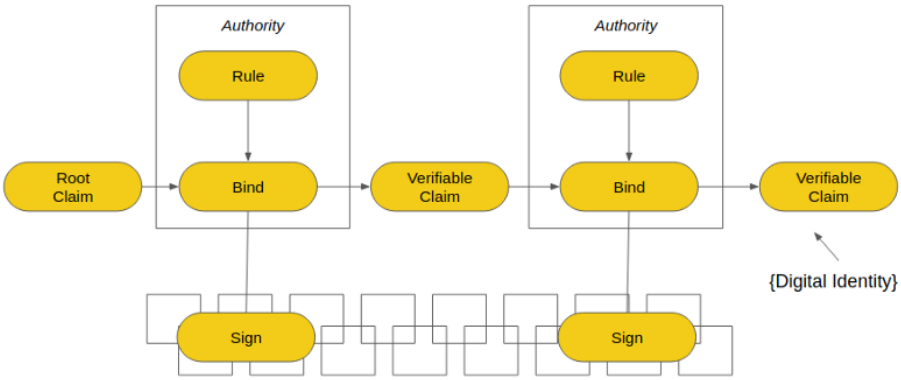
Tim Bouma Follow
Based in Ottawa. Does identity stuff. My tweets are my opinion but they can be yours too!
May 20 · 3 min read

Digital Identity: A Chain of Claims



In my never-ending (maybe obsessive) quest to distill the digital identity to its essence, the above is my latest thinking reflected in a diagram.

- I've long concluded that digital identity is a specific use case of the more general verifiable claim use cases.
- I've also concluded that a key component is public key cryptography, and its use of asymmetric key pairs enable various functions such as encryption, decryption, and signing, along with one-way functions for chaining (hashing).
- Finally, I believe the secret sauce of blockchain, or more generally, decentralized platforms, is the ability to have a public audit trail that is mutually maintained, either by untrusted parties (public blockchains), by trusted parties (permissioned blockchains) or, solely maintained by a single party (a database).

The part, or problem, for me, is understanding how the ingredients above, can yield a recipe that might fundamentally change how

institutions of trust operate.

I believe a lot of the potential related to applying these ingredients is to 'remove the intermediaries" or to remove the 'centralized authorities.' I do believe that intermediaries and authorities are still required, but they can be pushed to the edge of the ecosystem, thereby reducing their overall influence and control, especially in relation to the individual.

In pondering the role of an authority, it got me thinking —" what exactly is an authority?' Regardless of an authority's divinity, sovereignty, legitimacy or morality, I reduced an 'authority" to merely a set of rules that binds something together. For a government, this could be binding my name to my person; for Bitcoin, it is binding transaction outputs to my Bitcoin address. Of course, these are wildly different scenarios, but if you think about it, the legitimacy arises from following a set of agreed-on rules that can be mathematically validated in the trustless world, or adjudicated in the trusted world.

In the diagram above, I differentiate between a 'root claim' (a claim with a proof that exists outside of the system) and a 'verifiable claim', which is based on 'rules' carried out by an 'authority' resulting in a 'binding'. This binding is then 'signed' and written to a public audit trail, which can be verified by anyone, and hence the term 'verifiable claim.'

The diagram also shows that verifiable claims can be dependent on other verifiable claims, and ultimately, back to a root claim. This is the 'chain of claims' the title of my article.

A 'chain of claims' example: I may have a degree (verifiable claim) from a university (resulting from a rule that binds my degree to my name), which in turn relies on my birth certificate (verifiable claim) from a vital statistics register (resulting from a rule that binds my birth event to the name my parents have given me.)

What makes this interesting, is that this chain of verifiable claims (hashes, or Merkle proofs, thereof) can now be signed and registered on a public audit trail (blockchain) for independent verification.

So how does this relate to digital identity? As I've described in my previous posts, a digital identity is just a set of verifiable claims that are chained together. When I am presenting myself digitally—in the here and now—there is a bunch of verifiable claims or proofs in the mix: that I am actually present, that I am the same person that registered for a digital identity, that the person registering for the digital identity is the same person as the real person, and finally, that the 'real person' actually exists in the first place (the root claim).

So there you have it. This model might look complicated, but underneath it all, is a fractal-like simplicity (I hope). In this model, an 'authority' is neither 'good or bad' or 'centralized or decentralized'—it is just a bunch of rules used to bind things together, signed as claims, chained together down the line.

As always, this is a work in progress; I may be totally wrong, but trying out all of the wrongs might eventually result in the right. Comments welcome!