Portable Reputation Toolkit Use Cases

A White Paper from Rebooting the Web of Trust III Design Workshop

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

The proof of concept technical implementation is at https://github.com/WebOfTrustInfo/portable-reputation-toolkit/

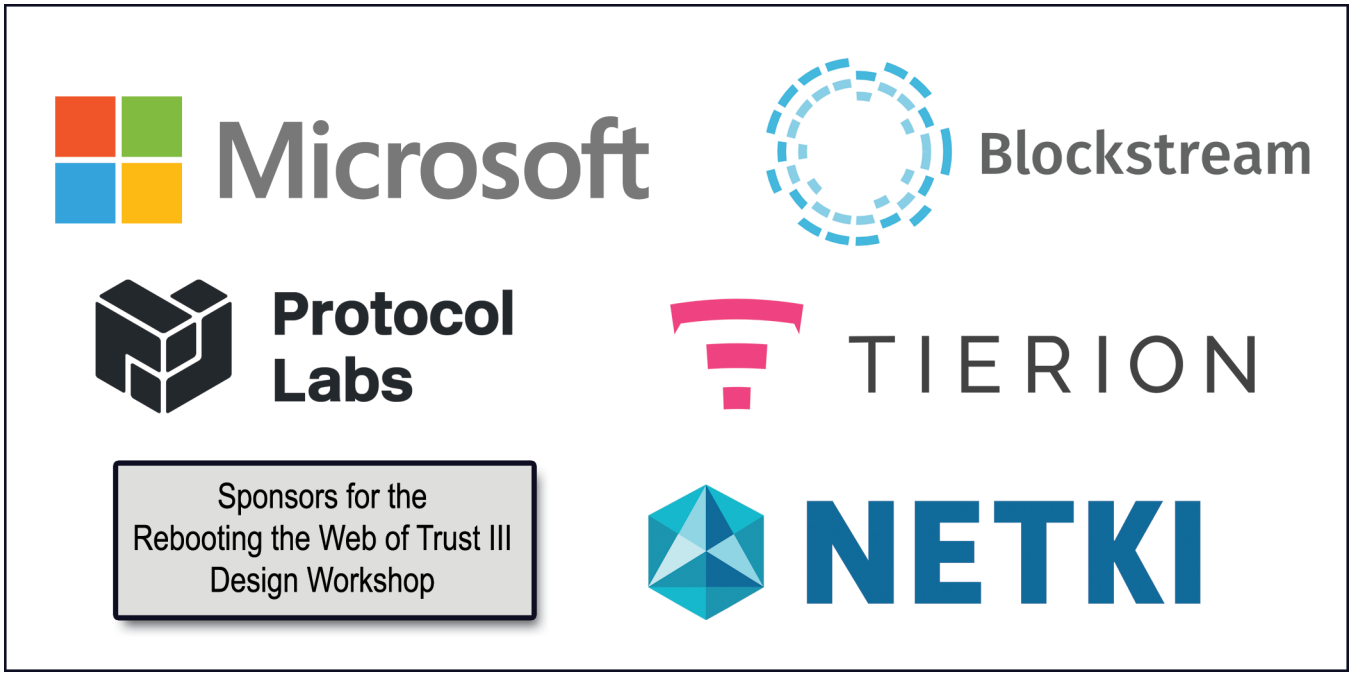
THE GOAL: DECENTRALIZED VERIFICATION

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

Claim Types: Assertion, Evidence, Evaluation

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

Claim Types: Assertion, Evaluation, Evidence

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 *assertion* that she is "competent at crypto code reviews". She signs the *assertion* 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 it 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 decide 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 "Verifed" 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.

