted links to enable access directly stored in the new system.

This is not to say that we think there will be *no* integration requirements involved in developing our proposed system. It is more that we do not wish to require full integration in this "minimum effort" design.

3. The Basic Technical System

The core of the system will be a distributed ledger. Only certain specific, recognised organisations will be granted access to this ledger. Only the key organisations on the system will have to host a copy of the ledger – while other minor participants can be served and hosted by the key organisations to reduce the IT burden. Also organisations that do not have full access right to the case data will not be permitted to participate as a "Node", as the node status implied full access rights.

This core technical system will then effectively offer a ledger to which:

- Every authorised user from approved organisation can add an entry.
- No one can edit, or remove, an entry once added to the ledger.
- Depending on the governance structure, all the organisations will potentially be able to read this.

In order to turn this technical backbone into an actually useable system we need:

- A precise definition of the permitted types of entries on the ledger.
- A precise definition of which organisations, and roles within each organisation, that can make each type of entry.
- A means to present the relevant subset of this information that is in a sensibly digestible form to each actual user within the organisations.

We will address the basic way in which this will work in the next three subsections.

3.1. The Types of Permitted Communication

We propose to strongly restrict the types of communication to a small number of strictly defined types of entry, each of which is designed to achieve a specific task. Appendix A contains a detailed definition. The precise types and definitions of permitted communication can be expanded later. The current prototype includes the following types of action:

Add and Record Incidents, Send Notifications,

Request/Close Actions,

Add New Evidence; Suggest Link,

Announce Potential New Case,

Start/Close Case Investigation; Add/Transfer Responsibility,

Briefly, they have the following uses:

- **Announcing a potential new case** corresponds to an organisation, such as the Helpline, informing GMP that they have interviewed certain modern slavery victims and that it might be worth investigating.
- **Starting a new investigation** is then triggered by GMP looking at one or more incidents and deciding to open a Case for police investigative work. This has the basic effect of showing the investigation as open on GMP's systems.
  - **Closing** marks the case as closed, which might be either due to it ending, or turning into an actual prosecution.

- **Add/transfer responsibility** amends the responsibility for an open investigation to include other police force(s), and other investigative units.
- **Request/Close Action:** here the police force requests someone like the fire & rescue service to take an action. The close action from that organisation then indicates it has happened and returns the information.
- **Add New Evidence; Suggest Link:** this tracks the progress of adding new evidence, and drawing links between existing sources of evidence.

3.2. Role Based Access Control (RBAC)

In order to control the flow of information within the system – who can make certain contributions, who can see specific case etc. – the prototype uses a system of role-base-access control.

Each user logging in is given a role correspond to their organisation and role within it. This is described in more detailed in Appendix 2.

Roughly, there are the following roles:

- Submitting New Incident – through first respondent such as the national helpline.
- Being requested to perform specified actions – organisations such as the fire & rescue service.
- Adding and linking pieces of evidence – the police in general, but with less restrictions than on formally advancing the 'flow' of a case.
- Initiating New Cases and controlling their operation – a branch of the police.

These roles are not the same as web based RBAC roles, they are defined in the blockchain architecture and hardcoded in the ledger policy, which adds security and make the system less prone to manipulation which often plagued standard web based RBAC systems.

3.3. User Interfaces

Naturally, we do *not* expect users to have to interact with the complexity of the specific elements of communication as they are written to the ledger. Instead, each organisation, and role, is given a specific interface. For example:

- The National Helpline will see an interface permitting them to:
  - Easily add a potential new incident.
  - Check the progress of ongoing suggested new cases related to the incidents they reported.
    - Adding new evidence/notes to the relevant police unit if this becomes important
- An officer at GMP would have several inboxes, each showing a particular functionality:
  - Potential new incidents in one set, and to accept them or not;
  - Accepted and open case in another;
  - Closed cases.
- An officer at the fire & rescue service would simply see a request from the police to undertake a specific action, with the information needed to understand it, and fill in a basic debriefing after it has been completed.

Which interface is presented to each user is controlled by the specific roles adopted by that user, and by their organisation within the overall system.

