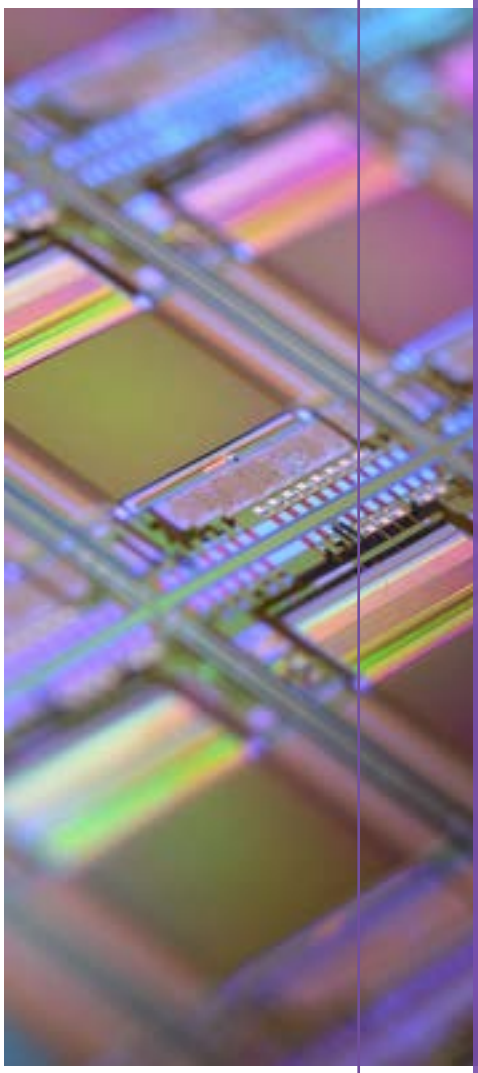


A DID Method Rubric Evaluation of did:ion

March 2022

This evaluation is based on the DID Method Rubric, published by the World Wide Web Consortium
https://w3.org/TR/did-rubric

A DID Method Rubric Evaluation of did:ion

This evaluation was compiled in support of the Department of Homeland Security's 2021 and 2022 Silicon Valley Innovation Program.

Prepared by Legendary Requirements
http://legreq.com

EVALUATORS

Joe Andrieu joe@legreq.com
Eric Schuh eric@legreq.com

CONTRIBUTORS:

Kyle Denhartog kyle.denhartog@mattr.global

EVALUATION DATE

2022-03-01

Available at https://didevaluations.com/ion/2022-03-01

FUNDED BY

MATTR https://mattr.global/ (supported in part by DHS SVIP contract 70RSAT21T00000030)

COPYRIGHT

Use Cases Referenced

LABEL	NAME	DESCRIPTION
use-case-1	**Long term verifiable credentials**	The use of DIDs as subject identifiers for long term (life-long) verifiable credentials such as a digital Permanent Resident Card from the United States Citizens and Immigration Service.
use-case-2	**Bootstrapping secure messaging**	Using DIDs to establish multi-party peer-to-peer secure channels. The channel itself provides a secure binding between the DID and the content passed through the messaging.
use-case-3	**Supply Chain**	DIDs for large-scale deployments of internet-tracked components traveling through the supply chain. As components travel through physical distribution, title is explicitly transferred via updates to the cryptographic material that controls the DID. Each component gets its own unique DID and the ownership of that component is tracked through the control of the DID. The current owner can always pass the ownership to a new owner, and demonstrate they are the current owner.

Methods Evaluated

	SPECIFICATION	NETWORK	REGISTRY
did:ion	did:ion is a bitcoin profile of the Sidetree protocol https://identity.foundation/sidetree/spec/. It uses bitcoin as the temporal anchor and IPFS for storing transactions bundles.		
	https://github.com/decentralized-identity/ion	Bitcoin and IPFS	Bitcoin and IPFS

Contents

1

Rule making

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

In this section

1.1 Open contribution (participation)

https://www.w3.org/TR/did-rubric#criteria-1

QUESTION

How open is participation in governance decisions?

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.

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.

ASSESSMENT

	Method	Spec.	Net.	Reg.	Notes
a-1	did:ion	A-	B	B	**Spec** (A-): Large organizations pay a larger fee, while individuals participate for free. This affects both influence and accessibility. **Net** (B) and **Reg** (B): Bitcoin is mostly open, but core devs hold elevated power. IPFS is open source, run on github, but primarily funded, resourced, and managed by Protocol Labs.

1.2 Transparency

https://www.w3.org/TR/did-rubric#criteria-2

QUESTION

How visible are rulemaking processes?

POSSIBLE RESPONSES

- **A** Agendas and participation details for all governance discussions are publicly announced, any 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.

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.

ASSESSMENT

	Method	Spec.	Net.	Reg.	Notes
a-2	did:ion	A	A-/A	A-/A	**Spec** (A): method spec maintained by DIF, using open and transparent processes. **Net** (A-/A) and **Reg** (A-/A): It can be hard to track conversations about Bitcoin Improvement Proposals (BIPs) and decision processes differ for different BIPs, which can affect visibility (A-). IPFS has great support for realtime zoom participation and notes.(A)

1.3 Separation of Power

http://didcriteria.com/criteria/1

QUESTION

What decision making bodies are involved in rulemaking?

POSSIBLE RESPONSES

List all of the deliberating bodies involved in setting or maintaining the method specification. Then, for each decision making body, evaluate criteria 1.4, 1.5, 1.6, and 4.2.

RELEVANCE

Rulemaking rarely occurs in simple structures. Identifying the different organizational entities that participate in setting rules allows evaluators to understand how rules get made. Understanding how rules get helps predict possible future developments.

It is worth noting that all entities who are beholden to sovereign states, which is pretty much all corporations, non-profits, and individuals, have consequences for violating the laws, regulations, and lawful court orders within their jurisdiction. Some decentralized systems go to great lengths to minimize the impact of possible coercion, including actions by nation states. It is understood that any participant in the process may be subject to the rule of law from any number of jurisdictions, e.g., patent law, employment law, financial reporting laws, dumping laws, zoning, environmental regulations, etc. As a result, all decision making bodies are subject to the jurisdictions in which they operate.

This complexity is true for all DID methods and, to our knowledge, most, if not all, DID methods have no intrinsic relationship to any particular jurisdiction. As such, we do not recommend including jurisdictional players, e.g., nation-states, cities, provinces, etc., as distinct operational layers, unless those players have a distinct role to play for that particular DID method.

ASSESSMENT

	Method	Decision Making Body	Notes
a-3	did:ion	Sidetree working group	The Sidetree working group at DIF is focused on the development and maintenance of the formal Sidetree specification, and a hub of coordination for Sidetree-based DID method node operators. This group also generates libraries, tooling, and documentation to aid Sidetree-based DID method node operators. https://identity.foundation/working-groups/sidetree.html
a-4	did:ion	DIF	DIF is an engineering-driven organization focused on developing the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interop between all participants. https://identity.foundation/
a-5	did:ion	Bitcoin community	Bitcoin advances through Bitcoin Improvement Proposals submitted to the bitcoin/bips repo using the process described at https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki These proposals are discussed by the community and curated by two editors.A Proposed BIP may progress to Final only when specific criteria reflecting real-world adoption has occurred. This is different for each BIP depending on the nature of its proposed changes.
a-6	did:ion	IPFS community	A peer-to-peer hypermedia protocol designed to preserve and grow humanity's knowledge by making the web upgradeable, resilient, and more open. https://ipfs.io/

SOURCE

New synthesis, in part from DID method Rubric v1.0.0 (draft)
https://www.w3.org/TR/did-rubric#criteria-5

1.4 Decision Making Structures

http://didcriteria.com/criteria/2

QUESTION

How is each decision making body structured?