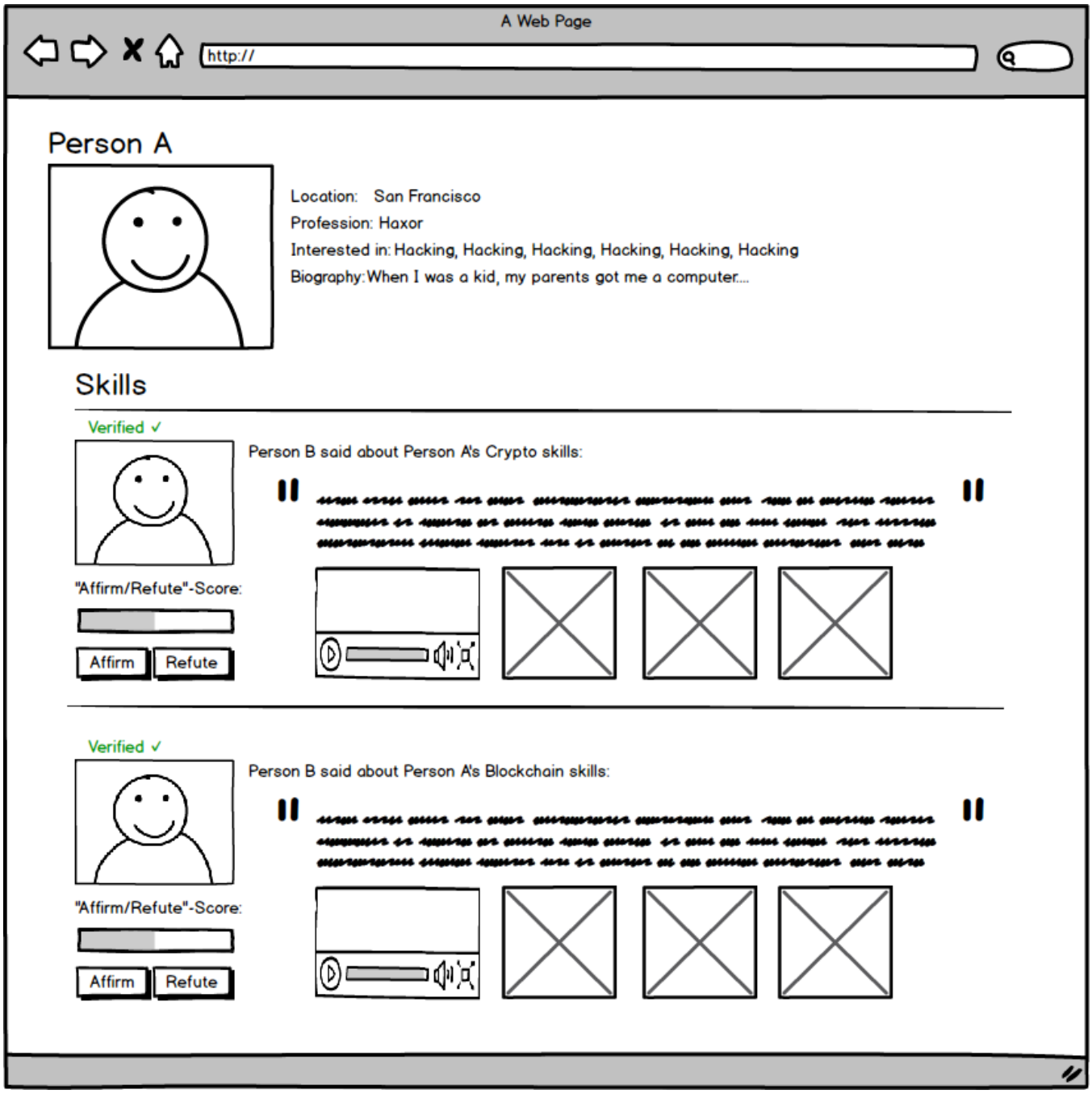
A user makes an **Assertion** using a JSON-LD claim format. It is signed with their DID and timestamped with a decentralized timestamping service like Open Timestamps. The assertion includes the submitter's DID and a target identifier that the the assertion is about. Later claims can evaluate or invalidate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

