Evaluating Blockchain within the Legal Frameworks of the *General Data Protection Regulation* and the *California Consumer Privacy Act of 2018*

August 3, 2018

Edward Percarpio
Regulatory Lead, Polyphonic Labs

Konrad Rauscher
Founder, Technology Lead, Polyphonic Labs

REDACTED

Table of Contents

EXECUTIVE SUMMARY

This Report examines the relationship between blockchain and two recently codified data privacy regulations: the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act of 2018 (CCPA). In light of new obligations imposed by these regulations (e.g. individual rights to access, delete, and port their personal data), privacy and security experts have questioned whether blockchain is able to comply with these new requirements. Skeptics note that blockchain has certain intrinsic characteristics – such as the immutability of the ledger – that prohibit the implementation of compliance requirements such as rectification or deletion. Proponents argue the opposite, stating that blockchain poses unique solutions to implementing otherwise difficult compliance requirements (e.g. verifiable erasure, 'objective' record-keeping). However, the current level of discourse around these topics often regards "blockchain" as a single immutable concept without considering how public, permissioned, and private ledgers offer unique challenges and different compliance obligations. From a legal perspective, too often does polemic jump to compliance obligations without first considering whether and how blockchain networks fit within the scope of the law itself.

When discussing blockchain/distributed ledger architectures and data protection regulations, further consideration is given to the application of these frameworks to the derivatives market. This additionally necessitates a comparative regulatory analysis of how GDPR and Know-Your-Customer (KYC) and Anti-Money Laundering (AML) requirements interact with each other and with blockchain.

This Report achieves the following tasks:

1. Describes the scope, definitions, and responsibilities of actors under the GDPR, CCPA, and American KYC-AML regulations.
2. Discusses the role of actors in a blockchain network and their legal responsibilities.
3. Examines the impact of different blockchain architectures on the legal responsibilities of its actors.
4. Discusses the ability of different distributed ledger architectures (e.g. Sovrin, Hyperledger Fabric, Teechain) to comply with regulatory requirements relevant to the derivatives market (e.g. KYC-AML, FCRA, GLBA, Dodd-Frank).
5. Provides recommendations for leveraging blockchain such that:
    a) Regulatory obligations can be met and, in certain circumstances, enhanced as opposed to traditional non-blockchain architectures.
    b) Entities can apply multiple blockchain designs (public, permissioned, private) to comply simultaneously with multiple national regulatory requirements.
    c) Security can be preserved in a post-quantum environment, while simultaneously maintaining regulatory transparency and accountability.

1 Introduction

The General Data Protection Regulation (GDPR) is a European Union regulation that offers EU citizens increased rights over their personal data, such as the right to access, port, rectify, and delete this data. Since the adoption of the GDPR in 2016, countries around the world have scrambled to implement similar principles in order to ensure that data remains able to flow smoothly across borders.[1] Notable countries that have made legal movements towards GDPR-oriented legislation include Brazil (LGPD), Japan (APPI), South Korea (PIPA), and Canada (PIPEDA). Some (e.g. Brazil) have implemented new legislation entirely, while others are updating existing legislation to maintain an "adequacy" designation (e.g. Canada).

While the US has yet to reach a national determination of whether it will toe the line, California recently passed a law granting its residents data privacy rights very similar to those afforded by the GDPR. Slated to come into effect January 1, 2020, the *California Consumer Privacy Act of 2018* (hereafter referred to as CCPA), puts pressure directly on the heart of the American tech industry to build technologies that implement these rights, or otherwise suffer strict penalties from both Californian and European regulators.

This shifting regulatory environment has prompted discussion around whether and how blockchain fits into these new regulatory requirements. Many pundits feel that blockchain is inherently incompatible with certain GDPR principles because of its immutability. From the perspective of these commentators, if an individual wishes to exercise their right to rectify or delete their personal data, companies that use blockchain technology to record personal data will lack the ability to remove or alter it and thereby fail to comply with two critical GDPR principles.[2] Others worry that even if one were to encrypt personal data on-chain as a potential solution for erasure,[3] blockchain's immutability makes it impossible for entities to update their encryption standards as existing methods of encryption become insecure with advances in processing power and decryption technologies.

While these arguments raise valid points about the potential conflict of certain blockchain constructs with current privacy laws, they often fail to discuss critical nuances in legal scope and requirements, and in different blockchain designs. This failure leads to myopic or misleading ideas of where/how blockchain and the GDPR help or hurt one another.[4] This report aims to provide a nuanced and thorough examination of the GDPR/CCPA as they pertain to blockchain, and provide recommendation for how blockchain could be leveraged to support certain GDPR principles and requirements.

[1] Chapter 5 of the GDPR restricts transfers of EU residents' personal data unless the country or entity has similarly robust legal safeguards in place. For more information, see the Annex.
[2] For examples of this concern in popular discourse, see here, here, or here.
[3] This will be discussed later in the report, but the essential idea is that an entity can implement effective data "erasure" by throwing away the encryption key, which makes the encrypted data inaccessible.
[4] E.g. the (mistaken) belief that personal data must be written on-chain, or the (mistaken) belief that the GDPR restricts personal data from leaving the EU, which would cause problems with blockchain's decentralized ledger system.

Before analyzing the GDPR/CCPA and blockchain as either symbiotic or conflicting constructs, it is essential that we first outline the parameters that constrain the scope of each law and bound the space in which we will discuss blockchain. This includes defining 1) the actors and their responsibilities in each law and in blockchain networks, 2) the types of personal data that each law regulates, and 3) the geographic/operational boundaries to which the laws restrict themselves. Then we can apply "blockchain" – or different blockchain manifestations and applications – to these legal structures and requirements to see how they impact or conflict with each other.

A final note regarding the legal scope of the Report: since the object of this Report is to contrast technological affordances/limitations with legal requirements, we will restrict our discussion of the GDPR/CCPA to the particular aspects of the laws that impose these requirements. This means that we will focus mostly on pertinent data subject rights (GDPR Arts. 15-20, CCPA Sec. 1798.100, 1798.105), business obligations (GDPR Arts 24-30), security and data protection by design requirements (GDPR Arts. 25 & 32), and certification standards (GDPR Arts. 42 & 43). This is not to say that other requirements (e.g. transparency obligations, data breach protocol) are less important; they just happen to be less relevant to a discussion involving blockchain. However, we do provide an Annex at the end of the Report that describes other critical GDPR requirements that fell beyond the scope of the Report.

6 Sovrin as a Use Case for Achieving Regulatory Compliance

6.1 Purpose and Structure

This section demonstrates how regulatory compliance can be achieved with distributed ledger networks. We consider distributed ledger models that we believe represent industry best practice in the field of regulatory compliance. We use one industry leader in particular – the Sovrin identity management system – as a case study to illustrate how distributed ledger technologies can help achieve regulatory compliance. By focusing on Sovrin, we do not mean to imply that Sovrin is the only, or the best, method for achieving compliance with GDPR/CCPA and KYC-AML regulations. Rather, due to limitations in scope, we chose to provide greater detail in the technical and legal implementation of a single model rather than giving a more superficial overview of many models. That said, alternative models and techniques – such as Hyperledger Fabric and Trusted Execution Environments – are briefly discussed as an addendum to the case study.

