PROGRAM MATERIALS
Program #29186
November 26, 2019

The Challenges of Identity Management and Decentralized Identity Systems- Legal Problems & Solutions

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

The Challenges of Identity Management and Decentralized Identity Systems

Charles Mondora and Victoria Dorum

Landman Corsi Ballaine & Ford P.C.

Overview

What Is Identity Management?	Identity credentials, claims and transactions
Types of Identity Management Systems	Federated/Centralized/Self-Sovereign (User-Centric)
Identity Management Challenges	Security and Privacy Considerations
Why Should You Care?	Domestic and International Regulatory Implications
What Is Decentralized Identity (DID)?	IDs that are self-owned, independent, and use blockchain and distributed ledger technology to protect privacy and secure transactions.
How Does DID Work?	Distributed Ledger Technology (a concept that includes blockchain technology)
Is DID the Future of Identity Management?	Current participants and work in the development of scalable DID standards
How Does DID fit into the Privacy and Cybersecurity Framework?	Cybersecurity, NY Shield Act, employment, banking and payment industries, CCPA, GDPR

What Is Identity Management ?

In the real world identity is made up of various government issued credentials:

- Birth certificate, driver’s license, marriage certificate, social security number.
- Real world credentials allow the identity holder a great amount of control over revealing their identity.

Online: digital identities are usernames, nicknames, account numbers, etc.

- A digital identity can belong to a person, group of people, organization or a non-human computational agent.
- Companies and corporation are the identity holders of individuals.
  - Ex.: an individual signs into an account using their user-name and password. Using the same sign in profile an individual signs into another account from a different company. The company that issued the individual the initial profile controls what information is shared and how it is shared. The identity owner has little control over their own identity and information associated with it.

Identity Management - Digital Identity

- Digital identity is different from an online identity because it is contextual.
  - A digital identity can be pseudonymized but still identify a particular account, it can build reputation and/or trust.
  - Digital identity vs. real world identity - no guarantee that the identity holder is who they say they are.

- Digital identities are transactional in nature.
  - Every virtual interaction that uses a digital identity is transactional in nature.
  - These transactions exemplify the benefits of identity systems.
  - Ex.: a digital identity enables the user to store their information on the cloud and easily access it later, save preferences for content a user chooses to see on a particular platform, keep credit card information on file, etc.

- Digital identities are issued, stored, verified and revoked by online organizations.
  - Identity Management is the process of maintaining digital identities by an organization.
  - Identity Management is important because it enables us to enter into online transactions.

Types of Identity Management

01 Centralized Identity Management

02 Federated Identity Management

03 Self Sovereign, i.e. Decentralized Identity Management

Centralized Identity Management

- Centralized - single sign in session for multiple logins by a single digital identity. Identifier is issued by a single authority. A single authentication credential to access different systems within a single organization.
  - SSO (Single Sign On) = allows a single account with an organization to be accessed by multiple web applications.
    - Ex.: Single Sign On session for both Gmail and YouTube.
  - Also allows web services to grant access to different sections in the same broader account.
    - Ex.: Online banking - move between checking and savings accounts without re-entering log-in credentials, although the two accounts are very distinct.
  - To a large extent, identity on the Internet today is still centralized.

Federated Identity Management

- Federated Identity Management is made up of a set of agreements and standards that enable the portability of identities across multiple enterprises and numerous applications to support a large number of users.
    - Single access to multiple systems across different enterprises. Users do not provide credentials directly to a web application, but only to the federated identity management system itself.
    - Ex.: the user's ability to log into different third party applications within a platform such as Google, Facebook and LinkedIn or Twitter accounts.
        - Originally, required to share the whole profile of the user, but this is no longer the case, but this is no longer the case.
- Large platforms switched to a user centric identity system, a sub-type of federated identity management.
    - Enables identity systems to only share parts of the user profile, which in certain circumstances a user may modify.

Challenges - Centralized Identity Management

- Identity and access management happens in one environment.
  - Users are locked into a single authority who can deny their identity or even confirm a false identity.
- The centralized authority is the owner and controller of the data.
  - Centralization innately gives power to the centralized entities and little to no power to the users.
- Security varies company to company.
  - A user’s data is as vulnerable as the greatest vulnerability within the centralized organization.

Challenges - Federated Identity Management

- The data belongs to the identity manager, not the user. Even in “user-centric” federated identity management systems, there is no real user control over the identity.
  - Users have little say and often little knowledge about how their identity is managed and how the data associated with their identity is collected and shared.
  - Policies created and maintained by the originating entity.
  - User tracking concerns.
- Service providers may get a hold of more data than is required.
- May contain weak links in the security chain; prone to phishing attacks; user ID’s and passwords are easily compromised.
- Identity may be revoked by the identity manger at any time for any reason.
  - If lose control over the identity originating account - lose control of all other accounts within the federation.

