Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity

Nitin Naik[1] and Paul Jenkins[2]

[1]School of Informatics and Digital Engineering, Aston University, United Kingdom
[2]Cardiff School of Technologies, Cardiff Metropolitan University, United Kingdom
Email: n.naik1@aston.ac.uk and pjenkins2@cardiffmet.ac.uk

***Abstract*—Digital identity has importance in the digital world representing users in a comparable manner to that of the physical identity in the real world. Digital identity comprises certain personal and confidential attributes related to identity owners, managed through an Identity Management (IDM) system. In most IDM systems, identity owners do not control their own identity and its related personal data. However, Self-Sovereign Identity (SSI) is an emerging IDM system which offers users the ownership and full control over their personal data. In the European Union, General Data Protection Regulation (GDPR) is the basic regulatory environment for anyone involved in processing personal data, whilst SSI is concerned with the requirement of managing identity and its associated personal data. If an SSI system could comply with the key GDPR principles then it could become both a desirable and appropriate IDM solution legally and universally. This paper evaluates this aspect of SSI and analyses SSI compliance and alignment with the key principles of GDPR. Furthermore, it investigates two different types of SSI ecosystems public permissionless blockchain based SSI ecosystem uPort and public permissioned blockchain based SSI ecosystem Sovrin, according to the various defined roles and their compatibility with GDPR roles. Finally, this paper performs the comparative analysis of uPort and Sovrin to assess their compliance with the key principles of GDPR.**

***Index Terms*—Self-Sovereign Identity; SSI; General Data Protection Regulation; GDPR; Distributed Ledger; Blockchain; Identity Management System; IDM; uPort; Sovrin.**

1. Introduction

As reliance on digital platforms is increasing, the importance of digital identity has intensified. Digital identity is the key to access any service in the digital world similar to a physical identity in the real world [1], [2]. Several Identity Management (IDM) systems were developed and employed to manage digital identity effectively, however, a significant issue with the majority of the IDM systems is that an identity owner never had control of their identity and its associated data [3], [4], [5]. Self-Sovereign Identity (SSI) IDM has recently been developed to solve this issue, by providing users with sovereign ownership of their identity and full control of their personal data [6], [7]. As the General Data Protection Regulation (GDPR) came into effect in 2018, to manage and govern personal data in the European Union (EU), the requirement to align SSI with the key GDPR principles became both desirable and necessary. SSI systems are based on distributed ledgers/blockchains, where compliance with GDPR is a challenging task due to the public and decentralised nature of distributed ledgers/blockchains. Therefore, this paper evaluates this aspect of SSI and its compliance with the key principles of GDPR. Furthermore, it investigates two different types of SSI ecosystems public permissionless blockchain based SSI ecosystem uPort and public permissioned blockchain based SSI ecosystem Sovrin, according to the various defined roles and their compatibility with GDPR roles. Finally, this paper performs a comparative analysis of uPort and Sovrin to assess their compliance with the key principles of GDPR.

The rest of the paper is structured as follows: Section 2 discusses self-sovereign identity and its underlying working procedure. Section 3 summarises the key principles of GDPR. Section 4 evaluates SSI compatibility with the key GDPR principles. Section 5 performs the comparative analysis of uPort and Sovrin based on the key principles of GDPR. Section 6 presents the summary of the paper and related future work.

2. Self-Sovereign Identity (SSI)

Self-Sovereign Identity (SSI) is a sovereign, enduring and portable identity for any person, organization, or body, that allows its owner to access all relevant digital services by utilising verifiable credentials linked to the identity in a privacy-preserving manner [8]. The ecosystem of a self-sovereign identity is illustrated in Fig. 1. It has three main roles *Issuer, Holder* and *Verifier*. An issuer creates and issues credentials to a holder. A holder receives credentials from an issuer, retains it and when it is required, it shares credentials with a verifier. A verifier receives and verifies credentials presented by a holder. This SSI is an emerging model of an identity which offers several essential features for a sovereign identity without dependence on any external administrative authority:

- An identity owner should be the sole owner of the identity with full control over its use and attributes.
- An identity owner should be able to decide the type of identity data used to define their identity.