Given the unique nature of Sovrin's approach to digital identity, we begin with a primer on Sovrin's conceptual framework for digital identity. This primer serves two purposes:

- to provide a foundation for understanding how Sovrin helps meet GDPR/CCPA obligations
- to describe a technical breakthrough in how roles can be assigned to actors in digital systems that protects the privacy of individuals and entities

The primer is structured as follows:

- Brief introduction to the Sovrin protocol
- Description of the three dimensions across which Sovrin separates digital identity
- Discussion of what takes place at the intersections of these three dimensions
- Overview of the significance of the Sovrin approach

Following the Sovrin primer, we discuss how Sovrin achieves compliance with core data protection principles and privacy by design requirements specified by the GDPR and CCPA in Sections 2-4 of this Report. Section 6.3 evaluates Sovrin's compatibility (and, generally, a Sovrin-type approach) with core data protection principles under the GDPR. Section 6.4 discusses Sovrin's ability to meet data subject rights requirements under the GDPR. Note: this section focuses heavily on the GDPR and less so on the CCPA. This is because as demonstrated in Sections 2.3 and 4.3, CCPA requirements, while slightly different in scope and legal implementation, are technically the same if not weaker to implement than GDPR requirements. In other words, if Sovrin can support data subject rights under the GDPR, it can also support consumer rights under the CCPA.

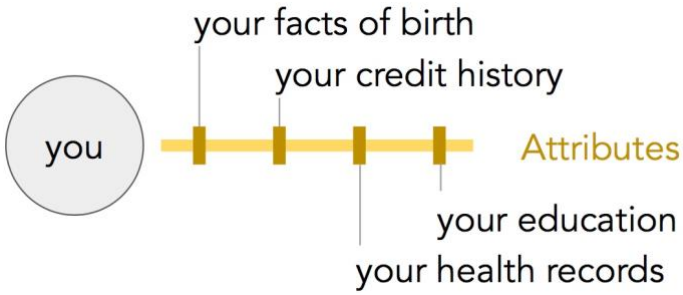
6.2 Sovrin Primer

The Sovrin Protocol is a set of standards, patterns, and tools that facilitate trusted interactions. Sovrin is rooted in the principle of Self-Sovereign Identity (SSI). SSI places the individual or entity (called an Identity Owner) in charge of their own identity management, as opposed to the

cross-context correlations that lead to privacy loss and data leakage via cookies, web beacons, and other technologies on the Internet.

Note also that it is for exactly this issue of linkability that proxy - or indirect - attributes are covered under the GDPR's definition of 'personal data', the CCPA's definition of personal information, and the NIST framework's definition of PII. As a result, the scope of these regulations cover vast swaths of data and metadata in interactions over the Internet (e.g. cookies, web beacons, IP addresses, and any other information linked to them). Yet because identifiers cannot be correlated to the same Identity Owner unless the Identity Owner authorizes the link through a Credential, these types of information (cookies etc.) would arguably fall out of the scope of personal data/information. This would not only increase consumer privacy but also decrease liability for companies handling this data. Most of all, it would reduce the pervasive issue of proxy identification in a traditional TCP/IP architecture.

6.2.1.2 Attributes



While I will have many DIDs over the course of my interactions on Sovrin, I only have one identity behind each DID. When I establish my identity on the Sovrin network, I am given a private ledger -- called a "Wallet" -- where I can securely store my attributes. My attributes are established through Claims, which are attestations made either by myself (the Identity Owner) or by another party. An Identity Owner who makes a Claim about another Identity Owner is called an Issuer. Claims are digitally signed by Issuers so that anyone receiving the Claim can know who issued it.

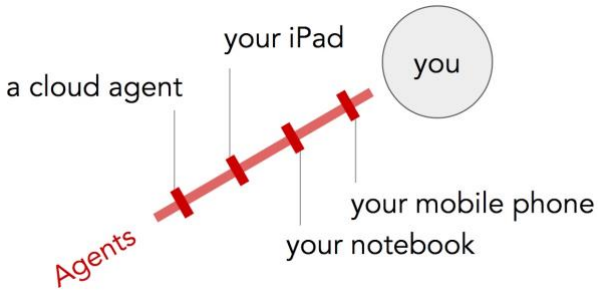
For example, say I have a Claim in my Wallet that represents my driver's license. In order for my driver's license to be valid, it had to be signed by my state's Department of Transportation. Upon producing the Claim for my driver's license, the DoT attested to multiple attributes associated with my driver's license (e.g. eye color, date of birth, height, etc.). Now, perhaps I want to establish a relationship with a bank through Sovrin, but the bank needs to verify my birthdate before I can open a bank account. Luckily, this attribute has been attested through the Claim representing my driver's license. I can now produce my birthdate along with the DoT's Claim that attests this particular attribute. (Note that I do not need to produce my entire driver's license - just the attribute necessary.) The bank will now be able to see that my DID now has a "date of birth" attribute linked to it, attested to by the DoT. If the bank agrees that this is a trusted Issuer, then it will proceed and open an account for me. If the bank needs more information, the process repeats.

Before moving on, it is important to note how DIDs work with attributes in situations like this. When the DoT issued a Claim about my attributes, it made a Claim to the DID associated with me. Yet this Claim is not intrinsically linked to the DID such that I can only use it if I am using the DID. Instead, the Claim was stored on my private ledger (Wallet) so that I could reproduce it for

other pairwise relationships in which I have a different DID than the one in which the Claim was originally produced. This gives me added privacy because Claims cannot be linked together unless I choose to do so for that particular relationship. (For example, if the bank needed to know my birthdate and blood type, I could produce the DoT's Claim about my birthdate and my doctor's Claim about my blood type. These Claims would now be linked to the same private DID used for my relationship with the bank.)

6.2.1.3 Agents

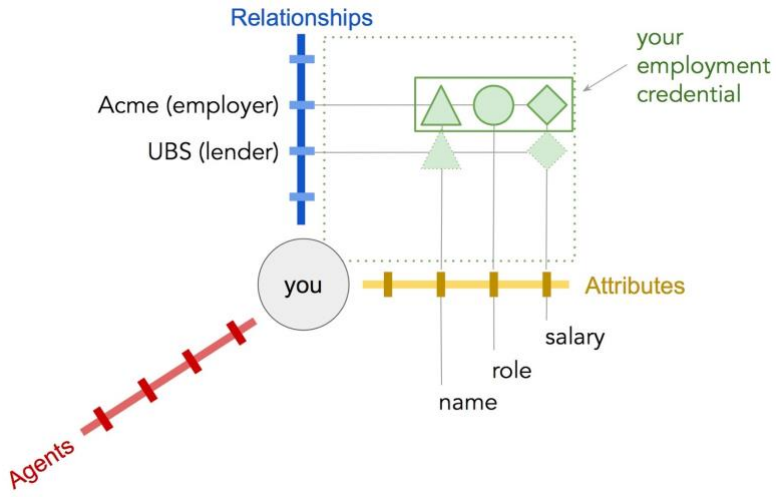
Agents are devices or services that fulfill tasks for us. Like in a traditional Internet network, devices are linked to our identities and also to the network through IP addresses. These can include a mobile phone, a physical notebook, software, or a third-party service provider. On a Sovrin network, I can only have one agent per device. I can also give an agent an endpoint, which can then serve as a simple message proxy, or I can even have it interact with other entities outside the Sovrin network.



