HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

The Identity Working Group

Background, Challenges, & Rewards

June 18, 2017

Hart Montgomery for Vipin Bharathan

Outline

- ★What is Identity?
- ★Importance of Identity
  - ★ Both within a blockchain and outside blockchain
- ★Current Status, Definitions, & Taxonomy
- ★Working Group Background

What is Identity?

अहं ब्रह्मास्मि *I am the Brahma*

तत्त्वमसि *Thou art that*

אֶהְיֶה אֲשֶׁר אֶהְיֶה *I am that I am*

What is an Identity?

An identity is a dynamic collection of sets of attributes attached to an entity

- Hart: height == 6’4’’
- Hart: ECDSA PK == XXXXXXXXXXXX

Why do we care about identity?

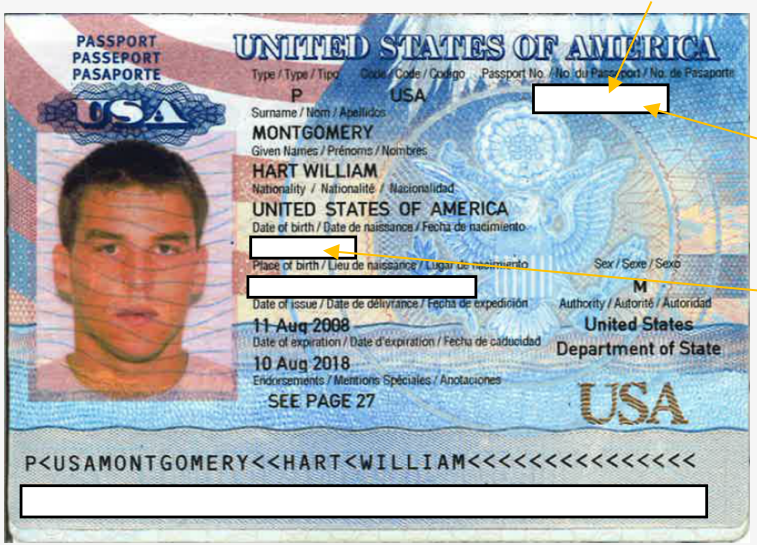
Fundamental to society—and blockchain!

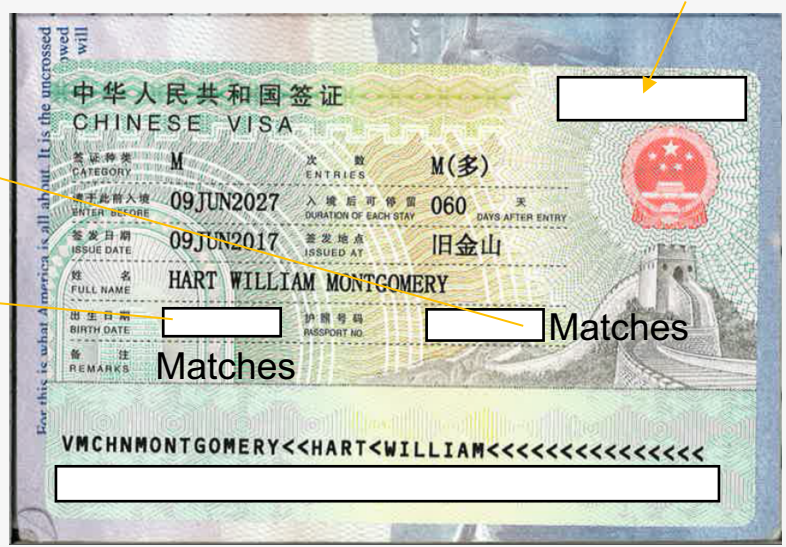
My Identity Yesterday:

Lots of Personal Information!

- ★Birthday + place of birth == almost entire social security number!
- ★Passport number—can impersonate me on many documents with it
- ★With the unredacted information above, you could probably take out a credit card in my name and easily commit credit card fraud
- ★ Lots of people saw these:
  - ★ At least four groups of people at the airport, the hotel desk staff, the currency exchange staff, perhaps even more
- ★But these people had a good reason to verify my identity!

What People Really Care About





Lots of Room for Solutions!

- ★Hyperledger Indy aims to address problems like this
- ★Main idea: prove that some piece of information about you is true without revealing that piece of information
  - ★ i.e., reveal that I am at least 21 years old (so I can have a beer in the US) without revealing my birthday.
- ★Still lots of work left to do!

EU General Data Protection Regulation (GDPR)

★Approved April 16, 2017, enforcement starts May 28, 2018
★Stiff Penalties (4% of Annual Turnover)
★Some Key Provisions: (looks a lot like self-sovereignity)

- Clear consent and easy revocation
- Right to be forgotten
- Privacy by Design
- Right to Access & Breach Notification

Privacy regulations → identity management needed!