Evaluate this criteria for each decision making body from 1.3.

POSSIBLE RESPONSES

Describe the governance structure of each decision making body.

- **A** Individual. Sole proprietorship
- **B** Informal Group. Unincorporated Partnership / Open Community
- **C** For-profit formal organization. For-profit Corporation / LLC / Partnership
- **D** Quasi not-for-profit formal organization
  a. B-Corp https://bcorporation.net/
  b. CIC https://en.wikipedia.org/wiki/Community_interest_company
- **E** Recognized not-for-profit formal organization. Not-for-profit public benefit organization (NGOs, 501c(3/4/6), etc)
  a. NGO
  b. Trade Association
  c. Charity
- **F** Public agency (federal, state, or local)
- **G** Other

RELEVANCE

Different governance structures have different implications for how decisions are made and who wields influence throughout the process.

ASSESSMENT

	Method	Decision Making Body	Governance Structure	Notes
a-7	did:ion	Sidetree working group	E	DIF Working Group. Committee with elected chair(s) and editors, all working group members can vote. (E)
a-8	did:ion	DIF	E	Committee with elected chair. All members of DIF can vote. (E)

a-9	did:ion	Bitcoin community	B	BIPs debated in public; telecon. Forks as “veto” in governance. (B)
a-10	did:ion	IPFS community	B-	Open debate, largely on Github.Primarily led by Protocol Labs (B-)

SOURCE

New synthesis, in part from DID method Rubric v1.0.0 (draft)
https://www.w3.org/TR/did-rubric#criteria-5

1.5 Cost to introduce rule change

http://didcriteria.com/criteria/3

QUESTION

How expensive is it to get a governance decision before each of the deliberating bodies?

Evaluate this criteria for each decision making body from 1.3.

POSSIBLE RESPONSES

- **A** Free to all
- **B** Inexpensive, but accessible
- **C** Modest cost for interested parties
- **D** Expensive and restricted
- **E** Not possible to participate because the rules are immutable

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.

ASSESSMENT

	Method	Deliberating Body	Cost	Notes
a-11	did:ion	Sidetree working group	A	Just raise a github issue (A)
a-12	did:ion	DIF	B	Active members of working groups generally have reasonable access to propose issues for the DIF steering committee. Emails from the public generally get
a-13	did:ion	Bitcoin community	C	Each BIP has its own mailing list and process, and anyone can propose a BIP. However, getting traction with other collaborators requires investment in networking, socializing, cajoling, etc. Processes are driven by developer-friendly mechanisms, such as github.com, which may be less than accessible to non-technical contributors.(C)

a-14	did:ion	IPFS community	C	IPFS innovations are proposed and tracked on github, and open to the public. However, getting buy-in and engagement requires time and effort. Processes are driven by developer-friendly mechanisms, such as github.com, which may be less than accessible to non-technical contributors. (C)

SOURCE

New synthesis, in part from DID method Rubric v1.0.0 (draft)
https://www.w3.org/TR/did-rubric#criteria-5

1.6 Cost to decide on rule changes

http://didcriteria.com/criteria/4

QUESTION

How expensive is it to participate as a peer in a governance decision by the governing body?

Evaluate this criteria for each decision making body from 1.3.

POSSIBLE RESPONSES

- **A** Free to all
- **B** Inexpensive, but accessible
- **C** Modest cost for interested parties
- **D** Expensive and restricted
- **E** Not possible to participate because the rules are immutable

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.

ASSESSMENT

	Method	Deliberating Body	Cost	Notes
a-15	did:ion	Sidetree working group	A-	Participation in the group is free and available to all. Getting the group to respond to your concerns takes developing rapport and credibility. (A-)
a-16	did:ion	DIF	C	Steering committee members are elected by membership; getting elected requires a reasonable investment in contributing to the work and developing respect in the community. (C)
a-17	did:ion	Bitcoin community	D	Although it is possible to establish oneself in the community of bitcoin developers, it requires a significant investment and “earning your way in the to club”. In addition, the governance process itself requires buy-in from multiple stakeholders such as core devs, miners, and users. However, it is not formally restricted. (D)

a-18	did:ion	IPFS community	D	Although it is possible to contribute and participate in high level decisions, all of which are widely distributed on Github, it appears that the core decisions are driven by employees of Protocol Labs. Employees of protocol labs find it less expensive, in terms of time and effort, to establish themselves as peers in the governance discussion, making decision making partially restricted in practice. (D)

SOURCE

New synthesis, in part from DID method Rubric v1.0.0 (draft)
https://www.w3.org/TR/did-rubric#criteria-5

2

Design

In this section

2.1 Cryptocurrency

http://didcriteria.com/criteria/5

QUESTION

What cryptocurrency, if any, is required for method operations?

POSSIBLE RESPONSES

- **A** None
- **B** At least one. [List the required crypto-currencies in the notes.]

RELEVANCE

The use of particular cryptocurrencies create a long term dependency on the viability of those currencies. Such dependency may be a deterrent for some applications. Similarly, if no cryptocurrency is used, there is likely a dependency elsewhere, such as on the organization managing consensus rules and operation.

ASSESSMENT

	Method	Spec.	Notes
a-19	did:ion	B	**Spec** (B): One must use bitcoin. BTC is required for anchoring transactions. The IPFS layer does not require cryptocurrency, but the bitcoin layer is required for all operations.

2.2 Permissioned Operation

http://didcriteria.com/criteria/6

QUESTION

Does one need permission to use the DID method?

POSSIBLE 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.

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.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-20	did:ion	A	A	**Net** (A) and **Reg** (A) Anyone can use did:ion; neither bitcoin nor IPFS are permissioned, anyone can stand up a node and participate fully.

SOURCE

Iterated from DID method Rubric v1.0.0 (draft)
https://www.w3.org/TR/did-rubric#criteria-6.

2.3 Interoperability

https://www.w3.org/TR/did-rubric#criteria-7

QUESTION

Does the DID method restrict access or functionality to particular client software implementations?

POSSIBLE 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.

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.

ASSESSMENT

	Method	Spec.	Net.	Reg.	Notes
a-21	did:ion	A	A	A	**Spec** (A), **Net** (A) and **Reg** (A): Anyone can use did:ion; neither bitcoin nor IPFS are permissioned, anyone can stand up a node and participate fully.

2.4 Scope of Usage

https://www.w3.org/TR/did-rubric#criteria-8

QUESTION

How widely can DIDs of this method be used?

POSSIBLE 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.

RELEVANCE

Different methods enable different scopes in which a DID might be considered usable or valid. Some DIDs are only resolvable within a limited context, others are suitable for global use. 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.

EVALUATION

	Method	Net.	Reg.	Notes
a-22	did:ion	A	A	A did:ion DID can be resolved by any observer.

