January 2019

ID

Digital ID

A Report on the Digital Identity Landscape & Providers

Presented By

BLOCKCHAIN
LEARNING GROUP INC.

Blockscale Solutions

Author Biographies

Primary Author

Chami Akmeemana

Chief Executive Officer | Blockchain Learning Group | Blockscale Solutions

chami.akmeemana@gmail.com

Chami Akmeemana is the CEO of Blockchain Learning Group and Blockscale Solutions. He is a Blockchain and AI Specialist. He pursued a Ph.D. in Bioceramic Engineering at Queen Mary, University of London, until deciding to forgo an academic career in favor of Law Enforcement. In 2002, he joined London's Metropolitan Police.

Chami has had 4 successful exits over the last decade and is passionate about the intersection of technology, business and social good. His experience includes serving as Director of Regulatory and Government Affairs at ConsenSys Inc; Fintech Advisor to the Ontario Securities Commission; Managing Director, Fintech and Blockchain at the Global Risk Institute; and Regulatory Advisor to the Republic of Liberland. Chami is also the Chairman of the Blockchain Association Australia and an Advisory Board member of doc.ai.

With Contributions from **R. Jesse McWaters**, Financial Innovation Lead at the World Economic Forum

R. Jesse McWaters leads the World Economic Forum's exploration of fintech and financial innovation. His work focuses on bringing together senior financial services executives, leading fintech players, and global regulators to understand how new entrants and new technologies, including blockchain, are transforming the competitive dynamics of the global financial ecosystem.

Table of Contents

Executive Summary

ID is a fundamental consideration for almost all digital systems in existence today. As digital identities progress beyond being mere login credentials on the internet and begin to represent legal tokens that affect personal rights and societal access, as is the case with the digital identities that are becoming an increasingly common part of humanitarian organizations and government projects, understanding the various aspects of ID solutions and thinking critically about how well they align with long-term program objectives becomes of utmost importance.

An increasing number of recent technological advances in things like the affordability and ubiquity of biometrics, the proliferation of smartphones, and blockchain or digital ledger technologies are helping to unlock the power of digital identities. When used together, these elements have the potential to create portable and permanent user-owned identity products that achieve new levels of security, privacy, and utility which are not possible with traditional identity products. However, like everything digital, room for problems abound if digital identity is done incorrectly.

Centralization has been one of the biggest risks of digital identities to date. Not only does giving custodianship of personal data to a single entity create risk of data loss and security breaches, it also bestows great power upon the company providing the service to allow or deny usage of that identity and all the access it enables. Being locked into proprietary technologies also creates a risk to the permanence of the identity, tying its fate to the continued existence of the company which provides it. While some of the newest ID solutions and standards out there purport to resolve some of these issues, as with any new or cutting edge technologies, it can be hard to see through the hype and find the credible players with viable and practical ID solutions that are ready for real world usage.

The core of this paper consists of a comparative summary of responses to a survey we issued to a group of some of the more popular digital identity companies out there which we feel have the industry presence and product readiness to be viable ID solutions. The aim is to educate the reader on what we think are some of the more important aspects of modern digital identities to consider and some of the questions which should be asked when evaluating potential ID solutions.

Introduction

Digital Identity

Digital Identity as a System

Digital Identity

From website logins and social media accounts, to national identity platforms which grant rights and access to social services for citizens, digital identities are becoming ubiquitous all across the world. They have progressed from loose collections of usernames and passwords which grant access to isolated digital services, to biometrically-enabled profiles which give agency to the undocumented and act as legal tokens that fundamentally enable or deny an individual the ability to participate in their society or economy. As acceptance of digital identities grows to become more common, and especially as more essential and critical services are bought online in large-scale government or humanitarian projects, it becomes paramount to understand the options and risks implicit to the various models of digital identities on offer when embarking on new technology projects.

Digital Identity as a System

Before we can assess the range of efforts presently underway to unlock the potential of digital identity, it is useful to reflect upon a deceptively simple question: "What is an identity"? It is important in this context that the answer captures the full scope of what is required to establish a fully functional identity system.

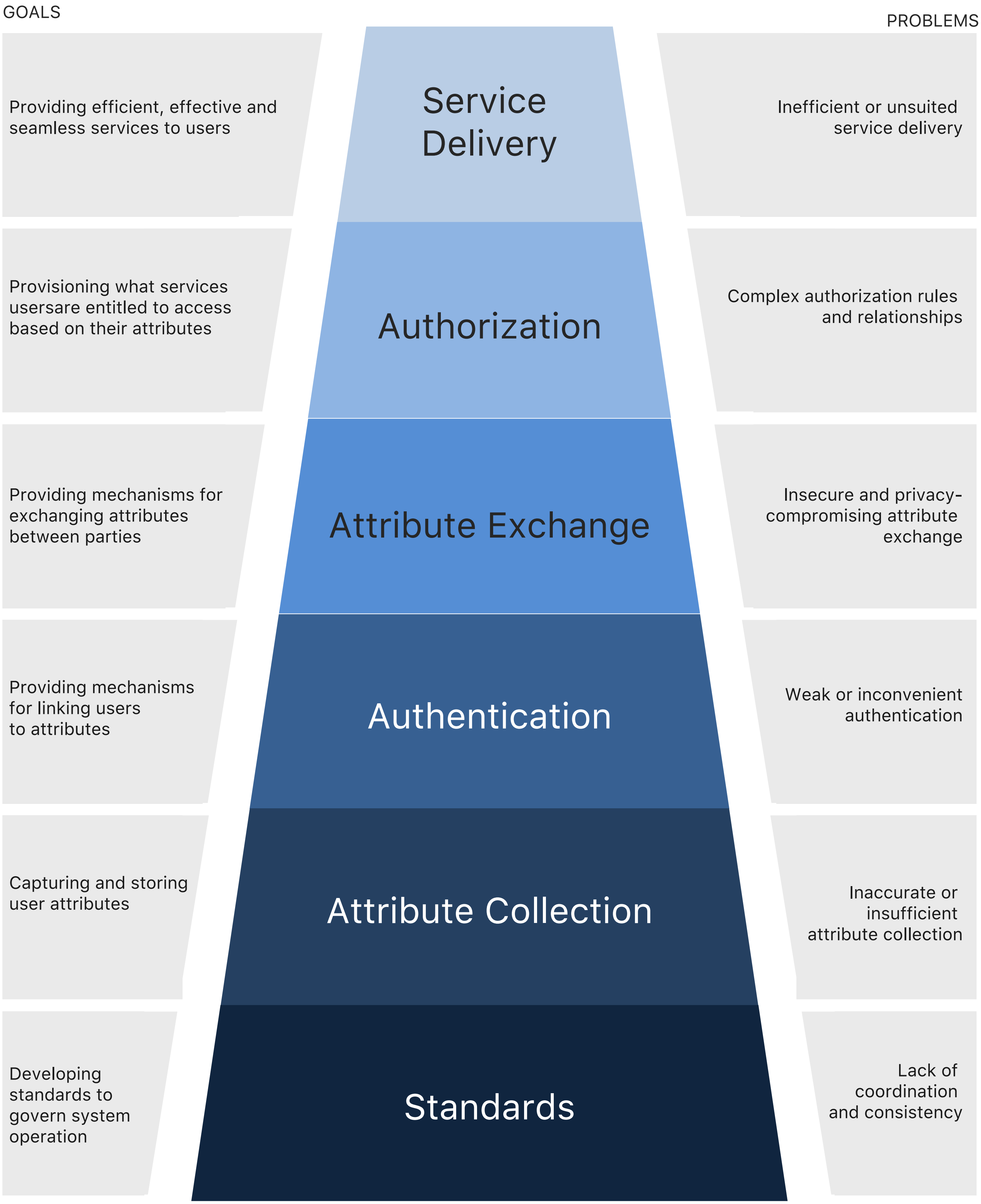
While we may be tempted to think of identity simply as the card that we carry in our wallet, the concept is much more nuanced and complex. Identity systems serve many political, social, and cultural roles. They can shape people's sense of belonging to a nation by giving them a physical token that connects them with their state, and enrollment processes can shape who shares in a sense of nationhood or sovereignty through choices about inclusion and exclusion. Their usage also grants rights and privileges in society, enabling personal independence and even a sense of pride through what this access represents. A primary utility of identity systems is to enable transactions where one or more parties must be satisfied that the entity they are transacting with has certain attributes (e.g. that they are of a certain age, or domiciled within a certain legal jurisdiction) based on the attestation of a third party rather than through direct observation. Although enabling these transaction is the focus of much of the material discussed in this document, this is only one aspect of a complete digital identity system.

There are numerous competing models for understanding identity as a system. One simple, illustrated model that may be useful to readers is taken from the 2016 World Economic Forum Report 'A Blueprint for Digital Identity'. This model thinks of identity as a 'stack' with multiple layers, each of which serves a different purpose in enabling transactions and suffers from a distinct set of problems in the current identity landscape. Before exploring the opportunities offered by the rise of digital identity systems, it is important to reflect on one particularly common error encountered while thinking about identity systems - confusing the layer of activities related to authentication with the broader system of identity. As we'll discuss, many recent advancements in the digital identity space have been made in the authentication of users, such as the proliferation of biometrics, which have improved user experiences and offered higher levels of assurance. However, authentication technology alone is not digital identity. The use of this technology, while valuable, still relies upon preexisting onboarding and attribute collection processes, secure storage mechanisms, and does not by itself provide a system for the exchange of these attributes between trusted parties. (see diagram on Pg. 7)

Opportunities in Digital Identity

Digital identifies have the potential to solve many of the problems associated with traditional ID tokens like government-issued cards or papers. Entire countries like Estonia and Pakistan with their national ID programs, and India with it's Aadhaar platform, have successfully established large-scale national identity systems to streamline service access for their citizenry with a single ID. Aid agencies, like UNHCR, are also creating biometrically-enabled digital identities for hundreds of thousands of undocumented refugees to allow them better access to aid programs and support. They empower a user to have control over their identity claims without relying on a physical token like a document that could easily be lost, damaged, or controlled by a malevolent party.

When designed thoughtfully, digital identities can also provide better security through mechanisms like multi-factor authentication and have increased resistance to forgery, misuse,



GOALS		PROBLEMS
Providing efficient, effective and seamless services to users	Service Delivery	Inefficient or unsuited service delivery
Provisioning what services usersare entitled to access based on their attributes	Authorization	Complex authorization rules and relationships
Providing mechanisms for exchanging attributes between parties	Attribute Exchange	Insecure and privacy-compromising attribute exchange
Providing mechanisms for linking users to attributes	Authentication	Weak or inconvenient authentication
Capturing and storing user attributes	Attribute Collection	Inaccurate or insufficient attribute collection
Developing standards to govern system operation	Standards	Lack of coordination and consistency

or theft in comparison to traditional identity tokens. They can also enhance privacy through contextual and consent-based disclosure of personal information when others wish to validate claims, such as license status or if a person has reached age of majority, without having to disclose irrelevant details like full date of birth or home address.

