

Portable Reputation Toolkit Use Cases

By Christopher Allen, Tim Daubenschütz, Manu Sporny, Noah Thorp, Harlan Wood, Glenn Willen, Alessandro Voto

This paper was created as part of a collaborative working group at the Rebooting The Web of Trust DesignShop. The proof of concept technical implementation is [here](#).

The Goal: Decentralized Verification

In social networks and markets and on value chains we have a hard time determining what is true and who to trust. Verified information is critical for the functioning of a networked democratic society. The portable reputation toolkit is intended to address these issues by using cryptographic signatures and decentralized technology such as decentralized identifiers, blockchain, and distributed data storage.

This white paper outlines several concrete use cases. These include decentralized fact checking for political journalism, decentralized Fair Trade supply chain certification, and decentralized skill certification without a centralized institution.

The process for each of these use cases is to:

1. Create assertions that can be traced back to individual user identities through signed claims
2. Refute or support assertions by referencing separate evidence
3. Run a search for verifiable information about an assertion and filter based on the trust of the sources
4. Determine if an assertion is likely to be true based on evidence, evaluations, and trust in those making the claims

Although perfect knowledge is fictional, we can decrease the costs of verification and increase the costs of lying.

Use Case: Decentralized Social Media Fact Checking For Political Campaign Journalism

Goal: Bob wants to know if Alice's assertion about politician Charles is backed up by reliable evidence.

Roles: Assertion Maker, Evidence Provider, Reader, Journalist

Alice the **Assertion Maker** posts the assertion in her social media timeline that the politician Charles is responsible for violently intimidating journalists that are writing unfavorable articles. As evidence to support her Evaluation she includes links to **Evidence Provider** Juan's videos of police officers physically harassing journalists at several political rallies and to leaked emails that are relevant.

Juan is a trusted news source who is has been certified for his skills using a Decentralized Certification (see below). The videos are signed by Juan's private key associated with a distributed identifier (DID). **Reader** Bob can now more accurately evaluate if the assertion is true based on Juan's evidence.

Journalist Elon searches for many assertions, evaluations, and signed evidence sources about politician Charles. Elon writes an article detailing the abuse of power by politician Charles. The article carefully references the assertions that have been verified through decentralized methods.

Use Case: Decentralized Skill Certification For A Security Reviewer

Goal: Bob wants to evaluate if he should hire Alice for a cryptographic security code review.

Roles: Employer, Worker, Skill Evaluator

Worker Alice is a security reviewer in the crypto community. **Employer** Bob wants to know if he should hire Alice for a code review of cryptography related code. Alice makes the proposition that she is "competent at crypto code reviews". She signs the proposition with her DID at a specific time. **Skill Evaluator** Charlie evaluates code and pen test reports by Alice as well as a video review of a former collaborator. He records his evaluation with references to the evidence affirming Alice's proposition that she is "competent at crypto reviews". Bob reviews Charlie's evaluation and hires Alice for a crypto review.

Use Case: Decentralized Fair Trade Supply Chain Certification

Goal: A Shopper wants to know if her coffee is Fair Trade based on Evidence provided by a supply chain of multiple companies and individuals

Roles: Product Owner, Supplier, Worker, Retailer, Shopper

Claim Types: Assertion, Evaluation, Evidence

The **Product Owner** for a coffee company creates a distributed identifier (DID) and a corresponding private key. The **Product Owner** publishes an **Assertion** that their Fair Blend coffee product is Fair Trade and signs it with their DID private key. The assertion is timestamped and made available to **Suppliers** and **Workers**. Initially there is no **Evidence** to evaluate if the assertion is true or false - so it is considered "Not Verified".

The **Product Owner** purchases coffee from a **Supplier**. The **Supplier** posts **Evidence** of their transaction and signs them with their DID. This **Evidence** is initially independent of any **Assertion**. The **Supplier** then posts an **Evaluation** that supports the **Product Owner's Fair Trade Assertion**.

The **Product Owner** places a physical tag on all products from this batch of coffee, linking the physical good to the **Fair Trade Assertion**. This could be a smart tag, as Chronicled has done for counterfeit sneaker checking on a blockchain.