2.5 Offline creation

http://didcriteria.com/criteria/7

QUESTION

Does the method require network communications to create a DID?

POSSIBLE RESPONSES

- **A** No. Creation is expected to be off-line. Only resolution, updates and deactivations require network or registry interaction.
- **B** Yes. Creation requires network coordination with a single party to complete the DID creation.
- **C** Yes. Creation requires network coordination with multiple parties in a known, constrained group to complete the DID creation.
- **D** Yes. Creation requires network coordination with and acceptance by an open, global consensus system to complete DID creation.

RELEVANCE

Communication is costly, with increasing costs the more parties are involved. This cost is not just in terms of the connection expense, but also the latency in processing transactions. The ability to create a DID without registering it on a global shared state greatly reduces the technical and financial cost of the method.

ASSESSMENT

	Method	Spec.	Notes
a-23	did:ion	A	All new did:ions start offline. Only updates need to be published.

2.6 Update Scalability

http://didcriteria.com/criteria/8

QUESTION

Assuming an average of no more than 1 update per quarter, how many DIDs can this method support?

POSSIBLE RESPONSES

- **A** Greater than 5 billion
- **B** Greater than 1 billion
- **C** Greater than 500 million
- **D** Greater than 50 million
- **E** Greater than 5 million
- **F** Less than 5 million

RELEVANCE

Some DID methods may be able to support the world's population, others may be more suitable to a particular type of use where only a small number of DIDs need to be supported. This gives a rough idea of the population base you may expect a particular DID method to support.

ASSESSMENT

	Method	Reg.	Notes
a-24	did:ion	A	A single did:ion node, which limits its operations to 10,000 ops per transaction, is capable of anchoring ~131 million DIDs, updated every quarter. However, any number of did:ion nodes can independently anchor different did:ion operations, making the capacity effectively limited only by the blocksize of bitcoin (and the impact from other transactions competing for space in each block).

2.7 Creation Cost

http://didcriteria.com/criteria/9

QUESTION

How much does it cost a DID creator to create a DID?

POSSIBLE RESPONSES

- **A** Only operational costs of running the algorithm (no externalized expense)
- **B** Less than $0.01
- **C** Less than $0.10
- **D** Less than $1
- **E** Less than $10
- **F** $10 or greater

RELEVANCE

Almost all operations are sensitive to the cost of creating the underlying identifiers. If such costs are close to zero, broad use of ephemeral keys is possible. As costs increase, it becomes more and more necessary to limit the number of identifiers created in order to keep systems.

ASSESSMENT

	Method	Reg.	Notes
a-25	did:ion	A	Offline creation has no network costs, just local computation.

2.8 Update & Deletion Cost (out-of-pocket)

http://didcriteria.com/criteria/10

QUESTION

How much does it cost*, out of pocket, to update or deactivate a DID document?

If the method has a tiered or variable cost structure, list all responses that apply and specify the cost structure in the notes. *This is the cost to the DID document controller.

POSSIBLE RESPONSES

- **A** Only operational costs of running the algorithm (no externalized expense)
- **B** Less than $0.01
- **C** Less than $0.10
- **D** Less than $1
- **E** Less than $10
- **F** $10 or greater

RELEVANCE

Depending on the method and governance, the price of updating and deleting a DID document will inform the cost of doing business with the particular method. Depending on the use case in mind this can be used, along with the scalability questions, to estimate the cost of maintaining a network using this DID method.

ASSESSMENT

	Method	Reg.	Notes
a-26	did:ion	B/C	Node operators who have staked ~$100,000 USD in BTC may update 10,000 DIDs in a single bitcoin transaction; at an average transaction fee of $3 (the current annualized average), that is $0.0003 per update. (B) Node operators who have not staked any BTC may update up to 100 DIDs in a single bitcoin transaction; at an average transaction fee of $3 (the current annualized average), that is $0.03 per update. (C) Cost scales deterministically between these two ends of the price spectrum.

2.9 Update & Deletion Cost (in-kind)

http://didcriteria.com/criteria/11

QUESTION

How much does it cost to update or deactivate a DID document using in-kind contributions?

POSSIBLE RESPONSES

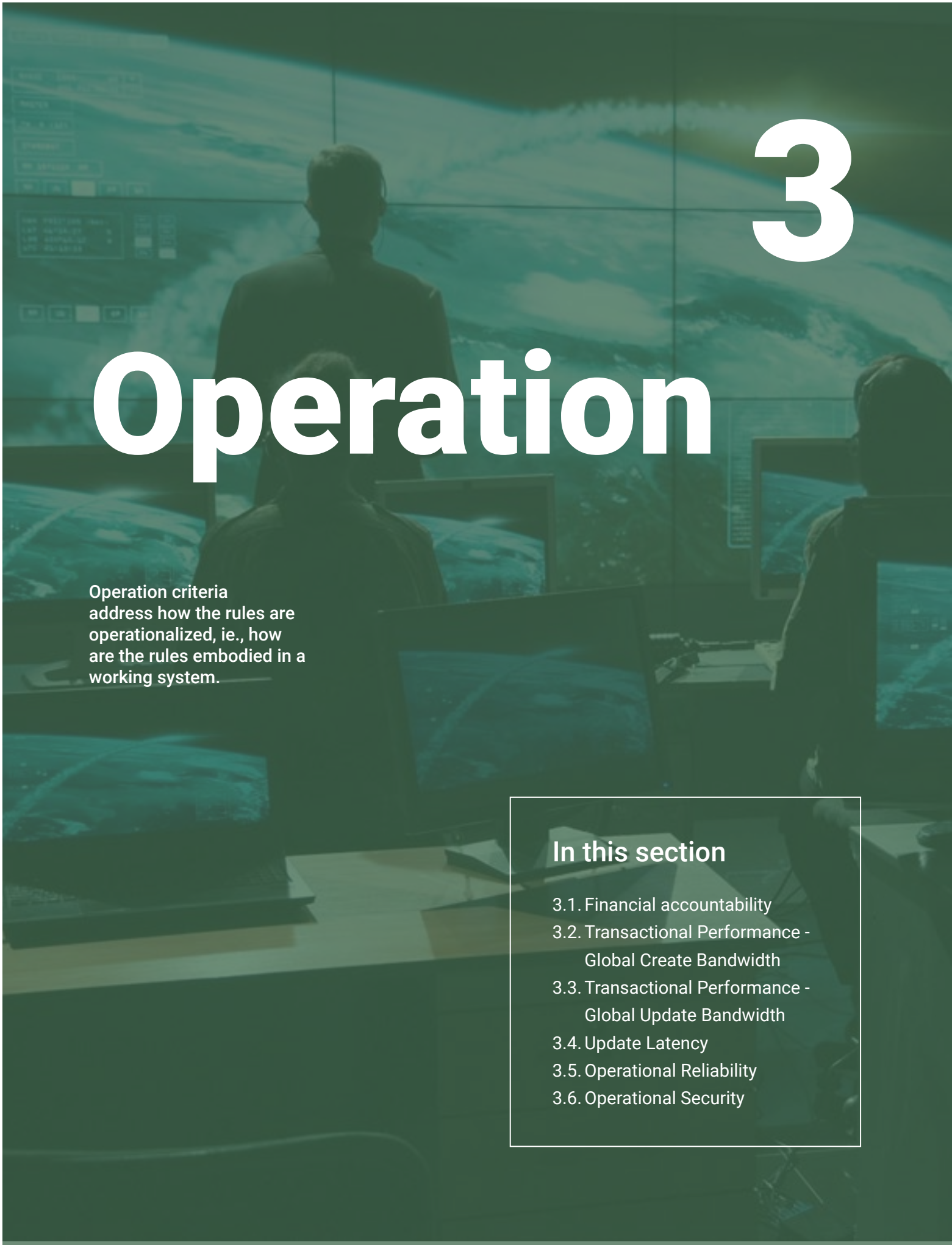
- **A** Only operational costs of running the algorithm (no externalized expense)
- **B** Less than $0.01
- **C** Less than $0.10
- **D** Less than $1
- **E** Less than $10
- **F** $10 or greater

RELEVANCE

Depending on the method and governance, there may be ways of reducing (or removing) the cost of updating or deleting a DID document, such as volunteering with the governance body or doing a set of work the network needs done.

