Old Dominion University

ODU Digital Commons

Cybersecurity Undergraduate Research

2022 Fall Cybersecurity Undergraduate Research Projects

A Review of Distributed Identity Technology in IoT Devices

Myles Perry
Old Dominion University

Follow this and additional works at: https://digitalcommons.odu.edu/covacci-undergraduateresearch

Part of the Information Security Commons

Perry, Myles, "A Review of Distributed Identity Technology in IoT Devices" (2022). *Cybersecurity Undergraduate Research*. 15.
https://digitalcommons.odu.edu/covacci-undergraduateresearch/2022fall/projects/15

This Paper is brought to you for free and open access by the Undergraduate Student Events at ODU Digital Commons. It has been accepted for inclusion in Cybersecurity Undergraduate Research by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.

A Review of Distributed Identity Technology in IoT Devices

Myles Perry

Advised by Dr. Bouk Safdar, Associate Professor at Old Dominion University

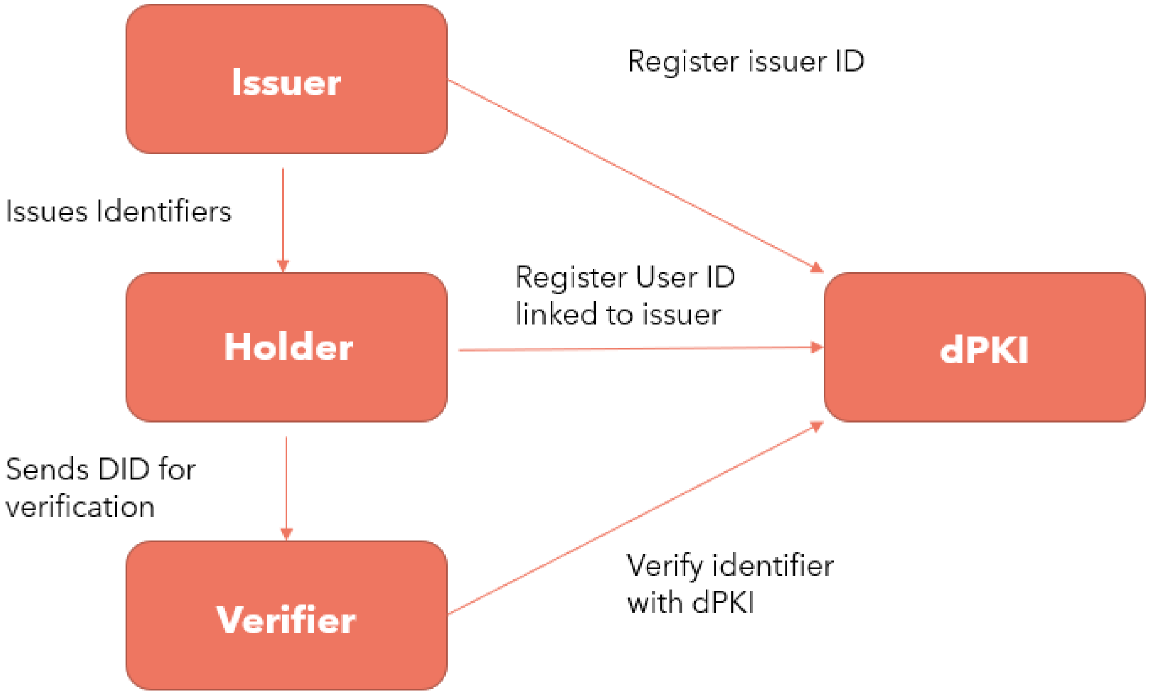
COVA CCI Undergraduate Research, Fall 2022

Abstract

Distributed identity technology provides solutions to many of the faults currently found in federated identity systems. Applying this technology to internet of things devices has many possible benefits in the realm of device authentication. However, this also provides new challenges not present in existing distributed identity systems. The large number of devices that would enter and leave the system means balancing sybil attack vulnerability and linkage attack vulnerability becomes challenging. Internet of things devices also have less memory and computing power than a standard personal computer or phone. This means any protocol to execute distributed identity in these devices must not be computationally taxing on the devices. As well, if the internet of things devices should provide data from their sensors to the chain, the protocol must have a method to verify the validity of the data. The existing protocols that have been developed each target these issues in different ways, but none design a protocol perfect for all desired use-cases.

1.1 Background on Distributed Identity

The subject of distributed identity has become of keen interest to cyber security researchers. Distributed identity stands in contrast to federated identity, the most familiar form of identity verification mechanisms in place. Distributed identity allows for the identity controller, analogous to a user, to control their identity data separate from any centralized registry or authority [1]. This is achieved through a decentralized public key infrastructure (dPKI) maintained by three categories of parties: issuers, holders, and verifiers. Issuers issue credentials. Holders are analogous to users that hold the credentials for presentation to verifiers. Verifiers request credentials from holders. The dPKI stores paired keys with the issued credentials. Issuers, holders, and verifiers, interact with the dPKI to issue and verify credentials anonymously and without a central authority and point of failure [2].