Addressing existing challenges and the shift to Self Sovereign Identity

- Self Sovereign Identity = give user control of own data.
  - To do that, a level of autonomy is required.
- SSI has been proposed since 2010s, but opinions about implementations differed. Additionally, concerns about costs and data management models prevented real momentum.
  - Building and replacing new data management systems can be costly.
  - Certain data management models can expose the companies to potential liabilities.
  - Self Sovereign Identities may make it difficult to establish trust.
- Policy makers recognized problems proliferating around the management of user identity and data, to a large extent as a result of lack of user control.
  - In Europe, the General Data Protection Regulation ("GDPR") was drafted with the intent to give users more control over their data and identities.
  - GDPR is made up of several articles and recitals that govern data processing and management of EU data subjects.

GDPR

Creates a uniform Data Protection standard within the European Union.

GDPR subject matter and objectives (Art. I):

1. Lay down rules for processing of data of natural persons and rules relating to free movement of personal data.
2. Protect fundamental rights and freedoms of natural persons, in particular right to the protection of personal data.
3. "The free movement of personal data within the Union shall be **neither restricted nor prohibited** for reasons connected with the protection of natural persons with regard to the processing of personal data."

Art. I of the GDPR signals that GDPR is not meant to restrict the transfer and processing of personal data. The Regulation is actually meant to promote the free movement and processing of data, while also protecting the rights of the individuals.

GDPR - Relevant Provisions

Six lawful bases for processing personal data (Art. 6)

- Consent = the ultimate basis for processing
- "Consent" is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."
  - Consent can be withdrawn by a data subject at any time
    - Must be notified of this right at the time consent is obtained
    - **Data controller must be able to prove that this level of consent was obtained**

- **Valid Consent is:**
  - **freely and affirmatively given;**
  - **revocable; and**
  - **provable.**

GDPR - Relevant Provisions

Privacy by Design and by Default (Art. 25)

- Privacy by Design states that any action a company undertakes that involves processing personal data must be done with data protection and privacy in mind at every step.
- Privacy by Default means that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user.

Data Minimisation (Art. 5)

- The data minimization principle requires entities to process only ‘adequate, relevant and limited’ personal data that is ‘necessary’.
  - No definition of what is adequate or relevant.
  - The assessment of what is ‘necessary’ must be done in relation to the purposes for processing.

GDPR - Relevant Provisions

Right of Access (Art. 15)

- Right of Access gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand what is being collected and how and why a company is using their data, and to verify whether that is done lawfully.

Right of Data Portability (Art. 20)

- The right to data portability allows data subjects to receive personal data they provided to a controller in a structured, commonly used and machine-readable format and to transmit those data to another controller
  - Promotes the free flow of data within the EU and fosters competition between the controllers

GDPR - Relevant Provisions

Right to Restrict Processing (Art. 18)

- Individuals have the right to request, either verbally or in writing, the restriction or suppression of processing of their personal data in certain circumstances.
    - When the right is exercised, companies are permitted to store personal data, but not use it.

Right to Object (Art. 21)

- Provides individuals with an unconditional right to stop the use of their personal data for direct marketing purposes.
    - An individual can object to the processing of personal data even if it is under the controller's "legitimate interests" unless the controller demonstrates compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject.

GDPR - Relevant Provisions

Automated Decision Making and Profiling (Art. 22)

- Rights related to Automated Decision Making and Profiling give individuals the right not to be subject to solely automated decisions, including profiling, which have a legal or similarly significant effect on them.
    - User inputs information and a decision is made relating to the user based on the data.
        - Ex.: automated refusal of a credit card application

Security of Processing (Art. 32)

- Personal data shall be:
    - “processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

NY Shield Act (Stop Hacks and Improve Electronic Data Security Act)

What's New?

- The SHIELD act expands data security and breach notification requirements to cover **<u>any business that collects private data of New York residents</u>**.
- Changes the definition of a security breach. A notification must be sent to any consumer whose data was **<u>simply accessed by an unauthorized party</u>** = more potential incidents and breaches will be covered.
- Protects a larger set of personal information, including: biometric information resulting from facial recognition software or other means; email addresses and their passwords, as well as security questions and answers; Social Security numbers; driver's license or non-drive ID card numbers; and any account number including debit and credit card information with or without security or access codes. This results in more data elements requiring notification if breached.

Section 899-AA (NY Breach Notification Law)

Previously:

- Breach notification requirements extended only to companies that conduct business in NYS.
- For a breach to trigger a consumer notification, private information would have had to be actively acquired by an unauthorized party.
- Private Information meant: (1) social security number; (2) driver's license number or non-driver identification card number; [or] (3) account number, credit or debit card number, in combination with any required security code, access code, [or] password that would permit access to an individual's financial account.

Businesses must comply within 240 days of when Governor Cuomo signed the law, or March 21, 2020.

NY Shield Act

The SHIELD Act requires businesses to develop, implement and maintain “reasonable safeguards to protect the security, confidentiality and integrity” of New York residents’ data, in three ways:

- Administrative Safeguards
- Technical Safeguards
- Physical Safeguards

NY Shield Act - S 5575 — B §3 (1) (c):

"Breach of the security of the system" shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of [personal] private information maintained by a business. Good faith access to, or acquisition of [personal], private information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure. In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.