6.2.2 Interactions Between Dimensions

6.2.2.1 The Relationship-Attribute Plane

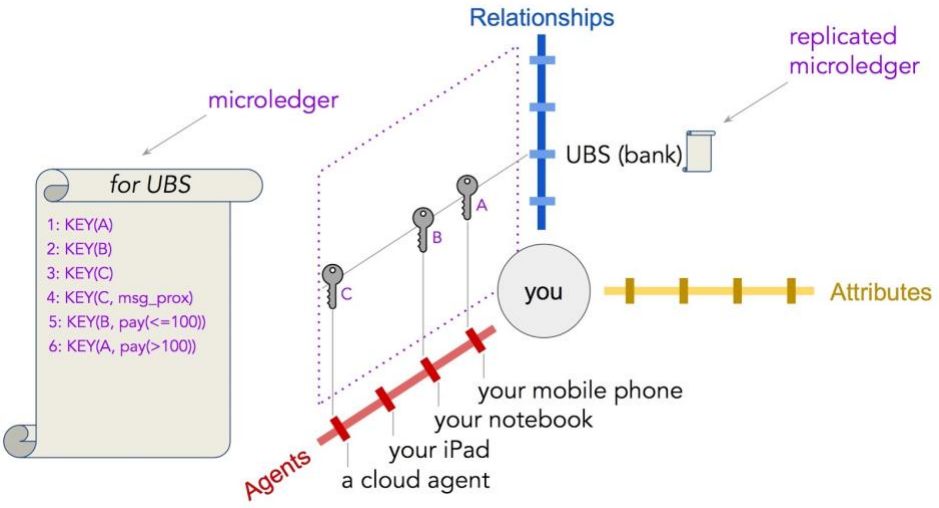
For every relationship, I can choose which attributes about my identity I wish to share and 'link' together as belonging to me via my pairwise DID. As referenced in an earlier example, it is common for entities to need more than one attribute over the course of a relationship. For example, in KYC-AML processes for CIP, financial institutions need at minimum four attributes: name, date of birth, address, and identification number. Through Sovrin, I am able to pick these specific attributes and link them together through a correlation proof to establish what we can call a "CIP Credential".



In this example, an 'employment credential', consisting of three claimed attributes, has been shared with Acme. Only the claimed attributes of 'salary' and 'name' have been shared with UBS. Such selective disclosure is key to 'data minimization

6.2.2.2 The Relationship-Agent Plane

Because an Identity Owner typically has multiple relationships and thus multiple DIDs, an agent must be able to support multiple DIDs. The Relationship-Agent plane is represented by a "Relationship State Machine," which is implemented with a microledger replicated across the Agents managing a relationship. Agents are classified within the microledger so the other party (or parties) in the relationship know how to regard each agent (identified by a public key). For example, an agent may not be authorized to sign on behalf of a person, but it may be authorized to communicate GPS coordinates or be a message relay. Note that an agent does not have its own DID - DIDs are orthogonal to Agents. Agents can be identified by a local name, or by the public key used in a particular relationship. Each DID-Agent combination requires a separate key. Because an endpoint must be unique per relationship (for the same reasons a private DID is unique per relationship), an agent must also be able to support multiple endpoints. Agents are authorized for certain types of activity for each relationship. This allows the Agent owner to use different agents in different contexts.



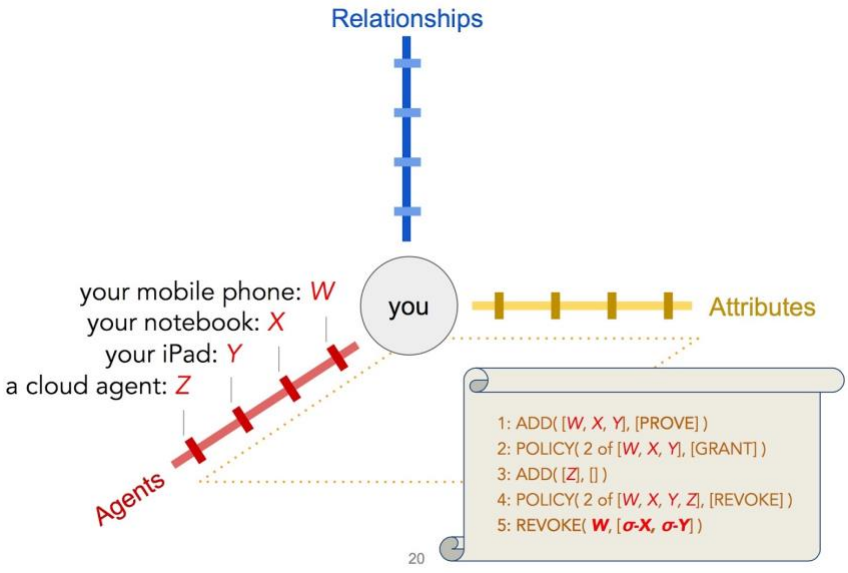
A key unique to the relationship with UBS is established for three of four Agents. These keys can define allowed behavior for each Agent, and also serve to identify the Agent involved in a given transaction. The microledger maintained by the agents on both sides of a relationship keeps track of what has taken place between both parties.

What's a Microledger?

A microledger is a small, ordered, append-only record of events that can be stored in a file or a database table. The microledger contains a log of events plus a merkle tree over those events. The merkle tree makes it easy to detect tampering and allows for safe and efficient propagation of new events. A microledger will also have a state, which is a projection of the events recorded in the microledger. A microledger is replicated across Agents involved in managing a relationship.

6.2.2.3 The Agent-Attribute Plane

The keys Agents have are stored in their own Wallets. Wallets can hold Credentials (verifiable collections of attributes). Agents have special keys that allow them to be able to generate proofs about Credentials they hold. The Agent Authorization Policy is a combination of a ledger smart contract and a cryptographic accumulator that allows for proving in zero knowledge that a device is an authorized device. This allows a person or organization to have a sophisticated recovery policy and to be able to revoke a compromised Agent (as exemplified in the diagram). A person may selectively copy credentials to different agents, effectively limiting which credentials are provable from which agents.



The ledger in the diagram above exemplifies the following process flow for revoking a lost phone as an Agent:

1. W, X, Y are established as Agents of the Identity Owner, and are authorized to PROVE (i.e. can generate proofs about the credentials they hold)
2. Policy established that two of the set {W, X, Y} are required to GRANT authorizations Agents
3. Z is established as an Agent of the Identity Owner, with no authorizations.
4. Policy is established that two of the set {W, X, Y, X} are required to REVOKE an Agent
5. Both X and Y are used in a request to REVOKE W, the lost phone

6.2.3 Summary

From this primer, a few observations can already be made. First, despite concerns about the incompatibility of blockchain with GDPR over data storage implications, Sovrin is able to solve this problem by not storing personal data "on-chain" (i.e. on the public Sovrin ledger). Rather, all personal data—including Credentials and Claims—live off the ledger in the Wallets and Agents under an Identity Owner's control. Furthermore, all transactions of this data take place off-ledger in the Agency Layer. Because the only information ever stored on the public Sovrin Ledger does not pertain to "natural persons", such data is is outside the scope of GDPR as the regulation does not apply to entities or things.

