Blockchain Usage for Government-Issued Electronic IDs: A Survey

Michael Kuperberg(✉), Sebastian Kemper, and Cemil Durak

Blockchain and Distributed Ledgers Group, DB Systel GmbH,
Frankfurt am Main, Germany
{michael.kuperberg,sebastian.kemper,cemil.durak}@deutschebahn.com

Abstract. Government IDs are traditionally plastic cards or paper-based passport booklets, sometimes with machine-readable contactless chips. Even though advanced implementations with cryptographic capabilities and online interfaces have been introduced, adoption and usage for online identification remain low. At the same time, there is a recognized need for trusted identities on the Internet, in Know-Your-Customer and Anti-Money-Laundering processes, and also in emerging blockchain-based, decentralized ecosystems. The contribution of this paper is a thorough analysis of the opportunities and state-of-the-art at the intersection of blockchain technology and government-issued electronical identity documents (eIDs), including existing implementations and pilots.

Keywords: Blockchain · eID · Government-issued electronic identities

1 Introduction

Blockchain-based applications and ecosystems require a state-of-the-art identity management. The same is true for the distributed ledger technologies (DLTs) in general, which are gaining momentum in governmental, financial and transportation areas. Most blockchain technologies have adopted the "keypair" approach to identity, where the ownership of the private key unlocks the ownership of assets and the ability to participate in the blockchain processes. Even the early, groundbreaking Bitcoin blockchain is underpinned by an advanced mechanism that relies on public-key cryptography despite being pseudonymous.

In non-permissioned blockchain implementations (such as Ethereum [12]), the keypair can be generated by anyone and joining the network is not restricted; smart contracts and the network protocols regulate the access management and the restrictions that apply to the identities (keypairs). In permissioned blockchain implementations, network participation is regulated, and keypairs are issued by authorities rather than by self-creation (cf. Certification Authorities in Hyperledger Fabric [19]). Whenever a blockchain-based application performs work that is required to be traced to a legal entity (person or legal body), the blockchain-based application must associate data (transaction in a block) with that entity. It is not imperative to maintain a blockchain keypair (identity) for

H. A. Proper and J. Stirna (Eds.): CAiSE 2019 Workshops, LNBIP 349, pp. 155–167, 2019.
https://doi.org/10.1007/978-3-030-20948-3_14

each legal entity: the blockchain activities can be performed by a blockchain participant that acts *on behalf of* the legal entity. However, such delegation runs counter to the original design principles of the blockchain approach, where each participant is self-sovereign in administering his/her assets, and can participate in the functioning of the network (e.g. though voting, block mining, etc.).

No matter which approach is taken, the blockchain participants in "serious" applications must be linked to verified identities. The process of establishing such as trusted identity is often compared to the Know Your Customer (KYC) process in banking, which is performed by live or online person-to-person interaction, using a physical identity document. The use of eID for KYC is very rare. Since KYC is a costly process, banks and businesses strive to reuse a verified identity across services. Identity reuse also helps to prevent stale data, but consumers are sceptical about data correlation, undesired creation of profiles, and data leaks.

Ideally, enrolling in a blockchain-based application using a trusted identity should be as easy as presenting an NFC-carrying government-issued electronic ID (eID) to a NFC-enabled smartphone. In such a case, the user would utilize multi-factor authentication (both for the phone and for the eID), and the eID would interact with the application servers. In the course of the interaction between the eID and the servers, a challenge-response pattern with cryptographic operations would be performed and a revocation list would be consulted. On successful completion, the blockchain-based application contains the association between the real-world identity and the blockchain-level keypair. In an even more advanced scenario, the eID would be used for transaction signing, and directly host the private key that is used in the scope of blockchain application.

In practice, however, such a flawless and uninterrupted workflow is hardly available, if ever. Cryptography-enabled eIDs are now widely available (cf. nPA in Germany), but the server-side integration remains challenging, and the pressure from consumers is not substantial enough. As a consequence, cryptocurrency exchanges resort to specialized service providers such as WebID [40]. In this paper, we do not consider specialized government-issued IDs which limited to narrow groups (e.g. members of parliament). Likewise, we do not consider sub-standard identification such as driver's licenses, credit cards with embossed photos, transportation smartcards or health insurance chipcards.