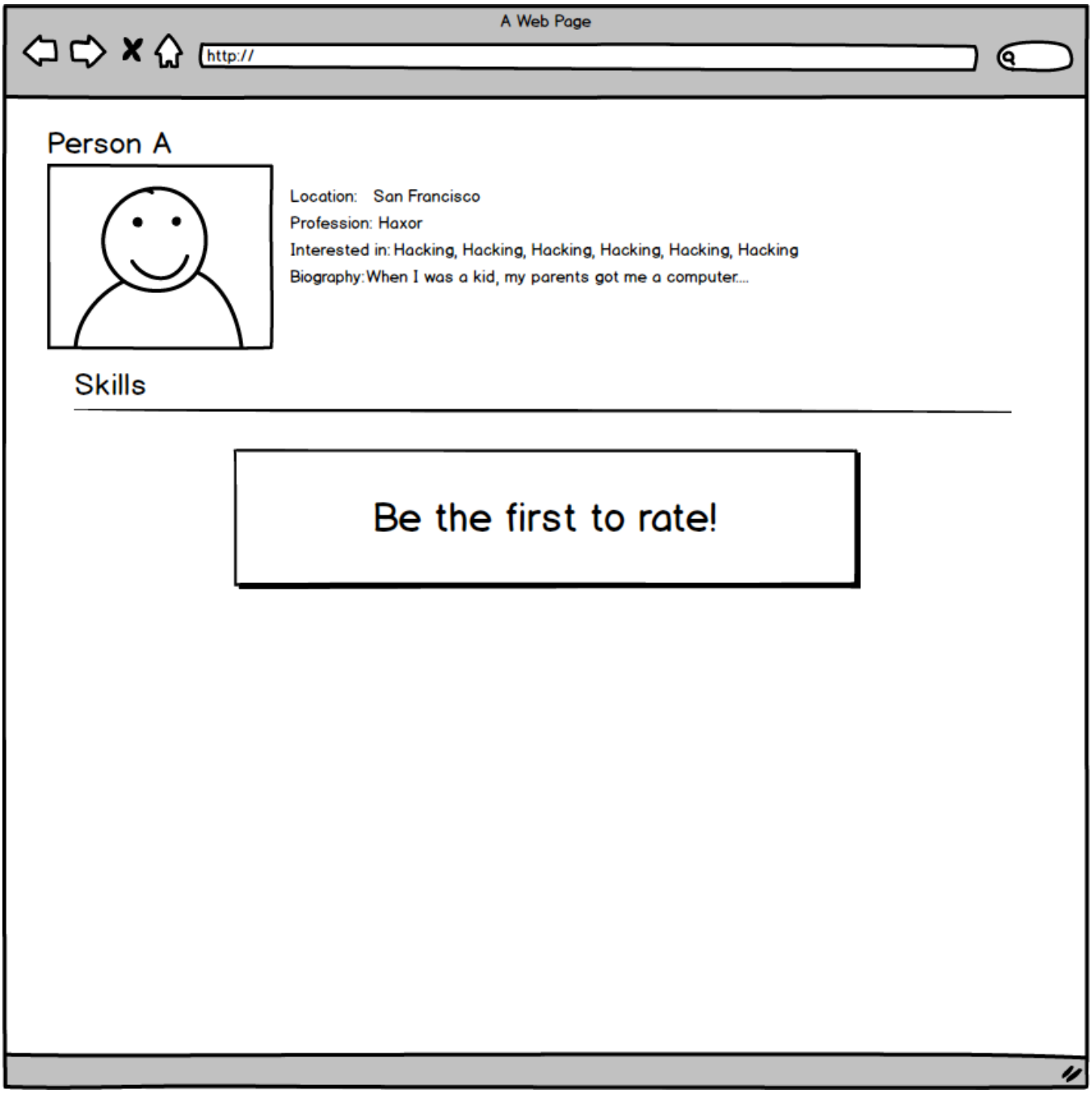
Users publish **Evidence** JSON-LD claims. Evidence is signed by a user's DID. Evidence JSON-LD claims link to media, with a unique identifier. The evidence doesn't have to be related to any assertion initially. Evidence can be related to any assertion at any time using an evaluation.

