Blockchain-based Identity Management: A Survey from the Enterprise and Ecosystem Perspective

Michael Kuperberg
Blockchain and Distributed Ledgers Group
DB Systel GmbH
Frankfurt am Main, Germany
michael.kuperberg@deutschebahn.com

***Abstract*—Identity management is a core building block for the majority of software solutions and landscapes. Competing with existing identity-managing solutions, Blockchain-based concepts and products have evolved in the context of verified claims and self-sovereign identities. The contribution of this paper is a systematic, criteria-driven survey of the solutions and technologies for this growing field, and their comparison with the capabilities of established solutions. By including an extensive set of requirements covering ecosystem aspects, end user functionality, mobility and overhead aspects, compliance/liability, EU regulations, standardization and integration, our work shows the highlights and the deficits of a wide array of solutions.**

***Index Terms*—identity management, IAM, blockchain, DLT, decentralization, self-sovereignty, verified claims, trust networks**

Managerial Relevance Statement

Stategic IT planning requires the understanding of available options and the assessment of their maturity. Additionally, managers must set the changing privacy and data protection laws into context, and be aware of technical responses to increased user awareness of data leaks and misuse. For identity and access management, the changed circumstances mean that the market is evolving and alternatives to centralized solutions and to the Identity-as-a-Service approach are being developed. One alternative is the concept of self-sovereign identity, which gives the control of the personal data back to the end user. Another alternative is the replacement of a central identity service owned by a single company through a network-governed multi-party solution, owned by a joint venture or by a consortium. Both alternatives are prevalently powered by blockchain technology, which is a specialized distributed ledger - capable of much more than just cryptocurrencies. This paper defines holistic evaluation criteria to assess these new approaches, investigates 43 blockchain-based identity solutions, and compares them to state-of-the-art.

I. Introduction

Identity and access management (IAM) forms the centerpiece of application ecosystems, both in enterprise environments and on the Internet. Beyond human users, IAM can also extend to things and machines in the scope of IoT (Internet of Things), interconnected vehicles and to Industry 4.0. Identity and access management are closely associated with privacy/confidentiality, non-repudiation and other security aspects that are the cornerstones of a trusted environment.

A large body of standards already does exist to convey information about identities/authentication and authorization/access rights (keys, certificates, roles, entitlements, claims, groups, attributes, etc.). These standards are designed for different areas and vary greatly in complexity and features. Implementation-wise, many IAM products are available in the market. Mobile devices such as smartphone have led to a wide acceptance of multi-factor authentication, one-time passwords and also biometrical logins using fingerprints and 3D face scans. Still, there is a demand for further features (such as vendor-independent claim issuance and verification) and also for new concepts, such as sovereign identities and for self-service identities in Machine-to-Machine environments.

Blockchain-based solutions that promise to deliver on these concepts are emerging in large numbers. At the same time, the blockchain technology and distributed ledgers (DLTs) are also gaining momentum in enterprise environments, expanding beyond the “early adopter” and “technology hype” spectrum. This momentum includes blockchain standards, technologies and products/frameworks that claim to add value in the context of IAM and IDaaS (Identity-as-a-Service). However, blockchain-based identities are mostly met with a fair amount of criticism and reservation in professional environments. This calls for a critical analysis of these newcomers and a comparison with established solutions.

The contribution of this paper is to provide an evaluation framework consisting of 75 criteria, which we also apply to 43 offerings. The resulting systematic survey of blockchain-based IAM solutions covers features, prerequisites, market availability, readiness for enterprise integration, costs and (estimated) maturity. This analysis includes the perspective of an enterprise architect/engineer, while at the same time addressing the central misconceptions found in the literature about IAM usability of blockchain technology and of DLTs.

The remainder of this paper is structured as follows: in Section II, we provide the foundations, describe state-of-the-art and set the scope for our survey. In Section III, an extensive analysis of related work is provided. In Section IV, we define the criteria that are used in Section V to evaluate 43 offerings and concepts for blockchain-based IAM. In Section VI, we summarize the findings of our survey. Section VII concludes and provides the directions for future work.

II. Foundations and State-of-the-Art

This section introduces the foundations that will be used throughout the paper. These include the state-of-the art for identity management, public-key infrastructures and cryptography, self-sovereign identities and verifiable claims, eIDs, Joint Ventures for IAM, Blockchains and Distributed Ledger Technology, decentralization as well as a summary of market forces in the IAM field and of laws / governmental standards.

To visualize the IAM use cases that blockchain-based solutions are involved in, Figure 1 shows how an end user interacts with authorities, service providers and identity providers. Some of the actors can belong to the same organization (e.g. a transportation provider, which can also be a business partner or a unit thereof). Note that consumer-to-consumer use cases are not shown, although ecosystems implementing such use cases have been created before (see e.g. Sec. II-G for PGP). Further identity-focused uses cases not shown in Figure 1 include joint ventures for identification (see Sec. II-C), judiciary, public recording of ownership and claims (e.g. land registries) as well as specialized service providers such as loyalty platforms, insurance/healthcare, business-owned reputation/credit scoring, and government-owned social scoring.

A. *IAM Market Forces - Demand/Offer and Ecosystems*

There is a number of driving forces that are reshaping the IAM market:

1) Decrease of *consumer trust* into major corporations that collect very high amounts of personal data, act as central intermediaries, and even sell/misuse it
2) Increased discomfort *of service providers* to share user data with IT giants (incl. social networks and media)
3) Political regulation to prohibit and punish the misuse and export of personal data to certain countries
4) The awareness for the commercial worth of user data ownership by service providers and networking effects
5) Lack of easy-to-use offerings for trusted identities on the Internet which could be used seamlessly and widely (including logins, issuance and checks of attestations/reputations, data sharing controls, data economy, etc.) while maintaining privacy
6) Lack of mechanisms to securely share and exchange data, incl. for Know-Your-Customer and AML scenarios

Ideally, using a trusted digital identity should be as easy as payments, where the end customer simply presents an NFC-enabled credit card (or just a smartphone) at a checkout in a supermarket. Even better, a trusted digital identity should be supported by mobile devices (in hardware and in operating systems) in such a way that an NFC-enabled smartphone or smart watch would function as a (partial) replacement for an ID card.

Beyond privacy-focused and IAM-centric driving forces, there is an ongoing demand for "simpler security": password safes generate *service-specific* complex random passwords, but the end users open the safe with their fingerprint or device passcode. Enterprise-grade IAM solutions deploy client certificates on (managed) end user devices but also rotate them without the need of action from the end user. However, "simpler security" is rarely achieved by empowering the (average) end user. On the contrary, it is often implemented by *minimizing* the work that needs to be performed by the end user. This must be kept in mind when analyzing the attractivity of novel IAM solutions.

Running authentication and authorization services costs the service providers significant money. Thus, service providers often elect to support lowest-cost authentication schemes (e.g. third-party login) over more secure but more costly schemes (e.g. self-hosted or self-administered two-factor authentication). Still, the service providers have to store the authorization data and other information on their own infrastructure. Established interoperability standards (such as OAuth [1]) are widely supported by the largest market players such as Google, or Facebook. This has led to the large use of "Sign in with Facebook" and similar comfort features for the end users but it is also perceived as a threat by some smaller players and traditional industries which desire ecosystems without de-facto centralization.

B. *Laws and Governmental Standards*

In the area of IAM, the General Data Protection Regulation (GDPR) [2] of the EU has mandated that *personal* data has to be used and stored in a controlled way. Additionally, persons can request to introspect the data stored about them and can also request to have their data deleted unless the service provider has obligations (or law-compatible interest) to store that data. The details and the scope of the GDPR are widely discussed (and partially contested), as in the position paper [3] of a blockchain industry group.

The GDPR laws mandate harsh penalties for GDPR violations; for example, a hospital was obliged [4] to pay ca. 400k EUR in penalties. Thus, novel IAM systems (such as those based on blockchains/DLTs) must take great care to comply with the GDPR, especially w.r.t. the "right to be forgotten".

Another law that is relevant to IAM is eiDAS [5]: the European directive about electronic identities. eiDAS defines which types of electronic IDs (and signatures) have a binding, authoritative validity equaling that of "traditional" signatures and proofs-of-identities. Each EU member issues a national law that "translates" eiDAS and adapts the impacted national laws. Modern eIDs such as the nPA [6] in Germany are designed to comply with eiDAS.

C. *Networks and Joint Ventures for Cross-Company IAM*

Single Sign-On (SSO) is an established technology to improve user experience: a single set of credentials is valid across multiple services. On the Internet, SSO often removes the need to login individually to each service: using standards such as SAML [7], the user is automatically logged in to each site that is connected to a given identity provider. Using *identity federation*, several identity providers create a network where multiple identities of a given user can be connected seamlessly and are mutually recognized.

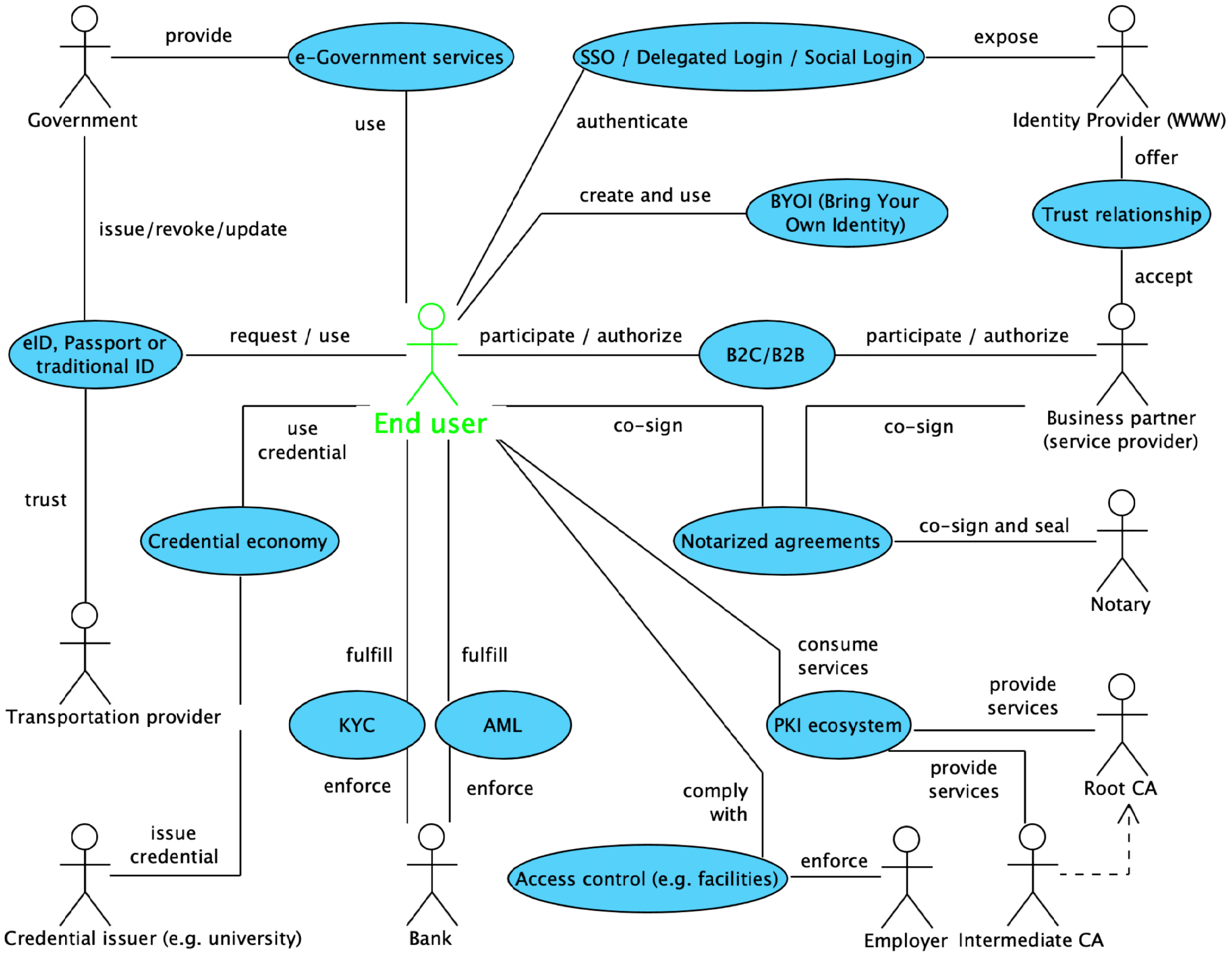

Fig. 1. A selection of use cases and actors in the area of identity and access management (IAM)

However, SSO mostly handles only authentication, but not authorization. Additionally, exchange of user attributes requires the use of standards such as OAuth 2.0 [1]. Yet even then, a centralized hub-and-spokes architecture maintains the dependency of service providers on the identity provider.

Bring-Your-Own-Identity is a concept which encourages a broader choice of standards-compliant identity providers, rather than requiring specific vendors or services. Identity-as-a-Service is the corresponding implementation concept where the identity provider is an external offering which is based on standards and can be exchanged. Most cloud computing providers offer it out-of-the-box; some products even carry in the product name, e.g. OneLogin [8].

One solution to mitigate dependencies on external identity providers are joint ventures (partnerships), where the identity provider is collectively controlled (or even owned) by several service providers. In such a network, data exchange between partners can be governed by mutual interests. A prominent example of such a venture is Verimi [9], founded by large companies such as Volkswagen, Daimler, Lufthansa and others alongside specialized government authorities such as Bundesdruckerei (Federal Mint). There are similar network concepts, e.g. NetID [10] and ID4me [11].