- An identity owner should be able to perform all the operations related to their identity and personal data or assign control of such functions on their behalf.
- An identity owner should be able to use their identity as long as they wish and their identity cannot be revoked or removed by anyone else.

Self-sovereign identity is unique from preceding identity models in that it employs new standards such as Decentralized IDentifier (DID) and Verifiable Credentials (VC) based on the distributed ledger/blockchain for creating a cryptographically verifiable digital identity that is fully governed by its owner [9], [10].

From the inception of identity management technology, there was no universally unique identifier which could be used as a standard interoperable mechanism, consequently, each employer or service provider was compelled to create their own. Circumventing this issue, SSI has offered a universally unique identifier called Decentralized IDentifier (DID). The DID is a permanent, universally unique identifier and cannot be taken away from its owner who owns the associated private key, which is completely different from other ephemeral identifiers such as a mobile number, IP address and domain name [9]. Only public DIDs alongside some other public credentials selected by DID owners could be stored on the distributed ledger/blockchain (or off-ledger/off-blockchain) in the form a DID document. This does not include private DIDs and identity related personal and confidential data and therefore, these are not stored on the blockchain alternatively it is maintained on the storage (e.g., digital wallet) of an identity owner or agent. The DID document is normally governed by the identity owner through holding its associated private key.

A claim is an assertion made relating to any entity. A credential is a group of claims used by any entity to prove their identity. A Verifiable Credential (VC) is verifiable through a signature or evidence supplied by an issuer who has either issued the VC or can confirm its correctness. A VC is used to represent similar information on the Web to that of a physical credential in the real world. The verifiable credentials should be linked with an identity through its unique identifier such as a DID.

Self-sovereign identity allows identity owners to control their identity related confidential data and retain this information on storage owned or controlled by them. Generally, this data is stored in a digital wallet, which is analogous to a physical wallet keeping all digital credentials as physical entities, however, digital credentials in the digital wallet are digitally signed, verifiable credentials and much faster to issue and verify than their physical counterparts. This means a user can control what to share with other organisations. The user can share an entire credential, part of a credential (known as claim), or Zero-Knowledge Proofs (ZKP) acquired from a credential [7]. The encrypted and persistent connection is established to transmit digital credentials securely and privately. The trust relationship between organisation and user is maintained through blockchain (see Fig. 1). The verifier

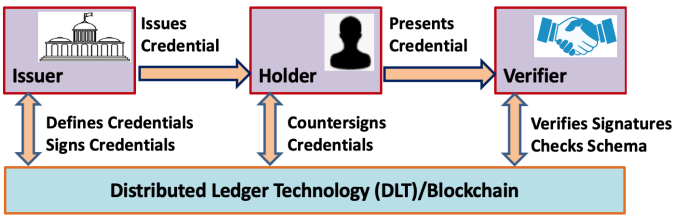

Fig. 1. Self-Sovereign Identity Ecosystem and its Components

verifies the digital signatures on received credentials using an underlying blockchain.

3. Key Principles of General Data Protection Regulation (GDPR)

There are seven key principles described in the Article 5 of the GDPR regime [11]:

3.1. Lawfulness, Fairness and Transparency

There must be a lawful basis for collecting, storing and processing of personal data without breaching any law. Personal data must be processed fairly and not in a misleading, unpredictable, unexpected or detrimental manner. The whole process must be transparent with respect to the purpose, access and time period of data.

3.2. Purpose Limitation

Personal data must only be collected for a specific, explicit and legitimate purpose. This purpose must be stated, and data is only collected for as long as necessary to complete that purpose. The existing personal data can only be used for a new purpose if either this is compatible with the stated original purpose for which the consent was given, or it is according to the law.

3.3. Data Minimisation

It must be ensured that the processed personal data is adequate, relevant and limited to what is necessary in relation to the stated processing purpose. Data collection is limited to the necessary minimum and requires the justification of the amount of data collected.