Unlike paper or plastic ID cards, digital identities can also be claims-based, validated and endorsed by multiple trusted parties like banks, community groups, or government agencies every time they are used. Those endorsements can then be tracked as part of the identity to increase its strength and trustworthiness over time in ways not previously possible with other identity systems, creating an identity that is based on reputation instead of the endorsement of a single sovereign authority which may not be attainable by all members of a population due to issues of inequality and discrimination.

Recognizing the potential of a truly portable digital identity and the increasing fragmentation of the ID space as new solutions arrive on the market, numerous working groups and consortiums like DIF and W3C are establishing standards and specifications with the aim of allowing for some degree of interoperability between the various technologies. The development of and adherence to these standards is key for the future of digital identities and their broader acceptance since an ID is only as useful as the amount of people who accept and trust it. Although enabling these transactions is the focus of much of the material discussed in this document, this is only one aspect of a complete digital identity system.

Risks of Digital Identity

One of the main risks of traditional digital identities is in the centralized storage of personally identifying information or credentials in that it becomes a target for data breaches. News reports of data breaches compromising the privacy and personal information of millions of people are now publicized often enough to harm public confidence in the ability of companies to protect their data, but the same can also happen to governments or any institutions who store sensitive personal information. Not only that, but having a master copy of the data stored in a single location also opens it up to corruption or data loss through hardware failure, accidental deletion, or misuse by actors who may have administrative control

Risks Of Traditional Digital Identities

Centralized storage of personally identifying information

over the system. This makes data security, storage, and privacy protection mechanisms key points to keep in mind when evaluating ID providers.

Another risk relates to the logical centralization or ownership of the data by a single entity. A common trend in consumer-oriented digital services is the popularity of federating ID services out to large, centralized technology companies like Facebook in the name of convenience due to the high utilization of these services by the general public. One must realize that this puts the control and security of the personal data involved in the hands of these companies, which could raise privacy concerns and may not be appropriate depending on the fundamental importance of the digital ID in question and the access it grants. The concern could also extend to the example of a humanitarian organization creating digital identities for a marginalized population. If they become the custodians of that data due to their involvement in the enrollment process and choice of technology solution, they (instead of the identity owner) become responsible for the maintenance and safeguarding of that digital identity and the access it provides, which is a responsibility that must not be taken lightly.

Parallels for both the privacy and centralization concerns can also be drawn to companies in the digital ID provider space. For ID providers who store, maintain, or enable access to digital identity data as part of their service, if their solutions or services are based on proprietary technology, you are investing in their ability to protect the privacy, security, and appropriate access to this data and limiting the portability of the identity. Adopting solutions or ID protocols that are based on open technologies and standards helps to mitigate this risk somewhat

Biometrics

Advances in biometrics are making things like fingerprint, facial, and iris scanning cheaper.

since they will likely have a higher degree of data interoperability with other technologies and could still retain utility beyond the life of the given service provider or company in question should they cease to exist in the future. While consortium-based identity models might mitigate this centralized risk somewhat, it is still important to understand the governance framework and philosophies of the foundations involved to ensure they align with the program objectives and rights of the affected user base.

Finally, with the drafting and enactment of data protection regulations becoming more common globally, like the European Union General Data Protection Regulation (GDPR), the custodianship of data and the ability to control it's proliferation and permanence are becoming increasingly important considerations when selecting solutions that could see international usage, as is the liability framework that surrounds them in the event of non-compliance.

Recent Trends in Digital ID Technology

Numerous advances in the sophistication and affordability of various complementary technologies has led to a large increase in the availability of ID solutions available on the market. Some of the recent traits and technologies that are now common to digital identity services are:

- **Biometrics:** Advances in biometrics are making things like fingerprint, facial, and iris scanning cheaper, easier to use, and more readily available. This is allowing biometrics to become an increasingly common component of digital identity solutions, both for enrollment and field-level authentication in use cases where it's warranted.

- **Smartphones:** While mobile devices have long played a role in digital identity schemes via registered SIM cards and groups like GSMA, the global proliferation of smartphones enhances the process further and enables other opportunities, like secure on-device storage of data and increasingly sophisticated biometric sensors which can be used for authentication.

- **ID Platforms:** Digital identities are increasingly shifting from functional items and proprietary technologies that facilitate access to a single service to more foundational ID platforms that adhere to open standards and utilize interoperable technologies. This vastly increases the power of a digital identity, creating the potential for it to be accepted by various entities for a variety of purposes, increasing its longevity and utility.

- **Self-Sovereign Identity:** Digital identities enable the possibility of a portable, lifetime identity, free from the control of any external institution or authority, whose utilization and claims are entirely controlled by the owner.

- **Blockchain and Digital Ledger Technologies:** Mainly by way of augmenting other technology solutions, blockchain is finding a place in many new digital identity services on the market. Its various cryptographic security mechanisms, data immutability, and decentralized network architectures can be leveraged for the design of secure, user-owned, attestation-based digital identity solutions.

Opportunities Created by Blockchain

If used appropriately, blockchain has the potential to address some of the common pitfalls associated with digital identities and can be instrumental in enabling the creation of user-owned, claims-based digital identities that are portable between services and put privacy and security first in their design. This comes from leveraging some of the unique characteristics inherent to the technology:

- **Decentralization:** Increases data and network resiliency, reducing some of the risks inherent in centralized storage of ID-related data and centralized control of infrastructure. Utilization of a public blockchain network for some part of the service can also help facilitate the creation of self-sovereign identities since it creates permanence and removes reliance on an external ID provider to store or provide access to the identity.

- **Cryptographic security:** Public key cryptography and digital signatures proves ownership of an identity through physical control of a key pair stored on a device like a mobile phone or a smart card. It also provides a means for securely signing transactions, and a way to encrypt personal data and provide pseudonymous access to it while maintaining personal privacy and controlling its dissemination. The emerging use of concepts like zero-knowledge proofs can also further enhance the data privacy in some implementations as it allows for proof of a claim to be provided without having to exchange the underlying data.

- **Immutability:** A tamper-proof, cryptographically secure, append-only blockchain ledger that through consensus can act as a single source of truth increases the integrity and trust of an ID system, allowing identity reputation to be built up over time via verifiable claims and attestations.
- **Transparency:** Since ID identifiers can be made visible to all network participants, it allows identities to be discoverable and portable, and also easily allows identity claims and signatures to be verified by counterparties. This does however mean that one has to be mindful of how correlatable the data stored on chain may be to a given individual to ensure it does not create any unintended privacy issues.

The existence of value exchange rails in some blockchain technologies also potentially allows for the creation of inventive cryptoeconomic incentivization mechanisms to encourage network participation in use cases that would benefit from it, though such schemes are not necessarily prerequisites to gain the underlying benefits of utilizing blockchain technology.

Blockchain: Proceed With Caution...

While blockchain has the potential to greatly enhance various aspects of digital identity services, one must also be cautious when evaluating ID services to cut through a lot of the hype that exists in the industry. Many companies in the space masquerade as comprehensive solutions which in actual fact are far from being production-ready or have little in the way behind them other than fancy marketing materials and unsubstantiated promises.

One must also consider the type of data that gets stored on chain given its permanence, since any bad or erroneous data entered by way of process issues or mistakes also ends up being permanent since immutability means that it can only ever be amended. This could easily introduce privacy issues or hinder one's ability to comply with GDPR-like regulations.

Finally, how private key storage and key recovery is handled are also important elements in any blockchain or cryptographically-enabled identity system since losing control of a private key means losing proof of ownership and control over a critically important part of your digital identity.

Private key storage

Losing control of a private key means losing proof of ownership and control

Current Landscape

An ID Comparison

Current Landscape: An ID Comparison

While Based on a series of questions covering key elements that we feel are important to consider when selecting an ID service, we reached out to companies in the current blockchain or cryptography-oriented ID landscape that we felt, based on industry presence and product readiness, have good potential as ID solutions.

We reached out to over twenty (20) ID providers globally to participate in this study. Five of them responded and what follows is a comparative summary of their responses.

Note: These responses were provided by the companies stated and do not reflect the views or opinions of the authors of this paper.

Companies:

- Civic (https://www.civic.com/)
- uPort (https://www.uport.me/)
- Sovrin (https://sovrin.org/)
- ShoCard (https://shocard.com/)
- Estonian ID (https://e-estonia.com/solutions/e-identity/id-card/)

ID Solutions

General Overview

ID Solutions

General Overview

Would they be described as an ID Provider?	
Civic	Civic is an identity company, powered by blockchain, that provides businesses and individuals with tools to control and protect their identity. The Civic Secure ID enables personal verified information to be stored on user mobile device using bank level encryption and biometric locks. Users safely access partner websites and services using the Civic Secure ID. Civic's Secure ID Platform (SIP) enables businesses to leverage the Civic Secure ID via the Civic App, Integration Portal, Civic Web Connect and Civic App Connect to perform login, age verification and know your customer verification activities. Additionally, Civic is spearheading the development of Identity.com, a decentralized identity ecosystem that is designed to facilitate on-demand and secure access to blockchain-based identity verification services.
uPort	Yes. uPort is a platform for self-sovereign identity and user-centric data management, anchored in Ethereum. It provides a mobile application which enables users to create a digital identity in a few simple clicks. From there, users can start interacting with uPort compliant services. For example, in the city of Zug, Switzerland, a citizen can then receive a credential verifying that he/she is a resident, and use that credential via uPort for multiple services like eVoting or eBiking. uPort also provides a rich set of tools and SDKs that developers can use to add uPort capabilities into their applications or solutions, guaranteeing they will deliver services their end users can trust.
Sovrin	No, the Sovrin Network is a public service utility enabling self-sovereign identity on the Internet. This decentralized identity network offers enterprises and developers free, open source code to create private and secure data management solutions that run on Sovrin's identity network. The Sovrin Network allows individuals to collect, share, and manage the individual components that make up their identities.

ID Solutions

General Overview

Would they be described as an ID Provider? (Continued...)	
ShoCard	Yes, ShoCard is a digital identity and authentication platform built on a public blockchain data layer, using public/private key encryption and data hashing to safely store and exchange identity data, which includes biometrics such as fingerprint, facial, iris and voice. ShoCard's approach to identity is different than existing solutions in that the user owns and carries her own data within her mobile app and is the sole person who decides with whom to share it with and which pieces of identification to share. The blockchain is then used to validate that information and confirm other third parties who have definitively certified the identity of the user. There is no privately held central location that holds user's private information and pieces of a user's identification do not need to be spread in other services in order to authenticate or prove ownership of an account. The mobile app is as easy and intuitive to use as a driver's license, but secure enough for a bank. They have three products: • **ShoCard Embedded:** B2B2C- Securely register for, verify and log into financial institutions, websites, membership/ID, stores, signing authority with delegation, and more. • **ShoBadge:** B2B- Enterprise no username or password Login with 6 factor authentication using SAML, OAuth, OpenID Connect • **ShoVerify and ShoKYC:** Allow enterprises and individuals to authenticate, conduct KYC and AML as well as sign documentation – all under one platform
Estonian ID	Yes, Estonia has a state-issued digital identity that enables to authenticate people without physical contact and use digital signing on a wide scale to use thousand of public and private services. In Estonia, every person can provide digital signatures using their ID-card, Mobile-ID or Smart-ID, so they can safely identify themselves and use e-services.

