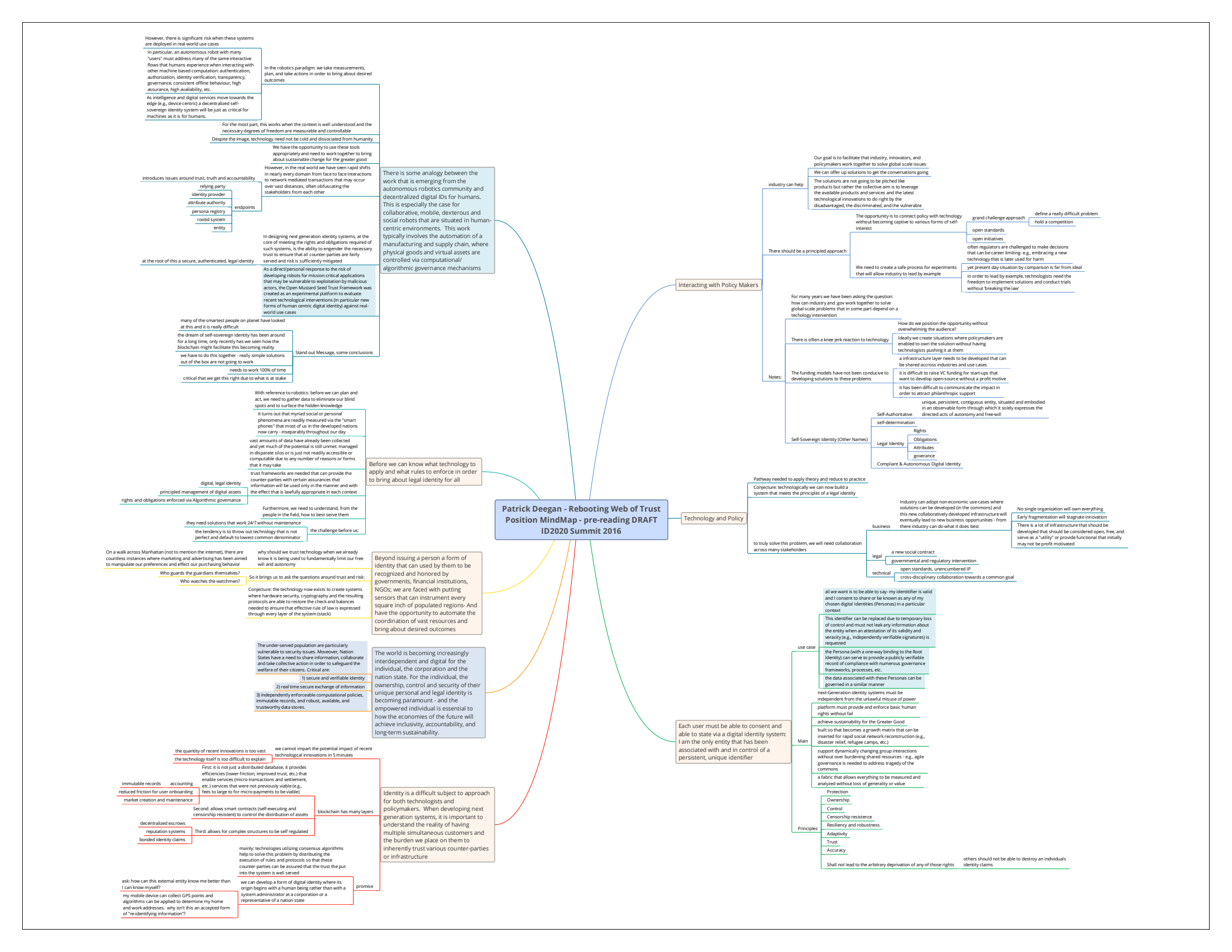
Patrick Deegan - Rebooting Web of Trust Position MindMap - pre-reading DRAFT ID2020 Summit 2016
Interacting with Policy Makers
industry can help
Our goal is to facilitate that industry, innovators, and policymakers work together to solve global scale issues
We can offer up solutions to get the conversations going
The solutions are not going to be pitched like products but rather the collective aim is to leverage the available products and services and the latest technological innovations to do right by the disadvantaged, the discriminated, and the vulnerable
There should be a principled approach
The opportunity is to connect policy with technology without becoming captive to various forms of self-interest
grand challenge approach
define a really difficult problem
hold a competition
open standards
open initiatives
often regulators are challenged to make decisions that can be career limiting- e.g., embracing a new technology that is later used for harm
We need to create a safe process for experiments that will allow industry to lead by example
yet present day situation by comparison is far from ideal
in order to lead by example, technologists need the freedom to implement solutions and conduct trials without 'breaking the law'
Notes:
For many years we have been asking the question: how can industry and .gov work together to solve global scale problems that in some part depend on a techology intervention
There is often a knee jerk reaction to technology
How do we position the opportunity without overwhelming the audience?