The contribution of this paper is to provide answers to the following question: **which eIDs, if any, are implemented using blockchain technologies or at least include blockchain-based functionality?** (such as a wallet for keypair management, participation in B2B/B2C (i.e. using smart contracts) etc.)

The remainder of this paper is structured as follows: in Sect. 2, we provide the foundations, describe state-of-the-art and set the scope for our survey. In Sect. 3, an extensive analysis of related work is provided. In Sect. 4, we define the evaluation criteria and use them to survey solutions and concepts. Section 5 summarizes the findings of our survey, concludes and provides the directions for future work.

2 Foundations

2.1 Blockchains and Distributed Ledger Technology

Blockchain is a subtype of Distributed Ledger Technology (DLT) and therefore shares similar features and characteristics with other types of DLTs. DLTs are, in general, replicated and cryptographically secured databases. In addition to the distribution of data, blockchains usually follow the *decentralization* approach: there is no single party that owns the database, and the ledger is maintained by a network of parties. Decentralized ledgers and blockchains use different fault-tolerant consensus mechanisms to ensure that a distributed network in a trustless environment can agree on a single truth about data states, transactions and a consistent state of the network, without having to rely on for central authorities or third-party intermediaries.

There are many blockchain and distributed ledger technology (DLT) products and their capabilities and maturity differ significantly. However, they all address, to differing degrees, the following key properties: tamper-proofness (immutability), programmability (through smart contracts), auditability and built-in trust.

In the context of identity management, blockchains and DLTs offer new paradigms and capabilities, such as self-sovereign identity [29], by making an identity-owning individual the final arbiter of who can access and use the personal data. By employing cryptographic algorithms and immutability, network participants can trust the records and accept them as impartial. But since identity information must be validated to be useful, a person's identity has to be verified, e.g. by having a trusted participant (or a significant number of participants) vouch for the validity of the information in a user's profile.

2.2 Identification and IDs

The terms *identity* and *ID/identifier* are used to distinguish individual entities within a group of comparable, same-typed entities. For example, a DNA can be used as an ID to distinguish two human identities. In general, the identity of a given person, organization, device etc. is the *entire* set of attribute values that enable to distinguish that entity from others in the group. An identifier is a sufficient (sub-)set of one or several attributes which forms a "primary key"; the identifier does not have to include *all* identity-forming attributes.

An identifier on its own is sufficient to denote the uniqueness of the identity in its group; it might be possible to create different identifier schemas for the same group. A global, cross-group schema for identity does not exist: each group has its own identifiers and attributes. The term *ID* is an abbreviation for "identity document"; it is often used for a physical manifestation of an identifier (e.g. a passport booklet). The term *identification* describes the process of delivering a proof, based on the given identity and using an identifier or an ID.

The identifier information can be permanently stored in a physical way as an item, which can be a passport, or a smartcard chip (i.e. computer hardware). Thus, both physical and virtual (i.e. non-material) representation of an identifier

are possible. The information items that represent the identifier can be represented as digital data (such as binary encoding of a DNA) or, substantially less often, as analog data (e.g. voice recording). The term "electronic identity" is often used alongside "digital identity", since digital information is mostly processed by electronic devices such as computers. The concept of electronic and digital identities enables them for use in online services, e.g. on the Internet.

For online services, two basic types of identification are prevalent. For the first, a person *possesses* a physical item (e.g. a biometric pass, an iris scan) and *presenting* that item constitutes the identification step. For the second, a person *knows* an immaterial, non-physical secret (e.g. a password) that is *associated* with an identity; identification is performed by presenting the secret or by providing an (indirect) proof of the ownership to the secret (e.g. a digital signature computed from a secret private asymmetric key).

The difference between the two types is that the first type usually can be (temporarily) transferred as long as it maintains a physical uniqueness (unless, of course, it is too easy to duplicate or to falsify). The second type must be safeguarded because knowledge is easily replicated, while possession is not: if another person obtains the secret, he/she can impersonate as the actual identity owner. The two types are often combined into multi-factor authentication (MFA). Of course, some non-secret identification elements (such as fingerprints or dynamic 3D face models) are non-portable, or can be easily falsified (e.g. fingerprints).

