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

May 5, 2020

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

Committee Chairs, Members of the Select Committee & LSO:

My name is Christopher Allen, and I am the founder of Blockchain Commons, a blockchain infrastructure development and research organization. I also represent the broader international standards W3C organization as co-chair of the Credentials Community Group. My past achievements include being co-author of SSL/TLS, the broadest deployed security standard in the world, and the basis upon which most Internet traffic moves securely.

Over the last three years, I have been quite proud to witness Wyoming, through the Blockchain Task Force, become a leader in the area of digital asset technology & regulation. It is because of laws successfully begun at those meetings that I established my organization Blockchain Commons to be domiciled in Wyoming and have encouraged other companies to do the same.

I was asked by the LSO to prepare in advance of your meeting next week to offer my thoughts on your possible agenda for the upcoming legislative year.

My personal first priority is to suggest this Committee reintroduce the 2020 HB0041 bill on the “Disclosure of private cryptographic keys”. I believe this topic is critical for the security of not only blockchain technology but also to the future of digital identity. As the Task Force heard in extensive testimony last year, once a private cryptographic key is disclosed to a judge it is permanently compromised, even if the judge attempts to protect it from further disclosure; all assets and identities tied to that private key are also permanently compromised, as is all future value that may accrue to that key (in the form of forks and airdrops).

Even if well-intentioned, such compelled disclosure could put at risk the entire custody businesses of multi-billion dollar companies because a private key cannot simply be changed once it's compromised, as a password can. To be clear, a judge can still achieve the desired outcome by compelling the *use* of private cryptographic keys (such as to turn over assets in a divorce proceeding, or to prove ownership of an asset) without requiring the disclosure of the key itself. 2020 HB0041 simply resolves essential differences between how cryptographic security works and how it is misunderstood by prosecutors & law enforcement.

In the category of Digital Assets & Property, I've found a few areas that need clarification as digital technology organizations move to Wyoming to implement the opportunities offered under the newly enacted legislation. New laws could accomplish some of these, others could simply be resolved with a formal letter from the Committee to regulators and third-parties parties requesting changes in their policies. These are as follows:

- In 2019-F125 custody of digital assets by banks is defined in 34-29-104 "Digital asset custodial services" and control is defined in 2020-SF0047. However, there are some ambiguities in leveraging newer and safer digital assets custodial practices that don't quite fit these current definitions and may apply outside of custodial services and rules about control by non-custodians. I suggest the following:
    - That in the case of assets held by multi-signature technology, if Wyoming entities hold the majority of the private keys or have sufficient authority to control or leverage digital assets held by private keys, then the assets should remain "located" in Wyoming. The existence of other non-exclusive non-control private keys used to ensure the resilience of holder's assets by parties outside of Wyoming should not put the assets under some other state's authority.
    - That custodial entities like banks and other fiduciaries may make use of multisignature technologies to add resilience to their custodial security and operational practices, and that such use should not violate their mandate to have exclusive control over the digital assets in their custody.
    - That private keys held by fiduciaries under a time-lock branch of a smart contract should not be considered to be in control of the digital asset, and thus custodial, until the time-lock is activated. This allows lawyers and other fiduciaries the ability to accept emergency time-lock keys to protect digital assets against disaster and or key loss of their proper holder.
    - There may be some other advantages and implications of multisignature technology and regulation that the office of the Banking Commissioner may want to research and suggest.
- I would like to see the funding of an independent review of the technical software and hardware requirements to meet the new Banking Commission's regulations for digital asset custodians. The current rules are great, but turning them into practice may turn up problems that can serve as feedback to Banking Commission's policies. For instance, in my first reading, some commonly accepted digital assets practices like BIP32 derived keys don't meet legacy FIPS hardware requirements, as FIPS covers only a small list of cryptographic algorithms that take decades to evolve. Other new blockchain tools like zero-knowledge proofs may also not follow legacy architectures. Digital asset custodians in Wyoming should be able to use best-practices of today, not of banks ten years ago. The funding for this research could potentially come out of application fees.

- There are also significant threats to “Digital Assets & Property” that fall outside the scope of pure digital assets blockchain-related laws, but are related to technology. In particular, the use of DRM (digital rights management) by big corporations and laws against circumventing DRM (so-called Anti-DRM laws) aids parties as diverse as John Deere and HP in disadvantaging and disenfranchising property owners: they prevent owners from repairing their tractors or even personal cars; they stop computer and printer owners from upgrading their hardware; and they result in purchasers of digital books having their ownership revoked arbitrarily. In addition, cryptographic researchers investigating the security of these practices or aiding property owners with tools to take control of their property are being arrested, deported, or sued even when such practices are covered by “fair use” laws. I believe this is a good time for Wyoming to take a strong stance against those leveraging anti-DRM laws to erode the rights of legitimate property holders in Wyoming. See https://www.eff.org/deeplinks/2018/09/defeating-drm-hill-climbing-our-way-glory

I had a few more general comments concerning the utilization of digital properties in Wyoming:

- *Cryptocurrency Payments to Attorneys.* I’ve been told by several companies seeking domicile in Wyoming that Wyoming attorneys are saying that the Wyoming Bar will not let them accept cryptocurrency as payments. (This may or may not be true.) Other attorneys have also told me that their insurance will not allow them to accept custody of cryptocurrency for trustee & fiduciary accounts. I would like to see Wyoming lawyers be able to accept digital assets as payment, to be able to hold those assets in a trust account on behalf of their client, and to be able to hold a private key that is part of a multisignature or time-lock smart contract to help protect the resilience of digital assets held by their clients. These may not require new laws: it could be that these problems can be addressed by sending a letter from the Legislative Committee to Wyoming Bar and to Wyoming regulators of insurance for lawyers.

- *Decentralized Registration of Companies.* At the final Blockchain Task Force meeting in Laramie last year, I presented a demo showing the opportunity to use decentralized identity blockchain technologies for the registration of corporations, which countries like Estonia have been doing for several years. I demonstrated how a Wyoming resident could apply to become a registered agent, and upon approval apply to create a Wyoming corporation by submitting electronic documents to the Wyoming Secretary of State. This demo used approaches and international standards to avoid vendor lock-in. The demo was in support of moving the year-old HB0017-2019 "Commercial Filing System" from "study" to "implement". I have not heard since if there is any progress by the Wyoming Secretary of State on this topic, and I encourage the Commission to urge completion of the study and to fund any implementation.

- *Registered Agents & Blockchain Laws.* I still have a concern that older laws and regulations about the requirements of registered agents to store information about their clients may conflict with some of the new 2018 and 2019 corporate blockchain laws allowing entities to use keys to represent stockholders. A registered agent should be able to offer other parties & authorities the ability to serve notice to their clients. Still, a higher standard should be held for the release of personal information of their clients, even if the registered agents are not lawyers. This may require some research by the LSO to see if these concerns are valid.

The LSO did not ask for comments about Digital Identity & Privacy. As an expert on these technologies and advisor to governments around the world about emerging best practices in these areas, I'd like to see future meetings of this Committee look into a number of these issues as well. I do believe these can impact and restrict Wyoming's ability to be a leader in attracting Digital Assets & Property businesses. In particular, given current events related to COVID19, enabling new practices such as contact tracing, immunity credentials, face recognition, biometrics, and others without sufficient regulation may significantly erode the expectations of privacy by Wyoming citizens.

Thank you for the opportunity over the last three years to address the Wyoming Legislature through my testimony. Let me know if you need more details on the topics above or if there are other ways I can be of service.

Regards,

Christopher Allen