Biometric Timekeeping Systems

Section 201-A
Fingerprinting of employees prohibited

Except as otherwise provided by law, no person, as a condition of securing employment or of continuing employment, shall be required to be fingerprinted. This provision shall not apply to employees of the state or any municipal subdivisions or departments thereof, or to the employees of legally incorporated hospitals, supported in whole or in part by public funds or private endowment, or to the employees of medical colleges affiliated with such hospitals or to employees of private proprietary hospitals.

Possible Liabilities related to biometrics:

- Biometrics = sensitive data
  - SHIELD Act revises the existing definition of covered PI to now include biometric information, such as a fingerprint, voiceprint, retina or iris image, or other unique physical or digital representation of biometric data, which is used to authenticate or ascertain the individual's identity.
- NY and NJ do not have biometrics specific laws **yet**.
  - Biometric-specific laws enacted by Illinois, Texas and Washington.

Considerations

- Where is the date stored and how is it processed?
- Are there adequate safeguards?
- Clear company policies
- Employee consent

Proposed Biometric Legislature

NEW YORK

AB 1911 - establishes the biometric privacy act; requires private entities in possession of biometric identifiers or biometric information to develop a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with the private entity, whichever occurs first.

- Provides a private right of action

NY 235 - relates to prohibiting private entities from using biometric data for any advertising, detailing, marketing, promotion, or any other activity that is intended to be used to influence business volume, sales or market share or to evaluate the effectiveness of marketing practices or marketing personnel.

Proposed Biometric Legislature

NEW JERSEY - AB 4640/SB 3153

- Personally identifiable information (PII) covers biometric data

- A business that collects a data subject's PII shall, at or before the point of collection, state the following:
  - description of PII, purpose, disclosure, contact of person responsible for data protection

- When PII is obtained, provide data subject with information about:
  - period of storage, right of accessibility

- Provide the following free of charge:
  - confirmation of whether data is or has been processed
  - Copy of PII within 30 days of request

- Right to opt out of processing
- A business shall maintain an information security program
- Provides a private right of action

Possible Solution?
Decentralized Identity Management:
Peer to Peer Model Using Blockchain

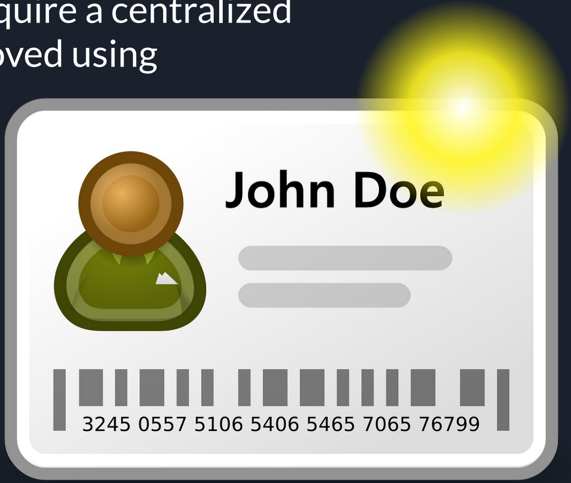
- Removes a centralized repository of identity data
- Provides the user with control and autonomy over what data is shared, how and when
- Provides a verification model
  - Enables validation of a digital identity, that is not offered by the current identity management systems
- Limits or eliminates the need of a company to store personally identifiable data

What is Decentralized Identity?

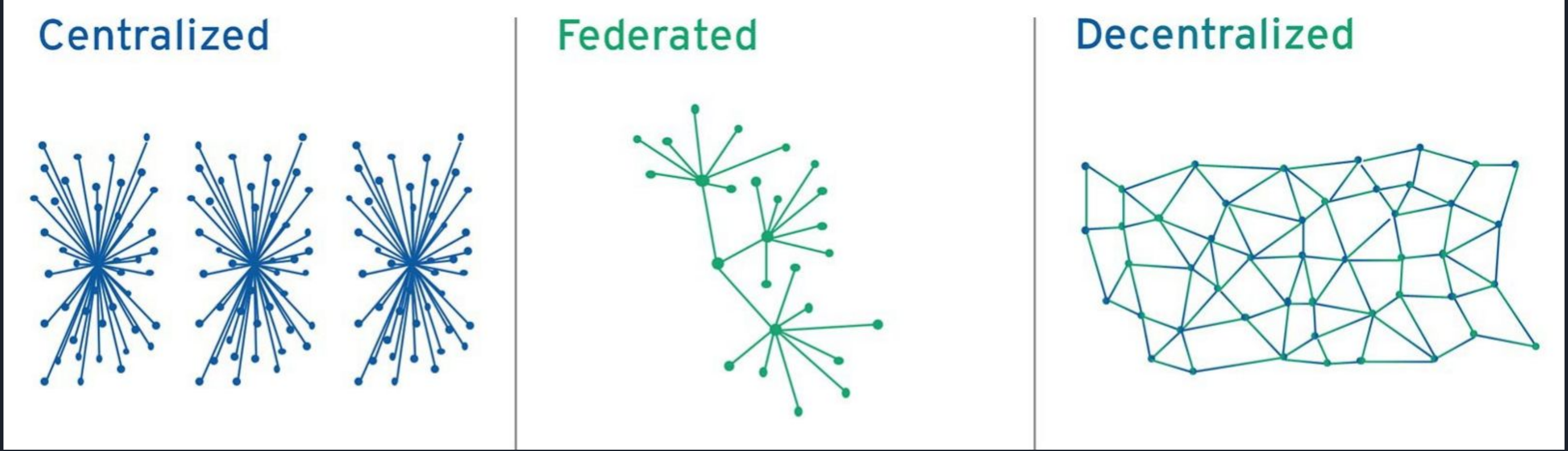
- Decentralized identity can replace identifiers, such as usernames, with IDs that are self-owned, independent, and use blockchain and distributed ledger technology to protect privacy and secure transactions.

