Rebranding the Web of Trust

A White Paper from Rebooting the Web of Trust

by Shannon Appelcline, Dave Crocker, Randall Farmer, and Justin Newton

Abstract

The *Web of Trust*. It's the buzzword for a new model of decentralized identity. However, it's also a phrase that dates back almost twenty-five years and has been heavily overloaded with meaning during that time. The classic definition of Web of Trust derives from PGP, but the top Google results refer to a website reputation rating system created by a Finnish internet company. Meanwhile, some use it as a big tent that includes identity authentication & verification, certificate validation, and reputation assessment, while the vibrant blockchain community is also drawing new attention to the classic concept.

To build a contemporary Web of Trust, we need to better define it. To do so, we must both understand what the classic Web of Trust was and create a model for the elements of trust that are contained within a more modern definition.

Rebooting the Web of Trust Sponsors

respect network

pwc

alacrity software

OIX OPEN IDENTITY EXCHANGE

1. What is the Historic Web of Trust?

Phil Zimmerman originated the phrase "Web of Trust" in PGP 2.0 (1992). However, his Web had a *very* limited meaning, focused on peer validation of public keys. This process occurs when a user identifies certain public keys as belonging to certain people. However, it goes a step beyond that: the owners of some of those trusted keys might in turn identify other public keys as belonging to other people.

These multiple levels of validation form an interlinked network that creates trust metrics for the correlation between a public key and a person's identifier — which came to be called the *Web of Trust*. A more accurate term for the original Web of Trust might be: a *decentralized key validation system.*

In the years since its advent, PGP has become more than just a technology. It has become the heart of a movement advocating confidentiality, privacy, security, and autonomy in computer services. This expanded emphasis requires that a contemporary definition of the Web of Trust move past the classic definition of PGP. However, this must be done with care because the contemporary Web of Trust contains … multitudes.

2. What is the Contemporary Web of Trust?

Modern cryptographers and privacy advocates embrace the term "Web of Trust" not just because of its origins in PGP, but also because it's meaningful to them. Deciphering that meaning requires examining what both Web *and* Trust mean to contemporary proponents.

The ***Web*** in Web of Trust refers to systems that are administered in a decentralized manner. PGP offered an example of a specific sort of Web of Trust that was created among peers — a style of integration that's often referred to as "peer-to-peer". However, like "Web of Trust", the term "peer-to-peer" has gotten muddied in the modern day; there's a confusion between peer systems and peer actors.

Using the term "decentralized" instead of "peer-to-peer" helps to move the Web of Trust away from that syntactic issue. However, decentralization has to be carefully defined as well. Is DNS centralized because individual authorities hold records or is it decentralized because there are many such authorities? Is blockchain centralized because there's a single transaction registry or is it decentralized because that database is created by many sources?

To be truly decentralized, a system should have neither a central authority for any aspect of the service *nor* a central coordination. Because of its coordination and authority alike, ICANN thus prevents DNS from being decentralized, while the competitive nature of blockchain ensures that it remains within the definition.

The ***Trust*** in Web of Trust is harder to define. That's in part because even PGP's Web of Trust was never about* trust*. A decentralized key validation system does support a promise of recognition: you can be relatively sure that someone is the same person they were before. But, that's a far cry from actually trusting the people that you're interacting with.

The scope of the Web of Trust has expanded a lot since the early days of PGP. Modern Web of Trust projects include the validation of keys, the validation of signatures, the verification of identities, the protection of privacy, the calculation of reputation, the expectation of behaviors, and much more. There is certainly some *trusti-ness* in all these projects: you're trusting that a key is valid, that a signer is authentic, that an identity is true, that a messages will remain private, that someone is an honest trader, or at least that they'll do what they have in the past. But does this trust match the dictionary definition of a "reliance on … integrity" or a "confident expectation of something"? Sort of yes and sort of no; these various projects muddle the standard definition of turst in part because they're all over the place: they approach trust in a lot of different ways.

Nonetheless, these "trusty" systems form a coherent and well-understood group and are a strong basis for defining contemporary Web of Trust systems.

3. How Do We Model a Web of Trust?

The contemporary Web of Trust can be drawn as a graph of Entities who come together to engage in Actions. Together these two parts encompass all of the elements included in the contemporary Web of Trust — including identity, validation, verification, privacy, and reputation.

The modelling of both of these elements focuses on simplicity: an Entity appears as concentric circles, while an Action appears as sequential steps. Outer levels of the Entity or certain steps in the Action may be left out, to produce simpler and more accessible sub-models.

3.1 A Proposed Entity Model

An ***Entity*** is an objective representation of some person, place, or thing. It's defined by up to four concentric circle: information attributes are built on a core identity, which may be verified and which may be authenticated.

Identity refers to the core concept of what an Entity is. It's represented by a *token* that usually has an externally visible network *identifier* such as an email address or a phone number.

Verification is the process by which an identity is said to be true and correct, not a fake, via some proof of that identity. This is not the same thing as *validation*, which is a mechanical process that shows whether an identity is properly formed.

