Ante: A Peer-to-Peer Anti-Corruption Platform

Table of Contents

Abstract

A blockchain based incident management platform introduces the capability to securely store and share incidents amongst parties to deliver aid more effectively. Blockchain provides part of the solution, but with incidents holding sensitive data, off-chain data storage is essential to the protection of human rights. Simultaneously, exchanging data amongst aid bodies can exponentially improve program outcomes whilst reducing expenditure. The blockchain is therefore utilized for on-chain storage of hashed incident data for verification of an incident's immutability whilst stored in an off-chain facility. This data governance model enables incidents to be reported and shared whilst protecting sensitive, anonymized data in contexts presently discouraging sharing by an affected population.

Ante: A Peer-to-Peer Anti-Corruption Platform

1. Introduction

Ante is a blockchain based platform solving the misalignment between incident reporting, management, and governance, and the biases of those mandating them. While commercialization of reported incidents seems uncharacteristic, a pragmatic approach must be taken that recognizes the flaws with a capitalist approach and provides a solution that reduces the corruption it introduces through misappropriation of the sensitive, personally identifiable data provided by individuals. By creating a technology framework that enforces third-party governance, commercially viable applications can be developed to solve pertinent issues such as conflict management, inequality, and sustainability whilst protecting the privacy of individuals.

Our mission is to enable the secure collection of data from people to drive effective aid.

2. Incidents

Typically, an incident is synonymous with an event or occurrence. However, in the case of incident reporting, the characteristics of an incident constitute its intrinsic value. Some relevant characteristics include the individual or group reporting the incident, the type of incident, the severity or extremity of the incident, and the frequency of the incident.

Incidents are poorly managed due to misappropriation of the information provided by the reporter. If there is commercial value to an incident being reported, it can often be handled to suit a commercial motive rather than one aligned with the incentive motivating its initial provision. If there is no commercial value to an incident being reported, there is generally no digital infrastructure to capture information and protect the reporter appropriately. This is observed in circumstances favoring both humanitarian and commercial use cases. In humanitarian use cases, there is an unavailability of ecosystems that encourage parties to report

incidents whilst protecting their anonymity. This requires humanitarian bodies to revert to outdated mechanisms such as face-to-face surveying and focus group discussions. In commercial use cases, we often observe that the bodies responsible for governing the preservation of human rights, laws, and guidelines are funded by those commercially misaligned with the rules they are intending to mandate. In other words, there is a misalignment between the enforcer and the party they are intending to protect due to the source of capital.

Secure, human-centered incident reporting that captures raw information from people among affected populations needs to be developed now more than ever. The United Nations' 2030 Agenda for Sustainable Development, which was adopted by all UN Member States in 2015, identifies a shared blueprint for peace and prosperity. This extends to goals including, but not limited to, climate, hunger reduction, poverty reduction, education, equality, and conflict reduction. While ambitious goals are a prerequisite for change, equally important are metrics for assessing the progress of such change. Presently, the metrics being captured and used most are unsuitable for the problems they are intending to mandate, including satellites, drones, radar technology, thermometers, and the Internet of Things (IoT).

The most valuable data is derived from people. Those within affected populations, as opposed to instrument-derived metrics, can provide unrivaled insights that can be used to drive highly targeted efforts in affected regions.

3. Incident Management

Ante will start with a focus on driving effective aid, but we recognize its capability in commercial use cases. Ante has been developed by identifying the hinderances demotivating affected populations in regions receiving aid from reporting incidents first-hand. Our focus has therefore been to securely store incidents whilst protecting the anonymity of the affected population; in other words, our focus has been the underlying technologies to support our

mission. In any case, these technologies will be governed by program-based smart contracts, with Ante providing boilerplate contracts for rapid deployment of new programs to reduce operational expenditure. This approach will also allow Ante to be used for delivering aid in other commercial use cases so it can eventually flourish as a profitable organization underpinned by a strong set of humanitarian-first governance principles. Some potential commercial use cases exist in medicine, human resources, and financial regulation.

4. Incident Exchange

An incident exchange is a new term representing a technology facility for exchanging incidents reported by an individual or group. Incident commercialization may seem peculiar, but it acknowledges that a capitalist society has hierarchies that introduce conflicting agendas motivated by money. This leads to human actions developing characteristics by crime and corruption which must be reduced to enable the longevity of a civilized, shared society. Safe incident management begins by acknowledging that incidents are assets that upon being reported hold value and therefore must be tradeable. An exchange will be developed as part of this platform as a mechanism of ultimately empowering the incident report's program officer by ensuring they control the incident whilst protecting the anonymity of the reporter. Incident reporting, approval, and privatization are all facilitated by an exchange that enforces the safe use of incidents, as defined in the smart contract of the program being undertaken.