- A DID is a new type of globally unique identifier that does not require a centralized registration authority because control of the identifier can be proved using cryptography and public key infrastructure.

- Decentralized ≠ self controlled.



Identity Management Systems

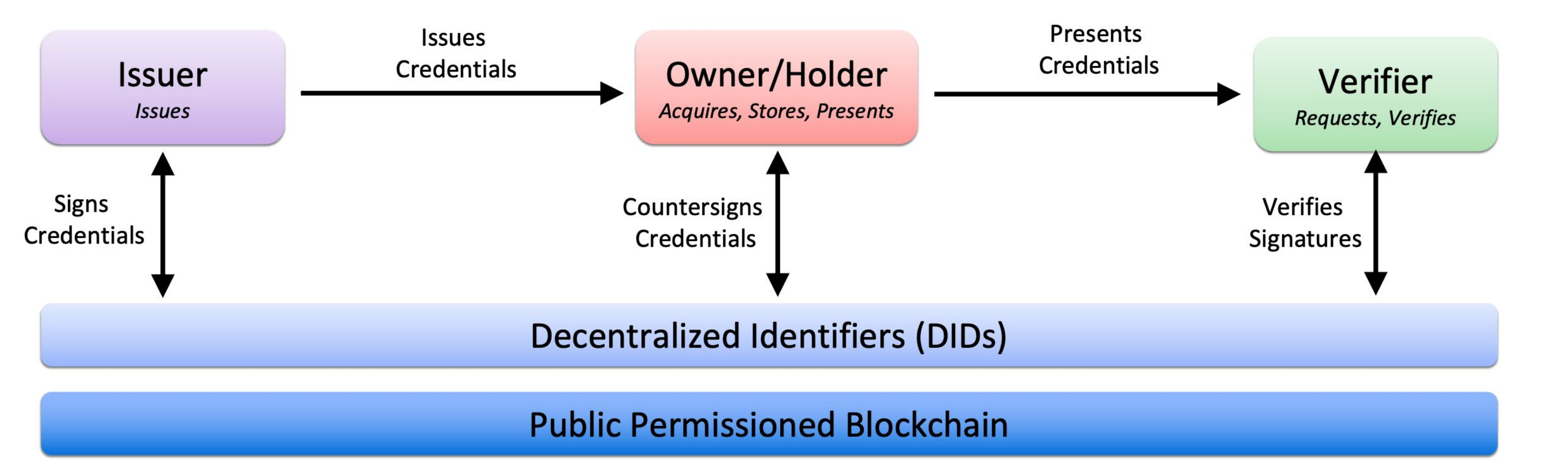


Identity transactions

- An identity transaction is made up of a claim, issuer, owner and verifier.
- Claim: a statement about you or an attribute you possess that is capable of being proven right or wrong. Ex: able to drive.
- Digital - verifiable claims: Cryptographic verification of a claim.
- Issuer: the entity that issues a credential
- ID owner: claimant
- Relying party/Verifier - the entity who the claim is being made to

How Decentralized identity works

Verifiable claim:



Sovrin SSI Credentials Demo: https://try.connect.me/faber.html

DID Advantages

Can address several issues:

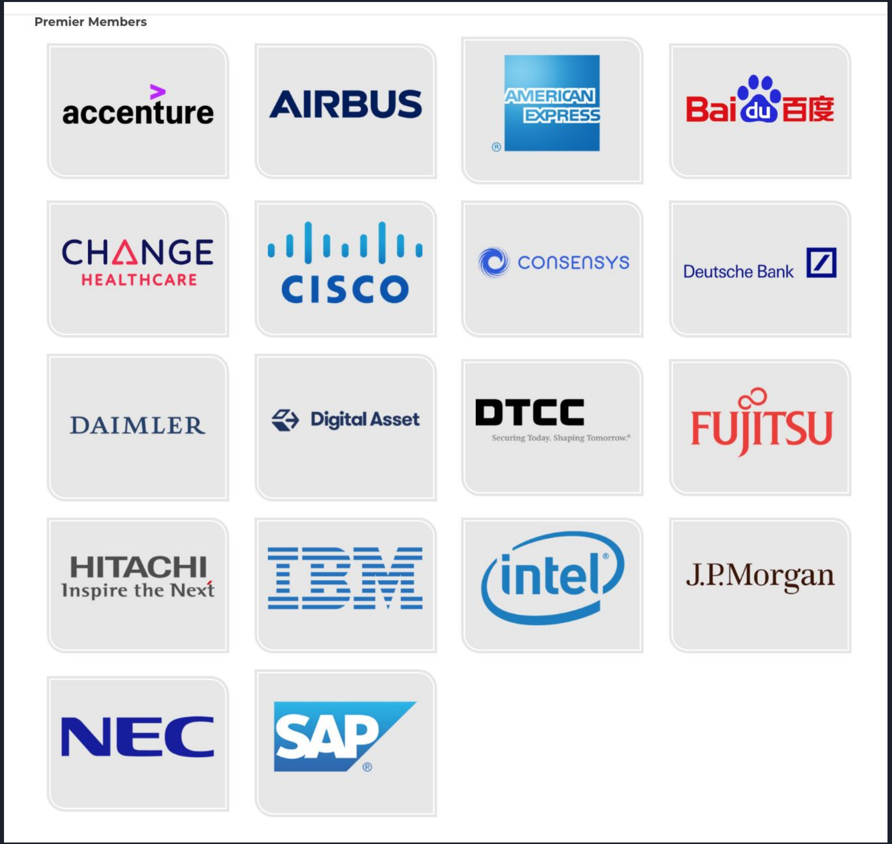
1. User privacy and autonomy
2. Verification
3. Cybersecurity
4. Legal Compliance

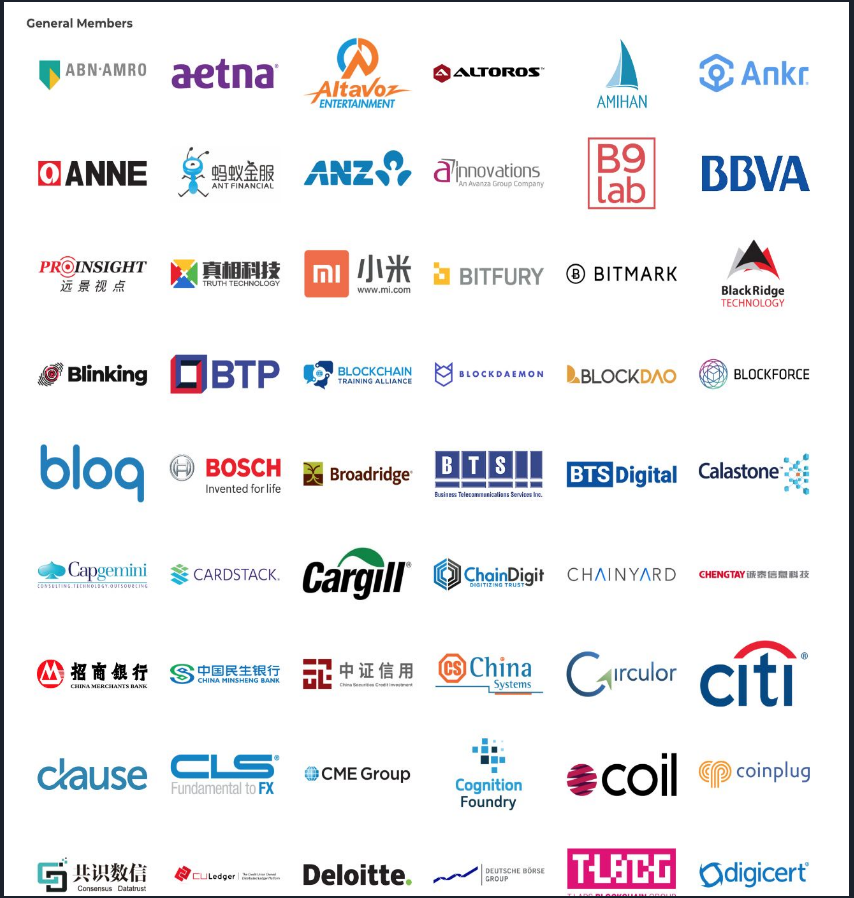
- Enables companies and organizations to engage its consumers and users with less risk, use electronic claim verification, and improve transparency and auditability.

- Enables developers to design user-centric apps and services and build apps that store data with users.

Is Decentralized Identity just a Concept?

- Yes and No
- Contemplated for a long time but not yet widely used
- Various standards for decentralized identity management systems are already in the making:
  - Sovrin - Non-profit foundation governing network to achieve self-sovereign identity (Member of DIF)
  - Decentralized Identity Foundation (DIF) - organization focused on development of foundational elements of a decentralized identity protocol
  - Hyperledger - Open Source Blockchain Project for Fabric and Indy designed to scale and optimize identity solutions. Indy is code base for Sovrin Trust Framework.
  - W3C - Standards specification of verifying and exchanging credentials; tandardizing schemas and operations for Decentralized Identifiers (DIDs)
  - OASIS - Standardizing protocols for communication between encrypted systems; Decentralized Key Management System


Premier Members


General Members

Hyperledger Membership: https://www.hyperledger.org/members

Landman Corsi Ballaine & Ford P.C.