Issuer
Register issuer ID
Issues Identifiers
Holder
Register User ID linked to issuer
dPKI
Sends DID for verification
Verifier
Verify identifier with dPKI

2.1 Existing Work

Since the publication of the original bitcoin whitepaper, there has been much interest and further development into the applications and capabilities of decentralized verification systems in both the academic and private sectors [3]. The proof of work algorithm laid out by the paper allows for decentralized nodes to individually verify on chain truth without the need for a centralized, governing authority that could be prone to manipulation by a nefarious actor. This capability has drawn the attention of many researchers in various fields. Firstly, the internet at large functions with many federalized, centralized databases of identity to provide the services it does. This materializes for the end user as the numerous accounts that must be made on nearly every website and the information that must be repeatedly provided. Any of these service providers may have a security breach, threatening the safety of user data. Distributed identity aims to solve this problem. Distributed Identity protocols create distributed public key infrastructure for the storage and verification of identifiers (identity data) with distribution and access under the thumb of the individual the identifiers belong to. Organizations that require identifiers or identity verification to provide their services may tap into a distributed identity framework to verify identity or gather identifiers with minimal storage of data and the ability to revoke access by the credential holder. This ability to verify identity algorithmically is very useful for internet of things devices, increasing the security of the vast IoT network that is ever-expanding.

The following sections will cover the related work covering approaches taken in the contemporary literature to construct networks that are (1) able to validate the data being entered from IoT devices, (2) able to avoid Sybil attacks in the network, and (3) execute their security processes with low computational cost.

2.2 Data Validation

When entering information from a device into the distributed ledger, the other participants in the system must have a reason to believe that the information being operated upon is trustworthy data. This requirement is especially true in distributed identity systems as the premise of validating identity cannot be successfully completed without faith in the data stored in the distributed public key infrastructure. Different approaches to this exist. In [4], the authors propose a consortium blockchain, with the consortium members providing the source of validation for identifiers. For example, these consortium members may be governmental organizations, companies, or schools. This allows for the trust of each identifier to be as strong as one's trust in the verifying organization. However, this encounters a limitation with many IoT devices when they must contribute information to the network such as sensor data. An oracle-based verification system is used in this case. An oracle is a method of verifying external data into the blockchain through decentralized verification. Generally, blockchain nodes will validate external data by taking on the role of a voter. These voters will stake funds according to the validity of the data presented [5, 6, 7]. The authors of [7] implement a single mode oracle in their data verification scheme. A single mode oracle contains one oracle that handles data verification. The alternative to a single mode oracle is an oracle network, which in and of itself poses new security concerns and has greater computational requirements, making it unfit for internet of things applications.

2.3 Protecting Against Sybil Attacks

Sybil attacks are of great concern in a distributed identity network. Sybil attacks describe an attack on the system where malicious nodes are able to enter the network too easily and gain a disproportionate influence in the network in regard to voting mechanisms. Distributed identity networks must balance the need to allow new users to become participants while also maintaining security. This is especially important with internet of things technology as numerous devices may enter and leave the network frequently, causing an unstable network topology. Therefore, the difficulty of identifying fraudulent nodes becomes somewhat more complicated than in a relatively static system. Many computationally expensive PoW algorithms have been developed to combat Sybil attacks, but internet of things devices tend to have limited computing power and memory to run these algorithms [6, 7]. Therefore, alternative methods have been developed.

The authors of [4] focuses predominantly on the sybil attack issue. To keep linkages hidden and keep multiple identities without introducing sybil attacks, they use a two-layer ID system—a masterID above several pseudonymous userIDs. The masterID is a secret to the public. The userIDs addresses the privacy issue of attribute linkage, where data linked together under a publicly available ID allows a nefarious actor to attempt and discern the real identity behind the publicly available ID. So masterID will prevent sybil attacks by virtue of being secret to the public, and many userIDs prevents linkage attacks by virtue of splitting up data under each ID. The authors of [10] make use of a physical unclonable function to give each internet of things device in the network a unique fingerprint. A physical unclonable function uses on-board microstructures unique to each device to generate unique outputs. This information allows the network to identify a fraudulent actor by physical unclonable function fingerprint. However, this presents the issue corrected by [4], allowing linkage attacks by nefarious actors on the network. Once the fingerprint of a device has been compromised, it cannot be altered to regain anonymity. The Rechained protocol requires nodes to self-verify by means of making a payment to the network in the form of the network's token [11]. This disincentivizes the creation of fraudulent or nefarious nodes by making it prohibitively expensive to generate them.

