A Comparative Analysis of Trust Requirements in Decentralized Identity Management

Andreas Grüner, Alexander Mühle, Tatiana Gayvoronskaya and Christoph Meinel

Abstract Identity management is a fundamental component in securing online services. Isolated and centralized identity models have been applied within organizations. Moreover, identity federations connect digital identities across trust domain boundaries. These traditional models have been thoroughly studied with regard to trust requirements. The recently emerging blockchain technology enables a novel decentralized identity management model that targets user-centricity and eliminates the identity provider as a trusted third party. The result is a substantially different set of entities with mutual trust requirements. In this paper, we analyze decentralized identity management based on blockchain through defining topology patterns. These patterns depict schematically the decentralized setting and its main actors. We study trust requirements for the devised patterns and, finally, compare the result to traditional models. Our contribution enables a clear view of differences in trust requirements within the various models.

1 Introduction

In the present, online services and electronic communication pervade everyday life, both in the private and business area. Banking, shopping, social networks and cloud services are a few samples in this regard. Securing these services in various dimensions is essential to prevent misuse, attract customers and finally create trust in a product or technology. A common factor in terms of security and a basic prerequisite for personalized use is the establishment and management of digital identities – commonly referred to as identity management [1]. The online service needs to differentiate and recognize users, for instance, to selectively enable functionality or

Andreas Grüner, Alexander Mühle, Tatiana Gayvoronskaya and Christoph Meinel
Hasso Plattner Institute (HPI), University of Potsdam, 14482 Potsdam, Germany, e-mail: {andreas.gruener|alexander.muehle|tatiana.gayvoronskaya|christoph.meinel}@hpi.uni-potsdam.de

grant access to user-specific resources. At the same time, fraudulent impersonation must be prevented.
In 2008, Satoshi Nakamoto published the foundations for a peer-to-peer currency named Bitcoin [2]. Bitcoin is a fully decentralized cash scheme that does not require a trusted third party. Subsequently, the idea of a decentralized cash scheme was generalized to obtain a decentralized execution platform for arbitrary operations, in general, called blockchain [3]. Hence, a blockchain enables the implementation of an identity provider that is decentralized and not a trusted third party [4]. The issuance of self-sovereign identities, which are in the possession and under true control of the user, is empowered by a blockchain-based identity provider. Trust requirements may significantly change by applying decentralized identity management without having an identity provider as a trusted third party.
In this paper, we investigate trust requirements in the decentralized identity management model and constitute a view on the differences when compared to traditional models. In this way, we address the points that are still lacking in the understanding. To achieve this, we outline decentralized identity management based on blockchain. Subsequently, we define topology patterns that reflect the relevant actors and their interaction paths. Using these patterns, we study trust requirements for the different entities and compare them to the trust prerequisites in the traditional models.
The rest of the paper is structured as follows. Section 2 presents related work on trust requirements in identity management, and the respective differences to our work. The general concept of trust and our evaluation methodology is outlined in Section 3. We illustrate in detail patterns and associated trust requirements in decentralized identity management in Section 4. Finally, we conclude our analysis with Section 5.

2 Related Work

Jøsang et al. [5] researched simple trust requirements in isolated, centralized and federated identity management as well as personal authentication management. Trust requirements are analyzed from the perspectives of the user and the service provider. The service provider implicitly covers the identity provider as well. The common identifier domain, meta-identifier domain and single-sign-on are subclasses of the centralized identity management model. Moreover, in identity federation structures the authors distinguish trust requirements between different service providers and users. Finally, personal authentication management, with a trust requirement to the tamper-resistance of the personal authentication device is evaluated. Kylau et al. [6] studied detailed trust requirements and associated risks in identity federation topologies. In general, the entities user, identity provider and service provider are differentiated. Kylau et al. analyzes the identity federation structures based on defined patterns. These patterns are clustered in direct trust topologies and patterns that additionally integrate indirect trust schemes. The paper concludes by comparing trust requirements and risks of the federated identity patterns. With