European Blockchain Services Infrastructure

European Blockchain Services Infrastructure (EBSI)

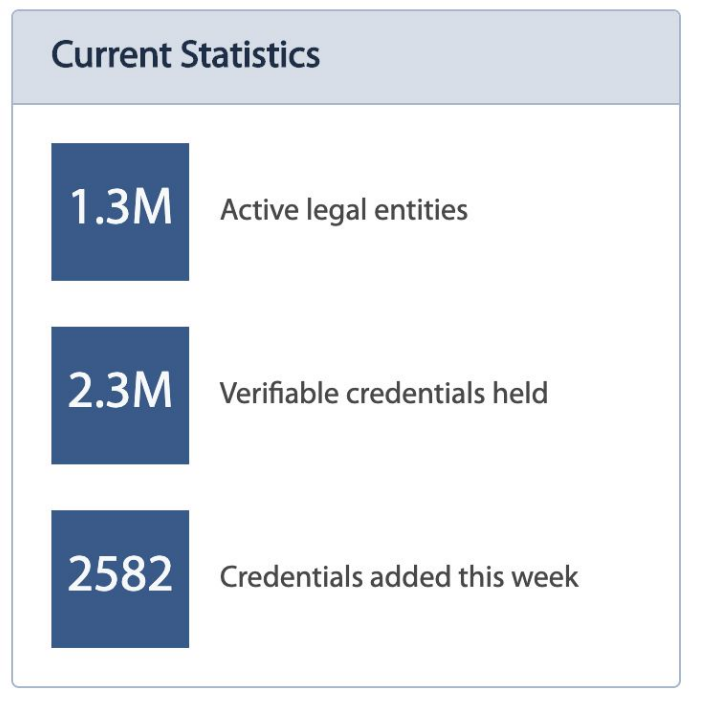
- ○ "The European Blockchain Services Infrastructure (EBSI) is a joint initiative from the European Commission and the European Blockchain Partnership (EBP) to deliver EU-wide cross-border public services using blockchain technology."
- ○ EBSI invested $4M Euros into developing a prototype of 4 applications using blockchain:
  - ■ Notarization - ability to create trusted digital audit trails and automate compliance checks in time-sensitive processes and prove data integrity.
  - ■ Diplomas - enable digital verification of education credentials; reduce verification costs and improve authenticity trust.
  - ■ European SSI- implement a generic self sovereign identity capability to enable users to create and control their identity without relying on centralized authorities
  - ■ Trusted Data Sharing - leverage blockchain technology to securely share data among customs and tax authorities

- ● Several US companies are also presently working on and funding the development of a DID standards.
  - ○ See Hyperledger Membership.

British Columbia’s use of Verifiable Credentials

- The Government of British Columbia Canada issued DIDs to companies to enable quick verification that an organization is registered to do business in BC as a corporation.
  - Other forms of businesses are to be added as well as other important verifiable data such as the permits, licenses, and other accreditations.
- As their case study explains a primary motivation for the project is to greatly reduce the bureaucracy associated with small business administration.

https://orgbook.gov.bc.ca/en/home



Current Statistics

1.3M Active legal entities

2.3M Verifiable credentials held

2582 Credentials added this week

Department of Homeland Security

- United States' Department of Homeland Security Science and Technology Directorate has been tracking, researching and investing into several blockchain initiatives.
- S&T's Blockchain Program focuses on security, privacy and interoperability and standards.
  - First implementation: tests starting in 2018 re: use of blockchain to verify certifications of origin used to qualify goods for preferential treatment under NAFTA and CAFTA-DR.
- Currently DHS is seeking to conduct more tests and implement blockchain solutions for the purpose of:
  - Tracking of goods' supply chains for compliance and audit purposes;
  - Issuance and verification of licenses, certifications, and other documents related to supply chain security and other issues;
  - Validating documentation proving citizenship, immigration and employment work-status authorization;
  - Validation of travel documents at TSA checkpoints.

See Cyber Security Division Technology Guide 2018 to find out more:
https://www.dhs.gov/sites/default/files/publications/CSD%202018%20Tech_Guide_Web%20Version_508.pdf

Privacy

Decentralized Identity Systems enable companies to:

- Accept existing verifiable credentials, Instead of issuing new digital identities for external parties like partners and customers;

- Limit the data they are collecting to only what is necessary or eliminate the collection of any personal data altogether;

- Based on the company’s business model, decide how the company will balance control over data between the organization and the user.

Selective Disclosure

Selective disclosure means that when you present claims from a verifiable credential, you can disclose only some of the claims rather than the whole credential. This is an important privacy-preserving capability.

Zero Knowledge proofs

ZKPs use some tricky cryptographic techniques to take privacy a step beyond selective disclosure. A ZKP based on a VC enables the holder to prove that something about a claim is true without disclosing the value of the claim.

- A calculation is being done without revealing calculation = cryptographically prove that you're over a certain age without revealing your age.

