A Minimal Approach to Linked Trust with Uncertainty

By Golda Velez <golda@whatscookin.us>

Achieving trust, or conversely reducing risk, requires a robust data set that in general is not under the control of the subject. Verifiable Credentials are a valuable input, as are SBTs (the concept of Soul-Bound Tokens, a not fully defined approach of blockchain based assertions), but in order to maximize the value of available data a minimal format is desired to allow third parties to make uncertain claims based on observed sources. Structured but uncertain data can then be included in the graph of potential inputs to decision making models.

Drawing from experience in combatting organized fraud, human rights advocacy, and a series of public discussions held in the dSocialCommons.org spaces, this paper proposes a minimal format that is simple and permissionless to use for any observer, whether or not they are the original source of the claim.

Proposed Format

For risk models, broad adoption and ability to import existing datasets may take precedence over verifiable challenge-response capabilities. Subjects of risk claims are also likely not to have a DID or wallet but may be identified in a practical sense by the URI of the identifier or device they have used in actions, or by a public handle. Claims linking URIs to each other will be key to creating an effective trust graph.

Further, in the frequent case that the information in the claim is scraped from existing web2 sources or is from other second or third hand data, the claim being made by the issuer is that the subject has made a claim about the object. The degree of uncertainty expressed refers to the issuer's level of uncertainty or conversely willingness to stake reputation that the contained claim is valid.

In the author's view the Verifiable Credential format is not required, but is used here as an example rendering to be compatible with standards:

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://trustclaims.whatscookin.us/claim/1001",
  "type": ["VerifiableCredential", "LinkedCredential"],
  "issuer": "https://trustclaims.whatscookin.us/issuers/101",
  "issuanceDate": "2022-08-19T00:00:00Z",
  "credentialSubject": {
    "id": "https://en.wikipedia.org/wiki/Myanmar_Army",
```

```
    "name": "Myanmar Military",
    "linkedClaim": {
         "claim": "harmed",
         "object": {
             "id": "https://en.wikipedia.org/wiki/Salingyi_Township",
         }
         "aspect": "risk:safety",
         "effective_date": "2021-12-07",
         "how_known": "second-hand",
         "source": [ "direct conversation with local resident", "https://twitter.com/S
         "qualifier": "12 villagers were burned to death by Myanmar military, accordin
         "confidence": .9,
         "reviewRating": {
             rating: -100,
             rating_max: 100,
             rating_min: -100
         }
    }
  },
  "proof": { ... }
}
```

Linked Claims

The importance of linked claims in assigning accountability and propagating assertions of either positive or negative impact may be seen in the following examples:

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://trustclaims.whatscookin.us/claim/1001",
  "type": ["VerifiableCredential", "LinkedCredential"],
  "issuer": "https://trustclaims.whatscookin.us/issuers/101",
  "issuanceDate": "2022-08-19T00:00:00Z",
  "credentialSubject": {
     "id": "https://chevron.com",
     "name": "Chevron, Inc",
     "linkedClaim": {
         "claim": "related_to",
         "object": {
            "id": "https://en.wikipedia.org/wiki/Myanmar_Army"
         },
```

```
         "aspect": "relationship:financial",
         "effective_date": "2022-07-19",
         "qualifier": "Public sources indicate Chevron continues financial relationshi
         "how_known": "web",
         "source": ["https://www.hrw.org/news/2022/07/19/myanmar-totalenergies-withdra
                    "https://www.sec.gov/Archives/edgar/data/0000093410/00012146592200

         "confidence": 0.8,
     }
  },
  "proof": { ... }
}
```

Any self-signed format would suffice, and in fact a format based on the Ceramic ComposeDB models written to IPFS using signed commits may be used in place of Verifiable Credentials.

The important aspects that enable linked claims are as follows:

- The ability of a third party to create a claim based on observations
- Distinguishing between first-hand, second-hand and public or web sources
- The ability to cite sources
- Staking of reputation by asserting a confidence level
- The ability to identify subject and object of claims by any URI, and to further link URIs to each other
- The ability to specify an effective date indepenent of the issuance date ie when did the information become public, or when was it known, vs when the claim was actually written
- Ability to make claims about the issuer of other claims
- Brief full text explanation in human readable format

Use Cases and Adoption

Verifiable Credentials are normally adopted by the holder for compelling reasons such as background checks required by employment.

Third-party claims may be unwelcome. Why would they be adopted?

Use cases may be risk-related, but not always. Example use cases include

- Anti-Spam labelling of domains/headers or other assets
- Whitelist labelling of friend of a friend

- Verified philanthropy based on direct claims of benefit or observations of credible volunteers
- Peer reviewed work is valuable for granting tokens, governance, hiring etc. Rolling up many granular claims that may be exported from a task tracker or from git commit history may be more valuable than "5-star" ratings
- Fraud prevention. Currently data about compromised devices, servers and phone numbers are not shared between organizations, and individuals reporting fraud have no easy way to add data into a larger ecosystem.
- Server reliability - even metrics on server uptime or downtime can be turned into claims

Having a minimal format with minimum overhead can lead to broad adoption in a wide heterogeneous set of use cases, which when linked together can be robust against coordinated bad actor attacks. Broad adoption and large aggregate data sets can also protect sensitive identities.

Ideally, the same schema will support claims about servers, laundry detergent and human rights violations.

Open Decentralized Storage

Writing claims to IPFS via Ceramic, Filecoin or other decentralized, content-addressed storage mechanisms provides a permissionless way for participants to add claims to the ecosystem with minimal overhead.

Other participants in the ecosystem that are running models to make predictions or scoring of entities may be incentivized to pin or maintain the storage of claims. By writing to a decentralized storage the claims are freed from control though signed by the issuer.

Potential for Abuse

Clearly any system that allows third party claims about individuals is subject to abuse, including doxxing and unwelcome linking of identities. This vulnerability is not unique to any particular format but is worth calling out that responsible modellers and those pinning or storing claims should be subject to mitigations of harm and should have methods to remove content from their systems that violates terms of service.

YAML Format

For human readability, a simple rendering of the suggested format follows:

```
issuer : who says
```

```
claim:

      subject: structured obj, text or did
      claim: fixed-vocab-string
      object: structured obj, text or did
      qualifer: string, (optional)
      aspect: fixed-vocab-string (optional)

      how_known: thing or array of thing
      source: thing or array of thing
      effective_date: date

      confidence: float, 0..1 (optional)

      reviewRating: (can use existing from schema.org, optional)
              rating: float, optional
              rating_max: float, optional
              rating_min: float, optiona

signature:
date_signed:
```

Related Work

TrustGraph by Harlan Wood

Decentralized Society: Finding Web3's Soul the SBT token paper by Vitalek Buterin, E Glen Weyl, Puja Ohlhaver May 2022

A Media Type for Reputation Interchange Reputons

Verifiable Credentials Data Model v2.0 11 August 2022

Open Reputation Feed proposal for Disincentivising Disinformation thru Credibility Staking

TrustNet from Alexander Cobleigh

Sharable Greylists a proposal from Matrix Foundation

LinkedTrust LinkedTrust at cooperation.org

Collaboration at and Beyond RWoT 11

The author of this paper seeks individuals that are interested in expressing or applying observed linked trust claims. We have a small team at Cooperation.org/WhatsCookin.us applying this format to several use cases, from

"coupons for good" to worker pools, and welcome any collaboration or extension of the ecosystem.

We are interested to support others who are working in the area of trust and reputation and to convert claims to and from other useful formats. While pragmatic use cases and adoption are foremost in our current efforts, we recognize the importance of standards bodies and hope to be in compliance with W3C standards.