ID Solutions

General Overview

How does their ID Solution(s) Work?

Civic	Individuals can access Civic's Secure ID Platform (SIP) through the Civic App. The Civic App stores a user's personal information securely on their mobile device, protected by biometrics and high-level encryption. With decentralized architecture, the Civic App enables users to share and manage their fully verified identity data. The Civic Secure ID stored in the mobile device proves that a real person has matching documents that prove their identity online. It uses a combination of selfie checks, liveness tests and document verification to verify identities. Civic partners can request a user's information through custom QR codes that are scanned with the Civic App. Once a user has unlocked the Civic App with their biometrics, the user can scan this code and review exactly which information is being requested. If the user doesn't have their identity already verified inside the app, they could choose to get verified with a 3rd party validator. Once the verification process is complete, users choose whether to approve or deny the initial verified information request. If the user is already verified, they can reuse existing verified identity information to respond to the request. Easy, convenient and secure. The Secure ID Platform allows for voluntary exchange between the user and an identity requester and allows for real-time authentication of personal information that is already verified by a trusted party.
uPort	Users can download the uPort app from their favorite app store and be up and running in a few minutes. The onboarding process to create a digital, decentralized identity is frictionless and free of any gas cost. The user's mobile phone is used by default as the user's Identity Hub, where off-chain attestations are stored. This enables the user to own any identity-related data issued to them in the form of attestations, and control what information they disclose to uPort compliant service-providers when they request it. uPort handles the issuance, storage, exchange and verification of off-chain (JWT) attestations. In addition, for users who want to interact with Ethereum applications, it also supports on-chain attestations. A user's attestational data can alternatively be stored or backed up in an Identity Hub of their choosing, such as a cloud Identity Hub provider. Users can recover their identity using either seed recovery, delegated or social recovery. uPort provides many tools for developers, such as libraries, a JS client, a mobile SDK and App, and a command-line client, which enable developers to seamlessly integrate uPort functionality into the products they are building.

How does their ID Solution(s) Work? (Continued...)

Sovrin	Sovrin enables people to interact online in the same way that they do in the physical world. In the physical world, humans accumulate documents from government, financial/education/ healthcare institutions, and more. They use these documents out of their intended context to assert things about themselves (showing your driver's license can prove with reasonable assurance that you are who you say you are). Sovrin enables this same thing but in a digital world. You can hold many different credentials and use them in other contexts aside from their intended use to prove things about you—only with added privacy features. For more information on this multi-source identity, see: http://www.windley.com/archives/2018/05/multi-source_identity.shtml
ShoCard	Through the ShoCard application, a person's identity and data are stored on their device and they are the only person who determines which ID details are shared. ShoCard uses the blockchain as a public, immutable ledger that allows third parties to validate that the original data or certification has not been changed or misrepresented. ShoCard's technology is optimized for the enterprise with ShoBadge. ShoCard allows users and enterprises to establish their identities with one another in a secure, verified way so that any transaction–whether it's to login, share personal information, or complete a financial transaction–can be accomplished quickly, seamlessly and with peace of mind. Creating a ShoCard ID can be done either through our App, or a company or entity can build in their technology into their existing Apps via their SDK (Software Development Kit). Some unique and secure authentication and fraud prevention solutions include: • **Credit card transactions —** verify individual's identity & authority to use the card (an improvement over the existing 3D Secure protocol). • **Financial accounts** — verify identity and account ownership without compromising privacy (biggest driver of identity theft), e.g. anti-phishing process, online banking security, no-password-login. • **Call Center** — Allow Customer Care groups to authenticate users in seconds over the phone. No more long series of questions to ask the user. • **Everyday authentication & authorization** — register for and log into websites, membership/ID, stores, institutions, signing authority with delegation, more • **Air Travel Identity Management** — Allow users to register once and travel through different airports with simple facial recognition. • **Enterprise Single Sign On** — multi-factor authentication using SAML.

ID Solutions

General Overview

How does their ID Solution(s) Work? (Continued...)

Estonian ID

As of July 2018, tokens for electronic documents bearing electronic identity of Estonian residents are plastic cards (ID card, Digi ID, e-Residency card, residence permit card) and mobile phone SIM cards (Mobile ID).

To give electronic signatures, ID cards are actively used with the government-sanctioned open-source software called DigiDoc.

Estonia uses a national PKI, meaning that the state undertakes to assure the existence and functioning of the public key infrastructure. Although a large part of the services related to the PKI are purchased from the private sector (e.g. certificate issuance, certificate validity confirmation, distribution of the public key); as well as preparing the key generation environment (e.g. chip on carriers of ID card type, SIM) and personalising the documents (carriers of ID card type), the most important aspects related to the PKI are still handled by the state.

The Estonian ID card serves as the digital access to all secure e-Services offered in Estonia.

ID Solutions

General Overview

Unique Differentiators for each Solution:	
Civic	Reusable verified identity is the core of Civic's Secure ID Platform, which allows people to safely, securely, and selectively share verified credentials with trusted identity requesters. An attestation is effectively a signature on a blockchain that enables users to share their personal information, the verification of previously audited personal information, or both, giving users full control over their data and identity, while ensuring data integrity for reuse. Requesters reward Validators for their initial verification services every time they request and accept verified user information. Identity.com is the decentralized, open source identity ecosystem that Civic is leading, which will be governed by smart contracts and applications of game theory. The ecosystem, which will be open-sourced by 2019, opens up access to on-demand, secure identity verification services, connecting users, identity requesters, and identity validators around the world.
uPort	uPort's solutions are designed to empower users and developers with a self sovereign identity platform which is compliant with regulations (i.e. GDPR), highly performant (maximizing off chain operations) and easy to use. Leveraging the power of Ethereum, uPort is blockchain agnostic and can run on public as well as private chains. The solutions are built leveraging open standards that the uPort team has been actively driving for several years. uPort is the only identity provider on Ethereum that enables the creation and utilization of DID-spec compliant DIDs. uPort differs from the proposed ERC 725 standard in the sense that uPort enables privacy preservation via off-chain transactions, whereas ERC 725 is based around on-chain attestations. Additionally, compared to other Ethereum-based ID solutions, uPort identity creation is free of charge and does not require any on-chain transaction. uPort also supports Ethereum transaction signing and arbitrary data signing compared to other self-sovereign identity solutions.
Sovrin	The Sovrin Network is designed with privacy by design on a global scale through the use of pairwise pseudonymous identifiers, peer-to-peer private agents, and selective disclosure of personal data using zero-knowledge proof cryptography. Simply put, when an identity holder decides to share a verifiable credential with a verifying entity using the Sovrin Network, they could create a proof containing only the specific information that was requested using a combination of elements from any of their verifiable credentials in their digital wallet. They then share the unique proof created for that specific relationship directly between their agent and the verifier's agent. This gives identity holders control over what specific data they allow each specific validating agent to see and for how long. Each party in the identity sharing relationship may use the agent of their choice that operates on the Sovrin Network.

ID Solutions

General Overview

Unique Differentiators for each Solution: (Continued...)

ShoCard	• ShoCard Is Blockchain Agnostic • With ShoCard, all of user’s PII data is always on their device with digital signatures of one-way hashes of their data on the blockchain and any third party can attest to the validity of that data creating a web-of-trust. Furthermore, third parties can attest attributes beyond identity associated with an individual such as their reputation, credit-score and others. Users can then decide with whom they share that data with and which pieces of data they share. Receivers can independently validate the authenticity of the user claims about their identity or attributes. • ShoCard has a patent pending for recovery of a user’s identity without a central server being in control of that data or aware of its content. Users can automatically create a multi-factor dynamic password to encrypt their data and retrieve it given those factors. This allows for recovery of their private-key and other PII without ever exposing that data to a central service. • Scalable: as public blockchains are inherently not scalable, the architecture of ShoCard is highly-scalable. ShoCard has created a solution that uses the public blockchains, but with scale. Their system can write five million user records on a publicly verifiable blockchain in 30 minutes. • Their Product Is Patented: » patent #9722790 on August 1, 2017 with priority date of May 5, 2015 » patent #9876646 on Jan 23, 2018 with priority date of May 5, 2015 » patent #10007913 on Jun 26, 2018 with priority date of May 5, 2015 » patent #10007826 on Jun 26, 2018 with priority date of Mar 7, 2017
Estonian ID	ID-card and Mobile-ID are state recognized eID solutions, widely used in both public and private sectors. eID solutions are issued and promoted in close public-private partnership.

ID Solutions

General Overview

Is their solution in production? If not, when do they expect it to be?	
Civic	Civic's Secure ID Platform (SIP) is live with over 130 partners using Civic's blockchain-powered identity verification services for various use cases. Partners include Anhuesher-Busch InBev for age verification, Brave for Know Your Customer (KYC), Rivetz and Telefonica to create a hardware rein enforced app that will be available to the Telefonica network, and wikiHow for secure login. Additionally, Civic recently launched Civic App Connect, which enables any Android or iOS app or any website to leverage the SIP to authenticate and register users, without ever needing them to provide a username or password. Civic also launched ID Codes, which enables anyone to securely and independently verify an advisory, business, or investment relationship. Identity.com is also live, with the first smart contracts and libraries being put in production at the end of Q3 2018. As more toolkits become available, additional Validators, Requesters and Credential Wallets for users will be able to join and participate in the ecosystem.
uPort	Yes, uPort is live on all Ethereum public networks. uPort app is readily available from the Apple App Store and on Google Play. uPort is currently used in production as well as in pilots by several cities, governmental bodies, educational institutions, healthcare insurances, and public infrastructure providers. Solutions leveraging uPort are being actively built for businesses and governments around the world by a network of global partners.
Sovrin	The Sovrin Network was officially launched in September 2017. Having made a significant network update in October 2018, the Sovrin Network is live and available for wide-spread use and adoption.
ShoCard	ShoCard was established in February of 2015 and their products have been in production for over two years.
Estonian ID	Yes, it has been live for 10 years

ID Solutions

General Overview

Was the Solution built in-house?	
Civic	Yes
uPort	Yes
Sovrin	Evernym donated the initial source code for the Sovrin Network. The Sovrin Foundation is tasked with growing and administering the Sovrin Network.
ShoCard	Evernym donated the initial source code for the Sovrin Network. The Sovrin Foundation is tasked with growing and administering the Sovrin Network.
Estonian ID	The solution was developed in tight cooperation between the public and private sector organizations. Roles of each stakeholder: • Ministry of the Interior: drafting legislation that determines the types and requirements for the electronic identity documents; • Police and Border Guard Board: issuing personal (electronic) identity documents enabling secure electronic authentication and electronic signing (ID card or another smart cards). • Ministry of Economic Affairs and Communications: determines the quality and reliability requirements of PKI services; • Information System Authority (RIA): development of software applications, necessary for using the PKI (ID card middleware including drivers, utility and client software). Estonian leading ICT players were involved in the development of eID components and infrastructure.