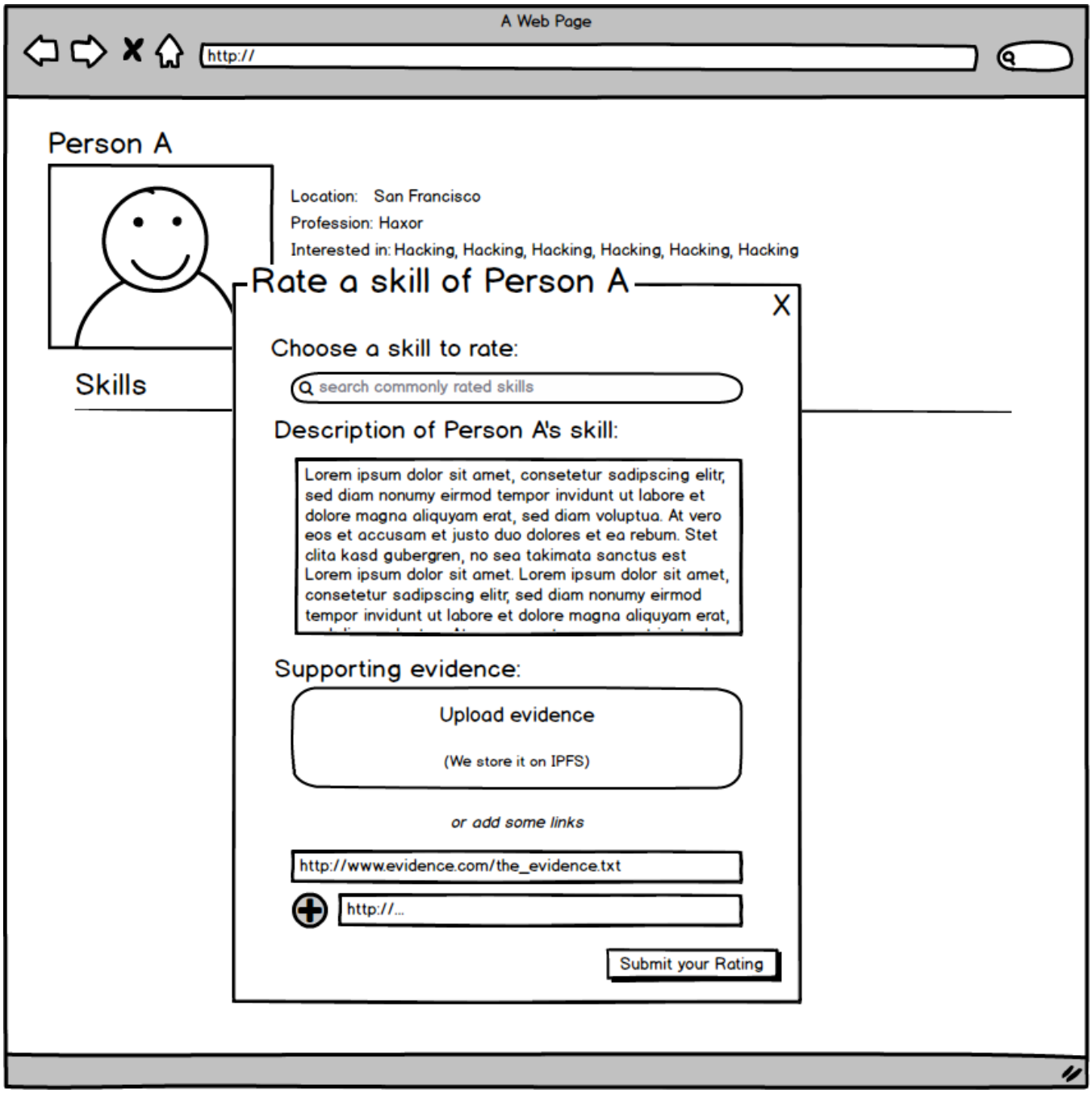
Any user can challenge or support an earlier assertion with an **Evaluation**. An evaluation references an assertion and evidence. It supports or refutes the assertion. This evaluation will always point to an assertion, and have a true/false or 0-1 float value judging its "truthfulness". Evaluations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