In some cases, online identification is performed though third parties ("identity providers") or through secondary documents such as driving licenses, banking cards, witnesses, or bank transfers. Third parties enable identification using website technology (e.g. through OIDC, OAuth and SAML) or through B2B offerings such as PostIdent and VideoID. Identification through bank transfers can work as follows: if the bank is trusted to have performed KYC and if the account ownership is not compromised or shared, a challenge-based approach is possible: the identity requestor provides a challenge (e.g. requests a minimum-amount transfer with a case-specific purpose text) and the identity owner proves his/her identity by performing the challenge-confirming transfer.

However, the most trusted identification comes from governments, which are traditional sources of identification/lifecycle documents for humans (and animals): they issue physical identification items such as passports, ID cards, birth certificates etc. Physical passports have the disadvantage of full disclosure of information (e.g. the past entry stamps or visas are available for every inspector) and high value for thiefs, and are also easily lost or damaged. Passports are often owned by the issuing government and not by the individual person; forced confiscation of physical passports and IDs restricts not only a person's ability to travel, but also removes essential entitlements and basic citizenship capabilities - even if the citizenship itself is not removed.

Digital identification documents issued by governments are often eIDs that are either a "smart" document/chipcard with some cryptographic/electronic equipment (as in Estonia [7], Germany [13] and certain other countries), or as a centralized IT system without a physical eID (as it is the case in the

Aadhaar [1] system in India). Aadhaar employ biometric "keys" to match them to the system-stored record; a person may obtain a "printout" as a non-binding proof of identity - but the printout on its own cannot be used for identification.

Thus, the use cases of government-issued eIDs vary from country to country and serve to identify citizens in order to access services provided by the specific government. These services may include the signing documents with digital signatures, conducting payments (such as in Estonia [38]) and may even entitle the user to vote. eiDAS (electronic IDentification, Authentication and trust Services) [34] is a binding EU regulation that establish a uniform framework for cross-border uses of electronic identification.

Virtual government eIDs, also referred as "virtual residency" or "e-residency", is an approach first introduced in Estonia. Estonian e-residency includes a digital ID, but requires a personal show-up at an Estonian embassy as part of the application and payment of an administration fee. If granted, e-residency includes a PKCS11-enabled smart card with online identification, eiDAS-compliant digital signature incl. timestamping (though not a general-purpose signing certificate, and only for BDOC/DDOC container documents), electronic voting (only for full citizens) and some other services. However, it does not entitle to "normal" citizenship and does not grant conventional residency rights.

A newer aspect of eIDs is the concept of self-sovereign identities (SSI). The goal of this approach 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. This "liberation" is fueled not by lawmaking or by regulation, but rather by the technical means and advances. The "Self-Sovereign Identity Working Group" is one of the interest groups driving this topic. With their project "X-Road" [20], Estonia tries to provide a system where citizens can decide which information is being shared between which institutions.

3 Related Work

In [47], Grech et al. describe how the blockchain technology can be of great use in national eID systems, especially in the context of self-sovereign identities. The authors highlight the blockchain potential for the Estonian national digital identity management system, although the focus is primarily on the uses and application of blockchain technologies in education sector. However, further eID implementations are not considered or evaluated.

In [3], Pisa et al. provide an analysis of the potential of the blockchain technologies in the framework of global economic development. Along with other topics, they also examine the blockchain technologies' suitability and role in providing and creation of secure digital ID systems by governments. While the authors describe a pilot project of a blockchain-based self-sovereign digital ID system in Canada, no other countries or solutions have been surveyed and no evaluation criteria have been defined.

[4] is an academic paper prepared for the European Union Blockchain Observatory and Forum by Third et al. It reports the use of blockchain and distributed

ledger technology for government services, with a special focus on digital identities. Among others, it introduces several use cases in national identity managements systems, specifying their maturity, the tech companies involved and so on. In [43], Lyons reports on a 2018 workshop titled "Government Services and Digital Identity". The report describes existing use cases of blockchain technologies in the public administration domain from different countries and identifies the projects of Zug residents' IDs [45] (Switzerland) as well as Estonian e-identity as priority use cases for Europe in the eID field.

In [49], Jun suggests the inevitability of replacement of bureaucracy with blockchain systems and claims the future of governments to be a blockchain government, for which he introduces four main principles. In his work, Jun lists an extensive amount of government-led blockchain projects and mentions Estonian e-identity and Zug residents' IDs. However, he does not provide detailed information on these projects, an evaluation, or any details.

