Rebooting the Web of Trust

Designing the Future of Decentralized Self-sovereign Identity

A White Paper from RWOT IX: Prague

A Rubric for Decentralization of DID Methods

by Joe Andrieu (joe@legreq.com),
Shannon Appelcline (shannon.appelcine@gmail.com),
Amy Guy (amy@rhiaro.co.uk),
Joachim Lohkamp (joachim@jolocom.com),
Drummond Reed (drummond.reed@evernym.com),
Markus Sabadello (markus@danubetech.com),
and Oliver Terbu (oliver.terbu@consensys.net)

***RWOT IX** was sponsored by:*

Protocol Labs

ABSTRACT

The communities behind Decentralized Identifiers (DIDs) bring together a diverse group of contributors who have decidedly different notions of exactly what "decentralization" means.

Rather than attempting to resolve this potentially unresolvable question, we propose a rubric — a scoring guide used to evaluate the performance of a product or a project — that teaches how to evaluate a given DID Method according to one's own requirements.

This rubric presents a set of criteria that an Evaluator can apply to any DID Method based on the use cases most relevant to them. We avoid reducing the Evaluation to a single number because the criteria tend to be multidimensional and many of the possible responses are not necessarily good or bad. It is up to the Evaluator to understand how each response in each criterion might illuminate favorable or unfavorable consequences for their needs.

While this rubric allows the evaluation of many aspects of the decentralization of a DID Method, it is not exhaustive and does not cover other factors that may affect selection or adoption of a particular Method, such as privacy, security, reliability, or efficiency.

BACKGROUND

A rubric is a tool used in academia to communicate expectations and evaluate performance. It clarifies what will be evaluated and how. Written records of an evaluation, which we'll call an Evaluation Report, document how a particular subject is measured against the criteria. For students, a rubric helps to clarify how their work will be evaluated by others. For Evaluators, a rubric provides a consistent framework for investigating and documenting the performance of a subject against a particular set of criteria. In short, a shared rubric improves decision making when selecting or comparing subjects.

A rubric consists of a set of criteria to be evaluated, possible responses for each criterion, and a scoring guide explaining both how to choose and interpret each response. The act of evaluating a rubric, which we call an Evaluation, provides a basis for self-evaluation, procurement decisions, or even marketing points.

The authors of this paper were inspired to develop a rubric for decentralization when discussions about the requirements for decentralized identifiers, aka DIDs, led to intractable disagreement. It became clear that no single definition of "decentralized" would suffice for all of the motivations that inspired developers of DID Methods to work on a new decentralized approach to identity. Despite this challenge, two facts remained clear:

1. The people invested in this work shared a common goal of reversing the problems with centralized identity systems; and

2. They also had numerous, distinct reasons for doing so.

Rather than attempt to force a definition of "decentralized" that might work for many but would alienate others, the group set out to capture the measurable factors that could enable Evaluators to judge the decentralization of DID Methods based on their own independent requirements. Instead of a top-down formal definition of "decentralized", the group chose a rubric as a mechanism for objective Evaluation with minimal embedded bias.

The result is this document.

HOW TO APPLY THIS RUBRIC

This rubric is meant to be applied by an Evaluator considering the decentralization of any given DID Method for suitability to their purpose. In short, you[1] apply the rubric by evaluating the criteria: ask each relevant question and select the most appropriate response. Pick the most important criteria for your use and apply that against the most relevant DID Methods under consideration. We call the result of that analysis an Evaluation and the written record of an Evaluation an Evaluation Report.

In simple steps:

1. Understand the use for which the DID Method is being evaluated.
2. Select the criteria that are most relevant to the use.
3. Evaluate one or more DID Methods against the selected criteria.

Each Evaluation should start with an explicit framing of the use under consideration. Are you evaluating the Method for use in Internet-of-Things (IoT)? For school childrens' extra-curricular activities? For international travel? The use, or set of uses, will directly affect how some of the questions are answered. This doesn't take a lot of work or detail; just identify them at the beginning of the process.

Where a given Method offers variability, such as multiple networks for the same Method, then evaluate each variant. For example, did:ethr supports Ethereum mainnet, multiple testnets and permissioned EVM-compliant networks such as Quorum. To apply a criterion to did:ethr, you will evaluate it against all the variations that matter ***to you***. Each variation should get its own Evaluation. This applies to Level 2 Networks[2] that can operate on multiple Level 1 Networks[3] as well as DID Methods that directly offer support for multiple underlying DID registries.

When creating an Evaluation Report, we recommend noting both the Evaluator and the date of the Evaluation. Many of the criteria are subjective and all of them are subject to change over time. Tracking

[1] Throughout this document we use the second-person pronoun "you" to refer to Evaluators of a DID Method applying this Rubric.

[2] A network built atop another network, such as the Lightning Network, which is built atop Bitcoin.

[3] A foundational network, such as Bitcoin.

who made the Evaluation and when they made it will help readers better understand any biases or timeliness issues that may affect the applicability of the Evaluation.

Be selective and acknowledge the subjective. Evaluations do not need to be exhaustive. There is no requirement to answer all the questions. Simply answer the ones most relevant to the use contemplated. Similarly, understand that any recorded Evaluation is going to represent the biases of the Evaluator in the context of their target use. Even the same Evaluator, evaluating the same Method for a different use, may come up with slightly different answers — for example, that which is economically accessible for small businesses might not be cost-effective for refugees, and *that* could affect how well-suited a given Method is for a specific use.

Finally, note that this particular rubric is about decentralization. It doesn't cover all of the other criteria that might be relevant to evaluating a given DID Method. There are security, privacy, and economic concerns that should be considered. We look forward to working with the community to develop additional rubrics for these other areas and encourage Evaluators to use this rubric as a starting point for their own work rather than the final say in the merit of any given Method.

In short, use this rubric to help understand if a given DID Method is decentralized enough for your needs.

EVALUATION REPORTS

To record and report an Evaluation, we recommend two possible formats, either comprehensive or comparative.