Second, so long as an Identity Owner uses a unique DID for each relationship, personal data attributes are only correlated to each other if the Identity Owner authorizes their 'linkage' in a

private relationship using a Credential. A Sovrin Identity Owner's ability to 'correlate' attributes on an as-needed and selective basis represents a technical achievement with high significance for privacy regulation compliance.

Moving of data storage and processing off-chain to the extent that Sovrin's model for SSI represents may raise concerns by those familiar with how conventional, public blockchains achieve their immutable and trustless characteristics. It should be noted, however, that Sovrin's protocol utilizes the public Sovrin ledger as an accounting mechanism for maintaining integrity and trustlessness in off-ledger relationships. It should also be noted that Sovrin is able to achieve viable off-ledger transactions without introducing a central authority.

6.3 Fitting Sovrin within Core Data Protection Principles

This subsection evaluates Sovrin's ability to meet data processing principles under Article 5 of the GDPR.

Obligation:

Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.

Article 6 of the GDPR sets out six lawful bases for the processing of personal data: consent, contract, legal obligation, vital interests, public interest, and legitimate interests.

While none of these lawful bases are new to the GDPR, the "consent" requirement has become more stringent. Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Additionally, the data subject has the right to withdraw this consent at any time and must be notified of this right at the time that consent is obtained. Finally, the data controller must be able to prove that this level of consent was obtained.

In sum, under the high standard set out in the GDPR, valid consent must be:

- freely given
- obtained through an affirmative act of the data subject
- revocable
- provable

Solution:

In the Sovrin model, transactions rely on a technical system of explicit consent for data to be shared in a pairwise relationship. However, it is the onus of the relying party (e.g. the bank) to properly notify the Identity Owner exactly how their personal data (e.g. a Claim) will be used. This does not relate to Sovrin or any technical architecture for that matter, but rather on controller-to-subject communication. It is also important to note that while consent is relied on as a technical means by which an Identity Owner shares data, it may not be the appropriate lawful basis. In the bank

example above, for instance, the bank would be using a lawful basis of "legal obligation" or performance of a contract (e.g. opening an account upon request) to collect CIP data.

While lawful basis is more strictly legal and dependent on the context of the relationship, it is important to bear in mind the rights enablement affordances that Sovrin achieves. For example, the Identity Owner can access the information held about them in any pairwise relationship by merely viewing the transparent Claims record. Since DIDs and strict access controls around extra-relationship information sharing make it such that information cannot be collected without literal disclosure from the Identity Owner (i.e. data subject). Regarding data portability, the Identify Owner can switch Agents or Wallet providers at will, by simply moving its claims from one private ledger to another. Objection and deletion can also be achieved through the Identity Owner's ability to revoke an entity's access to a particular Claim. Rectification, similarly, would consist of an Identity Owner revoking an out-of-date Claim and re-disclosing the correct Claim to the relying party. (Sovrin's ability to fulfill data subject rights obligations will be further expounded in Section 6.4).

However, if consent is indeed relied upon by an entity, the Sovrin network architecture allows both parties to easily track the consent along with its revocations and resubmissions. Because both the Identity Owner and the relying party both maintain a log of each digitally signed transaction on their respective copies of their shared private microledger, either can provide proof of consent (or lack thereof) to an auditor. Not only does the individual Identity Owner control the sharing of his personal data, but he is provided with a technical infrastructure that automatically logs consent receipts. This enables an unprecedented degree of transparency to all parties.

Obligation:

(b) Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

The **purpose limitation principle** means that personal data collected for one purpose should not be used or repurposed for a new, incompatible purpose. It is closely related to the lawfulness, fairness, and transparency principle and is designed to minimize correlation risks to the individual data subject and to prevent data controllers and processors from exceeding the limits of lawful processing of personal data. Under the GDPR, a party who is not necessarily a data controller can become one by exceeding the scope of processing that it has been authorized to undertake (at which point it breaks its legal contract with the controller and can incur controller-level liabilities under the Regulation). Thus, it is in the interest of processors to comply with the purpose limitation principle by not exceeding their authorized scope of processing.

Solution:

In the context of Sovrin, a Proof Request can show the purpose(s) for which data is being requested. A Verifier can delete this data once it has executed whatever transaction it was needed

for, and then can simply request it again if and when it's needed. The Verifier can, if necessary, make multiple requests with different purposes, each time making those purposes fully transparent to the Identity Owner who is the subject of the Proof Request. Through the use of a Sovrin Agent, an individual can compare the scope of a Proof Request and its purpose(s) against pre-defined consent parameters in order to more efficiently determine whether the data is being requested for a purpose that is "specific, explicit and legitimate." In this way, the Agent acts like an intelligent browser, and individuals can implement mechanisms (i.e. Link Contracts) akin to browser settings that help enforce the parameters of personal data disclosure. (This is also forward-looking towards compliance with the forthcoming e-Privacy Regulation).

Verifier: An Identity Owner that wants to rely upon (i.e. obtain access to and be able to evaluate the validity of) the claimed attributes of another Identity Owner

Proof Request: A request on the part of a Verifier for information (i.e. one or more cryptographically established identity attributes) from an Identity Owner

Link Contract: A record of who is sharing data with whom, for what purpose and with what controls on its usage. In Sovrin, a link contract is stored inside a XDI graph. Link contracts are themselves expressed in XDI. Among other stipulations, a link contract can specify how parties prove their identity, how updates are handled, who can use the data and how the data can be used. A link contract is stored on the XDI server (hosted by Agents) at each end of an off-chain relationship, such that the Agents for both parties adhere to the specifications of such a contract.

Obligation:

(c) Personal data must be adequate, relevant and limited to that which is necessary in relation to the purposes for which it is being processed.

The **data minimization principle** has multiple dimensions to it, including limiting the personal data that is collected, processed, and stored. In terms of collection and processing, the same features of Sovrin that give effect to the purpose limitation principle assist in achieving data minimization. Collection is limited by the Identity Owner's control over the sharing of their data and technical methods that minimize the amount of data that is shared to achieve a given purpose, thereby minimizing the data that is collected and ultimately processed. In Sovrin's model, the Identity Owner decides precisely which, if any, identity attributes it wants to disclose in the form of the Proofs it produces about the Credentials and Claims in her Wallet.

Solution:

Sovrin is specifically designed to minimize the storage of personal data. Despite concerns about the incompatibility of blockchain with GDPR over data storage implications, Sovrin solves this problem by not storing personal data "on-chain" (i.e. on the public Sovrin Ledger). Rather, all personal data—including Credentials and Claims—live off the ledger in the Wallets and Agents under the Identity Owner's control. Furthermore, all transactions of this data take place off-ledger in the Agency Layer.

Obligation:

(d) Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

The **accuracy principle** means that data controllers are responsible for taking reasonable steps to ensure that the personal data they hold and process is kept accurate and up to date. The accuracy principle is designed to prevent decisions that have legal or other significant effects on data subjects from being taken on the basis of incomplete or inaccurate information, and is closely related to the lawfulness, fairness and transparency principle. The accuracy principle is also the basis for several of the data subject's substantive rights, including the rights of access, rectification, and erasure.

Solution:

The distributed ledger technology that underpins Sovrin's approach to SSI allows for constant updating and pruning of the public digital record and allows a Verifier to ascertain the status or validity of a Credential or Claim in near-real time by referencing Revocation Registries housed on the Sovrin Ledger.