4 Survey

In this section, we only consider eIDs that have a DLT-related functionality or project (there are at least 30 countries with an eID setup). eIDs have already been studied by other authors [46], and analyses of DLT/blockchains are widely available (e.g. [51]). The general topic of blockchain-supported identity management has been studied as well [50], but mostly leaves out the specifics of government-issued eIDs. In contrast to other work, our survey focuses its evaluation on the *intersection* between government-issued eIDs and blockchain/DLTs; our analysis of related work (see Sect. 3) for this intersection has shown that there is no systematic evaluation of it.

4.1 Evaluation Criteria and Scope Definition

Our contribution starts with establishing the following evaluation criteria that we apply to blockchain-empowered eID solutions:

- eID uses a DLT as storage of identity data (e.g. [encrypted] public and/or private keys, certificates, non-revokable identity attributes such as age, sex, date of birth)
- eID uses a DLT as storage of authorization data (e.g. visas, driver's licenses, data releases, attribute changes, tickets or other entitlements etc.)
- eID built-in capabilities are used for keypair generation, keypair storage, transaction signing or similar aspects of DLT cryptography
- intersection of DLT and eID, but none of the above

For each country, we indicate the technology involved (if it is known); further information is available from the cited sources. There are country-overarching initiatives (e.g. for stateless ethnic groups, such as the blockchain-based solution in [26]), we consider them in the cases where the resulting eID is nationally recognized *in lieu of* a traditional government-issued eID.

We do not consider general blockchain-backed e-government activities such as e-voting, taxing, healthcare, land administration etc. unless these activities create an eID which is usable independently. Likewise, we do not consider blockchain-based IDs which open up a "gated" ecosystem without government actors (as for example in the planned cooperation [39] of Verified.me and IBM in Canada, where a solution based on Hyperledger Fabric has been announced).

We looked at government-issued eIDs of Australia, Canada, China, Germany, Georgia, Ghana, India, Japan, Luxembourg, Netherlands, Russia, Singapore, South Korea, Sweden, Taiwan and USA, but found no relevant intersection with DLTs or Blockchains. Only the following five countries have significant projects.

4.2 Dubai, United Arab Emirates (UAE)

In October 2017, a MoU [33] was announced to develop a unified digital identity for the entire UAE within the Smart Dubai [32] initiative, based on blockchain technology. The projects aims at the integration of the UAE's SmartPass [36] verified identity service (which is also employed in airport security) with the eID-enabled Dubai ID [6] online service to form a nationwide single system, allowing users to access federal and local government services by logging in once.

The technical partner for the unified digital identity project is ObjectTech [25], a UK startup; the details of ObjectTech's technology stack have not been published yet. ObjectTech's website claims that their solution is "*fully compliant with privacy and security regulations, such as PSD2 & GDPR; it exceeds both the letter and intentions of these initiatives*" and that it is quantum resistant. The pilot program is planned to be ready by 2020 (cf. [17,30]).

UAE's federal authorities [37] issue an eID card to residents (incl. non-citizens) and also offer digital signature and identification services to companies; an SDK for developers is provided [28]. Additionally, the "UAE PASS" app [35] is provided, which turns a mobile device into a secure form of identification for UAE online services; it is not connected to the eID chipcard (unlike the Dubai ID). However, neither SmartPass nor Dubai/UAE eIDs and digital passports are *backed* by DLT technology or *integrated with* a DLT as of January 2019. In October 2018, the company behind UAE Pass has announced to follow the "strategic direction for the adoption of blockchain technologies" [2].

4.3 Estonia

Estonia has both an eID for residents/citizens [7] and a "e-residency" program [8]. The eID is issued as a PKCS11 smart "ID-Card" with the ability to sign and encrypt documents and emails, perform online login, make payments [38], use telemedicine etc. The keypair stored on the smartcard is compatible to the X.509 standard; newer cards add a contactless interface (NFC).

In addition to the "ID-Card", a separate "digi-ID" card [41] is available for those Estonian citizens who already possess a valid "ID-Card" in any case. The main differences to the "ID-Card" is that the "digi-ID" lacks any printed or

embossed information, and thus can only be used in electronic environments, while the "ID-Card" also serves as a *visual* identity document.

