iS
CHANNEL

Addressing the Challenges Facing Decentralized Identity Systems

Andrei Volkov

MSc Management of Information Systems and Digital Innovation
Department of Management
London School of Economics and Political Science

KEYWORDS

Decentralized identity management
Decentralized identifiers
Digital identity
Self-sovereign identity
Blockchain

ABSTRACT

With data breaches becoming an increasingly prominent topic within society, businesses have begun directing resources towards enhanced security systems, while governments have seemingly attempted to grant individuals more rights over their personal data. With the development of new data management systems, organizations have the opportunity to create technologies that enhance and not endanger the privacy of data owners (Nyst et al., 2016). This paper discusses the concept of a decentralized identifier (DID) system, which shifts the control of personal data from centralized entities to the identity owners themselves. It places a focus on user data privacy by leveraging distributed ledger technology. Although a DID system presents numerous opportunities for data protection, it must first overcome a number of obstacles before replacing its centralized counterpart. This paper addresses two key challenges that DID systems face: scalability and interoperability. The proposed solutions to the scalability challenge include the implementation of a second layer protocol atop the distributed ledger, as well as a simplified user experience provided by a digital wallet application. Meanwhile, the key strategies for addressing the interoperability challenge include the use of a Universal Resolver, integration of distributed ledgers, and facilitation of compatible digital wallets and identity hubs. By addressing these challenges through collaborative efforts, developers may be one step closer to granting everyone control over their personal data.

Introduction

As our daily lives are now practically inseparable from the Internet, our identities have also rapidly shifted from the physical to the online space, forming digital identities. Typically, digital identities are stored and managed by centralized institutions. One of the key reasons for the use of centralized systems is that users give up some control of their personal data for the services that a centralized platform provides in exchange. As a result, the user can enjoy the platform's features in a cost and time-efficient manner, not having to worry about the security of her data as the company presumably promises state-of-the-art protection.

Recently, however, such a system has demonstrated several drawbacks concerning user privacy and security. The breach of Equifax, a credit-rating agency, exposed personal details of 147 million users, including their social security numbers, home addresses, credit card details, and driver's IDs (EPIC.org, 2019). The Cambridge Analytica scandal unveiled how the political consultancy utilized personal data of 87 million Facebook users who trusted the social network with their information (Confessore, 2018). Besides the security concerns with regards to hackers, users also relinquish their privacy to websites, which monetize personal data through third party targeted advertisements.

Due to the security concerns of existing digital platforms, new and improved systems must orient themselves around user data privacy. Technology can provide mechanisms that would protect an individual's identity, restrict access to unwarranted parties, and verify the validity of an identity to authorized parties, all while maintaining the identity owner's data private. One promising technology in the field of digital identity management is blockchain. In contrast to the existing centralized authorities, blockchain embraces a decentralized approach to data management. Instead of concentrating all the power in the hands of governments and commercial entities, blockchain offers users sovereignty over their own digital identities.

As the concept of decentralized identity management has gained much attention in recent years, with a number of projects currently going through development stages, it is necessary to address not only the opportunities that the technology presents but also the challenges that companies will face as they continue building and expanding their decentralized systems.

Corresponding Author
Email Address: volkovandreimail@gmail.com

This paper aims to advance the understanding of decentralized identity management by conducting a literature review of the challenges that the technology faces, while also imparting a set of potential solutions to address said challenges. Since the topic of decentralized identity management is nascent, the literature review will rely on additional primary sources in addition to available scholarly research. The primary sources comprise of white papers, blog entries from decentralized platform developers on GitHub, posts on community websites DIF and W3C, as well as individual developers' blogs and their companies' blog entries. To extend the findings of the literature review, the proposed solutions will be grounded via a case study through an examination of Microsoft's decentralized system, ION.

Current State of Decentralized Identity Systems

Digital Identities

An individual's digital identity is formed from a myriad of information that any given user provides to gain access to certain websites and services online. Since there are many interpretations of the concept, it is essential to define what a digital identity consists of. Nyst et al. (2016) argue that a digital identity consists of three factors: identification, authentication, and authorization. Identification covers the establishment of information about a user, which could include official documents provided by the individual (passports, SSNs) or an aggregate of data generated by the user through her use of online services (ibid, p. 8). Authentication addresses the assertion of the information provided in the identification step and usually requires authentication credentials (ibid, p. 9). Lastly, authorization determines which operations are granted to a user based on their identification and authentication (ibid, p. 9). Therefore, digital identity consists of all three requirements existing in a digital form.