Revocation Registry

"Revocation Registries" are cryptographic numbers (more specifically, an elliptic curve accumulator) maintained on the Sovrin Ledger by Issuers of revocable digital Credentials that use zero knowledge cryptography to confirm or deny whether a given DID is within or outside of a set of DIDs that have been revoked by a given Issuer

Obligation:

(*e) Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is being processed.*

The **storage limitation principle** is closely related to the purpose limitation and data minimization principles and is designed to prevent unlawful and unauthorized processing and to limit the data security risks posed by the long-term storage and retention of personal data. It is also related to the accuracy principle and the right to be forgotten in so far it is aimed at preventing decisions taken and legal effects for data subjects on the basis of inferences that may be drawn from stale data. Moreover, in the event of a request to be forgotten per the data subject's right to erasure, the acceptable data retention period for a controller or processor may be further shortened from what would ordinarily be a lawful period of time. The exception is for data retained and processed for "historical, statistical or scientific purposes," in which case the public interest may override the data subject's interests.

Solution:

Sovrin enables new data retention strategies that move from a traditional "data management" approach to a "data access" approach where you only use the precise data that you need when you need it, then delete it. You can then repeat if and when necessary. On the whole, this minimizes long-term storage requirements, presents a much lower organizational risk to processors, and facilitates compliance more effectively than the data management approach. Upon receipt of some personal data, the Verifier can execute the transaction they need to carry out and then simply delete the data if it is not needed it anymore. All they need to retain is the DID for the Identity Owner. If the data is needed again, it can be requested again using the secure, private and mutually authenticated Connection with the data subject via their DID.

Finally, because the vast majority of data exchanges in Sovrin happen in the Agency Layer in the context of private encrypted pairwise channels, the storage limitation principle is somewhat self-enforcing. Unique DIDs are created when a pairwise Connection is made and only utilized for purposes of that Connection. When the Connection is terminated (by either party), so is the storage of information in the context of that pairwise relationship.

Obligation:

(f) Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

The **integrity and confidentiality principle** is fundamentally concerned with data security and the security of processing. It is, in many ways, a threshold principle based on the philosophy that data protection cannot exist without data security. The obligation attaches to all processing, whether by a controller or processor and applies to both external (e.g. hacks) and internal (e.g. employees) security threats. One key technical or organizational measure for data security encouraged by the GDPR is pseudonymization, defined in Article 4 as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." In other words, minimize correlation risks to the individual in order to mitigate the impact of a potential security breach.

Solution:

The Sovrin approach promotes the integrity and confidentiality principle by minimizing the frequency and amount of data exchanged in the first place. As demonstrated in reference to the purpose limitation principle, data minimization and storage limitation principles above, Sovrin has made technical and policy decisions to minimize the amount of data that is shared, collected, processed and stored, including through the use of Zero Knowledge Proofs, microledgers, and private

Zero Knowledge Proofs

A zero-knowledge protocol is a method by which one party (the prover) can prove to (i.e. create Zero Knowledge Proofs for) another party (the verifier) that something is true, without revealing any information apart from the fact that this specific statement is true.

DIDs. Moreover, pseudonymization is a pillar of the Sovrin approach. All peer-to-peer communications and Credentials exchanged via Agent-to-Agent messaging are end-to-end encrypted. This means the data is not only encrypted in transit, such as it would be with HTTPS transport-layer encryption, but also the transmitted data is encrypted at rest after receipt by the Verifier, and can only be decrypted by a person or process with access to the Verifier's private key.

Instead of utilizing a public ledger, Sovrin has implemented a public permissioned model, whereby anyone can access the ledger (in terms of reading/writing to it) but only those with permission (e.g. Stewards) can run a node and participate in the consensus protocol to validate the record. This means that there is a level of governance that you could not have with a public permissionless ledger. The Sovrin Foundation implements this governance through a public Trust Framework that includes both security and privacy policies and practices that must be implemented by all Stewards to ensure the security and integrity of the Sovrin public ledger.

Trust Framework

A Trust Framework is a combination of technical "tools" (specifications) and legal/business "rules" (policies) that enables members of a community to trust each other in online transactions. In the Sovrin model, there is a base-level or foundational Trust Framework that is generally applicable to all parties who interact with or utilize the Sovrin Ledger in one form or another (the "Sovrin Trust Framework") as well as higher-level "Domain-Specific Trust Frameworks" that address the unique needs of a specific industry, community, or domain. These Trust Frameworks help address some of the key legal challenges to SSI adoption, including in relation to the GDPR.

Obligation:

(2) The controller shall be responsible for and be able to demonstrate compliance with the GDPR principles.

The **accountability principle** is closely related to the lawfulness, fairness and transparency principle and requires, at its core, an effective means to demonstrate compliance. Data controllers are primarily responsible for compliance with data protection obligations under the GDPR (see Section 2.1.2). Therefore, in order to determine the degree to which the accountability principle is given effect, we have to evaluate compliance and the auditability of that compliance in light of who the controller is in any given transaction.

Solution:

The Sovrin model for SSI promotes accountability through its multi-pronged approach to governance. At a technical level, the following elements provide an unprecedented level of accountability for controllers:

- The formation of private pairwise channels of communication
- The mutual authentication that happens through Connections

- An automatic, digitally signed, auditable record of each transaction taking place on each microledger

The Sovrin public distributed ledger allows for a fully transparent and auditable record of the public events that transpire in the Sovrin ecosystem. More importantly, in Sovrin, Trust Frameworks include legal and commercial policies that reinforce the accountability achieved by technical design decisions and introduce additional mechanisms for governance and accountability. Finally, because accountability attaches to the controller (usually the Verifier in a Sovrin-style exchange of Credentials), there are strong incentives for corporations and organizations acting as Verifiers to adopt the Sovrin solution as a means to demonstrate compliance.

Obligation: Privacy by Design and Default (Article 25)

In addition to the seven core principles outlined by Article 5, the GDPR imposes a general obligation to implement technical and organizational measures that give effect to all of these principles of data protection in an integrated fashion, an approach known as privacy by design and default. Rather than the conventional approach that companies have taken—where privacy and data protection were treated as afterthoughts left to compliance departments—privacy by design and default asks organizations to consider privacy and data protection from the start and build them in as key features of their products and services (this requires a degree of legal engineering of product offerings).

Solution:

Sovrin achieves privacy by design by establishing the following defaults within its protocol:

- *Pseudonymity by default* – the use of DIDs and public keys to achieve trustless, pseudonymous identity.
- *Private Agents by default* – the private data of Sovrin users, encrypted or otherwise, is not stored on Sovrin's ledger.
- *Selective disclosure by default* - cryptographic zero-knowledge proofs minimize the number of identity attributes that need to be shared to adequately establish identity for a given context, and only those that have been provided with the proper cryptographic keys may access these identity attributes.
- Robust governance mechanisms - including the use of a permissioned ledger and various Trust Frameworks.

6.4 Sovrin's Compliance with Data Subject Rights

Article 17 - Right to Erasure

Regulatory Obligation:

Data subjects have the right to have personal data erased under certain circumstances, including where the personal data is no longer necessary for the purpose(s) for which it was originally

collected; where the personal data was processed on the basis of consent and the individual withdraws their consent; where the individual objects to continued processing of personal data processed on the basis of legitimate interests and there is no overriding legitimate interest to continue to process it; where the data was processed unlawfully; where required by law; or where the data was processed to offer information society services to a child. This right is also designed to give effect to the accuracy principle and the lawfulness, fairness, and transparency principle.