5. Reputation Engine

Democratization of incident reporting is enriched by a reputation engine permitting a self-sustaining incident economy. A reputation engine is an algorithmic mechanism trained by human feedback to classify incidents autonomously on scale. With longer term programs common in the context of providing aid, reputation engines offer a mechanism for building trust amongst members of the affected population. A model has been selected to reduce the

capital expenditure otherwise necessary for incident approval by training the system to develop trust for incident reporters. This helps to build a reputation amongst members within the affected population, which consequently removes arduous approval processes that the adoption of such technologies would otherwise introduce.

Ante proposes utilization of SNARE (Spatio-temporal Network-level Automatic Reputation Engine), a reputation engine that accurately and automatically classifies incidents based on early-stage supervised learning. SNARE is supported by RuleFit, a predictive learning model improving accuracy based on incidents as they are reported and audited. RuleFit is responsible for creating "rules" from decision trees and then fitting a linear model with the original features and the new rules as input. The model takes the form:

$$F(x) = a_0 + \sum_{m=1}^{M} a_m f_m(x)$$

Where:

- $F(x)$ is the predictive output.
- x is an input variable derived from the training data.
- a's are the weights attributed to each decision tree.
- m's are the references to each respective decision tree.
- $f_m(x)$ is the prediction function of the m-th tree.
- M is the number of incidents reported by the appropriate party.

Self-Sustaining Network

We recognize this could be extended by allowing approved members to self-sustain the network by permitting them to approve incidents from unapproved members within the affected population.

6. Privacy

Preserving the anonymity of those using the network, particularly incident reporters, is paramount to its adoption. Incident reporters will be educated that Ante is a third-party platform with trustworthy governance protocols to protect their anonymity. With incidents not presently being reported due to lack of appropriate facilities and fears of corruptive behavior, anonymity is fundamental to incentivizing adoption of the platform. The decentralized nature of blockchain technology, which facilitates the storage of users and incidents of the platform, seems paradoxical to preservation of anonymity. However, by leveraging on-chain validation and off-chain storage, data will be securely stored by the program operator with verification of immutability by the network.

The below diagram demonstrates the off-chain storage of incident data verifiable by a 256-bit hash of the incident data on-chain.

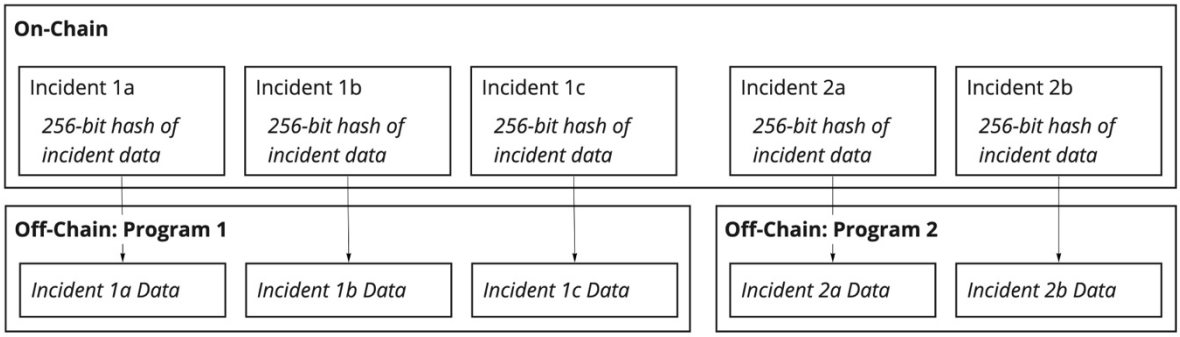

Figure 1: On- and Off-Chain Data Storage

On-Chain Hash

At the point of incident creation, a 256-bit hash will be generated and stored on-chain for verification of the incident data at a later stage (as a proof of immutability).

Off-Chain Incident Storage

Following storage of the 256-bit hash on-chain, the data will be stored in a complete state off-chain through a secure file storage mechanism such as via Amazon's S3.

