Blockchain & Money

Class 23

December 6, 2018

Class 23 Overview

- Readings and Study Questions
- Identity
- Identity and Access Management
- State Projects
- Identity & Blockchain Technology
- Your MIT Blockchain Diploma
- Conclusions

Class 23 (12/6): Study Questions

- What are the trade-offs of using blockchain technology for identity and access management (IAM)?

- What is self-sovereign identity? How might blockchain self-sovereign or digital identity applications be applicable within the financial sector?

- Will you ask for your MIT diploma digitally or on paper?

Class 23 (12/6): Readings

- ‘*Self-sovereign identity: Why blockchain?’* IBM
- ‘*Blockchain and Digital Identity – A Good Fit?’* Internet Society
- ‘*Can blockchain ease banks’ digital-identity concerns?’* American Banker
- *‘Blockchains and Digital Identity’* Toward Data Science
- ‘*Singapore Regulator, Banks Complete KYC Blockchain Prototype*’ CCN
- ‘*Digital Diploma Debuts at MIT*‘ MIT News

What is Identity?

Concepts of Identity

Attribute	Claim	Credential	Attestation
Age Address Citizenship Name	My Name is Gary		Third Party Validation Of Claim

Identity and Access Management Systems

Functions

- Authentication
- Authorization (Attribute Access Control Decisions)

Parties

- User
- Service Provider
- Identity Provider
- Attribute Authority (Certificate Authorities, Corporate Directory Services, & Domain Name Registries)

Identity Management Challenges and 'Pain Points'

- Privacy and Security
- Identity Theft and Forged Credentials
- Credentials –Physical Documents often with Images
- Updating Personal Identity Information (PII) for life changes
- Costs and Timeliness of Attestation
- Trade-Offs or Digital vs. Physical Credentials
- Centralization (Targets for Cyber Attacks, Jurisdictional Segmentation, Monopolistic Behavior, Censorship and Inclusion)

Large Data Breaches

- Adobe (2013) – 152 million
- Ebay (2014) – 145 million
- Equifax (2017) – 143 million
- Facebook (2018) – 50 million
- Friends Finder (2016) – 412 million
- Marriott (2018) – 500 million
- Quora (2018) – 100 million
- Under Armour (2018) – 150 million
- Yahoo (2013 & 2014) – 3 billion and 500 million

State Identity Projects

- Estonia – e-identity – State Issued Digital Identity
  - Started 2002 with ID-cards
  - Run on X-Road software
- India – Aadhaar - National Identification System
  - 12 digit ID
  - Biometrics – fingerprint and iris scan

Self Sovereign Identity

- People and Entities Control their Identities
- Direct Access without Intermediaries
- Identity Transportable
- Identities Widely Usable (Interoperable)

IAM and Blockchain Technology?

- Benefits
  - Address Verification Costs and Fraud
  - Trace Provenance
  - Accessible and Censorship Resistant
  - Facilitation of Self Sovereign Identity & Decentralized Identifiers (DIDs)

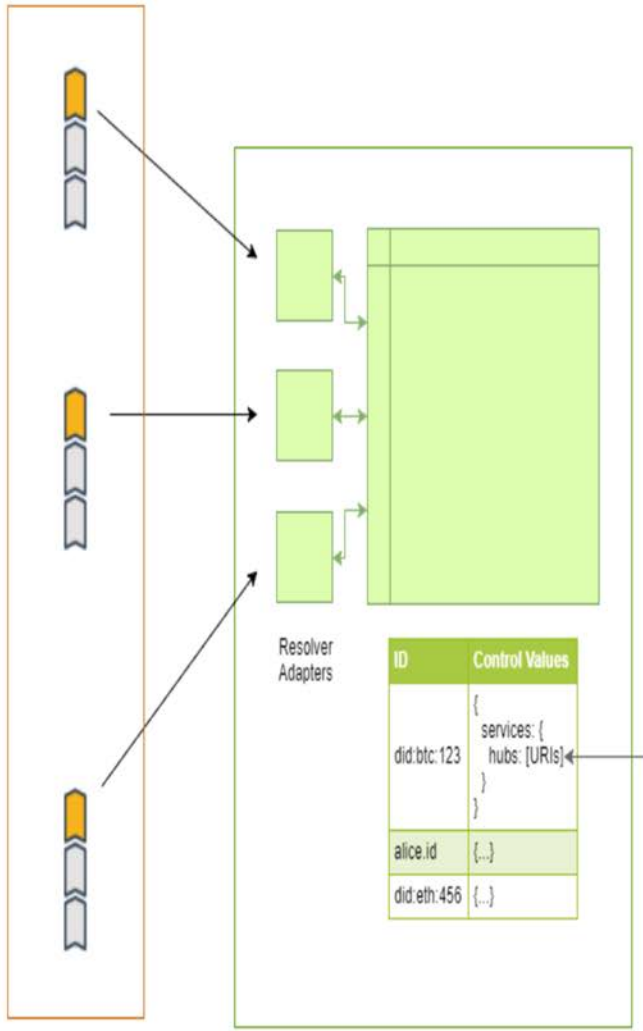
- Challenges
  - Privacy e.g. Storing Personal Identifiable Information on Blockchain
  - Access Controls
  - Collective Action and Adoption