A comprehensive Evaluation applies a single set of criteria to just one Method. This set is chosen by the Evaluator; it need not be all possible criteria, but it is all relevant criteria as judged by the Evaluator.

A comparative Evaluation includes multiple Methods in the same table to easily compare and contrast two or more different Methods. This may include any number of criteria. These are the type of reports we use as examples throughout the criteria list.

In addition to the selected criteria, we recommend each report include a header that specifies:

1. The Method(s) being evaluated
2. A link to the Method specification
3. The Evaluator(s)
4. The date of the Evaluation
5. A description of the use case(s) for which the Method is being evaluated
6. The rubric used for the Evaluation, along with reference to the specific version.
7. Optionally, a URL for retrieving the report.

An example comparative report header can be found in the section Comparative Evaluation Report Header.

CATEGORIES OF CRITERIA

We have grouped our criteria into five categories:

1. Rulemaking
2. Operations
3. Enforcement
4. Alternatives
5. Adoption

Evaluators should consider criteria from all five groups, as best fits your use cases. The first three are about how a given Method is governed: Rulemaking, Operations, and Enforcement. The latter two address issues of lock-in and accessibility: Alternatives and Adoption.

A few notes about governance. Our approach parallels the same breakdown in authority embodied in the United States Constitution.

- **Rulemaking** addresses who makes the rules and how. (This is the legislative branch in the US.)
- **Operations** addresses how those rules are executed and how everyone knows that they are carried out. (This is the executive branch in the US.)
- **Enforcement** addresses how we find and respond to rule breaking. (This is the judicial branch in the US.)

This mental model is key to understanding both the criteria of each section and why we included some criteria instead of others.

The sections on Alternatives and Adoption were created because we identified decentralization factors that have nothing to do with governance. As an example, a completely open system of formal "decentralized" governance could be *de facto* centralized because it is the only available option. For example, if there is only one wallet you can use for a given Method, that may be unacceptably centralized for a given use. On the other hand, if that wallet is already ubiquitous in the use cases that matter, this centralizing factor may not be as relevant given its accessibility by intended users. Similarly, some use cases would be dramatically limited if there were only one relying party who is willing to accept DIDs of a given Method. If a theoretical did:facebook Method is only accepted by Facebook (because no other services are willing to use it) that would affect its centralization, even if it is *possible* by design for any service to do so. The criteria in Alternatives and Adoption sections attempt to evaluate these factors.

THE ARCHITECTURE

When evaluating the governance of DID Methods, three potentially independent layers should be considered: the specification, the network, and the registry.

- The **specification** is the governing document for the Method that outlines how that particular Method implements the required and any optional components of the DID Core specification.
- The **network** is the underlying communications layer, i.e., how users of the Method communicate with others to invoke the operations of the Method.
- The **registry** is a given instance of recorded state changes, managed according to the specification, using the communications channel.

For Rulemaking, the criteria should be evaluated against all three of the above layers.

For Operations, the criteria should be evaluated against the network and the registry. The specification is taken as a given (it is the core output of Rulemaking).

For Alternatives, the criteria should be evaluated against the particular DID Method.

For Adoption, the criteria should instead be evaluated for each major software component: wallet, resolver, and registry.

For the examples in the rest of this document we refer to a set of Methods that are familiar to the authors and exhibit interesting characteristics for Evaluation. These are listed in the "Comparative Evaluation Report Header" table below.

COMPARATIVE EVALUATION REPORT HEADER

Comparison Evaluation (used throughout the criteria list)	
Evaluators	Joe Andrieu <joe@legreq.com>
Evaluation Date	2020-01-03
Use Cases	**Verifiable software development**. The signing of commits by developers and their verification to ensure that source code in a particular git repository is authentic. **User authentication.** The use of DIDs for authenticating users for access to system services. **Long term verifiable credentials.** The use of DIDs as subject identifiers for long term (life-long) verifiable credentials such as earned academic degrees.

Report URL	TBD
Rubric	**A Rubric for Decentralization of DID Methods v0.0.3**
Rubric URL	https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/final-documents/decentralization-rubric.pdf

Methods Considered

	Specification	**Network**	**Registry**
did:peer	https://openssi.github.io/peer-did-Method-spec/index.html	n/a (communications can flow over any agreeable channel)	Held by each peer
did:git	https://github.com/dhuseby/did-git-spec/blob/master/did-git-spec.md	git (an open source version control system) https://git-scm.com/	Any Method-compliant git repository
did:btcr	https://w3c-ccg.github.io/didm-btcr	Bitcoin	Bitcoin
did:sov	https://sovrin-foundation.github.io/sovrin/spec/did-Method-spec-template.html	Hyperledger Indy	A particular instance of Hyperledger Indy
did:ethr	https://github.com/decentralized-identity/ethr-did-resolver/blob/develop/doc/did-method-spec.md	Ethereum	Specific smart contracts for each network.
did:jolo	https://github.com/jolocom/jolocom-did-driver/blob/master/jolocom-did-Method-specification.md	Ethereum	Specific smart contracts for different networks and subnetworks.

Note: The evaluations in this document are made by Joe Andrieu <joe@legreq.com>. Other authors have expressed different evaluations, because of different weighting of the relevant of different characteristics in particular methods. This should be expected in any evaluation: they will always be colored by the particular perspective of the evaluator.

THE CRITERIA

1. RULEMAKING

Rulemaking addresses who makes the rules and how. Output of rulemaking are the rules.

1.1 OPEN CONTRIBUTION (PARTICIPATION)

1.1.1 Question

How open is participation in governance decisions?

1.1.2 Possible Responses

A) Anyone can participate in an open, fair process where all participants have equal opportunity to be heard and influence decisions.
B) Anyone can comment and contribute to open debate, but decisions are ultimately made by a closed group.
C) Debate is restricted to a selected but known group.
D) Debate is conducted in secret by an unknown group.