Self-Sovereign Identity

As a result of the security and privacy concerns in centralized systems, researchers have called for a more user-centric approach to digital identity management. One such approach, self-sovereign identity (SSI), proposes a model where a user has complete control and ownership of her data, without having to rely on a centralized authority. The key requirements of an SSI include (1) user's total control of own data; (2) authentication, security, and privacy are provided by the system, with no need for a centralized entity; (3) complete portability of the data as required by the user; (4) transparency of changes to the data provided by the system (Abraham, 2017).

Decentralized Identifiers

Consequently, SSI has led to the conception of DID. DID is an identification system that assigns a "standard, cryptographically verifiable, globally unique and permanent identity" to a user, granting full control of the data to the identity owner and eliminating the need for a centralized authority (Aydar et al., 2019). It operates through an association to an asymmetric key (a combination of a public and private key). Private keys, which are only seen and known by the identity owner, are associated with public keys, which can be seen by anyone with whom the identity owner interacts with. Thus, a user can verify her identity via DIDs to other users in the system, as well as receive and send any documents, without revealing any information about herself (ibid, p. 10). Such a system creates an environment of credibility, security, and privacy while also providing complete control of personal data to the identity owner. Yet, in order for a system of DIDs to exist, a distributed ledger technology, or blockchain, is required.

Blockchain for Digital Identity Management

Distributed ledger technology brings much promise to achieving a genuinely decentralized identity management system. Blockchain has several assets that make it ideal for a DID and satisfy the four aforementioned requirements of an SSI:

1. As blockchain is distributed by its nature, it cannot be controlled by a centralized authority, granting full control of data to the user;

2. Blockchain's "public-key cryptography and hashing" mechanism provides authentication of the identity holder while keeping her data private; the distributed ledger also prevents the possibility of a "single point of failure and denial of service attacks," providing security to the identity holder (ibid, p. 6);

3. The distributed ledger technology also accounts for the portability of data between various users/ entities in the system;

4. Blockchain's immutability and transparency are crucial to spotting any changes to the data in the system.

Hence, a decentralized digital identity is at the core of blockchain, making the technology appealing for the creation of a DID system.

Digital Identity Management

It is useful to illustrate a possible scenario of how a blockchain-based DID system could operate, as exhibited by Microsoft (Microsoft, 2018). Irina, a recent university graduate, wants proof of her degree to demonstrate it to future employers. The university provides her with a DID-signed diploma, which Irina then saves in her identity hub. This signifies that the university, a credential issuer, has authenticated Irina and verified her diploma, a credential, via a digital signature (Aydar et al., 2019). Now, Irina can grant partial access to her diploma to a potential employer, a verifier, via her digital wallet app, a user agent. The employer can then confirm the validity of the degree issued by the credential provider.

Such a system presents numerous benefits for all parties involved. Irina no longer has to reach out to the university every time a potential employer

requests proof of her degree, which saves time and money, as some universities request additional payments for such a service in the current centralized system. More importantly, Irina now has control over her own degree and job applications, without having to rely on her university. Furthermore, the university can no longer track what type of employer is checking the degree, which Irina may want to keep private. The university also benefits from time and cost-savings as it is no longer required to confirm the proof of degree for every student's potential employer request. The same could be said about the employer.

This simple case of a DID system could be expanded into a multitude of digital interactions that users may have. To enhance her own security and privacy, an identity owner could create multiple DIDs for all the possible interactions that she may have with other identity owners or institutions. Hence, if one DID is compromised, it does not affect other DIDs, keeping the user's identity and data protected (Aydar et al., 2019). Initially, each DID is an empty identity as it is not authenticated by any credential issuer; however, over time, DIDs gain credibility as more trusted parties assert the identity and information associated with the DID through a process of attestation (Microsoft, 2018). As a result, one could "require standard and verifiable claims from multiple trust providers before engaging in identity interactions and sensitive disclosures," (ibid, p. 15). Thus, the system also provides a level of trust amongst identity owners.