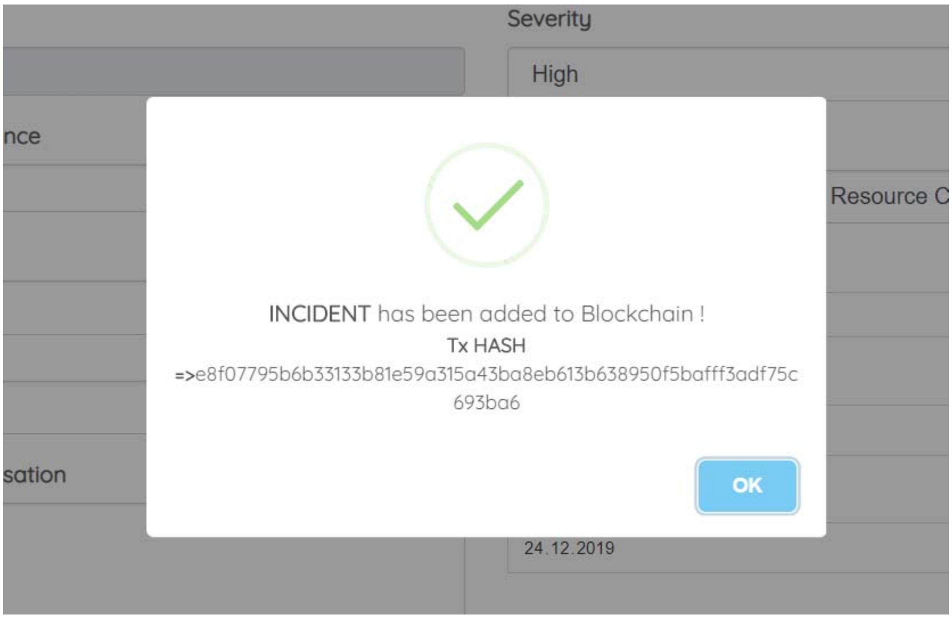
More detailed information of how each type of permitted communication affects the user interfaces of specific types of users can be found in Appendix A.

4. Demo - Modern Slavery Support Network

A prototype of the system described above is available on Enduring Net's web page (https://enduringnet.org/) Demo section together with a list of sample of usernames and passwords. It must be remembered that this is a prototype demonstration - all of these interfaces should be viewed as very preliminary. The prototype includes, on the landing page, functionalities, which include *Assign Roles*, *Organisations*, *Users*, *Incidents*, *Notifications*, *Actions*, *Cases*, *Link/Unlink*, *Query*, and *Personal Details* for keep records of victims and survivors.

Assign Roles, *Organisations*, and *Users* are administrative functions. Only user, "admin", has access to these three functions using them to define and update the user's role, and add/update oganisations and users on the network. In the full blockchain implementation, the Admin roles are defined according to the governance structure, their identities are checked *byte-to-byte* in the operation, so that a possible rogue admin account can be easily evicted. The security is further strengthened with the use of private/public key.

Incidents, *Actions*, and *Cases*, are three very similar interfaces in that they allow users to either create or modify an Incident, an Action or a Case. *Incidents*, for example, is the interface used to add a new incident into the system. This interface would typically be being used by an employee of the First Respondent in the modern slavery support network such as the national helpline or the police forces. On clicking *submit*, details of the incident would first be written to the ledger to record when the incident was added to the overall system, and secondly would be notified GMP and other intended organisations about this particular entry. To ensure immutability, a hash address is created, as shown below, when the incident is hard coded onto the blockchain.



INCIDENT has been added to Blockchain !

Tx HASH

=>e8f07795b6b33133b81e59a315a43ba8eb613b638950f5bafff3adf75c693ba6

The *Incident* interface also contains the *Add Information* option, which allows a user to add information to an incident previously submitted. The *Action* and *Case* interfaces work in a very similar manner.

The *Query* interface produces to a list of Incidents, Actions, Cases, New Users, and New Organisations etc that are present in the blockchain system. Future developments will make it possible to refine which are shown. For instance a police officer might be permitted to see only those Cases for which they are responsible.