Sovrin's Solution:

Any PII or other data that an Identity Owner may choose to associate with a DID is either (a) stored some someplace off-ledger (e.g., by a Sovrin app or agent) or (b) shared peer-to-peer with relying parties under a link contract that enables the Identity Owner to assert the right that private data be forgotten. With Sovrin's pairwise Connections and microledger technology, each individual Identity Owner will have a separate record of every data sharing event for every individual or entity they ever interacted with. An individual Identity Owner can use the records generated by their microledgers and pairwise Connections to prove what information they shared, when they shared it, and with whom they shared it to make a request to have certain data erased. Each Identity Owner in a pairwise Connection can use their respective Agent to seamlessly request the erasure of their data by the peer on the other end of the Connection. Such a request itself becomes a provable event via their shared microledger.

With this design, Sovrin infrastructure is ideal for implementing the right to be forgotten because *a* signed link contract stored with a Sovrin Agent gives an Identity Owner his/her own tool for exercising the right to erasure at any time. The Identity Owner can simply instruct his/her Sovrin agent to send a digitally signed "forget me" request to the relying party. That request includes the link contract under which the private data was shared (which also includes the Identity Owner's DID). Once the relying party verifies the digital signature on the 'forget me' request, the relying party will have everything it needs to delete the private data and return a signed acknowledgement (by either Sovrin agent or link contract) that it did so back to the Identity Owner, plus the audit trail necessary to prove compliance to a regulatory body. Because the request for erasure itself can be a provable event, if the erasure is not made the individual Identity Owner can use this proof of sharing and requested erasure to take action against a peer who continues to hold and process their data unlawfully

Articles 13 & 14 - Right of information

Regulatory Obligation:

Data subjects have the right to be informed about the collection and use of their personal data. This right is designed to give effect to the lawfulness, fairness, and transparency principle. This means that at the time when personal data is collected from an individual, the individual must be provided with information regarding the identity of the party who is collecting or requesting the data, the purposes for collecting or processing the data, how long the data will be retained, and who the data will be shared with (if anyone). This information must be provided in a concise, transparent, intelligible and easily accessible format, using "clear and plain language." These requirements do not apply where the data subject already has the information.

Sovrin's Solution:

When a Proof Request is received by an individual Identity Owner, it contains the details describing the requesting party (i.e. the Verifier) and the data that is being requested. The Identity Owner keeps their own record of this request through their Agent. If a given Verifier has already identified and authenticated itself to the Identity Owner in the process of establishing a pairwise Connection and making a Proof Request, the individual can be said to already have the information, meaning these obligations are automatically fulfilled for a repeat of the same Proof Request. In Sovrin's implementation of SSI, the Identity Owner has full control over their identity attributes. This means that the Identity Owner, as the data subject, will at all times have this information, which means the right of information is automatically realized in Sovrin's implementation of Self-sovereign Identity.

Article 15 - Right of Access

Regulatory Obligation:

Data subjects have the right to request and obtain access to their personal data and certain other supplementary information. This right is also designed to give effect to the lawfulness, fairness, and transparency principle. The right of access gives the individual data subject a right to obtain confirmation that their data is being processed, access to their personal data, and other supplementary information that would typically be provided to the individual via a privacy policy per their right to be informed. Upon the request of the data subject, this data must be provided without delay and at the latest within one month of receipt of the request. As a best practice, "Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data." Finally, a party who receives a request for access has a duty to use "reasonable means" to verify the identity of the person making the request.

Sovrin's Solution:

With Sovrin's pairwise Connections and microledger technology, each individual Identity Owner will have a record of every data sharing event with every individual or entity they ever interact with. They will therefore be able to prove precisely what they shared, with whom, and when. Not only can the Identity Owner use this information to demand access, but the recipient of a subject access request can use their private Connection (and their private key dedicated to this Connection) to authenticate the identity of a peer making this request. This solves the problems of both an Identity Owner (i.e. data subject) needing access and a Verifier (i.e. data controller) needing to provide it. This private channel can also be used by the Identity Owner to request access to any other personal data generated by the Verifier, or personal data disclosed to or shared with others.

Article 16 - Right to rectification

Regulatory Obligation:

Data subjects have the right to have inaccurate personal data rectified or incomplete data completed, including by way of supplementary information. This right is designed to give effect to the accuracy principle and to prevent decisions with legal or other significant effects on the data subject from being made on the basis of inaccurate or incomplete information.

Sovrin's Solution:

As described above, an individual Identity Owner in the Sovrin ecosystem can use the microledgers generated in the context of each pairwise Connection to prove exactly what information was shared, when it was shared, and with whom it was shared. Moreover, through its respective Agent, either party in a pairwise relationship has a seamless means to request a correction or other modification to their personal data from their peer on the other end of the Connection. Such a request itself becomes a provable event via their shared microledger, such that if the changes are not implemented the requesting party (who is the subject of a rectification request) can use this proof of sharing and requested rectification to enforce its rights against the peer (acting as the data controller in respect of that data). This mechanism also helps reinforce the accountability principle.

Article 18 - Right to Restrict Processing

Regulatory Obligation:

Data subjects have the right to restrict processing by a data controller where the accuracy of the personal data is contested (while accuracy is under review); the processing is unlawful but the data subject requests restriction rather than its erasure; the controller no longer needs the data for processing but the data is required for the establishment, exercise or defense of legal claims; or where the data subject has objected to processing and the controller is considering whether its legitimate grounds override those of the individual data subject.

Sovrin's Solution:

As covered extensively with respect to the rights to rectification and erasure, the Sovrin solution—primarily through the use of private pairwise Connections and corresponding shared microledgers—allows the Identity Owner (i.e. data subject) to easily and verifiably exert this right over any personal data shared with a Verifier in the context of that pairwise channel. Moreover, in respect of the public ledger, to the extent that no personal data is ever stored on the public ledger, there is no obligation to restrict processing in respect of the Sovrin Ledger.

Article 20 - Right to Data Portability

Regulatory Obligation:

Data subjects have the right to view, access and obtain their personal data from one data controller and to reuse or transmit that personal data to another controller for their own purposes. According to the Article 29 Working Party, the right "represents an opportunity to 'rebalance' the relationship

between data subjects and data controllers, through the affirmation of individuals' personal rights and personal data concerning them."
The right applies where three conditions are met:

1. the personal data was provided directly by the data subject to a data controller;
2. the processing was based on the consent of the data subject or the performance of a contract;
3. where processing is carried out by automated means.

The data controller must provide the personal data in a "structured, commonly used and machine-readable format." Where requested by the individual and technically feasible, the data controller may be required to transmit the data directly to another controller. Finally, data portability and the transfer of personal data thereunder requires that the transferring party take reasonable measures to verify the identity of the receiving party.

At first glance, data portability feels as though it has little to do with the protection of the personal data of a natural person, perhaps apart from a tangential connection to the transparency principle. Rather, this right encapsulates the GDPR's second objective—namely, to promote commerce and growth by enabling the free movement of data across the EU. Data portability is mutually beneficial for the individual who can more conveniently access and move her data across service providers or organizations with ease, as well as the commercial entity who can more readily absorb and onboard new users and customers. Data portability also fosters competition when individuals are not locked into the products or services of one service provider and can switch providers without many impediments. This is in line with other pro-competition initiatives in the EU such as the Open Banking initiative.