1.1.3 Relevance

Governance determines how the rules of the underlying network are set and maintained. The more parties that are able to contribute to governance debates, the more decentralized the governance.

1.1.4 Examples

Method	Spec.	Net.	Reg.	Notes.
did:peer	B	C	C	did:peer has no intrinsic **network**. It can use any communications channel between parties. Only those two parties are privy to the **registry** decisions made about communications and recordation. The **specification** is openly developed on github by a listed set of contributors and issues may be raised by anyone.
did:git	B	C	D	The git **network** is the git source code, which is controlled (currently) by 16 people. They do not have a public issues process. The **specification** is openly developed on github by a listed set of contributors and issues may be raised by anyone. Each **registry** is controlled by potentially unknown parties as negotiated in "meatspace".

did:btcr	B	D	D	Changes to the bitcoin protocol, which control the **network** and **registry**, are chaotic and uncertain. They use BIPs, but the path to adoption is uncertain and the relative power of developers, miners, and users is open to debate. The **specification** is openly developed on github by a listed set of contributors and issues may be raised by anyone.
did:sov	B	B	B	The Sovrin Foundation has an open community governance model for its **network**, **specification**, and **registry** but has not yet had open elections of trustees.
did:ethr	C	B	n/a	The **network** is Ethereum, which evolves through EIPs proposed by anyone, discussed by “the community”, and ultimately adopted by Ethereum core devs. The **specification** is published on GitHub with issues open to the public. The smart contract for the **registry** is immutable.
did:jolo	D	B	D	Jolocom’s **network** is Ethereum. Decisions over Jolocom’s smart contracts (the **registry**) are made by an unknown group within Jolocom. The **specification** (as listed in the DID Method Registry) is currently archived and not open to public comment.

1.2 TRANSPARENCY

1.2.1 Question

How visible are rulemaking processes?

1.2.2 Responses

A) Agendas and participation details for all meetings are publicly announced, the meetings are broadcast in real-time to any listeners, and all minutes and recordings are captured in realtime and publicly reviewable in perpetuity.
B) Minutes of meetings are reviewable by the public, including all votes and who cast them, but real-time observation may be limited.
C) All current rules are publicly available.
D) Rules may be changed without public notice.

1.2.3 Relevance

While participation measures active contribution, transparency measures the visibility of discussions affecting rule making. If such discussions are only visible to a limited group, it centralizes decision making in ways that Evaluators and users cannot easily see.

1.2.4 Examples

Method	Spec.	Net.	Reg.	Notes
did:peer	C	n/a	B	Rules for accepting changes to the business rules (**registry**) are bilaterally negotiated between the peers, subject to conformance with the **specification**.
did:git	C	n/a	D	The controllers of a git repo (**registry**) are a limited set, but their decisions are “meatspace protocol” and hence not explicitly transparent.
did:btcr	C	C	C	The **specification** is maintained by volunteers, operating in an open fashion but without formal processes for announcements and meeting notes. The **network** and **registry** are bitcoin, which has a fairly public but messy innovation process, without formal meetings or votes.
did:sov	B	B	B	The Sovrin Governance Framework actually requires all minutes of Sovrin governance discussions are public with a handful of exceptions for legal reasons (e.g., HR actions, legal actions). See Section 9 of Sovrin Governing Body Policies—https://sovrin.org/wp-content/uploads/Sovrin-Governing-Body-Policies-V1.pdf.
did:ethr	C	C	D	The governance of the did:ethr method (**specification**) is controlled by a smart contract, which is immutable.
did:jolo	C	C	D	Jolocom does not expose the internal and/or customer conversations that drive rulemaking (**specification**, **registry**).

1.3 BREADTH OF AUTHORITY

1.3.1 Question

How many independent parties actively participate in the governance authority?

1.3.2 Responses

A) Rules are decided by an open set of multiple parties.
B) Rules are decided by a closed set of multiple parties.
C) Rules are decided by a single known entity.
D) Rules are decided by an unknown party.

1.3.3 Relevance

Is the governing authority for the DID Method innately centralized? Is the Method governed by a single entity, who could make arbitrary changes to the governance? Or is it governed by a closed set of parties, without fully open access? Or is there a legitimate effort to open the decision making process to multiple competing and cooperating parties?

1.3.4 Examples

Method	Spec.	Net.	Reg.	Notes
did:peer	B	B	B	There is only one editor to the did:peer **specification**, but the repository itself lists 14 contributors with actual commits. The **network** and **registry** rules are ultimately decided by the parties participating in each did:peer context (a closed set of peers).
did:git	B	B	D	There is only one editor to the did:git **specification**, with a total of three contributors with actual commits (although more are listed). The **network** is git (controlled by an unknown population) and the **registry** is a particular repo under the control of potentially unknown parties.
did:btcr	B	A	A	The **specification** lists 4 editors and the repo lists 4 committers. The **network** and **registry** is bitcoin, which relies on an informal process of any number of parties.
did:sov	C+	C+	C+	All three layers are ultimately under the control of the Sovrin Foundation, which itself has a governance framework to coordinate input from multiple parties.
did:ethr	B	B	n/a	The **specification** is now under DIF control and the **registry** is immutable. The **network** is Ethereum, which is controlled by Ethereum core devs.
did:jolo	C	B	C+	The **specification** and **registry** are controlled by Jolocom, sometimes in coordination with customers. The **network** is Ethereum, which is controlled by Ethereum core devs.

1.4 PUBLIC V PRIVATE ECONOMICS

1.4.1 Question

How privatized is the economic interest of the governing authority?

1.4.2 Responses

A) The governing authority is established for the public good without rents or remuneration.
B) The governing authority is established for the common good of a limited set of parties.
C) The governing authority is established to enhance profits for a limited set of parties.
D) The governing authority is established to extract rents.

1.4.3 Relevance

The underlying financial goals of DID Method creators may affect the centralization of their Method. If the goal of a Method is to enhance or support a certain group, then there may be centralization focused on that group and their interests. In the most centralized extreme, a Method may be created explicitly to establish a monopoly market that it can extract rent from. The opposite extreme is a Method created explicitly for the public good.