3.4. Accuracy

All necessary steps should be taken to ensure that the stored personal data is not incorrect or misleading as to any matter of fact. The personal data may need updating or erased, without delay in order to maintain its accuracy if it is inaccurate or incomplete. No old and outdated personal data should be retained in any way.

3.5. Storage Limitation

The personal data must not be kept for longer than its intended time period of use and it must be deleted when it is no longer required. The retention period or condition of personal data must be stated with the appropriate justification at the beginning of the process.

3.6. Integrity and Confidentiality (Security)

All pertinent security measures must be established to protect the personal data. These security measures generally include protection against unauthorised or unlawful processing, protection against accidental loss, destruction or damage, which can be achieved through encryption, pseudonymisation and anonymisation of personal data, and security certifications in accordance with industry best practices. GDPR does not state specific measures because technological and organisational best practices are constantly changing and improving.

3.7. Accountability

This principle is to ensure the responsibility of every role involved in processing personal data to comply with all the other GDPR principles and demonstrate that compliance through apposite measures and records are met.

4. Evaluating SSI Compatibility with the Key Principles of GDPR

GDPR only applies when personal data of an EU data subject is processed, thus, it does not apply when there is no personal data. SSI is based on the distributed ledger/blockchain, which is a class of technology with several versions: private, public, permissioned and permissionless. These different versions of blockchain varies in their technical design/architecture, governance arrangement and complexity. Therefore, the compatibility between the GDPR and blockchain based SSI can only be assessed and analysed on the basis of a specific SSI system and its underlying blockchain. Consequently, it cannot be concluded in general that the GDPR and SSI systems are compatible or not without considering a specific SSI system. However, this evaluation attempts to include both compatibility and incompatibility aspects of the GDPR and SSI systems in general.

4.1. SSI Compatibility with Lawfulness, Fairness and Transparency

In an SSI system, a holder (normally an identity owner), holds the identity and its associated personal data and has full control over it, therefore, any exchange or collection of personal data is only possible on a lawful basis when the identity owner provides their consent. When a holder has been delegated, the authority to manage the personal data of someone else (i.e., an entity/data subject other than the holder), then the authorised holder has the necessary legal rights to consent to any exchange or collection of personal data on behalf of an entity/data subject to ensure their interests and confidentiality are protected. The extent of fairness and transparency is dependent on the type of an SSI system employed, which can ensure that users are able to monitor any potential mishandling of personal data and stay informed regarding the complete processing. However, the compliance of the key GDPR principles to SSI systems has several challenges; one of the biggest challenges is to define personal data which determines the applicability of GDPR regulation on specific data and its corresponding operations and processing. For example, there is no specific guidance on the data stored on a blockchain, such as public keys and transactional data whether it can be considered as personal data in the context of GDPR. Furthermore, it is unclear when personal data is appropriately anonymised to meet the GDPR criteria, thereafter, how will it be considered at later stage. All these considerations require further GDPR guidance on the applicability of the GDPR principles to SSI systems and the underlying blockchain technology.

4.2. SSI Compatibility with Purpose Limitation

SSI systems enable identity owners to decide when and with whom to share what personal data and for what purpose by giving their consent. Blockchain can be used to track and manage the consent between various roles of an SSI system. However, the clarification of the purpose is dependent on the type of an SSI system and their data use policy. The data processing purpose should be written explicitly whether it is limited to only transactions or can be extended to all other associated processing and new purposes if necessary, which is an ambiguous area and not every SSI system is fully compatible in this respect. Therefore, requiring further strict alignment of this key principle with some SSI systems.

4.3. SSI Compatibility with Data Minimisation

Most SSI systems allow users to store personal data off-the-chain and generally in their wallets, however, transactions are performed through the blockchain. The blockchain is designed to achieve resilience through replication and data is replicated on many different locations. Additionally, it is an append-only database that constantly grows as new data is added. Both aspects of blockchain do not comply with the data minimisation principle. This is again varied from one SSI system to another; however, it is another compatibility issue, requiring greater alignment.

