A Peek into the Future of Decentralized Identity (v2)

Leo Sorokin

Table of Contents

Abstract

As digital transformation sweeps across the globe, it has affected everyone – from citizens to employees, from corporations to governments. Digital identity is a foundational enabler for business processes in the digital economy. Decentralized identity is the next evolution of digital identity capabilities and brings with it an opportunity to streamline how people interact with other institutions, physical objects, and with one another. This paper considers the future world of decentralized identity and offers clarity around the benefits of decentralized identity, terminology, sample scenario, and a sample technical implementation, while also addressing some of the limitations of this model. This paper further grounds the reader in the current state of decentralized identity capabilities while outlining the evolution of identity practices from past to present.

Introduction

Digital identity is rapidly gaining criticality in our world as organizations digitally transform. Identity plays a pivotal role in a digital transformation and can empower both governments and businesses to provide secure whilst restricted access to data for any stakeholder whether employee, partner, customer, or citizen. Digital identity is becoming a vital component of security in a world with data proliferation on a myriad of devices and a network perimeter that is ever-more challenging to define.

One active area under development in the identity space is the concept of *decentralized identity*. Decentralized identity is a fundamental shift from *account-based credentials* toward *verifiable credentials* and is a major philosophical as well as technical change in the way identity-related information is acquired and presented. The World Wide Web Consortium (W3C) is working on publishing standards around *Verifiable Credentials* and *Decentralized Identifiers*.[i],[ii] However, as with any technology standard, it must be broadly adopted by the community for it to be useful at scale.

Today, a person's digital identity (and associated personal data) is strewn across many online services, with access to such services being primarily performed via a username and password. Such an account-based credential is usually provisioned directly by the service provider, or by a large and rather centralized identity provider (IdP), such as Google, Facebook, or Twitter with which a service provider application will federate. This account-based federated model, however, has some significant limitations: the IdP may stop offering its services to third-parties; the identity supported by this IdP may be compromised thus impacting every service provider application that uses that identity; the IdP may track an individual's activities across multiple services; and an IdP may decommission the account being used for authentication. There are many challenges with the federated identity model, but going back to identity silos where each service provider provisions and manages its own set of credentials for its users, resulting in users having to manage dozens of such account-based credentials is not ideal either.

Decentralized identity strives to place the individual at the center of digital identity experiences by attempting to insert the individual at the center of identity data exchange. At its simplest, decentralized identity attempts to map physical wallets and the physical cards within them to a very similar concept in the digital world – a digital wallet with digital cards.

Today, there are many that are very excited about the potential of this model as well as many that are skeptical. Although decentralized identity and the concepts underpinning it attempt to solve the challenges we have had with digital identity over the past few decades, it is still too early to predict how individuals, governments, and corporations will approach it, and how each of these actors will be able to derive value from it.

Decentralized Identity Benefits

A decentralized identity system can be used to replace a traditional username and password during a typical *authentication* sequence. This is perhaps the first use-case most will think

about. However, authenticating in a passwordless manner is possible today even without any decentralized identity components. As such, the true value of decentralized identity can be more easily understood during *authorization*. During authorization, the service provider may mitigate risk by requiring the individual to present one or more digitally signed attestations commensurate with the level of risk that specific transaction entails and the level of value being obtained. This capability could be leveraged to increase trust between the parties, improve the user experience for the individual, while at the same time lowering costs for the business.

The purpose of decentralized identity is to empower individuals to own and control their digital identity and how their identity data is accessed and used. The premise behind decentralized identity decouples it from the notion of a username and password or the traditional account-based model. A digital identity is not yet another username and password-based account that is provisioned and maintained by a third party. With a decentralized identity model, the individual can be both authenticated and authorized to perform a transaction with one service, and then present the same identity information to another entity with which the individual might prefer to interact. In addition, the individual can become their own identity provider, which is more difficult to accomplish with the centralized or federated models we have today.

Decentralized digital identity and the *personal data* associated with it should enable the individual to have more control over how that data is accessed and used. As a byproduct of this philosophy, personal data should be presented by the individual to service providers on an as-needed basis, with specific terms of use. This principle is fundamental to decentralized identity. In a decentralized identity ecosystem, there is no one single central authority; value is exchanged in a more peer-to-peer manner. Since the individual controls and owns their personal data, they are the ones to enable other parties to access it by granting them specific permissions. This is in stark contrast to today's reality where personal data may be shared and stored by third parties outside the individual's control with the individual having no means of specifying the terms of use under which the identity-related information is shared.