Autonomy

Decentralized Identity Systems enable the identity holder to:

- Have better control over the usage of their data
- Possible control over the monetization of the identity owner's data

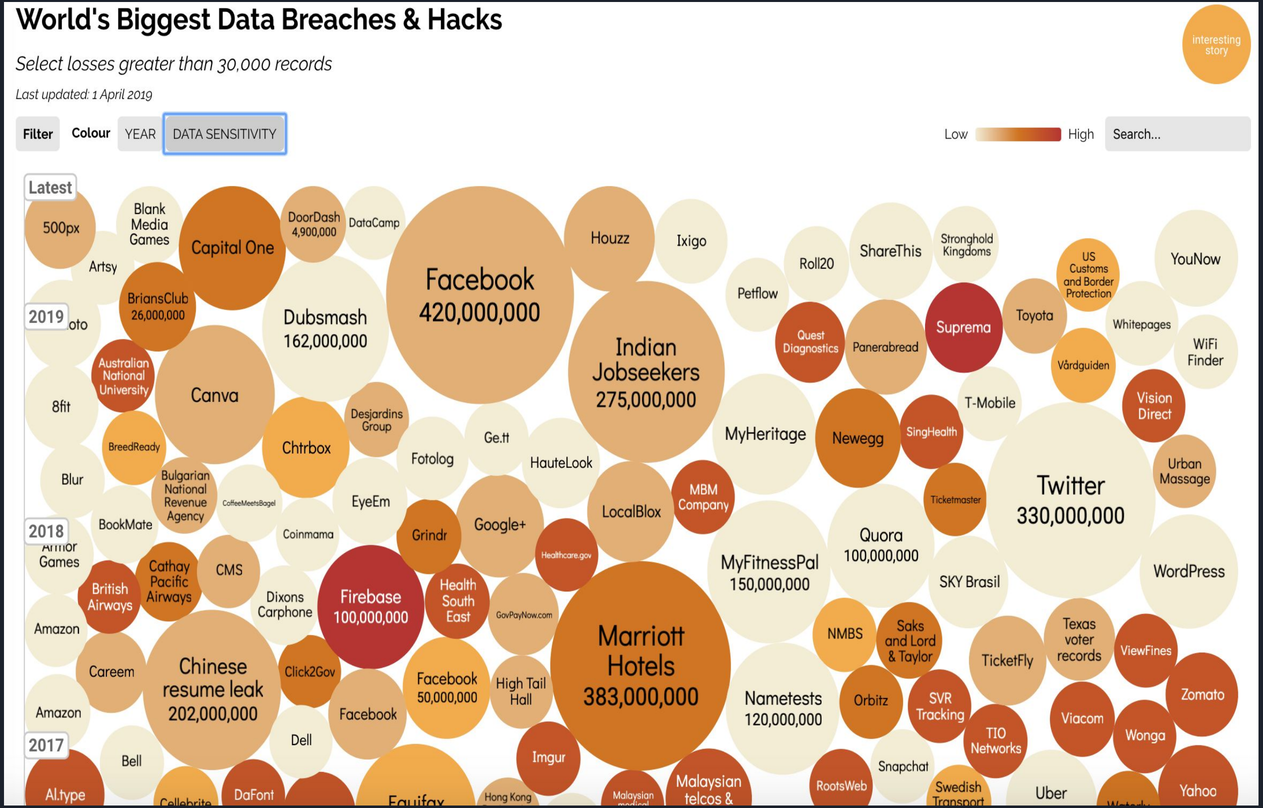
Security

- The most important aspect of data management.

- Security provisions are written into almost every data privacy law and regulation.

- Every organization in United States that uses technology has compliance obligations, regardless of its online presence or business model.

https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

Last updated: 1 April 2019

Filter Colour YEAR DATA SENSITIVITY

According to a data breach report done by Risk Based Security, the first six months of 2019 have seen more than 3,800 publicly disclosed breaches exposing 4.1 billion compromised records.

.https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

Landman Corsi Ballaine & Ford P.C.

Security

- No data is stored on the blockchain.

- Decentralization = no one party control the data, so there is no single point of failure or someone who can override a transaction.

- Using blockchain technology to decentralize identity is about digital validation and keys. A digital wallet with cryptographic keys that cannot be recreated without physical access to the device to validate identity.

- Data is stored either with the user/identity owner or trusted organizations/identity issuers.

- Decentralization minimizes the entities who hold data.

Banking with DID

- Currently every merchant/financial transaction online requires a customer to give their credit card information to the company it is making a purchase from.
    - Convenience and automated repeat transactions encourages repeat business, therefore companies want to enable users to store and save their credit card information with the account.
        - Financial information is a treasure trove for hackers.
            - DIDs enables transactions directly between the bank and the company without storing any of the payment information by the company.
                - Payment information is cryptographically protected.
                    - The payment can be processed without ever providing the company with the credit card number.

Decentralized Identity Management - Regulatory Compliance (GDPR)

Consent

- Decentralized Identity Systems are designed and centered around the ability of an identity owner to affirmatively and freely agree (explicit consent) to what identity information will be disclosed and how it will be used.
- The identity owner decides when to give its DID to a party and affirmatively accepts a proof request from a verifier.
  - This acceptance can then be tracked and revoked by the identity owner.
- All transactions are cryptographically signed and recorded on the ledger, therefore both the DID owner and verifier have proof of consent in each transaction.