1.4.4 Examples

Method	Spec.	Net.	Reg.	Notes
did:peer	A	B	B	The **specification** was developed to demonstrate a way that anyone can use DIDs without a distributed ledger. Each **network** and **registry** is established solely for the benefit of each pair of peers.
did:git	A	A	B	The **specification** was developed to demonstrate how you might use DIDs to enhance git-based software development. Git itself (the **network**) was developed so anyone could have better software development practices. Any given **registry** (a repo) is assumed to be established for the common good of its controllers.
did:btcr	A	A	A	The **specification** was developed to demonstrate how you could use Bitcoin for DIDs. The **network** and **registry** were created as a public benefit proof of concept for decentralized digital cash.
did:sov	B	B	B	All three elements are developed and maintained for the common good. As a 501(c)4 the Sovrin foundation is a social welfare organization that must operate primarily to further the common good and general welfare of the people of its community.
did:ethr	C	C	C	The **specification** and **registry** were created by a private company (uPort) to support their business. The smart contract is a common good and free to use. However, the **network**, Ethereum, was created to create wealth for its creators.

did:jolo	C	C	C	The **specification** and **registry** were created by a private company (Jolocom) to support their business, but are now available for anyone to use. Similarly, the **network**, Ethereum, was created to create wealth for its creators.

1.5 COST

1.5.1 Question

How expensive is it to participate in governance (in time, money, or effort)?

1.5.2 Responses

A) Free to all
B) Inexpensive, but accessible
C) Modest cost for interested parties
D) Expensive and restricted
E) Not possible to participate

1.5.3 Relevance

Governance takes resources, which can limit the ability of interested parties to influence rulemaking. Generally, the more expensive it is to participate, the more governance centralizes to those parties most able to make the investment.

1.5.4 Examples

Method	Spec.	Net.	Reg.	Notes
did:peer	B	n/a	n/a	The **specification** is available for engagement via Github, but participating in decision making takes time and requires expertise. The **network** and **registry** are negotiated on a case-by-case basis, so participation could be anywhere on the spectrum.
did:git	B	D+	D	The **specification** is available for engagement via Github, but participating in decision making takes time and requires expertise. Git itself (the **network**) is partially influenceable through online issues, but real change requires deep expertise and is controlled by a handful of developers. The governance of any given **registry** is, by design, a question of “meatspace” negotiations, which is expensive and limited to the parties who control the repo.
did:btcr	B	D	D	The **specification** is available for engagement via Github, but

				participating in decision making takes time and requires expertise. The **network** and **registry** (bitcoin) are theoretically open to any participants, but influencing the direction of bitcoin is notoriously expensive and unpredictable.
did:sov	B	B	B	The did:sov: method (**specification**) together with 100% of the Sovrin ledger and Sovrin infrastructure (**registry**) are governed by an open public non-profit organization that is open to anyone to participate. The Sovrin Governance Framework Working Group is an all-volunteer community-driven effort in which over 50 volunteers have participated for over three years to develop a fully public governance framework on which anyone can comment and suggest improvements. The Sovrin ledger operates on the Hyperledger Indy open source code base (**network**) to which anyone can contribute.
did:ethr	C	D	E	The **specification** is available for engagement via Github, and managed by DIF. The **network** itself, Ethereum, is expensive and difficult to influence: not impossible for an outsider, but expensive. Governance of the **registry** is not accessible except with uPort's permission.
did:jolo	D	D	E	While the did:jolo **specification** is available online, it is archived and not open to further engagement. Jolocom has sole control over who can participate in developing specifications based on did:jolo, and they work with customers to customize the Method. The **network** itself, Ethereum, is expensive and difficult to influence: not impossible for an outsider, but expensive. The **registry** is immutable and therefore not open to participation.

2. OPERATION

2.1 PERMISSIONED OPERATION

2.1.1 Question

To use the DID Method, do you need permission?

2.1.2 Responses

A) Anyone can participate fully (full read/write and participation in consensus).
B) Anyone can read/write, but consensus mechanism is permissioned.
C) Anyone can read, but writing and consensus is permissioned.
D) All participation is permissioned.

2.1.3 Relevance

Permissioned operation impacts the availability of the network to various participants, which can affect inclusivity with regard to underserved or vulnerable populations. Permissioned networks also expose the permission giver to legal or other attacks.

2.1.4 Examples

Method	Net.	Reg.	Notes
did:peer	A	D	By design, did:peer can use any communications channel (**network**) and only the participation of the participants is required. Unfortunately, for those outside the peer context, the **registry** is inaccessible.
did:git	A	D	Git software (**network**) is available to anyone. Participation and access is controlled by the repo (**registry**) maintainers.
did:btcr	A	A	The bitcoin **network** (and thus **registry**) is open to anyone.
did:sov	C	C	The Sovrin foundation limits writing and consensus access, but the **network** is open to all for reading.
did:ethr	A	A	The Ethereum **network** is open to anyone. The **registry** is accessible to anyone.
did:jolo	A	A	The Ethereum **network** is open to anyone. The **registry** is accessible to anyone, although some subregistries/subnetworks may have alternate rules.

2.2 FINANCIAL ACCOUNTABILITY

2.2.1 Question

How transparent and fair are the economics of the Method?

2.2.2 Answers

A) All operational finances are transparent and accounted for.
B) Compensation for primary operators is transparent.
C) Some financial flows are visible.
D) Operation is privatized with no visibility.

2.2.3 Relevance

Similar to Governance criterion #3, financial accountability reflects the integrity and sustainability of the DID registry. The more open, transparent, and accountable the system, the greater the confidence a DID controller may have that it will remain stable and operational, and therefore continue to provide service.

