Bootstrapping decentralized identities with extant systems

A topic paper for ID2020 Workshop – Jon Geater

> "You can use your idealism to further your aims, if you realize that nothing is Nirvana, nothing is perfect."
>
> — Jon Stewart

Goals

The goals of the workshop as stated are:

1. "Bring together the top contributors in decentralized identity"
2. "Showcase use cases and requires for decentralized identity and trust"
3. "Discuss and suggest approaches to drive adoption of these technologies"

If we believe (as we must, for consistency) that decentralized identities are the model for the future of digital interaction then clearly goal #3 is paramount: we have to find ways of increasing adoption broadly and globally. Goals #1 and #2 are easy: bring passionate people together to do something they're passionate about and they'll have a great time producing all kinds of output and proudly showing each other the fruits of their hard work. But adoption is something different, requiring us to bring along with us the reluctant, the rejected, and the recalcitrant. We have to win the confidence of the skeptical and the scared. We have to overcome societal inertia.

So what challenges stand in the way of adoption, and what can we do to overcome them more effectively? While a great many of the challenges facing widespread adoption of decentralized identity are very far from technical, there are some identity technologies available to us today that will help us to progress if we can work with them rather than seek to replace them.

Essentially when we're talking about rebooting the web of trust in the real world there's rarely a chance at a hard restart: we stand a better chance with a warm reset.

Human factors

> "Never attribute to malice what can be explained by stupidity. Don't assign to stupidity what might be due to ignorance. And try not to assume your opponent is the ignorant one—until you can show it isn't you. M. N. PLANO"
>
> — David Brin, *The Transparent Society*

Many of the barriers to adoption of secure identity technologies relate to UX in one way or another. It's tempting to blame lack of user education for poor adoption of higher-security or better privacy systems than the ubiquitous Pa55w0rd, but the fact is that participating in a cryptographic protocol is Hard, and as a community we have not yet come up with many things that are usable by the average non-expert.

As put forward at the 2015 workshop (and many other times besides) PGP is seemingly simple but famously hard to use at any scale. 2-factor systems are frustrating and clumsy. And when it comes to Bitcoin or blockchain IDs people are not generally equipped to take full responsibility for a private key with no inherent backup or recovery. And so technologies either stay niche, or are forced to re-introduce abstractions, 3rd parties and centralization in order to finesse the hard bits.

So how to develop new decentralized identity technologies that are strong *and* usable? And as quoted by David Brin, relying on increasing technical literacy among the populace may be folly on our part as designers: willful ignorance of how people wish and are able to manage and present their identity online.

Power factors

> "Most men and women will grow up to love their servitude and will never dream of revolution."
>
> — Aldous Huxley, *Brave New World*

While the aims of decentralized identity are many and varied, front and centre is the desire to help to address the balance of power in digital life. According to Huxley, however, the public at large don't want to be helped.

To what degree this is really true is, of course, debatable. And it is certain that the Internet Age has brought about great change in this respect. Nevertheless we cannot ignore that identity is critical to many important areas of established society where centralized control is fundamental, and there are real benefits to these systems that people will be unwilling to risk without a very solid alternative. This alternative must not only reach the same or better technical standard, but it must also provide the same non-technical comforts of legal protection and so on.

Idealism

> "I have always known that the pursuit of excellence is a lethal habit"
>
> — John Irving, *The World According To Garp*

We must absolutely strive for perfection, but along the way we must recognize that *the perfect is the enemy of the good.* Historically there has been a common tendency in the computer science community – and particularly the crypto and security world – to design protocols and systems that are somehow complete and perfect. Arguably this is a major reason for the usability of infosec products being so poor, with unimaginably complex configuration surfaces which aim for 100% coverage and 0% failures, when in fact the real world they're trying to model is much less clear-cut.

Trust is not the same as security, and if we are rebooting we should take the opportunity to re-assert this difference.

Embrace and extend

> "Someday we may look back on this era as a time when rational compromises might have enhanced both security and liberty, but those compromises were refused because each side was so busy self-righteously being right."
>
> — David Brin, *The Transparent Society*

Whether facing technical or economic barriers, ignorance or willful obstruction, or simple inertia, we can make progress in small steps by compromising and working with what we have today even when it may not align with the ultimate goals of decentralization. There will always be areas of life in which centralized control and identity are legitimate and valuable, and we have to find ways of merging these into our vision the same way that aspects of non-digital life are blended and overlapping.

Action

> "The search for Nirvana, like the search for Utopia or the end of history or the classless society, is ultimately a futile and dangerous one. It involves, if it does not necessitate, the sleep of reason. There is no escape from anxiety and struggle."
>
> — Christopher Hitchens, *Love, Poverty, and War*

We have a lot of work to do. We need all the help we can get and we need to focus on winning the right battles and ceding the rest.

A great output from the workshop would be a set of models or architectures that make real progress in some of:

- Harmonizing decentralized ID technologies with prominent ID standards currently being promulgated by existing central authorities (eg NIST SP 800-63, European certified digital signature, etc). Can we make use of existing centrally verified/issued identities to bootstrap larger decentralized webs? While this raises serious issues over linkability/anonymity for certain use cases, it can help to bootstrap decentralization for other use cases and move the technologies forward.
- Making existing systems easier to use. If LetsEncrypt can genuinely work for TLS on websites, what can we do to fix PGP usability, for example? Replacing key signing parties and difficult directory systems with open ledger and reputation systems (eg BlockchainMe) is a good start: what more can we do? Identity-Based Cryptography systems are superficially attractive for transacting in low-trust scenarios but generally require a central private key derivation service that presents technical, economic, and social challenges to their general use. Can we take some lessons from the IBE camp while solving the need for a single Trusted Third Party in the middle?
- Designing the new systems to be easier to use and user-appropriate from the start. A protocol or system that relies absolutely on the generation and safe-keeping of a long-lived personal cryptographic secret is likely to face significant problems in the real world. Systems and services are already available to overcome these challenges with BitCoin wallets (for example) but in doing so they change the attack landscape (and therefore trustworthiness) of the system as a whole.
- Many earlier attempts at making open identity (such as the Identity Metasystem promulgated for years by Kim Cameron) have suffered in part precisely because of decentralized factors: the economics and incentives of running shared parts of the system were troublesome. Now we have a chance to address some of those problems with technologies that are intended to be shared and jointly operated, and can potentially re-use a lot of the earlier thinking. PKI doesn't have to be that bad…