the increasing complexity of the pattern, the trust requirements and the associated risk increase as well. Ferdous and Poet [7] evaluate attribute aggregation models in federated identity management with regard to risk as well as trust and functional requirements. These models are clustered according to a taxonomy that strongly considers the location where the attribute aggregation occurs. In general, attributes are aggregated at either the service provider, identity provider or user level.
In contrast to the previous work, we study trust requirements in the decentralized identity management model based on blockchain technology by devising appropriate patterns. Furthermore, we compare the derived trust prerequisites to the traditional models in order to evaluate differences. We consider the attribute aggregation manner and do not concentrate on the aggregation location.

3 Analysing Trust in Identity Management

In this section, we provide a general background on the notion of trust, the relevant actors and their domains of trusted interactions. Additionally, we outline our evaluation methodology for analyzing the trust requirements.

3.1 The Notion of Trust

Trust is a pervasive and significant phenomenon in social societies with a diverse and manifold range of meanings and definitions [8]. In human relationships trust is fundamental for cooperation, conversation and mutual interactions between persons or institutions. A definition of trust is subjective in nature and depends on the contextual setting [9]. Jøsang et al. [8] created a definition based on the former work of McKnight and Chervany [10] that characterizes decision trust as

> *the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible.*

First of all, the interpretation emphasizes entities that rely on each other unilaterally or bilaterally. Secondly, a certain situation is required that is related to the dependency. Finally, negative consequences are named in case the dependency is misused from the perspective of the relying party. The potential occurrence and impact of the adverse effect reflects the actual risk.
Embedding the definition of decision trust into the context of identity management, determining the acting parties is the starting point for analyzing mutual trust relationships. We differentiate the user, the service provider, and the identity provider. Additionally, we consider the attribute provider as derived entity from the identity provider.

- **User (U)** The user is characterized as the subject who is represented by the digital identity. The user is in possession of a credential to solely control and use the digital identity.
- **Service Provider (SP)** The service provider offers a service that requires users to authenticate and convey attributes. Based on the authenticated user and the transmitted attributes, the service provider may adopt its service.
- **Identity Provider (IdP)** The identity provider offers capabilities to create, manage and employ digital identities. An additional role of the identity provider is the supply and verification of user attributes.
  - **Attribute Provider (AP)** The attribute provider offers a subset of the identity provider's functionality with the focus on the allocation and validation of user attributes.

3.2 Trust Domains and Requirements

The trust domains cluster the situations where dependencies between the different actors exist. Aligned with the decision trust definition, a dependency indicates that an actor relies on another entity. This reliance reflects a trust requirement of the trustor towards the trustee. The violation of a trust requirement implies an adverse impact for the trusting party. We consider the following domains with the listed trust requirements for the comparative analysis.

- **Privacy** A digital identity and its attributes represent personal information of the user that are protected by a variety of regulations [11]. Additionally, statistics and profiles can be derived from the use of the digital identity at a service provider or identity provider. The user expects that the individual-related information is kept private and is solely evaluated and disclosed for the intended and consented purpose.
  - ***T1a*** The identity resp. attribute provider protects the privacy of the user.
  - ***T1b*** The service provider protects the privacy of the user [5].
- **Credential Management** A credential is required to enable a user to control their digital identity and to prevent impersonation attacks. The identity provider needs to securely generate, change and store the credential or related verification information. Moreover, the user has the responsibility to protect and not to share the credential.
  - ***T2a*** The identity provider implements secure credential management [5].
  - ***T2b*** The user protects the credential [5] and does not deliberately disclose it.
- **Authentication** A service provider requires user authentication. During authentication, the user demonstrates the possession of the credential to control the digital identity at the identity provider. The identity provider forwards the success

or failure result to the service provider. The service provider maps the logged in digital identity to internally administrated datasets.

  - ***T3a*** User authentication is done adequately by the identity provider [6].
  - ***T3b*** User mapping is managed correctly by the service provider [6].

