Embedding Human Wisdom in Our Digital Tomorrow

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

by Daniel Hardman, Kaliya Young, and Matthew Schutte

Much of what we know as a species has accreted through experience. We've seen things work and fail, and we've reacted: we've created checks and balances, institutions and procedures, making calculated tradeoffs for the net benefit of individuals and communities. This wisdom is embodied in laws, social norms, patterns, proverbs, and traditions.

The digital landscape, with its turbulent pace and its jockeying technologies, is a new dimension of shared experience. Identity is a central aspect of that new dimension. Who we are, how we interact, how we give and receive value, and how we hold one another accountable are all integral to identity — and they are every bit as important to the digital landscape as they were in pre-digital times.

Software and hardware are more malleable than human nature. Building the code and machines that run a social network can be done in months or years, and mostly by those writing the code — but changes in the nature of friendship, trust, family, employment, and other human relationships are evolutionary, incremental, and undirected, and they unfold over generations and centuries more often than months. This mismatch in evolution matters; we risk rushing into digital construction, and not pausing to consult moral calipers or experiential plumb lines. Widespread surveillance, doxing, online bullying, and the existance of child pornography are all evidence that our digital universe has the same opportunities and pitfalls familiar in other contexts.

Microsoft
Blockstream
Protocol Labs
TIERION
NETKI
Sponsors for the Rebooting the Web of Trust III Design Workshop

We should be deliberate about transferring our wisdom into this brave new digital world. A number of different themes highlight how this wisdom could be advantageous or problematic for our digital future.

THEME 1: VULNERABILITY

Communities often distribute privilege, power, and status unevenly. The reasons for such patterns may be good, bad, or mixed. * Parents care for young children, and proxy them in early interactions; in declining years, children often caretake for their elder parents. This stewardship is at its core altruistic. However, it can turn abusive, so we've created hotlines, requirements for reporting, restraining orders, and social norms as safety rails. * Immigrants cross national borders without the language and cultural skills that would empower them; remediation takes time and effort, and in the meantime, generosity and exploitation are both possible. Regardless of efforts to create equity, disparity emerge: the wealthy accumulate more wealth and the poor are unable to accumplate anything, there are the educated and the unschooled, healthy and sick...

Digital systems need to facilitate patterns of behavior that society has evolved to cope with vulnerability. A digital identity needs to support the notion of guardianship and delegation, for example, but it also needs to make guardianship revocable, with strong accountability and an appeals or dispute process. This sort of technical requirement is not a "nice-to-have" when identity transactions are written to immutable ledgers; it is foundational.

Dictatorships are described paternalistically by their supporters, but experienced as oppressive by most of their population. Will the digital frontier be friendly to coups and power plays, or will it bias toward equal access, symmetric power, and self-correcting imbalance? Will fads and witch-hunts abound, or will systems be resilient to them?

What attitude will digital identity systems take regarding the role of the individual in relation to a group, organization, or state? Today, we see an accountability mismatch and inconsistencies between individuals and corporations (consider the recent Libor and Wells Fargo scandals). Individuals have limited resources, a single physical location, direct legal accountability backed by the threat of force, and one limited lifetime; companies may exist in many locales and jurisdictions, with dynamic membership, diminished sensitivity to force, and unknown lifespan. If the identities of these two types of entities (or of entities at other points on the individual/collective spectrum) are treated the same in digital contracts, transactions, and reputation, will it have the outcomes we hope?

THEME 2: SHADOWS

Shadows on multiple scales are real and affect how individuals, groups, societies, and cultures operate. Examples include, at the individual level drug addiction, at the interpersonal level emotional abuse, at the family level secret keeping, at the social level systemic discrimination of various populations. The emerging digital world can and does actively reveal the shadows.

The leak of the Panama Papers offers an example of how Information and Communication Technologies have enabled the surfacing of the collective shadow of international money systems. This created a global conversation about issues around the use of international banking systems by the elites.

Another example is the public conversation via social media (where anyone with an account can speak to a public audience) spurred by the Donald Trump tape about him assaulting women. Women used that media to speak out with the hashtag #notokay to share their own experiences of abuse by men and surface the extent of it in society.

This trend to surface shadows on multiple levels will continue; we need to understand what healthy collective processes (social and emotional technologies) to use for composting and processing shadows that are surfacing on multiple levels. This will be key to supporting healthy social outcomes rather than creating active suppression that could cause them to fester and eat away at social fabric.

To be clear the authors are not advocating that "everything" needs to be public; privacy is a need of the vulnerable that a wise digital ecosystem will safeguard it. Accountability is also a social good, paired with social and technical norms for how this is achieved in various transactions types.

THEME 3: HEALING

People make mistakes. Things break. We act with imperfect information. And we have a variety of patterns for coping: forgiveness, forgetting, temporary kludges, approximations that are "good

enough", consensus, escalation procedures, heuristics ...

Some identity systems are imagined in ways that depend on idealizations with no room for mistakes. Distributed ledgers are usually assumed to be immutable; the smart contracts they enable are supposed to be executed with automated logic that's 100% trustable; security assumes that key pairs are not compromised.

What happens if these idealizations prove to be untrue (or undesirable)? A smart contract that has a bug is a scary prospect — and it's even scarier if exploitable by hackers. How will debugging and upgrading to a more robust version of the contract happen? Do contracted parties both have to sign off on the upgrade, or can it be imposed by an arbiter? Is the upgrade documented? Is its timing negotiable?