Link/Unlink allows authorised personnel to connect incidents and cases to facilitate police investigation of complex cases.

Notifications and *Actions* interface conceptually contains any notable events of which a user of the system should be aware. These will include things like an action they have initiated being reported as being complete, a modification made to a case for which they are responsible etc etc.

Personal Details link some reference numbers such as PersonalID, IncidentID, ActionID, and CaseID to off-chain records of victims and survivors.

Overall, the demo's interfaces, while still at an early level of development, serve to illustrate quite well how the eventual system might operate.

5. Feedback arising from the Demonstration Session

One major item of feedback arising from the demonstration session was that victims records were not integrated well enough to really benefit from the further development of this type of system. As the ledgers do not contain actual personal details due to GDPR, there is a major concern that multiple incidents and personal IDs are actually belong to the same natural person. There is a strong need to allow the investigative unit a efficient and accurate personal records matching capability.

Other observations seemed to be on two levels:

- That all of the agencies use different database fields, names, etc. to represent different concepts.
- That the forces may use different *concepts* in terms of how an investigation might proceed.

Here we simply address how these concerns affect the ability to implement this specific system.

The answer is slightly complex. Because our proposed system sits as a distinct layer on top of any existing databases, and mainly focuses on coordination communication and actions, it definitely does not require a full, strict data integration in order to operate. Indeed the system is still designed to offer benefits in the envisaged international use cases, where it will be impossible to hope for either data or process integration.

The amount and types of data, and thus user roles, that are allowed in the system and focuses much more on simply passing information regarding the existence of modern slavery cases between relevant organisations. Such a system has a minimal real benefits for the current scenarios with a smaller well defined unit of operation is unclear. The efficiency gain is the strongest when the system involves a heterogeneous group of organisations, NGOs and the peripheral support organisations. A potentially greater impact can be envisage when data and process integration between organisations (who hold victims personal data) is more developed.

Appendix A:

Types of permitted communication

For each permitted communication type we define:

- Its name - this will be in bold as the subchapter title
- Its semantic intent – i.e. what effect is hoped to be achieved by writing the performative to the ledger.
- Interface Effects – how this might get displayed on the interfaces.
- Who Can Do it – the set of people who have permission to put the performative onto the blockchain
- Data Fields – this description purposefully omits the detailed entries used to actually define a case. This is done to make the actual process of the system operating clearer.

Submit Potential New Case

- Semantic Intent == to bring a new, potential, case to the attention of the police/other organisations on the blockchain (configurable).
- Interface Effects == The new information/case is displayed at the client of the relevant organisation(s)
- Who Can Do it == For the Manchester case it would be Unseen, or an equivalent highly credible organisation. In general there is no reason not to permit less credible sources but the relative lack of credibility in the report will need to be noted.
- Data Fields ==
    - Specific Organisation(s) to contact – either a specific organisation, or a chain public notification. Manchester police in the Manchester case.
    - The organisation submitting the information.
    - The information actually describing the case – both the amount made ‘public’ & a reference for contact the submitting organisation for more data.

3.4. Start New Investigation

- Semantic Intent == to take up a node describing a potential new case as an actual investigation – the precise details of what this means would need to be carefully modelled! At this point this subchain of the overall blockchain is ‘owned’ by that police force.
- Interface Effects == Notification to Unseen, Some list of open investigations in the police database
- Who Can Do It == police. Maybe specific people within the police?
- Data Fields
    - The ID of the ‘evidence’ node they’re taking as starting the investigation from. If the police get the evidence directly & start an investigation directly from that then the interface

  - software shows it as one operation to the operator, but it is assigned to the chain as two steps (submitting the case, then starting the investigation on it.).
  - Maybe the 'investigation ID'

3.5. Add New Evidence

- Semantic Intent == To add new information to a case, or to expand/comment on existing evidence.
- Interface Effects == All the information for each active case is bundled up neatly somehow on the interface of the people responsible for it.
- Who Can Do It == police responsible for the case.
- Data Fields
  - Free text field in case actual commentary is needed
  - Semi formal data fields as per the initial submission of evidence. (Detailed requirements work would be needed here.).