- **Attribute Management** Attributes are a substantial part of a digital identity. A service provider may use these properties within the offered service (e.g. for age verification). Moreover, the characteristics can be applied to decide if a user is eligible to consume a service. Therefore, the properties must be correct and reflect reality. Additionally, the attributes must be revoked in a timely manner if the validity period has expired.

  - ***T4a*** Delivered attributes of the users are correct.
  - ***T4b*** Invalidated attributes are revoked in a timely manner.

3.3 Objective and Evaluation Methodology

The objective of our contribution is to analyze trust requirements in decentralized identity management and to identify differences and common features with regard to the traditional identity management models. To achieve this, we elaborate bilateral trust relations of the outlined actors according to the described trust requirements. Moreover, we add an indicator to describe the required level of trust that is needed. The level of trust relates to the degree of dependency towards one trusted third party and is differentiated in the following way.

- **Absolute** The dependent actor needs to completely rely on a trusted third party. There is no significant compensating control or trust distribution between several third parties to reduce the overall required trust allocation.
- **Limited** In any given situation, the trust requirement does not apply unconditionally for an entity. A major compensating control may exist that degrades the needed trust. Besides that, the required trust might be reduced by distributing the dependency to several entities in order to remove a single trusted third party.

4 Trust Requirements in Decentralized Identity Management

In the following sections, we start with a characterization of decentralized identity management based on blockchain and outline a respective architecture. Afterwards, we define patterns in this setting and describe associated trust requirements between the actors. Finally, we compare the trust requirements with the traditional types of identity management.

4.1 Decentralization Characteristics

A common characterization of traditional identity management models is the consolidated implementation of central functions at an identity provider. Therefore, the identity provider represents a trusted third party towards the user and the service provider. The decentralization of identity management and therefore, the remediation of the identity provider as trusted third party needs to consider the characteristics **execution**, **storage**, **attributes**, **namespace** and **organization**.
The identity provider is implemented as software and **executed** in a server environment under full control of the hosting party. Trust is required to believe that the implementation works as expected and does not deviate from published properties. An identity provider **stores** under its control user information and specific attributes of digital identities. The decentralization of storage refers to the relocation of an identity provider-owned storage to a user-defined position. In case a certain **attribute** is delivered by a single entity, the attribute's validation and correctness rely solely on the specific provider. An aggregation of attributes from various providers drives decentralization [12]. The identifier of a digital identity is generated within a **namespace**. An essential prerequisite for identifiers is their uniqueness that needs to be managed in a decentralized way. An identity provider is operated by an **organization**. This organization is usually in control of the identity provider and reflects a point of centralization.

4.2 Decentralized Identity Management Based on Blockchain

Blockchain enables the implementation of a decentralized identity provider adhering to the outlined characteristics. Programs are executed decentralized with a common and transparent consensus by all participating nodes in the network [4] [3]. A wide range of projects with different implementation approaches exists [13]. uPort [14] is a solution based on smart contracts on the public and unpermissioned blockchain Ethereum [3]. Moreover, Sovrin [15] applies a distinct set of public and permissioned blockchains to implement decentralized identity management. A common factor is the decentralization of the organisation, namespace and attributes. Nodes can join an unpermissioned blockchain independently from any registration process. Therefore, no organization exerts control over it. In the case of Sovrin, there is a fine-grained trust model with a voting scheme to enable democratic participation in the blockchain network [15]. Besides that, the namespace is managed as a decentralized registry on the blockchain. Furthermore, the attributes are depicted as Verifiable Claims [16] that are comprised of claims and attestations. A claim is a statement about a user and the attestation is a verification of the statement. Having multiple attestation authorities, a service provider does not need to rely solely on a single attribute provider. The decision about the storage location of the attributes is conveyed to users and their preference, according to the user controls primitive in Allen's principles of self-sovereign identity [17].