4.4. SSI Compatibility with Accuracy

Most blockchains are public, therefore, SSI systems do not store personal data on the blockchain itself, rather they store the data privately off-the-chain. This allows updating and erasing of personal data when necessary without any further impact. Furthermore, it may comply with the most important right of users in GDPR, which is the *Right To Be Forgotten or Right To Erasure* depending on how and where the identity is maintained. However, some DIDs, keys, hashes and other data may be stored on the blockchain. Additionally, the blockchain is an append-only database, wherein, data can be added but removed only in exceptional circumstances. This feature makes it difficult to comply with the *Right To Be Forgotten or Right To Erasure* as updating and erasing data on a blockchain could be very difficult, thus, complying with this right may be more challenging for some SSI systems.

4.5. SSI Compatibility with Storage Limitation

As previously mentioned, most SSI systems do not store personal data on the blockchain itself rather store it privately

off-the-chain. This allows erasing of personal data when necessary or at a specified time period without affecting the process and can comply with GDPR in principle. However, the deletion of other blockchain data may not be easy as discussed earlier and this would pose a challenge in complying with this principle. Furthermore, it is dependent on the specific SSI system in applying this principle effectively and informing users of the retention period or condition of personal data explicitly. Therefore, some SSI systems require further alignment for the compliance of this key principle.

4.6. SSI Compatibility with Integrity and Confidentiality (Security)

Most SSI systems incorporate necessary security measures to protect personal data and transactions through decentralisation, encryption, anonymisation and pseudonymisation. Distributed management and storage of an SSI system prevents a single point of failure and attack. Blockchain uses cryptography to support transaction confidentiality in addition to access controls preventing unauthorized use. It comprises audit trails and traceability, the use of consensus mechanisms to commit transactions, and transaction immutability for robust security. Many SSI systems employ pseudonymisation and anonymisation used in securing users identity and personal data. Thus, most SSI systems are able to comply with this key principle.

4.7. SSI Compatibility with Accountability

Those SSI systems which are based on permissioned blockchain and governance model could support greater accountability where a competent authority can apply necessary technical, procedural, and organizational measures to comply with this principle. It may raise the level of accountability and insight in the data and transactions by offering audit trails and traceability features thus assisting organisations in proving compliance against specific regulations. However, permission-less blockchain and the decentralised nature of a blockchain may pose greater legal and compliance challenges. One of the biggest challenges is to determine correct GDPR roles for their corresponding SSI roles in an SSI system, which may vary from one SSI system to another depending on the task assigned to, and performed by each role. The possible generalised mapping of some of the common SSI roles with GDPR roles is shown in Table I. Additionally, most of the existing blockchains were not designed to comply with GDPR principles, therefore, it requires greater alignment at the design level and further guidance on the application of GDPR principles to SSI systems.

Critical Analysis

GDPR is mainly focused towards a centralised network design with defined roles, whereas SSI is based on the blockchain technology which is mainly a de-centralised network design where everyone has equal access to it. This is a significant difference between the two systems, which poses several challenges towards their alignment. In summary, SSI systems which are based on a public permissionless blockchain pose greater challenges with respect to GDPR compliance, as everyone has equal access and rights whilst working with a blockchain. Conversely, SSI systems which are based on a public permissioned blockchain are able to comply with the majority of key GDPR principles, as they comprise a governance model and are operated by a consortium of trusted organisations. Currently, EU regulators have acknowledged the requirement for further guidance on the compliance of GDPR to SSI systems [12]. The EU Blockchain Observatory and Forum has been developing a blockchain ecosystem which will be GDPR compliant and will offer several guidance and amended features for SSI and its underlying blockchain [12]. For example, the EU and government agencies can perform a significant role as an issuer of verifiable credentials and make GDPR compliance with SSI more efficient.

