Decentralized Identity
& Blockchain Architect

@ChristopherA
ChristopherA@LifeWithAlacrity.com
www.LifeWithAlacrity.com
cell +1.510.908.1066

Executive Director &
Principal Architect
Blockchain Commons, LLC
7302 Yellowstone Rd
Cheyenne, WY 82009-2077
www.BlockchainCommons.com
main +1-307-222-2140

Founder, Chairman,
Rebooting the Web Of Trust Inc.
www.WebOfTrust.info

September 15, 2021

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

Committee Chairs, Members of the Select Committee & LSO:

Earlier this year, in SF0039, we defined digital identity using the fundamental legal basis of *"Principal Authority*", which was drawn primarily from the *Laws of Agency*.

Over the course of the summer, I've been discussing this concept with a number of people, focusing on how we can advance it to the next stage, where we can truly give people self-sovereign control over their digital identities. I've included a paper that I recently prepared that includes many of my thoughts based on those discussions. It is also is published at https://www.blockchaincommons.com/articles/Principal-Authority/

In short, I believe that one of the next steps for our definition of digital identity is to build upon the *Laws of Agency* that we've already established as our foundation, and to clearly define duties that are due to principals from the agents to whom they delegate their authority.

This essentially requires us to codify the limited customs that exist for digital identities to date, as well as define expectations and practices. As a start, I've suggested what duties might come from the principles of self-sovereign identity that I first laid out five years ago.

I would be very pleased to support work in this direction if my continued involvement with the Identity Subcommittee is desired. Otherwise, I hope you'll use this as a possible direction for future work on digital identity, and I will remain happy to help when it would be constructive to do so.

Regards,

Christopher Allen

Blockchain Commons

Supporting Open Blockchain Infrastructure, Internet Security & Cryptographic Research

Principal Authority: A New Perspective on Self-Sovereign Identity

September 15, 2021

CATEGORIES

Articles

TAGS

Digital Identity, Legislation, Self-Sovereign Identity

This summer, we've been iterating through an article intended to talk about the success that Blockchain Commons has had working with the Wyoming legislature to help to define a first-in-the-country legal definition of digital identity.

The Digital Identity Working Group for the Wyoming Select Committee on Blockchain meets again next week, on September 21-22, 2021. I will be providing testimony there at 2pm MST. As a result, we've decided to release the current draft of this article on digital identity and how Wyoming has defined it using Principal Authority, with the goal of helping to shape the agenda for digital identity for the next year, both in Wyoming and elsewhere.

—Christopher Allen

In 2016, I wrote *"The Path to Self-Sovereign Identity"* to talk about the historic evolution from centralized identity to user-centric identity and to define the next step: a self-sovereign digital identity that was controlled by the user, not some third party. In it I also offered *10 Self-Sovereign Identity Principles* which have been widely accepted by the decentralized identity community.

Self-sovereign identity has matured and grown considerably since, as I chronicled in *"Self-Sovereign Identity: Five Years On"*. There are now specifications, products, and entire companies supporting the concept. However, recent legal efforts to define self-sovereign identity may be just as important for catapulting it into the mass market.

Defining Identity

Defining identity is by no means easy. That core topic could encompass a paper much longer than this. The following are some various definitions of identity drawn from the *RWOT Glossary*:

> ***Identifier:*** A label that refers to an entity and can be used to establish or maintain an identity. For example, a name or UID.
>
> ***Identity:*** A conceptual construct that enables the differentiation between distinct entities that are individually considered to be unique, but which may possess class or group characteristics. An identity gives these entities the ability to interact as peers in collaborative or competitive ways. It is not the entity that it represents.
>
> ***Identity, Digital:*** A digital representation of an entity, managed by digital tools, over which that entity has personal or delegated control.
>
> ***Identity, Functional:*** How we recognize, remember

> and respond to specific people and things.
>
> ***SSI: Self-sovereign identity.*** A decentralized digital identity that does not depend on any centralized authority and whose information is portable.

Digital identity is just one aspect of a complex, interconnected web of different digital models. It's not the same thing as identification (where you prove you are a distinct entity with unique characteristics), authentication (where you prove you were the same entity as before), or personal data (which is information related to an identified or identifiable entity).

Those other elements all need to be considered, but it's digital identity, and now self-sovereign identity, that gives us the linchpin to do so.