4.3 Decentralized Identity Management Patterns

To analyze trust requirements in this model, we abstract from the actual peculiarities of the various blockchain implementations to a generalized architecture that is outlined in different patterns. This architecture comprises the service provider and the attribute provider as distinct actors. In Figure 1 and Figure 2 the actors are depicted as rectangular shapes with rounded edges. A decentralized blockchain-based identity provider connects the different entities with regard to identity management functions. However, attributes are actually provided by the attribute provider and not by the identity provider itself. The decentralized identity provider is presented as a dashed circled line in the figures. An arrow between the service provider and the attribute provider reflects the usage of attributes for a user upon a service request. An arrow between a service provider and multiple attribute providers illustrates an aggregated usage of attributes.

4.3.1 Bilateral Integration

The simplest pattern is the bilateral integration comprising a single service and attribute provider. This pattern is shown in the left section of Figure 1. The service provider relies solely on one attribute provider for user attributes. The decentralized identity provider implements functions for credential management and identifier registration. A user registers a digital identity on the decentralized identity provider and the attribute provider supplies certain attributes of the digital identity. Upon requesting access at a service provider, the decentralized identity provider authenticates the user and mediates the attributes from the attribute provider. Based on the authentication result and the conveyed attributes, the service provider conducts an access decision.
The user is required to trust the attribute and the service provider with regard to adherence to privacy obligations. From the user's point of view, the trust requirements *T1a* and *T1b* apply absolutely toward the respective party. The trust prerequisite *T2a* is not applicable in this context, because the decentralized identity provider transparently implements secure credential management that can be publicly verified. Equally alike, therefore the prerequisite *T3a* is not appropriate in this environment. The decentralized setting also enables a public verification of the authentication. Therefore, no actual trust is required by the user. In contrast, the user needs to rely on the service provider that the user mapping is conducted appropriately. Therefore, trust requirement *T3b* applies absolutely between the user and the service provider. Moreover, the user depends on the attribute provider to convey correct and valid attributes. Thus, trust prerequisites *T4a* and *T4b* are fully applicable as well.
Analysing the service provider, trust requirements *T1a*, *T4a* and *T4b* apply absolutely towards the attribute provider. The attribute provider is a trusted third party for the service provider. The service provider expects the adherence to privacy regulations as well as the correctness and validity of the user's attributes. Besides that, the trust demand *T2b*, the protection and secure credential storage, exists towards

the user. In contrast, demands related secure credental management (*T2a*) and authentication (*T3a*) are not applicable due to the decentralized nature of the identity provider.
The attribute provider fully expects that the service provider protect the user's privacy according to *T1b*.

4.3.2 Multiple Aggregated Integration

The multiple aggregated integration pattern is presented in the middle section of Figure 1. The pattern consists of a service provider and several attribute providers. The service provider receives aggregated attributes of a user that are composed of both attribute providers. Attribute aggregation considers the same attribute from multiple attribute providers to verify the delivered attributes of a single provider. Thus, trust in one attribute provider is decreased.
Comparable to the bilateral integration, the privacy trust requirements (*T1a*, *T1b*) and *T3b* regarding user mapping are fully applicable to the user. Moreover, the service provider requires *T1a*, *T2b*, and the attribute provider expects adherence to *T1b*. On the contrary, the trust requirements *T4a* and *T4b* with reference to the properties of the digital identity apply differently. The user and the service provider depend on the attribute providers to provide correct attributes and that attributes are revoked in due course if they are not valid anymore. The trust requirements *T4a* and *T4b* are solely applicable in a limited manner in this pattern, because the same attributes are delivered by multiple attribute providers. Therefore, an absolute dependency towards one attribute provider is eliminated.