Decentralized Identity Management - Regulatory Compliance (GDPR)

Privacy by Design:

- Decentralized Identity Systems create a standardized approach to Identity Access Management design centered around user control and data protection in compliance with the spirit of GDPR at every step.
- DID uses fair and open standards that can help users achieve more privacy and independence online.

Data Minimization:

- DID allows users to be in control of their data by default and set permissions to let processors request personal data for particular uses or verify identity without processing data.
  - Zero knowledge proofs and selective disclosure

Decentralized Identity Management - Regulatory Compliance (GDPR)

Right of Access

- Decentralized Identity Systems allow greater access and control over the identity owner’s own data.

Right of Data Portability

- A single DID can be widely used by the identity owner without duplicating and storing information with multiple service providers.

Decentralized Identity Management - Regulatory Compliance (GDPR)

Right to Restrict Processing

- Data is not stored on the ledger and is not processed by the verifier for the purpose of identity verification.
- To the extent that personal data is stored and processed by the issuer of a DID, the right to rectification, erasure and restriction of processing would depend on the policies of that organization.
- Where information hubs are involved, the data owner should be able to withdraw consent for processing with the use of DID.
  - However, rectification and erasure processes are still unclear.

Right to Object

- An identity holder can easily and verifiably assert this right through the use of a DID

Decentralized Identity Management - Regulatory Compliance (GDPR)

Automated Decision Making and Profiling

- DID puts the identity owner at the center of decision-making with respect to the sharing of their identity and certain identifiers.
    - Zero knowledge proofs may mitigate the concern over automated decision making and profiling, but will not eliminate them.

Security of Processing

- DID promotes security through cryptography encryption and by minimizing and/or eliminating the actual processing of data.
    - In many cases, verification of a DID does not require the processing of actual personal data.
        - Personal data remains with the issuer.
        - When personal data is disclosed to share with others it can be done via a secure private channel.

KYC: Know Your Customer

- A section of the Bank Secrecy Act of 1970 that sets forth requirements and regulations of financial transactions

- KYC laws were introduced in 2001 as part of the Patriot Act, which was passed after 9/11 to provide a variety of means to terrorist by taking anti-money laundering measures.

- Financial institutions must comply with: Customer Identification Program and Customer Due Diligence

Non face-to-face transactions under KYC laws in U.S.:

- In circumstances where a financial institution establishes a relationship with a customer remotely, the institution needs to employ non-documentary methods to verify the identity of the client since it cannot use a document to compare the customer to the photo identification, or needs to establish appropriate reliance agreements in order to rely on a third party who will conduct CIP on behalf of the institution. As part of its CIP, a financial institution should define whether it will accept remote account opening, and if so, what documentary and non-documentary methods will be used to verify customer identity. As a general rule, regulators encourage the use of more than one method to verify identity.

KYC: Know Your Customer

- Presently Identity owner have to go through the KYC process with different entities and submit the same information again and again
- With DIDs the organizations do not have to perform the same checks again b/c information can be proven to have been previously verified
- Trusted claims save costs spent on verification for the entity required to comply with KYC

<u>Considerations</u>:

- Are KYC requirements for the different entities the same? (Although possible to use different DIDs to go through one KYC process)
- Is storage of certain documents necessary as part of KYC?
- How do we establish trust? (Who do the relying parties choose to trust?)
  - What if the issuer of the DID is hacked?
- No guidance yet on use of DIDs in this context by US regulators.

Considerations:

The case of lost keys

- What key rotation and recovery mechanisms would be implemented to mitigate risk of the ID holder's loss of keys?
- What if an someone gets a hold of the issuer's keys and verifies false DIDs?

Identity hub security concerns

- Are there any obligations on the entities who access identity hubs with respect to security of the data?
- The extent of identity hubs's compliance with data portability, access, objection, rectification and other GDPR requirements is not yet clear.

Ownership and Processing of Data

- Who is determining the purposes and means of data processing in relation to a DID?
- Who owns the data?

Practical concerns:

- Who will pay for verification of a DID?

Is DID right for everyone?

- DIDs can help replace traditional Identity Management Systems and build trust, as well as simplify and accelerate online transactions in a way that is not currently possible.
- DID would enable peer-to-peer and business-to-business interactions without reliance on time-intensive onboarding processes.
- With the use of DIDs, identity owners can benefit from being in control over their own identity and use it securely and privately for different purposes.

However,

- DIDs can pose challenges to companies whose business model relies on data aggregation.
  - Social media sites
- Some business models require certain data to be collected.
  - Ex., when dealing with an online merchant for purchase of goods, even if a DID is used for payment, the merchant has to know where to ship the product.
  - Even if a business is not required to collect certain data, it may want to for marketing purposes, to conduct analytical market research regarding its sales and clients or to build customer relationships.

Questions?

Landman Corsi Ballaine & Ford P.C.

Charles Mondora: cmondora@lcbf.com

Victoria Dorum: vdorum@lcbf.com