Sovrin's Solution:

Sovrin's version of Self Sovereign Identity is the ultimate data portability tool. Just as in the physical world, I can take my documents with me from one location to another and present them to verifying or requesting parties as needed, Sovrin enables the same functionality in the digital realm. Because the Identity Owner holds Credentials and other personal data in a portable digital Wallet, the Identity Owner is free to use and move these credentials as desired. This in squarely in line with the Article 29 Working Party's view that primary aim of data portability is enhancing individuals' control over their personal data and making sure they play an active part in the data ecosystem. Finally, Sovrin offers a strong technical solution in respect of a transferring party's ability to authenticate the party receiving the data that is subject to a transfer request per the right data portability.

Article 21 - Right to Object

Regulatory Obligation:

Data subjects have the right to object to three kinds of processing:

1. direct marketing;

2. processing based on legitimate interests of the data controller or the performance of a task in the public interest or the exercise of official authority;
3. processing for research or statistical purposes.

The right to object to direct marketing is absolute in the sense that the individual need not demonstrate any grounds for this objection and as soon as the individual objects, the processing must cease. In the case of the other two bases for objecting, the controller must cease processing unless it can demonstrate compelling legitimate grounds which override the interests of the data subject or the processing is for the establishment, exercise or defense of legal claims.

Sovrin's Solution:

As with the right to restrict processing, Sovrin Connections and microledgers enable Identity Owners to easily and verifiably exert this right over any personal data shared with a Verifier.

Article 22 - Rights in respect of automated decision-making and profiling

Regulatory Obligation:

Data subjects have the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

The only exceptions are:

1. where this kind of automated processing or profiling is necessary for entering into or the performance of a contract between the data subject and data controller;
2. the decision-making is authorized by applicable laws that include suitable measures to safeguard the rights of the data subject;
3. the decision-making is based on the data subject's explicit consent.

Sovrin's Solution:

Sovrin Connections enable the data subject to easily and verifiably exert this right via Link Contracts. While it might appear that Sovrin Agents would themselves be subject to this automated decision-making rule, in fact *Sovrin Agents only act on behalf of the data subject and always remain under the control of the data subject*. Thus a Sovrin Agent does not operate under the control of an external data controller that would be subject to this rule.

6.5 Alternatives to Achieving Secure, Trustless, Off-ledger Interactions

As our case study of Sovrin describes, using a distributed ledger as an accounting and transparency mechanism while moving the storage and processing of personal data off-chain can be an effective approach for achieving compliance with data privacy regulations, while retaining the trustless and decentralized characteristics of 'vanilla' blockchains. Sovrin's SSI model is not the only means for achieving this type of solution, however. Accordingly, in this section we provide a cursory

summary of alternative approaches off-ledger transactions, intend to 'round out' our treatment of off-ledger-type solutions for data privacy regulations. This summary includes introductions to (i) the more general concept of state channels, of which Sovrin's 'Agency Layer' is a particular implementation and (ii) the technique of Trusted Execution Environments and (iii) the use novel use of TEEs by Teechain.

6.5.1 State Channels

State channels are private, two-way pathways opened between two users that want to communicate with each other in the form of transactions, off chain. These communication pathways allow for the same data integrity and trustless properties of on chain transaction processing for transactions that take place off chain by utilizing a ledger or set of ledgers as an accounting and validation mechanism for off chain transactions. Payment channels are a subset of state channels where the state being tracked is payment.

Both participants in a state channel signs off chain transactions with their private key (or equivalent for other cryptographic schemas) to establish that they are authorized and undeniably true. Because of their off-chain nature, such transactions can take place without the potential for latency introduced by on chain consensus mechanisms. State channels usually have a limited lifespan, predetermined based on time or amount of transactions carried out. Participants can also close their channel by providing the last-updated state of transactions within the channel to the blockchain. If the other participant agrees that the state provided is indeed the final one, they let the channel close. If not, they can upload their version of the most recent state and since all transactions are signed and time stamped, such a dispute will always be won by the honest party.

The contents of transactions that take place within a state channel are private and known only to its participants - this is highly significant - by utilizing state channels, sensitive data is only shared with those that need to have access to it. Once a channel closes, the transaction history of the channel is recorded on an immutable ledger as a hash, which can be referenced by those who have access to said transaction history (i.e. the parties involved in a state channel) to establish the validity of a given record of this same transaction history. In addition to significantly reducing the amount of information that individual nodes need to store, state channels also reduce the number of transactions that need to be processed by nodes, as the set of transactions that took place in a state channel can be processed as a single transaction when the state channel closes.

For situations in which the off-chain transaction state of more the two parties must be monitored, multi-hop state channels have been proposed. Such channels processes transactions in a manner that involves multiple participating nodes as opposed to only the two nodes sending and receiving a payment or evaluating a state. Successful multi-hop payment channels were demonstrated by the Bitfury Group in May of 2017 on the Bitcoin Lightning Network. Multi-hop state channels, which are more complex, are still in the developmental phase. Until recently, proposals for state channels in general had seen little adoption due to their incompatibility with current blockchain protocols, practical limitations, and implementation complexity. New conceptions of how they can be achieved, however, by efforts such as Teechain, Sovrin, and IBM's deployment of Hyperledger Fabric are moving this concept from the theoretical to the feasible.

6.5.2 TEEs

A Trusted Execution Environment (TEE) is a trusted region on a processor isolated from, but running in parallel to, the main operating system of a device that utilizes both hardware and software to protect the integrity and privacy of data. TEEs are intended to guarantee robustness in the presence of an attacker who has full control of the hardware and has compromised privileged software, including the OS and hypervisor of a virtual memory.

By only storing, managing, and using encryption keys within a TEE, data, communications, and cryptographic operations can be secured with no opportunity for eavesdropping. This is particularly relevant for increasing the security of state channels and other privacy-by-design blockchain techniques (such as Audit-enabled Privacy, discussed in Section X.x) because cryptographically-established access permissions are only as secure as the security of the private keys that endow access. The most advanced TEE implementations, such as Intel's Software Gaurd Extensions (SGX), embed devices with unique identities via roots of trust - a set of functions, part of a trusted computing environment, that are always trusted by a processor's OS. These enable key stakeholders (i.e. network operators, data processors) to identify whether the device they're interacting with is authentic - otherwise known as remote attestation functionality.

It is worth noting that Sovrin's Agency Layer allows for similar environments without the use of special hardware with OS-level software to establish locations for secure data processing and storage. This allows for Sovrin Agents to be run from personal computing devices, such that the processing and storage of data in the Sovrin network can occur in a more decentralized manner - i.e. not consolidated across the purchasers of expensive TEEs.

6.5.3 Teechain

Teechain is an innovative off-chain payment protocol that demonstrates a novel approach for (i) utilizing TEEs to address shortcomings of previous payment channel deployments and (ii) further increasing the resiliency of TEEs. Of particular significance is Teechain's use of TEEs to enable asynchronous blockchain access for payment channels, which allows for validated offline transactions and reduces the latency for payment channel transactions.

