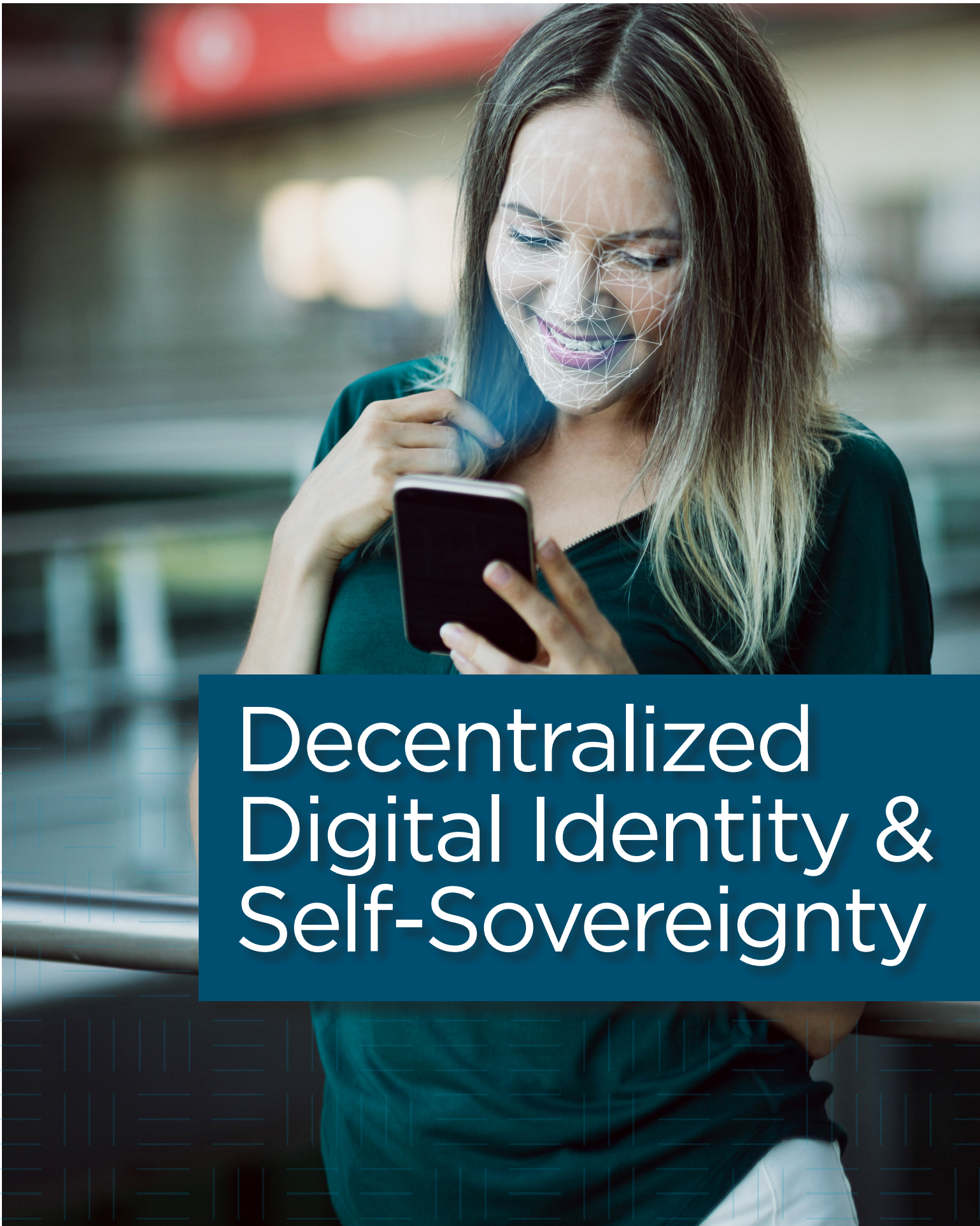
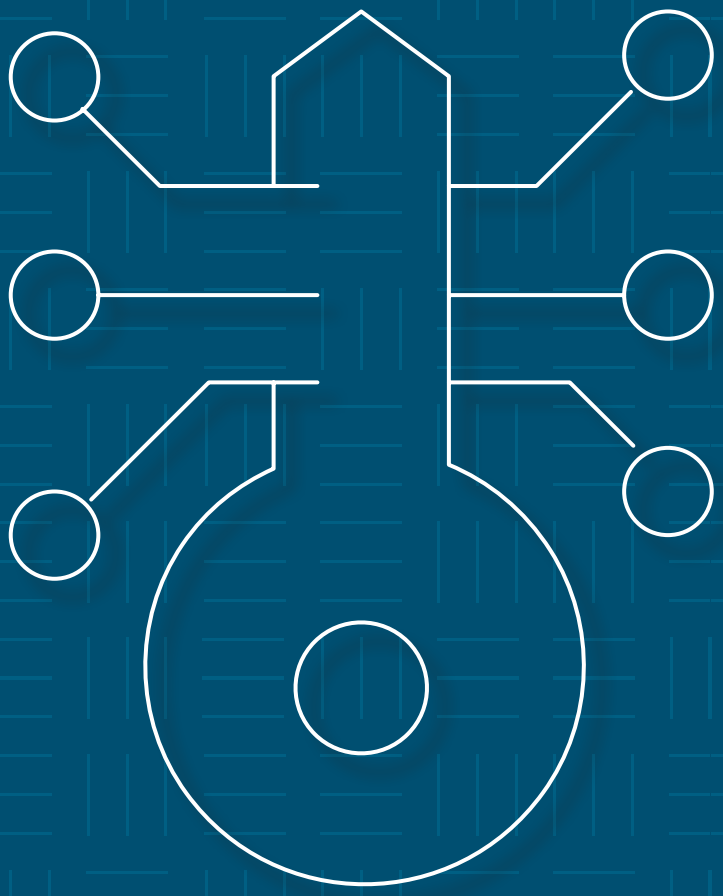
CompTIA
Blockchain & Web3 Industry Advisory Council