IAM Blockchain Technology Projects

- Bitnation – Decentralized Borderless Voluntary Nation
- Civic Secure Identity – ICO for Secure Identity Platform
- Cambridge Blockchain LLC – Identity Compliance Solutions
- Democracy Earth Foundation – Promoting Inclusion through Distributed ID
- Distributed Identity Foundation – Standard Setting for Distributed IAM
- Existence ID - ICO for Secure Identity
- The Infocomm Media Development Authority of Singapore – KYC project
- Rebooting Web-of-Trust - Events for Decentralized Identity Systems
- SecureKey – Permissioned Consumer ID Network
- Sovrin Foundation – ICO for Self Sovereign Identity
- Spring Labs –Identity and Credit Related Data Security

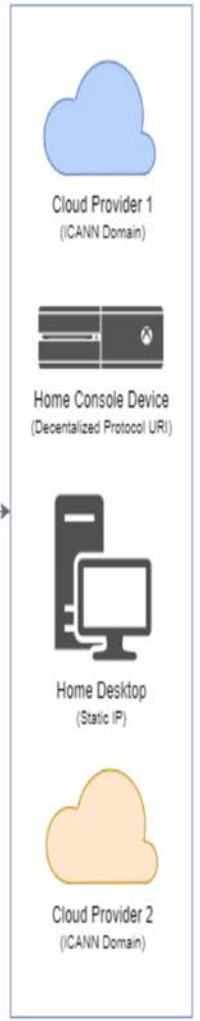
Distributed Identity Foundation

Decentralized Identity Members

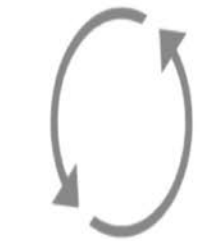


Blockchains/Ledgers or other Decentralized Systems

Universal Resolver



Identity Hubs

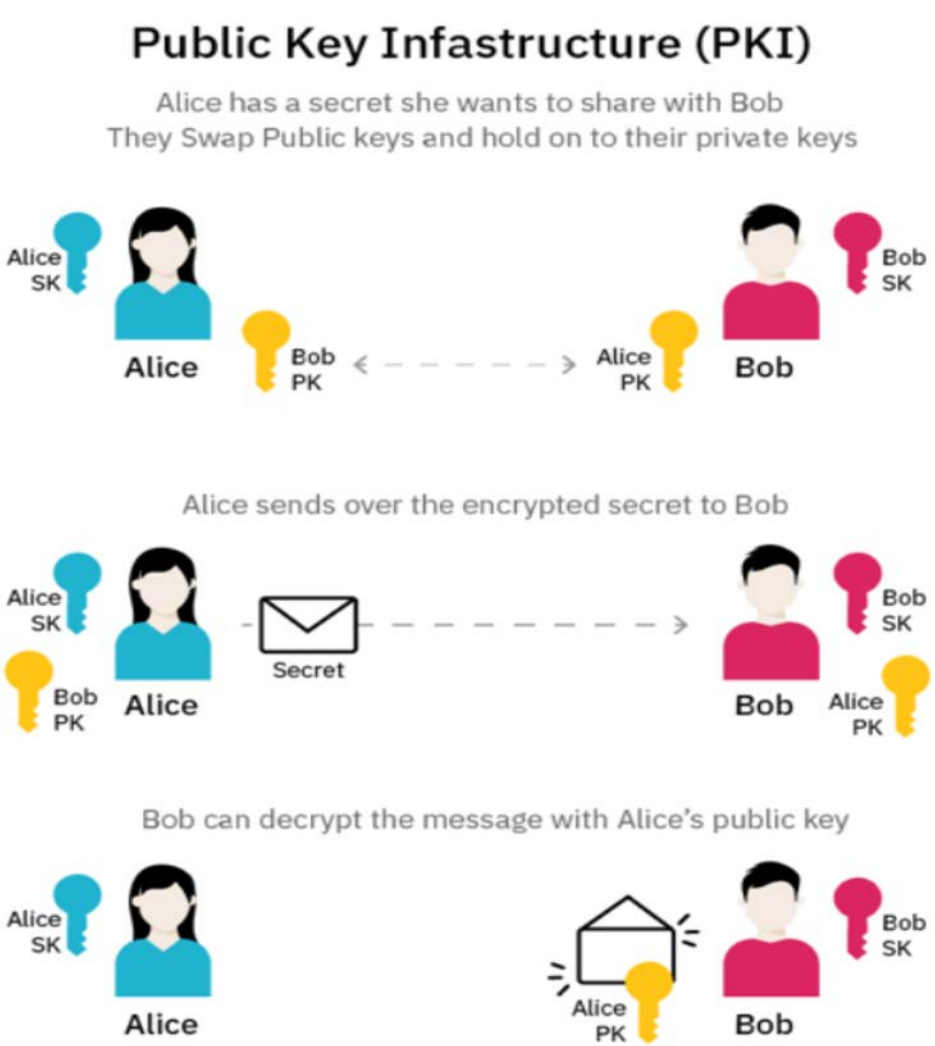


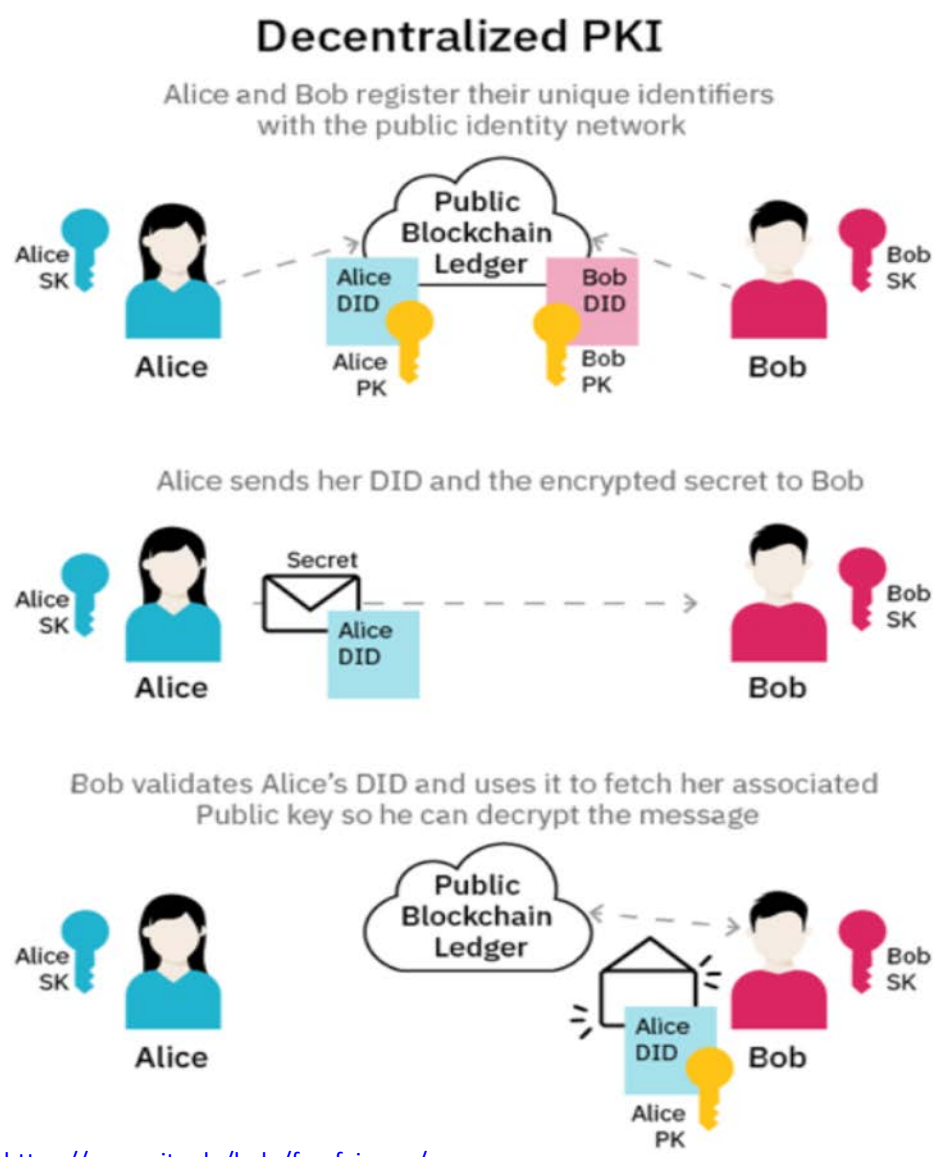
Devices are associated with Identity Hubs via identity-signed registration of device-specific public attestation keys.

Hub-associated devices synchronize state and update locally cached data via subscription to, and processing of, the Identity Hub change feed.