Verimi's offering is not blockchain-based and it is closed-source, but it provides industry-grade APIs following open standards such as OAuth 2.0 [1] and OpenID Connect [12]. Users' personal data does not leave the EU, according to Verimi (cf. GDPR mandates). Verimi end users can add details such as postal addresses, phone numbers, banking documents and passport/IDs. Trusted user verification is performed by video-based interactive authentication (through WebID [13]).

Acceptance of joint ventures by users depends not just on user friendliness, but also on how much data will be exchanged and correlated by the participating companies, and whether user incentives (rather than additional costs) will be provided, especially when existing user data must be migrated.

The topic of identity reuse is driven by interest groups and organizations such as OIX [14] (Open Identity Exchange), GPSBD [15] (Global Privacy and Security by Design), IDPro [16], Secure Technology Alliance [17] and others. The FIDO alliance [18] works on authentication standards which would improve Bring Your Own Identity and Identity-as-a-Service.

D. Self-Sovereign Identity (SSI) and Verifiable Claims (VC)

A substantial number of the revolution-promising newcomers (cf. Section V) build their use cases on the promise of *self-sovereign identities* (SSI). The "Self-Sovereign Identity Working Group" [19] is one of the interest groups driving this topic. Their primary goal is to "liberate" the data from the service provider siloes and to give the end users the ultimate control over their data contents and over the sharing of their data. Often, the goal of SSI is condensed to the phrase "so no one else can put the plug on the user's identity".

The concept of *Verifiable Claims* (VCs) [20] employs cryptography to enable tamper-proof and digitally signed claims. VCs usually require three parties: the claim bearer, the claim requestor and the claim issuer. The VCs must be retractable (revocable); logically, the claim issuer as a third party could retract a claim in a manipulating, or even criminal way: the VC bearer depends on VC issuer, which is a third party, limiting the claim bearer's sovereignty. To protect against such misuse, claim issuance must follow a balanced protocol. Obviosly, self-issued VCs are not a trusted option.

Additionally, a reliable service for revocation lookup is needed; this mechanism is similar to OCSP [21] for conventional CA-issued certificates. Revocation lists are therefore also a dependency which limits the sovereignty of the claim bearer. Placing the revocation list provision into the hands of the VC bearer would suffer from lack of trust.

In general, SSI and VC proponents can build on the existence of working, proven technologies for credential and claim management: CAs and client certificates within PKI landscapes. However, it is often the case that the costs of running an appropriate PKI mean that PKI-based VCs are limited to use in corporations and government/military agencies.

The base assumption of the SSI proponents is that service providers (or the "data siloes") will cooperate with the end users in the area of SSI and VC. In a data-driven ecosystems where ownership and analysis of information are key assets and the core value proposition, this "revolutionary" data-minimizing stance will obviously be met with opposition. Within the limits set by the lawmakers, service providers will strive to save (and sell) as much personal data as possible - finding a provider-individual optimum between users' willingness and provider's hunger for data.

In reality, end users often face the choice to accept an offering, based on fixed business terms with the provider-minimized data protection - or not to use the service provider at all. Even today, "configurable" offerings with the possibility to *opt out* of data collection are often deliberately disincentivized by service providers through coupling them with reduction in capabilities and decreased end-user comfort. Such pseudo-choice is also often well-hidden in the settings.

As for the competition between companies, an *average* user will not migrate away from an established service to an SSI newcomer, unless the competitor is functionally/economically equivalent or better, a "threshold of pain" is reached and the costs of the transition are also acceptable. Furthermore, the service providers are likely to continue by diversifying their identity interaction by the user groups: the majority of users might prefer the convenience of "Sign in with <enter your IT giant here>", but the privacy-conscious and the SSI proponents will still be able to create their own, provider-specific logins (thus missing out on SSO).

E. eIDs (Government-issued electronical/online Identities)

Governments are traditional sources of identification / life-cycle documents for humans (and animals): they issue passports, ID cards, birth certificates etc. "Digital identification" issued by governments is often called *electronic IDs* (eIDs). eIDs come either as "smart" documents/chipcards with some cryptographic/electronic equipment, or as a centralized IT system where a person's document is just a 'printout" of the identifier, as it is the case in the Aadhaar [22] system in India (which also contains biometric data).

Estonian government offers [23] a digital ID as part of the "e-residency", which requires a personal show-up at an Estonian embassy as part of the application and an administration fee (Estonian e-residency does not entitle to "normal" citizenship and does not grant residency rights). If granted, e-residency includes a PKCS11-enabled NFC-based smart card with online identification, eiDAS-compliant digital signature incl. timestamping, electronic voting (for citizens) and some other services. An integration with NFC-enabled smartphones is available. Still, at the end, this solution is less versatile than a "conventional" PKI solution, and requires substantial invest of time and money.

Valuable insights into eID are provided by manufacturers, such as by Gemalto [24]. Possible integration of eIDs into ecosystems includes "virtual transportation tickets" (which are stored in a central system and referenced by the eID of the ticket holder), eGovernment, banking services etc. As with SSO, a single eID with cross-use is both valuable and vulnerable. Criminal control of such an eID (especially when the PIN code is also in criminal hands) is especially dangerous - at the same time, it is simpler to perform an emergency deactivation and pattern detection of a single card than to address the loss of several cards.

F. Representing an Identity, Attributes and Claims

There are two different basic types of identity representations: *owning* a physical item (e.g. an ID card) and *knowing* (a secret). The difference between the two types is that the first type can be disclosed as it maintains a physical uniqueness (unless, of course, it is too easy to duplicate). The second type must be safeguarded because knowledge is easily replicated, while possession is not. The two basic types are often used in conjunction: e.g. in two-factor authentication (2FA) where a password login is supplemented by a one-time access token sent to a mobile device. In this case, the owned mobile device is the item that is attached to an identity. In the physical world, an additional secret is often used to protect the item, e.g. when a smartphone is locked using a passcode or a fingerprint.

In the past, the secret was often stored not just by secret owner (the "client side"), but also by the "service provider" – e.g. to enable password recovery and "human error resolution". With the obvious advantages, this also brought the disadvantage of potential identity theft or denial. Even if the password is not stored in cleartext at the service provider (this is now instead widely done through hashed and salted passwords), it must be matched against a record to check the authentication.

Alternatively, password-less authentication (e.g. using client-side X.509 certificates [25]) is used. Another vendor-independent identification technology is GSMA Mobile Connect [26], designed to be used from mobile devices (e.g. smartphones) when connected to the mobile network.

For decentralized landscapes, the W3C has developed Decentralized Identifiers (DIDs) [27]. These are complex mechanisms utilizing URLs, resolvers and cryptography. DIDs are used in several offerings analyzed in our paper.

Most end users are accustomed to site-specific, UI-oriented presentations of identity attributes and claims (achievements, properties, capabilities, entitlements, certifications, laudations, citations, confirmations etc.). Unlike for calendaring (where iCalendar is a *de facto* format written and read by most current applications), attributes and claims have no generic de facto interchange format that could be used in IAM. Still, there are some standards for attributes and that might be suitable for processing by machines and could be used for blockchain-based IAM: LDAP [28] data formats (or even vCard format for electronic business cards) or IMS Open Badges [29].

High-level identity representation standards include ISO/IEC 24760-1:2011 [30]. Security standards in information technology include, for example, ISO 29115 [31], the "Entity authentication assurance framework" (due to be renewed in 2019). There are several additional standards (and certifications) in the area of "information security".

G. Enterprise-Grade PKI and PGP/GPG

In environments based on Public Key Infrastructure (PKI), a Certificate Authority (CA) issues certificates for various tasks, e.g. for authentication of individuals towards a service provider, for email signing, or for code signing. The common approach is to define a set of "root certificates" which are trusted by the end user with almost no interaction needed: often, the root certificates are distributed as "trust anchors" with an operating system or with a web browser.

From the root certificates, a "certificate chain" descends to an end-user or website certificate. Overall, there is a forest of certificates and the found trust relationships can be checked against it. Finally, there are certificate revocation standards which are designed to ensure that lost/stolen certificates can be detected and considered untrustworthy. Despite a high intrinsic complexity, PKI and certificates are widely used in the enterprise environments.

Products such as Microsoft Active Directory or Amazon Web Services (AWS IAM) include not only the PKI core, but also the administrative tools and integration interfaces. These products have been audited and certified; they have reached a considerable maturity from decades of use and millions of users. Moreover, they are integrated in the cloud landscapes of the respective vendors and co-evolve with those. Existing enterprise-ready solutions for PKI and IAM have been integrated with some blockchain products in the scope of cloud offerings, such as Microsoft's Azure stack [32] to run Ethereum as private/consortium networks.

PGP [33] is a product for encryption of data (incl. emails), with OpenPGP [34] being the underlying standard; GPG [35] is an open-source alternative to PGP. Unlike X.509, PGP also supports a "web of trust" which does not require hierarchies (with a CA as the trust anchor). In the "web of trust", participants verify the keys in a peer-to-peer way, e.g. in person. PGP has a mature support in email clients (though it must be installed separately) but has not achieved a substantial spread in private or enterprise environments – in contrast to X.509-based, PKI-oriented standards such as S/MIME. Combinations of PGP and Blockchains have been proposed in a paper [36] by Wilson and Ateniese and in a thesis [37] of Costa.

H. Blockchains and DLTs from the Enterprise Perspective

Solutions based on blockchains that follow the WORM principle mostly tend to keep personal data (PII) off-chain, while storing hashes (integrity codes) or statements/claims/entitlements on-chain. It is being debated whether storing encrypted data on a WORM blockchain is future-proof: even if the encryption key is being intentionally discarded at some point, advances in computing power (or future discoveries of implementation weaknesses) mean that the encrypted data may be decrypted even without the decryption key.

There are many blockchain and distributed ledger technology (DLT) products; their capabilities and maturity differ significantly. To start with, the prominent Ethereum [38] blockchain is unpermissioned, public and append-only with WORM semantics (write once, read many); this property inhibits any deletions or modification. However, Ethereum is open-source and can be deployed in isolated private networks.

Joining the *public* Ethereum main network is unrestricted and free; everyone can create a free, pseudonymous "account" (also called "wallet"), which is technically an asymmetric keypair. Ethereum can store not just data, but also executable code: so-called smart contracts. Each Ethereum full node replicates all data. Other blockchains (and DLTs) share some of the properties with Ethereum, while differing in others. For example, Hyperledger Fabric [39] is permissioned.

Pseudonymous participation means that the blockchain itself does not require the users to disclose their real identity at any stage; yet the use of a given keypair constitutes an identifier for all the transactions to or from the given address. On Ethereum (as on Bitcoin), there is a full visibility of all transactions (asset exchanges) on the public ledger. However, the underlying real identity is disclosed if the end user registers with regulated market exchanges, which must comply with local laws for KYC (know your customer) and anti-money laundering (AML). Exchanges are needed to convert cryptocurrencies into Fiat currencies with the effect that pseudonyms can then still be traced back to the real-world identity.

The anonymity on a given blockchain also means that there is no bank-like central authority to block an account in case of identity theft or misbehavior - but also that each user must herself safeguard against forgetting (or losing) the private key. Of course, any person is free to possess more than one keypair (identity) on a given blockchain - without any visible links between the identities unless explicitly made clear (deducing these links is possible through extended analysis using both on-blockchain and off-blockchain data, such as IP assignment history of the internet provider).

Most blockchains also have no built-in provision for a more integrated treatment of the IAM aspects. For example, there is no interface to PGP, X.509 certificates or CAs (Certification Authorities) in Bitcoin or Ethereum. Despite the obvious limitation of such blockchains, there are still limited niche use cases to use them from the IAM perspective. A working example is the Bernstein [40] approach, where hashes of intellectual property rights are saved on one or several public blockchains. The timestamping and fingerprinting of property rights can thus be seen as an (unusual) aspect of IAM.

The majority of the data stored on public blockchains records asset transfers concerning cryptocurrencies and tokens. Still, it is possible to store further data in the transactions and blocks, or even executable code and rules (often called "smart contracts"). Such data could be custom or standard information from IAM, making this information both public and highly replicated. Smart contracts could automate claim management and reputation administration. Assuming that the given public blockchain continues to be available for sufficiently long periods, this information would be independent of a single vendor, service provider, or any other further party.

Still, the high transaction costs of *public* blockchains and their low throughput / high latency render them quite unsuitable for the larger share of the IAM use cases. Additionally, data protection standards such as GDPR [2] give individuals certain rights to ask for their personal data to be deleted – something that most public blockchains with WORM semantics (incl. Ethereum) can hardly offer.

For some DLTs/blockchains, the technical possibility of having branches within a blockchain instance has led to controversial views: the presence of two branches can mean that there can be two conflicting versions of a fact, where each branch holds a state change with the same precondition but with different postcondition. Such a conflict could even be an "agreed" state that is stored across nodes. Obviously, conflicting IAM "facts" are not desirable – although even in conventional system, data reconciliation is a standard case (which consumes a substantial amount of resources).