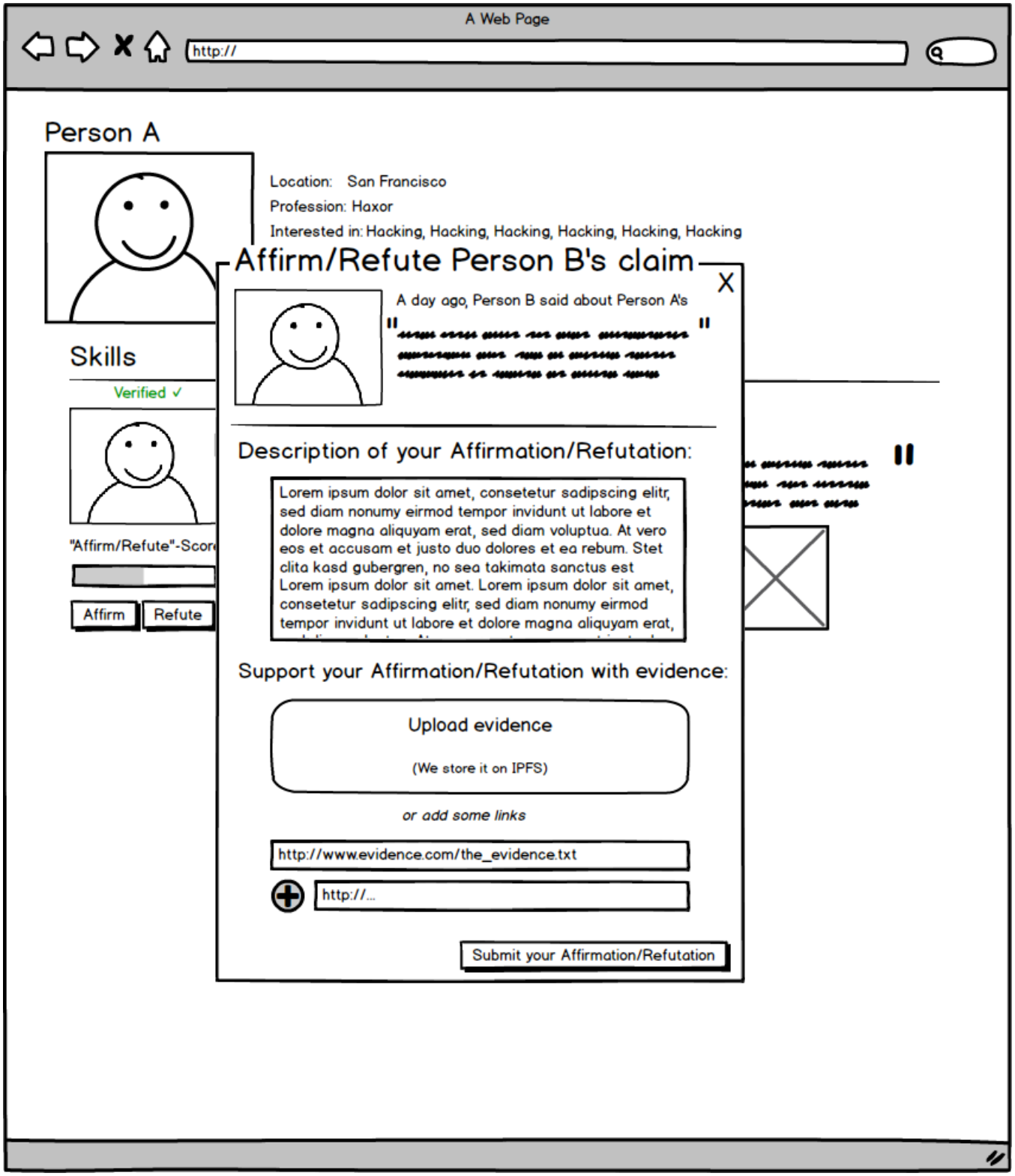
The end user validates the truthfulness of an assertion by querying evaluations and evidence associated with it using an algorithm called a **Filter**. Users can develop a list of trusted evaluators for themselves, import a list from others, or use a filter template that includes evaluator trust parameters 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
Be the first to rate!


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
X
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


A Web Page
http://
Person A
Location: San Francisco
Profession: Haxor
Interested in: Hacking, Hacking, Hacking, Hacking, Hacking, Hacking
Affirm/Refute Person B's claim
X
A day ago, Person B said about Person A's
Skills
Verified ✓
"Affirm/Refute"-Scor
Affirm
Refute
Description of your Affirmation/Refutation:
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,
Support your Affirmation/Refutation with evidence:
Upload evidence
(We store it on IPFS)
or add some links
http://www.evidence.com/the_evidence.txt
http://...
Submit your Affirmation/Refutation

Additional Credits

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

Lead Editor: Noah Thorp

About Rebooting the Web of Trust

This paper was produced as part of the **Rebooting the Web of Trust III** design workshop. On October 19th through October 21st, 2016, over 40 tech visionaries came together in San Francisco, California to talk about the future of decentralized trust on the internet with the goal of writing 3-5 white papers and specs. This is one of them.

Workshop Sponsors: Blockstack, Microsoft, Netki, Protocol Labs, Tierion

Workshop Producer: Christopher Allen

Workshop Facilitators: Christopher Allen and Brian Weller, additional paper editorial & layout by Shannon Appelcline, and additional support by Kiara Robles and Marta Piekarska.

What's Next?

The design workshop and this paper are just starting points for Rebooting the Web of Trust. If you have any comments, thoughts, or expansions on this paper, please post them to our GitHub issues page:

https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/issues

The next Rebooting the Web of Trust design workshop is scheduled for Spring 2017 in Paris, France. If you'd like to be involved or would like to help sponsor these events, email:

ChristopherA@LifeWithAlacrity.com