WHITE PAPER



Decentralized Digital Identity & Self-Sovereignty



Created by CompTIA's

Blockchain & Web3
Industry Advisory Council

Special thanks to Elena Dumitrascu and Wes Jensen of CompTIA's Blockchain and Web3 Industry Advisory Council for developing this project.

Table of Contents:

Overview

With the increasing use of digital technologies in various aspects of our lives, the importance of decentralized digital identity has become more apparent. We've seen in recent years the need to present vaccination details to travel or access a business. This type of health information is part of your digital identity, along with banking information, employment, education and of course driver's license, passport, resident card and birth certificate. In all those cases, our data goes through a proxy before it ends up in our wallets, aka an identity federation service. The big change happening is putting the user in control, removing the proxy and facilitating trust directly from the issuer to the user and the places where these IDs are presented, also called self-sovereign identity management.

In this post we will describe the emergence of decentralized digital identity, how it's reshaping IT security and how MSPs can use decentralized identities to improve the security and privacy posture of their customers.

Decentralized digital identity is the digital representation of an individual or an organization that is used to establish trust and enable secure interactions online. In this article, we will explore the importance of decentralized digital identity in various domains where it matters.

The cybersecurity industry is closely looking at decentralized identity (DCI) as a means to provision users with access, remove federation services and going password-less. It is well known by now that passwords and multifactor authentication (MFA) are not strong enough to prevent security breaches.

- "Dormant accounts represent 24.15% of the average company's total accounts."
  - Oort, State of Identity Security Report 2023

- "The average company has 40.26% of accounts with either no MFA or weak MFA."
  - Oort, State of Identity Security Report 2023

Decentralized Identity Standards Will Build the Internet of Tomorrow

As large organizations start to deploy decentralized digital identity credentials, it becomes imperative that MSPs stay abreast of the latest developments. Demand will begin to trickle down to enterprise branches and small-and medium-sized businesses and customers looking to use these products will need help.