The **Retailer** buys the Fair Blend Coffee from the **Product Owner**. The **Retailer** has a standard filter for **Fair Trade Assertions**. A list of trusted keys is maintained, with weightings for each source. An algorithm crunches through the relevant Evaluations and Evidence to determine a Rating for the Assertion that the Fair Blend product is Fair Trade. The assertion Rating can evaluate to "Verified", "Not Verified", or "Contested". At the time the Retailer purchase the coffee for their store the Fair Trade Assertion evaluates to "Verified".

Several **Workers** challenge the **Fair Trade Assertion**. They post Evidence on their employment and wages and documentation of a market price snapshot from a trusted ticker oracle. They post an **Evaluation** that compares their personal information to the **Fair Trade Assertion's** timestamp to show the price was under market rates. They use their DID to sign their Evaluation of the **Evidence** that challenges the **Fair Trade Assertion**.

In the retail store, a **Shopper** waves their phone over the NFC tag, which brings up their Fair Trade Association filter app. A filter in their app determines a challenge to the **Fair Trade Assertion** came from the DIDs of workers who participated in producing Fair Blend coffee. The app presents a "Contested" claim message, noting both the **Supplier's** supporting **Evaluation**, the **Worker's** challenge and the associated **Evidence**. The shopper chooses another filter to get a second opinion. They choose to buy a different coffee that has a "Verified" **Fair Trade Assertion** from a different **Product Owner**.

At the register the **Shopper** complains to the **Retailer** that the Fair Blend coffee is no longer Fair Trade. The **Shopper** contacts the **Product Owner** and puts pressure to remediate the payment issue with the **Workers**. Once remediated the **Product Owner** and **Workers** provide new **Evidence** and **Evaluations** of the **Fair Trade Assertion**.

The **Shopper** returns to the **Retailer** and waves their phone over the NFC tag, which brings up their Fair Trade Association filter app. The app presents a “Verified” rating for the **Fair Trade Assertion**. The **Shopper** purchases the Fair Blend coffee, confident that it has been produced ethically.

General Use Case

A user creates a **Distributed Identifier** (DID). They get an accompanying private key that they use to sign assertions.

A user makes an **Assertion** using a JSON-LD claim format. It is signed with their DID and timestamped with a decentralized timestamping service like Open Timestamps. The assertion includes the submitter’s DID and a target identifier that the the assertion is about. Later claims can evaluate or invalidate the statements by pointing to the assertion.

Users publish **Evidence** JSON-LD claims. Evidence is signed by a user’s DID. Evidence JSON-LD claims link to media, with a unique identifier. The evidence doesn’t have to be related to any assertion initially. Evidence can be related to any assertion at any time using an evaluation.

Any user can challenge or support an earlier assertion with an **Evaluation**. An evaluation references an assertion and evidence. It supports or refutes the assertion. This evaluation will always point to an assertion, and have a true/false or 0-1 float value judging its “truthfulness”. Evaluations are signed by the creators DID and timestamped.

The end user validates the truthfulness of an assertion by querying evaluations and evidence associated with it using an algorithm called a **Filter**. Users can develop a list of trusted evaluators for themselves, import a list from others, or use a filter template that includes evaluator trust parameters and weightings. The filter factors in the evidence, the evaluations, and the trust in the reputation of each of these to determine the truth or falsehood of the assertion. The user can apply multiple filters and audit the Filter to gain multiple perspectives.

Appendix: Example Workflow For Decentralized Certification

A Web Page

[http://](#)

Person A



Location: San Francisco
Profession: Haxor
Interested in: Hacking, Hacking, Hacking, Hacking, Hacking, Hacking
Biography: When I was a kid, my parents got me a computer...