Challenges Facing DID Systems

Scalability

The issue of scalability is one of the most frequently-cited challenges for blockchain, and distributed ledgers for DIDs are no exception. The challenge is two-fold as there are both technological and user adoption concerns. From a technological perspective, scalability can be interpreted as blockchain's ability to maintain its processing capabilities while expanding the network (Hileman and Rauchs, 2017). As the Bitcoin network grew, the time between the initiation of a transaction and its addition to the block extended to 10 minutes (Croman et al., 2016). Such a delay diminishes the throughput rate to 7 transactions/sec, which is minuscule compared to the average 2,000 transactions/sec of a centralized platform such as Visa, which at times achieves a rate of 56,000 transactions/sec (ibid, p. 1). This challenge becomes particularly relevant when projects such as Microsoft's ION set ambitious goals of providing a DID to 7.5 billion people (Microsoft, 2018). Without achieving at least parity with centralized systems, proponents of DIDs may find it difficult to convince the average consumer to switch over to a decentralized platform.

User adoption, therefore, is also a vital component of the scalability challenge. Besides the deterring slow transaction speeds of blockchain, the average user will also be reluctant to use DIDs due to the seemingly complex concept of the technology. Since a DID would primarily serve as a privacy and security solution, it is worth examining the current state of security maintenance by average users. According to an analysis of password breaches conducted in the UK, 55% of adults re-use the same password across multiple websites (NCSC, 2019). Hence, proposing DIDs to the average identity owner would be challenging, particularly if the DID platform's user experience is more complicated than a centralized system's process of creating a username and password.

Interoperability

Similar to scalability, interoperability is a common challenge across distributed ledgers, meaning DID systems will have to address the problem as well. The issue stems from the fact that seemingly identical distributed ledgers may have varying "security, integrity, and usability considerations," leading to difficulties in interactions across ledgers (Lesavre et al., 2020, p. 35). Currently, the repository service GitHub contains over 6,500 blockchain-related projects, which utilize differing specifications, consensus mechanisms, and programming languages (Deloitte, 2018). Such a multitude of projects leads to a complex integration process amongst them. Furthermore, a research study carried out by Hileman and Ruachs (2017) demonstrated that "only 25% of distributed ledger networks are interoperable with other distributed ledger networks and applications" (p. 74).

Thus, as it is highly unlikely that all users would utilize a single DID system, the question of interoperability becomes critical. A DID system's limited capability to only operate within the confines of its own distributed ledger would also drive down the user adoption rate.

Addressing DID Challenges

Scalability Solutions

Second Layer Protocol

Blockchain's slow throughput rate, as seen with Bitcoin transactions, is predominantly attributed to the block size and the block generation time (Croman, 2016). To amend this issue, the Bitcoin community has frequently proposed to increase the size of the blocks. DID research, however, has shifted the issue away from merely focusing on the block sizes and instead proposes for DID systems to operate on a blockchain as well as an additional protocol on top, the second layer protocol (Lesavre et al., 2020). The belief is that such a network would transfer transactions and operations away from the blockchain layer, alleviating the processing power, and providing more opportunities for scaling up (ibid).

An example of such a network is Microsoft's ION, a public and permissionless DID system which utilizes a second layer protocol called SideTree built atop of the Bitcoin blockchain (Simons, 2018). SideTree accelerates the throughput rate by bundling DID operations together into batches, instead of adding them individually onto the blockchain (ibid). SideTree's nodes process batches by adhering

to predetermined rules that "enable them to independently arrive at the correct decentralized public key infrastructure state" (Buchner, 2020). Furthermore, SideTree nodes provide endpoints to carry out specific tasks, such as "create, resolve, update, recover, and deactivate," pertaining to DID documents (Tsai et al., 2020). The SideTree layer only utilizes the underlying blockchain's consensus mechanism to serialize the DID batches in a sequential and consistent manner (Buchner, 2020). Since SideTree does not require additional consensus mechanisms, it addresses the issue of small block sizes, as it is not encumbered by the underlying blockchain's limited transaction rate. After the protocol consolidates multiple operations into batches, it places the files in a distributed content-addressed storage, as seen on DIF's website (Tsai et al., 2020). The only thing that is actually anchored to the blockchain itself is a reference to the batches (ibid). The batch data itself is stored as one. As nodes operate simultaneously while processing batches of DIDs, SideTree can run tens of thousands of operations per second (Simons, 2019).