ASSESSMENT

	Method	Reg.	Notes
a-27	did:ion	n/a	The method does not provide for any kind of in-kind contributions. It is worth noting that some node operators are offering free updates to the public based on a modest Proof of Work.



3

Operation

Operation criteria address how the rules are operationalized, ie., how are the rules embodied in a working system.

In this section

3.1 Financial accountability

http://didcriteria.com/criteria/12

QUESTION

How transparent are the economics of the method?

POSSIBLE RESPONSES

- **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.

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.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-28	did:ion	C	C	**Net** (C) and **Reg** (C): Bitcoin transactions are transparent; IPFS transactions are free. Node operator costs are also transparent: the did:ion fee algorithm, as set forth in https://github.com/decentralized-identity/ion/blob/master/docs/design.md, outlines how different operators can stake different amounts of BTC and achieve different cost scales. However, the price charged to end-users, if any, is a private business matter.

SOURCE

Iteration from DID method Rubric v1.0.0 (draft)
https://www.w3.org/TR/did-rubric#criteria-9

3.2 Transactional Performance - Global Create Bandwidth

http://didcriteria.com/criteria/13

QUESTION

How many DIDs of this method can be created per time period, globally?

POSSIBLE RESPONSES

Methods with offline creation should respond “n/a” to this question.

- **A** More than 1,000,000 Transactions Per Second
- **B** 100,001 - 1,000,000 TPS
- **C** 10,001 - 100,000 TPS
- **D** 1,001 - 10,000 TPS
- **E** 101 - 1,000 TPS
- **F** 11 - 100 TPS
- **G** 1-10 TPS
- **H** Less than 1 TPS

RELEVANCE

The number of new DIDs that can be created in a second inform the scalability of the network in regards to onboarding new users and allowing for new uses by existing users.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-29	did:ion	n/a	n/a	**Net** (n/a) and **Reg** (n/a): Creation is offline, so there is effectively no limit.

3.3 Transactional Performance - Global Update Bandwidth

http://didcriteria.com/criteria/14

QUESTION

How many DIDs can be updated per second, globally?

POSSIBLE RESPONSES

- **A** More than 1,000,000 Transactions Per Second
- **B** 10,001 - 1,000,000 TPS
- **C** 101 - 10,000 TPS
- **D** 11 - 100 TPS
- **E** 1-10 TPS
- **F** Less than 1 TPS

RELEVANCE

Along with creation, update performance of the registry can inform as to how many users make use of the method at any given time.

ASSESSMENT

	Method	Reg.	Notes
a-30	did:ion	B	Assuming 500 bytes per BTC tx, 1 MB block size, and 1 block per 10 minutes, if ALL transactions in a BTC block contain updates, there could be as many as 35,000 updates per second with did:ion.

3.4 Update Latency

http://didcriteria.com/criteria/15

QUESTION

How much time does it take for an update to become globally available after submission by the DID controller?

POSSIBLE RESPONSES

- **A** Less than 1 second
- **B** 1 to < 60 seconds
- **C** 1 to < 10 min
- **D** 10 min to < 1 hour
- **E** 1 hour to < 1 day
- **F** 1 day to 2 weeks
- **G** Greater than two weeks
- **H** Updates not guaranteed

RELEVANCE

Different registry mechanisms have different guarantees for some notion of finality. The longer one has to wait for confirmation, the greater the latency for high security transactions. The shorter the duration, the more one has to critically validate the race conditions that may be present in determining finality. Depending on the algorithm, there are likely trade-offs between the stability of consensus and the speed at which consensus is pursued.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-31	did:ion	D/H	D/H	**Net** and **Reg**:Updates to did:ion DIDs are ultimately anchored on BTC, which averages one block per every ten minutes. Some nodes may batch the BTC anchor operation, which could add to the delay, but this is not a requirement of the method. (D and D) Similarly, due to the dynamically adjusting market for bitcoin transactions, it is possible for a controller to submit a transaction to the ION node and for it to go un-anchored because the ION node is not configured with a competitively priced bitcoin transaction fee. (H and H).

3.5 Operational Reliability

http://didcriteria.com/criteria/16

QUESTION

For each layer, how many operational components may be offline without that layer losing availability?

Evaluate with layers from 4.5 Operational Layers.

POSSIBLE RESPONSES

Fill in yourself.

Options might be:
- Equation based on the consensus algorithm
- Known number
- Percentage
- NONE (specific components MUST be operational)
- OPTIONAL (operations do not depend on the layer being available)

RELEVANCE

Along with the type of consensus algorithm the number of offline nodes has both security--i.e. DDOS attacks--and reliability implications.

ASSESSMENT

	Method	Layer	Response	Notes
a-32	did:ion	Bitcoin nodes	All but one (as long as the one can reach the rest of the network.)	As long as you can reach at least one bitcoin node, you can process transactions. However, subnetworks operating in isolation may lead to reorganization when reconnected to the global network. For the individual party using bitcoin, as long as they can reach one directly (and presumably that node can reach others), then bitcoin's gossip protocol will work.

a-33	did:ion	Bitcoin miners	All but one (but txs will be slow)	Bitcoin miners solve cryptographic puzzles to produce blocks. As long as at least one miner is solving those puzzles, new blocks will be created and the network will process transactions. However, the difficulty of those puzzles is dynamically adjusted every 2016 blocks (approx every 2 weeks). In a period when hashpower drops suddenly (because a substantial group of miners have gone offline for any reason), then bitcoin will process fewer blocks until either the miners return or the next difficulty adjustment.
a-34	did:ion	IPFS nodes	All but one (as long as that one has the file you need)	IPFS does not guarantee the storage of files in the network, so it's possible that the ION transaction bundle that MUST be retrieved is not actually hosted by anyone on the network. However, it only takes one party to sustain the existence, with other nodes propagating the file based on access. In the case of did:ion, we anticipate several parties willing to host the modest amount of transaction data needed to keep the method functional. In the absolute worst case, the single individual who needs their did:ion DIDs to resolve can host their own IPFS node.
a-35	did:ion	ION Nodes	All but one (including your own)	As long as bitcoin and IPFS are operational, then any single ION node is sufficient for publishing to or reading from the network.
a-36	did:ion	did:ion Resolver	All but one (including your own)	As long as bitcoin and IPFS are operational, then any resolver can read from the network and verify the current DID document for any given did:ion DID.
a-37	did:ion	Resolution Client	All but one (the client you are using)	The Resolution Client must have access to a did:ion Resolver and thus must be online to properly resolve a did:ion.