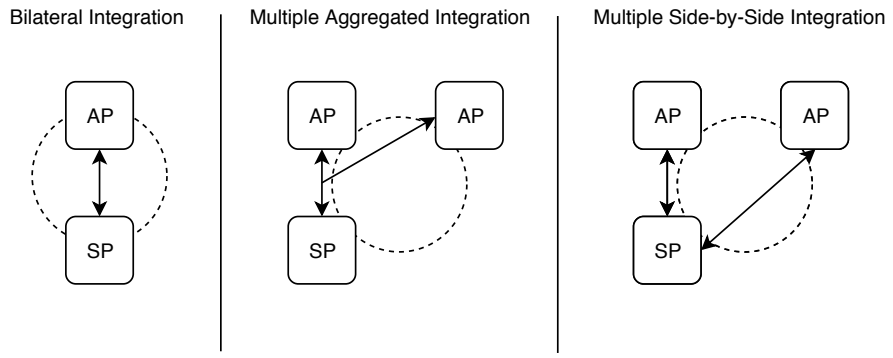

Fig. 1 Decentralized Identity Management Patterns - Part 1

4.3.3 Multiple Side-by-Side Integration

The multiple side-by-side integration pattern is presented in the right section of Figure 1. The pattern consists of a service provider and several attribute providers. The service provider aggregates the attributes of a user that are received from both attribute providers. In this pattern, attribute aggregation combines different attributes from the providers to obtain all required properties of a digital identity for the service provider. There is no decrease in trust for a single property that is received from multiple attribute providers. That approach differentiates the multiple side-by-side pattern from the multiple aggregated integration pattern.
In this pattern, trust requirements for all actors are fully comparable to the bilateral integration. For the user, the trust requirements *T1a*, *T1b* and *T3b* are completely applicable. Furthermore, the service provider requires fully *T1a*, *T2b* and the attribute provider expects adherence to *T1b*. Service provider and user require absolute trust towards the attribute providers with regard to *T4a* and *T4b*.

4.3.4 Multiple Service Provider Integration

The multiple service provider integration pattern is presented in the left section of Figure 2. The pattern consists of several service providers and one attribute provider. The attribute provider is the single source of attributes of digital identities. Two service providers are representatively depicted in the pattern. However, multiple service providers can be assumed.
In general, trust requirements are analogous to the bilateral integration pattern. The user has absolute trust demands according to *T1a*, *T1b* and *T3b*. The service provider requires absolutely *T1a* and the attribute provider expects adherence to *T1b*. Service provider and the user require absolute trust towards the attribute providers with regard to *T4a* and *T4b*.
A difference exists in the limited applicability of trust requirement *T2b* with regard to credential protection. The digital identity of the user can be employed at a multitude of service providers and has, therefore, a significant importance for the user. One digital identity enables the user to interact in the online world in contrast to a large number of service-specific digital identities within other identity management models. This leads to an increased interest of the user to protect the credential and lowers the risk of deliberate disclosure. Therefore, a limited level of trust regarding *T2b* is needed.

4.3.5 Arbitrary Aggregated and Side-by-Side Integration

The arbitrary aggregated and side-by-side integration pattern is the most complex in nature (see Figure 2) of all such patterns. The pattern is comprised of several service providers and manifold attribute providers. Properties from different attribute providers are aggregated to decrease trust into a single provider and to ensure com-

pleteness for service consumption. The pattern most likely reflects a realistic setup with numerous entities and different interaction paths that are connected by a common decentralized identity provider.
The applicability of trust requirements within this pattern is a composition of the previously described structures. The privacy trust prerequisites *T1a* and *T1b* apply absolutely towards the attribute and the service provider from the user's perspective. Additionally, the user relies fully on an appropriate identity mapping by the service provider covered under *T3b*. Furthermore, attribute trust requirements *T4a* and *T4b* from user and service provider towards the attribute providers are applicable absolutely or in a limited manner depending on the attribute aggregation strategy. Requirement *T1a* applies fully towards the attribute provider. Moreover, the attribute provider completely expects that the service provider protects the user's privacy according to *T1b*.
The trust requirement *T2b* to securely protect the credential of the digital identity exists with limited trust towards the user by the service provider. Due to the holistic applicability of the digital identity, the user has a strong interest in protecting the credential.