The question of what is actually stored on the blockchain is also quite pertinent in matters of scalability. As seen in the SideTree protocol as well as other proposed DID systems (Aydar et al., 2019; Goodell and Aste, 2019), no personal data should be kept on the blockchain itself, even in an encrypted state. Not only is this vital for the security and privacy aspects of DID networks, but it also greatly benefits the system's scalability efforts. A second layer protocol makes this possible as no DID data has to overload the distributed ledger itself. Instead, only a reference or consent proof of said data is anchored to the blockchain. By utilizing a second layer protocol in this manner, ION is able to offload the operational burden from the underlying blockchain. As a result, the number of DID operations being processed at once increases drastically, expanding the overall capacity of the network. Thus, Microsoft's use of SideTree as the second layer protocol is an essential step towards achieving a truly scalable DID solution.

Digital Identity Wallet For Improved User Experience

In order to reach a large user base, a DID system not only has to achieve scalability via its technical specifications, but it also needs to present a flawless customer-facing solution. In its current state, a DID solution will fail to go beyond the "innovators" phase of the Technology Adoption Cycle (Karlsson, 1988) as the system will be too complicated for the average user to understand. Even if the average user may see the value of privacy and security that a DID system provides, she will continue utilizing a centralized system due to its simplicity and familiarity. Thus, user experience is a vital feature of scalability.

The key to a satisfying user experience lies in a digital identity wallet, which takes the form of a phone and desktop application. The wallet serves as the primary and sole space where a user has to interact with the DID system. Through the wallet, a user should have access to her identifiers, private keys, and credentials, which are all only visible to her (Lesavre et al., 2020). The app also serves as space for users to interact with one another. Through the wallet, users send authentication requests, trusted issuers verify users and send credentials, and third parties can access credentials that are granted by the users. To simplify experience further, APIs could be used to trigger particular operations within the network, which could be easily initiated by a user scanning a QR code, a function already implemented by a DID startup CryptId (Jacobovitz, 2016). Users should also be able to generate new identifiers directly on the app, offline, without having to rely on a centralized authority to provide it for them (Lesavre et al., 2020). Such a feature is also beneficial for scalability since the blockchain would not be strained with facilitating operations for identifier generation. To further simplify access to the wallet, users could be asked to provide biometrics to sign onto the app, a feature that most smartphone providers allow.

Without a centralized authority, the responsibility of maintaining private keys falls onto the users. If a private key is lost or deleted, certain credentials could be lost forever, as the user does not have access to the equivalent of a "forgotten password" option since there are no centralized authorities. In order to prevent this, developers of DID networks could include mechanisms such as "a custodian designated by the user, a list of user-appointed trustees, and time delay mechanisms, in the case of a private key being deleted" (Lesavre et al., 2020, p. 18). From this, it is interesting to note that the growth of the custodian market is inevitable. Just as with the storage of private keys on cryptocurrency exchanges, users will seek out custodians with the rise of DID networks. The DID purists, however, might argue that relying on custodians defeats the purpose of a decentralized system since the identity owner is, once again, relying on a mediator.

Microsoft's ION proposes a digital wallet, referred to as a User-Agent app (Microsoft, 2018). The purpose of the app is to "aid in creating DIDs, managing data and permissions, and signing/validating DID-linked claims" (ibid, p. 10). ION's ultimate goal is to create an app that would be accessible to the average user to the point where she would not even have to understand or see the term DID. Hence, DID network developers should approach their projects with the same mindset. Only a seamless app experience will comfort the user in the transition from a traditional centralized platform to a DID network.

