Dan Elitzer
Bitcoin, startups, FinTech | Designing ventures w @IDEOcoLAB | Co-Founder @MITBitcoinClub, @MI...
May 24 · 5 min read

A Framework for Identity

How do you identify yourself? Is it your name? Your email address? Phone number? Drivers license? Facebook account?

Last summer, IDEO coLAB brought together 25 students from top Boston-area universities—including Harvard, MIT, Tufts, and RISD—to design venture prototypes exploring the future of trust, transactions, and reputation. Before the program, I hadn't given much thought to the concept of "identity" or identity systems. But abstract concepts start to take shape and become more tangible when you run into them repeatedly. Over and over throughout the summer, we saw teams wrestle with identity-related challenges as they designed their ventures:

- When you're distributing digital tokens representing voting rights for community projects, how do you ensure there's a real person behind each account?
- How can a university issue digital diplomas that graduates can prove are authentic and belong to them?
- In the event of an emergency, is there a way to automatically give doctors access to your relevant medical history, while keeping it secure and private at other times?

You can probably think of some fairly straightforward answers to those questions. But when you go to implement them, you quickly find that the

solution either makes fraud trivial or introduces a level of friction that users won't tolerate.

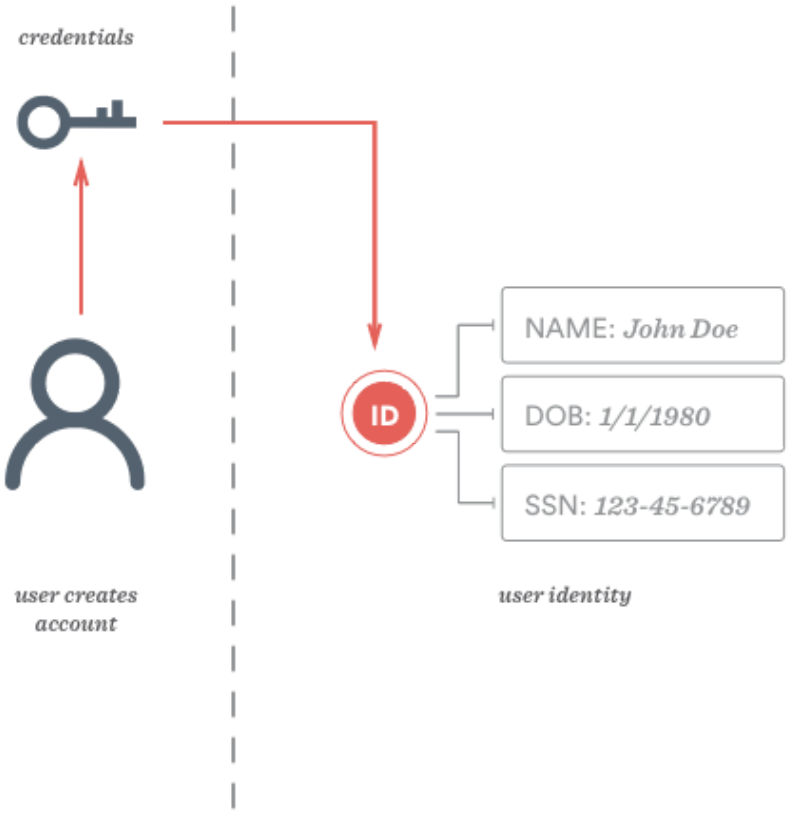
. . .

Our exploration of digital identity continued into the fall, and in October IDEO coLAB and the MIT Digital Currency Initiative co-hosted a workshop. Students and professionals collaboratively explored how blockchain technology might play a role in solving identity-related challenges in the financial services and health care industries.