Turning Digital Identity into Law

For self-sovereign identity to truly achieve international success, I feel that it needs to not just be embraced by the technological sector, but also to have a basis in law. In recent years, I've been progressing toward that goal through work with various state and national legislatures.

Collaborating with the Wyoming legislature has borne the first fruit. This year they passed *SF0039* on digital identity, which the Governor signed into law and which went into effect on July 1, 2021. It defines digital identity as follows:

> (xviii) "Personal digital identity" means the intangible digital representation of, by and for a natural person, over which he has principal authority and through which he intentionally communicates or acts.

So where's the self-sovereign identity in that?

As with much legislation, it's all about the careful selection of words.

Defining Principal Authority

To understand how Principal Authority relates to self-sovereign identity requires insight into what Principal Authority is. The concept comes out of English Common law. It appears in most Commonwealth countries but has also found its way into the laws of other countries, including the United States. It's primarily used in the *Laws of Agency*, an area of commercial law where an agent is empowered to take on certain tasks.

As the name would suggest, Principal Authority first requires a Principal: a person or entity. It then requires that entity have Authority: some power. Principal Authority is thus the power derived from a person or entity, which they can use or which they can delegate out to others. When applied to digital identity, Principal Authority says that a Principal has Authority over his identity — which is a clear restatement of self-sovereign principles.

In fact, the recognition of a Principal is itself a statement of the first of the principles of self-sovereign identity: *existence*. It asserts that digital identity is always a representation of an actual entity, who predates any digital representation, and who is also the first and foremost beneficiary of that representation.

However, in drawing on the Laws of Agency, the concepts of Principal and Principal Authority go beyond that. Because the person at the heart of an identity has the ultimate power to control the self-sovereign digital representation that they've created (and/or that they use), this means that any others who exert Principal Authority over that identity data are doing so only as agents of the Principal.

By focusing on Agency, the concept of Principal Authority also ensures that the Principal always has the ability to revoke their delegation to the agents whom they have temporarily offered Authority regarding

their identity. This is a requirement for other self-sovereign principles such as *portability*, and it's a real necessity in the digital world, where we might need to delete personal data or to cancel Terms & Conditions that we signed without real, informed consent.

Altogether, this new definition of Principal Authority adds a lot of nuance to self-sovereign identity, and much of that comes thanks to the implicit incorporation of Agency.

Defining Control

In saying that a Principal has the ultimate authority to control their digital identity, care also needs to be taken to define what that control means. It means that a Principal has (or can delegate) the Principal Authority to identify as that identity; to authenticate as that identity; and to know the contents of the data held by that identity.

However, any digital identity also exists as part of a larger ecosystem, and the Principal does not have control over the larger ecosystem. They *cannot* control how other entities rate, rank, or note the reputation of their identity; and they *cannot* control comments, flags, or other notes that other entities might attach to their identity.

Further, a Principal cannot necessarily prevent other entities from creating new digital identities related to them, which may or may not link to an existing identity. (Though states are increasingly recognizing the limits of voluntary disclosure of information, digital identity laws will ultimately never prevent a police station from creating their own identity record related to a criminal, or a civic authority from creating government-related identity records.)

In other words, self-sovereign identity, and the establishment of Principal Authority over it, lays down boundaries for what the Principal controls — boundaries that are much wider than those established for digital identities controlled by third parties. However, those boundaries still exist.

Fundamentally, control of a digital identity means that the Principal

can expect to maintain the continuity of that identity for as long as they see fit, but in doing so must accept the battle scars inflicted by interactions in a larger ecosystem that are implicit to the identity itself.

Agents & Their Duty

The ability to delegate Principal Authority, as revealed by the Laws of Agency, may be as crucial to self-sovereign identity as the concept of a Principal itself. It allows the empowerment of agents by a Principal — who might be physical agents or, in the increasingly digital world, virtual agents. But, it also institutes the core requirement that those agents be working for the good of the Principal when they are exerting Principal Authority over the identity holder's identity data.

This concept of "duty" is crucial to the Laws of Agency. Duty requires that an Agent only use their delegated Principal Authority as the Principal requests, in a way that benefits the Principal, and with care and due diligence, while frequently reporting back what they've done.