A large number of end-user computing activities take place on mobile devices such as tablet and smartphones. These devices do not provide a stable network connection, nor do they have the bandwidth or storage available to enable them to participate as full nodes of a public blockchain. From the IAM point of view, mobile devices are often "managed" by specialized, enterprise-run software which enables additional Certificate Authorities (CAs). Mobile device management also supplies authentication certificates over the air (and rotates them periodically) and hardens the device security by imposing rules for device lock codes and passwords. Despite a first attempt by HTC [41] and by Sirin Labs [42], wide native mobile device support for blockchains/DLTs is almost non-existing, neither at hardware level nor at OS level: blockchain capabilities are introduced by hand-picked apps, through mobile browsers or browser extensions.

Even for desktop computing, there is hardly any first-level support for blockchain protocols (or for wallets) at operating system or hardware levels. Device users install custom apps/browsers/extensions to store their secrets (keypairs) and to administer their accounts in proprietary wallets. Fake apps and insecure implementations have been known [43] to rob cryptocurrency users of their assets, with no central authority to recover the lost funds. Even very large hacks (e.g. the hack [44] of the Ethereum DAO, which actually led to concerted community action in the form of a hard fork) may or may not resolve the incidents to a satisfactory degree (where losses are recovered fully, and undesired effects are reversed).

Many mainstream blockchain implementation are limited in comparison to "standard" software: e.g. in Ethereum, there are no reliable timers and no "callouts". Beyond the products covered by this paper, there are dozens of other blockchain tools on the market, supplemented by over hundred cryptocurrencies. As the technology continues to evolve quickly, it will have to measure itself against more established technologies (such as container-based distributed microservices).

I. Decentralization

Many blockchain projects hail "decentralization" as a synonym for a better architecture: less monopoly/oligopoly, more control for the end user, more room for the market forces, etc. While technical decentralization has long arrived (cloud computing, peer-to-peer networks, ...), business-level decentralization can be seen as the journey back from the supermarket to the farmer's market. In fact, having a one-stop shopping experience ("A to Z", as the logo of the online market leader says) is significantly more comfortable to most end users than individually querying (or visiting) several separate shops.

The market outside the ICO-powered blockchain startups shows that centralization happens in different forms: aggregators (e.g. travel deals), price comparison engines (e.g. energy contracts, powered by commission), online marketplaces (e.g. sales of used items) or auctions (e.g. concert tickets). In fact, the "lookup" and the "connect" functionalities that will be needed by blockchain-using marketplaces (and other offerings) very much resembles that of "trackers" in P2P networks: a tracker is a logically central "exchange place" for information about where to find the actual decentralized data (the data itself is replicated and/or split into segments).

At the same time, conventional blockchains with the "all nodes store the entire blockchain data" setup (i.e. full replication) can be considered to be more centralized than distributed architectures where information is stored only partially by the partners. Partial distribution of data (e.g. a given network partner is restricted to the dataset which is truly relevant to him) may improve speed and throughput, but offers a smaller resilience against data loss, and impedes distributed consensus.

III. Related Work

In [45], Lim et al. provide a survey of the Blockchain Technology for IAM and Authentication. While they cover some of the offerings analyzed in this survey, they do not research the support for IAM standards and protocols. Some of the most promising offerings (such as Civic) are missing.

In [46], Grüner et al. examine the suitability of blockchain for IAM, by applying a decision model to uPort, Sovrin, and ShoCard. In contrast to our work, they limit the analysis to a few players, and do not consider enterprise-grade interfaces and application integration as key evaluation criteria.

In [47], Jacobovitz provides a survey of blockchains in IAM as of 2016. However, the report does not cover strong competitors such as Sovrin or Hyperledger Indy; other mentioned competitors (e.g. BlockAuth, Cryptid) have since gone out of business. In contrast to our work, integration aspects and MFA are not evaluated. In [48], Yang et al. provide a "Survey of Confidentiality and Privacy Preserving Technologies for Blockchains", written in December 2016. The authors work for R3, though that company's Corda DLT product is not featured in the survey. Other prominent offerings, such as uPort or Sovrin, are also not featured in the report.

In [49], Mühle et al. perform a survey on what they consider to be the essential components of a solution for self-sovereign identity. However, their work does not investigate whether the found components/offerings can be integrated into the enterprise-grade architectures that already established, using standardized interfaces and protocols.

In [50], Stokkink and Pouwelse introduce a "generic provable claim model" using zero-knowledge proofs. Their work targets a self-sovereign identity for the Netherlands and was part of a government-conducted pilot [51] in 2018. However, it is not shown how the work integrates with existing IT applications.

In [52], Ahmed and Kostiainen propose "identity aging" as a consensus approach. The authors present two own implementations of self-sovereign identity and provide a comparison (w.r.t. efficiency and security) to 14 other consensus approaches. In contrast to our work, analysis of integrability and end-user friendliness is not undertaken. In [53], Dunphy and Petitcolas provide a critical technology-level evaluation of three offerings for blockchain-based identities based on seven "laws of identity" and contrast the three offerings with Facebook Connect. However, they do not analyze aspects of enterprise integration or any other offerings, and do not compare the offerings to conventional PKI. In [54], Dunphy et al. list open challenges for DLT-based decentralized digital identities, but do not survey market offerings. In [55] and in [56], Augot et al. present a user-centric system for verified identities on the Bitcoin blockchain. They list some related blockchain-based approaches, but do not survey them in a systematic manner.

In [57], Schanzenbach et al. present a prototypic implementation of a system for self-sovereign identities, albeit without blockchain or DLT components. Unlike most self-sovereign identity approaches, the authors discuss how their approach can participate in an established standard (here, OpenID Connect).

In [58], Othman and Callahan describe the specification and implementation of decentralized storage option for biometric credentials, done via blockchains using DIDs within the IEEE 2410-2017 BOPS (Biometric Open Protocol Standard).

In [59], Der et al. discuss ISAEN, a standard for self-sovereign identities for human beings - however, ISAEN is currently not implemented. In [60], Guggenmos et al. discuss the "platformization" of blockchain-based digital identities, but do not analyze any product or solution and do not set up criteria for their evaluation. In [61], Al-Bassam proposes a PKI based on smart contracts (to overcome vulnerabilities of conventional CAs) – however, beyond a CA PoC, there is no implementation or product for the end users.

In [62], Baars compared (as of 2016) several blockchain-based identity solutions and also checked them for support by the passport.js JavaScript library, which supports more than 300 hundred authentication methods. The author proposes a new solution based on his findings, but the solution has not been implemented yet. In [63], van Wingerde compares uPort and Sovrin in a systematic way.

In the book "New Solutions for Cybersecurity" [64], a section by Shrier et al. is dedicated to decentralized, blockchain-based approach to data security and to identity management in particular. The only described solution is Enigma [65] (cf. Sec. V-G), which uses advanced techniques such as secure multi-party computation (sMPC) and provides a public test network. In the book "Hands-On Cybersecurity with Blockchain: Implement DDoS protection, PKI-based identity, 2FA, and DNS security using Blockchain" [66], the author shows how to implement different security aspects (2FA, PKI-based Identity, DNS and DDoS protection) using blockchain technology - some aspects are covered using Ethereum, and some using Hyperledger Fabric. However, the book does not provide an analysis of products on the market and does not target building a production-ready IAM solution. In the book "Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity" [67], the author describes (from the perspective of a law center) the intersection of the EU data protection directive and the opportunities of blockchain-based identity systems. It focuses on concepts and does no market analysis.

A substantial number of up-to-date publications on identity management and on using blockchains/distributed ledgers for IAM is regularly provided by market research companies. These include Gartner (e.g. [68]–[72]) and others. While this survey investigates technical features and the architectural details of integration and standard compliance, the market research documents work on a higher abstraction level and do not consider academic research.

IV. Evaluation Criteria

The evaluation criteria introduced in this section will be used in the Section V to analyze the identified offerings. They are grouped into Table I (compliance and liability criteria: CL01 through CL12), Table II (criteria for end-user experience: U01 through U32) and Table III (technology, implementation, integration and operations criteria: T01 through T29).

Note that we do not include quantitative properties such as performance (throughput, latency etc.) or overhead because we found that it is simply too early to compare the established

TABLE I
COMPLIANCE AND LIABILITY CRITERIA

Number	Criterium description
CL01	GDPR Compliance and Support (incl. inspection, download and deletion of personal data), explicitly asserted and guaranteed by the vendor / service provider - mandatory for services available to EU customers
CL02	Control over geographical distribution of data (e.g. restriction to EU or exclusion of certain countries)
CL03	Credentials and access material can be rotated and withdrawn following central rules
CL04	Audit trail (user actions such as logins are protocolled, and so are changes to identity or access properties and privileges), in a GDPR-compliant way
CL05	Avoidance of liability for third-party offences (e.g. for situation where data is written to a shared co-owned ledger, but the data turns out to be punishable by law)
CL06	End-user data cannot be evaluated or sold by the identity provider (data sharing is turned off by default, but end users can choose to opt-in as well to opt-out again)
CL07	Identity export and transfer can be controlled to prevent identity theft (e.g. by preventing the export of a X.509 client certificate from a managed mobile/desktop device)
CL08	Hosting model (provider-offered service and/or provider-managed cloud hosting and/or customer-managed cloud hosting and/or customer-managed on-premise hosting)
CL08a	For hosted solutions: support desk (incl. contact over the phone) with quality-of-service
CL08b	For hosted solutions: Service Level Agreements (availability, performance, recovery time objective ...) and Support Level Agreements (bug fixing, patches, . . .)
CL08c	No obligation for service providers to use a proprietary token/cryptocurrency to pay for IAM services
CL09	Certification by third parties (e.g. TÜV) w.r.t. security and data protection (implementation and/or deployment)
CL10	Payment model for service use (e.g. prepaid, postpaid or pay-as-you-go) and fixed prices in a convertible fiat currency (to prevent cryptocurrency rate fluctuation risks)
CL11	Purchase/usage includes rights to audit or even to reuse the source code; reuse rights might be restricted, as in the case of GPL open-source license
CL12	IAM network traffic from/to IAM-using backend applications can be isolated from internet traffic (e.g. through a VPN or a VPC)

solutions with the blockchain-based newcomers. As part of the evaluation, Sec. VI-F discusses our observations about performance research in blockchain-based identities.

The criteria attempt to include the points of view of a EU-based product manager and of an enterprise architect, who have specific needs and priorities. Obviously, a company usually has other priorities than an academic researcher, a blockchain enthusiast or a startup. For enterprise usage, blockchain-based IAM must However, most blockchain-based IAM offerings are currently being built starting with an Minimum Viable Product. Therefore, enterprise requirements are often on the roadmap, but not implemented yet.

There is already a number of publications explaining and summarizing IAM requirements, e.g. [76] and [77]. However, we found that blockchain-relevant requirements have not been established in a systematic way, and that they have not been combined with traditional requirements for IAM. Therefore, our contribution is to establish the requirements that cover both worlds and include decentralization and SSIs.

We have classified the criteria into must-have requirements and desired options, the latter are marked accordingly. This classification will not apply universally: for example, GDPR is a central must-have for EU companies, whereas it might be only optional in other countries. The first eleven criteria in Table III are relevant for blockchain-based networks, but usually not for conventional IAM implementations.

It should be mentioned that established IAM solutions do not necessarily fulfill all of the above criteria: Table IV shows how a mainstream solution covers the *majority* of these. Note that a deployment of Microsoft Active Directory is not limited to usage within in a single company: through Federation Services, its IAM functionality can be used by external partners and systems. Additionally, cloud-native AD deployments (e.g. Azure AD) exist, and protocols such as Kerberos, LDAP and SAML enable standard-compliant integration.

V. Survey of Market Offerings for Blockchain-based IAM

In this section, we look into 43 approaches with different levels of maturity and availability. We chose not to filter and include both implemented market-ready solutions and unimplemented proposals, in alphabetical order. For the implemented offerings, we provide key insights (current as of April 2019) using the criteria from Section IV. An evaluation of the insights is provided in Sec. VI-A.

A. Abacus; BanQu; BitID; Bitnation; Blockchain Helix

Abacus [78] is an Ethereum-based open-source "identity and compliance protocol for permissioned tokens": it has backend workflows for KYC, AML etc. and its primary targets are fintechs/cryptocurrencies. The Abacus homepage and whitepaper do not disclose a business model and do not provide a UI or app for the end users.

BanQu [79] is a DLT-based for-profit solution for an "Economic Identity", focusing on disadvantaged parts of the world society such as refugees and the "unbanked". BanQu promises to provide a DLT-based credit record, and to support mobile phones (incl. legacy handsets) Technical details or design of the app are not publicly disclosed; real-world deployments and reports of user experience are not provided.