2.2.4 Examples

Method	Net.	Reg.	Notes
did:peer	D	D	The financials of both parties have no visibility.
did:git	A	D	The financials of both parties have no visibility. However, the underlying git software (**network**) is free and open source.
did:btcr	A-	A-	Bitcoin is transparent, although operations are somewhat obscured by pseudonymous transaction addresses.
did:sov	B	B	The Sovrin Foundation publishes an annual report with details about overall finances for their operation, and the books are required to be openly available for inspection by anyone.
did:ethr	A-	A-	Ethereum is transparent, although operations are somewhat obscured by pseudonymous transaction addresses.
did:jolo	A-	A-	Ethereum is transparent, although operations are somewhat obscured by pseudonymous transaction addresses.

2.3 INTEROPERABILITY

2.3.1 Question

Does the DID Method restrict access or functionality to particular wallet implementations per the specification? (Whether or not any given wallet works with the resolver or registry is covered elsewhere.)

2.3.2 Responses

A) Any wallet can work with any resolver on any registry.
B) Any wallet can work with multiple resolvers and multiple registries.
C) Some implementations of some wallets can work with some resolvers.
D) There is a single combined suite of resolver, registry, and wallet.

2.3.3 Relevance

The ability to communicate with different (ideally all) resolvers and registries significantly increases the applicability of a decentralized identity layer / usability of a given wallet. Vice versa, limited capability to work with other Methods and registries restrict usage.

2.3.4 Examples

Method	Net.	Reg.	Notes
did:peer	A	A	did:peer is agnostic regarding the software that implements it.
did:git	A-	A-	did:git is predicated on using git software. However, git itself uses a protocol that any software could implement. Although we know of no other implementation in widespread use, we know of no limitations in the protocol itself.
did:btcr	A	A	Bitcoin has no restrictions on the software used to access the network.
did:sov	A	A	did:sov: has no restrictions on any software that implements it.
did:ethr	A	A	Neither Ethereum nor the smart contract has any restrictions on the software used to access them.
did:jolo	A	A	Neither Ethereum nor the smart contract has any restrictions on the software used to access them.

2.4 LIMITED RESOURCE RESOLUTION

2.4.1 Question

How much memory is required for DID resolution, without relying on authoritative intermediaries (e.g. blockchain explorer APIs)? We consider the amount of memory required to fully resolve a DID of the method, whether that memory is stored locally or processed ephemerally via communications.

2.4.2 Responses

A) Minimal. Less than 1MB
B) Modest. 1MB to 1GB
C) Substantial. 1GB to 128 GB
D) Exceptional. Over 128GB in memory

2.4.3 Relevance

Whether or not one can resolve a DID directly on a resource-constrained device affects the granularity at which smaller devices can be part of the ecosystem. If small edge devices, such as a smart watch, smart speaker, or even a mobile phone, are incapable of directly resolving a DID of the DID Method, then the method will lead to cloud-based services like blockchain explorer APIs, which themselves become a point of centralization. Many find this option an acceptable engineering trade-off. Others would prefer solutions that allow even the smallest devices to be fully capable of resolving DIDs in an authoritative manner.

2.4.4 Examples

Method	Net.	Reg.	Notes
did:peer	A	A	did:peer
did:git	B	varies	Git for Windows(**network**) is just shy of 50 MB (please update if there are smaller versions available). However, one must still download the entire repo (**registry**) containing the registry material.
did:btcr	D	D	To definitively resolve, one must operate a full node.
did:sov	A	A	The Sovrin ledger is based on Hyperledger Indy which supports highly efficient state proofs for cryptographic verification of resolution responses. A full node is not required.
did:ethr	B	B	A full ethereum node takes >100GB, but a light ethereum node can support this method with less than 256kb.
did:jolo	B	B	A full ethereum node takes >100GB, but a light ethereum node can support this method with less than 256kb.

2.5 LIMITED RESOURCE REGISTRATION

2.5.1 Question

What are the minimum resources required to create a trusted DID without relying on intermediaries?

2.5.2 Responses

A) Minimal. Less than 1MB
B) Modest. 1MB to 1GB
C) Substantial. 1GB to 128 GB
D) Exceptional. Over 128GB in memory

2.5.3 Relevance

Being able to create a DID in constrained situations enables certain types of decentralized applications that otherwise are not possible. On the edge, many devices rely on gateways to manage compute-, memory-, and bandwidth- intensive tasks. For example, while a smart lightbulb might use ZigBee or 6LowPAN, it will typically use a hub to connect to the Internet, even for access from devices within the local IP network. The more resources it takes for small devices to participate in registration, the greater the percentage of those that will need to rely on centralizing factors like hubs and gateways.

2.5.4 Examples

Method	Net.	Reg.	Notes
did:peer	A	A	did:peer
did:git	B	varies	Git for Windows (**network**) is just shy of 50 MB (please update if there are smaller versions available). However, one must still download the entire repo (**registry**) containing the registry material.
did:btcr	A-	A-	To register a DID, one must simply get a transaction on the ledger, unless you choose to host a continuation DID Document elsewhere, which would require its own resources.
did:sov	A	A	Registration of a DID is a single transaction that can be performed by a thin client.
did:ethr	A+	A+	The smart contract used for did:ethr recognizes any valid public key as a DID, without requiring registration. This means DIDs can even be created offline with full usability. Only rotation and the registration of service endpoints require network access.
did:jolo	A+	A+	The smart contract used for did:ethr recognizes any valid public key as a DID, without requiring registration. Only rotation and the registration of service endpoints require network access.

2.6 SCOPE OF USAGE

2.6.1 Question

How widely can DIDs of this Method be used?

2.6.2 Responses

A) Universal: DIDs can only be created and used universally, between any number of parties.
B) Contextual: DIDs can be created and used contextually, between any set of collaborating parties.
C) Paired: DID can be created and used pairwise, between any two parties.
D) Central: DIDs can only be created and used with a single, centralized party.