ID Solutions

General Overview

Do They Define Their Solution as a self sovereign ID? What are their positions on Self Sovereign ID's (upsides/downsides)?	
Civic	Yes. Civic's mission is to provide every person on Earth with a digital identity that they can use to interact privately and securely with the world. Civic's ecosystem is designed to incentivize participation by trustworthy "Validators," who may include financial institutions, government entities, and utility companies, among others. Validators will be able to verify the identity of an individual or business, known as a "User," and 'stamp' or record this approval on the blockchain in the form of an attestation. Parties known as "Requesters" who are seeking to verify the same information about a given User, and who may include other Validators, would no longer need to independently verify that information and could instead leverage the work already performed by trusted Validators. The Civic app is the digital identity wallet, which contains claims and attestations, along with a user-driven permission to share data with trusted parties in the Identity.com Marketplace The Identity.com ecosystem is intended to ensure that users remain in complete control of their personal information, by requiring the user's consent before an identity verification transaction can be completed.
uPort	Yes, they define their solution as being one of a self-sovereign identity provider. They believe that self-sovereign / user-centric identity is the natural and logical next evolution of identity, and that blockchain enables it for the first time. Furthermore, they maintain that Self-sovereign identity enables us to solve many of the challenges of the current identity landscape around identity ownership, data ownership, reputation fragmentation, password management, and centralized storage. They believe self-sovereign identity requires secure architecture, flexible infrastructure, open standards, powerful functionalities, and a developer ecosystem, and attempt to focus on these main topics.
Sovrin	Yes. The Sovrin Network is a self-sovereign identity solution and the Sovrin Foundation is a strong proponent of SSI. Identity on the Sovirn Network are completely owned, controlled, and managed by the individual or organization.

Do They Define Their Solution as a self sovereign ID? What are their positions on Self Sovereign ID's (upsides/downsides)? (Continued...)

ShoCard	Yes, they are proponents for self sovereign ID's, allowing users to own their own identity, with the underlying BYOID philosophy (which stands for "Bring Your Own Identity," which means a consumer or employee keeps all of their PII within their own devices, rather than surrendering that data and trusting it to companies and organizations. BYOID, verified using blockchain as an immutable ledger, allows users to control what personal information is shared and with whom. They further feel that BYOID is valuable to industries serving consumers because the user is able to take back control of the data they choose to share with the organization. Instead of entrusting a company to protect their PII, a consumer knows their data is safe on their own device. They feel that adopting a technology that emphasizes data security and addresses the concerns of their users will become a key differentiator as data becomes increasingly vulnerable. The platform can also be integrated into an existing, consumer-facing system using a software development kit (SDK). For example, an airline can integrate ShoCard's blockchain-based IMS into their app to allow travelers to bypass waiting lines at the counter and gate at walking speed.
Estonian ID	Yes, the user of Estonian eID plays the central role in the administration of identity. However, people that use the Estonian eID rely on the state and its continuity in providing the secured infrastructure. Estonian eID scheme has a proven track record and high usage rate, making it a convenient and secure solution.

Self Sovereign ID's

Allowing users to own their own identity, with the underlying BYOID philosophy

ID Solutions

General Overview

Is the Solution Compliant with GDPR?	
Civic	Yes, Civic is developed to provide privacy by design.
uPort	Yes. uPort indicated that by design, due to the fact that they are a self-sovereign identity system, a user has to explicitly provide consent to selective disclose his or her data, making them compliant with GDPR. With uPort's new architecture, it is also guaranteed that no personally identifiable information linking back to the user is written on-chain which is critical to guarantee the right to be forgotten to the users, one of the cornerstones of GDPR.
Sovrin	Yes. No personally identifiable information OR credentials exist on the ledger. Sovrin is built with privacy by design from the ground up. For more information, see: https://medium.com/evernym/is-self-sovereign-identity-ssi-the-ultimate-gdpr-compliance-tool-9d8110752f89
ShoCard	Yes, ShoCard claims that their turnkey blockchain-based IM platform gives users control over their data and helps company's move toward GDPR compliance by allowing users to: • Authenticate users without storing their PII data • Reduce requests to access, erase, and correct user data • Obtain definitive proof of consent for permission-based User data • Remove the liability of maintaining user authentication codes with service-providers • Allow users to delete their identity and any encrypted data associated with it
Estonian ID	Yes

ID Solutions

Mechanics & Specifics

Do They Self-Define their Solution as a Blockchain ID?

Civic	Yes
uPort	Yes
Sovrin	Yes
ShoCard	Yes
Estonian ID	No answer provided

What About Their Solution Suggests it is a Blockchain ID?

Civic	Civic relies on attestations, or a 'stamp' of approval on the blockchain, to prove that a user's identity has been validated by a trusted third party. Initially, the Civic App captures the user's personal information locally, which is then validated by a trusted party. Once the user's information is validated, the attestations to this validation process are written on the blockchain, the original personal information is only stored on the user's mobile device in encrypted form. The user can use these attestations to prove the authenticity of their personal information to parties requesting it.
uPort	uPort identities are rooted in Ethereum, and their system could not function without the Blockchain or a trusted, decentralized source of truth.
Sovrin	Sovrin uses a distributed public ledger as an anchor for the public decentralized identifiers (DIDs) This allows a verifier to determine who issued the credential that is presented to them, what combination of information it should contain (the schema), and if it has been tampered with or revoked. With this information listed on the public ledger, identity holders get privacy, security, and control of their data while the verifier can trust the verifiable credential they are presented with.
ShoCard	Data stored on the blockchain is immutable and hence cannot be hacked, modified or deleted, and no PII is ever stored on the blockchain. Only digital signatures of one-way hashes of data are stored on the blockchain. Information exchanged using the blockchain is incapable of becoming compromised, making ShoCard the most secure identity management platform.
Estonian ID	All log entries are linked cryptographically to each other (Sequential Log), a security logger that guarantees the credibility of the validation service. Each log entry is based on mathematical methods from the previous logical record, and therefore nobody has the ability to hack or change it.

ID Solutions

Mechanics & Specifics

How are the Private Keys Stored?

Civic	The Civic App manages and stores the private keys locally on the user's mobile device. Information is also encrypted and backed up on the Cloud connected to the mobile device, if the user chooses. If the app is deleted, then the keys are lost. A new identity is created if the user downloads the Civic App again and chooses not to restore from an existing backup.
uPort	They are stored locally on the user's device.
Sovrin	Identity holders store their private keys in the agent (digital wallet) of their choice that is controlled by the individual. Keys are pairwise and pseudonymous on Sovrin and shared agent to agent, or peer to peer, so only agents in that relationship may access the data.
ShoCard	The public/private keys are encrypted and stored onto the users phone. When available, they are stored on a separate secure hardware such as the TPM. One of the most important aspects of any identity management is protecting the user from identity theft where another user is able to recover one's ID. ShoCard provides such recovery mechanism with a patent-pending multi-factor, split-key encryption mechanism without any server holding the data being aware of its content.
Estonian ID	On the card/chip along with an application.

What is the Recovery Mechanism?

Civic	Civic's securely encrypted backups allow the user to retain access to their identity if they delete and reinstall Civic and even across devices. Since every person's identity is unique, users will not be able to set up another new Civic Secure ID without resetting the old ID.
uPort	Seed recovery and Shamir Secret Sharing-based social recovery.
Sovrin	Sovrin has a DKMS involving multiple agents and backup, social recovery, etc.
ShoCard	ShoCard claims a proprietary and patent-pending recovery mechanism. At a high-level, they designed their Account Recovery process so that service providers can maintain private key recovery information, but not read or hijack it. Since passwords can be hacked or forgotten, ShoCard doesn't require a password on top of other factors for recovery. This is a critical aspect of their design, because if the service provider was able to provide a forgot- password mechanism to reset a password, it would also mean that they had the ability to maliciously reset the password on a user's behalf and access their data. Instead, they obfuscate the recoverable information in a way that only the user is able to retrieve it. In order to recover a private key, ShoCard requires the user to have access to multiple assets. Typically, this is their phone number, email, biometrics, an ID, a scanned document, or a phrase. ShoCard uses a split-key mechanism requiring at least three factors for recovery, but no password necessary. Once the user has proven access to these assets, the service provider retrieves the fourth factor, which is a unique Salt (a long unique value). This gives the users mobile device, and only their device, the information it needs to retrieve a private key.
Estonian ID	No answer provided

ID Solutions

Mechanics & Specifics

What is the weakest link in the system and how do the Solution providers mitigate it?	
Civic	There has been an influx of negative media around blockchain, starting with the Silk Road and currently with failing cryptocurrencies and fraudulent ICOs. According to CNBC, over 800 cryptocurrency projects are worthless. One of the biggest problems right now, is that it will take time to build trust and reliance on blockchain technologies and building adoption.
uPort	Assuming the receipt of attestations is their weakest link, uPort are able to prove that an attestation provider is really who they say they are due to the fact that they have some public identifying info which is stored on the Ethereum blockchain, which states that the specific ID in questions pertains to that specific entity. The same goes for attestation receivers. Additionally, uPort supports a new DID method (did:https) which allows attestation providers to store their DID document under a well-known URL under their domain. This will increase the trustworthiness of the provided attestations.
Sovrin	The Sovrin Network is a new public service utility enabling the creation and the use of self-sovereign identity on the Internet. The Sovrin Network will only grow when there is wide-spread adoption of this new way of managing data. Therefore, Sovrin is an open source project, housed in Hyperledger Indy, a distributed ledger purpose-built for decentralized identity. Developers that use the tools and libraries from Hyperledger Indy can create identity solutions that are interoperable across jurisdictions, uses, and agencies. The solutions created out of this community will drive the overall use and growth of the Sovrin Network.
ShoCard	Know Your Customer (KYC) Using ShoCard Regulatory requirements for KYC and AML are top priorities for financial institutions and perhaps one of the more challenging and expensive processes necessary for regulatory compliance and fraud prevention. Customers required to gather KYC information often find the process laborious and repetitive. Furthermore, existing KYC methods are limited in what they can offer beyond a single-time verification of an identity. ShoCard's patented solution streamlines user data collection processes that meet some of the basic requirements of KYC. ShoCard goes beyond regulatory requirements by offering biometric verification using facial recognition and creating an immutable identity, which serves to streamline future customer activities (e.g., registration, login without usernames and passwords,secure and auditable call-center authentication, transaction authorization, certified attribution of user credentials, etc.).
Estonian ID	If the attackers get a hold of your mobile device, they might have a chance to implement a brute-force attack and run through all possible PIN combinations. If it happens, the server shall lock the certificate and prevent the attack.

ID Solutions

Mechanics & Specifics

How are the Solution Providers working with interoperability between identities?

