CHRISTOPHER ALLEN

Decentralized Identity &
Blockchain Architect

Co-Chair,
W3C Credentials Community Group

Founder, Chairman,
RebootingWebOfTrust Inc.

Executive Director,
Blockchain Commons, LLC
7302 Yellowstone Rd
Cheyenne WY 82009-2077

@ChristopherA
+1=307-222-2140
+1.510.908.1066
ChristopherA@LifeWithAlacrity.com
http://www.LifeWithAlacrity.com

June 9th, 2020

TO: Wyoming Legislative Select Committee on Blockchain, Financial Technology, and Digital Innovation Technology

Committee Chairs, Members of the Select Committee & LSO:

Thank you for having me back to testify again on the future of blockchain and related technologies in Wyoming.

As some of you know already, my name is Christopher Allen, and I'm an expert in the fields of digital identity, internet security, and the blockchain. Besides being the founder of Blockchain Commons, which is working on several projects that make blockchain technology more accessible, I'm also: the coauthor of the TLS standard, which is the most broadly deployed security standard in the world; the founder of the Rebooting the Web of Trust design workshops, which have released over 50 white papers on decentralized technologies on the internet; and the co-chair of the W3C Credentials Community Group, which has developed the Verifiable Credentials standard. I was central to the incubation of Decentralized Identifiers (DIDs) and am now working closely on their integration with Verifiable Credentials (VCs), both of which are core to many of the identity technologies now being discussed here and elsewhere.

In my testimony today, I want to focus on four main points:

1) Our private key disclosure work should include consideration of identity keys.

2) We generally should plan to do a deeper dive into newer decentralized forms of digital identity, perhaps with new laws, and perhaps with a new task force or sub-committee.

3) As we expand into new public-health technology, we should be careful.

4) Our new blockchain initiatives should require demonstrable interoperability with standards, to avoid vendor lock-in.

Here are some more detailed thoughts on each of these topics:

IDENTITY KEYS. I've spoken previously about HB0041-2000, on the "Disclosure of private cryptographic keys". I wanted to bring additional attention to its current focus on cryptocurrency, as seen in the statement that it is about "digital security or virtual currency to which a private key provides access". We should note the fact that private keys are also used to control access to other things, such as digital identity. I personally do consider these uses a type of digital asset, but it is not clear that the law does. This can be resolved by adding identity keys in the next version of the bill. However, it's likely that in order to do this we will need another bill in place first to establish terminology and the foundation of decentralized digital identity law.

DECENTRALIZED DIGITAL IDENTITY. That brings me to the next topic I'd like to address: decentralized digital identity. I would love to see Wyoming lead the way in this field, as they have so successfully with their blockchain legislation. However, this topic is sufficiently large that it would probably require a multi-year effort and a new task force or sub-committee, much as when you started working with tokens and digital assets. I do believe this would be worth it: though other states and even nations are considering updating their laws regarding decentralized digital identity, they're not really aware of the intricacies and opportunities of privacy-focused blockchain-based decentralized identity; Wyoming could pursue their opportunities, and once established become a world technology leader by doing so.

In considering digital identities, I have three core suggestions.

First, I'd advocate that you do not focus on digital identity using the property-rights law models, as the digital identity community has identified this as being inadequate. Yes, property laws might be sufficient if a stolen digital identity is used to steal real property or digital assets, but there are many other situations where it would not be. What if a stolen digital identity were used to vote? To make decisions at a company? To make statements or take actions damaging to your reputation or rights? To make false statements or take actions that benefit someone else? A digital identity is much more personal and intrinsically linked to someone than property, and it should be treated as such. I would point you to the work of Elizabeth Renieris on the concerns of using property law for digital identities: https://www.linkedin.com/pulse/do-we-really-want-sell-ourselves-risks-property-law-data-greenwood/

Second, we need to be careful to ensure that if someone loses their digital identity, they don't lose access to civic services. India has long offered one of the biggest alarm bells to the rest of the world because they've denied services to people who's digital identity has, in some way, been confused by the system. Kenya may be an up-and-coming hotspot exemplar of this problem: citizens are reporting problems getting new identities and concerns that it will deny them access to schooling, health care, housing, and more. There is a natural primacy that a person has "existence" and thus has rights in the real world that must override any failure in the digital system. Civil servants must have processes to be able to override the digital system. Administrative staff in India and Kenya do not. https://www.nytimes.com/2020/01/28/world/africa/kenya-biometric-id.html

Third, I'd advocate that you dig deep into the subtleties of decentralized digital identity, of which this right to "existence" is just the first principle. I first chronicled ten principles for identity in my early work, "The Path to Self Sovereign Identity" (see near the bottom of http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html) which has been broadly accepted world-wide as the basis of decentralized digital identity architecture. A copy of the 10 principles is enclosed. I would suggest that Wyoming consider these ten principles when enacting new digital-identity legislature, as I believe considering everything from the rights of existence to right to control, requirements for portability and consent, and beyond could help make Wyoming a true leader in this field.