In a decentralized identity environment, it may be possible to possess a digital card for a drivers' license, credit card, or even a passport, and have them available on a mobile device. In another scenario, it may help when traveling abroad while having to visit a doctor. Today, it would be very cumbersome and not practical to share medical history and medications with a doctor, other than through a simple verbal explanation. However, with a healthy decentralized identity ecosystem of issuers and verifiers, it would be possible to share important medical information in a digital privacy-preserving manner, thus enabling the doctor to make a better medical decision and provide the patient with a much better service. An additional example is a mortgage lender that may need the homeowner to provide proof of active property insurance. To that end, the homeowner can present the property insurance information to the mortgage lender and the lender can periodically verify the current status of the insurance policy on its own without unnecessarily burdening the homeowner with having to constantly present this documentation to the lender for verification on a recurring schedule. While centralized or federated identity might also support these use cases, decentralized identity might be better suited for them.

Decentralized identity may enable new business models and value exchange. It may pave the path for fully digital-only experiences that remove the requirement for individuals to present themselves in-person to perform high value transactions. Decentralized identity may also enable a better in-person user experience in a variety of situations without requiring a person to carry a physical wallet at all. There are also potential benefits for businesses to streamline how they might verify and build trust with their customers. There is definite potential here, but only time and the market will tell if the great expectations for decentralized identity will be fully realized in practice over the long term.

Decentralized Identity Terminology

The following are the primary components involved in a decentralized identity experience. These definitions have been simplified to make it easier to understand the actors and how they interact:

- *Self-sovereign identity* is a term that describes a digital movement that is founded on the principle that an individual should own and control their identity without the intervening administrative authorities.
- *Verifiable credentials* are attestations that an issuer makes about a subject. Verifiable credentials are digitally signed by the issuer.
- *Issuer* is the entity that issues verifiable credentials about subjects to holders. Issuers are typically a government entity or corporation, but an issuer can also be a person or device.
- *Holder* is the entity that holds verifiable credentials. Holders are typically users but can also be organizations or devices.
- *Verifier* is the entity that verifies verifiable credentials so that it can provide services to a holder.
- *Verifiable presentations* are the packaging of verifiable credentials, self-issued attestations, or other such artifacts that are then presented to verifiers for verification. Verifiable presentations are digitally signed by the holder and can encapsulate all the information that a verifier is requesting in a single package. This is also the place where holders can describe the specific terms of use under which the presentation is performed.
- *User agent* or *digital agent* is the software application that holders use (typically a mobile device app) that receives verifiable credentials from issuers, stores them, and presents verifiable credentials to verifiers for verification.
- *Identity hub* or *repository* is the place where users can store their encrypted identity-related information. An identity hub can be anywhere – on the edge, on the cloud, or on your own server. Its purpose is to store personal data. Some implementations may allow other entities to access the identity hub of the user if the user specifically grants such access. You can think of an identity hub as the individual's personal data store.

- *Decentralized Identifier (DID)* is an identifier that is created and anchored in a decentralized system such as a blockchain or ledger and can represent any entity in the ecosystem – an issuer, a holder, a verifier, and even an identity hub.
- *Digital cards* represent verifiable credentials that users collect over time and are stored as part of the user agent or the identity hub of the user. It's somewhat simpler to refer to them as digital cards rather than verifiable credentials when speaking about them.
- *Digital wallet* represents a digital metaphor for a physical wallet and is generally represented by the combination of the user agent and the underlying capabilities of the computing device, such as secure storage and secure enclaves on a mobile phone. The digital wallet contains digital cards.
- *dPKI* is a decentralized public key infrastructure and is usually implemented via an immutable blockchain or ledger – a place where DIDs can be registered and looked up alongside the associated public keys of the DID and its metadata. dPKI can be described more generally as the *verifiable data registry*, as the dPKI is just one of many possible implementations for a verifiable data registry. While this paper refers to dPKI, the reader should be aware that a verifiable data registry need not necessarily be "decentralized".
- *Universal resolver* is an identifier resolver that works with any decentralized identifier system through DID drivers. The purpose of a universal resolver is to return a DID document containing DID metadata when given a specific DID value. This capability is very useful because DIDs can be anchored on any number of disparate dPKI implementations.

The figure below highlights some of the terminology just outlined with the major actors and their relationships. It also represents the sample scenario we will cover later in this document.