Identity is also an
essential part of the blockchain

Identity In Chains

Public Blockchains

★No need for identity to run a node
★No need for identity to write to the chain
★Need identity for transacting

Private Blockchains

★Need an identity to read
★Need an identity to write
★Need an identity for transacting

Identity in Blockchains

Two different focuses of identity in blockchains:

- ★Identity for blockchain membership and permissions
  - ★ It's very important in permissioned blockchains to make sure that users can do exactly what they are allowed—no more and no less.
  - ★ Example: Hyperledger Fabric membership services
- ★Identity as an outside function
  - ★ Enable users on the blockchain to prove various facts about their identities to other blockchains or entities outside of the blockchain
  - ★ Example: Hyperledger Indy

Identity for Blockchain Membership & Permissions

- ★One of the core functions of the blockchain
  - ★ My opinion: probably the hardest one to implement correctly.
- ★Essential for any kind of meaningful security guarantees on the blockchain
- ★Lots of ongoing work amongst the different Hyperledger projects
  - ★ Can be very different for different projects—e.g., Fabric and Sawtooth do this in very different ways
- ★Many challenges remain!
  - ★ Bootstrapping blockchains and identities is still essentially open
  - ★ Complicated revocation policies
  - ★ More granular access


“Identity is an edge protocol” Alexander Ainslie quoted by Ian Grigg

Taxonomy of Identity I

Nodes

Natural Persons

Institutions

Identity Has Many Dimensions

- ★True Identity versus Digital Identity
- ★Hierarchical Public Key Infrastructure (HPKI) vs self-sovereignty (distributed PKI)
- ★Identity of the Infrastructure vs Identity of Transactors
- ★Identity of nodes vs Identity of natural persons vs identity of corporate and other entities
- ★Trusted Execution Environments (TEEs), i.e. Intel SGX
- ★Biometrics
- ★Anonymity and Privacy including unlinkability.

Identity Isn’t Static

★Genesis or creation
★Extinction: natural, voluntary (right to be forgotten), or forced
★Changes-provided by owner of identity, others (accumulation of attestations)
★Key Management - lost keys and revocation, key recovery
★Interoperability

Requires an approach that takes into account the lifecycle of an identity and the keys associated with it!

Verifiable Claims

- ★Identity owner
  - ★ HPKI=Enterprise
  - ★ DPKI=Individual or Subject
- ★Attesting Party
  - ★ HPKI=Single (CA Chain)
  - ★ DPKI=Multiple
- ★Verifiable Claim (non-repudiable)
  - ★ HPKI=single chain
  - ★ DPKI=many chains plus selective disclosure
- ★There is a W3C working group

Enterprise <--> Self Sovereign(DPKI)

- ★Hierarchical PKI is used heavily in the enterprise (X.509)
  - ★ GDPR is pulling Enterprises toward DPKI
- ★Many identity systems in a large enterprise
- ★Most DLTs incubated in Hyperledger have an Enterprise centric view
- ★Self-Sovereign model gives true control back to the user (DiD->DDO)
- ★We propose a thin layer to convert between Self-Sovereign & X.509
- ★Key management is going to be crucial in all systems
- ★Hardware security modules can be used to increase security
- ★Regulatory changes

The Identity Working Group

Challenges

- ★Subject is vast and diffuse
- ★Group calls are every two weeks
  - ★ Anyone can show up at the calls
- ★Global reach
- ★No pressure on individuals to produce anything
- ★No Timeline
- ★Pareto rule for contributions
- ★Pareto rule for air time
- ★No institutional support

Solutions

- ★Charter for defining the work output
  - A whitish yellow paper
  - An implementation of a public Identity utility
- ★Create community
- ★Create work streams
- ★Promote asynchronous collaboration environment
- ★Iterate
- ★Use knowledge from “Identity Warriors”

Proposed Timeline

★Identity WG paper: first versions of most sections will be iterated on starting now

★We have a strong group of volunteers

★Draft version of the Identity WG paper by end of summer

★Reference implementation of identity utility by the end of the year

THANKS!

★Members of the Identity WG
★The Linux Foundation
★The Marketing Committee of Hyperledger
★Sovrin & Evernym and their contribution, Indy
★All the active & incubated DLTs under the Hyperledger umbrella

VOLUNTEER!

JOIN THE CALLS! MAILING LINKS, ROCKET CHAT CHANNEL!

You will participate in a truly open source community helping solve one of the most challenging problems in DLT. Please engage, contribute and make a difference!

All links to the workings of the Identity working group
https://wiki.hyperledger.org/groups/identity/identity-wg

Join the mailing list https://lists.hyperledger.org/mailman/listinfo/hyperledger-identity-wg