The third eID in Estonia is the "Mobiil-ID" [42], which is small SIM-sized card for mobile phones. "Mobiil-ID" serves as a person's identification and as a digital signing solution, very similar to the two other cards. Like the previously mentioned cards it can be used to access specific e-services such as e-taxing and digitally sign documents, but with the added value of not requiring an external card reader during the process. To utilize the "Mobiil-ID", the user uses two PIN codes: the first code is needed for identification to the card and the second code is needed to unlock the signature functionality. "Smart-ID" [31] is the corresponding mobile app in order to access the "Mobiil-ID" functionalities.

According to the information on the e-Estonia project website [5], the underlying infrastructure for all these eID functionalities includes Guardtime's KSI [21] Blockchain technology for security and safety purposes. Guardtime itself states that they have succeeded in creating a "reliable service for the government that would continue to function even under cyber-attack". Even though the implementation [15] of KSI is accessible as to January 2019, it is not transparent to which specific extent the blockchain technology is used within the Estonian eID solutions described above. Guardtime has been working together with the Estonian Government on a digital signature system since 2007, and KSI is used for "independent verification of all government processes".

Beyond the above building blocks, e-Estonia also utilizes "X-Road" [20], a solution which is used to connect various public and private e-Service databases. Every data exchange over X-Road is signed, encrypted, authenticated and logged. To avoid any misunderstandings, e-Estonia officially stated that X-Road itself is not based on the blockchain-technology [44].

4.4 Finland

The Finnish eID was introduced in 1999 and was among the very first operational national eID scheme in the world; it is non-obligatory and the fees are relatively high. Currently, the Finnish eID system sees relatively low use; it does not employ or support blockchain technologies.

In 2015, independently from the general countrywide eID scheme, the Finnish Immigration Services [24] and the Helsinki-based startup company MONI [23] started a project in which the partners associate a digital identity with the prepaid MasterCard debit cards which are provided to asylum seekers and refugees who are lacking official/paper identification documents. According to [16], the debit cards are linked to corresponding unique digital identities that are created for refugees on blockchain; this turns the debit cards into a kind of government-issued eIDs. Deployed on an Ethereum blockchain platform, the solution potentially enables thousands of refugees to participate in everyday tasks [14,18,48] until they receive normal ID documents. However, the software in the trial also appears to record the financial transactions made with the card *on the blockchain*. As of January 2019, it is planned to terminate the trial until May 2019.

4.5 Luxembourg

The national eID in Luxembourg is a chipcard that also supports digital signatures, using the software provided by LuxTrust [22]. In a project called EDDITS [9], LuxTrust supports the InTech blockchain company to link Ethereum identities to conventional, CA-issued X.509 certificates - this corresponds to the third criterium in Sect. 4.1. The resulting pilot implementation can be regarded as a blockchain-supported eID on its own (even though the recognition and adoption of EDDITS are minimal); the resulting eID still fulfills the second criterium from Sect. 4.1 as authorization data is stored on a blockchain.

4.6 Switzerland

As of January 2019, the development of government-issued eID in Switzerland is still ongoing [11], but not even a pilot is available yet.

The Ethereum-based, uPort-powered resident's ID in the Swiss city of Zug has been among the pioneers of blockchain-based identity. However, as reported in [45], the validation of the app-created ID has to take place in the city office, through a human-to-human interaction; there is no national, government-issued eID to be integrated with yet. The Zug ID is only recognized in the city itself.

Another project is the "Schaffhauser eID+" blockchain-secured [27] electronic identity solution. The system, which has been implemented jointly by Swiss e-government specialist Procivis [10] and the IT services of the canton and town of Schaffhausen (KSD), is in production use. In fact, we consider it to be an interesting case of an intersection between a government-issued eID and the DLT technology, even though it does not use a "traditional" card-shaped eID. As for the classification in Sect. 4.1, the second scenario (DLT stores authorization data) is explicitly supported; support of the other two scenarios (DLT stores identity data; eID capabilities are used for DLT cryptography) is not declared.

5 Conclusions

Table 1 summarizes our findings. The most developed use case of government-issued eIDs and blockchain technology can be found in Estonia (EE), with the e-Identity ID card which is deployed on the KSI Blockchain, and trials/pilots are ongoing or in development in Switzerland (CH), Luxembourg (LU), Finland (FI) and United Arab Emirates (UAE). For the Estonian eID, the details of what data exactly is stored on the blockchain (and how) have not been published yet.