7. Network

The network supporting Ante will require low cost, fast writing of new incident data to the public blockchain. With a higher incident volume allowing more valuable insights to be derived, Ante will encourage humanitarian bodies to adopt its incident reporting mechanism at scale. This will need to be coupled with low costs, acknowledging the limited capital expenditure available by those implementing humanitarian programs (including, but not limited to, not-for-profit and non-government organizations). Therefore, a low cost and rapid high-volume network will be prerequisites for Ante.

8. Permissions Model

Incident reportability on scale is powerful, but in the absence of shared incidents between programs, the most effective aid will be hindered. A strong governance framework for exchanging incidents amongst program officers is critical to maximizing the success of each program. By financially incentivizing incident exchange between programs, the intent is to create an opportunity for programs utilizing similar data sets to collaborate in the interest of maximized positive societal impact.

Exchanging incidents will be enabled via a cloud-based web platform that integrates with the off-chain data store. While a program officer will be responsible for storage of their own data off-chain, on-chain verifiability will confirm immutability. A program officer will be able to elect data on an element-level they would like to exchange with other parties offering aid. Once an agreement has been established between both parties, an object-based permissions model will be used to exchange the appropriate data securely. This will be implemented using the below flow.

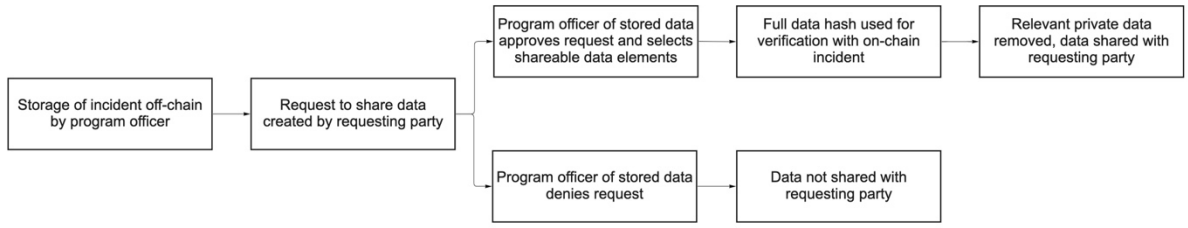

Figure 2: Data Exchange Process

9. Tokenomics

The tokenomics model has been constructed to incentivize the desired actions of parties reporting incidents and the humanitarian bodies allocating program-based capital expenditure. It is presently uncommon for the affected population within a region receiving aid to be financially rewarded for their contribution to incident reporting. This is coupled with the corruption that exists within such ecosystems that disincentivizes incident reporting by those most affected by humanitarian programs. We will develop two financial models; one more suitable to the existing policies of humanitarian bodies, and the other providing financial recognition to the parties reporting incidents to incentivize their contribution. The latter will be coupled with an optional reputation engine to encourage the development of long-term benefits to the affected population through development of trust.

Unfunded Incident Reporting

Unfunded incident reporting does not provide any financial benefit to the party reporting the incident but does require a financial contribution for use of the technology and participation on the exchange. The tokenomics as well as incident movement with validation is demonstrated in the diagram below.

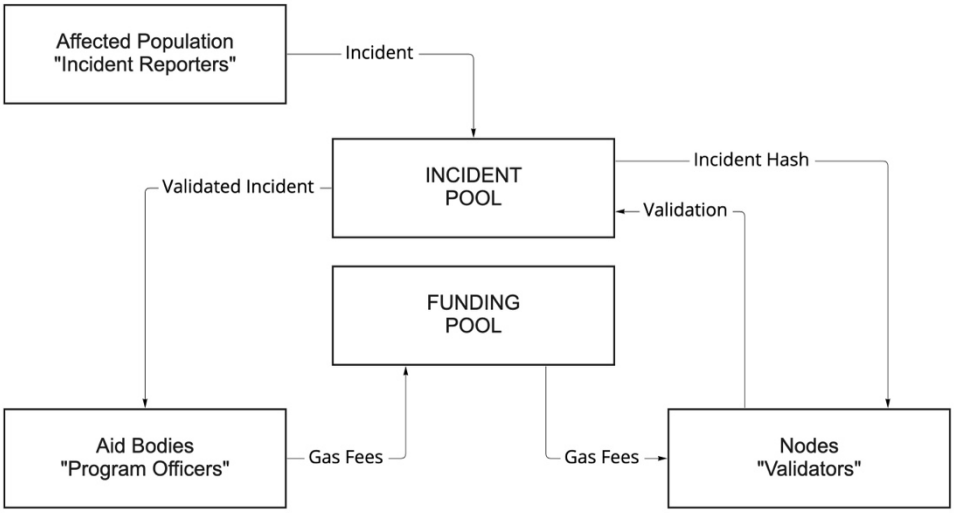

Figure 3: Tokenomics of Unfunded Incident Reporting

Funded Incident Reporting

Funded incident reporting builds upon unfunded incident reporting by providing a financial benefit to the party reporting the incident. This also introduces the potential benefit of trusted parties via the reputation engine. The tokenomics as well as incident movement with validation is demonstrated in the diagram below.