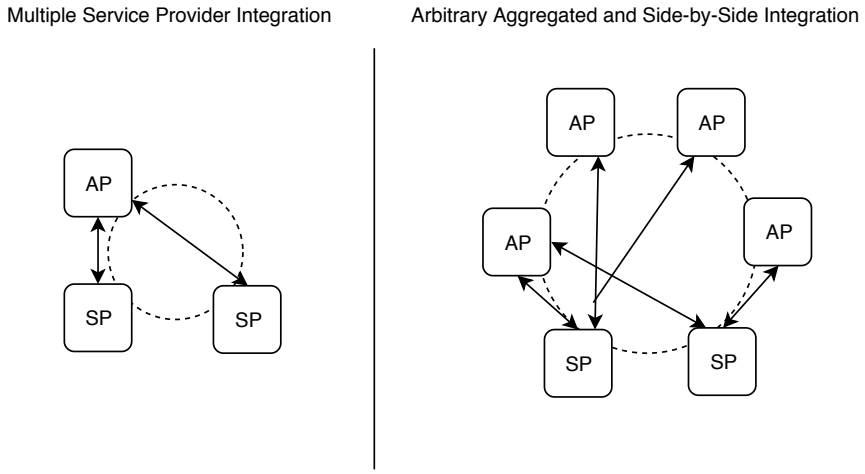

Fig. 2 Decentralized Identity Management Patterns - Part 2

4.4 Comparison to Trust Requirements in Traditional Models

Traditional models comprise isolated, centralized and federated identity management. The advancement in this area promoted the comprehensive usage of specific

digital identities and fostered the reduction of digital identities with a simultaneously increasing number of online services.

4.4.1 Isolated Identity Management

Isolated identity management denotes service-specific digital identities at a service provider [18]. The digital identities are solely applicable at a determined service and no overarching usage is possible. In the isolated setting, the identity provider and the service provider are one entity [5], requiring no trust between each other.
For the user, the trust requirements *T1a*, *T2a*, *T3a*, *T4a* and *T4b* are suited with an absolute trust level towards the identity provider. Moreover, the prerequisites *T1b* and *T3b* apply for the user towards the service provider with an absolute rating as well. In both cases, the user is confronted with a trusted third party either being the identity or service provider. The trust requirements *T1a*, *T2a*, *T3a*, *T4a* and *T4b* of the service provider towards the identity provider and the prerequisite *T1b* in reverse direction are not applicable. In contrast, the service provider and the identity provider absolutely require *T2b* towards the user.

4.4.2 Centralized Identity Management

Centralized identity management moves from a service-specific to an organization-specific use of digital identities [18]. Therefore, a converged digital identity can be used at several services within an organization. The service provider and the identity provider are separate entities belonging to the same trust domain. Thus, a limited trust level is required for mutual relationships.
Comparable to the isolated model, the service provider and the identity provider are trusted third parties for the user and vice versa. Therefore, respective trust requirements apply absolutely. Trust requirements *T1a*, *T2a*, *T3a*, *T4a* and *T4b* that exists from the service provider to the identity provider are applicable with limited trust rating. Similarly, prerequisite *T1b* exists in reverse direction.

4.4.3 Federated Identity Management

In federated identity management, digital identities are used across organizational and trust boundaries [18]. The identity provider represents a distinct trusted third party that is independent of a service provider and its organization.
Generally, the trust requirements apply similarly to the centralized identity management model. However, the trust requirements that exists between identity provider and service provider in both directions apply with an absolute rating. Additionally, the trust requirement *T2b* towards the user is limited in rating because the federation of an identity provider with several service providers increases the employability, and thus the value of the digital identity for the user.