Hub-Associated Devices

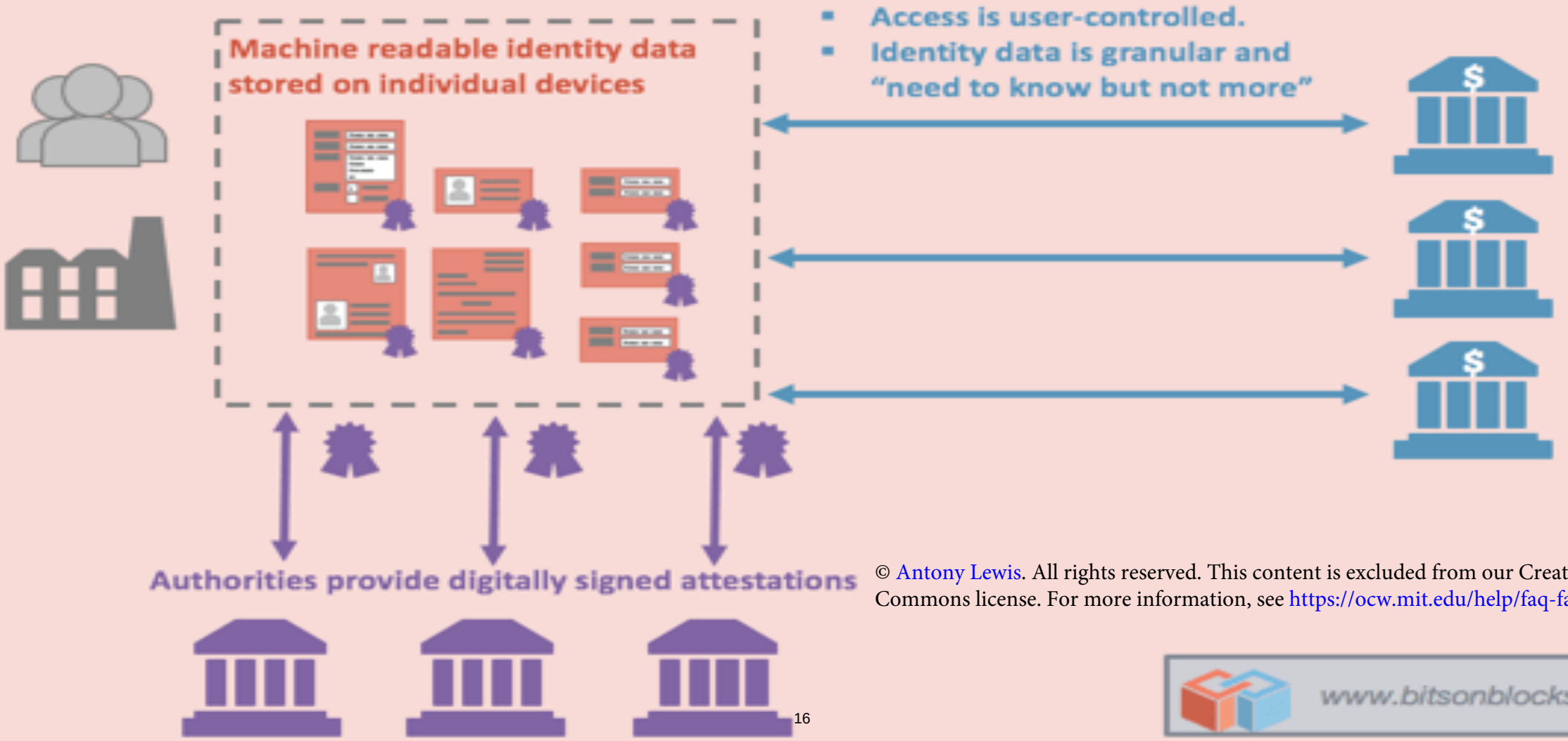
Public Key Infrastructure





SELF-SOVEREIGN IDENTITY PLATFORM

- Platform creates and enforces rules governing the workflow and approvals needed for data updates
- The platform does not store identity data
- Data transfer is secure, encrypted, point to point, over the web



MIT Diploma

Image of MIT's digital diploma system was removed due to copyright restrictions. You can see the image here.

Blockchain Seminar Dinner – 12/11

- David Burt, the Premier of Bermuda
- Elected July 2017 as Bermuda’s Youngest ever Premier
- Leads the Progressive Labour Party
- He has a master's in information systems development from George Washington University
- Will be talking about his government's various initiatives exploring blockchain technology, including a government-issued digital currency

Conclusions

- Modern Economies Extensively rely on Identity and Access Management
- Significant Issues of IAM in Digital Economy – Hacks, Fraud, Censorship, Costs, & Market Power
- Digital Signatures an Important part of Current IAM systems
- Self Sovereign Identity may Address these Issues
- Many Blockchain Technology projects being Explored
- For Adoption, must overcome Privacy, Control and Adoption Challenges

15.S12 Blockchain and Money
Fall 2018