BitID [80] is a simple "Bitcoin Authentication Open Protocol" designed for authentication using the essential property of public-key cryptography: the server presents a challenge (nonce) to the client, the client signs it with the private key and the server verifies the signature using the public key. In BitID, the identity is the Bitcoin address. BitID is not a full

TABLE II
CRITERIA FOR END-USER EXPERIENCE

Number	**Mandatory?**	**Criterium description**
U01	yes	End users do not have to pay separately for basic identity services (the costs are covered by the service providers)
U02	yes	Identity is suitable for single sign-on to services (websites, apps, etc.) and/or for single sign-out; vendor-independent standards are used for both use cases
U03	yes	Identity is usable from mobile devices (apps and/or websites and/or at the level of the operating system)
U04	yes	Identity is usable from desktop devices (ditto)
U05	yes	Dashboard with current logins, detailed data exchange and history or identity usage
U06	yes	Usage of the identity does not require the installation of a dedicated app and/or of a dedicated browser extension
U07	yes	MFA or 2FA (Multi-Factor Authentication / Second-Factor Authentication) are supported
U08	yes	Identity and/or entitlements can be exported (in a portable way, e.g. on a portable drive), preventing vendor lock-in
U09	yes	Identity and/or entitlements can be synchronized across devices and/or can backed up automatically
U10	yes	Recovery of lost access credentials (through a support desk / password hints / trustees / backup password / through trusted devices with active sessions)
U11	yes	Self-registration is possible
U12	yes	User-selectable "initial secret" (e.g. initial password)
U13	yes	Identity is not bound to an email address, mobile phone number, exact first/last name, or specific device
U14	yes	Ability to create multiple identities/identifiers with the same provider, and ability to use one or several of them from the same or multiple devices concurrently
U15	yes	A ecosystem-wide registry is available to find identities by attributes and/or hierarchy
U16	yes	Identity information and entitlements can be relayed using headless technologies (such as NFC or Bluetooth)
U17	no	Representative identity information can be exported into a tamper-resistant and timestamped "business card" (partial or full "snapshot" that is not suitable for authentication, authorization or impersonation), and the "business card" can be exchanged electronically (e.g. over email, or by storing on a ledger)
U18	no	Integration with government-issued electronic ID documents (eIDs), e.g. for signing (cf. eiDAS)
U19	no	Identity includes a client-side certificate/keypair for authentication, authorization, signing and encryption
U20	no	Users fully own identities and associated data (self-sovereign sdentity)
U21	no	Users can selectively share their data with service providers (with/without payment to the data owner)
U22	no	Identity doubles as the address of an account (wallet) which can send/receive blockchain-based assets
U23	no	Identity can be used to sign emails, documents, code, or claims (locally or remotely)
U24	no	Identity confirmation by third parties (governments, businesses, individuals) is supported, leading to a *trusted* identity to prevent identity duplication and theft; identity verification is anchored in a peer-to-peer "Web of Trust" (cf. [35]) or by trusted authorities
U25	no	Identities can be structured into hierarchies, with known trust anchors (roots)
U26	no	Inclusion of photos (user-supplied; validated or not) and/or biometrical data as identity attributes
U27	no	Identity theft and identity cloning are *monitored*, detected and eliminated
U28	no	Ability to name trustees (e.g. parents, children, supervisor or a lawyer) to administer the ID in case of medical emergency or death
U29	no	Support for explicit impersonation for specified scopes and periods of time (this is distinct from authorization aspects, such as fine-granular partial delegation of capabilities and entitlements to another identity)
U30	no	Identity does not terminate even if credentials are not rotated within the given timeframe
U31	no	Seamless migration of existing accounts (incl. deactivation of migrated accounts)
U32	no	Support for zero-knowledge proofs instead of direct data release to service provider
Number	**Mandatory?**	**Criterium description**

self-sovereign identity offering, even if the identity it uses cannot be taken away by a centralized authority. Examples for implementing smartphone apps with BitID are provided, but market usage of BitID has been very low.

Bitnation [81] calls itself "the world's first Decentralized Borderless Voluntary Nation" with services such as blockchain-based ID, embassies and with a decentralized market for legal services called Pangea. It is open-sourced, implemented with Ethereum (on the public network), includes interfaces for integration, has a mobile app for Android and iOS (TestFlight only), and claims to be blockchain-agnostic. Bitnation defines two tokens, one of which can be bought on cryptocurrency exchanges while the other must be earned through community services such as arbitration. As of April 2019, there are no external services or end-user websites that make use of Bitnation's technology.

Blockchain Helix [82] calls itself the "DNA of the Digital Identity" and focuses explicitly on self-sovereignty and compliance with EU laws. As of April 2019, only an alpha version is available (which is a demonstrator, not a functioning service platform); registration is only possible with a mobile app (Android only). Architecturally, the Helix puts the user between the "trust provider network" (i.e. the endorsers of attestations) and the "trust taker" (i.e. service providers in need of an attestation). There is no public documentation on the design and implementation details, and the source code is not open-sourced. There are no known applications or end-user websites that use the services of Blockchain Helix.

B. Blockpass IDN

Blockpass [83] advertises its solution as an identity system for "the regulated industries and the Internet of everything". Blockpass describes itself as a "self-sovereign identity verification service that only stores a cryptographic representation of [user's] verified identity on a blockchain whitelist" so that a user's data "is stored on [user's] mobile device" and shared only with those whom the user chooses.

TABLE III
TECHNOLOGY, IMPLEMENTATION, INTEGRATION AND OPERATIONS CRITERIA

Number	Mandatory?	Criterium description
T01	yes	The blockchain network is permissioned to ensure that only authorized parties can set up nodes, access data and vote
T02	yes	The blockchain network is based on an established non-niche product (e.g. Ethereum or Hyperledger Fabric)
T03	yes	Admission to the blockchain network is regulated, e.g. by a subset of participants (e.g. "authorities" or "founders") or by a majority vote of all/active network participants
T04	yes	Active participation (e.g. voting and block creation) in the network operation is incentivized (e.g. through "gas" paid for transactions or for mining of blocks)
T05	yes	Network participants can vote on changes to the source code of rules and governance (e.g. through smart contracts), and how to truncate / rollover data
T05	yes	Separate/isolated test network open for inspection and trials (before purchase and without commitment)
T07	yes	Data is sharded or sliced: nodes can choose to store only a relevant part of the data (e.g. a subset of identities which are relevant to a given service provider)
T08	yes	The implementation has a broad adaptation base and is backed by a consortium, multi-vendor foundation or interest group (to prevent technology lock-in, product lock-in, vendor lock-in, consultant lock-in etc.)
T09	yes	Only the public key of the identity is stored on-chain; the wallet address is derived from it
T10	yes	Only hashes of assertions and claims are stored on-chain (but neither the unencrypted nor the encrypted cleartext of the assertions/claims)
T11	yes	Conventional protocols (such as LDAP [28] and/or SAML 2.0 [7] for SSO and/or OpenID Connect [12] and/or OAuth 2.0 [1]) are exposed for integration with service providers and in-house applications
T12	yes	Identity federation functionality is available (using standards such as JSON Web Tokens [73] and others) to establish cross-trust between several identity providers and/or identity consumers
T13	yes	Endpoints of the identity provider are accessible from firewalled environments and networks (e.g. they run on port 443 and use TCP/IP, which is mostly open to permit HTTPS traffic)
T14	yes	SDKs and/or APIs and/or SPIs (incl. provided and/or required interfaces) are available or interface implementation facilities (e.g. read/write data access) are available to interface with external services, e.g. with KYC registries such as those of SWIFT [74] or AML services such as those of Swiftdil [75]
T15	yes	Standards for Distributed IDs (DIDs) and Verified Claims (VCs), see Sec. II-F, are supported
T16	yes	Traffic to and from the identity provider is protected at the network protocol level (e.g. using TLS 1.3, which also permits authenticating the client to the server at the protocol level)
T17	yes	Trusted/audited protocolling of read and/or write accesses to identity and services in the operations backend
T18	yes	Support for lifespan limitation and credential rotation
T19	yes	Support for identity rollout ("push") onto managed devices and for remote removal from these device
T20	yes	An independent authoritative registry for lookup and validation by any participant
T21	yes	Continuity management and risk mitigation (e.g. SLAs and asset release in case of bankruptcy)
T22	yes	Relevance of quantum cryptography to the security of the implementation has been studied
T23	yes	Suitability for identities of non-human entities (e.g. organizations, roles, things, machines, animals)
T24	no	End users (and not just companies) can participate in the consensus (by running a full node) and/or can run a light node
T25	no	Source code inspection by customers is possible (e.g. through open-sourcing of the code)
T26	no	Source code verification by independent third parties is being performed (e.g. on each release), with network-sponsored financial rewards for the "white-hat" discovery of bugs
T27	no	Import of third-party certificates (e.g. X.509), keypairs and claims is possible
T28	no	Trust hierarchy (comparable to root CAs and intermediate CAs for X.509 certificates) can be established
T29	no	Proactive online lookup on every usage of the identity, e.g. using revocation lists
Number	**Mandatory?**	**Criterium description**

Blockpass is implemented on the basis of Ethereum and the proprietary PASS token (which powers the ecosystem) is therefore an ERC-20 Token; Blockpass offers a JavaScript SDK but no standards-based IAM APIs. In addition to the app and the certificates, there is an automated verification system, the KYC admin platform and the actual ID keys.

While using a blockchain technology implies some decentralization, the architecture of BLOCKPASS explicitly includes a central server, which is, at best, only an intermediate stage towards a sovereign identity. Even more surprising, the USERID is generated by the server (which stores a truncated version to "the blockchain") - and the USERID is not the keypair (which is generated on the user's mobile device). The relation between the keypair and the USERID is not made explicit in the whitepaper.

The end user interfaces with BLOCKPASS via a mobile app (iOS and Android only; no web app or other OSes offered). It explicitly offers only one identity per person, bound to an email address (it is unclear whether that email can be exchanged). The email is verified, but no MFA using text messages or OTP apps is offered. Also, at the time of the survey, no password recovery function was offered and only two verifying services are available: passport data validation (supplied by Onfido.com, which is a separate service of its own) and a service that checks sanction lists.

These verification services work by taking the user-supplied profile data and issuing certificates. However, it is unclear (from the app) whether these certificates or any other data are stored on the blockchain. While one free verification is provided for each of the two services, it is unclear how much a re-verification (e.g. when changing a surname after marriage) would cost. But even more importantly, the app does not state explicitly what happens to the supplied data.

To access a service which makes use of BLOCKPASS' KYC/AML functionality, the user has to scan a QR code from the mobile app. However, neither the app nor the website nor the whitepaper provides a list of such services. At the end, it is unclear what exactly constitutes BLOCKPASS' advantage

TABLE IV
COVERAGE OF EVALUATION CRITERIA BY AN ESTABLISHED ENTERPRISE-GRADE IAM SOLUTION (MICROSOFT ACTIVE DIRECTORY); MANDATORY CRITERIA ARE SET IN **BOLD**

Offering	CL01	CL02	CL03	CL04	CL05	CL06	CL07	CL08	CL08a / CL08b / CL08c	CL09	CL10	CL11	CL12
MS AD	yes	yes	yes	n/a	n/a	yes	yes	all four	yes / yes / yes	yes/yes	n/a	no	yes

Offering	**U01**	**U02**	**U03**	**U04**	**U05**	**U06**	**U07**	**U08**	**U09**	**U10**	**U11**	**U12**	**U13**	**U14**	**U15**	**U16**
MS AD	**yes**	**yes**	**yes**	**yes**	**yes**	**yes**	**yes**[i]	**n/a**[ii]	**n/a**[iii]	**yes**	**yes**	**yes**	**yes**	**yes**	**yes**	**yes**[iv]

Offering	U17	U18	U19	U20	U21	U22	U23	U24	U25	U26	U27	U28	U29	U30	U31	U32
MS AD	no	no	yes[v]	*no*	n/a[vi]	n/a	yes	n/a	yes	no	yes	no[vii]	yes	yes	yes	no

Offering	**T01**	**T02**	**T03**	**T04**	**T05**	**T06**	**T07**	**T08**	**T09**	**T10**	**T11**	**T12**	**T13**	**T14**	**T15**	**T16**
MS AD	n/a	n/a	n/a	n/a	n/a	n/a	n/a	**yes**	n/a	n/a	**yes**	**yes**	**yes**	**yes**	n/a	**yes**

Offering	**T17**	**T18**	**T19**	**T20**	**T21**	**T22**	**T23**	T24	T25	T26	T27	T28	T29
MS AD	**yes**	**yes**	**yes**	**yes**	n/a	n/a	**yes**	n/a	n/a	n/a	n/a	yes	handled by the service provider

[i] Add-ins required [ii] X.509 client certificates with private and/or public keys can be exported; for centralized identity systems, a provider-managed export of credentials/entitlements is possible (e.g. for migration purposes), but client-triggered export of credentials/entitlements is not viable because the result's validity is questionable [iii] for centrally stored identities, only the "keys" to that identity are stored on end-user devices; for AD identities, these "keys" (e.g. passwords or certificates) can be synchronized across devices and backed up [iv] through add-ins, e.g. by sending certificates with public keys [v] can be created through AD Certificate Services, to be installed on demand [vi] users have no direct control in a centralized IAM setup [vii] only available through formal agreements and governance

over "conventional" KYC as with Onfido.com and others - the identity offered by BLOCKPASS is currently not of much value to the end users.

C. Bloom

Bloom [84] describes itself as an "end-to-end protocol for identity attestation, risk assessment, and credit scoring". It offers a self-sovereign ID platform based on Ethereum (incl. state channels for better scaling) and IPFS; iOS and Android apps are provided. Intra-network payments, incentives and governance are implemented using the proprietary BLT token. The Bloom website does not list any customers or integrations.

D. Cambridge Blockchain

"Cambridge Blockchain" [85] advertises a solution (though not a named product) that is touted as a simplification for identity compliance. It is described to be based on a private, permissioned blockchain (though no specific technology is specified, and the implementation is neither explained nor downloadable). Its solution is claimed to address KYC and privacy laws by using attestations (from trusted parties), where the attestations are given to the service provider by the end user, rather than by other third parties.

From the information on the homepage, it remains unclear how the implementation balances the visibility of blockchain-stored data ("transparency", as some data is provided to the regulators) with the privacy demands of end customers. The website also mentions a "marketplace for identity services" yet does not explain who will assume the seller's role. There are some mentions of a blockchain-based "Enterprise Data Management" software by the same startup, but this is not explained any further.