Civic	Civic is working to ensure that the technology is chain agnostic and interoperable, Additionally, the Civic Secure ID Platform and Identity.com is designed to be compatible with future decentralized identity standard, including W3C standards, like Verifiable Credentials, and DIDs.
uPort	In terms of identities between blockchains, uPort are founding members of the Decentralized Identity Foundation which is focused on interoperability between decentralized identity systems. DIF has defined specs for Identity Hubs and Universal Resolvers. Additionally, uPort is an active member in W3C Verifiable Credentials Working Group and W3C Credentials Community Group, working on Verifiable Credentials and Decentralized Identifiers (DID).
Sovrin	The Sovrin Network is based on the creation of relationships. Identity holders may collect a verifiable credential from any issuer of their choice and share them with any verifier they please, who then trust the credential based on the information held in the credential compared to the claim definition. Interoperability is key in these relationships.
ShoCard	ShoCard employs open standards. Based on their viewpoint that with such a large world population, there will not be only one identity provider so the companies that will succeed need to be able to interoperate. ShoCard can integrate with other security and identity solutions via SAML, OAuth, OpenID Connect and others.
Estonian ID	National scheme of eID in Estonia has supportive tokens that can be used in parallel or provide similar outcome if one shall be attacked/suspended.

ID Solutions

Mechanics & Specifics

How are the participants incentivized to engage in attribute attestation?

Civic	Civic is spearheading the development of Identity.com, which creates incentives based on the economics of the ecosystem. Identity.com is powered by CVC tokens and is designed to incentivize good behavior in the ecosystem. Most importantly, this will incentivize participation by trustworthy identity verification providers or 'Validators.' These Validators will be able to verify the identity of an individual or business user and record this approval on the blockchain in the form of an attestation. Through smart contracts, Validators will be able to offer identity verification services and generate revenue every time an attestation is created or used. At the time of this report, Civic is a Requester and Validator in the Identity.com ecosystem.
uPort	They currently are not; however, incentivization mechanisms could easily be built on top of uPort due to the fact that we are Ethereum based.
Sovrin	Using the Sovrin Token. This is discussed in detail in section 6 of our white paper from January 2018
ShoCard	ShoCard's business model is working with B2B2C and B2B so there's less reliance on incentivizing participants attribute attestations which are usually done by trusted authorities. The incentives are instead removal of business friction, cost and easier user-experience.
Estonian ID	No answer provided

How are participants incented to maintain the rails for the exchange of identity attributes and how are individual transactions between parties paid for / monetized?	
Civic	Identity.com is powered by CVC tokens. This will allow ecosystem participants to transact in identity verification services while ensuring network integrity. Civic's Token Behavior Model, predicated on game theory and smart contracts, aims to incentivize appropriate types of network behavior that optimize accuracy and efficiency without using oracles that violate user privacy. The Model uses a staking mechanism to ensure compliance and should assure the actors' good behavior.
uPort	For on-chain uPort attestations, the Ethereum network handles the exchange of identity attributes. For the managing and transacting of privacy-preserving off-chain JWT attestations, uPort maintains the rails for the exchange of identity attributes. Off-chain attestation transacting is free, so there are no fees that need to be paid. uPort does not monetize the maintenance of these rails.
Sovrin	Using the Sovrin Token. This is discussed in detail in section 6 of our white paper from January 2018
ShoCard	ShoCard's business model is working with B2B2C and B2B so there's less reliance on incentivizing participants attribute attestations which are usually done by trusted authorities.
Estonian ID	Individuals pay for Mobile-ID and eID based on the state fees. In case of eID it's a one-time fee. In case of Mobile-ID it's monthly service fee paid for telcos

Is there a liability framework in place for the use of the solution? Which party would be liable in the event of an issue such as when a piece of identity data is bad? Who is responsible for bearing any costs related to resulting errors?

Civic	The Identity.com staking mechanism will require that identity 'Validators' hold a defined minimum amount of CVC tokens to be an active player in the identity ecosystem. This is intended to kickstart trust in the network, and Validators accumulate a reputation, based on their identity verification accuracy, as they participate in the ecosystem. The network will provide adjusted incentives, like decreased stake, for Validators to increase or maintain identity accuracy at a particular confidence level, rather than maintaining reputation alone. Validators in the ecosystem own the attestations they have created, so they are liable for the validity of those attestations. Requesters can challenge Validators and their attestations both within the ecosystem and outside, if needed, as their identity is known to each other.
uPort	The issuer of that piece of data would be at fault if the piece of data was bad. The determination of who is responsible for bearing those costs would be left up to the affected parties.
Sovrin	Not that is maintained by Sovrin. Private insurance is possible. See Section 6 of the white paper from January 2018.
ShoCard	ShoCard's authentication model follows the real-world models. For example, if a user has a certification from a bank stating that they opened an account and hence completed KYC and that they may own a particular account only attests to what that bank has done. The bank doesn't make any guarantees as to the quality of the user – just that the user was able to provide the necessary credentials to have the bank open an account in their name. With ShoCard's certification, the bank isn't liable for validation of the user, but only a certification of what they have done with the user's identity. This is inline with the way identification is used today in the real-world.
Estonian ID	In case of electronic use, the service is regulated by the eIDAS, setting forth requirements to Certification Service Providers and regulating their operation and supervision. CSP must carry out an annual audit to ensure organization and system reliability. CSP-s must also have liability insurance tosafeguard against compensating faults made while providing the service.

ID Solutions

Mechanics & Specifics

How, if at all, does the system enable users to minimize their sharing of attributes?	
Civic	Civic's approach to identity verification allows users to present previously created attestations and verified credentials that are needed to conduct business with an identity Requester, without the need to share additional, unnecessary personal information. For example, when you go to a bar, a bouncer usually looks at your physical ID, which discloses your address, birthdate, full name, and other unnecessary information. With Civic, a user could scan a QR code to prove that they're over 21 without sharing excess information. Initially, the Civic App helps the user capture their personal information through an ID document, which is then validated by a trusted Identity.com Validator. Once validated, the attestation that this data is valid is written on the blockchain. Personal information elements can be attested individually, separating out information such as address, birth date, name, etc. This allows Civic users to provide the minimum amount of information needed to prove that they meet a Requester's criteria.
uPort	uPort allows users to selectively disclose only those attributes which are required by the requesting party.
Sovrin	Sovrin uses Zero-Knowledge Proofs (ZKP) to minimize disclosure. This allows an identity holder to prove any combination information using any of their verifiable credentials, without revealing the actual piece of information.

How, if at all, does the system enable users to minimize their sharing of attributes? (Continued...)

ShoCard	In order to protect user privacy, the blockchain should only be used for proof of work and verification of assertions made by a user. It should not be used as a general store of identity information – encrypted or otherwise. The reason for this is that any personally identifiable information (PII) on a public blockchain can be potentially compromised by hackers. Even encrypted data is subject to such hacking. Blockchain records are immutable and once written, cannot be deleted or modified. Furthermore, it is important for any blockchain-enabled IM to take measure so that simple hashes are not used for obfuscating PII data. Through brute force, such hash data can be discovered and allow hackers to piece different components of user data together. To avoid such hacks, the ShoCard system uses the blockchain only to verify data, not to store it. The blockchain serves as a repository of certifications. An individual can self-certify their identity and third parties can certify an individual's identity as well. Users can also share only pieces of their data, instead of their identity in its entirety. While many aspects of their identity may have been certified, they may need to only share their facial image and age in order to prove that they are over the age of 21. In such a case, they can specifically share only those 2 attributes and not the rest of their identity.
Estonian ID	No answer provided

ID Solutions

Mechanics & Specifics

How are the Providers Ensuring User Privacy?

Civic	With Civic, personal information is only stored on the user's mobile device, using best-in-class encryption and biometric security. Combined with cryptographic methods, the Civic App is well equipped to deal with modern privacy and cyber security standards. Users are in control of every action performed in the Secure Identity Ecosystem, so they are both aware and are an active participant in their personal information presentation or verification processes. Additionally, Civic's attestation model allows users to share only the minimum required attested personal information, ensuring users maintains control of their personal information. Most importantly, Civic's Secure ID Platform reduces the risks of system wide failures, by eliminating the need for centralized storage of personal data. If one user gets hacked, the entire system is not compromised.
uPort	Off-chain JWT-based attestations and application-specific accounts. The user will also be able to selectively disclose only the data that is needed.
Sovrin	The privacy of each identity holder is provided through the Sovrin Network's use of non-correlation architecture in the decentralized identifier (DID) exchange (including pairwise pseudonymous DIDs) and Zero-Knowledge Proof cryptography in credential presentment.
ShoCard	ShoCard's approach to identity is different than existing solutions in that the user owns and carries their own data within their mobile app and is the sole person who decides with whom to share it with and which pieces of identification to share. The blockchain is then used to validate that information and confirm other third parties who have definitively certified the identity of the user. There is no privately held central location that holds user's private information and pieces of a user's identification do not need to be spread in other services in order to authenticate or prove ownership of an account. A user's voluntary sharing of their data with a third-party is their explicit permission for data sharing and the data is shared only with the party they specify.
Estonian ID	The Government contributes actively to proper information system development, its deployment and a systematic review within the Public Information Act. The system processes are maintained by the Estonian Information System Authority, and supported by a meta-information registry, called RIHA or the Administration System of the State Information System

ID Solutions

Mechanics & Specifics

How are claims made and verified? What data is required to be shared and made available? Also, what interactions must be made available i.e. communication with a network node?	
Civic	The Civic App enables users to share and manage their attestations and verified credentials. Once a user's personal information is validated, the attestations are written to the blockchain. A user can present attested information to a Requester to verify the user's identity. Requestors can request a user's information through custom QR codes that the user scans with the Civic App or through Civic's App to App native iOS and Android integration. Once a user has unlocked the Civic App with their biometrics, the user scans the QR code (on desktop), reviews exactly which information is being requested, and chooses whether to approve or deny the request. This process currently leverages a browser/app-side library, the Requester's server-side Civic Secure ID Platform library and the Civic server to manage the end to end handshake. In the future, self-hosted options will become available on Identity.com
uPort	Any arbitrary data is written, signed by the attestor, and then sent to the receiving party. The receiving party then must accept the receipt of the attestation. The data required to be shared is the cryptographic signature of both the attestor and the receiver. For on-chain attestations, users must be connected to Ethereum. For off-chain attestations, communication is done via HTTPS, and the Ethereum chain only needs to be interacted with to prove the identity of the parties involved in the transaction.
Sovrin	Claims are a combination of a schema and a claim definition. Claims are made by an entity issuing claims (based off a schema and definition) to another entity. The issuing entity can set the schema and definition themselves by writing to the ledger or reference existing schemas. Claims are verified when the claim is presented to an interested party by verifying the public key of the issuer (signature) on the credential. Someone can trust a claim only to the degree that they trust the issuer of the claim.