This is a notable change from the way that digital identities have been treated traditionally. Compare that to banks, who represent you in financial transactions, and then sell your spending data; compare that to Facebook, who collects as much personally identifiable data and other information as you're willing to give them, then sells that to advertisers; or compare it to Google, who infers personally identifiable and demographic data based on the information you input into their tools and the choices you make. In large part, you don't even know what these identity representatives and data holders are doing. In the world before *Europe's GDPR* or *California's CCPA*, you had little input into their actions. Even now, with those early and rough attempts to protect digital self-sovereignty, you're typically opting-out, not opting-in — which is barely agency at all — and you're still not protected against people who are self-serving nor those who are inferring information from scattered pieces of data.

That's because any duties currently required of the entities to whom you grant agency over your data are quite minimal. Maybe there's a

duty of privacy, maybe there's a duty of safety, but in general they don't need to work in your best interest. That's why we need to ensure that new definitions of digital identity, particularly self-sovereign identity, follow the Laws of Agency in ways that our current systems do not.

This sort of agent agreement needs to be part of delegation. To date, this has been true to a limited extent with federation protocols such as SAML and Oauth, but that needs to be extended to every person. Wyoming's digital-identity law is the first example of legislation that focuses on Agency in this way, and that's much of its power.

However, this isn't a simple issue. Even with Agency-focused legislation, we need to determine a source for duties. This article will try to outline some of them, using not just the traditional duties of agents, but also the self-sovereign principles themselves. However, it's a mere starting point, with a stronger legal foundation required.

Principal Authority & The State

Before defining duties, it's important to note one other interesting element of Principal Authority and its foundation in Agency: it focuses not just on a single person's authority, but also on their ability to delegate to and require duties from other entities. In other words, it's a peer-to-peer relationship; this relationship works within the context of a state who recognizes the concept of Principal Authority, respects its ability to enable Agency, and enforces its established duties.

However, though the state is involved, this peer-to-peer relationship still lies in stark contrast to traditional property law, where property is always in some way *beholden* to the state: the state might be the original source for property, they might be able to reclaim it by eminent domain, and they might be able to seize it through asset forfeiture. Those ideas all run counter to the idea of self-sovereignty — which is yet another reason that we choose to focus on the Agency of Principal Authority, not property law, as the core legal metaphor for self-sovereign identity.

Restating the Self-Sovereign Principles

The use of Principal Authority to empower self-sovereign identity provides a legal foothold for many of my original 10 principles.

What follows is a restatement of the self-sovereign principles that reorganizes the original ten as rights and duties that are suggested by customs, expectations, and best practices, but which need to be better codified to become true duties. It also proposes five additional duties that could come from customs implicit in the Laws of Agency.

Together, these ideas may allow us to both better understand how to turn the self-sovereign principles into concrete usage and also to more easily translate them into duties bound by legislation.

The Rights of Self-Sovereign Authority

Some principles of self-sovereign identity are implicit in the idea of a Principal.

1. **Existence.** The definition of Principal requires that there be a real entity at an identity's heart.
2. **Control.** The definition of Principal Authority says that the Principal always retains control of an identity, within specifically defined boundaries, no matter who is holding it at a particular time.
3. **Persistence.** Because of their uncontested Principal Authority, a Principal may decide to have an identity last for as long as they see fit.
4. **Consent.** Anything that happens within the defined boundaries of the digital identity is implicitly with the consent of the Principal, who may delegate or revoke Principal Authority at any time.

Self-sovereign rights recognize that an identity exists to benefit its Principal. These core principles likely derive explicitly from a definition of digital identity such as that created by the Wyoming legislature.

The Duties of Self-Sovereign Identity

The remaining principles of self-sovereign identity can be stated as duties owed to a Principal by an agent who has been granted Principal Authority over an identity for certain purposes.

1. **Access.** An agent must provide the Principal with access to data related to their digital identity.
2. **Transparency.** An agent must be open about how they will administer a digital identity.
3. **Portability.** An agent must make a digital identity portable upon the request of the Principal.
4. **Interoperability.** An agent must use standard, interoperable protocols when making an identity portable, and should also use those interoperable protocols when interacting with other identity systems.
5. **Minimization.** An agent must minimize the data collected, stored, transmitted, and shared regarding an identity so that it only includes data that is strictly necessary in the context of a request made by the Principal.
6. **Protection.** An agent must place the protection of the identity above their own needs or desires.