TABLE I
POSSIBLE GENERALISED MAPPING OF SSI ROLES WITH GDPR ROLES

SSI Roles	**GDPR Roles**
Holders	Data Controllers
Issuers	Data Controllers/Data Processors
Verifiers	Data Controllers/Data Processors
Developers	Mostly No GDPR Roles
Transaction Authors	Data Controllers
Transaction Endorsers	Data Processors
Node Controllers/Stewards	Data Processors
Identity Providers	Data Controllers/Data Processors

5. COMPARATIVE ANALYSIS OF UPORT AND SOVRIN SSI ECOSYSTEMS BASED ON THE KEY PRINCIPLES OF GDPR

5.1. uPort SSI Ecosystem

The uPort system is an open-source identity management system providing self-sovereign identity to users, organisations, and entities [13]. It is based on the public permissionless blockchain Ethereum and utilises its smart contracts for identity management [14], [15]. uPort is effective with on-chain Ethereum transactions in addition to the ability of exchanging data off-the-chain. The uPort provided identity is completely owned and governed by the owner of that identity and not by the third-party. Moreover, identity related personal data is held by the owner in their digital wallet thus, information releases are kept to a minimum [16]. Fig. 2 shows the layered architecture of uPort SSI ecosystem exhibiting various roles as exemplified in Table I to understand GDPR compatibility [14], [17], [18].

End User Interface Layer: At this layer, each user owning a uPort identity has access to the digital wallet on a smartphone, tablet, desktop, or other local device, which holds credentials containing certain information about that identity owner. Here, an issuer creates and issues credentials to a holder and a verifier receives and verifies it.

Provider Layer: At this layer, providers (mostly developers) offer software for the integration of uPort functionality and services.

Smart Contract Layer: This layer runs on a public permissionless blockchain. A smart contract which is a piece of code that is capable of monitoring, executing and enforcing an agreement without the involvement of third parties. Every identity is associated with a smart contract. There are different types of smart contract for different functions related to an identity: controller contract, proxy contract and registry contract. As uPort is based on public permissionless blockchain Ethereum, therefore anyone can run a node and interact with the blockchain.

5.2. Sovrin SSI Ecosystem

The Sovrin system is an open-source identity management system for providing self-sovereign identity to users, organisations, and entities [19]. It is based on the public permissioned blockchain Hyperledger Indy. It is a permissioned blockchain, therefore, only trusted institutions called stewards can operate nodes while participating in the consensus process. The Sovrin provided identity is completely owned and governed by the owner of that identity and not by the third-party. Moreover, identity related personal data is held by the owner in their digital wallet thus, information releases are kept to a minimum [19]. Fig. 3 shows the layered architecture of Sovrin SSI ecosystem exhibiting various roles as exemplified in Table I to understand GDPR compatibility [18], [19], [20].

Credential Exchange Layer: At this layer, each user who owns a Sovrin identity has access to the digital wallet on a smartphone, tablet, desktop, or other local device, which holds credentials containing certain information about that identity owner. Here, an issuer creates and issues credentials to a holder and a verifier receives and verifies it.

Agent-to-Agent Layer: At this layer, developers develop hardware or software offering Sovrin functionality and agencies provide services to identity owners.

Sovrin Ledger Layer: This layer runs on a public permissioned blockchain in accordance with the Sovrin Governance Framework, where, stewards operate a node and transaction authors write transactions which are approved by transaction endorsers. The only types of information written to the Sovrin Ledger is the following: schema, credential definitions, participants and roles, revocation registries, anywise DIDs (for the creation of a non-reciprocal relationship).

5.3. Comparative Analysis

Table II presents the comparative analysis of uPort and Sovrin SSI ecosystems based on the key GDPR principles. This comparative analysis shows that the uPort ecosystem is based on a public permissionless blockchain posing greater challenges with respect to GDPR compliance; whereas Sovrin ecosystem is based on a public permissioned blockchain, which is able to comply with the majority of key GDPR principles, as it comprises a governance model and is operated by a consortium of trusted organisations. This confirms the previous analysis which indicated that an SSI system based on a public permissioned blockchain is relatively more compatible with GDPR. This GDPR compatibility could be enhanced by employing a private permissioned blockchain but it may affect some of the basic principles of SSI such as sovereignty and control of personal data.