ID Solutions

Mechanics & Specifics

How are claims made and verified? What data is required to be shared and made available? Also, what interactions must be made available i.e. communication with a network node? (Continued...)	
ShoCard	User's can share their data with a Verifier through a secure exchange. The Verifier presents the user with a challenge-string and a request. The ShoCard User then responds to that request with the information it has and pointers to the certifications of her data on the blockchain. This response is signed with the user's private-key and encrypted with the Verifier's public key. Upon receipt, the Verifier will decrypt the message with its private-key, verify that the message was properly signed using the public key passed to it. It then verifies that the self-certifications of the user on the blockchain can be verified using the same public-key. This attests to the relationship between the user's App and the blockchain records. It also verifies any of the third-party certifications the user has passed it to verify that the user was authenticated by some authority that it trusts. That authority may even be the Verifier itself. The user decides which certificaitons and data pieces to share. This is usually confirmed by the user by using a PIN, TouchID, FaceID or equivalent. For high value transactions, a verifier may even ask the user to use Facial comparison that it performs using their self-certified selfie that has been previously certified.
Estonian ID	Privacy of all Citizen data, and its use, is guarded by the Data Protection Inspectorate. If misuse of information is suspected, the citizen can claim.

ID Solutions

Mechanics & Specifics

How can the Provider's ID be used across various networks and applications?	
Civic	Civic's Secure ID Platform (SIP) enables reusable identity verification. Once a Civic user has their identity validated, they are able to share their verified credentials with any Requester in the Identity.com ecosystem that accepts those credentials. Wherever users see the Connect with Civic button, both on desktop or mobile, they can use their Civic Secure ID to authenticate.
uPort	uPort is network and application agnostic; their developer tools allow anyone and any application to integrate uPort. uPort is deployed on all public Ethereum networks, and provides the infrastructure for deploying it on private networks.
Sovrin	Sovrin based solutions can integrate into other networks or applications with the Indy SDK.
ShoCard	**ShoCard** allows users and enterprises to establish their identities with one another in a secure way for any transaction–whether it's to login, share personal information, or complete a financial transaction. Creating a ShoCard ID can be done either through their App, or a company or entity can build in ShoCard's technology into their existing Apps via ShoCard's SDK (Software Development Kit). **ShoBadge** is their enterprise level identity authentication solution, which uses mobile devices combined with disruptive, secure blockchain technology as the basis for trusted sharing. It allows employees, contractors, vendors... to login securely into work applications (i.e. email apps, marketing apps, HR, Operation... apps) without a username and password and also may be used by employees to access physical buildings. ShoBadge uses 6 Factor Authentication that includes biometrics, geofencing, etc. The ShoBadge system leverages the blockchain, instead of a database, as an independent source of truth for identity certifications and because the blockchain is immutable, it cannot behacked, modified or deleted. Note that user data is never written on the blockchain by the ShoBadge system, instead what's written are identity certifications that are used to independently verify a user. By leveraging hashes, salts, and digital signatures, the ShoBadge system ensures that identity certifications written onto the blockchain cannot be reverse engineered into their original data.
Estonian ID	No answer provided

ID Solutions

Mechanics & Specifics

How are their systems Governed? How are ID’s issued or created and stored?	
Civic	When Civic set out to build Identity.com, a decentralized identity ecosystem, it chose not to rely on centralized decision makers or oracles that can easily become single points of failure. Instead, Civic focused on building a set of rules that would enable every Identity.com participant to act with each others’ best interest in mind. The Token Behavior Model Civic designed focuses on the mandatory goal alignment between ecosystem participants, including Users, Validators, and Requestors. It creates a set of rewards and punishments that places malicious actors in a zero-sum game that quickly leads to exponential losses. To adequately incentivize the actors, Civic approached staking from a completely different angle, compared to traditional crypto approaches – using it not to generate revenue for the entity staking, but rewarding them with less stake as they increase their reputation in the network.
uPort	The uPort team guides and performs the development of the uPort platform, but the system is able to be run and be governed in a decentralized manner; there is no group or organization that governs the system. uPort was designed as an open platform. If additional governance structures are required for issuing attestations, application providers could implement these structures on top of uPort. Attestations and identities which were issued outside of that governance structure won’t be affected.
Sovrin	The Sovrin Trust Framework is the legal foundation for the Sovrin Network to function as a global public utility for self-sovereign identity and was developed through a community-driven process led by the Sovrin Trust Framework Working Group, agreed to by the Stewards, and was approved by the Sovrin Foundation Board of Trustees. This governance document serves to define the business, legal, and technical terms that all members of the Sovrin Community agree to follow. The Trust Framework gives guidance so that everyone may reap the rewards of the Sovrin Network.

How are their systems Governed? How are ID’s issued or created and stored? (Continued...)	
ShoCard	ID’s are created by the user who downloads the ShoCard app, then uploads their ID cards and creates a private PIN, Touch ID and takes a selfie to prove that they are the person in charge of their identity. Along with this process, a unique electorinc-ID, referred to as ShoCardID along with a unique pair of private-key/public-key are created on the phone. The ShoCardID is equivalent to a blockchain address while the private-key is generated on the phone itself and is never shared with any other party or service. Through the ShoCard application, a person’s identity and data are stored on their device and they are the only person who determines which ID details are shared. ShoCard uses the blockchain as a public, immutable ledger that allows third parties to validate that the original data or certification has not been changed or misrepresented. Enterprises may also utilize the ShoBadge SDK/APIs to verify their employees and to eliminate username and passwords and create a seamless login experience for their employees when they sign onto their work applications or enter into their job site (without use of fobs or physical badges).
Estonian ID	Answered previously

ID Solutions

Additional Considerations

ID Solutions

Additional Considerations

How will network effects be built out? Is there a particular use case to be used as a wedge to build usage momentum?	
Civic	In addition to product and use updates to the Secure ID Platoform, Civic is continuing to build out Identity.com, a decentralized, open source ecosystem that reduces the overall costs and burden of identity verification, from age verification to Know Your Customer (KYC) checks. The ecosystem will simultaneously enhance privacy and security, thereby improving the user experience and disrupting the current market for such services. The more "doors" the Civic "key" is able to open, the more attractive it will be for both users and new partners. As the identity.com ecosystem grows, too, it will be subject to the same market forces, with more Requesters, Users and Validators attracting the attention of their respective counterparts to join and build an ever-growing network that enables access to on-demand, secure, accessible identity verification for everyone. Identity.com and Civic are using the power of the CVC token to seed the initial network effects and will continue to create programs to spur network growth.
uPort	uPort has seen strong traction in very varied use cases ranging from government (e-voting, digital services to citizens...) to public infrastructure (contractor and employee access and authorization to railway sites) as well as issuance of university certificates. The network effect will kick in at full speed once services will start to add themselves to existing uport enabled infrastructure, therefore increasing exponentially the value to the end user. For example, the city of Zug started issuing Zug IDs to its residents last year via uPort, and earlier this year deployed a production system for e-voting. Recently a local partner added a solution which enables residents already equipped with a uPort-enabled Zug ID to unlock and use their biking service in Zug. This proliferation of services will be the key to drive more and more value to end users and will create a stronger incentive for service providers to tap into the network, thereby creating a snowball effect. In addition, uPort would like to build the attestation ecosystem on Ethereum. Their main target audience in that market is developers who want or need an identity solution for their platform or product, whether for accessing a service or preventing sybil attacks and providing proof of individuality. uPort is thus focused on providing these developers with the features they find useful today to achieve network effects in that space.

ID Solutions

Additional Considerations

How will network effects be built out? Is there a particular use case to be used as a wedge to build usage momentum? (Continued...)

Sovrin	The Sovrin Foundation is a member of Hyperledger, a Linux Foundation Project. Sovrin uses Hyperledger Indy, one of the projects under the Hyperledger umbrella. The initial code for Hyperledger Indy was contributed by the Sovrin Foundation. As an open source project, Sovrin has great interest from a variety of developers and organizations. Network effects will be built out partly by our growing community of diverse Stewards who operate the validator nodes that provide consensus to the public ledger.
ShoCard	No answer provided
Estonian ID	No answer provided

ID Solutions

Additional Considerations

Where do the Providers feel the demand for this solution coming from?... what specific problem(s) is their specific solution solving?	
Civic	According to a Wall Street Journal report, over 16 million U.S. consumers had their identities compromised in 2017. According to Javelin Strategy & Research, identity theft cost victims nearly 17 billion in 2017. Our personal information is more valuable and vulnerable than ever, and it has become clear the security and privacy of personal information is an increasing concerns for businesses and consumers alike. The way we share and store personal information is broken. Offering safe and secure identity verification services, Civic helps mitigate consumer protection and data privacy problems by giving users the ability to authorize any sharing of their personal information and to ensure that personal information is kept out of centralized databases , where is vulnerable to hacks. Additionally, a Civic Secure ID is stored locally in a mobile device, protected by biometrics. This means that even if a malicious actor has stolen a social security number, with a Civic Secure ID system in place, it would be impossible to use that number with any Civic partner without physical access to the mobile device and the biometric information that protects that credential. Lastly, according to the World Bank, there are more than one billion people that don't have access to official identification documents, and two billion adults who don't have access to banking. Civic and Identity. com open up access to on-demand, secure identity verification that lowers barriers of entry and enables more users around the world to prove who they are.
uPort	uPort solves the problem of Blockchain for Identity, and Identity for Blockchain; that is, they enable truly self-sovereign identity, something that was made possible for the first time by blockchain technology, and they also provide a platform for blockchain-based dapps to easily do 'identity' and to get users to easily interact with their systems.
Sovrin	For providers of the platform (Sovrin), the demand is coming from businesses wanting to reduce costs and liability related to managing customer data. For market providers (i.e. those building on Sovrin), they are primarily in education, finance, healthcare, air travel, and other high-security industries solving the problem of trust in a digital world.

ID Solutions

Additional Considerations

Where do the Providers feel the demand for this solution coming from?... what specific problem(s) is their specific solution solving? (Continued...)	
ShoCard	Our clients are enterprise service providers who enable their employees, contractors and consumers to perform different actions. The overwhelming demand is to first remove the friction and security vulnerability of username/passwords with an easier to use and more secure interface. Furthermore, they are requiring a new ID paradigm that can expand with their future needs without requiring them to overhaul their identity systems again and again. For financial institutions, creating a shared-identity to optimize KYC and lower fraud as well as provide one common way for users to login to their services, be it on a mobile device, web browser, an ATM, over the counter, or on the phone is a priority. For air travel, the promise of speedy authentication of the 99.9% of travelers while being able to stop the small questionable travelers with high levels of security and reliance on biometrics, yet maintaining user privacy and control is the driving motivation. Manual inspection of validation of user identity during air travel increases the cost for governments, airports, airlines and dilutes the traveler experience.
Estonian ID	Answered previously

ID Solutions

Additional Considerations

Are end consumers asking for this solution? If so, in what capacity/context?	
Civic	Yes, consumers are looking for the greater control and protection for their personal information. Privacy concerns arise whenever personal information is collected, processed, or stored, and storage of personal information has grown on an unprecedented scale. There have been many high-profile hacks in recent years, and people have lost control over their personal data. According to the New York Times, the Equifax breach allowed hackers to steal 147 million people's sensitive personal information. Both businesses and individuals need a convenient solution to control and protect personal information to help people win back control over their identity information. It's time to move away from knowledge-based authentication online and introduce possession based authentication – proving you not only know, but also own the data you present.
uPort	Yes; almost everyone needs identity, regardless of what they are building.
Sovrin	Yes, there are some privacy/crypto enthusiasts and early adopters asking for this solution. But primarily, it is businesses that are asking for it.
ShoCard	During usability testing, many consumers have specifically asked for our service. However, our service requires enterprises to participate in order for users to utilize the full capacity of the distributed identity they have with ShoCard. Ownership of their ID in an obvious form that is easy to use and increased security that eliminates the need to have transactions rejected or fraud taken place using their ID and eliminating the need for usernames and passwords across multiple sites are the key use cases that consumers have referenced.
Estonian ID	No answer provided

ID Solutions

Additional Considerations

What do they see as the biggest hurdle for adoption?