Authentication is the process by which a person proves that he is in control of an identifier, usually by means of authentication such as a password or private key.

Attributes are extensible data that define (but do not identify) an entity. This might include physical attributes like age, hair color, shoe size; mental attributes like IQ, Myers-Briggs type, or accumulated knowledge; historical attributes like transaction history, voting record, or criminal record; or entirely ephemeral attributes like aspirations, fears, or plans.

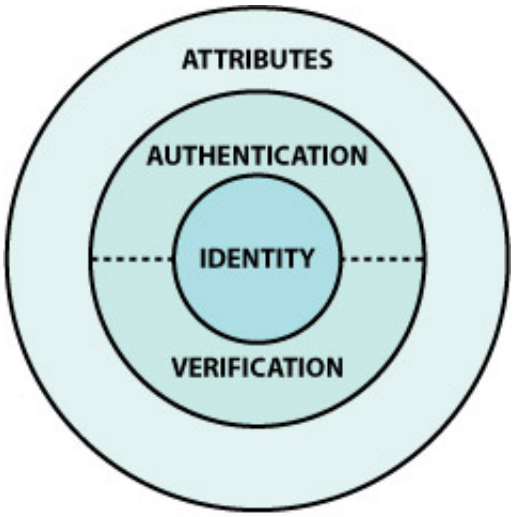

Figure 1: Entity Model

Attributes are created and evaluated through objective, mechanical methods. Some of these attributes might be inherently objective, such as hair color. Others might be the objective encoding of subjective analysis by other Entities. For example, deciding whether an entity is a good or bad credit risk might involve a somewhat subjective decision, but that result is then recorded as an objective fact via a mechanical means.

Though attributes are connected to an Entity, they aren't necessarily controlled by that Entity. Instead, attributes exist in a large and diffuse cloud around the Entity. Some attributes (such as name and hair color) are closely held because they are actually controlled by the Entity. Other attributes (such as credit score and eBay rating) might be much more distant in the Entity's solar system because they're controlled by other Entities or by the Web of Trust's community as a whole.

3.2 A Proposed Action Model

Entities define the identity side of the Web of Trust, but in order for them to come together into a Web, they must perform Actions together.

An ***Action*** is something that occurs outside of the solar system of Entity, when he connects with another Entity. Where an Entity is an objective representation, an Action is instead a subjective interaction. It's defined by up to five sequential steps: decision of privacy, creation of expectations, experience of activity, interpretation of activity, and statement of reputation. Then the rules of the community (or if you prefer the Web) may introduce one final step: manipulation of feedback.

Decision of Privacy requires for Entities to decide what they're going to reveal to each other as part of the Action. They must each decide how much of their Identity, their Verification, their Authentication, and their Attributes to expose, if any; the Entities might decide to reveal nothing, creating a totally anonymous Action.

Creation of Expectations allows each Entity to look at exposed Identity, Verification, Authentication, and Attributes and to compare that to the context of the Action. Then each Entity decides what will he believes will happen over the course of the Action.

Experience of Activity is when the Action actually occurs, and each Entity sees the results.

Interpretation of Activity requires each Entity to subjectively view the results of the Action and decide what they mean.

Figure 2: Action Model

Statement of Reputation combines an Entity's expectations of an activity and his interpretation of the experience. He then proclaims what it says about the other entity.

From the point of view of each Entity, the Action is now complete. They've made their decisions about the Action, they've conducted the Action, they've seen the results of the Action, they've interpreted those results, and they've reported those results. However, a Web of Trust doesn't tend to blindly accept input from the Entities that compose it. Instead, it usually adjusts data before sending it back into the system — just like PGP's Web of Trust validated keys across the Web using very specific rules.