4.4.4 Comparison

During the evolution of traditional identity management models, starting from isolated over centralized to the federated approach, there was no decrease in trust between the actors. In contrast, the level of required trust for the various prerequisites increased overall, leading to the highest trust requirements in the federated identity model. Additionally, from a user's perspective the most trust, in terms of requirements and associated rating, is demanded across all traditional identity management models. The dependency of the user is significantly higher in the case of the service provider and identity or attribute provider than vice versa. In contrast, the identity provider is the target of the majority of trust requirements by having at the same time the lowest number of trust prerequisites towards the other entities. Thus, the traditional identity management models have a very disparate distribution of required trust between the actors with a detrimental situation for the user.
The application of decentralized identity management based on the blockchain, reduces the imperative trust prerequisites in general for all entities when considering the most complex arbitrary aggregated and side-by-side integration pattern. The blockchain enables the implementation of an identity provider to replace needed trust by the user and the service provider that is both transparent and public verifiable. At the same time, trust in a certain attribute can be limited by aggregation from different providers. Specifically, the following significant differences in trust requirements exist.

1. Trust in credential management and authentication of the identity provider by the user and the service provider (*T2a*, *T3a*) is remediated in the decentralized identity setting.
2. User and service provider trust in attribute management (*T4a*, *T4b*) is reduced by applying attribute aggregation for the same attribute utilizing several attribute providers.

However, even if trust requirements are generally reduced, a disparate trust distribution between the user and service respective to the identity or attribute provider still exists in the decentralized identity management model.
A detailed overview of the trust requirements and related ratings in the various models and patterns are shown in Table 1. A dash (-) reflects no trust. A small dot (·) and large dot (•) implies limited respectively absolute trust.

5 Conclusion

We outlined decentralized identity management based on blockchain and devised interaction patterns. Based on these patterns, we analyzed trust requirements and compared it to the traditional models. In conclusion, a reduction of trust towards the identity and attribute provider is a significant benefit of applying the decentralized model based on blockchain.

		T1a			T1b			T2a			T2b			T3a			T3b			T4a			T4b		
		U	SP	IdP/AP	U	SP	IdP/AP	U	SP	IdP/AP	U	SP	IdP/AP	U	SP	IdP/AP	U	SP	IdP/AP	U	SP	IdP/AP	U	SP	IdP/AP
Isolated	U	-	-	●	-	●	-	-	-	●	-	-	-	-	-	●	-	●	-	-	-	●	-	-	●
	SP	-	-	-	-	-	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	IdP/AP	-	-	-	-	-	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Centralized	U	-	-	●	-	●	-	-	-	●	-	-	-	-	-	●	-	●	-	-	-	●	-	-	●
	SP	-	-	·	-	-	-	-	-	·	●	-	-	-	-	·	-	-	-	-	-	·	-	-	·
	IdP/AP	-	-	-	-	·	-	-	-	-	●	-	-	-	-	-	-	·	-	-	-	-	-	-	-
Federated	U	-	-	●	-	●	-	-	-	●	-	-	-	-	-	●	-	●	-	-	-	●	-	-	●
	SP	-	-	●	-	-	-	-	-	●	·	-	-	-	-	●	-	-	-	-	-	●	-	-	●
	IdP/AP	-	-	-	-	●	-	-	-	-	·	-	-	-	-	-	-	●	-	-	-	-	-	-	-
Bilateral	U	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	-	●	-	-	-	●	-	-	●
	SP	-	-	-	-	-	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	●	-	-	●
	IdP/AP	-	-	-	-	-	-	-	-	-	●	-	-	-	-	-	-	●	-	-	-	-	-	-	-
Mult. Aggregated	U	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	-	●	-	-	-	·	-	-	·
	SP	-	-	-	-	-	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	·	-	-	·
	IdP/AP	-	-	-	-	-	-	-	-	-	●	-	-	-	-	-	-	●	-	-	-	-	-	-	-
Mult. Side-by-Side	U	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	-	●	-	-	-	●	-	-	●
	SP	-	-	-	-	-	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	●	-	-	●
	IdP/AP	-	-	-	-	-	-	-	-	-	●	-	-	-	-	-	-	●	-	-	-	-	-	-	-
Mult. Service Provider	U	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	-	●	-	-	-	●	-	-	●
	SP	-	-	-	-	-	-	-	-	-	·	-	-	-	-	-	-	-	-	-	-	●	-	-	●
	IdP/AP	-	-	-	-	-	-	-	-	-	·	-	-	-	-	-	-	●	-	-	-	-	-	-	-
Arb. Agg./ Side-by-Side	U	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	-	●	-	-	-	·/●	-	-	·/●
	SP	-	-	-	-	-	-	-	-	-	·	-	-	-	-	-	-	-	-	-	-	·/●	-	-	·/●
	IdP/AP	-	-	-	-	-	-	-	-	-	·	-	-	-	-	-	-	●	-	-	-	-	-	-	-