To help guide discussion at the workshop, we developed a simple framework of the core functions of an identity system. During a concurrent project, the IDEO coLAB team made a few iterations. It's not perfect, but we've found it useful for organizing our thinking and analyzing where blockchains and other emerging technology might be applicable:

Issue

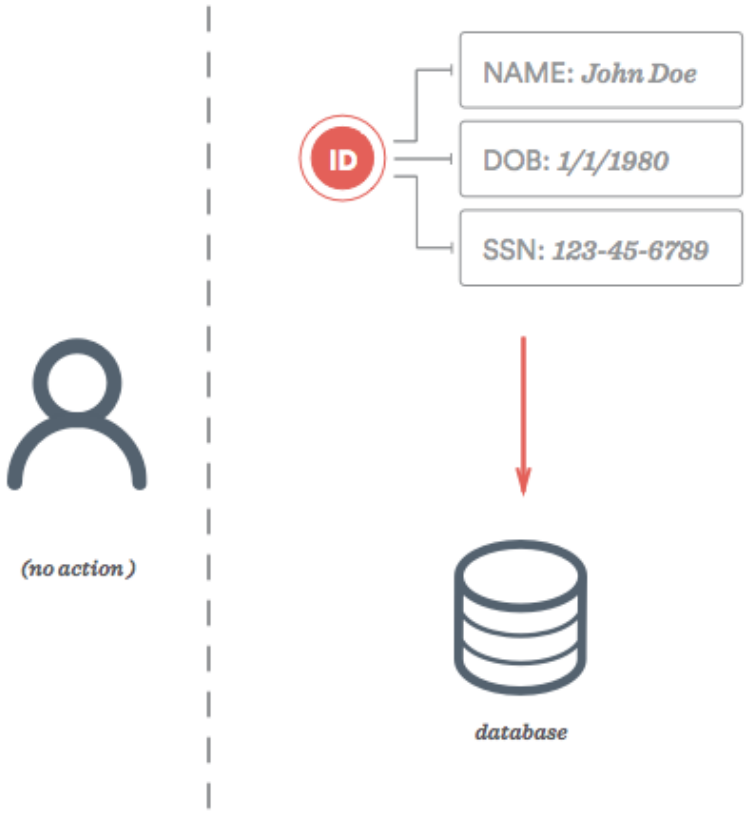
Whether it's the US government assigning Social Security Numbers or Google letting you select an email address, there needs to be a way to create new identities and assign identifiers.



Identities need to be created or issued

Store

Identity data needs to be stored somewhere. Usually this is a private database with administrator-controlled access, but technologies like IPFS and Blockstack are examples of new models for data storage and retrieval.