In the physical world, many mortgage delinquencies were probably forgiven for a time, in the wake of Hurricane Katrina. Will our digital world offer an analog, and if so, how easy will it be to trigger?

Is it possible for friends to help me recover keys if Katrina destroys every device I own, and also damages the ISP that hosts some of my cloud data? If a thief steals a key to my house, I can change the locks when I find out; are there digital equivalents?

In normal human experience, youthful indiscretions might be overlooked after years of responsible behavior; in a digital world where no information is forgotten, are there provisions for judicious squinting to skip minor details? Who decides how such provisions work — and are they subject to revision?

THEME 4: TENSIONS

Humans are forever making imperfect tradeoffs. Do we go out and work in the rain to plug the roof of our shed, or do we sit in our snug living room and clean up the damage when the sun is shining? Either choice has pluses and minuses. We make these tradeoffs based on incomplete information (Will the storm get worse? How bad is the leak?), and then we live with the consequences. Sometimes we use temporary workarounds (like running out in the rain and throwing a tarp over the hole in the roof).

Identity systems that are too idealized in one dimension may be uncomfortable or downright dangerous when they can't accommodate human messiness and tradeoffs. For example, a system that perfectly captures history and disallows repudiation may provide excellent accountability but it may also be ripe for misuse. Edwin Black's *IBM and the Holocaust* is a cautionary tale in this regard; superb record-keeping from the census made the Nazi's ability to find and send Jews, and others to the death camps. Making the so called final solution far more efficient than it might have otherwise been.

Temporariness and simplification are interesting considerations. If a person gets a job, discovers that it isn't a good fit after a few weeks, and leaves, should it be okay to omit the detour on a resume or job application? This sort of gloss is innocent and even important to our truth-telling in human contexts; we may agree that describing the detour gets in the way of what's essential. But an identity system that logs everything and treats all events as equally important can't model such choices. If a person has a right to be forgotten, do ex-spouses have a right for their short, unhappy marriage and subsequent divorce to be forgotten too?

Identity depends on context; a system that erodes that principle may conflate things that humans would separate (or vice versa). How should an identity be transferred (or preserved, or transformed) when an individual has a gender transition or chooses to be identified as non-binary, for example? If a person develops Alzheimers, or has a traumatic brain injury, or gets diagnosed as schizophrenic, is their identity invariant? How about a corporation under different CEOs, boards, or legal jurisdictions? Certainly there are facets of identity (the same person may be a mom, a CMO, a patient, a passport holder, and a Den Mother); are there also degrees of identity and sameness, rather than just binary equality? Are we friendly to the truth that identity unfolds as a process, and that the process may be experienced differently by different observers?

THEME 5: COMPLEXITY AND GESTALT

Western thought is generally prejudiced toward an objective, discrete view of reality. We believe in countable, quantifiable things, and we tend to be at least partially unaware of intangibles and systemics.

When a neighbor beautifies their yard, they create value for themselves but they also do so for those who live nearby. Is this a transaction that's associable with their digital identity? In the "real world," it definitely has the potential to affect

reputation and relationships; it may even have monetary consequences if it changes street appeal and thus home prices... Similarly, a corporation that bulldozes a mountaintop might have legal rights that permit the choice, but might steal a beautiful view from thousands of people. Is such behavior recordable on a ledger, or on the reputation systems that depend upon them?

Viewing everything as a transaction yields certain types of insights, but it may be counterproductive as well. If a neighbor shares cookies over the fence, and comes home later to find their flower patch weeded and edged, framing what happened as a tit-for-tat saps the potential for a shared sense of identity — a "we" that emerged from willing friends. The Israeli daycare study, where parents who were fined for late pickup showed spikes in tardiness because they felt entitled by the transaction, speaks to this risk.

Should identity ecosystems ever be tentative? Humans certainly are ... Are we building a gods-eye view with Newtonian sensibilities about objective truth, or something much more pragmatic and integrative?

Work on metacurrencies may teach us something here.

THEME 6: ORGANIZATIONAL CHOICES

The majority of the protocols that run the internet today are at least somewhat centralized, and they tend to be client-server oriented: HTTP, SMTP, DNS, trust chains with certificates, and so forth. Globally useful handles (email addresses, gamer aliases, profiles on social media, phone numbers) are all dispensed by corporations or governments.

Perhaps this reflects our tendency to trust institutions over individuals as a source for verification. State-issued IDs are assumed to be more trustworthy than a hand-written note in the family bible, for example. Are they, in actuality?

It's difficult for an individual to start up a service on their own, without help from an organization like an ISP, an Autonomous System, a domain registrar, etc. Do we like this?

Some voting mechanisms have evolved to balance the power of individuals (or small groups) relative to larger groups; bicameral legislatures are an example.

We'd like to also enable ad hoc and collaborative, grass-roots organizing. It needs to be possible to do tomorrow's equivalent of the march on Selma, and have the organizations built for such efforts not be marginalized by status quo power, just because they are new.

CONCLUSION

There are invisible architectures embedded in the systems that our society relies upon to make decisions and coordinate efforts. Some of these are a result of the contexts and capabilities present at the time of their emergence. However, they are not without consequences.

Hence, as we go about designing and building new systems for fostering interaction and coordination through digital processes, we should be deliberate about what we are building.

If we are unaware of our own assumptions, we may simply re-create in digital form, the very structures that we had hoped to transcend.

Additional Credits

Humanness in Digital Identity Working Group: Daniel Hardman, Kaliya Young, Matthew Schutte

Insights: Natalie Smolenski, Shannon Appelcline, Robert Clint, Joe Andrieu, Zachary Larson

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