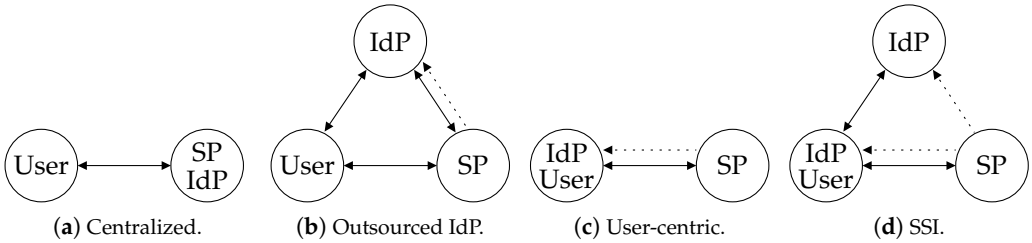

(**a**) Centralized. (**b**) Outsourced IdP. (**c**) User-centric. (**d**) SSI.

Figure 1. The IAM models. Constant lines represent interactions, and dashed lines mean trust.

2.4. Self-Sovereign Identity

In the early days of the web, the conception of the client–server model shaped the idea that in the digital world, people are users of online systems rather than human beings, i.e., entities that need identification, authentication, and authorization to access and perform tasks online [43]. This digital model assumes administrative precedence because it was built on the foundation that servers (companies, online businesses) are more important than clients (individuals) and, therefore, dictate the rights of clients [44]. This web fabric holds to this day and is exacerbated by the need for the creation of legislation, such as the European Union's General Data Protection Regulation (GDPR) [45] and the California Consumer Privacy Act (CCPA) [46], to specify the rights of individuals and their digital data in a society increasingly dependent on digital interactions.

The fundamental premise of SSI is that individuals have sovereignty over their digital selves and thus control over their data. This concept fundamentally distinguishes SSI from previous identity models, which viewed individuals as users. In this new model, sovereign individuals store and manage their data, thereby controlling with whom their private data are shared and to what extent.

Although philosophers such as John Locke and Stuart Mill have written about the sovereignty of individuals in past centuries [47,48], Loffreto [49] established the first widely accepted [3,50–53] link between sovereignty and digital identity [49]. Thereafter, the meaning of sovereign identity was debated [54–57], and technology standards were proposed [58,59]. Significant momentum was obtained, especially in academia [19,60], after Christopher Allen laid out what he proposed to be the ten principles of SSI [3], which are detailed next.

First, individuals must have an *existence* independent of their digital selves, i.e., they cannot exist only virtually. A (self-sovereign) identity works by sharing the desired (digital) aspects of the individual. Second, people must *control* their identities by owning and managing their attributes, which does not prohibit them from making *claims* about other people. Third, people must have *access* to their data and claims by storing them or being readily available if they are outsourced. Fourth, all systems must be *transparent* and the underlying algorithms must be free and open-source, thus allowing detailed examination by anyone. Fifth, identities must *persist* forever or as long as individuals wish. Sixth and seventh, identities and their claims must be *portable* across different systems and technologies, which requires *interoperability* between standards and implementations. Eighth and ninth, people need to *consent* to the use and sharing of their data, while data disclosure must be *minimized* to the absolute minimum. For instance, to find out if a person can buy an alcoholic beverage, it is unnecessary to share their date of birth. Tenth, at the end of the day, individuals' rights must be *protected*, which means that systems must be designed to avoid censorship and to protect individuals' rights, even at the expense of the system.

In SSI, any assertion about a subject is referred to as a *claim*. A *credential* is a collection of one or more assertions made about a subject by an entity. It could be, for example, a government-issued driver's license that contains a person's date of birth, name, and address. A *Verifiable Credential (VC)* is a credential that includes a revocation list or another method of revocation and contains cryptographic material that ensures the credential's integrity, as well as the issuer's identification and non-repudiation [58]. Additionally, a