2.4 Computational Efficiency

Since internet of things devices have low computational power and limited memory capabilities, distributed networks must be designed with this constraint in mind. [4] and [7] lower the requirements for internet of things devices serving as nodes by turning them into light-nodes. These, by design, minimize the necessary memory storage of the present block being operated on by the nodes of the network. [10] uses identity-based cryptography (IBC) on top of existing blockchain architecture to achieve a lightweight verification technique, useful for internet of things devices. Rechained circumvents computational complexity by requiring all nodes to register themselves with the network through a payment to the network [11]. This effectively offloads the computational workload onto the mass of the network.

3.1 Comparison of Existing Schemes

The schemes for effective distributed identity technology applicable to internet of things devices is addressed by [3], [7], [10], and [11]. They each design systems that address the issues of Sybil attacks in an internet of things network, the computational limitations these devices have, and the need to validate the data internet of things devices send on-chain. The following table summarizes each scheme and its approach to each design criteria.

	Yin et al.'s SmartDID	Bochem and Leiding's Rechained	Shi et al.'s Protocol	Babu et al.'s Protocol
Sybil Attack Reduction	Two-layer ID system—MasterIDs and UserIDs	Disincentivize the creation of nodes by requiring token payment	n/a	Uses a PUF to uniquely identify every device
Computational Efficiency	IoT devices are configured as light nodes	Nodes use tokens as validation in lieu of actual computation	Uses a fast byzantine fault tolerant mechanism to lower node requirements	Uses a lightweight Identity based cryptography to decrease computing and memory requirements
Data Validation	Verifies data with trusted issuers in a consortium blockchain	n/a	An oracle allows users to validate data entering the chain	n/a

Shi et al.'s protocol lacks a mechanism for Sybil attack reduction [7]. The Rechained protocol [11] and Babu et al.'s protocol [10] both lack techniques to validate data submitted to the chain by nodes, limiting the use-cases they could be applied to. SmartDID offers solutions to all the criteria, but limits the trusted data issuers via a consortium blockchain [3].

4.1 Further directions

The protocol presented by SmartDID stands as the most complete and flaw-free design for distributed identity protocols with internet of things applications [4]. However, other designs are able to achieve verification with a permissionless network. SmartDID relies on a consortium blockchain to achieve validation of credentials and identity data. As well, Rechained manages to create a network that can handle internet of things devices that don't remain connected to the internet, as validation is handled through a direct payment scheme [11]. A future development is a protocol that achieves protection from sybil attacks and linkage attacks, while also allowing for internet of things devices to provide sensory data to the chain with oracle validation.

Reference List

[1] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, C. Allen, "Decentralized Identifiers (DIDs) v1.0," w3.org, https://www.w3.org/TR/did-core/, accessed 11/16/2022.

[2] L. Sorokin, "A Peek into the Future of Decentralized Identity (v2)", IDPro Body of Knowledge, 1(7), February 2022, doi: https://doi.org/10.55621/idpro.51

[3] S. Nakamoto, "Bitcoin: a Peer-to-Peer Electronic Cash System," March 2019.

[4] J. Yin, Y. Xiao, Q. Pei, Y Ju, L. Liu, M. Xiao, C. Wu, "SmartDID: A Novel Privacy-preserving Identity based on Blockchain for IoT," *IEEE Internet of Things Journal,* September 2021.

[5] J Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, A. Kastania, "Astraea: A Decentralized Blockchain Oracle," in *Proceedings of the 2018 IEEE International Conference on Internet of Things, 2018.* Place of Publication: IEEE, 2018.

[6] J. Peterson, J. Krug, M. Zoltu, A. K. Williams, S. Alexander, "Augur: a Decentralized Oracle and Prediction Market Platform (v2.0)," August 12, 2022.

[7] P. Shi, H. Wang, S. Yang, C. Chen, W. Yang, "Blockchain-based trusted data sharing among trusted stakeholders in IoT," *Software: Practice and Experience,* July 9, 2019.

[8] U. Asfia, V. Kamuni, S. Sutavani, A. Sheikh, S. Wagh and N. M. Singh, "A Blockchain Construct for Energy Trading against Sybil Attacks," 2019 27th Mediterranean Conference on Control and Automation (MED), 2019, pp. 422-427, doi: 10.1109/MED.2019.8798489.

[9] B. Prünster, D. Ziegler, C. Kollmann, B. Suzic, "A Holistic Approach Towards Peer-to-Peer Security and Why Proof of Work Won't Do," In *Proceedings of the Security and Privacy in*

Communication Networks, SecureComm 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 255. Springer, Cham. https://doi.org/10.1007/978-3-030-01704-0_7

[10] E. S. Babu, A. K. Dadi, K. K. Singh, S. R. Nayak, A. K. Bhoi, A. Singh, “A distributed identity-based authentication scheme for internet of things devices using permissioned blockchain system,” *Expert Systems,* January 4, 2022.

[11] A. Bochem, B. Leiding, “Rechained: Sybil-Resistant Distributed Identities for the Internet of Things and Mobile Ad Hoc Networks,” *Sensors*, May 8, 2021.