2.6.3 Relevance

Different Methods enable different scopes in which a DID might be considered usable or valid. For example, peer DIDs are only usable between the two peers who share unique DIDs with each other; other parties are unable to resolve the DID, find the DID Document, or use its information to establish secure interactions. In contrast, BTCR records all DIDs on a public ledger, meaning that all DIDs are fundamentally accessible to any party who might receive the DID. Contextual DIDs are a middle ground that allow a set of parties to use DIDs, while those outside that group cannot meaningfully do so. Finally, central DIDs use the DID syntax and DID Documents to establish secure communications, but authority to use these DIDs resides with the central party, who may revoke that ability at their discretion.

2.6.4 Examples

Method	Net.	Reg.	Notes
did:peer	A+	C	Did:peer is communication-layer independent, so it can be used on any **network**, including direct physical links. However, only those parties to the creation of the DID (**registry**) can actually use it. The DIDs have no use outside that direct peer-to-peer relationship.
did:git	A	B	Anyone can set up a git-based repo and use did:git (**network**). However, to interact with a given repo (**registry**), one must be aware of the repo, including which instance of it is authoritative.
did:btcr	A	A	Open, permissionless, and globally resolvable.
did:sov	A	B	Transactions on the Sovrin ledger are publicly readable by anyone (**network**). Transactions may be written by any Transaction Author, however for GDPR reasons personal data may not currently be written to the Sovrin ledger. See https://sovrin.org/data-protection/.
did:ethr	A	A	Open, permissionless, and globally resolvable.
did:jolo	A	A	Open, permissionless, and globally resolvable.

2.7 AUDITABILITY

2.7.1 Question

Who can retrieve cryptographic proof of the history of changes to a given DID Document?

2.7.2 Responses

A) Anyone
B) Only a select group, including parties not involved in a given DID transaction
C) Only parties to the transaction
D) Not available

2.7.3 Relevance

Trustlessness is a prerequisite of a decentralized system. If you *have to* trust the source of a DID Document (i.e., if you can't verify cryptographically a DID Document that is returned from resolution), then you are at the mercy of a potentially centralized authority. If, instead you have a cryptographic audit trail, then the current state of a DID cannot be compromised by an intermediary or central party.

2.7.4 Examples

Method	Reg.	Notes
did:peer	C-	DID:peer maintains a cryptographic journal, but it is only available to the peers and, technically, can be refused (each peer may suspend interactions at any time).
did:git	B-	*If* you have access to the authoritative git repo, you can see the cryptographic journal. However, within the method specification, there is no way to know if the repo you are inspecting is, in fact, definitive.
did:btcr	A	Anyone can see everything.
did:sov	A	Anyone can see everything — the Sovrin ledger is completely public.
did:ethr	A+	Anyone can see updates and deletes. Creation is private.
did:jolo	A+	Anyone can see updates and deletes. Creation is private.

3. ENFORCEMENT

The matter of enforcement is a tricky question, one that the authors did not have sufficient time to explore and resolve. Although we are forced to leave this section for future collaboration, we want to share some of our insights.

In state-level governance, enforcement is an operational matter for the police and a judgmental matter for the courts. In other words, the police and the courts constitute the enforcement powers of governance.

For distributed systems, especially those like Bitcoin and Ethereum, enforcement is a function of both social and technical functions.

Technical enforcement could include such notions as which cryptography is used to ensure proper authentication of transactions or the details of a consensus mechanism such as proof of work (POW) or proof of stake (POS). Should a given cryptographic technique prove to be compromised, that would affect the ability of the system to enforce its own rules, making the specific cryptography used by a given Method a significant factor in evaluating the suitability of a given Method. Further, understanding the decentralized nature of a given POW or POS mechanism requires an Evaluation of both the means for executing the mechanism as well as a profile of those parties who could potentially influence or even undermine that mechanism.

Social enforcement mechanisms rely on community or institutions. For Methods that have explicit governing bodies, like did:sov, presumably enforcement is a matter under their jurisdiction. Nodes on the network that operate outside the guidelines of the governing bodies can presumably have permission revoked as a means of enforcement. Methods that do not have formal governing bodies may, nevertheless, have a strong enough community to correct violations, as Ethereum did in response to the DAO hack[4].

Finally, all Methods operate in (and across) one or more geographic jurisdictions, each with potentially distinct laws and mechanisms of enforcement. Identifying the potential enforcement mechanisms that *could* apply to the Method, to those using a Method, or to the operators of a Method, is almost certainly going to be relevant to certain Evaluators. We have already seen GDPR and various US laws being applied based on where different servers are physically located, with lawsuits brought against server operators. It is inevitable that similar actions will eventually be brought against DID Method operators at various levels.

In short, understanding the process for identifying violations and enforcing the rules as set by the rulemakers is vital to a complete Evaluation of the decentralization of a DID Method. We regret that we were not able to sufficiently explore these issues for this rubric and we look forward to working with subsequent collaborators to flesh out criteria that can provide suitable guidance for enforcement criteria.

4. ALTERNATIVES

For each major software component (Wallet, Resolver, and Registry), ask each of the following questions.

In this section, because DIDs are so early in the development lifecycle, most DID methods in production have only one implementation and some have none. Therefore, we have not standardized the responses nor provided examples. Consider these open-ended essay questions for consideration. As the market matures, this subset of questions will improve.

4.1 ACTIVE IMPLEMENTATIONS

4.1.1 Question

How many (active) substitutable, interoperable implementations support this Method?

[4] https://www.coindesk.com/understanding-dao-hack-journalists

4.2 MARKET SHARE

4.2.1 Question

How large is the share of use by each of the top three implementations?

4.3 PLATFORM SUPPORT

4.3.1 Question

Which platforms have implementations?

4.4 LANGUAGE SUPPORT

4.4.1 Question

Which programming languages have implementations?

4.5 ROGUE RISK

4.5.1 Question

If there is one dominant implementation, how many programmers would need to be compromised to get a back-door into distribution?

4.6 FORKABILITY

4.6.1 Question

Is it forkable?