3.6 Operational Security

http://didcriteria.com/criteria/17

QUESTION

How many operational components may be compromised without compromising the network?

Evaluate using the layers defined in 4.5 Operational Layers.

POSSIBLE RESPONSES

Fill in yourself. Options might be:

- Equation based on the consensus algorithm
- Known number
- Percentage
- Unknown
- N/A -- If the algorithm isn't dependent on the particular layer

RELEVANCE

Informs how easy it may be to orchestrate a take over of the network and get false transactions accepted by the consensus mechanism.

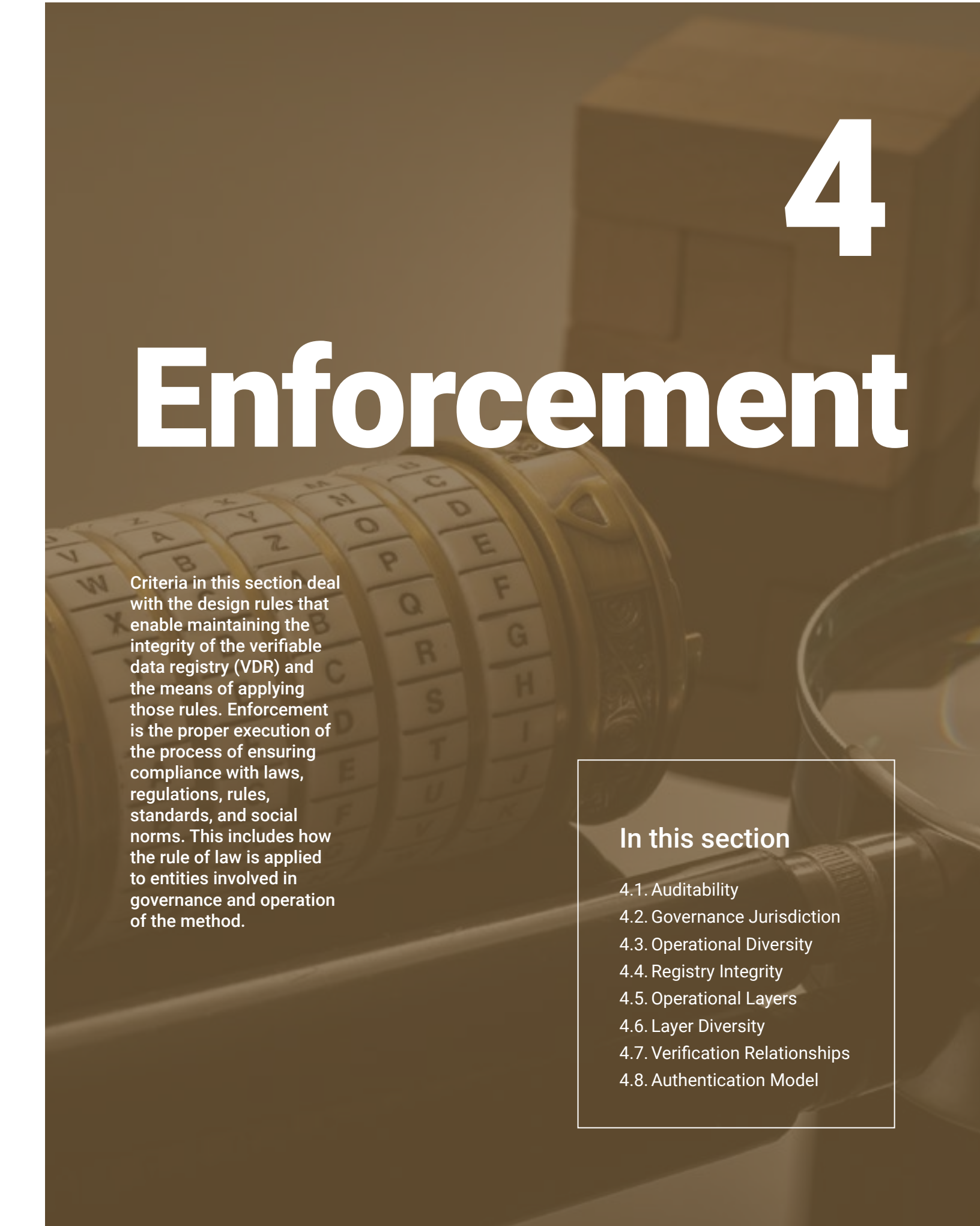
ASSESSMENT

	Method	Layer	Response	Notes
a-38	did:ion	Bitcoin nodes	All but one (the one that can propagate your transaction to a winning miner)	If the bitcoin node a transaction is posted to is compromised the node can choose not to post the requested transaction to other nodes, effectively denying access to the gossip network. However, any transaction can be posted to any number of peers. No single node has a privileged position in this manner, so you just need to find one node that will propagate the transaction to an (eventually successful) miner. In practice, gossip flows freely without much impedance. It is important to note that this form of compromise can only prevent transactions, it cannot enable fraudulent ones.

a-39	did:ion	Bitcoin miners	49% of expected hash power	Bitcoin mining works as long as the longest chain is legitimately the hardest one to compute. As long as there is enough hash power engaged in mining to prevent what is known as a “51%” attack, then the network can be considered secure. It’s worth noting that the amount of hash power is dynamic, mostly going up, but occasionally going down. As long as there is not a pool of hashpower that is suddenly offline, the active hashpower can defend against consensus attacks.
a-40	did:ion	IPFS nodes	n/a	The nodes themselves do not secure the authenticity of content. If you can get ahold of the file, you can verify it is correct, WITHOUT any further interaction with IPFS. In fact, it’s fully possible to be essentially offline from IPFS and verify whether or not you have the tx bundles needed to resolve a given did:ion DID. So as long as the file is available, it’s content cannot be compromised (assuming the validity of the content-based hash algorithm, which is core to IPFS in any case).
a-41	did:ion	ION Nodes	All but one (the one that can propagate your updates)	Each ION node has the same security profile as its two components: a bitcoin node and an IPFS node. As long as bitcoin and IPFS are uncompromised, the ION node is secure. Note, however, that once you rely on a particular ION node rather than running your own, you are trusting that node to act appropriately.
a-42	did:ion	did:ion Resolver	All but one (the one you trust to verify bitcoin and IPFS state)	Each did:ion resolver has the same security profile as its two components: a bitcoin node and an IPFS node. As long as bitcoin and IPFS are uncompromised, the did:ion resolver is secure. Note, however, that once you rely on a particular did:ion resolver rather than running your own, you are trusting that node to act appropriately.
a-43	did:ion	Resolution Client	All but one (the one you trust to operate correctly)	Whatever client you use must be trusted to operate correctly.

4

Enforcement



Criteria in this section deal with the design rules that enable maintaining the integrity of the verifiable data registry (VDR) and the means of applying those rules. Enforcement is the proper execution of the process of ensuring compliance with laws, regulations, rules, standards, and social norms. This includes how the rule of law is applied to entities involved in governance and operation of the method.