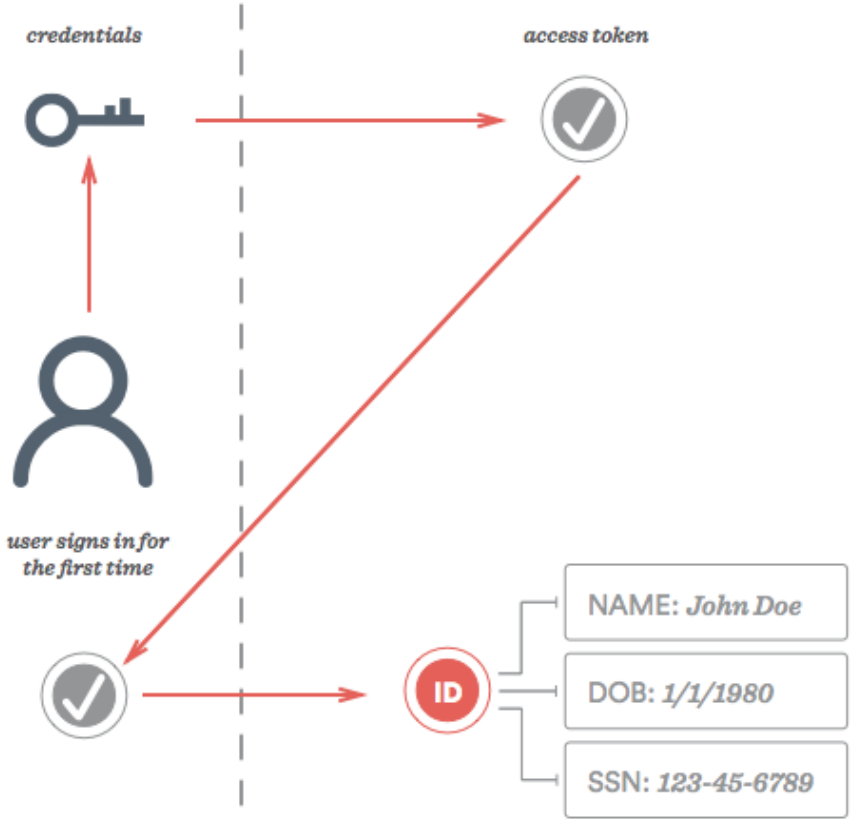


Identity data needs to be kept in a secure manner

Authenticate

Individuals need to prove they are who they say they are when attempting to assert their identity. This is done using one or more factors of authentication: something you know (a password), something you have (a mobile phone), or something you are (photo or fingerprint). For example, think of what happens when you present your drivers license at a bar or

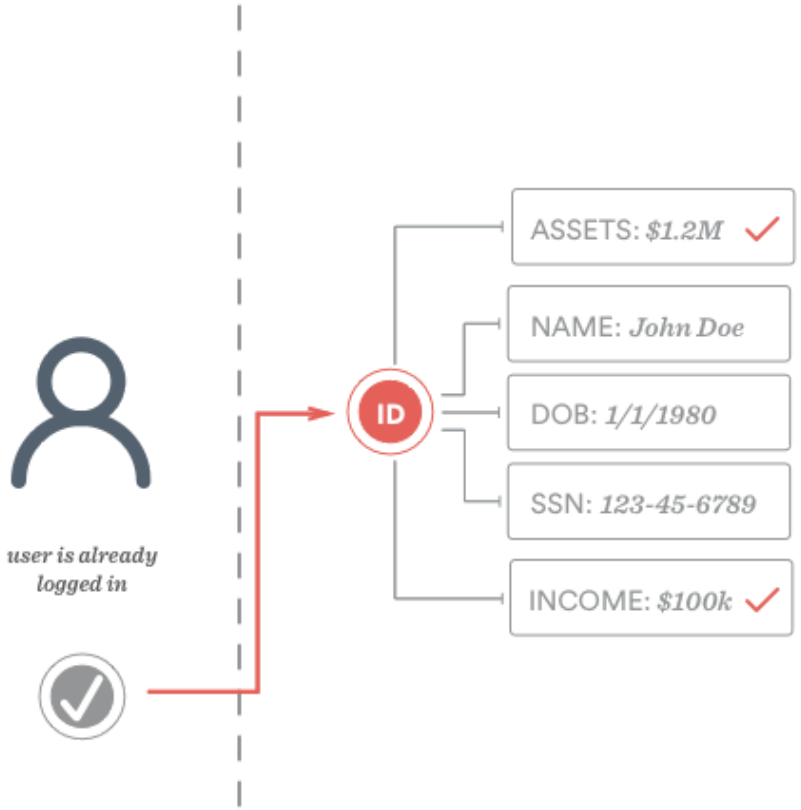
airport. The person inspecting it looks at your photo, then at you, to make sure you're the person represented on the card.