New web standards are being rolled out to support decentralized identity. The World Wide Web Consortium (W3C) and Decentralized Identity Foundation (DIF) are two major global standards bodies focused on developing new methods that transform how we digitally share our identities. They are bringing together the IT, Government and Business communities together to solve global interoperability. W3C has played a similar role in the past when they rolled out the HTML and CSS standards. In the late 90s as these standards were being rolled out, we saw massive adoption of internet communications such as websites and email.

Decentralized identity standards are the current work of these groups and it is expected to have just a big of an impact in the ways we communicate digitally. The DCI standards allow credentials earned from across the globe to be read, validated, and displayed with speed, privacy and trust. The recommendations and standards from these organizations will provide a higher level of identity assurance, privacy protection, and security. Ultimately, this will affect how individuals manage their identity and how companies building applications will be required to meet the standards.

Last fall, the W3C announced that decentralized identifiers (DIDs) v1.0 are an official Web standard.

The DIF formed to advance the interests of the decentralized identity community and currently works on interoperability, standards, and security for decentralized identity.

What does it mean for individuals? They get better control over where and how their personal information is used.

This new type of decentralized and verifiable identifier, which does not require a centralized registry, will enable both individuals and organizations to take greater control of their online information and relationships while also providing greater security and privacy. Using our earlier example of vaccination proof, an individual's vaccine information would remain encrypted until they selected to share. Further, the place they shared this information with would simply have a just a proof token and not the whole vaccination record stored on their servers.

Decentralized Digital Identities are Built Using Verifiable Credentials

Let's explore the technical "how it works" along with some key terminology this new industry is introducing.

What is a verifiable credential?
In its simplest form, a verifiable credential (VC) is a document that can be reliably traced back to its source and validated as genuine. Held in a VC wallet (a digital wallet locked with a PIN or Passphrase) and under the full control of the user.

Who are the key players?

- **User.** also called a holder or a subject. This is the person, asset of business that controls the VC.
- **Issuer.** A trusted organization, confirming the claims a user makes about their digital identity. Typically, this is a government body, employer, insurance provider or education institute.
- **Verifier.** A trusted organization that requests verification of a credential and confirms those claims meet their requirements. Typically, this can be an employer, bank or education institute.

What is a Decentralized Identifier (DID)?
In a VC world, people, assets and organizations have a Decentralized Identifier (DID). A DID is a unique identifier not containing any personally identifiable information. They are publicly available and owned by the person, asset, or company.

DIDs are used to digitally sign a claim about a person, asset, or company. The issuer digitally signs the document using their DID. These signatures cannot be tampered with, and, as a result, the claims can be trusted immediately.

How Does It Work?
The how is the most important part. As part of the standards around Verifiable Credentials there are the concepts of Expiry, Revocation, Resolution & Verification.

- **Expiry.** When a Verifiable Credential is issued, its expiry date can be set. Once this date has passed, the credential will need to be re-issued or it can no longer be used.
- **Revocation.** The Verifiable Credential can be revoked by the issuing authority (the organization that issued the credential) and once this is done, it can no longer be used.
- **Resolution.** The DIDs in the Verifiable Credential must be resolvable. Using a very similar method to how the World Wide Web uses the address CompTIA.org to find CompTIA's website, VC Wallets are able to "resolve" the DID that is supplied with a credential. If they cannot resolve the DID, the credential is immediately rejected because the signing DID is not what and where the credential says it is.
- **Verification.** Checking the Verifiable Credential for validity. Once the DID has been verified, the credential can be examined for expected outcomes such as 'has the credential expired'. These verifications are built right into the web standard, making them compatible with modern software systems and giving the reader instant confirmations of the expiry dates or whether or not the credential has been revoked. Links to the reference standards can be found at the bottom of this blog.