5. ADOPTION (AND DIVERSITY)

Similar to the alternatives section, this section is limited because DID methods are just beginning to reach production, and so we have minimal knowledge of current adoption. As the market matures, we anticipate this section improving.

5.1 ACCEPTANCE

5.1.1 Question

How many relying parties accept DIDs of this Method?

5.2 USERS

5.2.1 Question

How many daily active users use this Method?

5.3 INTERNATIONAL ADOPTION

5.3.1 Question

How many different countries have significant usage?

5.4 IN WHICH COUNTRIES?

5.4.1 Question

Which countries have significant usage?

5.5 LANGUAGE SUPPORT

5.5.1 Question

How many (human) languages are supported?

6. NOT DECENTRALIZATION CRITERIA

We reviewed a lot of proposed criteria for inclusion in this rubric. Not all of them turned out to be a good fit, often because they were simply not related to decentralization. They were useful criteria for evaluating a DID Method, but we specifically limited ourselves to ONLY consider those criteria that specifically capture some notion of decentralization or its related benefits.

We've included a list of additional considered criteria in Appendix B.

Maturity was one of those categories of criteria that we liked, but just wasn't related to how decentralized a Method is. We considered the maturity of the specification, such as how long it has been published. We considered the organizational maturity of the lead proponents of the Method: is this Method backed by a major player that has been around a while or is its only advocate a small startup? We even considered the operational maturity of the Method: how long had the Method been live, in production?

These are all excellent questions to ask when considering supporting, adopting, or contributing to a particular DID Method, but sadly, they do not capture anything about how decentralized a Method is. A system simply doesn't become more or less centralized just because it is around a long time.

What can happen over time is that a given Method might improve in its adoption or diversity, as more institutions, users, and platforms add support in various ways, and these aspects of a Method can shift how decentralized a Method might be, but maturity itself does NOT affect centralization.

The authors had similar discussions considering security, privacy, and reliability criteria. All of these are important, but not directly related to the question of decentralization. While decentralization *can* improve reliability, it can also undermine it if done poorly. Similarly, security and privacy don't necessarily impact decentrality and vice-versa.

We encourage everyone using this rubric to consider it as one tool for evaluating only the decentralization aspect of DID Methods. Other Evaluations will also be necessary to make a fully informed decision about adopting, supporting, or contributing to any given Method.

Conclusion

This Rubric for Decentralization of DID Methods provides one framework for evaluating how "decentralized" a given DID Method is. It offers a set of criteria which can be used selectively by Evaluators to better understand and document their considerations when deciding to support or adopt a given DID Method.

We look forward to feedback and improvements on this document and will be proposing it as the foundation for further development in the Decentralized Identifier Working Group (DID WG) of the World Wide Web Consortium. Today, comments are welcome in the Rebooting Web of Trust repository in which this document is published. Our intention is to move this conversation to the DID WG, should the group accept this contribution as a starting point for future work.

Appendix A: Terminology

Evaluator - The individual or organization applying this rubric to evaluate a DID Method.

Evaluation - The process of and analysis from answering the question in each selected criterion for a given DID Method. Evaluation could refer to deciding the answer to a single criterion or to a "complete" set, where completeness is in the judgment of the Evaluator.

Evaluation Report - The output of an Evaluation. The written documentation of the result of evaluating one or more DID Methods against this rubric. In practice, this is a completed report template, with answers for all of the criteria selected by the Evaluator.

Network - the channel that enables communication of DID Method operations, .e.g, for BTCR, any of the main bitcoin networks can be used (mainnet, testnet, etc.). For did:ethr, the network is any EVM-compliant network (each DID specifies one and only one such network).

Registry - the instantiated storage and integrated business logic that record the effect of DID Method operations. In did:ethr, the registry is a smart contract. In did:btcr, the registry is the specific bitcoin network (the network and the registry are the same).

Appendix B: Possible Additional Criteria

6.1 MATURITY

6.1.1 How long has the specification been published?

A) Just a concept sketch
B) A complete draft...
C) ...
D) …
E) Published as a fixed, recommended specification
F) [Published for X years]

6.1.2 How mature is the entity who controls the specification?

6.1.3 How long has the specification been in live usage?

6.2 CRYPTOGRAPHY

6.2.1 Can the individual use their own cryptographic material for key generation without sharing secrets?

6.2.2 Can DID Controllers specify their own cryptographic suite for key generation / signing / hashing / etc.?

6.2.3 Can DID Controllers specify ANY cryptographic suite for key generation / signing / hashing / etc.?

6.2.4 Do DID Controllers have cryptographically provable control over DID Documents?

6.2.5 Are all registry transactions publicly inspectable and cryptographically verifiable?Does the Method support specific cryptographic capabilities?

A) Multi-sig
B) Shamir secret sharing
C) HD Keys
D) Object Capabilities

6.2.6 Does the Method provide a cryptographic DID, or does it try to provide a human-readable name?

6.2.7 Do DIDs with a few random substitutions result in different valid DIDs, or is there cryptographic error correction to identify transmission errors and typosquatting?

6.2.8 Can the Method-specific-id be generated without the use of a per-Method centralized registry service (as required in section 7.1 of the DID specification)?

6.3 FIDUCIARY COMMITMENTS

6.3.1 Do operators of resolvers accept fiduciary responsibility to users? Do any?

6.3.2 Do operators of registry nodes accept fiduciary responsibility to users? Do any?

6.3.3 Do the parties in charge of governance accept fiduciary responsibility to users? Do any?

6.3.4 Do wallet creators & maintainers accept fiduciary responsibility to users? Do any?

6.4 RELIABLE RECOVERY

6.4.1 Are there mechanisms to recover from key loss?

6.4.2 Are there non-administrative mechanisms to recover from key loss

6.4.3 Are there cryptographically robust mechanisms for key recovery that allow individuals to select specific advocates or stewards?