Identity duties says that agents will tell you how they're using your identity, use it in the most minimalist way possible, and make it easy for you to reclaim the identity. However, legislation may be required to turn these best practices into duties bound by law.

The Duties of Self-Sovereign Agents

The idea of Principal Authority itself suggests additional duties that were not included on the original list of principles of self-sovereign identity, but which are generally defined in the Laws of Agency to be due from agents to Principals.

1. **Specificity.** An Agent will use Principal Authority to serve specific tasks as instructed by the Principal, or as required by Custom, and do nothing more with an identity.

2. **Responsibility.** An agent will serve those tasks with reasonable care and skill, with due diligence, and without further delegation.
3. **Representation.** An agent will act in the best interests of the Principal, without secret profit, and will not take on other responsibilities that might conflict with that.
4. **Fidelity.** An agent will serve those tasks in good faith.
5. **Disclosure.** An agent will maintain accounts and report their actions back to the Principal.

Agent duties say that agents will be trustworthy in their use of your identity. These duties are more likely to implicitly be a part of any legislation that was built atop the Laws of Agency.

Taking the Next Steps

Wyoming's definition of personal digital identity helps us to lay more foundation for self-sovereign identity, but it's still just a starting point.

There's more to do.

Laws of Custom

To start with, the Laws of Agency are largely built on Laws of Custom, which are as likely to be common law as any formally codified legislation. When creating new laws related to self-sovereign identity, we'll be creating new Laws of Customs for the digital frontier, an area that's so fresh that the tradition of customs has been limited.

This creates real challenges, as we must decide what customs we want to create and then we must develop them from common law to *legal customs* to (eventually) codified duties. We can integrate these with the Laws of Agency, and we can figure out how that interrelates with old common laws such as the *Use Laws*. We may even need special courts to set these common laws and achieve remedies, such as the *Court of Chancery*.

Fundamentally, there's a lot of work to be done here; recognizing the

existence of a Principal and the use of delegatable Principal Authority bound by the Laws of Agency is just a starting place. New customs, even though understood as best practices, will not automatically become legal duties.

Open Questions

Beyond that, I'm not a lawyer. There may be other legal elements that can support our definition of digital identity. Are there additional duties that we could bring in? Are there fiduciary or agency laws that we could leverage? Are there other legal models of interest we can draw from, such as the UNCITRAL Model Law of Electronic Commerce approach, which says that "The actions, promises, rights and obligations of a person shall not be denied legal validity on the sole ground they are effectuated through their digital identity"? These possibilities need to be studied, preferably with the help of legal experts.

Even once we've fully defined digital identity, we still must consider how digital identity may need to be more carefully protected. Are there ways we can give specific protection to private keys used for signatures and to express authority? Can we protect against the theft of private keys that might allow impersonation or false witness? Can we prevent the misuse of digital biometric or genetic information? Can we protect against other "crimes of authority"?

There's also a flipside: digital identity should give us some new advantages not found in traditional identity. For example, there have always been problems with individuals with low market power being at a disadvantage when negotiating with larger parties. Can new digital identity laws help start to resolve that imbalance?

Final Notes

One of the most important steps going forward will be to continue working with the Digital Identity subcommittee in the Wyoming legislature. However, I'd also welcome discussions with other states and nations, to ensure that we have great definitions of digital

identity that support self-sovereign identity *everywhere*.

If this is important to you too, consider *supporting Blockchain Commons* to make this a reality.

Offering Some Thanks

This article was written by Christopher Allen with Shannon Appelcline. Thanks to commentators who made time to talk to us about it, including Joe Andrieu, Dazza Greenwood, and Clare Sullivan. (Our conclusions are ours; they may or may not agree with them.)

Many thanks to Wyoming State Senator *Chris Rothfuss* who invited me to join the Wyoming Digital Identity subcommittee and to the others members of the Digital Identity subcommittee in the Wyoming legislature, including Brittany Kaiser, Carla Reyes, Diedrich Henning, Scott David, and once more Clare Sullivan and Dazza Greenwood. Thanks to their hard work, Wyoming now offers the first definitions of personal digital identity in the United States, laying the foundation for these additional ideas.

Previous
← *2021 Q2 Blockchain Commons Report*