Interoperability Solutions

Universal Resolver

All DID networks have to implement solutions that would allow users to interact across platforms. The Universal Resolver, as proposed by the Decentralized Identity Foundation (DIF) (2020), is one such solution that would integrate multiple DID systems via a single resolver of DIDs. Thus, every DID system must incorporate application code that would link their own system's method for interpreting DID documents to the Universal Resolver (ibid). By doing so, DID systems would interact with one another via a ubiquitous interface,

without having to adapt to each other's application specifications.

From a technical perspective, the Universal Resolver is able to read and communicate all types of DID documents via "drivers" for each identifier class (Sabadello, 2017). As DIF operates via open-source platforms, developers continuously contribute their DID drivers to the network, allowing the Universal Resolver to comprehend a vast number of DID documents (ibid). As these drivers have a direct connection to their own distributed ledger's nodes, the resulting network is blockchain-agnostic (ibid). This means that no matter the underlying blockchain that is used in a particular DID system, be it Sovrin, Bitcoin, or Ethereum, the Universal Resolver can process their documents and allow the systems to communicate with one another, without burdening them to fetch each other's technical specifications.

With the help of DIF's Universal Resolver, Microsoft's ION will allow the users of its digital wallet app to look up, authenticate, and request identifiers from users operating on all other DID systems (Microsoft,2018). Thus, in a scenario where a trusted entity sends a credential to a user, the credential's associated DID is processed via one of the drivers registered on the Universal Resolver, which then fetches the corresponding DID document (ibid). Such an interoperable system would create an all-around comprehensive directory of DIDs, allowing users to send and receive documents regardless of what DID systems their digital wallets operate on. Thus, the interoperability feature would also contribute to DID systems' scalability efforts, as average users would be inclined to adopt the technology only if there was a significant presence of other users and trusted entities utilizing it.

Integration of Distributed Ledgers

Another worthwhile interoperability solution is the cross-integration of ledgers. Here, the concept is to integrate competencies and features of one system into another. For example, various distributed ledger providers have integrated Hyperledger Indy's DID capabilities into their own systems. Cordenity, a smart contract created by the Corda Platform, implemented Hyperledger Indy's libraries into its own blockchain (Kopnin et al., 2020). According to Corda, the reasoning behind this integration is that "while Corda is best suited for developing decentralized applications for managing complex inter-organizational workflows, Indy is the leading open-source platform for self-sovereign identity" (ibid). Thus, Corda's smart contract operations rely on the credentials and documents that are authenticated by Indy's DID system.

Interoperable Digital Wallets & Identity Hubs

Due to various advantages and specializations of some DID systems over others, users and entities are likely to use varying digital wallets. To meet the identity owners' expectations and improve their user experience, developers of DID systems should consider facilitating interoperable digital wallets. Not only would the interoperable wallets allow users to manage their own private and public keys easily, but it would also ease the user authentication and credential transfer process for entities operating on differing DID systems. Developers could use protocols such as BIP-32, which facilitate the interoperability amongst digital wallets for cryptocurrency storage and management, as inspiration for the convergence of DID wallets (Maxwell et al., 2019).

Concluding Remarks

The aim of this paper was to further the understanding of the challenges and opportunities of DID systems via a literature review supported by a case study. The review highlights a number of findings related to decentralized identity management. The proponents of enhanced security and privacy in the digital space have to consider ways in which they could prioritize the interests of identity owners, granting them control over their personal data. The development of a network of DID systems is a step in the right direction. To address the challenges of scalability and interoperability, as well as numerous other obstacles, the developers of DID systems should seek collaborative efforts via open-source platforms. Additionally, in order to successfully implement DID networks into our digital ecosystem, DID advocates must clearly illustrate its advantages to the identity owners as well as businesses. This paper explored user adoption from the average identity owner's perspective. Hence, future research could examine the possible solutions to increasing adoption rates of DID systems from governmental and business perspectives.