PUBLIC-HEALTH TECHNOLOGY. Obviously, the COVID-19 crisis has thrust us straight into a conversation on public health and using technology to improve information connection and dispersal. I've been getting many calls about the technology and recently testified on AB 2004 in California, a bill focused on verifiable health credentials, building on much of my work with the World Wide Web Consortium standards body. My best advice here is: be careful. We should undoubtedly use legislation to enable the use of privacy-preserving public-health technologies in healthcare pilots. But, we need to be aware that the verifiable credentials technology was not initially designed for the public health scenarios that it's now being used for and thus will require testing and consideration to address other public-health requirements. We also should carefully consider other repercussions such as the possibility for use for discrimination, or unintended consequences of using this technology, such as people deliberately infecting themselves. Overall, though there is great use for verifiable credentials and decentralized identity to protect personal privacy in public health, we also need to be thoughtful and to take care.

INTEROPERABILITY. Finally, I wanted to speak to a need for HB0070-2019, the "industry leading filing system", which I still hope will be reprioritized to ensure that Wyoming is a leader in this space. When some form of corporate "digital birth certificate" is moved to vendor selection, we need to ensure that any solution supports broad interoperability of multiple kinds of DIDs and VCs. This sort of interoperability has already become a major focus at the Department of Homeland Security, which wants to "Help develop and champion interoperability standards specifications that are patent free, royalty free, and free to implement". This is part of their "Strategic approach to ensure competitive interoperable marketplace of solution providers". We should similarly ensure that there is no vendor lock-in for the HB0070-2019 system and by doing so future proof it. However, I suggest that our scope should be larger than just this corporate filing records system: we should ensure that interoperability and flexibility are central to any blockchain or digital identity systems.

Thank you again for this opportunity to address the Wyoming Legislature through my testimony. I always remain available for any discussions or clarifications of my testimony, and I am particularly available for any work you need regarding digital identities and the principles I've suggested for their use.

Regards,

Christopher Allen

The 10 Self-Sovereign Identity Principles

(from "The Path to Self-Sovereign Identity" by Christopher Allen, April 25 2016, published at http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html)

1. **Existence.** *Users must have an independent existence.* Any self-sovereign identity is ultimately based on the ineffable "I" that's at the heart of identity. It can never exist wholly in digital form. This must be the kernel of self that is upheld and supported. A self-sovereign identity simply makes public and accessible some limited aspects of the "I" that already exists.

2. **Control.** *Users must control their identities.* Subject to well-understood and secure algorithms that ensure the continued validity of an identity and its claims, the user is the ultimate authority on their identity. They should always be able to refer to it, update it, or even hide it. They must be able to choose celebrity or privacy as they prefer. This doesn't mean that a user controls all of the claims on their identity: other users may make claims about a user, but they should not be central to the identity itself.

3. **Access.** *Users must have access to their own data.* A user must always be able to easily retrieve all the claims and other data within his identity. There must be no hidden data and no gatekeepers. This does not mean that a user can necessarily modify all the claims associated with his identity, but it does mean they should be aware of them. It also does not mean that users have equal access to others' data, only to their own.

4. **Transparency**. *Systems and algorithms must be transparent.* The systems used to administer and operate a network of identities must be open, both in how they function and in how they are managed and updated. The algorithms should be free, open-source, well-known, and as independent as possible of any particular architecture; anyone should be able to examine how they work.

5. **Persistence.** *Identities must be long-lived.* Preferably, identities should last forever, or at least for as long as the user wishes. Though private keys might need to be rotated and data might need to be changed, the identity remains. In the fast-moving world of the Internet, this goal may not be entirely reasonable, so at the least identities should last until they've been outdated by newer identity systems. This must not contradict a "right to be forgotten"; a user should be able to dispose of an identity if he wishes and claims should be modified or removed as appropriate over time. To do this requires a firm separation between an identity and its claims: they can't be tied forever.

6. **Portability.** *Information and services about identity must be transportable.* Identities must not be held by a singular third-party entity, even if it's a trusted entity that is expected to work in the best interest of the user. The problem is that entities can disappear — and on the Internet, most eventually do. Regimes may change, users may move to different jurisdictions. Transportable identities ensure that the user remains in control of his identity no matter what, and can also improve an identity's persistence over time.

7. **Interoperability.** *Identities should be as widely usable as possible.* Identities are of little value if they only work in limited niches. The goal of a 21st-century digital identity system is to make identity information widely available, crossing international boundaries to create global identities, without losing user control. Thanks to persistence and autonomy these widely available identities can then become continually available.

8. **Consent.** *Users must agree to the use of their identity.* Any identity system is built around sharing that identity and its claims, and an interoperable system increases the amount of sharing that occurs. However, sharing of data must only occur with the consent of the user. Though other users such as an employer, a credit bureau, or a friend might present claims, the user must still offer consent for them to become valid. Note that this consent might not be interactive, but it must still be deliberate and well-understood.

9. **Minimalization.** *Disclosure of claims must be minimized.* When data is disclosed, that disclosure should involve the minimum amount of data necessary to accomplish the task at hand. For example, if only a minimum age is called for, then the exact age should not be disclosed, and if only an age is requested, then the more precise date of birth should not be disclosed. This principle can be supported with selective disclosure, range proofs, and other zero-knowledge techniques, but non-correlatibility is still a very hard (perhaps impossible) task; the best we can do is to use minimalization to support privacy as best as possible.

10. **Protection.** *The rights of users must be protected.* When there is a conflict between the needs of the identity network and the rights of individual users, then the network should err on the side of preserving the freedoms and rights of the individuals over the needs of the network. To ensure this, identity authentication must occur through independent algorithms that are censorship-resistant and force-resilient and that are run in a decentralized manner.