The company has partnered with some prominent players such as IHS Markit, LuxTrust (see below), Infrachain (see below) etc. Overall, the website of "Cambridge Blockchain" lacks in-depth information. However, our research has revealed that the company has patented its approach (US9667427B, EP3234878A1 etc.).

E. Civic and Identity.com

Civic [86] self-describes its offering as a "Secure Identity Ecosystem" and with >90 integrations (incl. ICOs), it has one of the largest partner bases in the market segment of blockchain-based identities. Venture-funded with over USD 30M from several investors, Civic works towards commercial viability through service fees (rather than software sales): the service provider ("requestor" in the KYC process) must use a wallet with the proprietary, ERC20-based CVC 'token'.

Civic claims that its app helps to control and protect identities while using biometrics (in fact, fingerprints or Apple's Face ID) and blockchain on a mobile device. Civic is designed in a way that the identity data resides on users' mobile devices, and not on Civic's infrastructure; thus, identity data must be exchanged directly between a Civic user and a service provider (or, similarly, between a Civic user and an authenticating authority). Civic itself is also not an authentication authority, so it cannot revoke or invalidate identity assertions or data. GDPR compliance of Civic is neither confirmed nor negated.

Civic defines a "verified identity" for password-less logins and MFA. The technology (which includes "Secure Private Sign-up" and "Secure Private Login" as well as a separate KYC module) is based on hashed identity data, a public identifier for the authenticating authority, and a flag (also on the Ethereum blockchain) indicating the data is still valid. The authenticating authority can also "revoke" (i.e. invalidate by a new blockchain transaction entry) an identity assertion which has become obsolete – provided that the authenticating authority is indeed aware of the changed circumstances. For KYC based on "conventional" ID documents, an OCR-based functionality alongside a plug-in mechanism and a marketplace are envisioned.

Identity.com [87] is a sibling if Civic, “an open source ecosystem” for “on-demand, secure identity verification”. The offered components and libraries cover all roles in the Civic process. Identity.com explicitly states that as the number of participants grows, Civic will “stop being the only player in the ecosystem”.

No peer-to-peer interaction between end users is currently available in Civic. There are no imports of existing identities; other authentication options (e.g. NFC-enabled identity cards) are not supported. Additionally, certain aspects in the Civic app raise questions about privacy and reliance on “conventional” technologies. For example, to log in with the “Civic Secure ID”, a user needs a username and a password; a “primary email address” and a mobile phone number also need to be specified, and a confirmation SMS has to be received. Finally, identity checks require internet access. Like most of blockchain-based competitors, Civic does not offer any import of synchronization opportunities with other identity providers. Support for app-less identity use and storage is not offered.

F. Colendi; Datum; Decentralized Identity Foundation (DIF); Dock.io; Dominode; EDDITS

Colendi [88] describes itself as a blockchain-based “credibility evaluation and global identity for the sharing economy”. It is built on Ethereum and provides Android and iOS apps; GDPR compliance is clearly not given due to the fact that the users’ contact data cannot be deleted since it is replicated and permanently stored on the DLT. The open-sourcing of the smart contracts is announced for 2019. So far, the homepage does not advertise any partners or third-party integrations.

Datum [89] is a system for “Blockchain Data Storage and Monetization”, based on a proprietary blockchain and featuring custom utility tokens (DATs) as well as a marketplace. The mobile app is initialized by creating a “sovereign ID”, even though the official whitepaper does not mention this, only remarking that “Users can link their data to their verified identity such as uPort or Civic”. In fact, identities in Datum are simply keypairs, with seed-based recoverability. Beyond the app, no ready-to-use integrations or products are available.

The Distributed Identity Foundation [90] (DIF) has published drafts/standards for identity attestation, self-sovereign identity and data, and discovery in the absence of a centralized directory. One of the key focus areas for DIF are decentralized IDs (DIDs [91], [92]), and the associated tools. As of April 2019, work is underway to make DIDs (which are rather complex) a W3C standard. At the same time, actual tool support for DIDs and associated “universal resolvers” is in a very early stage; uPort (see below) makes some use of DIDs.

Dock [93] is a decentralized, Ethereum-based data exchange protocol. It is one of the offerings that promise that the end users can “take back control” of their data, and of how it is being shared. Dock requires a proprietary token (DOCK), and promises to uncover “all the places where [the user’s personal] information lives”. Seamless (i.e. password-less) login is available – but only to the offerings which participate in the Dock blockchain network. While [93] claims to have more than 1 million users and promises a REST API as well as GDPR compliance, there is no publicly released smartphone app and only less than 10 partners (mostly hiring websites) are named on the homepage.

Dominode [94] describes itself as a reinvention of “regulated identity”, which means a verified and trusted identity. The website mentions permissioned access to a global business network, and a few other technical details as well as use cases. However, no further details or apps were published at the time of the survey.

EDDITS [95] stands for “Ethereum Decentralized Digital Identity & Trust Services”, and it includes a DApp that allows the users to manage their ERC-725 identities. EDDITS is an offering from a cooperation with the (conventional/PKI) trust center run by the Post authority of Luxembourg. The prototype implementation links the trusted, “conventional” X.509 certificate to the blockchain through a Smart Contract, which parses and verifies a standard RSA signature and issues a claim (using ERC-725/ERC-735). At the time of the survey, EDDITS was a prototype that could be used from a Web3-enabled web browser, which is usually done by adding MetaMask [96] plugin to a conventional Web browser. Key recovery and other features are not yet covered by EDDITS.

G. Enigma

Enigma [65], [97] strives to address two shortcomings of blockchain technology (lack of privacy and issues with scalability/throughput) by an innovative approach: “input data is kept hidden from nodes in the Enigma network that execute [smart contract] code”. The Enigma privacy protocol performs a decentralized computation of sensitive data in the sense that data is encrypted using JavaScript on client-side device, so that data is not sent in cleartext to remote blockchain nodes even though these nodes process data from the client.

Technically, Enigma is a permissionless P2P network, with “secret contracts” and “strong correctness and privacy guarantees”. The contracts run in a modified Ethereum Virtual Machine, making use of a Trusted Execution Environment (TEE), based on Intel’s SGX [98] technology. However, SGX has already been exploited [99] the reliance on it raises the question on malicious modification to the EVM/TEE. The key highlight of Enigma is that the SGX-based secure enclave of the “worker node” and the client’s local environment directly negotiate a shared trusted secret using elliptic curve cryptography, although both operate in untrusted environments. Using the negotiated secret, the worker’s secure enclave can decrypt the client’s input - at the same time, all data processed by other blockchain nodes (and outside the enclave) remains encrypted.

As other approaches, Enigma hopes to monetize data (in the areas of IoT, financial services, healthcare etc.) without selling or disclosing the actual data. As Ethereum, from which it is derived, Enigma has incentives to “power” the node-side computation. It is technically possible to set up Enigma in a private/consortial environment. When applying source code changes to the Enigma implementation, the GNU AGPL open-source license means that the changes *must* also be open-sourced under the AGPL even if the changes are not published.

At the time of the survey, 3 years after Enigma was first described in a PhD thesis, the first and only application built on it is Catalyst [100], a "revolutionary platform for data-driven cryptoasset investing". Also, being a platform and a protocol, Enigma does not per se offer IAM services: it offers technical means to *implement* such functionality.

H. FinID.me; Ethereum ERCs, ERC725Alliance and Enterprise Ethereum Alliance; Gemalto Trust ID Network; IBM Trusted Identity; ID2020

FinID.me [101] brands itself as "Blockchain powered eID", as a trusted services provider and claims compatibility with EU regulations (which would be eiDAS and GDPR). FinID webpage mentions the provision of an eiDAS Qualified Electronic Signature and the use of Ethereum ERC-725 and ERC-735. No further information is provided, and no implementation (or smartphone apps) were available during the survey.

ERC-725 [102] is a well-known "Ethereum Request for Comments" (i.e. a proposed standard) for "proxy identities". Other identity-relevant ERCs include ERC-735 [103] and ERC-1484 [104]; these ERCs add claim management and other central capabilities to the sovereign identity. There is even a dedicated "ERC725Alliance" [105] which functions as an online community for this area of interest; some of the offerings using ERC-725 (e.g. Ethereum DApps) can be found there as members. A part of the products in this survey (such as uPort) use ERC-725 as an element of their stack. However, ERC-725 per se is only a UI-less collection of Solidity functions (for public or private blockchains). The contract state must be instantiated for each identity, be it through an API call (e.g. web3js) or through a separate UI (usually a wallet-like end-user application).

The Ethereum Enterprise Alliance (EEA) [106] is a consortium of companies to drive the enterprise adoption of the well-established open source Ethereum Blockchain. The EEA includes Special Interest Groups (SIGs) and Technical Working Groups (such as the "Digital ID Task Force"), but both are open to paying members only. The "Enterprise Ethereum Client Specification" was publicly released by EEA in May 2018 and includes provisions for private transactions, although no implementation of those has started yet.

The "Gemalto Trust ID Network" [107] is designed to support the transition from siloed identities to self-sovereign identities as well as to decentralized/federated identities. This network is built using R3's Corda [108] technology (which is a DLT but not a traditional blockchain). The press release mentions a mobile app as part of the oncoming pilot, but that app remains to be released publicly, and is not described in further detail. Gemalto also provides traditional technologies such as Identity-as-a-Service and Authentication-as-a-Service.

IBM Trusted Identity™ [109] is an approach that is based on Hyperledger Indy (see below) and W3C Verifiable Credentials standard (see Sec. II-F), building on IBM's involvement in the DIF and Sovrin foundations- Additionally, IBM has partnered with SecureKey [110] (a company that builds "trusted identity networks") and with Canadian authorities to field the technology of the attribute sharing in a real-world setting. At the time of the survey, IBM did not have an own distinct/branded product, app or a service to be purchased, but there is Verified.Me [111], which is an *announced* blockchain-based solution from SecureKey, based on Hyperledger Fabric technology to be built in partnership with financial providers, Gemalto and others. No technical details are provided about Verified.Me on the homepage or in social media.

ID2020 [112] is an alliance that sees portable, MFA-secured digital identities as a way to improve refugees' situation. ID2020 is supported by the UN, ITU and further agencies; its ecosystem's founding partners include Microsoft, Accenture and further companies as well as foundations. With an elaborate governance model and a manifesto, ID2020 takes a very systematic approach, incl. a stepwise selection of solution candidates. No implementation or architecture exists yet.

I. Idento.One; Jolocom; KYCLegal

Idento.One [113] positions itself as a broker between the user and the service provider. As of April 2019, the only source of information about Idento.One is their homepage; A whitepaper or technical documentation is not yet available there or on social media. The design maxim of Idento.One is that the user is given exclusive control and the private key over the data which is stored in a "safe" on the blockchain (i.e. encrypted). As the broker, Idento.One offers the user to "get the data back" from the service provider and into the safe, and afterwards to share only as much data as the user wants (or needs). At the same time, Idento.One offers "GDPR as a service" to the service providers, which would not need to store any data by themselves. Finally, the concept of Idento.One includes real-life validation of a digital identity.

Jolocom [114] proposes an open-source "Universal Identity Protocol" to create a self-sovereign identity on decentralized infrastructure, using the W3C DID standard. The Jolocom SDK provides a binding for Ethereum (though without using ERC-725 and similar standards), but the protocol is open for other blockchain implementations. During the survey, only an alpha Android version of Jolocom's SmartWallet app was available for testing; it includes a login functionality for websites, based on QR code scanning.

KYCLegal [115] is an offering that builds on smartphone apps which store the end users' data. End users control the data provision to services through this app, and login to websites (by scanning a displayed QR code). Separately, an app for the so-called "agents" is provided; the website says that the agent "receives reward for every verification". The apps are not universally available (for example, the iOS app is not available in Germany). With the ICO for the KEY.Legal token having finished in March 2018, no further deals, activities or publications have surfaced on the webpage or Twitter since then, and no technical information is available.

J. NameID and NameCoin

Namecoin [116] is an experimental open-source Bitcoin fork for the registration and transfer of identities (names) and key/value pairs (assets). Assets can include DNS entries, GPG keys, TLS certificates and other elements of the "decentralized web" and are attached to an identity. As its name implies, Namecoin is centered around a cryptocurrency coin (NMC) which requires an appropriate wallet, and which is sold at cryptocurrency exchanges but can also be mined. To use Namecoin's DNS-like infrastructure, specific client software must be installed and configured by the end user.

NameID [117] turns a Namecoin identity into an OpenID identity – OpenID [118] is a blockchain-independent standard. NameID promises easy login into *any* of the OpenID-enabled websites. For example, to login into NameID, a challenge message must be locally signed in the NameID software, using the private key; a Mozilla browser plugin is available to simplify the workflow. The OpenID server can be used for free; this does not cover the end user's expenses to set up the Namecoin identity.

The distributed network of Namecoin serves as the ledger recording the attributes of the identities. However, the NameID infrastructure itself is centralized: the OpenID "core" runs on the NameID infrastructure – not on the device of the end user, and not on any Bitcoin-like distributed network. Thus, NameID sees all the sites which the user is logging to using OpenID (this is openly acknowledged in the FAQs). At the same time, every user can set up a clone of the NameID infrastructure using the source code of the project.