Individuals need to prove they are who they say they are

Authorize

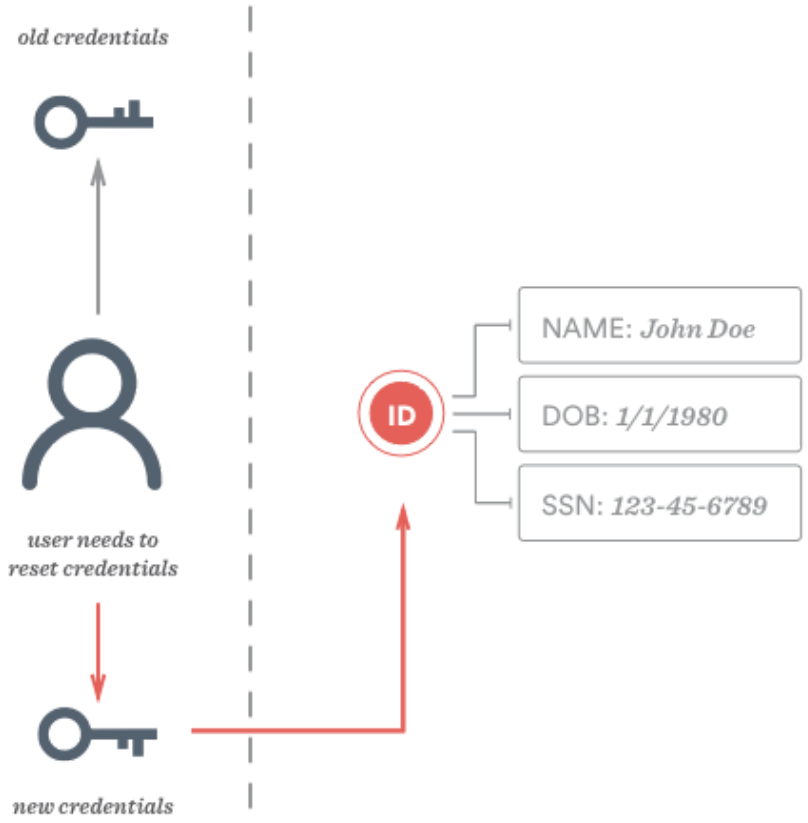
Once they've authenticated themselves, individuals are authorized to perform certain tasks. Whether it's being able to access the transaction history for your bank account or being able to enter a bar, identity systems get utility from enabling you to take actions and interact with people or businesses based on knowing who you are or certain information about you.



Individuals are given permission to access services or perform tasks based on identities or attributes

Recover

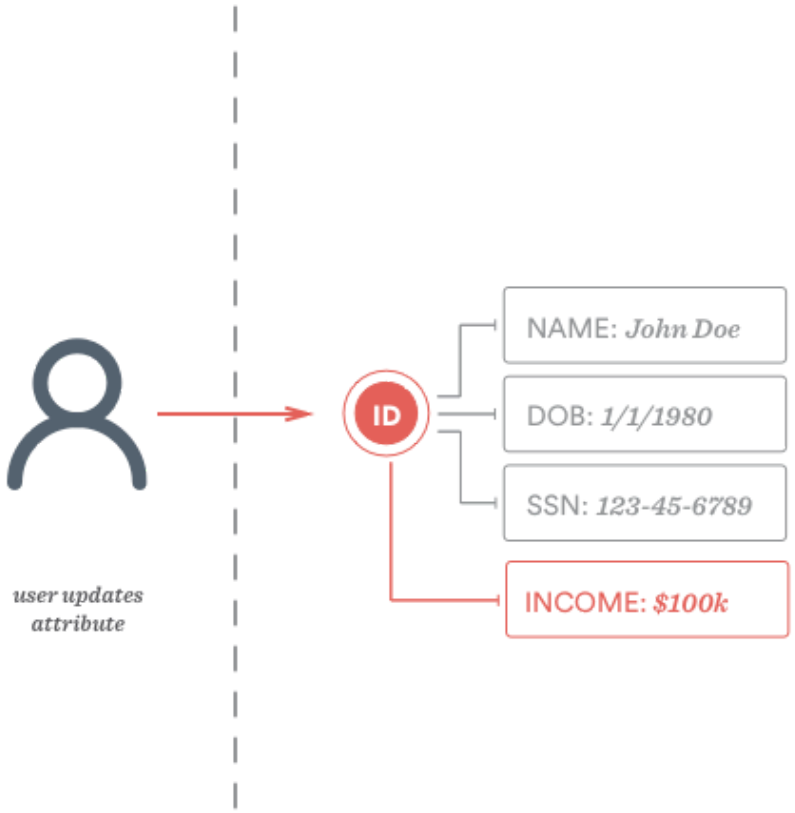
Stolen wallet or forgotten password? Individuals need a way to regain access to their identity data, should they lose it. (Note: This is often the part of the process where the usability vs security tradeoff is most stark—protecting an account with a random 32-character password and fingerprint isn't much good if "recovery" can be done using your zip code and the last four digits of your social security number. Conversely, asking the average user to print a recovery key when they create their account is absurd.)