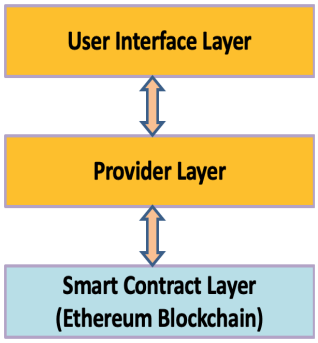

Fig. 2. uPort Layers

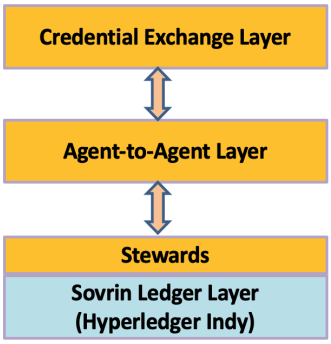

Fig. 3. Sovrin Layers

6. Conclusion

This paper evaluated the compatibility of SSI with the key GDPR principles. Subsequently it evaluated two different types of SSI ecosystems public permissionless blockchain based SSI uPort and public permissioned blockchain based SSI Sovrin, according to the various defined roles and their compatibility with GDPR roles. Finally, it performed a comparative analysis of uPort and Sovrin ecosystems to assess their compliance with the key GDPR principles. It concluded that SSI systems which are based on a public permissioned blockchain are able to comply with the majority of key GDPR principles as compared to SSI systems which are based on a public permissionless blockchain. In future, it will be worthwhile analysing some other emerging SSI ecosystems and their compliance with the key principles of GDPR.

References

[1] N. Naik and P. Jenkins, "A secure mobile cloud identity: Criteria for effective identity and access management standards," in *2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud 2016)*. IEEE, 2016.

[2] ——, "Securing digital identities in the cloud by selecting an apposite federated identity management from SAML, OAuth and OpenID Connect," in *11th International Conference on Research Challenges in Information Science (RCIS)*. IEEE, 2017, pp. 163–174.

[3] P. Windley. (2017) Fixing the five problems of internet identity. [Online]. Available: https://www.windley.com/archives/2017/10/fixing_the_five_problems_of_internet_identity.shtml

[4] N. Naik and P. Jenkins, "An analysis of open standard identity protocols in cloud computing security paradigm," in *14th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2016)*. IEEE, 2016.

[5] N. Naik, P. Jenkins, and D. Newell, "Choice of suitable identity and access management standards for mobile computing and communication," in *2017 24th International Conference on Telecommunications (ICT)*. IEEE, 2017, pp. 1–6.

[6] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *The Sovrin Foundation*, vol. 29, 2016.

[7] A. Palomares. (2019) The next identity management evolution: Self sovereign identity. [Online]. Available: https://atos.net/en/blog/the-next-identity-management-evolution-self-sovereign-identity

[8] N. Naik and P. Jenkins, "Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems," in *2020 IEEE International Symposium on Systems Engineering (ISSE)*. IEEE, 2020.