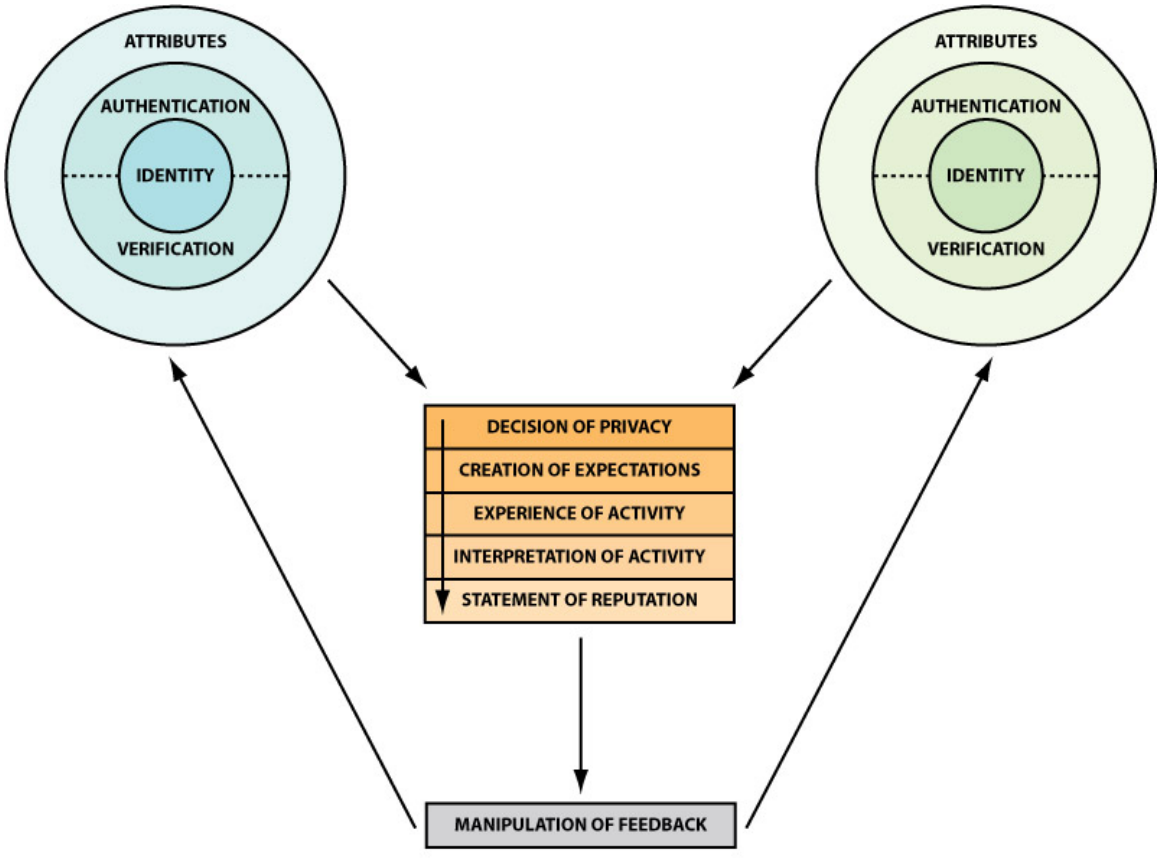

Figure 3: Entity Interaction

Manipulation of Feedback is the final step, where an automated system takes any reputation data stated by an Entity and adjusts it according to specific rules defined by the Web of Trust that the Entities are members of.

Together these rules for reporting reputation and for massaging feedback can do a lot to control the feel of the entire Web. They can discourage negative feedback by bridging problems between Entities; or they could do the opposite. The end result helps to describe what sort of Web is actually being created: is it a true Web of Trust, or is it a Web of Shame?

After the feedback systems have massaged reputation data, it's fed back into the appropriate Entity as a new, updated, or expanded attribute. Such attributes are usually of the loosely held type, because they're not directly controlled by the Entity.

When combined, Entities and Actions create a pictorial model of the contemporary Web of Trust that encompasses the many elements found in its big tent. Questions of identity and verification are addressed by Entities, while privacy, expectations, and reputation all appear in Actions.

3.3 How Does Blockchain Relate to the Web of Trust?

Blockchain has recently become an important player in the contemporary Web of Trust, but it's not actually core to the definition of the term. That's because blockchain is fundamentally a tool. One of its core functions is to create dated certifications of existence in a (hopefully) decentralized way. With that functionality, Blockchain can (and has) become central to the creation of a number of proposed Web of Trust technologies. However it's ultimately just a component that might be used, not an ends in itself.

4. Should We Rename or Reclaim the Web of Trust?

Defining the modern Web of Trust makes it clear that there's real linguistic trouble with the term as it's currently used — especially in its relation to tricky word, "trust". That raises the question of whether the term actually can be reclaimed as part of the modern rubric, or if the field needs to be renamed entirely.

The authors of this paper produced a handful of alternate names for a roomful of crypto, privacy, and decentralization experts. They included: Acknowledgement (ACK) Network, Distributed Identity, Identity Network, Trust Network, Trust Nexus, Web of Characters, Web of Identity, Web of Insights, Web of Names, Web of Recognition, and Web of Validity. By a show of hands, the original Web of Trust was twice as popular as any other option — and the most popular alternatives like Trust Nexus and Trust Network still had the word Trust in them, in any case!

Rather than renaming the Web of Trust, we thus suggest ***Rebranding*** it, with the new, broader definition found in this paper. Entities and Actions. Decentralization. Identity, validation, verification, privacy, reputation, and behavior. These are the many topics encompassed by the contemporary Web of Trust — a movement that's even now expanding and growing.

Additional Credits

Lead Paper Editor: *Shannon Appelcline*

About Rebooting the Web of Trust

This paper was produced as part of the ***Rebooting the Web of Trust*** *design workshop. On November 3rd and 4th 2015, 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: *Respect Network, PricewaterhouseCoopers, Open Identity Exchange, and Alacrity Software*

Workshop Producer: *Christopher Allen*

Workshop Facilitators: *Christopher Allen and Brian Weller with graphic facilitation by Sonia Sawhney and additional paper editorial & layout by Shannon Appelcline*

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: http://bit.ly/weboftrust-issues. We are also planning for more gatherings on this topic in the near future, with the object being to have something notable ready for release on the 25th anniversary of PGP, in July 2016. If you'd like to be involved or would like to help sponsor these events, email:

ChristopherA@LifeWithAlacrity.com