6.5 SUBSTITUTABILITY

6.5.1 Are the DIDs portable to other Methods?

6.5.2 Are the DIDs portable to multiple registries?

6.5.3 Does the Method allow DID Controllers to specify where the DID Document resides?

6.5.4 Does the Method allow DID Controllers to specify wherever they want the DID Document to reside?

6.6 REVOCATION / DEACTIVATION / DELETION

6.6.1 Is it possible to provably remove a DID from the system (and all nodes)?

6.6.2 Is it possible to provably remove a DID Document from the system (and all nodes)?

6.6.3 Are revocations and deactivations provably documented?

6.6.4 Do revocations and deactivations allow for publicly visible explanations?

6.6.5 Can cryptographic material be selectively revoked or rotated?

6.7 RESOLUTION

6.7.1 Are all DIDs globally resolvable to a definitive, provably current DID Document?

6.7.2 Are private DIDs (which are NOT globally resolvable) supported?

6.7.3 Can access to DID Documents be limited to authorized parties?

6.7.4 Can you get older versions by version number and by timestamp?

6.7.5 Can you get cryptographic proof of the history of changes to a given DID Document?

6.8 COSTS

6.8.1 How much does DID creation and key rotation cost a DID Controller?

6.8.2 Must individual DIDs be written to the registry?

6.8.3 How much do changes to a DID Document cost the DID Controller?

6.8.4 Do changes to DID Documents require updating the registry?

6.8.5 What is the total cost of ownership for a typical DID and DID Document?

6.8.6 Are there free versions of wallets?

6.8.7 Are there free versions of registry software?

6.8.8 Are the free versions of resolvers?

6.9 CENSORSHIP RESISTANCE (ANSWER EACH WITH A YES OR NO)

6.9.1 Is there a single legal or natural entity, or set of known entities, who can be targeted with intent to manipulate the operation or governance of the Method?

6.9.2 Is participation in operation of the Method dependent on identification using traditional legal credentials, such as a birth certificate, driver's license, or passport?

6.9.3 Are activities on the registry traceable to real world individuals?

6.9.4 Can DIDs be disabled or revoked by an administrator?

6.9.5 Can DID Documents be edited or removed by an administrator?

6.10 UNCATEGORIZED (ANSWER EACH WITH A YES OR NO)

6.10.1 Is the Method name definitive? (there are no known alternative forks or namespace collisions)

6.10.2 Is the Method resilient against registry forks?

6.11 PARTIAL CRITERIA FROM DANIEL HARDMAN

6.11.1 Permissioned: governed/operation vs. use/creation

6.11.2 Open source: multiple independent implementations

6.11.3 Open standard

6.11.4 Does the individual create and control?

6.11.5 Can the individual choose how keys are managed?

6.11.6 Does the issuer/controller have a fiduciary responsibility to DID Controller?

6.11.7 Does it support social recovery?

6.11.8 What does a single DID cost? TCO

6.11.9 Is resolution observable?

6.11.10 Are stealth DIDs supported?

6.11.11 Is deactivation publicly documented?

6.11.12 After control is lost can other people deactivate?

6.11.13 Possible confusion between implementations and DID Methods

6.11.14 Does it support HD Keys?

6.11.15 Are transactions publicly cryptographically verifiable?

6.11.16 Are DIDs permanent (unremovable--still able to be deactivated but all traces can never vanish)?

6.11.17 Can you get the latest version and older versions? Provable order of versions?

6.11.18 Is the Method published?

6.11.19 Is that Method independently implementable?

6.11.20 did:web and the .onion TLD (truly decentralized) RFC 6761 and 7686

6.11.21 Is there a centralized database?

6.11.22 Is its blockchain byzantine fault tolerant?

6.11.23 Does a single party control a majority of the source of truth? (Under what conditions can the DID controller lose capability?)

6.11.24 If you give control away, can you get it back?

Additional Credits:

Lead Author: Joe Andrieu joe@legreq.com

Authors: Shannon Appelcline shannon.appelcine@gmail.com, Amy Guy amy@rhiaro.co.uk, Joachim Lohkamp joachim@jolocom.com, Drummond Reed drummond.reed@evernym.com, Markus Sabadello markus@danubetech.com, and Oliver Terbu oliver.terbu@consensys.net.

Many thanks to contributions from Kai Wagner.

Sample APA Citation:

Andrieu, J., Appelcline, S., Guy, A., Lohkamp, J., Reed, D., Sabadello, M, and Terbu, O. (2020). A Rubric for Decentralization of DID Methods. *Rebooting the Web of Trust IX*. Retrieved from https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/final-documents/decentralization-rubric.pdf.

About Rebooting the Web of Trust

This paper was produced as part of the Rebooting the Web of Trust IX design workshop. On September 3rd to 6th, 2019, over 60 tech visionaries came together in Prague, The Czech Republic to talk about the future of decentralized trust on the internet with the goal of writing at least 5 white papers and specs. This is one of them.

RWOT Board of Directors: Christopher Allen, Joe Andrieu, Kim Hamilton Duffy

Members of the Organizing Committee: Dan Burnett, Dmitri Zagidulin

Sponsors: Digital Contract Design (Gold), Protocol Labs (Silver), Digital Bazaar (Ongoing Sustaining), Jolocom

Community Sponsors: Blockchain Commons, Consensys, Learning Machine, Legendary Requirements

Workshop Credits: Christopher Allen (Founder, Co-Producer), Joe Andrieu (Co-Producer and Facilitator), and Shannon Appelcline (Editor-in-chief).

Thanks to our other contributors and sponsors!

Thanks also to Paralelní Polis and the Institute for CryptoAnarchy in Prague.

What’s Next?

The design workshop and this paper are just starting points for Rebooting the Web of Trust. If you have any comments, thoughts, or expansions on this paper, please post them to our GitHub issues page:

https://github.com/WebOfTrustInfo/rwot9/issues

The next Rebooting the Web of Trust design workshop is scheduled for 2021. If you'd like to be involved or would like to help sponsor the event, please join our email list for announcements at:

http://eepurl.com/geACd1