In this section

4.1 Auditability

https://www.w3.org/TR/did-rubric#criteria-12

QUESTION

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

POSSIBLE 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

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.

ASSESSMENT

	Method	Reg.	Notes
a-44	did:ion	A	Both BTC and IPFS resources are publicly readable.

4.2 Governance Jurisdiction

http://didcriteria.com/criteria/18

QUESTION

In which jurisdiction is the governing body located?

Evaluate this criteria for each decision making body from 1.3.

POSSIBLE RESPONSES

Free text. The evaluator should provide the most relevant description of jurisdiction.

RELEVANCE

Different jurisdictions have different laws which may affect the operation of the method.

ASSESSMENT

	Method	Decision Making Body	Notes
a-45	did:ion	Sidetree working group	The sidetree working group is run by the Decentralized Identity Foundation.
a-46	did:ion	DIF	DIF is a project of the Joint Development Foundation Projects, LLC, a Washington state non-profit.
a-47	did:ion	Bitcoin community	Bitcoin governance is a hodge-podge of semi-public discussion in various forums and ultimately decided through adoption of proposals by implementers and operators.
a-48	did:ion	IPFS community	IPFS is a project of Protocol Labs, a Delaware corporation.

4.3 Operational Diversity

http://didcriteria.com/criteria/19

QUESTION

How many independent legal entities currently maintain the operational integrity of the Verifiable Data Registry?

POSSIBLE RESPONSES

- **A** Open ended, unknown, or unknowable.
- **B** Capped. [State lower and upper bounds in Notes.]
- **C** One
- **D** Zero

RELEVANCE

Singular—or small numbers of—entities controlling the consensus of a network can orchestrate malicious attacks.

ASSESSMENT

	Method	Reg	Notes
a-49	did:ion	A	Bitcoin and IPFS allow any number of legal entities to participate in consensus.

4.4 Registry Integrity

http://didcriteria.com/criteria/20

QUESTION

What type of integrity mechanism is used by the method's Verifiable Data Registry?

POSSIBLE RESPONSES

- **A** Proof of Work
- **B** Proof of Stake
- **C** Byzantine Fault Tolerant algorithm based
- **D** Electoral — Select parties vote with thresholds
- **E** Unanimous — All parties countersign
- **F** Unilateral — Latest signed version defined as authentic
- **G** Standards-based specifications determined by institutional authority, used by anyone
- **H** Other - Add your own

Note: For registries which use a hybrid of any of the above approaches, select the one that is the closest fit then either denote via slash—e.g. C/A for a hybrid Byzantine Fault Tolerant algorithm that utilizes POW at some layer—and describe in the notes at a high level how the consensus algorithm functions.

RELEVANCE

The consensus mechanism used by the method registry has implications for scalability, speed of operations, security and possibly environmental impact.

ASSESSMENT

	Method	Reg.	Notes
a-50	did:ion	A	The VDR for did:ion is Bitcoin, which is Proof of Work

4.5 Operational Layers

http://didcriteria.com/criteria/21

QUESTION

What layers of operational components establish and maintain integrity of the Verifiable Data Registry?

For each layer, evaluate criteria 3.5, 3.6, and 4.6.

POSSIBLE RESPONSES

A List each layer

RELEVANCE

The manner in which a Verifiable Data Registry (VDR) manages integrity defines how that integrity might be compromised. To understand how the VDR of a given method maintains integrity, this criteria identifies the operational components of the VDR for further evaluation in other criteria, namely 3.5, 3.6, and 4.6.

Unfortunately, network topology inevitably introduces parties that may be able to disrupt or compromise network interactions. For example, DNS servers--often under the control of the user's ISP or the corporate IT department--can return "fake" IP addresses; corporate firewalls can prevent traffic to or from certain addresses; corporate system administrators may prevent users from configuring alternative Certificate Authorities, even international internet traffic can be restricted or denied, purely at the network layer.

Because nearly every DID method known at this point depends on Internet-based networking, every DID method faces these same problems. As such, we don't recommend specifying common network components as distinct layers unless those layers have specific roles unique to the particular DID method.

For this criteria, we are talking about the operational components that have specific, unique, or privileged roles with regard to the evaluated DID method(s). The parties which fulfill said roles should be considered when evaluating the fitness of the given method(s).

ASSESSMENT

	Method	Layer	Notes
a-51	did:ion	Bitcoin nodes	Full nodes keep up-to-date chain state and propagate gossip to other nodes. A lightweight or partial node does not maintain the entire state, but may participate in gossip. For this analysis, we consider all nodes that propagate gossip.
a-52	did:ion	Bitcoin miners	Bitcoin miners compete to solve cryptographic puzzles in exchange for earning mining rewards. As long as “51%” of the mining power is honest, the network is secure. Mining power is typically measured in hash rate or the number of cryptographic hash calculations per second.
a-53	did:ion	IPFS nodes	Participants in the IPFS network are called nodes. Nodes are the most crucial aspect of IPFS - without nodes running the IPFS daemon, there would be no IPFS Network. Protocol Labs manages two primary implementations of the IPFS spec: Go-IPFS and JS-IPFS. Go-IPFS is meant for server-side operation while JS-IPFS runs in the browser. There are different types of IPFS nodes. Depending on the use-case, a single IPFS node can serve one of many functions: Preload, Relay, Bootstrap, Delegate routing For this evaluation, we consider all IPFS nodes as a singular operational unit for interacting with the IPFS network.
a-54	did:ion	ION Nodes	Full ION Nodes run both an IPFS and Bitcoin node and provide full read and write capability for the registry. It prepares IPFS transaction bundles and posts them to IPFS, then packages those updates into BTC transactions for submission to the BTC mempool (and eventual inclusion in a BTC block).
a-55	did:ion	did:ion Resolver	did:ion Resolvers connect to bitcoin and IPFS networks, but may not be running a full node of either, although all implementations are expected to be able to verify all did:ion containing BTC blocks as well as all IPFS bundles referenced therein. They provide read-only access to the Verifiable Data Registry, interpreting BTC transactions and IPFS bundles to return the current, canonical DID document.
a-56	did:ion	Resolution Client	Any application that requests did:ion resolution from a resolver.

4.6 Layer Diversity

http://didcriteria.com/criteria/22

QUESTION

How many operational components need to be compromised to compromise the verifiable data registry?

Evaluate with layers from 4.5 Operational Layers.

POSSIBLE RESPONSES

- **A** Open ended, unknown, or unknowable.
- **B** Capped. [State number in Notes]
- **C** One

RELEVANCE

Depending on the type of integrity mechanism, the number of nodes that may fail without compromising the registries integrity has implications for security and reliability.

