

The Four Horsemen of the SSI Apocalypse

Jeremy Grant
Managing Director, Technology & Innovation Group
Venable LLP
@jgrantindc | jagrant@venable.com

The Four Horsemen



Of the SSI Apocalypse

Some opening thoughts

- My heart has always loved the concept of SSI – my head has found it troubling.
- If self-sovereign/decentralized/user-centric identity is going to work, we need to come to grips with some core truths – and find ways to address them. Otherwise, this will end up on what is already a pretty big ash heap of other promising but ultimately underwhelming identity ideas
- I will walk through “four horsemen” – things that are holding back SSI and that need attention
- I’ll end with some things I am hopeful about 😊

Who are the Four Horsemen?

- War, Famine, Conquest, & Death
- According to the Book of Revelation, they are four guys whose appearance each represents a different facet of the apocalypse (aka, the end of the world)
- In the context of this speech – they represent four things that have never made any sense in the SSI movement (IMHO), and that if not addressed and/or taken seriously, may ensure the end of the SSI world



And just to be clear...



What are the Four Horsemen

Of the SSI Apocalypse?





1. Key management sucks

- Premised on the idea that everyone will manage a bunch of cryptographic keys – one for every attribute they want to prove about themselves
- The problem –
 - Nobody wants to do this.
 - Key management is hard and nobody is good at it – it's where all sorts of things go wrong in the cryptography world.
 - If you lose your device and your keys are on it – then what? Most people are not going to deal with 12-word recovery phrases. So you start over?
 - How about getting a new device? Is there a way to use one to bootstrap another?

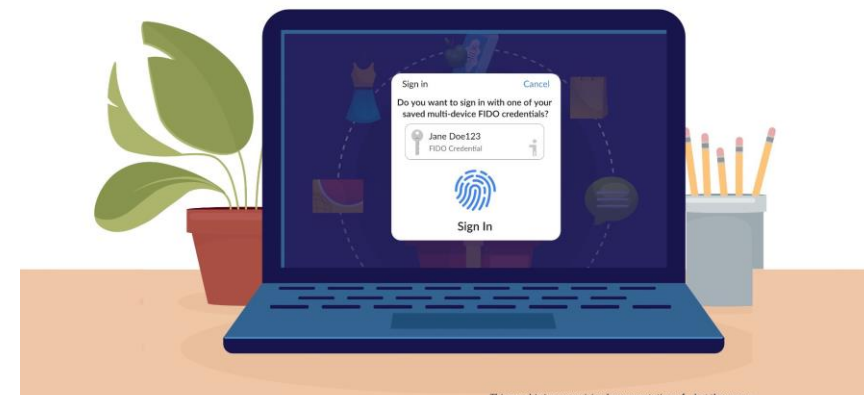




1. Key management sucks

Look at what is happening in the FIDO ecosystem with multi-device passkeys – driven by a realization that key management sucks and consumers and RPs can't really deal with it...and so the only way to bring user-friendly unphishable AuthN to the masses is to have centralized providers sync your keys.

But if SSI is about decentralized identity...what are we doing here?



This graphic is a genericized representation of what the user e

Multi-device FIDO Credentials

noun

1. *FIDO credentials that are backed up, allowing users to restore the credential to, and use it from, another device.*

Scalability	User Experience	Security
FIDO credentials are available to users whenever they need them—even if they replace their device.	The user experience will be familiar and consistent across many of the user's devices using the same simple action that consumers take multiple times each day to unlock their devices.	Proven resistance to threats of phishing, credential stuffing and other remote attacks. No need for passwords as an alternative sign-in or account recovery method.



2. Where are the validated attributes?

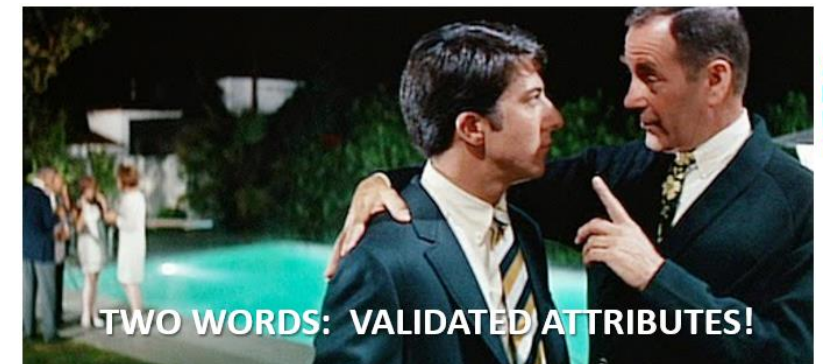
The Self-Sovereign Vision (2015)





2. Where are the validated attributes?

- Around 2018 (ish) – realization that nobody in any high assurance use case cares who you say you are unless it's validated by an authoritative source
- Meanwhile, dozens of companies got funded around the idea
- None of the investors seem to ever have bothered to ask a key question: “Are there any authoritative issuers looking to digitally sign cryptographic assertions as to the validity of attributes on the blockchain?”
- The US lacks a digital identity strategy – let alone one focused on validated attributes





3. Privacy is oversold

- I'm continually told that the reason we all need SSI is that it will restore control over my data to me. But will it?
- If I present my SSI credential to a company – are they going to then delete the information after? Why would they do that?
- Are companies going to block data brokers from getting it?
- There is an illusion that just because I choose to reveal my data at a granular level that it then disappears.
- It's nice that I can reveal a subset of attributes like “over 18” – but that's a far cry from the idea that SSI is going to enable a “digital revolution” that keeps my data out of other places.