Civic	The blockchain community is proving technology to the world, which largely has no precedent for how blockchain could impact day-to-day lives. Right now, true consumer use cases are limited in availability, and the biggest hurdle for adoption is turning blockchain technology into actionable use cases that are easy to understand and to engage with for the ordinary consumer.
uPort	People understanding what self-sovereign identity is, and being sophisticated enough to handle it.
Sovrin	Organizations building on Sovrin see the biggest hurdle for adoption being the work to integrate with existing legacy identity systems.
ShoCard	Encouraging early adoption is always a hurdle when launching a new technology - especially one that is trying to crack a problem that has been around for decades. ShoCard is creating a blockchain-based ID management solution to help meet that challenge. Getting users/enterprises to trust that our solutions work and that they are undeniably the most secure and safe way to store and verify a user's identity. Our biggest competition and hurdle is the ever "hated" existing username/password paradigm. No one likes it, but it is the only way things have been done for nearly 4 decades.
Estonian ID	No answer provided

ID Solutions

Additional Considerations

Is their system fully open, permissioned, or private?	
Civic	Civic is a private company, offering identity verification solutions through the Secure ID Platform, while contributing to the development of the Identity.com ecosystem. Identity.com is a decentralized, open source identity ecosystem, which will be open to any company that wants to leverage Identity.com ecosystem and technology. Identity.com will help ecosystem participants, including Users, Requesters, and Validators, eliminate the costs and inefficiencies of identity verification services while improving privacy and security and creating a best-in-class experience for all ecosystem participants. Civic and identity.com operate using best available public chains.
uPort	Fully open; although they support private / permissioned chains as well.
Sovrin	The Sovrin Network is Public - Permissioned. Public means anyone can use the Sovrin ledger to make transactions. Permissioned only relates to who can actually operate the network and run the validator nodes. Consensus is reached by trusted entities called Stewards using a permissioned ledger. Validator nodes do not restrict access to the network.
ShoCard	The solution is blockchain agnostic. It supports both public and permission-based private blockchains. ShoCard states that it is more than a fully integrated App, it is an Identity Management Platform. Some of their clients require a permission-based blockchain which is critical for bringing them onboard.
Estonian ID	No answer provided

ID Solutions

Additional Considerations

What do the Providers believe a blockchain itself should be used for at a transactional level, vs complimentary second layer systems built on top?	
Civic	For both Civic and Identity.com, a blockchain is the underlying layer that enables decentralized operation, I ncluding attestations and smart contracts to help regulate the marketplace.
uPort	Blockchain should be used to anchor identities; the blockchain should be utilized as infrequently as possible, however, due to costs and scalability issues.
Sovrin	The Sovrin ledger is used for a few, very specific purposes. No personally identifying information (PII) is written to the ledger. The Sovrin ledger records public DIDs, revocation accumulators, claim definitions, and schema definitions. Keys, credentials, and other important information is stored in agents controlled by the identity owner. Agents communicate peer-to-peer to transact.
ShoCard	They believe the blockchain is better suited for a complimentary system. They designed the architecture of ShoCard to be highly-scalable. Public blockchains are inherently not scalable. ShoCard has created a solution to use the public blockchains, but with scale. They state that their system can write five million user records on a publicly verifiable blockchain in 30 minutes. In their opinion, using the blockchain for transactional solutions is not feasible and cannot operate with scale and performance.
Estonian ID	No answer provided

ID Solutions

Additional Considerations

How do they plan on scaling their system to address both the transactional volume and operational costs the system would require if used by billions of entities?	
Civic	Civic’s Secure ID Platform (SIP) and Identity.com are built to be agnostic to current technologies and capabilities, so that both are ready to incorporate scaling upgrades of current and future blockchains, as demand increases for the services being provided.
uPort	They plan to address scalability issues by minimizing the number of blockchain transactions a user has to make while interacting with their system. A few examples are their divergence away from their Proxy Contract-based identities, and their utilization of off-chain attestations.
Sovrin	Because more identity transactions in Sovrin occur peer-to-peer, the ledger doesn’t have to be involved except for reads to anchor and verify public DIDs and definitions. The architectural roadmap includes observer nodes for read operations (identity ledgers have many more reads than writes) and key management message families for P2P DID exchange.

ID Solutions

Additional Considerations

How do they plan on scaling their system to address both the transactional volume and operational costs the system would require if used by billions of entities? (Continued...)

ShoCard	Public blockchains are inherently limited in storage and lack scale. Hence, sidechains are used to hold the certification data. Each record is hashed, and those hashes are written to the public blockchain as proof of work every 20 minutes or so. By maintaining the certification data on a dedicated sidechain, it is efficiently distributed to multiple nodes; whereas, the ultimate proof of work still ends up on the public blockchain. The blockchain caches keep a local copy of the blockchain for faster "read" access so that verifications can be managed independently of what happens with a public blockchain. While a public blockchain in the distributed network can be used for verification, the distributed nature of the blockchain and immutability of the records, make any local copy as viable as any other network copy. The ShoCard Blockchain Adaptor abstracts the interface to the blockchain that maintains the proof of work, so the ShoCard Service layer can remain efficient. The Blockchain Adaptor layer allows the rest of the ShoCard system to remain blockchain agnostic. This is an important architectural decision that will pay dividends in the future. Any system that is limited to only one blockchain can become obsolete or lack the ability to scale due to congestion, increase cost of transactions, or obsolescence of the blockchain. For example, due to increased traffic, the Bitcoin blockchain has become increasingly congested. The cost of transactions is now exceeding $.60, and it can take up to 40 hours to confirm a transaction. The same transactions a year ago cost about $.05, and it would be confirmed in roughly 10 minutes. It is unwise to assume that any particular blockchain infrastructure is suitable over the years.Hence, the ShoCard architecture was designed agnostic as it can use multiple blockchains at the same time and adopt new ones in the future. Since records written to the blockchain are immutable, any existing writes are permanently viable, and any future writes can be directed at a different blockchain, including private blockchains for private applications.
Estonian ID	No answer provided

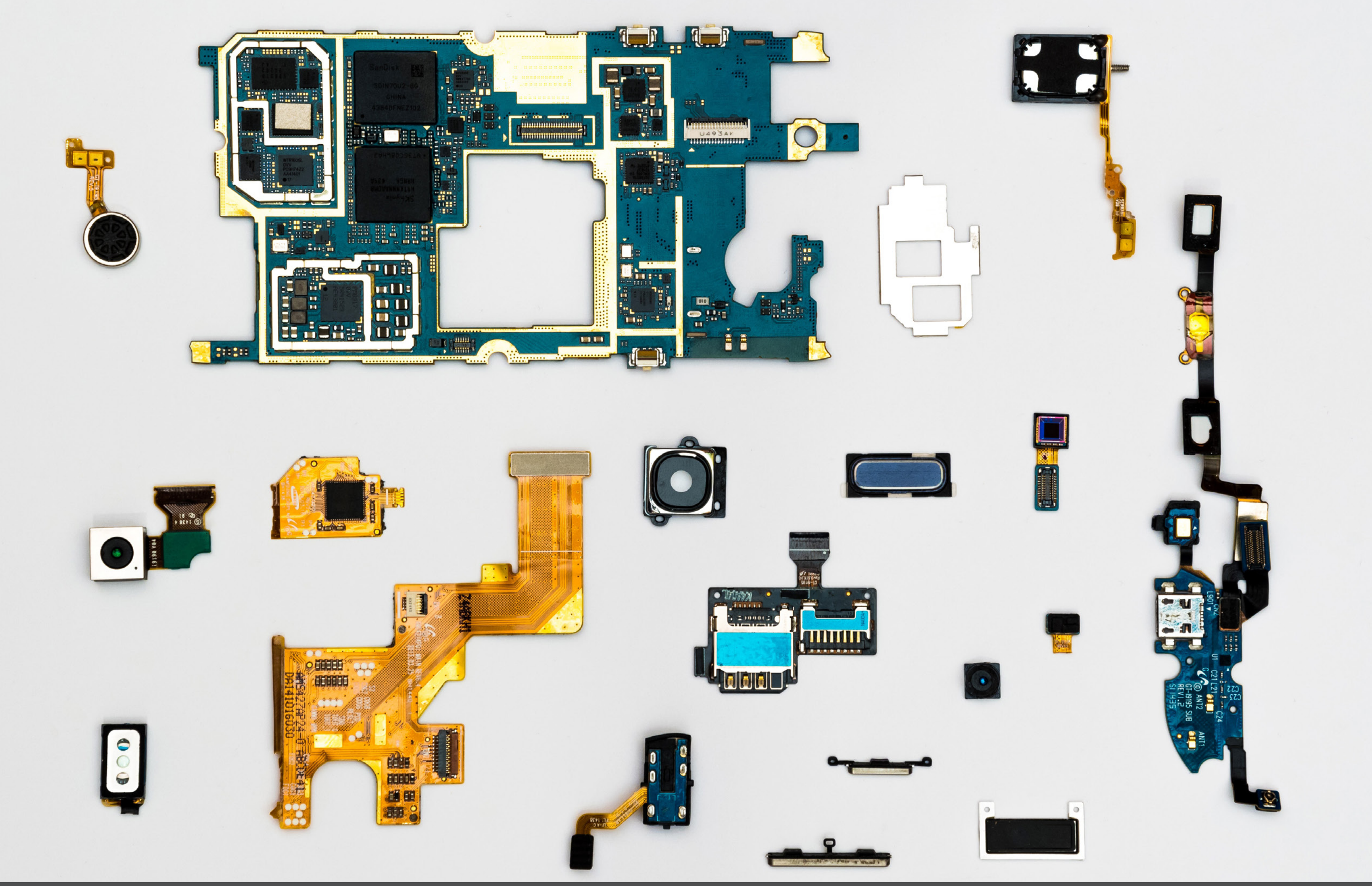
What are the types of ID-related data you believe should/shouldn’t be stored on a blockchain?

Civic	Blockchain offers a compelling solution to the problem of combining accessibility with privacy and security. Blockchain solves the problem of dealing with highly sensitive or classified information in a way that still enforces all the privacy and confidentiality rights that consumers and regulators expect. User data should be on their respective mobile devices, encrypted and protected by biometrics, while attestations that the data has not been tampered with can live on the blockchain for open, transparent verification. The blockchain is also a great way to record identity verification transactions, enabling applications of game theory in marketplace governance.
uPort	Anything that is even remotely sensitive.
Sovrin	No PII data, even hashed, should ever be written to the blockchain. Even pseudonymous identifiers can be correlated which compromises privacy. That is why Sovrin uses unique pairwise pseudonymous identifiers for each relationship.