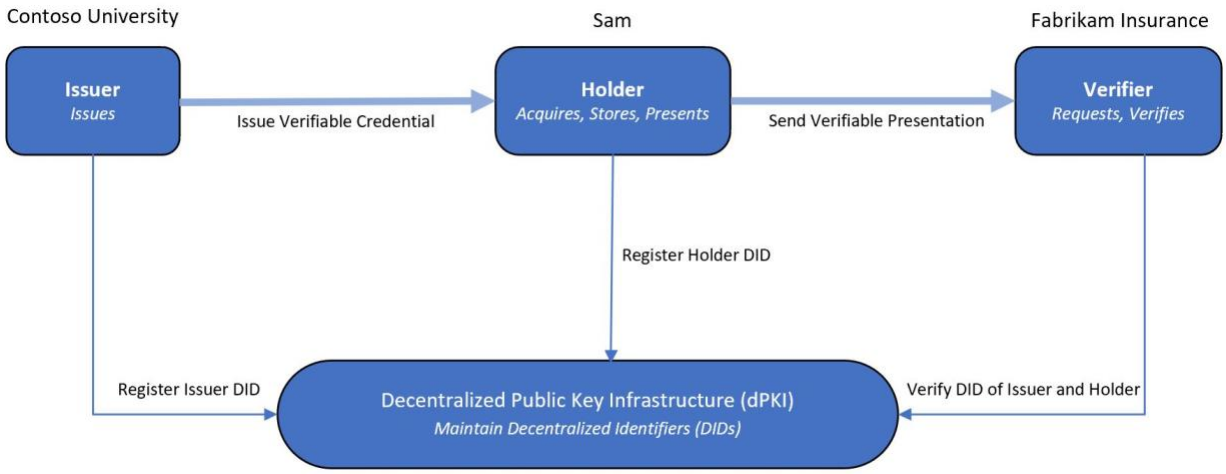

Figure 1 - Verifiable Credential Issuance and Presentation

It is essential to note that no personally identifiable information should be stored on the decentralized public key infrastructure. Personal identity data is stored as part of the individual's digital wallet or identity hub in a secure location.

Usually, the holder will present verifiable credentials to verifiers during a business transaction in real-time, like the way we currently present our passport at a border crossing. However, in more advanced scenarios, some implementations may enable the holder to grant a verifier-specific access to data in the holder's identity hub. That way, the verifier can access data that the individual has allowed access to, instead of the individual having to manually present verifiable credentials to the verifier on a recurring schedule. Nevertheless, the more traditional approach still requires the holder to present verifiable credentials to the verifier explicitly, but the verifier will have the ability to periodically check the status of the credential, such as whether or not the credential has been revoked by the issuer, on its own without burden to the holder.

Now that you are armed with an understanding of the terminology, let's take a closer look at a sample scenario.

Decentralized Identity Scenario

The example below is meant to provide an end-to-end use-case of the value and utility of a decentralized identity ecosystem. It is not a comprehensive or exhaustive description of all that is possible with decentralized identities as it represents just one possible decentralized identity flow.

Suppose Sam wants to purchase vehicle insurance from Example Insurance, but to get a good rate, Example Insurance requires proof that Sam is a graduate of ABC University. In our decentralized identity scenario, the actors are as follows:

- Sam as the verifiable credential subject and holder.
- ABC University as the verifiable credential issuer.
- Example Insurance as the verifiable credential verifier.

The following sequence of steps represents a flow where the end-goal is for Sam to receive a digital diploma from ABC University and then present it for verification to Example Insurance in order to claim the automobile insurance discount:

1. Sam receives an email from ABC University congratulating Sam on graduating while also providing a QR code Sam can use to scan with Sam's mobile phone. Sam has an app on Sam's phone that is registered to handle such a request. This app represents Sam's *digital wallet* that will hold all the *digital cards* that were collected over time. Sam scans the QR code, the digital wallet app launches, and Sam is informed that in order to receive Sam's digital diploma Sam needs to sign-in to the ABC University website.

2. In our case, Sam presses on the link and enters Sam's existing credentials to authenticate on the University's website or if Sam didn't have such a credential, Sam may be asked to come in person to the registrar's office to do ID proofing and receive their credentials. Once Sam provides their existing credentials, Sam is informed that Sam can go ahead and *accept* this digital card from ABC University. Once Sam accepts the card, Sam is asked to secure this operation with a biometric, such as a fingerprint, face, or even a PIN. After Sam performs this action, the card is now securely stored in Sam's digital wallet. Sam can inspect the card, view the data that the card has about Sam (which was attested to by the university), such as Sam's full name, major, graduation date, and issue date. Also, Sam can view the activity that this card was involved in, such as when it was issued, to whom it was presented, and how it was used - all of this can be done from the digital wallet app on Sam's phone. Each such activity can be considered as a *digital receipt* or *verifiable history* that Sam can use to track who has (or had) access to the data for this card. These digital receipts are stored locally along with the card in Sam's digital wallet, which is always under Sam's control. More generally, we can also refer to this digital card as a *verifiable credential*.