4. Why do I need a coin?

- I have United miles, Marriott points – now I need to acquire an alternative currency just to prove who I am?
- Or if I am a business, I need to acquire them so I can pay for the service?
- Thankfully, this is not part of the VC model – but I still get pitches each month based on the idea that there is a coin powering these things





Bonus Horseman – Choice!

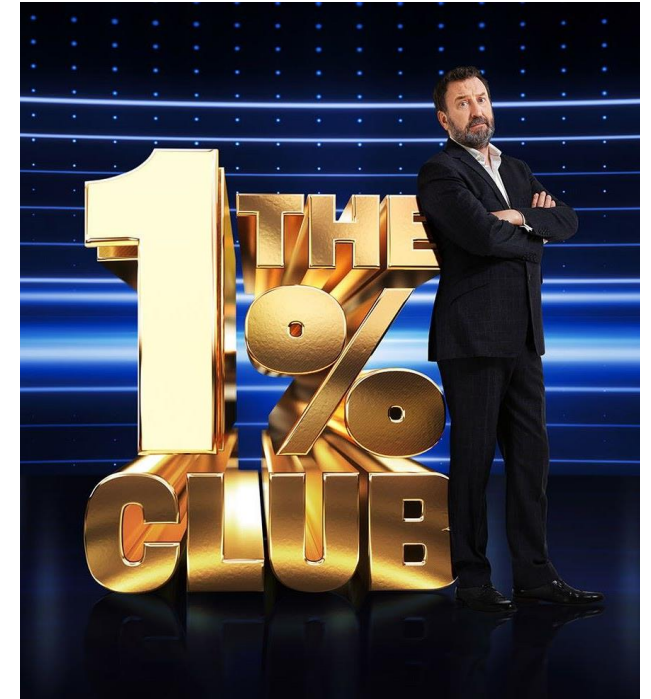
- Giving people choices over when and how they share their information – and what specific attributes they share – is great in theory.
- In practice, it tends to overwhelm people.
- We need more work on the UX here – how do we enable granular sharing of attributes without making it a burden?



A plea: let's not build “Identity for the 1%”

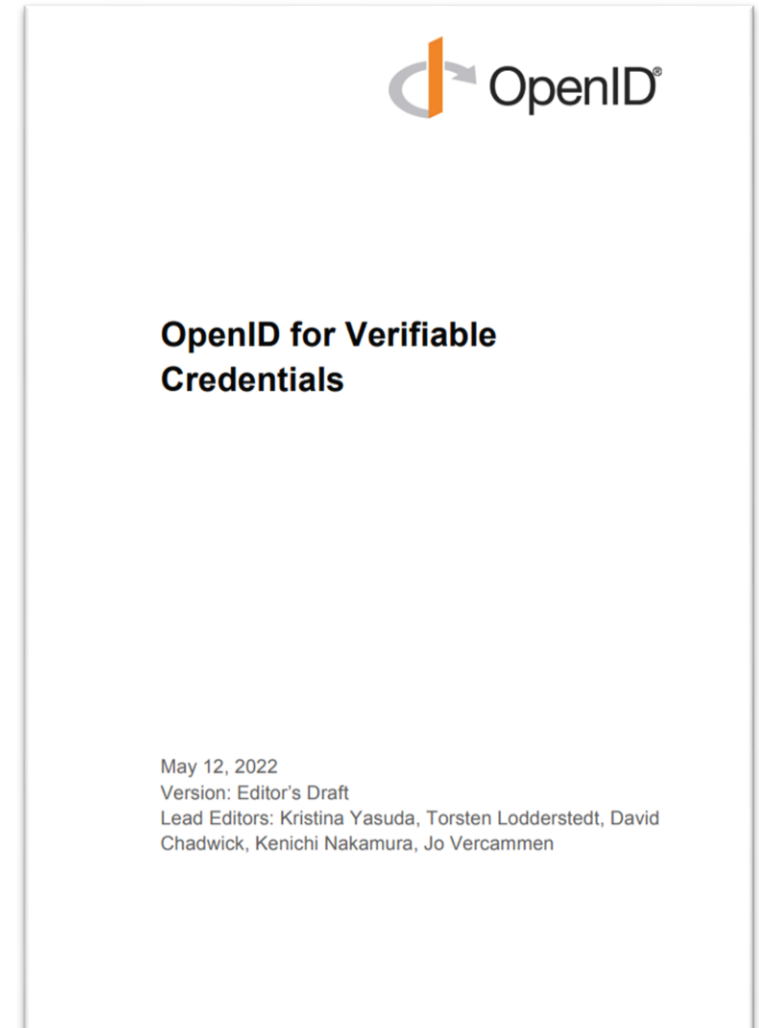
Identity designed by identity weenies...for identity weenies...around the things that identity weenies dream of.

But that most people don't really care about – or have the ability to easily manage or use.



Things I am excited about

- Standards emerging – hooray W3C!
- OIDF paper – you can do VC without blockchain
 - Focus on the concept of what a VC should be, not any single technology that underpins it
- Digital wallets – may help solve UX challenges
- Serious people are now building systems that don't embrace the "horsemen" and take more pragmatic approaches



A closing thought



- Much of the promise around SSI is based on what it offers the user...
- ...but what is the value for relying parties?
- The idea of identity systems that come with new restrictions on how Relying Parties can use them may not be something RPs find overly compelling – for this new ecosystem to gain traction, we must find ways to appeal to RPs

THANK YOU!



Jeremy Grant

Managing Director, Technology & Innovation Group, Venable LLP
@jgrantindc | jagrant@venable.com