K. ObjectTech; Passport ID; PeerMountain; Persona.im; Pillar; Rate3; VETRI and eID+; SelfKey

ObjectTech [119] strives to combine AI, biometrics and blockchains for seamless travel, resulting in "fully verified digital wallets" and "digital passports". The website of the UK-based claims that the product will be fully compliant with GDPR, PSD2 [120] and similar privacy/security regulation. However, neither the website nor the social media channels provide any technical details or independent reports.

Passport ID [121] is a blockchain-based approach to a trusted ID: "Once identity information is provided by a user, Passport.io Team authenticates submitted data against public records and available information to verify legitimate customers. [...] We provide notary nodes to government agencies and trusted companies around the world to verify identities of Passport.io accounts." Services for identity-using businesses are announced as well. While an iOS app is provided, neither source code nor developer documentation is publicly available, not even after a "Personal Passport" is created online. Likewise, the website does not list any corporate customers or integrations.

PeerMountain [122] promises an ecosystem that includes sovereign identity and that is built on Ethereum-based PMTN utility token (as of April 2019, the token sale is ongoing). The website mentions European patent 17195509.9 as the underlying principle and also states that "it is our intent to release the Peer Mountain client SDK for Android and iOS as open source, and to open-source the Peer Mountain Attestation Engine SDK". However, despite an abundance of well-made illustrations and a whitepaper, there is neither a publicly released app nor a running node (or source code) to try or to analyze.

Persona.im [123] describes itself as a "zero knowledge digital identity management system built on blockchain". In Persona.im, a "web of trust" involves individuals to add validation/verification to an identity; each validation contributes 5 % (independently of the validator's renommee), up to a max. total of 90 %. For additional one-time 10%, a monetary transaction needs to be performed. The homepage of Persona lists some interesting use cases: e.g. cryptographic signing of news, to prevent fake news (though this case can also be accomplished with conventional PKI). As of April 2019, Persona has released the Betas of the trust protocol and of the wallet application (macOS, Linux, Windows); IPFS is used for file type attributes uploaded on the public Ethereum test-net. Persona introduces a proprietary, exchange-traded token (PRSN), and their website features a web-based transaction explorer. With only 1-3 commits per month, the public Github repository shows very low activity.

Pillar [124] is a project that aims to give the personal data ownership back to the users, but at the time of the survey, it was simply an open-source wallet for cryptocurrencies and tokens, funded by an ICO. The "data locker" functionality with some identity management is on the roadmap for 2019. According to the website, Pillar already has 60 employees.

Rate3 [125] is a tokenization protocol, fueled by the proprietary RTE utility token. Rate3 includes identity management based on Ethereum (or Stellar) public blockchains, but only internally and as much as is needed for Rate3 itself. There is no smartphone app or UI for the end users.

VETRI [126] by Procivis is an approach for sovereign identity and "getting rewarded" for one's personal data, centered around a wallet and a marketplace. VETRI is fueled by the proprietary VLD token; at the same time, the platform self-describes as "not-for-profit". At the time of the survey, only the VLD token, a white paper and a roadmap were available – a product or an app were not available for end users. eID+ is the second offering [127] by Procivis in the IAM market area and it also uses blockchain protocols/standards for some tasks; the website includes the documentation of its architecture, but the app is only available as an on-request demo. For eID+, the FAQs say that "Pilot projects are already under way and clients have been secured", but no testimonials from an independent third party have been published yet.

SelfKey [128] is a self-sovereign approach which promises users "full ownership" of the digital identity. It is based on a wallet application, which is a macOS/Windows desktop solution (unlike many competitors) and can also manage other Ethereum tokens (and the ETH accounts). The self-created identity (stored on the local computer only) can be enriched with data from passports, driving licenses, and self-taken photos. The SelfKey approach relies on an own marketplace, with the promise that the user will be able to "instantly apply for Financial, Cryptocurrency, Corporate and Immigration Services". However, these services would only be accessible if the user possesses the KEY tokens which SelfKey uses to finance itself. Additionally, a trusted verification of the identity is needed. At the time of the survey, all services in the SelfKey marketplace were demos.

L. ShoCard and ShoBadge

A ShoCard [129] identity is created on the smartphone in the ShoCard app, where it is passcode-protected and encrypted. Optionally, a conventional ID card can be scanned so that the textual details can be recognized from the ID card - but this does not "upgrade" the ShoCard ID. Additionally, bank cards and loyalty cards can be added to the app. The setup includes MFA and so does the app usage.

ShoCard's selling point is to eliminate the username / password authentication, and to provide the end users with better control of their personal data. As with other "novel" IAM offerings, it remains to be studied whether "one credential for many services" (as with SSO, client certificates and other technologies) is more secure than individual, MFA-secured, rotated and repetition-checked credentials. The four-digit ShoCard app passcode might be a long-term risk, in particular when it is not rotated.

ShoCard servers (not the app itself) place the identity onto a blockchain - yet not the encrypted full identity, but a hashed and signed "footprint" of it. When a user needs to share the information with a third party, the particular information is encrypted (to be decrypted by the destination only) and placed onto the blockchain. Whether placing such PII on the public blockchain is a long-term, GDPR-compliant solution is not fully clear. ShoCard app data can only backed up to Dropbox (but not to local phone storage, and not to the default backup location of the user's smartphone, e.g. onto the Apple iCloud). Companies can use the SDK to integrate the ShoCard technologies into their frontend and backend implementations.

When it comes to "trusted verification" of the user's identity (e.g. by an authority), ShoCard places the "trusted identity" into the mobile app (since the identity data is released on a case-to-case base). At the time of the survey, ready-to-use "trusted authorities" are not yet listed by ShoCard. ShoCard publishes the costs on its homepage, which makes it stand out from the competition; a free trial is also available. KYC and AML (based on driver's license or a passport) are billed separately, biometrics-based facial recognition (not just for iOS) and phone support are available for some packages.

In addition to the ShoCard app and technology, the company also offers ShoBadge, which it touts as "the next generation of enterprise-level identity authentication" and even as "the most secure identity management system available" (the information whether ShoBadge has been independently audited or certified is not available).

As with other blockchain-based, smartphone-oriented offerings, it remains unclear how a multi-device, multi-profile setup will work for ShoCard. Many (if not most) users use several devices: not just a smartphone, but also a tablet, and often a portable computer. Sometimes, these devices are kept in sync (e.g. in the Apple ecosystem) and so are the identities on these devices: for example, the built-in "password safe" of Apple devices is synced over iCloud (it is claimed that the data is encrypted by the user password in such a way that even Apple cannot decrypt it). Such central, cloud-based synchronization makes it rather easy to onboard new devices, and to wipe data from lost or stolen devices (a function that is also often found in EMM software). In contrast to cloud-based offerings, ShoCard does not offer any inter-device synchronization, or even Dropbox-less device migration: ShoCard data cannot be exported to any secondary or on-device storage, let alone in a human-readable way.

ShoCard claims that its technology will "invert identity management to be controlled by each user and shared with the workplace" - but there is still the need for a verifier of an identity to turn it into a trusted, authenticated identity. And authorization is still being performed at the service provider side - thus, identity management will continue to be split between the end user and the service provider (as it is today, where the end users are responsible for maintaining the shared secrets behind their identity).

However, even with ShoCard, the service provider can withdraw the end user's access to a service. The major difference is that the end users still can maintain their "audit trail" (the trusted history of interactions and attestations) because that trail cannot be simply deleted by the service provider. But the end user is not fully self-sovereign since ShoCard, as any technology, must permit the service provider to withdraw an attestation, e.g. because an error has happened or because the user did disqualify. In a WORM-based technology, this can be done by appending a new entry to the audit trail. Still, if the ShoCard approach evolves to remove the dependency on company's own, and thus proprietary, infrastructure, it could qualify as a self-sovereign identity.

M. Sovrin, Hyperledger Indy and Evernym

Sovrin [130] is the open-source sovereign identity framework in the portfolio of the Hyperledger foundation, originally developed and donated by the Evernym [131] company through the Sovrin foundation. Sovrin makes use of the Hyperledger Indy [132] project (Indy stands for independent), which is in the "incubation" status. Sovrin/Indy employ decentralized identifiers (DIDs). The underlying blockchain is public but permissioned; it is a custom development (rather than Ethereum or a similar off-the-shelf product). There is no official/central Sovrin app available in the app stores for Android or iOS. Sovrin is well-documented, at different abstraction levels and with examples.

Nodes in the Sovrin framework are run by stewards (organizations), and stewards are admitted based on a formal written application. Nodes can be validator nodes, or read-only "observer" nodes. A steward's reputation has to be obtained and maintained by performing work activities for the Sovrin network from which the community will benefit. Sovrin stewards include companies from 4 continents and well-known market players such as IBM, Cisco and others.

In Sovrin, a person (identity) can use several identifiers, i.e. one for each service. The interactions in Sovrin are designed using pseudonyms ("cryptonyms") to minimize the opportunities for unwanted correlations. Architecturally, Sovrin takes an approach based on cryptographically secured verifiable claims, which (along with all private data) are stored off-ledger by each self-sovereign identity owner, wherever the owner decides. Sovrin documentation states that "no private information is ever stored on the ledger, in any form." Claims can be private or public; every Sovrin identity owner is enabled to issue claims about another identity owner or even about herself, but Sovrin stewards are regarded as a higher authority for claims issuance – especially when they have performed law-compatible KYC on the identity for which the claim is issued. The initial round of Sovrin stewards enjoys a particularly high reputation, they are denoted as "trust anchors". To reduce overhead, only a small subset of information is stored on the shared ledger; personal data is stored on "microledgers" (which capture bilateral information exchange between two participants). Further technical details can be found in the paper [133] by Khovratovich and Law.

An identity owner enters into a formalized "Identity Owner Agreement" with the Sovrin foundation, which is a US-based non-profit foundation. The agreement does not detail the compliance with GDPR and does not specify the jurisdiction governing any conflicts between the identity owner and the Sovrin Foundation (or with the members of the foundation).

Evernym (as a company) positions itself as a turnkey solution provider, as well as one of the node-hosting stewards in the trust network and a provider of backend tools for processing of claims. Luxoft [134] has integrated the blockless R3 Corda DLT with the identity management features of Hyperledger Indy. In 2017, a partnership with IOTA has been announced, later complemented by a partnership with MOBI [135]; further use cases are being implemented. The Sovrin community works on a governance framework for the stewards.

N. Sphere Identity; SpidChain; Taqanu; TENZ-ID; Tierion and Chainpoint

Sphere Identity [136] promised on its website that the product (a blockchain-based solution for self-sovereign identities) would launch in 2018. At the time of the survey, no technical details have been published, but one can sign up for the upcoming beta version (i.e. one is added to the waiting list).

SpidChain [137] promises a decentralized self-sovereign digital identity based on blockchain technology, described in a short whitepaper from 2017. At the time of the survey, no implementation or details were available.

Taqanu [138] is advertised as a decentralized blockchain-based self-sovereign identity for a "global ID" with an attestation framework. At the time of writing, neither a whitepaper nor any technical details were available.

TENZ-ID [139] by Tenzorum calls itself an "uncensorable, unstoppable identity on the Blockchain". TENZ-ID is an Ethereum-based open-source solution that consists of a "Blockchain framework for user-onboarding powered by a modular multi-signature key management system" and a "permissionless network protocol to reward delegated meta-transactions". Tenzorum strives to onboard ETH-less users onto the Ethereum blockchain, by allowing third parties to pay for the "Ethereum gas" needed to perform the transactions on that blockchain. At the time of writing, TENZ-ID was under development.

Tierion [140] calls itself a "Blockchain proof engine", with the message of lowering the "costs and the complexity of trust". Its flagship business product is called Proof [141], which -once it is launched- is set up to permit the verification of data, including a timestamp, using data written to the public Bitcoin blockchain. Proof's website claims that this happens "without depending on a trusted third-party", with promises such as "no need to trust authorities or middlemen" and "proofs are independently verifiable forever" (as of April 2019, competing offerings such as Bernstein [40] have been commercially available for quite some time). The underlying technology is called Chainpoint [142], and is an open standard for "linking data to the blockchain to create a timestamp proof". The website claims that the Chainpoint network provides more than 7000 nodes to connect to. Chainpoint is not specific to IAM, and there is a command-line application (open source, Linux/macOS only) to verify its proofs. So far, neither Chainport nor Proof.com provides technology or APIs for end-user identities.

O. uPort and Ethense

uPort [143] is an undertaking of Consensys, which is the organization behind such widely used Ethereum projects as MetaMask and Ethereum. uPort is an Ethereum-based "open identity system" that allows users to "register their own identity on Ethereum, to send and to request credentials, to sign transactions, and to securely manage keys & data". Selective data sharing is enabled through a dedicated smartphone app ("Self-Sovereign Wallet"); uPort also provides reusable components and protocols for developers.

There are private (smartphone-stored) and public (blockchain-stored) "claims", i.e. attestations (verified or open) about attributes of an identity, which form the "history" of an identity. At the time of writing, central parts of uPort were under continued development (e.g. the mobile SDK); uPort has announced that all of its code has been open-sourced. At the same time, several pilots have been reported (e.g. Protea [144] by Linum Labs), but *operational* websites or production-level services that do use uPort are almost non-existing, despite the project's visibility and activity.