The EDDITS project (Luxembourg) [9] is a pilot that utilizes the eID functionality to create trusted on-blockchain identities. For the Ethereum-based Zug ID pilot, an electronic identity is created on-chain, but it does not interact with a government-issued eID document/certificate. Transaction signing, or even key storage on the eID cards, remain a vision for the future. None of the studied government-issued eID solutions declares that it stores primary identity data (such as keys, certificates or attributes) on a DLT or blockchain, even in encrypted form.

Table 1. Comparison table of eID-using blockchain solutions (see Sect. 4.1 for a definition of "identity data" and "authorization data")

Authority that issues eID	United Arab Emirates Governm.	Estonian Governm.	Finnish Immigration Services	Governm. of Luxembourg via LuxTrust	Switzerland City of Zug	Switzerland Canton of Schaffhausen
Rollout status	Pilot starting 2020	In use	In use till 30.04.2019	Pilot phase	Pilot phase	In use
Level	National	National	National	National	Municipal	Canton
Solution used for	Digital passport; "ID locker"	Data integrity, timestamp	Unique Digital Identities	Trusted blockchain identities	Self-sovereign identities	Self-sovereign identities
DLT stores identity data	No	No	No	No	No	No
DLT stores authorizations for eID	Planned	No (but the DLT acts as an access log)	No (but the DLT stores payment transaction history)	No	No	Yes
eID capabilities for DLT cryptogr.	No	No	No	Yes	Yes	Unspecified
GDPR	Compliant	Compliant	Unspecified	Unspecified	Compliant	Unspecified
eID Type	Mobile app	Multiple	Multiple	X.509 cert.	Mobile app	Mobile app
Implem. Partner	ObjectTech	Guardtime	MONI	Intech	uPort and ti&m	Procivis
Blockch. Type	Unspecified (Q1/19)	Private	Unspecified	Public testnet: Kovan	Public	Unspecified
Blockch. Technol.	Unspecified	KSI Blockchain	Ethereum Blockchain	Ethereum; ERC-725 ERC-735	Ethereum + uPort	Unspecified

For our future work, we plan to address the following question: which eIDs are *suitable* for use in blockchain-/DLT-based applications? Additionally, we plan to study how blockchain transactions can be (co-)signed by eIDs.

Acknowledgements. Moritz Stumpf provided additional insights to the Estonian eID landscape.

References

1. Aadhaar Online Services. https://uidai.gov.in
2. ADSSSA showcases blockchain implementation in bid to accelerate 'One Government' services model. https://www.darkmatter.ae/press-release/adsssa-showcases-blockchain-implementation-in-bid-to-accelerate-one-government-services-model/
3. Blockchain and economic development: hype vs. reality. https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf
4. Blockchain for government and public services. https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory-_blockchain_in_government_services_v1_2018-12-07.pdf
5. Blockchain for Smart-ID. https://e-estonia.com/egoverment-blockchain-guardtime/
6. Dubai ID. https://www.dm.gov.ae/en/Pages/Login.aspx
7. e-Identity of Estonia. https://e-estonia.com/solutions/e-identity/id-card/
8. E-residency 2.0 White Paper. https://s3.eu-central-1.amazonaws.com/ereswhitepaper/e-Residency+2.0+white+paper+English.pdf
9. EDDITS. https://eddits.io/
10. eID+. https://procivis.ch/eid
11. Etablierung einer national und international gültigen elektronischen Identität (E-ID). https://www.egovernment.ch/de/umsetzung/schwerpunktplan/elektronische-identitat/
12. Ethereum. https://www.ethereum.org
13. The German National Identity Card (nPA). https://www.personalausweisportal.de/EN/Home/
14. Government services and digital identity. https://www.eublockchainforum.eu/sites/-default/-files/research-paper/20180801_government_services_and_digital_identity.pdf
15. Guardtime KSI on Github. https://github.com/guardtime/ksi-tool#start-of-content
16. How Blockchain is Kickstarting the Financial Lives of Refugees. https://www.technologyreview.com/s/608764/how-blockchain-is-kickstarting-the-financial-lives-of-refugees/
17. How blockchain is used by governments as a form of national identity. https://medium.com/@bryzek/how-blockchain-is-used-by-governments-as-a-form-of-national-identity-e24a4eefb7d8
18. How Finland is Using the Blockchain to Revolutionise Financial Services for Refugees. https://reliefweb.int/report/finland/how-finland-using-blockchain-revolutionise-financial-services-refugees
19. Hyperledger Fabric. https://www.hyperledger.org/projects/fabric
20. Interoperability Services. https://e-estonia.com/solutions/interoperability-services/x-road/
21. KSI Technology Stack. https://guardtime.com/technology
22. Luxembourg based company InTech launches innovative blockchain-based on-line service. https://www.luxtrust.com/luxembourg-based-company-intech-launches-innovative-blockchain-based-on-line-service-eddits-for-associating-strong-digital-identities-with-ethereum-addresses-in-partnership-with-lux/
23. Moni. https://www.moni.fi