3.6. Request Action On Case

- Semantic Intent == To request that some organisation – such as another police force – take a specific action regarding the case. Interviewing a subject, investigating a specific building etc etc.
- Interface Effects == the request is passed along to the desired organisation and shows up in their client.
- Who Can Do It == police.
- Data Fields
  - Organisation to contact
  - Whatever is needed to specify the desired task. Free form English perhaps or some more detailed formality.

3.7. Close Action on Case

- Semantic Intent == To report that the action has happened. The actual *effects* of this action are then added as a 'Add New Evidence' field linked to the original 'Request Action'. This just formally closes it off as an active to do.
- Interface Effects == Now reported as done/hidden on the clients. Notifcation to requesting force.
- Who Can Do It == An organisation with an open 'Request Action'
- Data Field – None (see above, any results are returned as a new evidence node.).

3.8. Add/Transfer Responsibility

- Semantic Intent == Two different performatives described here! The Add one adds a second police form as responsible for an active investigation. The transfer responsibility one moves it.
  For instance, an investigation moves from GM Central body to a more local police force or such like.
- Interface Effects == Now shows as an active investigation in the local police forces, perhaps not in the more central one. The acceptability of this sort of transfer might need to be verified via messaging *before* it is committed to the chain.
- Who Can Do It = police force 'owning' the current case. Presumably also various formal rules about this sort of thing.
- Data Field == The New Organisation.

3.9. Close Open Investigation

- Semantic Intent == to close an open investigation. The data is obviously *not* deleted from the blockchain, so this just moves it about the user interfaces and signifies the end of active investigation.
  It might also be useful to have a 'snooze' option, whereby an investigation is deprioritised for the moment but kept as formally open in case more evidence turns up later.
- Interface Effects == The Investigation is marked as closed. Moved to a closed list on the interface.
- Who Can Do It == Police with active responsibility for the case.
- Data Fields
  - Investigation to close

3.10. Suggest Link

- Semantic Intent == to suggest that there is a link between two formally unrelated nodes. Linking evidence to an existing case etc.
- Interface Effects == the information in the linked nodes shows up when considering the node linked from in the interface screen.
- Who Can Do It == Very definitely the Police, maybe other organisations like unseen. AI systems running within the blockchain itself?
- Data Fields ==
  - Strength of confidence in link (some sort of list)
  - Evidence for/nature of link (written description)
  - IDs of the two nodes that are linked.
  - The organisation suggesting the link.

Appendix B:

User Roles within the demo

- **Incident Submitter:** These organisations are those permitted to introduce new (potential) incidents of modern slavery into the DLT. The primary example of this in the current situation is the national modern slavery helpline, and other first respondents.

- **Information Provider:** This role is similar to *Incident Submitter*, but rather than providing a full new incident after interviewing a victim, the user provides relevant intelligence. This might involve suggesting links between incidents, or be more general having arisen through reading news stories etc. The bar for reaching this level of involvement in the system is lower than for other roles – essentially any organisation who is trusted to review the publicly available information on the ledger can contribute in this way.

- **Potential Incident Receiver:** An organisation that can receive a potential incident from a helpline. Essentially the police, and in particular Project Challenger, the Modern Slavery Unit within Greater Manchester Police.

- **Legal Case Processor:** Someone who has adopted a potential case of Modern Slavery as a police investigation. This will always be the police. In the first instance, it is always likely to be GMP.
  This 'user role' only represents the *ability* to take on a generic case. At any given time, the question of *which* legal case processors can take measures on a given case is defined by the set of steps in the DLT system before it.
  For instance, if a potential case is sent to the Modern Slavery Unit in GMP and they take it up as a case then only GMP can explicitly log further major changes, such as closing the case, on the ledger.

- **Task Provider:** A system user who will provide a discrete task to police. Like the fire service doing search & rescue.
  The system is not intended to cover the details of this operation, simply that they have requested the fire service to perform a given action and that it has subsequently been achieved.

- **Admin:** This role would be taken by a strongly trusted person at GMP. They will be able to view the entire chain of entries on the actual DLT system.