ID Solutions

Additional Considerations

What are the types of ID-related data you believe should/shouldn’t be stored on a blockchain? (Continued...)	
ShoCard	User data is kept on the user’s device. Our services never receive or store the data. The data on the phone is encrypted and the key stored on a separate hardware component on the phone when available (e.g., the TPM). To decrypt the data, the user must have 1. Physical access to their phone 2. Have PIN or Touch ID or equivalent to decrypt and view the data. The blockchain doesn’t store any of the user’s PII. It only maintains digital signatures of hashes of the data that are signed by the user and third parties. Those signatures cannot be reverse engineered back into the original data. By taking data that once would have been stored in a large database and moving it instead to user devices, the data is decentralized and creates the necessity for the hacker to compromise multiple devices, instead of one, valuable centralized database. The hacker is de-incentivized because it takes too much effort. In order to protect user privacy, the blockchain should only be used for proof of work and verification of assertions made by a user. It should not be used as a general store of identity information – encrypted or otherwise. The reason for this is that any personally identifiable information (PII) on a public blockchain can be potentially compromised by hackers. Even encrypted data is subject to such hacking. Blockchain records are immutable and once written, cannot be deleted or modified. Furthermore, it is important for any blockchain-enabled IM to take measure so that simple hashes are not used for obfuscating PII data. Through brute force, such hash data can be discovered and allow hackers to piece different components of user data together.
Estonian ID	No answer provided



Summary of Findings

Summary of Findings

While the approaches and feature offerings of the surveyed companies all differ, general themes like a clear concern for user privacy, careful consideration of what data gets stored on-chain blockchain-based solutions, scalability plans, and consideration of the EU General Data Protection Regulation are common throughout. All solutions also seem to leverage mobile devices as the primary physical token of their solution, with the exception of the plastic card offerings of the Estonian e-ID platform which stores the key pairs on the physical cards.

The solutions that take a more centralized approach like the Estonian e-ID have already seen large-scale production rollouts and have proven their scalability while some of the newer and more decentralized offerings like Sovrin and uPort which purport greater self-sovereignty are still growing in their utilization or building out their networks as of the time of writing.

Specializations are visible, like a focus on building out an identity service ecosystem with Civic, or large rollouts with multiple form factors and services like the Estonian e-ID, or recurring themes of existing system integrations with ShoCard. Sovrin and uPort have a clear emphasis on things like self-sovereignty and building out solution-agnostic and flexible identity platforms, suggesting these products are all differentiated enough to be focusing on slightly different market segments. The suitability of each of the providers would have to be assessed accordingly based on the intended use case and level of responsibility and involvement desired by the prospective customer.

Generally speaking, many of the themes and challenges of digital identities were considered in the answers of all participants suggesting a good degree of thoughtfulness as it relates to the intended audience and markets for their products.

Picking the Right ID Solution

An ID is only as strong as the claims made against it and only as usable as the extent to which it is trusted by others. It is important to think critically not just about the technology but about all aspects of prospective ID products to find one that will integrate well within your organization's or program's objectives.

Some additional considerations are:

User Onboarding / Initial Registration

How complicated is the process to issue a new digital identity? What sort of safeguards exist to ensure data quality? What protections are in place to mitigate the risk of identity duplication or impersonation? Can the process scale with the envisioned number of identities being provided with your program?

Authentication

What does the authentication process to validate a digital identity or claim look like to an end user? What sort of devices or steps are involved in executing it? What kind of information is disclosed or exchanged during the process?

System Integration

What integration options are there with existing services, hardware, or technologies that might need access to the ID solution to perform authentications? What level of user and developer community support is there for the product to provide technical integration support? Is the solution interoperable with other ID products or networks which may already have a more established user base?

Usage Costs

For services which require payment to validate or make claims, what does the cost model look like and how will it be funded for target users (by the users directly or in a delegated fashion as operational costs of a program)? How will funds be created for continued maintenance and improvements to the ID system?

Summary of Findings

Picking the Right ID Solution (Continued...)

System Sustainability

Digital identity systems represent a significant investment by all stakeholders. How can the continued operation and improvement of the system be assured? What does the product roadmap look like?

Strength and Scale of Supporting Network

If the ID solution involves a network of trusted validators or authenticators, how big is the supporting network and who does it consist of? What does the governance structure look like? Do they have the capacity to provide services for the size of the prospective user base of your project? What sort of technical support is on offer from the company should there be questions or issues?

Ease of Use

How easy is it to understand the ID product and what level of digital literacy is required to use it? What sort of hardware or devices does the solution run on and how easy are they to obtain in the target environment? Does the system provide any offline utility if planned usage is in an area with limited connectivity?

User Protections

What measures are in place to ensure the rights, privacy and freedoms of the user are protected? Are there any barriers to inclusion? What degree of privacy preservation is taken in identity transactions? What safeguards are in place to ensure the identity cannot be revoked or controlled by an external entity? Are there any supervisory or liability standards in place to guide the governance of disputes between users?

The Future of Digital Identity (Where Things Are Going)

Now is an exciting time where the level of technology and prevailing attitude of most populations towards digital services is creating a climate where a truly portable, lifetime digital identity has the potential to become a reality. The coming decade is likely to be filled with further enhancements and refinements on the concept which will allow for greater interoperability between solutions and broaden the amount of places where a digital identity will be accepted as a valid credential when accessing a service. Reusable KYC assurances are also likely to become more common, reducing the burden identity verification has on businesses.

Better user-controlled privacy and information disclosure models also have the potential to create opportunities for ID owners to be compensated for the consensual disclosure of their personal information to interested parties. This changes the current practice of large identity or claims providers profiting from the sale of their troves of personal information to 3rd party companies, giving the control and ownership of this information back to individuals.

Finally, the advent of self-sovereign identity solutions based on reputation and claims instead of the issuance by a central authority has the potential to create identities that are stronger, more trustworthy, and have greater privacy controls than the forgeable, state-issued documents and license cards that we rely on today. As this form of identity becomes more popular, it will gradually create better identity assurance amongst individuals than exists presently, lowering counterparty risk for all those involved and creating more opportunities for people to transact with each other in trusted ways.

Getting Started

Given the sheer volume of digital identity products available on the market and the complexities of the technologies behind them, embarking on a project that contains a digital identity component can be a daunting task that can require much education and research. Fortunately, plenty of widely available material has been written on the topic of identity by various experts and agencies like the UN, the World Bank, and USAID to help get this process started. Once the market has been scanned and a shortlist of potential vendors has been identified, it is then important not just to rely on marketing materials and presentations, but to actually see the product in action to confirm how it works and get a sense of the user experience.

An initial proof-of-concept is a good next step to confirm the technical viability of integration within your potential project, followed by a pilot phase or small-scale rollout to see how the solution works in the hands of real world, on-the-ground users in your target environment. Taking a phased approach will also help to uncover some of the challenges that will be faced when scaling up to a full rollout.

Summary of Findings

Final Considerations: Do Your Research

Do Your Research

Ask the hard questions to ensure the digital identity solution you choose aligns with the needs of your program

Identities are important for what they represent and the rights and access which they grant or deny. Solutions purporting to provide them require careful scrutiny and consideration, not just of the technological factors and promises they make, but also of the companies behind them. Ensure their motives, the maturity of their products, and the talent behind their organization are considered to confirm the long-term viability and support of the solutions they provide. Just as easily as digital identities can create opportunities for a population, the utility they grant can be compromised if they've been implemented or designed poorly and their power can be taken away entirely if the company behind them ceases to exist.

Ask the hard questions and do your research to ensure the digital identity solution you choose aligns with the needs of your program and protects the rights, freedoms, and privacy of the individuals who will bear them.

Glossary

Blockchain & ID terminology

Phrase	Definition
AML	Anti-money laundering - due diligence activities that financial institutions or other regulated companies must perform to verify the identity of their clients for the purpose of conducting business
API	Application programming interface - a clearly defined intermediary layer which allows different applications to communicate with each other
authentication	The process or actions for linking users to identifying attributes
authorization	The means of granting access to an identified user based on what their attributes allow
attestation	An assertion by a party or the showing of evidence that a claim is true
B2C	Business to Consumer
BYOD	Bring your own device
BYOID	Bring your own identity
claim	A statement or assertion of something one claims to be true
credentials	Attestations of qualifications, status, rights or entitlements typically endorsed by an authority
DIF	Decentralized Identity Foundation
DID	Decentralized Identifiers - digital identities which are fully under the control of the subject
DKMS	Distributed Key Management System
ERC725	A self-sovereign identity standard for Ethereum
ERC780	An open identity and claims protocol for Ethereum
GDPR	European Union General Data Protection Regulation
GSMA	GSM Association / Global System for Mobile Communications - trade body that represents the interests of mobile network operators worldwide

Glossary

Blockchain & ID terminology

ICT	Information and Communication Technologies
IM	Information Management
IMS	Information Management System
JWT	JSON Web Token - an open standard that acts as a means of representing digitally signed claims to be transferred between two parties
KYC	Know your customer - due diligence activities that financial institutions or other regulated companies must perform to verify the identity of their clients for the purpose of conducting business
multi-factor authentication	A method for confirming a user's claimed identity based on presenting two or more pieces of evidence across different factors; typically something a user knows, something a user possesses, and something the user uniquely is
nash equilibrium	A game theory concept that reflects a stable state of a system in which there is no incentive for participants to deviate from an initial strategy to gain an advantage
OAuth	Open Authorization - an open standard for token-based authentication and authorization on the internet
OpenID	An open standard and decentralized authentication protocol
P2P	Peer to Peer
PII	Personally identifiable information
PKI	Public key infrastructure
QR code	Quick Response Code - a machine-readable two-dimensional matrix barcode
SSI / Self-sovereign identity	The concept of a long-lived, portable, user owned identity that can only be accessed in full by the person or entity to whom it belongs and exists outside the control of any 3rd party or intermediary
SAML	Security Assertion Markup Language - an open standard for exchanging authentication and authorization data between parties

Glossary

Blockchain & ID terminology

SDK	Software development kit - a collection of tools that allow for the creation of applications for a certain software package, framework, or platform
SSO	Single sign-on - a session and authentication service which allows a user to access multiple applications with one set of login credentials
TPM	Trusted Platform Module - a tamper-proof, secure chip designed to cryptographically secure hardware on a device
W3C	World Wide Web Consortium - an international community that collaboratively develops standards for the world wide web
ZKP / Zero-knowledge proof	A cryptographic method or protocol by which one party can prove to another party that they know something without conveying or disclosing the underlying information in question

BLOCKCHAIN
LEARNING GROUP INC.

Blockscale Solutions

www.blockchainlearninggroup.com
www.blockscalesolutions.com

✉

murtaza@blockchainlearninggroup.com
murtaza@blockscalesoltuions.com

@BlockchainLG
@BlockscaleSolns