ASSESSMENT

	Method	Layer	Response	Notes
a-57	did:ion	Bitcoin nodes	A	The only effective way bitcoin nodes could compromise the verifiable data registry is to deny the update operations for a given DID. For this to be a certain compromise of the network ALL bitcoin nodes would need to be compromised to ensure no node chooses to propagate a given update.

a-58	did:ion	Bitcoin miners	A	Bitcoin mining works as long as the longest chain is legitimately the hardest one to compute. As long as there is enough hash power engaged in mining to prevent what is known as a “51%” attack, then the network can be considered secure. It’s worth noting that the amount of hash power is dynamic, mostly going up, but occasionally going down. As long as there is not a pool of hashpower that is suddenly offline, the active hashpower can defend against consensus attacks. Note that the only effect of compromising bitcoin would be the potential removal of did:ion DID operations. In this manner, an attacker could deny access to updates to DID documents, but given the offline creation capability of did:ion, the DID itself would still appear as valid as it was when initially created. Unless the private keys are compromised, the most an attacker can do is deny updates to the DID document. In some cases, this should be considered a compromise. However, such an attack would NOT allow the false presentation of a supposedly authentic DID document for a given DID.
a-59	did:ion	IPFS nodes	A	The only effective way IPFS nodes could compromise the verifiable data registry is to deny the update operations for a given DID. For this to be a certain compromise of the network ALL IPFS nodes would need to be compromised to ensure no node chooses to propagate a given update. Unless the private keys are compromised, the most an attacker can do is deny updates to the DID document through some denial of service scheme. In some cases, this should be considered a compromise. However, such an attack would NOT allow the false presentation of a supposedly authentic DID document for a given DID.
a-60	did:ion	ION Nodes	A	The only effective way ION nodes could compromise the verifiable data registry is to deny the update operations for a given DID. For this to be a certain compromise of the network ALL ION nodes would need to be compromised to ensure no node chooses to propagate a given update.
a-61	did:ion	did:ion Resolver	C	If the did:ion Resolver you are using chooses to lie to you, you will receive an apparently compromised verifiable data registry. The registry itself, if you used a resolver that was operating truthfully, would not be affected.
a-62	did:ion	Resolution Client	C	If the Resolver Client you are using chooses to lie to you, you will receive an apparently compromised verifiable data registry. The registry itself, if you used a resolver that was operating truthfully, would not be affected.

4.7 Verification Relationships

http://didcriteria.com/criteria/23

QUESTION

What verification relationships are supported by the method per specification?

POSSIBLE RESPONSES

Select all that are supported.

- **A** None
- **B** Authentication
- **C** AssertionMethod
- **D** Key Agreement
- **E** CapabilityInvocation
- **F** CapabilityDelegation
- **G** Other
- **H** Any

RELEVANCE

The verification relationships a method supports inform the ways in which DIDs of the method can be used. See section 5.3 of the Decentralized Identifiers specification for details on verification relationships.
https://www.w3.org/TR/did-core/#verification-relationships

ASSESSMENT

	Method	Spec.	Notes
a-63	did:ion	B,C,D,E,F	The did:ion specification only enumerates the Verification Relationships as they appear at the time of this assessment in the did-core specification.

4.8 Authentication Model

http://didcriteria.com/criteria/24

QUESTION

How does the method authenticate a given DID operation as coming from the legitimate DID controller?

POSSIBLE RESPONSES

Include as many as apply to this method.

- **A** None
- **B** Cryptographically signed transactions
- **C** Cryptographic challenge string & signed response
- **D** Authenticator App
- **E** Biometrics
- **F** Email
- **G** DNS Record
- **H** HTML over HTTP
- **I** SMS/MMS
- **J** DID document update
- **K** Other
- **L** Any

RELEVANCE

The way in which DID updates are authenticated can have implications on not only the trustworthiness of the method but also informs someone who wants to use the method what they may need to implement technologically to properly make use of the method.

ASSESSMENT

	Method	Spec.	Notes
a-64	did:ion	B	ION uses JWK and JWS to ensure that DID operations are properly authorized.

5

Adoption (and diversity)

Adoption criteria address how widely the method and its implementations are used by various parties and systems.

In this section

5.1 Financial Entanglements

http://didcriteria.com/criteria/25

QUESTION

How was the method funded?

POSSIBLE RESPONSES

- **A** State-sponsored funding
- **B** Regulated not-for-profit entity
- **C** Private equity
- **D** Operational budget
- **E** Cryptocurrency
- **F** Tokenized Initial Coin Offering
- **G** Initial Public Offering (public equity funding)
- **H** Other -- State what in the notes

RELEVANCE

Funding can create financial entanglements. Those methods that depend on outside financing should be further evaluated to understand the potential consequences of funding to-date.

ASSESSMENT

	Method	Spec.	Net.	Reg.	Notes
a-65	did:ion	D	E/C/D	E/C/D	**Spec** (D): Specification was developed largely by independent firms using operational budgets **Net** and **Reg**: Bitcoin is a self-funding cryptocurrency (E), IPFS was developed by Protocol Labs, using some combination of private equity and operating budget (C/D).

5.2 Organizational Maturity in Time

http://didcriteria.com/criteria/26

QUESTION

How long has the organization(s) behind the method been operational?

POSSIBLE RESPONSES

- **A** Over 20 years
- **B** Over 10 years
- **C** Over 5 years
- **D** Over 1 year
- **E** Less than 1 year
- **F** There is no organization per se

RELEVANCE

The age of the organization(s) behind a method can be used to give an idea into organizational maturity. It is not a sole indicator and should be taken as a data point in evaluating the method organization's current state.

ASSESSMENT

	Method	Spec.	Net.	Reg.	Notes
a-66	did:ion	A/D	C	C	**Spec**: The major organizations behind the did:ion specification are DIF (D) and Microsoft (A). DIF is also the organization driving the Sidetree specification, which did:ion is based on. **Net** (C) and **Reg** (C): Are based on bitcoin and IPFS Microsoft has existed for more than 20 years. DIF and Protocol Labs (the organization behind IPFS) are younger, but each have existed for at least five years. Bitcoin started in 2009, but really has no formal organization.

5.3 Release Status

http://didcriteria.com/criteria/27

QUESTION

Can the method be used for production today?

POSSIBLE RESPONSES

- **A** A. Yes. A production system is available to the general population.
- **B** B. No. A test network is operational.
- **C** C. No. Only an internal developer network is operational.
- **D** D. No. The software is not yet running on any network.

RELEVANCE

Some errors only become apparent after sufficient time to test edge cases and performance boundaries.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-67	did:ion	A	A	**Net** (A) and **Reg** (A): All major components are in production and available to the public.

5.4 Maturity

http://didcriteria.com/criteria/28

QUESTION

How long has the underlying network/registry been available to third parties for non-trivial use?

POSSIBLE RESPONSES

- **A** The network/registry has been operationalized for ten years or more.
- **B** The network/registry has been operationalized for five years or more
- **C** The network/registry has been operationalized for one year or more
- **D** The network/registry has been operationalized for less than one year
- **E** The network/registry is not operationalized for non-trivial use

RELEVANCE

Some errors only become apparent after sufficient time to test edge cases and performance boundaries.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-68	did:ion	D/A/B	D/A/B	**Net** and **Reg**: did:ion entered production on Jan 22, 2021 (less than one year at the point of this Evaluation) (D). Bitcoin has been in operation since 2009 (A) and IPFS since 2015 (B).

6

Security

Security criteria address how the method is cryptographically secured.