Ideally we create situations where policymakers are enabled to own the solution without having technologists pushing it at them
The funding models have not been conducive to developing solutions to these problems
a infrastructure layer needs to be developed that can be shared accross industries and use cases
it is difficult to raise VC funding for start-ups that want to develop open-source without a profit motive
it has been difficult to communicate the impact in order to attract philanthropic support
Self-Sovereign Identity (Other Names)
unique, persistent, contiguous entity, situated and embodied in an observable form through which it solely expresses the directed acts of autonomy and free-will
Self-Authoritative
self-determination
Legal Identity
Rights
Obligations
Attributes
goverance
Compliant & Autonomous Digital Identity
Technology and Policy
Pathway needed to apply theory and reduce to practice
Conjecture: technologically we can now build a system that meets the principles of a legal identity
to truly solve this problem, we will need collaboration across many stakeholders
business
Industry can adopt non-economic use-cases where solutions can be developed (in the commons) and this new collaboratively developed infrastructure will eventually lead to new business opportunities - from there industry can do what it does best
No single organization will own everything
Early fragmentation will stagnate innovation
There is a lot of infrastructure that should be developed that should be considered open, free, and serve as a "utility" or provide functional that initially may not be profit motivated
legal
a new social contract
governmental and regulatory intervention
technical
open standards, unencumbered IP
cross-disciplinary collaboration towards a common goal
Each user must be able to consent and able to state via a digital identity system: I am the only entity that has been associated with and in control of a persistent, unique identifier
use case
all we want is to be able to say- my identifier is valid and I consent to share or be known as any of my chosen digital Identities (Personas) in a particular context
This identifier can be replaced due to temporary loss of control and must not leak any information about the entity when an attestation of its validity and veracity (e.g., independently verifiable signatures) is requested
the Persona (with a one-way binding to the Root Identity) can serve to provide a publicly verifiable record of compliance with numerous governance frameworks, processes, etc.
the data associated with these Personas can be governed in a similar manner
Main
next-Generation identity systems must be independent from the unlawful misuse of power
platform must provide and enforce basic human rights without fail
achieve sustainability for the Greater Good
built so that becomes a growth matrix that can be inserted for rapid social network reconstruction (e.g., disaster relief, refugee camps, etc.)
support dynamically changing group interactions without over burdening shared resources - e.g., agile governance is needed to address tragedy of the commons
a fabric that allows everything to be measured and analyzed without loss of generality or value
Principles
Protection
Ownership
Control
Censorship resistence
Resiliency and robustness
Adaptivity
Trust
Accuracy
Shall not lead to the arbitrary deprivation of any of those rights
others should not be able to destroy an individuals identity claims
Identity is a difficult subject to approach for both technologists and policymakers. When developing next generation systems, it is important to understand the reality of having multiple simultaneous customers and the burden we place on them to inherently trust various counter-parties or infrastructure
we cannot impart the potential impact of recent technological innovations in 5 minutes
the quantity of recent innovations is too vast
the technology itself is too difficult to explain
blockchain has many layers
First: it is not just a distributed database, it provides efficiencies (lower friction, improved trust, etc.) that enable services (micro-transactions and settlement, etc.) services that were not previously viable (e.g., fees to large to for micro-payments to be viable)
immutable records
accounting
reduced friction for user onboarding
market creation and maintenance
Second: allows smart contracts (self-executing and censorship resistent) to control the distribution of assets
Third: allows for complex structures to be self regulated
decentralized escrows
reputation systems
bonded identity claims
promise
mainly: technologies utilizing consensus algorithms help to solve this problem by distributing the execution of rules and protocols so that these counter-parties can be assured that the trust the put into the system is well served
we can develop a form of digital identity where its origin begins with a human being rather than with a system administrator at a corporation or a representative of a nation state
ask: how can this external entity know me better than I can know myself?
my mobile device can collect GPS points and algorithms can be applied to determine my home and work addresses. why isn't this an accepted form of "re-identifying information"?