Table 1 Overview of Trust Requirements in Traditional Identity Management Models and Decentralized Patterns

References

1. G. Williamson, D. Yip, I. Sharoni, and K. Spaulding, *Identity Management: A Primer*. MC Press Online, LP., 2009.
2. S. Nakamoto. (2008) Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: https://bitcoin.org/bitcoin.pdf [Accessed: 2019-01-18]
3. G. Wood. Ethereum: A secure decentralised generalised transaction ledger. [Online]. Available: https://pdfs.semanticscholar.org/ac15/ea808ef3b17ad754f91d3a00fedc8f 96b929.pdf [Accessed: 2019-01-18]
4. C. Meinel, T. Gayvoronskaya, and M. Schnjakin, "Blockchain: Hype oder innovation," Hasso-Plattner Institute, Prof.-Dr.-Helmert-Strae 2-3, 14482 Potsdam, Germany, 2018.
5. A. Jøsang, J. Fabre, B. Hay, J. Dalziel, and S. Pope, "Trust requirements in identity management," in *Proceedings of the 2005 Australasian Workshop on Grid Computing and e-Research - Volume 44*, ser. ACSW Frontiers '05. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2005, pp. 99–108. [Online]. Available: http://dl.acm.org/citation.cfm?id=1082290.1082305
6. U. Kylau, Y. Thomas, M. Menzel, and C. Meinel, "Trust requirements in identity federation topologies," in *2009 International Conference on Advanced Information Networking and Applications*, May 2009, pp. 137–145.
7. M. S. Ferdous and R. Poet, "Analysing attribute aggregation models in federated identity management," in *Proceedings of the 6th International Conference on Security of Information and Networks*, ser. SIN '13. ACM, 2013, pp. 181–188.
8. A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, Mar. 2007.
9. C. Castelfranchi and R. Falcone, *Trust Theory: A Socio-Cognitive and Computational Model*, 1st ed. Wiley Publishing, 2010.
10. D. H. McKnight and N. L. Chervany, "The meanings of trust," University of Minnesota, Tech. Rep., 1996.
11. A. Satariano. (2018) What the g.d.p.r., europes tough new data law, means for you. [Online]. Available: https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html [Accessed: 2019-01-18]
12. A. Grüner, A. Mühle, T. Gayvoronskaya, and C. Meinel, "A quantifiable trust model for blockchain-based identity management," in *2018 International Conference on Blockchain*, August 2018.
13. (2018) Blockchain and identity. [Online]. Available: https://github.com/peacekeeper/blockchain-identity [Accessed: 2019-01-18]
14. C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena. (2016) uport: A platform for self-sovereign identity. [Online]. Available: http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf [Accessed: 2019-01-18]
15. D. Reed, J. Law, and D. Hardman. (2016) The technical foundations of sovrin. a white paper from the sovrin foundation. [Online]. Available: https://www.evernym.com/wp-content/uploads/2017/07/The-Technical-Foundations-of-Sovrin.pdf [Accessed: 2019-01-18]
16. M. Sporny and D. Longley. (2018) W3c community group draft report. verifiable claims data model and representations 1.0. [Online]. Available: https://www.w3.org/2017/05/vc-data-model/CGFR/2017-05-01/ [Accessed: 2019-01-18]
17. C. Allen. (2016) The path to self-sovereign identity. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html/cointelegraph.com/news/first-iteration-of-ethereum-metropolis-hard-fork-to-appear-monday [Accessed: 2019-01-18]
18. P. Windley, *Digital Identity*. O'Reilly Media, Inc., 2005.