Skills

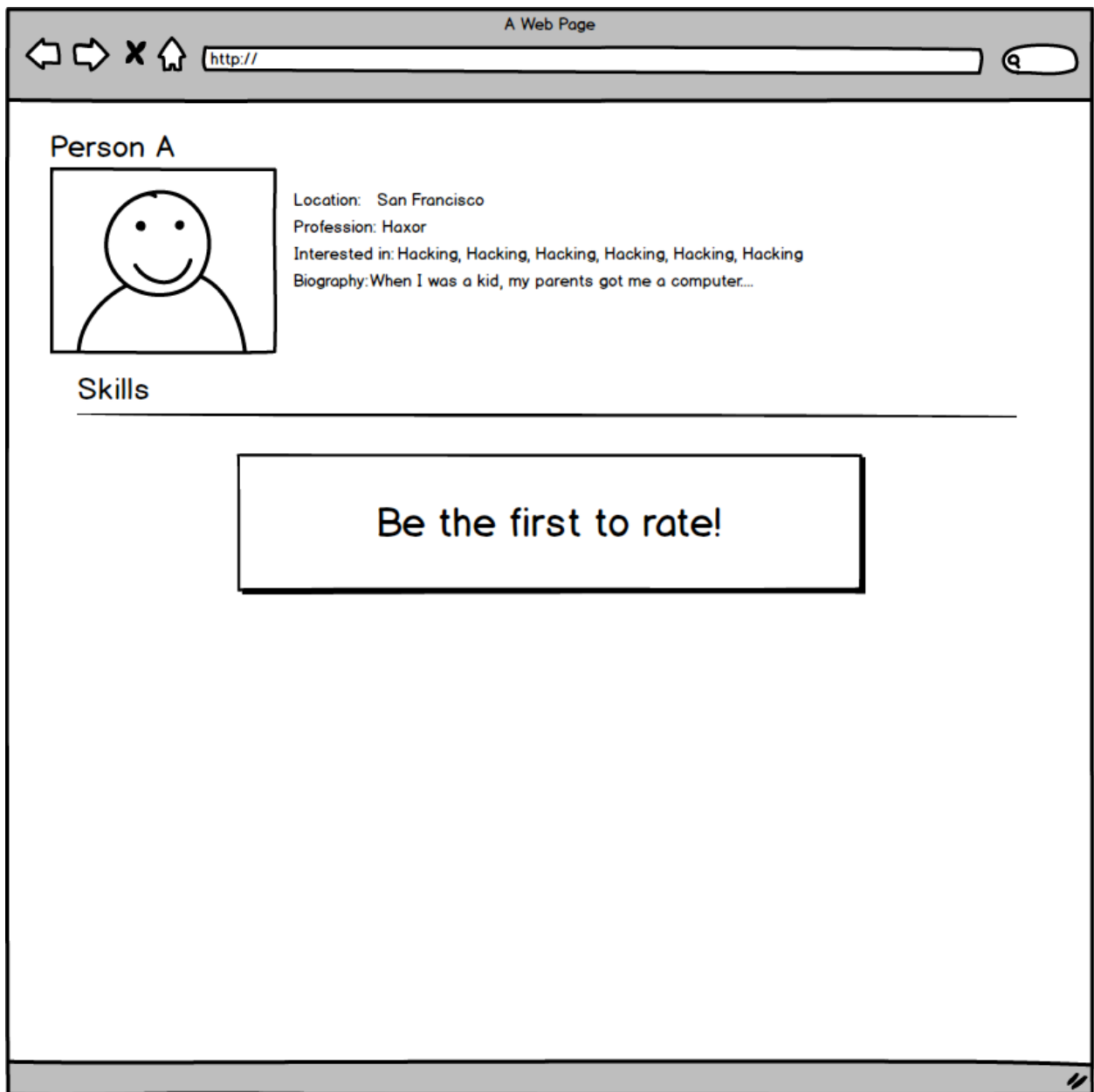
Verified ✓

Person B said about Person A's Crypto skills:

"Affirm/Refute"-Score:

Person B said about Person A's Blockchain skills:

"Affirm/Refute"-Score:



A Web Page

←

→

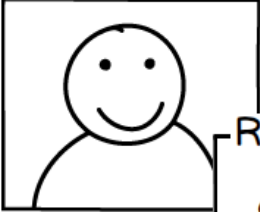
✕

🏠

http://

🔍

Person A



Location: San Francisco

Profession: Haxor

Interested in: Hacking, Hacking, Hacking, Hacking, Hacking, Hacking

Skills

Rate a skill of Person A

Choose a skill to rate:

🔍 search commonly rated skills

Description of Person A's skill:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,

Supporting evidence:

Upload evidence

(We store it on IPFS)

or add some links

http://www.evidence.com/the_evidence.txt

+

http://...

Submit your Rating

11