The world is becoming increasingly interdependent and digital for the individual, the corporation and the nation state. For the individual, the ownership, control and security of their unique personal and legal identity is becoming paramount - and the empowered individual is essential to how the economies of the future will achieve inclusivity, accountability, and long-term sustainability.
The under-served population are particularly vulnerable to security issues. Moveover, Nation States have a need to share information, collaborate and take collective action in order to safeguard the welfare of their citizens. Critical are:
1) secure and verifiable identity
2) real time secure exchange of information
3) independently enforceable computational policies, immutable records, and robust, available, and trustworthy data stores.
Beyond issuing a person a form of identity that can used by them to be recognized and honored by governments, financial institutions, NGOs; we are faced with putting sensors that can instrument every square inch of populated regions- And have the opportunity to automate the coordination of vast resources and bring about desired outcomes
On a walk across Manhattan (not to mention the internet), there are countless instances where marketing and advertising has been aimed to manipulate our preferences and effect our purchasing behavior
why should we trust technology when we already know it is being used to fundamentally limit our free will and autonomy
Who guards the guardians themselves?
Who watches the watchmen?
So it brings us to ask the questions around trust and risk:
Conjecture: the technology now exists to create systems where hardware security, cryptography and the resulting protocols are able to restore the check and balances needed to ensure that effective rule of law is expressed through every layer of the system (stack)
Before we can know what technology to apply and what rules to enforce in order to bring about legal identity for all
With reference to robotics: before we can plan and act, we need to gather data to eliminate our blind spots and to surface the hidden knowledge
It turns out that myriad social or personal phenomena are readily measured via the "smart phones" that most of us in the developed nations now carry - inseparably throughout our day
vast amounts of data have already been collected and yet much of the potential is still unmet: managed in disparate silos or is just not readily accessible or computable due to any number of reasons or forms that it may take
trust frameworks are needed that can provide the counter-parties with certain assurances that information will be used only in the manner and with the effect that is lawfully appropriate in each context
digital, legal identity
principled management of digital assets
rights and obligations enforced via Algorithmic governance
Furthermore, we need to understand, from the people in the field, how to best serve them
they need solutions that work 24/7 without maintenance
the challenge before us:
the tendency is to throw out technology that is not perfect and default to lowest common denominator
There is some analogy between the work that is emerging from the autonomous robotics community and decentralized digital IDs for humans. This is especially the case for collaborative, mobile, dexterous and social robots that are situated in human-centric environments. This work typically involves the automation of a manufacturing and supply chain, where physical goods and virtual assets are controlled via computational/ algorithmic governance mechanisms
However, there is significant risk when these systems are deployed in real-world use cases
In particular, an autonomous robot with many "users" must address many of the same interactive flows that humans experience when interacting with other machine based computation: authentication, authorization, identity verification, transparency, governance, consistent offline behaviour, high assurance, high availability, etc.
As intelligence and digital services move towards the edge (e.g., device centric) a decentralized self-sovereign identity system will be just as critical for machines as it is for humans.
In the robotics paradigm: we take measurements, plan, and take actions in order to bring about desired outcomes
For the most part, this works when the context is well understood and the necessary degrees of freedom are measurable and controllable
Despite the image, technology need not be cold and dissociated from humanity
We have the opportunity to use these tools appropriately and need to work together to bring about sustainable change for the greater good
However, in the real world we have seen rapid shifts in nearly every domain from face to face interactions to network mediated transactions that may occur over vast distances, often obfuscating the stakeholders from each other
introduces issues around trust, truth and accountability
endpoints
relying party
identity provider
attribute authority
persona registry
rootid system
entity
In designing next generation identity systems, at the core of meeting the rights and obligations required of such systems, is the ability to engender the necessary trust to ensure that all counter-parties are fairly served and risk is sufficiently mitigated
at the root of this a secure, authenticated, legal identity
As a direct/personal response to the risk of developing robots for mission critical applications that may be vulnerable to exploitation by malicious actors, the Open Mustard Seed Trust Framework was created as an experimental platform to evaluate recent technological interventions (in particular new forms of human centric digital identity) against real-world use cases
many of the smartest people on planet have looked at this and it is really difficult
the dream of self-sovereign identity has been around for a long time, only recently has we seen how the blockchain might facilitate this becoming reality
Stand out Message, some conclusions
we have to do this together - really simple solutions out of the box are not going to work
needs to work 100% of time
critical that we get this right due to what is at stake