The Swiss city of Zug has piloted a sovereign, uPort-based citizen ID which is restricted to that city's residents. In the pilot, the Zug authorities confirm that an identity indeed belongs to a resident of the city (the identity owner has to visit a branch office in person and has to present a conventional passport/ID card). The confirmation outcome is stored in the uPort app of the user, not on the public Ethereum blockchain (which serves as the "directory" layer for the keypairs used to sign the uPort attestations). However, as of April 2019 there were no continuous service offerings where the Zug citizen ID could be used; possible use cases are being evaluated but it is unclear when they will be available for the pilot participants. A test-wise digital ballot using the ID attracted 72 participants in June 2018, from a total city population of around 30.000. In December 2018, rentals of city bikes through the uPort app have been enabled in Zug.

Ethense [145] is another product from Consensys and is targeting the ecosystem of credentials such as university degrees or certificates of completion. Based on Ethereum and reusing uPort, it is a decentralized approach that is being piloted, and some parts of the code are open-sourced.

P. Verity, XAIN and others

Verity [146] brands itself as a framework for "universal trust, reputation, and credentials". As of April 2019, there is no whitepaper or any other information; the last post on social media is from May 2018.

XAIN [147] describes itself as "The Trusted Access Control Protocol for Machine Networks" that "leverages blockchain technology to increase trust & transparency between users and enterprises". XAIN was originally called "eXpandable AI Network" but has since shifted to developing technology that enables trust in decentralized human-to-machine interactions. XAIN implicitly administers machine identities but has no product or service that would include IAM for humans.

VI. Evaluation

A. Evaluation Summary

From the analysis of all the individual offerings in the previous section, none of the offerings satisfies all of the mandatory criteria that we defined in Tables I, II and III in Sec. IV.

Judging by maturity and adoption, the five most promising offerings are Blockpass IDN, Civic, ShoCard, Sovrin and uPort. Still, none of these fulfills *all* of the requirements from Section IV, and none has the maturity of conventional IAM offerings. Sovrin has a particular appeal as it is the only solution backed by a multi-vendor consortium, rather than a single company. Civic and uPort also strive to create an ecosystem, rather than just a component that can be reused.

For all of the offerings, the end-user relevance and market penetration are in very early stages. The vast majority of the offerings lacks standard-compliant interfaces (such as OAuth or SAML) to be integrated by service providers with the same ease as conventional IAM solutions. Even without such standards, none of the offerings can boast a production-level integration with a large user base.

B. Compliance and Liability

In terms of compliance and liability (cf. Table I), all of the studied offerings are in the very early stages. In particular, GDPR compliance (as guaranteed by Verimi and similar blockchain-less IAM solutions, cf. Section II-C), can only be offered by running a permissioned consortial network where the location of the blockchain nodes is strictly regulated. For the Sovrin network, there is a series of articles covering GDPR in details, but no guarantees are given. None of the solutions is certified by a trusted third party (such as TÜV).

C. End User Experience

From the end user experience, it is our impression that the current approaches to self-sovereign identity repeat the path once taken by PGP, i.e. peer-to-peer and decentralized exchange of identity information. However, we found that all of the studied offerings have no compatibility with PGP or with the widely established X.509 certificates. Thus, it is questionable whether the blockchain-based approaches will be able to compete with established players, unless the entry barriers for end users are minimized. In particular, we believe that OS-level support for identity standards is vital. Furthermore, we believe that support for multiple identities with the same vendor, and concurrent usage on multiple devices, are what end users have come to expect in the blockchain-less sphere.

D. Technology, Implementation, Integration and Operations

Technologically, we found that the inherent properties of DLTs and blockchains offer not only new opportunities, but also pose limitations. Most prominently, where the WORM principle prohibits deletion of data from the ledger, personal data must be kept off-chain, which severely limits the usability of the ledger. Taking core identity data off-chain means that not only private keys (cleartext/encrypted/hashed) are the responsibility of the end user, but also the assertion and claims. We believe that vendor-specific apps are not a long-term answer to this challenge, and OS-level integration as well as interchange formats are a better solution.

In an enterprise setting, the existing IAM infrastructure is the essential centerpiece for users and applications. Very often, it is based on Microsoft Active Directory running in a fault-tolerant, multi-server setup (on-premise or in the cloud). For large and mission-critical installations, it is *currently* unrealistic to fully replace such an installation with a blockchain-based solution in the near term. Therefore, the blockchain-based solution (e.g. for sovereign identity) must be integrated into such a landscape. None of the studied offerings has a concept or a roadmap for this important task.

E. Support for Mobility and Mobile Devices

The concept of sovereign identity is often implemented by providing the end user not just with the *control* of the identity, but also with the *storage responsibility* for the identity. The most obvious choice for storing an identity is a mobile device: portable, better protected against malware and viruses than a personal computer, and often with biometric protection. By introducing the criteria U03, U06, U09, U13, U14 and T19 (see Sec. IV), we also thematize the issues related to mobility. For example, most vendor-specific apps for blockchain-based and/or sovereign identities support only one identity on a device, without the possibility to switch or logout/login - a restriction (cf. criterion U14) that does not have to exist.

Support for blockchain-based identity solutions in mobile devices goes beyond providing an offering-specific smartphone app, and should ideally be found natively in the layer of the operating system or in a mobile browser (see Sec. II for details). It should be noted the the "secure enclave" functionality is not used by any of the studied offerings. In contrast to that, blockchain products such as R3 Corda are already making used of the Intel SGX functionality on desktop/server CPUs.

At this point, we acknowledge that it is clearly possible to create a more extensive set of evaluation criteria incl. extra-functional attributes such as app performance, app responsiveness, user comfort, etc. However, these criteria would imply a *quantitative* app analysis which would require a large study of its own, an endeavour that would not fit the scope of this paper and would require test automation as well as a very large amount of resources.

A broad peer-reviewed set of evaluation criteria for *any* type of mobile apps could also be applied to the subcategory of identity apps - however, researching such a catalogue did not bear any fruits. The closest match are comparisons of app development frameworks, but these fall short of our needs.

The challenge of *evaluating* the "mobility" aspects of blockchain-based identities lies not only in the quick innovation and renewal cycles of both the apps and the devices, but also in the subjectivity of important user experience factors. Controlled experiments and user surveys are possible research approaches, but they cannot be accomodated in this paper.

F. Performance and Overhead

Performance and overhead are clearly a concern for blockchains and DLTs, and independent benchmarking research is already delivering first in-depth results [149] and tools [150]. In contrast to that, we have found very few reliable *quantitative results* for identity management solutions based on DLTs. In a bug-tracking entry [151], the developers of Hyperledger Indy/Sovrin study the stability under the following load: average sustained throughput of 10 write transactions per second and 100 read transactions per second (the ledger is pre-loaded with 1 million transactions, there are 25 steward nodes with 1000 concurrent clients). The results of the study are mixed, and response times are not specified.

In [50], durations of two simple actions (claim attestation and claim verification) are measured for a set of five research-grade implementations of zero-knowledge proofs. However, this ArXiv report encompasses only a tiny section of the workload that would arrive at a blockchain-based identity solution. Beyond that, we have not come across quantitative statements for any of the studied offerings, neither for overhead nor for performance in general. Also, peer-reviewed research on these subtopics appears to emerge only slowly. We expect an increased interest when the usability of blockchains for IoT identities will be studied, and when scaling issues will need to be tackled for real-life deployments.

G. Current Research Priorities

We found no dominating topic(s) that would be the primary research priority across a substantial number of projects. Possible candidates would have been zero-knowledge proofs, GDPR, homomorphic encryption, and minimization of runtime overhead. However, it appears that many startups have not acquired enough funding to go beyond the initial round or a Minimum Viable Product (MVP).

For the larger projects, such as Sovrin, we see substantial activity at performance and platform stability level (somewhat surprisingly, discussions are underway to replace the Sovrin's underpinnings, incl. the consensus algorithm implementation). Outside of Sovrin, we expect to see research on large-scale hybrid deployments in the areas of e-government and eIDs (electronic ID documents).

VII. Conclusions and Future Work

Sovereign and decentralized identities have been created to counter the perceived limitations of centralized, conventional IAM systems. Envisioning ecosystems and networks with fewer middlemen, this novel approach must compete with established application landscapes and identity providers.

The underlying blockchain technology is both promising and complicated, and the adoption of blockchain-based IAM has been quite slow despite high expectations and claims of disruption and progress. To succeed, the novel identity approaches must provide substantial benefits to *both* end users *and* to service providers. These benefits can include security, ease of use, data protection, transparency, and also cost reduction – taking into account the costs for migration and user training.

In this paper, we have established an extensive structured set of 75 evaluation criteria for assessing blockchain-based IAM solutions. Following these criteria, we have evaluated 43 offerings. We found that the analyzed products have not only very different levels of maturity, but also that only a couple of them *could* compete with the established blockchain-less solutions when it comes to end-user convenience. Most solutions lack a clear business model required to run a multi-node network over prolonged periods of time.

Concerning the compliance and enterprise-grade aspects (such as liability, integration into application landscapes, continuity management etc.), the high maturity of conventional IAM solutions is not yet found in the blockchain-based IAM solutions and offerings. PKI infrastructures (especially in enterprise environments) are very sophisticated when it comes to SSO, credential rotation and revocation, document signing, email security etc. For the decentralized and sovereign identities, such sophistication remains a very large challenge.

The unique selling point of the decentralized approaches is the avoidance of a central "data broker", which could misuse or sell the end users' data at discretion. In blockchain-based approaches, the central broker (organization) is replaced by a central network, albeit one which is run by several parties/companies - which may or may not form a consortium. However, in practice, many end users strive to isolate the services they use from each other; usually through non-intersecting sets of credentials. As the password management capabilities of devices and operating systems improve, this managerial task becomes easier and almost automated. Whether Decentralized IDs can achieve a similar convenience effects and user acceptance remains a research question. It should be noted that conventional, blockchain-less technology (such as PGP) already includes the foundations to enable peer-to-peer trust assertions and decentralized cryptography.

When it comes to verified identities, the already-established blockchain-less IAM solutions (such as conventional accounts) can be extended to "trusted" identities by adding a law-compliant trusted authentication, i.e. through eID cryptography, video authentication, PostIdent [152], WebID [13] or similar. Therefore, verification of identities cannot be seen as a unique value proposition of blockchain-based identities.

As part of our future work, we plan to extend the evaluation criteria to identities for machines and things, i.e. to IoT. We also plan to develop an improved concept for blockchain-based identities, which combines the best of the existing and novel concepts, and which is based on a GDPR-compliant ledger that permits consensus-based, audited data deletion and updates.

Acknowledgments

Moritz von Bonin, Patrick Charrier, Cemil Durak, Sebastian Kemper and Malte Plescher provided valuable feedback and suggested improvements to the text.

References

[1] OAuth 2.0. [Online]. Available: https://oauth.net

[2] "2018 reform of EU data protection rules." [Online]. Available: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

[3] N. Eichler, S. Jongerius, G. McMullen, O. Naegele, L. Steininger, and K. Wagner, "Blockchain, data protection, and the GDPR," Blockchain Bundesverband e.V., Tech. Rep., 2018. [Online]. Available: https://jolocom.io/wp-content/uploads/2018/07/Blockchain-data-protection-and-the-GDPR-_-Blockchain-Bundesverband-2018.pdf

[4] "First Hospital GDPR Violation Penalty Issued: Portuguese Hospital to Pay €400,000 GDPR Fine." [Online]. Available: https://www.hipaajournal.com/first-hospital-gdpr-violation-penalty-issued-portuguese-hospital-to-pay-e400000-gdpr-fine/

[5] "Trust Services And Electronic Identification (eID)." [Online]. Available: https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

[6] "The German National Identity Card (nPA)." [Online]. Available: https://www.personalausweisportal.de/EN/Home/

[7] SAML 2.0. [Online]. Available: https://www.oasis-open.org/standards

[8] "OneLogin." [Online]. Available: https://www.onelogin.com/pages/identity-as-a-service-idaas

[9] "Verimi." [Online]. Available: https://verimi.de/en

[10] "netiD Login Standard." [Online]. Available: https://netid.de

[11] "id4me Login Consortium." [Online]. Available: https://id4me.org

[12] OpenID Connect. [Online]. Available: https://openid.net/connect/

[13] "WebID Identity Company." [Online]. Available: https://www.webid-solutions.de/en/

[14] "OPEN IDENTITY EXCHANGE." [Online]. Available: https://www.openidentityexchange.org

[15] "Global Privacy and Security By Design." [Online]. Available: https://gpsbydesign.org/who-we-are/

[16] "IDPro by Kantara." [Online]. Available: https://idpro.org

[17] "Secure Technology Alliance." [Online]. Available: https://www.securetechalliance.org

[18] "FIDO Alliance." [Online]. Available: https://fidoalliance.org

[19] "Self-Sovereign Identity Working Group." [Online]. Available: https://blockchainhub.net/self-sovereign-identity/

[20] "Verifiable Claims Data Model and Representations." [Online]. Available: https://www.w3.org/TR/verifiable-claims-data-model/

[21] "OCSP." [Online]. Available: https://tools.ietf.org/html/rfc2560

[22] "Aadhaar Online Services." [Online]. Available: https://uidai.gov.in

[23] "e-identity of Estonia." [Online]. Available: https://e-estonia.com/solutions/e-identity/id-card/

[24] "Gemalto eID programs." [Online]. Available: https://www.gemalto.com/govt/identity

[25] "X.509 standards." [Online]. Available: https://www.itu.int/rec/T-REC-X.509/en

[26] "GSMA Mobile Connect." [Online]. Available: https://www.gsma.com/identity/mobile-connect