TABLE II
COMPARATIVE ANALYSIS OF UPORT AND SOVRIN SSI ECOSYSTEMS BASED ON THE KEY PRINCIPLES OF GDPR

GDPR Principles	uPort SSI Ecosystems	Sovrin SSI Ecosystems
1. Lawfulness, Fairness and Transparency	User is the sovereign owner of their identity and personal data, and controls the access to personal data. Therefore, this provides users greater control over collecting, storing and processing of personal data.	User is the sovereign owner of their identity and personal data and controls the access to personal data. Therefore, this provides users a greater control over collecting, storing and processing of personal data. It is a relatively fairer and transparent system.
2. Purpose Limitation	It is a **Privacy Preserving** system. Users are not required to disclose personal data in order to create uPort identifiers for low value accounts. It uses various methods to minimize the correlation of a user's on-chain smart contract interactions between different dapps. Identity owners decide to whom they want to share what personal data for what purpose by giving their consent.	It is a **Privacy by Design and Privacy by Default** system. It uses anonymous credentials based on **Zero-Knowledge Proofs (ZKPs)**, which allows users to share the information that maintains the anonymity of users. Identity owners decide to whom they want to share what personal data and for what purpose by giving their consent.
3. Data Minimisation	Identity and its related personal data is stored on the storage **owned or controlled** by the identity owner. However, data stored on the blockchain poses some challenges as a blockchain is an append-only database that is constantly growing when new data is added to it. Additionally, data is replicated on many different locations, which is a significant challenge for the data minimisation principle.	Identity and its related personal data is stored on the storage of an **Edge Agent** controlled by the identity owner, but it may also be stored on the storage of a **Cloud Agent** (protected from unauthorized access). However, data stored on the blockchain poses some challenges. It is currently a challenging task as a blockchain is an append-only database that is constantly growing when new data is added to it. Additionally, data is replicated on many different locations, which is a significant challenge for the data minimisation principle.
4. Accuracy	User can update their attributes and revoke their verifiable credentials. However, the immutability of data, transactions, and blocks in a blockchain potentially affects the rights of data subjects.	It has a **hierarchy of roles**, where a user can update their attributes and revoke their verifiable credentials in an authorised manner through that hierarchy. However, the immutability of data, transactions, and blocks in a blockchain potentially affects the rights of data subjects.
5. Storage Limitation	It does not store identity and its related personal data on the blockchain. This assists in resolving the storage limitation issue of personal data to a greater extent. However, the deletion of other blockchain data may not be easy due to the immutability of the blockchain.	It does not store identity and its related personal data the on the blockchain. This aids resolution of the storage limitation issue of personal data to a greater extent. However, the deletion of other blockchain data may not be easy due to the immutability of the blockchain.
6. Integrity and Confidentiality	It is based on a public **permissionless** blockchain, therefore, **anyone** can operate nodes and take part in the consensus process. It requires credentials and biometry for controlling identity through blockchain. Users can securely publish their identity including transfer their credentials, sign transactions and control their keys and data.	It is based on a public **permissioned** blockchain, therefore, only **trusted institutions called stewards** can operate nodes while participating in the consensus process. It requires credentials and biometry for controlling identity through blockchain. Users can securely publish their identity including transfer their credentials, sign transactions and control their keys and data using powerful cryptography.
7. Accountability	The use of blockchain offers the opportunity to raise the level of accountability and insight in the data and transactions. However, currently, it does **not** provide a governance framework for greater accountability.	The employment of **Governance Framework** and use of blockchain support greater accountability where the competent authority can apply necessary technical, procedural, and organizational measures to comply with this principle. The **Sovrin Governance Framework (SGF)** is the legal foundation of the Sovrin Network as a global public utility for providing greater accountability.

[9] Sovrin.org. (2018) Sovrin: A protocol and token for self-sovereign identity and decentralized trust. [Online]. Available: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[10] N. Naik and P. Jenkins, "Self-Sovereign Identity Specifications: Govern your identity through your digital wallet using blockchain technology," in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud 2020)*. IEEE, 2020.

[11] Ico.org.uk. (2020) Guide to the general data protection regulation (GDPR). [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

[12] Eublockchainforum.eu. (2020) Eu blockchain observatory and forum: An initiative of the european commission. [Online]. Available: https://www.eublockchainforum.eu/

[13] uport.me. (2020) uport identity system. [Online]. Available: https://www.uport.me/

[14] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena. (2018) Uport: A platform for self-sovereign identity. [Online]. Available: https://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf

[15] N. Naik and P. Jenkins, "uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain," in *2020 IEEE International Symposium on Systems Engineering (ISSE)*. IEEE, 2020.

[16] M. Sena. (2018) Privacy preserving identity system for Ethereum dApps. [Online]. Available: https://medium.com/uport/privacy-preserving-identity-system-for-ethereum-dapps-a3352d1a93e8

[17] P. Braendgaard. (2017) What is a uPort identity? [Online]. Available: https://medium.com/uport/what-is-a-uport-identity-b790b065809c

[18] P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 20–29, 2018.

[19] Sovrin.org. (2020) Innovation meets compliance data privacy regulation and distributed ledger technology. [Online]. Available: https://sovrin.org/wp-content/uploads/GDPR-Paper_V1.pdf

[20] ——. (2019) Sovrin Glossary V2. [Online]. Available: https://sovrin.org/wp-content/uploads/Sovrin-Glossary-V2.pdf