24. Moni-based Reception allowance for Refugees. https://migri.fi/en/reception-allowance
25. ObjectTech. https://www.objecttechgroup.com/
26. Procivis and the Rohingya Project partner to provide electronic identity to the Rohingya diaspora. https://procivis.ch/2018/04/04/procivis-and-the-rohingya-project-partner-to-provide-electronic-identity-to-people-without-legal-documentation/
27. Procivis eID+. https://www.cnlab.ch/fileadmin/documents/Publikationen/2018/Procivis_eID__Herbsttagung_2018-09.pdf
28. SDK for UAE eID. http://sdk.emiratesid.ae
29. Self-Sovereign Identity Working Group. https://blockchainhub.net/self-sovereign-identity/
30. Smart Dubai to launch a unified digital identity card. https://embeddedsecurity-news.com/2017/10/uae-tra-smart-dubai-to-launch-a-unified-digital-identity-card/
31. Smart-ID App. https://e-estonia.com/solutions/e-identity/smart-id/
32. SmartDubai. https://smartdubai.ae
33. Telecommunications Regulatory Authority and Dubai Smart Government Sign MoU to launch unified digital identity. https://www.ica.gov.ae/en/media-centre/news-and-reports/news.aspx
34. Trust Services And Electronic Identification (eID). https://ec.europa.eu/digital-single-market/en/trust-services-and-eid
35. UAE PASS Mobile App. https://smartdubai.ae/apps-services/details/uae-pass
36. UAE SmartPass. https://smartpass.government.ae/
37. United Arab Emirates eID. https://www.ica.gov.ae/en/home.aspx
38. Using ID-cards for Payments. https://eid.eesti.ee/index.php/Using_ID-card_for_payments
39. Verified.me. https://verified.me/
40. WebID Identity Company. https://www.webid-solutions.de/en/
41. What is Digi-ID. https://www.id.ee/index.php?id=34410
42. What is Mobiil-ID. https://www.id.ee/index.php?id=36892
43. Workshop report government services and digital identity. https://www.eublockchainforum.eu/sites/default/files/reports/workshop_3_report_-_government_services2fdigital_id.pdf
44. X-Road not to be confused with blockchain. https://e-estonia.com/why-x-road-is-not-blockchain/
45. Zug ID: Exploring the First Publicly Verified Blockchain Identity. https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702
46. Carretero, J., Izquierdo-Moreno, G., Vasile-Cabezas, M., Garcia-Blas, J.: Federated identity architecture of the European eID system. IEEE Access **6**, 75302–75326 (2018). https://doi.org/10.1109/ACCESS.2018.2882870
47. Grech, A., Camilleri, A.F.: Blockchain in education, vol. 33, p. 132. Publications Office of the European Union, Luxembourg, January 2017. https://doi.org/10.2760/60649
48. Guggenmos, F., Lockl, J., Rieger, A., Fridgen, G.: Challenges and Opportunities of Blockchain-Based Platformization of Digital Identities in the Public Sector (Research in Progress), June 2018
49. Jun, M.: Blockchain government - a next form of infrastructure for the twenty-first century. J. Open Innov.: Technol. Market Complex. **4**, 7 (2018). https://doi.org/10.1186/s40852-018-0086-3

50. Lim, S.Y., et al.: Blockchain technology the identity management and authentication service disruptor: a survey. Int. J. Adv. Sci. Eng. Inf. Technol. **8**, 1735 (2018). https://doi.org/10.18517/ijaseit.8.4-2.6838
51. Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H.: Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. **14**(4), 352–375 (2018)