[27] "DID (Decentralized Identifier) Data Model and Generic Syntax 1.0." [Online]. Available: https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/draft-documents/DID-Spec-Implementers-Draft-01.pdf

[28] "LDAP." [Online]. Available: http://www.openldap.org

[29] "Open Badges v2.0." [Online]. Available: http://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/index.html

[30] "ISO/IEC 24760-1:2011." [Online]. Available: https://www.iso.org/standard/57914.html

[31] "ISO/IEC 29115:2013." [Online]. Available: https://www.iso.org/standard/45138.html

[32] M. Gray, "Ethereum Blockchain-as-a-Service now on Azure." [Online]. Available: https://azure.microsoft.com/es-es/blog/ethereum-blockchain-as-a-service-now-on-azure/

[33] "PGP." [Online]. Available: https://www.pgp.com/

[34] "OpenPGP Message Format." [Online]. Available: https://tools.ietf.org/html/rfc4880

[35] "GnuPG: the GNU Privacy Guard." [Online]. Available: https://gnupg.org

[36] D. Wilson and G. Ateniese, "From pretty good to great: Enhancing PGP using bitcoin and the blockchain," *CoRR*, 2015. [Online]. Available: http://arxiv.org/abs/1508.04868

[37] P. F. Costa, "Ethereum blockchain as a decentralized and autonomous key server: storing and extracting public keys through smart contracts," Ph.D. dissertation, University of Bologna, 2017. [Online]. Available: http://amslaurea.unibo.it/14306/

[38] Ethereum. [Online]. Available: https://www.ethereum.org

[39] Hyperledger Fabric. [Online]. Available: https://www.hyperledger.org/projects/fabric

[40] "Bernstein.io." [Online]. Available: https://www.bernstein.io

[41] "HTC Exodus." [Online]. Available: https://www.htcexodus.com/eu/

[42] "Sirin Labs Blockchain Smartphone." [Online]. Available: https://www.htcexodus.com/eu/

[43] "3 fake Bitcoin wallet apps appear in (and are quickly removed from) Google Play Store." [Online]. Available: https://blog.lookout.com/fake-bitcoin-wallet

[44] "The DAO, The Hack, The Soft Fork and The Hard Fork." [Online]. Available: https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/

[45] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, "Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 4-2, pp. 1735–1745, 2018.

[46] A. Grüner, A. Mühle, and C. Meinel, "On the relevance of blockchain in identity management," 2018.

[47] O. Jacobovitz, "Blockchain for Identity Management," Ben-Gurion University, Beer Sheva, Israel, Tech. Rep., 2016. [Online]. Available: https://www.cs.bgu.ac.il/ frankel/TechnicalReports/2016/16-02.pdf

[48] Z. W.-O. Danny Yang, Jack Gavigan, "Survey of confidentiality and privacy preserving technologies for blockchains," R3 Research, Tech. Rep., 2016. [Online]. Available: https://z.cash/static/R3_Confidentiality_and_Privacy_Report.pdf

[49] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A Survey on Essential Components of a Self-Sovereign Identity," 2018.

[50] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," 2018.

[51] UNOPS, "The Legal Aspects of Blockchain," UNOPS, Tech. Rep., 2018. [Online]. Available: https://www.blockchainpilots.nl/books

[52] M. Ahmed and K. Kostiainen, "Identity Aging: Efficient Blockchain Consensus," 2018.

[53] P. Dunphy, L. Garratt, and F. Petitcolas, "Decentralizing Digital Identity: Open Challenges for Distributed Ledgers," –, 2018.

[54] P. Dunphy and F. A. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," *IEEE Security & Privacy*, vol. 16, no. 4, p. 20–29, Jul 2018. [Online]. Available: http://dx.doi.org/10.1109/MSP.2018.3111247

[55] D. Augot, H. Chabanne, O. Clémot, and W. George, "Transforming face-to-face identity proofing into anonymous digital identity using the Bitcoin blockchain," *CoRR*, vol. abs/1710.02951, 2017. [Online]. Available: http://arxiv.org/abs/1710.02951

[56] D. Augot, H. Chabanne, T. Chenevier, W. George, and L. Lambert, "A User-Centric System for Verified Identities on the Bitcoin Blockchain," *CoRR*, vol. abs/1710.02019, 2017. [Online]. Available: http://arxiv.org/abs/1710.02019

[57] M. Schanzenbach, G. Bramm, and J. Schütte, "reclaimID: Secure, Self-Sovereign Identities using Name Systems and Attribute-Based Encryption," *CoRR*, vol. abs/1805.06253, 2018. [Online]. Available: http://arxiv.org/abs/1805.06253

[58] A. Othman and J. Callahan, "The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity," *CoRR*, vol. abs/1711.07127, 2017. [Online]. Available: http://arxiv.org/abs/1711.07127

[59] U. Der, S. Jähnichen, and J. Sürmeli, "Self-sovereign Identity - Opportunities and Challenges for the Digital Revolution," *CoRR*, vol. abs/1712.01767, 2017. [Online]. Available: http://arxiv.org/abs/1712.01767

[60] F. Guggenmos, J. Lockl, A. Rieger, and G. Fridgen, “Challenges and Opportunities of Blockchain-based Platformization of Digital Identities in the Public Sector (Research in Progress),” in ., 06 2018.

[61] M. Al-Bassam, “SCPKI: A smart contract-based PKI and identity system,” in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. ACM, 2017, pp. 35–40.

[62] D. Baars, “Towards Self-Sovereign Identity using Blockchain Technology,” Master’s thesis, University of Twente, 2016.

[63] M. van Wingerde, “Blockchain-enabled self-sovereign identity,” 2017.

[64] H. Shrobe, D. L. Shrier, and A. Pentland, *New Solutions for Cybersecurity*. MIT Press, 2018.

[65] “Enigma.” [Online]. Available: https://enigma.co

[66] R. Gupta, *Hands-On Cybersecurity with Blockchain*. Packt, 2018.

[67] S. Kulhari, “Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity (Forthcoming),” MPG, Tech. Rep., 2018.

[68] H. Farahmand, “Blockchain: Evolving Decentralized Identity Design,” Gartner, Tech. Rep., 2017.

[69] ——, “Blockchain: The Dawn of Decentralized Identity,” Gartner, Tech. Rep., 2018.

[70] N. Henein and M. Horvath, “5 Steps to Managing Privacy in the Blockchain,” Gartner, Tech. Rep., 2018.

[71] D. Mahdi, F. Gaehtgens, and J. Care, “Innovation Insight for Bring Your Own Identity,” Gartner, Tech. Rep., 2018.

[72] C. Pettey, “The Beginner’s Guide to Decentralized Identity,” Gartner, Tech. Rep., 2018.

[73] JSON Web Tokens. [Online]. Available: https://tools.ietf.org/html/rfc7519

[74] End-to-end KYC Solutions by SWIFT. [Online]. Available: https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/complete_end-to-end-kyc-solutions

[75] The one-stop AML compliance service. [Online]. Available: https://www.swiftdil.com

[76] J. Leskinen, “Evaluation criteria for future identity management,” in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2012, pp. 801–806.

[77] S. Banihashemi, E. Homayounvala, A. Talebpour, and A. Abhari, “Identifying and prioritizing evaluation criteria for user-centric digital identity management systems,” *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 7, 2016. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2016.070707

[78] Abacus Protocol. [Online]. Available: https://abacusprotocol.com/

[79] BanQu. [Online]. Available: https://banqu.co/

[80] BitID. [Online]. Available: https://github.com/bitid/bitid

[81] Bitnation. [Online]. Available: https://bitnation.co/

[82] Blockchain Helix. [Online]. Available: https://blockchain-helix.com/

[83] Blockpass IDN. [Online]. Available: https://www.blockpass.org/

[84] “Bloom Identity Protocol.” [Online]. Available: https://bloom.co

[85] Cambridge Blockchain. [Online]. Available: https://www.cambridge-blockchain.com/

[86] Civic. [Online]. Available: https://www.civic.com/

[87] Identity.com. [Online]. Available: https://www.identity.com/

[88] “Colendi Decentralized Scoring and Microcredit.” [Online]. Available: https://www.colendi.com

[89] Datum. [Online]. Available: https://datum.org/

[90] Distributed Identity Foundation. [Online]. Available: http://identity.foundation/

[91] “Decentralized Identifiers (DIDs) v0.11.” [Online]. Available: https://w3c-ccg.github.io/did-spec/

[92] Distributed IDs. [Online]. Available: https://w3c-ccg.github.io/did-spec/

[93] Dock.io. [Online]. Available: https://dock.io

[94] Dominode. [Online]. Available: https://dominode.com/

[95] EDDITS. [Online]. Available: https://eddits.io/

[96] MetaMask. [Online]. Available: https://metamask.io/

[97] Enigma. [Online]. Available: https://www.enigma.co/

[98] Intel SGX. [Online]. Available: https://software.intel.com/en-us/sgx

[99] Intel Secure Enclave Vulnerability. [Online]. Available: https://www.wired.com/story/foreshadow-intel-secure-enclave-vulnerability/

[100] Catalyst. [Online]. Available: https://www.catalystcrypto.io/

[101] FinID.me. [Online]. Available: http://finid.me/

[102] EIP-725. [Online]. Available: https://eips.ethereum.org/EIPS/eip-725

[103] EIP-735. [Online]. Available: https://github.com/ethereum/EIPs/issues/735

[104] EIP-1484. [Online]. Available: https://eips.ethereum.org/EIPS/eip-1484

[105] ERC-725 Alliance. [Online]. Available: https://erc725alliance.org/

[106] Enterprise Ethereum Alliance. [Online]. Available: https://entethalliance.org/

[107] Gemalto Trust ID Network. [Online]. Available: https://www.gemalto.com/brochures-site/download-site/Documents/fs-Trust-ID-Network.pdf

[108] R3 Corda. [Online]. Available: https://www.corda.net/

[109] IBM Trusted Identity. [Online]. Available: https://www.ibm.com/blockchain/solutions/identity

[110] SecureKey. [Online]. Available: https://securekey.com/

[111] Verified.me. [Online]. Available: https://verified.me/

[112] ID2020. [Online]. Available: https://id2020.org/

[113] Idento.one. [Online]. Available: http://idento.one/

[114] Jolocom. [Online]. Available: https://jolocom.io/

[115] KYC.Legal. [Online]. Available: https://kyc.legal/

[116] NameCoin. [Online]. Available: https://namecoin.org/

[117] NameID. [Online]. Available: https://nameid.org/

[118] OpenID. [Online]. Available: https://openid.net

[119] ObjectTech. [Online]. Available: https://www.objecttechgroup.com/

[120] “Payment services (PSD 2) - Directive (EU) 2015/2366.” [Online]. Available: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

[121] “’Passport ID’ iPhone App by https://www.passport.io from Paymentwall.” [Online]. Available: https://itunes.apple.com/gb/app/passport-id/id1396492672

[122] “Peer Mountain and Peerchain.” [Online]. Available: https://www.peermountain.com

[123] “Persona.im.” [Online]. Available: https://www.persona.im

[124] Pillar. [Online]. Available: https://pillarproject.io/

[125] Rate3. [Online]. Available: https://www.rate3.network/

[126] VETRI. [Online]. Available: https://vetri.global/

[127] eID+. [Online]. Available: https://procivis.ch/eid

[128] SelfKey. [Online]. Available: https://selfkey.org/

[129] ShoCard. [Online]. Available: https://shocard.com/

[130] Sovrin. [Online]. Available: https://sovrin.org/

[131] Evernym. [Online]. Available: https://www.evernym.com/

[132] Hyperledger Indy. [Online]. Available: https://www.hyperledger.org/projects/hyperledger-indy

[133] Sovrin: digital identities in the blockchain era. [Online]. Available: https://sovrin.org/wp-content/uploads/AnonCred-RWC.pdf

[134] Luxoft Partners with R3 and Integrates Identity Management Applications on Corda. [Online]. Available: https://www.luxoft.com/pr/luxoft-partners-with-r3-and-integrates-identity-management-applications-on-corda/

[135] “Mobility Open Blockchain Initiative.” [Online]. Available: https://dlt.mobi

[136] Sphere Identity. [Online]. Available: https://sphereidentity.com/

[137] SpidChain. [Online]. Available: http://www.spidchain.com/

[138] “Taqanu.” [Online]. Available: https://www.taqanu.com

[139] TENZ-ID. [Online]. Available: https://tenzorum.org/tenz_id/

[140] Tierion. [Online]. Available: https://tierion.com/

[141] Proof.com. [Online]. Available: https://proof.com/

[142] Chainpoint. [Online]. Available: https://chainpoint.org/

[143] uPort. [Online]. Available: https://www.uport.me/

[144] Protea. [Online]. Available: https://www.protea.io/

[145] Ethense. [Online]. Available: https://consensys.net/academy/ethense/

[146] Verity. [Online]. Available: http://verity.site/

[147] XAIN.io. [Online]. Available: https://xain.io/

[148] “BlockID.” [Online]. Available: https://www.blockid.cloud

[149] P. Thakkar, S. Nathan, and B. Viswanathan, “Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform,” in *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, Sep. 2018, pp. 264–276.

[150] “Hyperledger Caliper.” [Online]. Available: https://www.hyperledger.org/projects/caliper

[151] “Measure performance improvements (JIRA entry INDY-1717).” [Online]. Available: https://jira.hyperledger.org/browse/INDY-1717

[152] “Postident.” [Online]. Available: https://www.deutschepost.de/en/p/postident.html