

Web기반 DID메소드 동향 분석

임도현¹, 김건민¹, 조세빈¹, 진현석², 박태준³, 김경백³

¹전남대학교 (학부생),
전남대학교 인공지능융합학과 (²대학원생, ³교수)

Analysis of Trends of Web based DID methods

Dohyeon Lim¹, Geonmin Kim¹, Sebin Jo¹, Hyeonseok Jin², Taejune Park³,
Kyungbaek Kim³

¹Chonnam National University (Undergraduate Student),
Dept. of Artificial Intelligence Convergence, Chonnam National University
(²Graduate Student, ³Professor)

요약

web3가 확산되고 새로운 인증 기술이 필요해짐에 따라 다양한 DID(Decentralized Identifier) method가 생겨났으나 많은 method들이 기존에 있는 인프라를 활용하지 못하여 Web 기반의 DID method가 새롭게 제안되었다. 본 논문은 Web기반으로 동작하는 DID method들에 대한 동향 분석과 더불어 해당 method들의 형식과 동작 방식을 설명한다. 각 method들의 흐름을 파악함으로써 DID 활성화에 따른 상호 운용성을 고려할 때, blockchain 기반 기술뿐만 아니라 Web 기반 기술까지 고려한 탈중앙화 지원 방안에 대한 필요성을 제안하고자 한다.

I. 서론

블록체인 생태계가 활성화됨에 따라 DID에 대한 관심이 높아지고 많은 DID method[1]가 생겨났다[2]. 그러나 추가적인 인프라가 필요하다는 번거로움으로 인해 최근 Web 생태계와의 호환성을 위한 DID method들이 제안되었다. 본 논문에서는 Web 기반 DID method들의 형식 및 절차를 설명하고 DID 운용시 Web 기술 고려의 필요성을 언급한다.

II. Web기반 DID methods

2.1 did:web

did:web[3]은 DNS(Domain Name System)를 활용하여 DID를 식별하는 method이다. did:web의 identifier는 URL(Uniform Resource Locator)로 변환되고, 이를 통해 DID document에 접근할 수 있다.

did:web 구조는 did:web:에 domain 형식의 식별자가 붙는 형태이다. 예시는 다음과 같다.

```
did:web:w3c-ccg.github.io
did:web:w3c-ccg.github.io:user:alice
did:web:example.com%3A3000
```

did:web의 resolution은 식별자를 URL 형식에 맞게 변환하는 작업이다. did:web:을 제외한 나머지 요소에서 “:”를 “/”로 교체하고 “%3A”를 “:”로 교체한다. 하위 디렉토리가 없다면 “/.well-known”을 추가로 삽입한 뒤 마지막에 /did.json을 삽입한다. 완성된 URL HTTP GET 요청을 보내는 것으로 DID document를 획득하게 된다.

2.2 did:webs

did:webs[4]는 did:web과 마찬가지로 기존의 웹 인프라를 활용하여 DID를 게시하고 검색할 수 있도록 한다. 더불어, KERI(Key Event Receipt Infrastructure)[5]를 사용하여 분산된

형태의 신뢰 기반을 구축한다.

did:webs의 식별자는 소문자로 작성된 did:webs:에 domain과 KERI의 식별자인 AID(Autonomic Identifier)가 붙는 형태이다. 아래는 그 예시이다.

```
did:webs:example.com:1234
did:webs:example.com%3A3000:user:alice:1234
```

did:webs의 resolution은 did:web과 동일하게 URL 형태로 변환하는 작업이나, 추가로 keri.cesr에 대한 HTTP GET 요청이 들어가게 된다. keri.cesr을 KERI System을 통해 검증하게 되고, 이를 기반으로 DID document를 생성하여 URL을 통해 얻은 DID document와 비교 후 무결성을 검증하게 된다.

2.3 did:dns

did:web에서 개선점을 제공한 method로, DNS 인프라를 활용하여 DID를 게시하고 검색한다. 이를 통해 DNS 시스템과 호환성을 유지함과 동시에 사용자가 해당 did가 무슨 목적으로 쓰일지 domain을 통해 유추할 수 있도록 한다.

did:dns[6]의 DID는 소문자로 작성된 접두사 did:dns:에 domain이 붙는다. 아래는 그 예시이다.

```
did:dns:danubetech.com
did:dns:support.examplecompany.com
```

did:dns의 resolution은 DID의 식별자에서 domain name을 추출한 뒤 DNS lookup을 수행하여 반환받은 RR을 resolution 하여 이루어진다. 해당 RR에는 did:key에 해당하는 문자열이 담겨 있으며 이를 기반으로 생성된 DID document의 did:key 식별자를 did:dns의 식별자로 대체한 뒤 완성된 DID document를 반환한다.

III. 결론

본 논문에서는 높아지는 DID에 대한 관심도에 따라 제안된 여러 DID method 중 기존 인프라를 최대한 활용하여 운용할 수 있는 Web 기반 DID method에 대한 조사를 수행하였다. 조사 결과 did:web은 DNS와 함께 HTTPS 통

신에 필요한 인증서, did:web 식별자를 URL로 바꾸어 줄 파서가 필요했다. did:webs는 did:web과 동일하나 추가적으로 KERI라는 분산 인증 시스템을 도입하여 DID document에 대한 신뢰도를 높였고, did:dns는 DNS와 함께 RR에 ip대신 did:key에 해당하는 문자열을 삽입함으로써 did:key에 대한 해석기를 요구하였다. 이렇듯 Web기반 DID method들은 기존 웹 서비스에 활용되는 DNS, 웹 브라우저를 최대한 활용하기 위해 블록체인 기반 method와 다른 동작 방식을 채택했으며 필요한 인프라 역시 다르다. 범람하는 DID method들의 상호 운용성을 보장하기 위해서는 블록체인 기술 및 네트워크에 대한 호환성뿐만 아니라 널리 사용되고 있는 Web기술도 고려해야 하며 이들 모두를 아우를 수 있는 탈중앙화된 신뢰 기반 구축이 필요하다.

ACKNOWLEDGEMENT

본 연구는 한국인터넷진흥원(KISA)-정보보안 특성화대학 지원사업의 지원을 받아 수행된 연구임. 이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(IITP-2022-0-01203)

[참고문헌]

- [1] W3C, Decentralized Identifiers (DIDs) v1.0 (2022), <https://w3.org/TR/did-core/>
- [2] 이강효, 박소현, 김현준, 하태균, 유주열, 김경백. (2022). 분산신원증명(DID)과 공개 키 기반(PKI) 간 상호운용가능한 신뢰연결 프레임워크 기본모델 제안. 한국통신학회논문지, 47(10), 1606-1619, 10.7840/kics.2022.47.10.1606
- [3] W3C, did:web Method Specification (2024), <https://w3c-ccg.github.io/did-method-web/>
- [4] ToIP, did:webs Method Specification (2023), <https://trustoverip.github.io/tswg-did-method-webs-specification/>
- [5] Samuel M. Smith, KERI whitepaper(2019), <https://arxiv.org/abs/1907.02143>
- [6] Danube Tech, did:dns Method Specification(2022), <https://danubetech.github.io/did-method-dns/>