References

Abraham, A. (2017). E-Government Innovationszentrum Whitepaper about the Concept of Self-Sovereign Identity including its Potential. www.egiz.gv.at

Aydar, M., & Ayvaz, S. (2019). Towards a Blockchain Based Digital Identity Verification, Record Attestation and Record Sharing System. http://arxiv.org/abs/1906.09791

Buchner, D. (2019). Decentralized Identity. GitHub. https://github.com/decentralized-identity/identity-hub/blob/master/explainer.md

Buchner, D. (2020). DID Method implementation using the Sidetree protocol on top of Bitcoin. GitHub. https://github.com/decentralized-identity/ion

Confessore, N. (2018). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. The New York Times. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Croman, K., Decker, C., Eyal, I., Efe Gencer, A., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Gün Sirer, E., Song, D., Wattenhofer, R., & Tech, C. (n.d.). On Scaling Decentralized Blockchains (A Position Paper) Initiative for CryptoCurrencies and Contracts (IC3) 1 Cornell.

Electronic Privacy Information Center. (2018). Equifax Data Breach. EPIC.Org. https://epic.org/privacy/data-breach/equifax/

Goodell, G., & Aste, T. (2019). A Decentralized Digital Identity Architecture. In Frontiers in Blockchain (Vol. 2, p. 17). https://www.frontiersin.org/article/10.3389/fbloc.2019.00017

Hileman, G., & Rauchs, M. (2017). Global Blockchain Benchmarking Study. Cambridge Center for Alternative Finance.

Holmes, A. (2019). Biggest hacks and data breaches of 2019: Capital One, WhatsApp, iPhone - Business Insider. Business Insider. https://www.businessinsider.com/biggest-hacks-and-data-breaches-of-2019-capital-one-whatsapp-iphone-2019-9?r=US&IR=T

Jacobovitz, O. (2016). Blockchain for Identity Management. The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University

Karlsson, C. (1988). Innovation adoption and the product life cycle. In Umeæ Economic Studies (Issue 185). http://www.diva-portal.org/smash/get/diva2:792156/FULLTEXT01.pdf%0Ahttp://hj.diva-portal.org/smash/record.jsf?pid=diva2:36369

Kopnin, A., Koren, A., & Vodopian, D. (2020). Combination of Hyperledger Indy and Corda. GitHub. https://github.com/Luxoft/cordentity

Lesavre, L., Varin, P., Mell, P., Davidson, M., & Shook, J. (2020). A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. https://doi.org/10.6028/NIST.CSWP.01142020

Maxwell, G., Reiner, A., Lombrozo, E., & Caldwell, M. (2019). Hierarchical Deterministic Wallets. GitHub. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki#Abstract

Microsoft. (2018). Decentralized Identity. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY

Microsoft. (2018). Decentralized Identity.

NCSC. (2019). Most hacked passwords revealed as UK cyber survey exposes gaps in online security. National Cyber Security Centre. https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

Nyst, C., Makin, P., Pannifer, S., & Whitley, E. (2016). Digital Identity: Issue Analysis Executive Summary. www.chyp.com

Othman, A., & Callahan, J. (n.d.). The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity.

Reed, D., Sporny, M., & Sabadello, M. (2020). Decentralized Identifiers (DIDs). In W3C. https://www.w3.org/TR/did-core/#dfn-did-documents

Richardson, B., & Waldron, D. (2019). Combating synthetic identity fraud | McKinsey. https://www.mckinsey.com/business-functions/risk/our-insights/fighting-back-against-synthetic-identity-fraud

Sabadello, M. (2017). A Universal Resolver for self-sovereign identifiers. Medium. https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c

Sadabello, M. (2017). Universal Resolver. GitHub. https://identity.foundation/

Schatsky, D., Arora, A., & Dongre, A. (2018). Reaping value from blockchain applications. Deloitte. https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/value-of-blockchain-applications-interoperability.html

Simons, A. (2019). Toward scalable decentralized identifier systems. Microsoft. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/toward-scalable-decentralized-identifier-systems/ba-p/560168#

Sovrin. (2020). Innovation Meets Compliance. The Sovrin Foundation.

Swan, M. (2015). Blockchain for a New Economy. O'Reilly Media.

The, F., & Internet, D. (n.d.). Decentralized Identity - What Lies Ahead of Us: The Open(Interesting) Research Issues. https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

Tsai, H. (2020). Sidetree Protocol Specifications. GitHub. https://github.com/decentralized-identity/sidetree/blob/master/docs/protocol.md

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477