Self-Sovereign Digital Wallets and Governance

Decentralized digital identities are made up of digital credentials (also called verifiable credentials). We are seeing two types of wallets come to market. The first one simply stores and presents a digital credential. For example, a mobile driver's license. This can be presented to prove age or ability to operate a vehicle. The second type is for complex business rules such as the ability to perform a specific job or be allowed in a secure room. This type of wallet must meet the conditions of the verifier, support different issuance protocols and have flexibility for how your data can be presented "in a bundle."

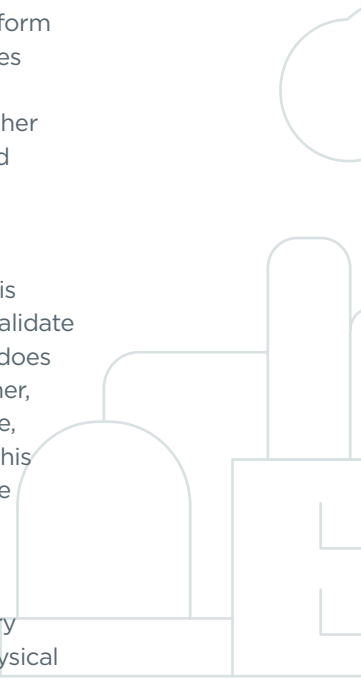
Wallets can be made available in a closed off ecosystem: one where the holder, the issuer and the verifier have agreed to exchange information with each other using a specific platform. Ledgers can be easily deployed in this scenario. All participants agree to be a member of that ecosystem and join the ledger.

Wallets can also be available in an open ecosystem: where the holder, the issuer and the verifier are running different platforms and solutions for exchanging this information. In this case, non-ledger solutions are beneficial. These solutions are built using interoperable standards and give the user more portability. For example: they can hold and present a university degree, a driver's license and an insurance certificate, all issued by different organizations using different solutions.

Potential Use Cases in Other Industries

Let's explore some real-life scenarios of decentralized identities in use today.

Retail:
Jane is an expert shopper. She shops at her favorite department store so often that she has achieved the coveted "diamond" level within the department store rewards program. This program can only be used by Jane and does not extend to her family or friends. Upon arrival, the department store has placed a kiosk by the entrance that uses facial recognition. Once Jane scans her face at the kiosk, the facial recognition platform sends a request in the form of smart contract to Jane for the purpose of validating that she is who the store believes her to be. Jane opens her DID wallet and accepts the request for credentials from the department store. Within 30 seconds, Jane is greeted by a store employee that has all her buying data and preferences loaded on their smart tablet. Jane enjoys her personalized concierge for the remainder of her visit.



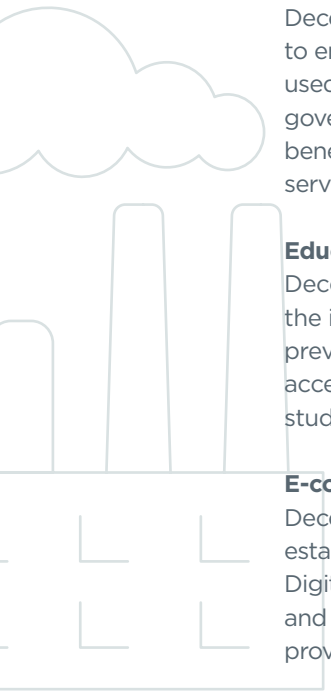
Personal Identification:
John is finally getting some rest and relaxation from an exhausting military career and is traveling to the mountains of Colorado. At the airport in Los Angeles, John wishes to validate his ID with the airport security and flight staff. While proud of his military career, John does not like to draw attention to himself or discuss his time in service. At the security scanner, John is prompted to provide his Digital ID wallet. John has decided to provide his name, picture, and date of birth, height and weight information, but nothing further. Because his California License has been verified by the California Department of Motor Vehicles, the airport security platform accepts his credentials allowing him to proceed to his gate.