In this section

6.1 Robust Crypto

https://www.w3.org/TR/did-rubric#criteria-24

QUESTION

What is the lowest security level (“bits of security”) allowed in the processes that ensure integrity of the verifiable data registry?

https://en.wikipedia.org/wiki/Security_level

POSSIBLE RESPONSES

- **A** No combination of required features produces a profile with less than 256 bits of security.
- **B** Less than 128 bits
- **C** Less than 128 bits
- **D** Less than 64 bits

RELEVANCE

A DID method that requires implementations to support something weak (e.g., 1024-bit RSA) is guaranteeing that its users will cooperate by default with encryption that’s relatively easy to crack, with hashing that’s not adequately collision-resistant, etc.

ASSESSMENT

	Method	Reg.	Notes
a-69	did:ion	B-	Secp256k1 theoretically guarantees 128 bit security. However, some theoretical attacks have shown a reduction of approximately 5 bits. (B-)

6.2 Expert Review (cryptography)

https://www.w3.org/TR/did-rubric#criteria-25

QUESTION

Does the system use cryptographic and security primitives that are well vetted by technical experts, and battle hardened in the school of experience?

POSSIBLE RESPONSES

- **A** Experts generally consider the system very secure, and this opinion is reinforced by a track record of secure production use.
- **B** The theoretical security of the system looks excellent, and no known attacks or substantive criticisms are unaddressed. However, limited review or limited experience informs the opinion.
- **C** Credible reports of vulnerabilities or design shortcomings have not been addressed.
- **D** The system actively uses mechanisms that are officially deprecated.
- **E** The system uses mechanisms that have not been vetted.

RELEVANCE

Exotic crypto and other security mechanisms without expert review and a production track record is likely to contain hidden risks.

ASSESSMENT

	Method	Reg.	Notes
a-70	did:ion	A	Bitcoin's security has proven robust. (A)

6.3 Expert Review (consensus)

http://didcriteria.com/criteria/29

QUESTION

If the method makes use of a distributed consensus mechanism, has the registry's consensus mechanism undergone sufficient review?

POSSIBLE RESPONSES

- **A** Yes. A formal proof has been published in a peer reviewed journal.
- **B** Yes. A formal proof has been published.
- **C** No. An informal argument has been published.
- **D** No. The consensus algorithm is opaque to registry users.

RELEVANCE

Decentralized systems are notoriously difficult to get right. Consensus ordering, in particular, is known to be a hard problem solved by distributed ledgers. Even simpler registries may trade off provable finality with probabilistic finality. It is vital that the method used for high-value or life-critical application be rigorously evaluated for potential flaws.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-71	did:ion	A	A	**Net** (A) and **Reg** (A): Bitcoin's proof of work consensus algorithm has been thoroughly reviewed. IPFS uses a Kademlia hash table algorithm, which has also undergone thorough academic review since publication in 2002. However, compromising the hash table would not compromise the content of a DID document; rather it would affect the ability to resolve the DID to that DID document. IPFS's content-hash addressing is based on multihash, and did:ion requires using the SHA-256 variant of multihash. SHA-256 is extremely well reviewed.

6.4 Availability

https://www.w3.org/TR/did-rubric#criteria-28

QUESTION

How robust are protections against attempts to suppress information flow, whether legal (cease and desist) or technical (denial of service)?

POSSIBLE RESPONSES

- **A** The VDR is practically immune from this risk.
- **B** The VDR has reasonable protections in place. However, motivated and well resourced attackers could temporarily disrupt access in a targeted context.
- **C** Attackers could permanently disrupt access in a targeted context.

RELEVANCE

Control over an identifier is far less valuable if the propagation of that control can be limited by someone else.

ASSESSMENT

	Method	Reg.	Notes
a-72	did:ion	A/B	The underlying components of bitcoin and IPFS are practically immune from this risk, in theory (A). However, in practice, there is concern about the number of did:ion nodes independently running and anchoring DID documents. Those nodes could be susceptible to targeted attacks (B). We believe that a growing network will reduce this risk as a more diverse population of nodes would provide greater resilience.

6.5 Provenance

https://www.w3.org/TR/did-rubric#criteria-29

QUESTION

Is the current state of a DID document provably correct from a history that's visible to anyone who can resolve the DID?

POSSIBLE RESPONSES

- **A** The update history of the DID document is recorded, accessible, and linked appropriately to its predecessor. Arbitrary versions can be queried and proved correct, and they have a reasonably useful timestamp.
- **B** The update history of the DID document exists, and a forensic analysis could prove correctness. However, it's not exposed for consumption of ordinary resolvers, it lacks supporting metadata, or it's exposed in a very suboptimal way.
- **C** Limited evidence of proper DID document updates exists.
- **D** No evidence of proper DID document updates exist; the user has to trust the system's assertion that the current state resulted from something appropriate.

RELEVANCE

It's possible to tamper with systems that don't actively prove the correctness of their current state. Such tampering is not easy to discover.

ASSESSMENT

	Method	Reg.	Notes
a-73	did:ion	B	As long as the IPFS-based transaction bundles are available (either via IPFS or somewhere else), the provenance of each DID document is independently validatable. Similarly, if bitcoin state is lost, it would be impossible to verify the provenance of did:ion DID documents. In both cases, it is relatively straightforward to address this by retaining your own copy of the state information, e.g., running your own bitcoin node and hosting the did:ion transaction bundles on your own IPFS node. In addition, late publishing https://identity.foundation/sidetree/spec/#late-publishing could allow multiple versions of DID documents to be simultaneously seen as canonical.

6.6 United States Federal Compliance

http://didcriteria.com/criteria/30

QUESTION

Is the method compliant with US Federal requirements for the use of cryptography?

POSSIBLE RESPONSES

- **A** A. Both registry consensus *and* transaction validation are compliant
- **B** B. Transaction validation is compliant but consensus is not
- **C** C. No. Neither consensus nor transactions are compliant

RELEVANCE

Many US Federal programs and projects require use of cryptography according to standards set by the National Institute of Standards and Technology (NIST), such as:

- FIPS 186-5 (https://csrc.nist.gov/publications/detail/fips/186/5/draft)
- NIST 800-131Ar2 (https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final)
- SP 800-186 (https://csrc.nist.gov/publications/detail/sp/800-186/draft)
- NIST FIPS 186-4 (https://csrc.nist.gov/publications/detail/fips/186/4/final)
- NIST 800-38D (https://csrc.nist.gov/publications/detail/sp/800-38d/final)
- NIST 800-38F (https://csrc.nist.gov/publications/detail/sp/800-38f/final)
- FIPS 180-4 (https://csrc.nist.gov/publications/detail/fips/180/4/final)
- FIPS 800-107r1. (https://csrc.nist.gov/publications/detail/sp/800-107/rev-1/final)

ASSESSMENT

	Method	Spec.	Net.	Reg.	Notes
a-74	did:ion	B	B	B	**Spec** (B), **Net** (B), and **Reg** (B): Bitcoin is likely not NIST compliant thanks to the adoption of Schnorr signatures (with the taproot extension), which are not yet NIST approved. However, recent signals from NIST suggest that (1) bitcoin use of cryptography is not prima facie out of compliance and (2) NIST's previous evaluations of Schnorr hinged on patent concerns; now that those patents are expired, many are optimistic that Schnoor will be given serious consideration in future evaluations. IPFS allows non-approved hash algorithms through multihash, however did:ion adds the requirement that all hashes be SHA-256, which is NIST compliant.

LEGENDARY
REQUIREMENTS