Individuals need a way to regain access to their identity data

Update

Users or administrators need to be able to add, remove, or edit attributes associated with an identity. Pieces of our identity information change over time: an address gets changed, a new degree is earned, a drivers license expires, etc. Digital identities need to evolve along with the people they represent.

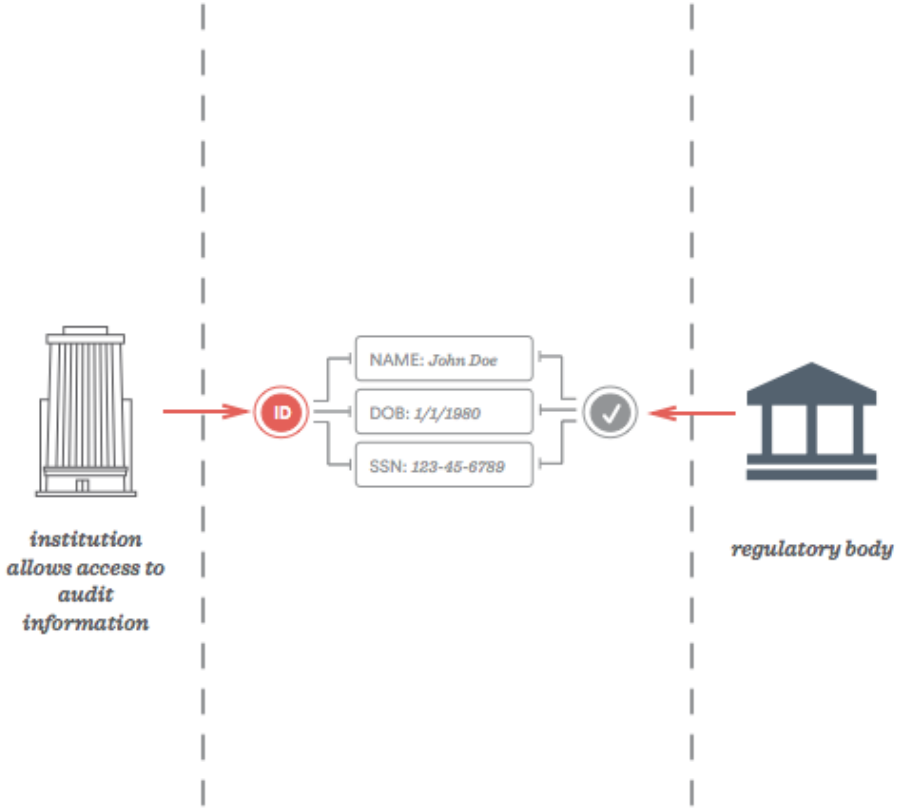


Individuals can add/remove/edit attributes associated with their identity

Audit

How can someone check that your identity data is accurate? In the context of regulated industries such as financial services or health care, identity data and the process by which it is recorded and accessed needs to be auditable by relevant government institutions. For user-controlled identity systems like

PGP, code is open source and trusted parties that host data (e.g., Keybase) ideally go to great lengths to enable public auditing.



The validity and integrity of identity data should be auditable by specified parties, such as regulators, users, and other institutions who rely on accurate identity information

. . .

From our experience, these are the core components of any identity system. Each presents its own unique challenges for system design and opportunities for creating better user experiences. How will the system be used? How might it be hacked or exploited? Is a universal digital identity system possible or desirable… and by whom?

We will continue to use this framework within IDEO coLAB as a starting point for our work around the future of digital identity, which we're pursuing in ways both big and small. One example is the machine shop certification system we prototyped over one week—you can read about it here. Identity is also relevant for *things*, not just people, so we'll be extending this theme in context of our Internet of Things + Blockchain Fellowship this summer.

We look forward to sharing more about what we're thinking and doing in this space over the coming months. If you're interested in learning more, visit our website at http://ideocolab.com/ and sign up for our newsletter.

Graphics by Reid Williams, whose collaboration on this framework has been invaluable.