Employment:
John is a contract worker at a large hospital. He needs to present valid credentials every day before he starts his shift. Traditionally, John shared his personal information via physical documents. By transforming from a "paper trail" to a digital platform, John started using digital credentials. With blockchain for workforce verification, the hospital can ensure a zero-trust approach for tasks such as employment verification, credit history, criminal records, education, and more. This we call zero-trust security for the workforce. Every day, each user is authenticated across all the critical credentials they own, ensuring safer more secure access.

Data Storage:
Distributed storage or dStorage is increasing in popularity. Code storage within smart contracts on platforms such as the Ethereum chain is steadily growing. While there is concern around the capable storage size of the chain, smaller distributed use cases such as decentralized identification (DIDs) are perfect for today's blockchain ecosystem. Because a decentralized identifier is a unique set of numbers and letters that identifies

an identity in a verifiable and decentralized way, just like a fingerprint does for a person, dStorage functions allow individuals to gather and secure their own information while controlling data sharing.

The data stored on the blockchain is referred to as "on-chain". Conversely, data stored off the blockchain is referred to as "off-chain". With DID's, on-chain dStorage stores only the transactions made between the individual and the share-to entity. The personally identifiable information (PII) is stored by the user or app in an encrypted form using protocols such as IPFS (InterPlanetary File System), JSON-LD (linked documents) or JWT (JSON Web Tokens). Worth noting here is that a blockchain component is not required but compatible with DIDs and decentralized digital identities.



Government Services:
Decentralized digital identity is gaining momentum with the government sector. It is used to enable secure interactions between citizens and the government. Digital identity can be used to verify the identity of participating citizens and authenticate them when they access government services online. This includes everything from filing taxes to applying for social benefits. Digital identity also enables governments to provide more efficient and effective services to citizens.

Education:
Decentralized digital identity is transforming the education sector. It is used to verify the identity of students and faculty, enable secure access to educational resources, and prevent cheating. Digital identity is used to authenticate students and faculty when they access online courses and educational resources. It also enables institutions to track student progress and provide personalized learning experiences.

E-commerce:
Decentralized digital identity is reducing friction in the e-commerce sector. It is used to establish trust between buyers and sellers, prevent fraud, and protect personal information. Digital identity is used to verify the identity of buyers and sellers, authenticate transactions, and protect payment information. Digital identity also enables e-commerce platforms to provide more personalized and secure experiences to their customers.

Financial Services:
Decentralized digital identity is building trust in the financial services sector. It is used to establish the identity of customers and prevent fraud. Financial institutions use digital identity to verify the identity of their customers, perform customer due diligence, and monitor transactions for suspicious activity. The use of digital identity also enables financial institutions to comply with anti-money laundering (AML) and know-your-customer (KYC) regulations.

Healthcare:
In the healthcare sector, digital identity is used to protect patient information and ensure privacy. Digital identity is used to authenticate users, including patients and healthcare providers, and grant them access to electronic health records (EHRs). Digital identity enables secure sharing of patient information between healthcare providers, which improves the quality of care and reduces medical errors.

Conclusion

In conclusion, decentralized digital identity is becoming increasingly important in various domains where it matters. From financial services to healthcare, government services to education, and e-commerce, decentralized digital identity is used to establish trust, prevent fraud, protect personal information, and enable secure interactions online. As the use of digital technologies continues to grow, the importance of decentralized digital identity will only increase. It is important for individuals and organizations to understand the importance of digital identity and take steps to protect it. This includes using strong passwords, enabling two-factor authentication, and being vigilant against phishing attacks. By working together to protect digital identity, we can create a more secure and trusted digital world.

Links
https://www.w3.org/TR/vc-data-model/#abstract
https://identity.foundation
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5cxkr?culture=en-us&country=us


Username
****
Touch to unlock