Most payment channel deployments require synchronous access to the blockchain. This means that the parties in a channels must leave the channel at the same time, with a hashed record of the state of the channel being recorded as a transaction on the blockchain. Although a user on such a deployment can, at any time, settle the channel for all parties, it is possible for a user to request the channel to be settled at a depreciated state, using the 'previous' capabilities that accompany said depreciated state (i.e. stale state exploit). To prevent such attacks, many solutions require users to monitor the blockchain and react to such misbehavior by providing an authenticated timestamp of the 'non-stale' state of the channel that was recently closed in such a manner, which places a burden on users and allows for invalid records to be written on-ledger, even if temporarily. Addressing such erroneous entries places a burden on the blockchain network, which decreases its performance.

Teechain avoids necessity of such monitoring by use of collateral in the form of on-blockchain deposits to secure payment commitments within a given channel. The collateral is maintained by TEEs, allowing users to dynamically move funds between payment channels - important for enabling multi-hop channels. Because the TEEs protect the internal channel state and release it only upon channel termination, they ensure that users cannot launch attacks by using a stale state exploit. This approach is intend to avoid such attacks on payment channels, and simplifies the protocol such that network performance is improved.

Teechain mitigates known failures of TEEs with two strategies: (i) backups to persistent storage and (ii) a novel variant of chain-replication, both of which are intended to increase the resiliency of data contained in TEEs by establishing additional sources of data validation. Although Teechain's protocol is intended to be able to function on any TEE, their first implementation uses Intel's SGX. Although Teechain's solutions were developed for payment channels and not state channels, which are more complex, their techniques demonstrate how TEEs can be used to secure off chain transactions, and enable offline off chain transactions. It should be noted, however, that Teechain's payment channel solution, offline-enabled and efficient as it is, only allows only for payment-type transactions - not the more complex types of off-ledger interactions enabled by Sovrin-type state channel.

6.6 Sovrin Alternatives for KYC-AML Compliance

This section is comprised of two parts. 6.6.1 introduces a conflict between Sovrin's protocol and KYC-AML and then describes a modification Sovrin's protocol that could resolve this conflict. 6.6.2 introduces an enterprise-oriented distributed ledger model - Hyperledger Fabric - which was designed for KYC-AML compliance in mind, while Sovrin was not. Included in this introduction is an overview of two features of Hyperledger Fabric that are uniquely suited for achieving KYC-AML compliance.

6.6.1 Potential Conflict between Sovrin and KYC-AML

As discussed in Section 6, when one of the Sovrin Identity Owners in a relationship requests the relationship to be closed, access to data shared over the course of this relationship disappears. This aspect of the Sovrin protocol represents a potential conflict with record-keeping requirements specified by CCD, specifically the requirement of hold records of personal information for five years after an account is closed. We propose on approach identical to Sovrin but with one key difference as a solution for this conflict: In relationships where AML / KYC compliance is required by one or both Identity Owners, a second, *compliance* microledger is also maintained across the Agents used by both Identity Owners for said relationship. This compliance microledgeer would maintain a record of the personal information attributes specified by CCD under its record-keeping requirement - name, date of birth, address, and ID number. Unlike the 'primary' microledger used in conventional Sovrin relationships, this compliance ledger would persist for five years after the termination of the relationship.

6.6.2 Hyperledger Fabric

Hyperledger Fabric is a business blockchain framework hosted by the Linux Foundation. Fabric is actually related to Sovrin, as the latter is a protocol running off of Hyperledger Indy - an identity blockchain framework and the brainchild of Sovrin foundation. Fabric was developed to address the unique set of considerations (KYC-AML regulations, specifically) faced by enterprise applications. In addition to utilizing state channels, Fabric proposes two techniques of practical significance for achieving KYC-AML compliance within a distributed ledger network.

The Zero Knowledge Asset Transfer feature of Hyperledger Fabric allows transactors to issue assets and request transfer of their assets without revealing anything to the public ledger for the assets being exchanged. Unlike other privacy-preserving asset management systems for blockchain, ZKAT is tailored to the needs of enterprise networks. In particular, the auditability of the privacy-preserving transactions within Fabric is a crucial differentiator from other schemes available. This feature is known as *Audit-enabled privacy* - each user is assigned a specific auditor who is entitled to unlimited access to all the transactions of that user. The auditors are passive; they may come in afterwards and extract the confidential information of all transactions the audited user is involved in, but they cannot access the data for any other party. Because Audit-enabled privacy allows for KYC and AML compliance within blockchain networks by granting auditors, and auditors only, access to personal data for specific users, data processors (besides auditors) and network operators are not subject to the data privacy regulations that come with handling such data.

With Fabric, private transactions (i.e. state channels) can be combined with anonymous client authentication (i.e. Audit-enabled privacy) to avoid leaking the connection between the identity of the transaction's creator and the ledger stored (hashed) data.

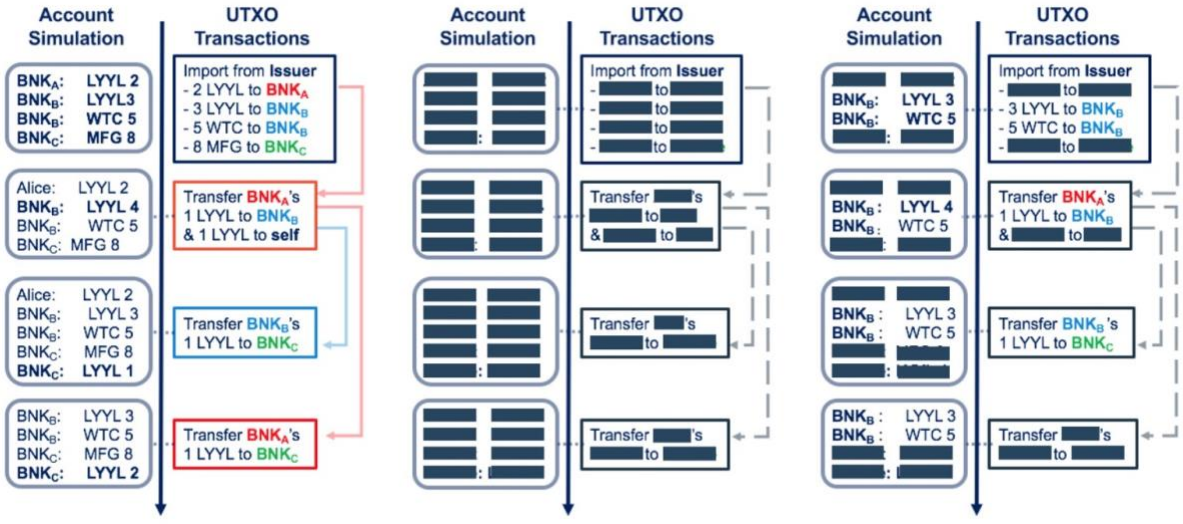


Figure 5: Audit-enabled privacy

In the figure above, the access to on-ledger financial data provided by distributed ledger protocols to an auditor is shown across three different privacy mechanisms. The model on the left has no privacy mechanism. The model in the middle supports full privacy, concealing the identities of transaction participants and traded assets details. The model on the right demonstrates the secure

auditing capability of ZKAT - the auditor assigned to a specific Bank is allowed unrestricted access to all transactions involving this bank.