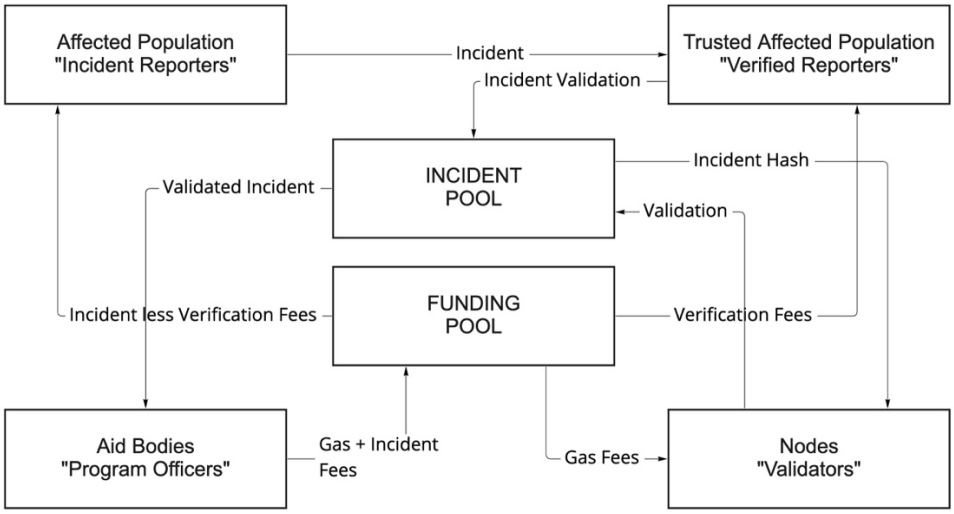

Figure 4: Tokenomics of Funded Incident Reporting

Note: The distribution of incident and verification fees will be configured by the program officer.

Our intent is that by recognizing the higher adoption of funded incident reporting programs by affected populations, more bodies will utilize this mechanism tokenomics model.

Incident Exchange

The incident exchange will also leverage a funding mechanism whereby the requesting party will provide their request in the form of a bid, with all fees (less gas) being transferred to the program officer of the incident data. This data can only be exchanged by the original program officer to protect the data ownership and disincentivize agents.

10. Future Roadmap

While the launch of Ante will be focused on humanitarian efforts, we recognize that its governance framework can be applied to other commercial use cases. There are three key phases that constitute the release of Ante.

Phase 1: Incident Reporting

Securely reporting incidents with program officers with an anonymized framework is fundamental to building a trustless ecosystem. With the corruption that presently exists within developing nations, there is a lack of security underpinning the reluctance of members within an affected population to report incidents to which they are exposed. Combining this with a strong reputation engine is pivotal to adoption of the platform's first release.

Phase 2: Incident Exchange

Poor data governance and politics prevents humanitarian bodies, both public and private, from establishing data exchange policies. By developing a framework for exchanging incidents supported by the blockchain technology mandating the appropriate storage of incidents, de-identified data can be exchanged that promotes the efforts of humanitarian bodies providing varying aid in the same region.

Phase 3: Commercialization

The primary focus of humanitarian aid will be leveraged to combat pertinent issues in other verticals. After applying a framework to incident governance for humanitarian applications in developing nations, Ante will build its profile as a technology company with strong humanitarian principles. This will be utilized to address relevant issues such as company licensing and third-party evaluations to reduce capitalism motivated corruption.

11. Conclusion

We have proposed a system for incident reporting on scale to deliver aid more effectively. We began by demonstrating a model for storing incident data off-chain to preserve security. This was coupled with an on-chain verification mechanism to govern the integrity of incident data. An exchange has also been suggested to enable sharing of incident data between programs undertaking aid to the same people but with varying, positively motivated intentions. Supporting this with a powerful reputation engine reduces manual labor exponentially by utilizing predictive learning to attribute trust to reporters of incidents. By developing this framework, we will build trust in areas where our society has failed the people it was built to protect.

Through these efforts, we will fulfil our mission of enabling the secure collection of data from people to drive effective aid.