3. Now, to claim Sam's discount, Sam navigates to the Example Insurance website on Sam's mobile phone and notices the *Verify Credentials* button. This is a deep link and when Sam presses it, the digital wallet app opens with a permission request. The permission request indicates that Example Insurance needs to receive a ABC University alumni digital card for Sam to get Sam's discount. Note that Sam doesn't have to authenticate to Example Insurance with a username and password nor use a federated IdP. Sam can simply present the digital diploma Sam already possesses in Sam's digital wallet. In our scenario, Sam only presents Sam's ABC University alumni digital card to Example Insurance, but Sam could also present other digital cards Sam has in Sam's digital wallet such as a digital card that proves Sam is a resident of a specific territory or to prove Sam's current address. Once Sam authorizes the permission request with Sam's biometric such as a fingerprint scan, Example Insurance now receives the digital card and is able to verify that it was indeed issued to Sam by ABC University, and it is indeed Sam who is presenting this digital card to Example. Once Example Insurance completes the verification, it can now offer a discount to Sam! Sam can now view that Sam's digital wallet app has a receipt for this card, indicating that this card was presented to Example Insurance on a given date and for a specified purpose with Example's terms and conditions. Some implementations may further enable Sam to *revoke* the access Example Insurance has to view Sam's digital card. This revocation action may generate another *receipt* that clearly indicates the date and time Sam revoked Example's access to Sam's digital card. Once again, Sam can accomplish all this from Sam's digital wallet app on Sam's mobile phone, and all the digital cards that Sam collects over time and Sam's associated receipts are under Sam's control.

4. Sam can collect many such digital cards in Sam's digital wallet and at some point may even need to present multiple cards, such as in the case if Sam wants to attend an advanced enterprise architecture training academy, both proving Sam is a ABC

University alumni as well as a certified enterprise architect. The academy can then instantly verify both credentials presented and enable Sam to access Sam's advanced training material.

It is important to clarify that Sam sends a *verifiable presentation* to Example Insurance. The verifiable presentation contains a nested artifact which is the *verifiable credential* Sam has received from ABC University. In this manner, Example Insurance that is acting as the verifier, can verify the following two critical elements:

- Based on the digital signature of the *verifiable credential*, Example Insurance verifies that the verifiable credential is authentic and was indeed issued by ABC University to Sam
- Based on the digital signature of the *verifiable presentation*, Example Insurance verifies that it is indeed Sam who is performing this credential presentation

After Example insurance has verified the above, it is able to confidently present Sam with Sam's vehicle insurance discount.

Decentralized Identity Technical Implementation

The following sequence is a technical explanation of the same scenario presented above. It outlines the steps that must be taken to setup the decentralized identity experience as well as the verifiable credential issuance and presentation flows. However, this scenario assumes that the decentralized public key infrastructure (dPKI) has already been setup and will not be detailed here.

Setup

1. ABC University represents the issuer. A generates a decentralized identifier (DID) tied to a public/private key pair and registers their DID on the dPKI. The private key is stored by the ABC University IT team in a Key Vault or Hardware Security Module. The corresponding public key is published to a decentralized ledger such as a blockchain so that anyone can find it.

2. ABC University IT publishes a DID document that associates its DID to the registered public Domain Name System (DNS) domain, such as A.edu. This represents a domain linkage verifiable credential. ABC University IT can host this file on their website which both proves ownership of the domain and the specific DID. The verifier (such as Example Insurance) can use this DID document to confirm the DID ownership for ABC University and ensure that the verifiable credential it receives is indeed issued by ABC University and not by some other issuer claiming to be ABC University.

3. ABC University IT develop a contract that describes the requirements for the issuance of the verifiable credential. For example, ABC University IT can specify which attestations should be self-issued directly by the user, and which other verifiable credentials, if any, the individual must first provide. In our scenario, the IT team has mandated that the

student authenticate with a federated IdP that supports the OpenID Connect protocol, so that it will be able to receive a security token and extract claims from it, such as first name, last name, and student number. The issuer will then be able to map it to attributes it will issue in the verifiable credential. Importantly, ABC University will indicate the schema(s) to which the verifiable credential will conform, so that other verifiers around the world will be able to consume the content of the verifiable credential those verifiers receive.

4. Finally, ABC University IT administrators can setup and customize the branding of the soon-to-be-issued verifiable credential cards such as card color, logos, icons, images, and helpful text. The administrators can customize the helpful text strings via metadata that will appear as part of the cards based on the attestations issued with the card for credential data. This will help design the look and feel of verifiable credential alumni cards issued by ABC University, and ensure the issued digital cards reflect the brand of the university. In the future, these graphical elements should be standardized so that students enjoy a consistent digital card visual rendering experience regardless of which vendor develops the user agent or digital agent the student chooses to use.

Verifiable Credential Issuance

1. The credential issuance request flow begins when Sam scans a QR code using Sam's mobile phone. The purpose of the issuance request is for Sam's user agent to retrieve the requirements for credential issuance as dictated by the issuer and to display the appropriate UX to the user via the user agent. As such, the QR code is displayed on the ABC University website and scanning the QR code opens Sam's digital wallet mobile app and triggers an issuance request retrieval operation from the user agent to ABC University. Once the user agent receives the issuance request from ABC University, it begins the flow to issue the credential. The issuance request is digitally signed by ABC University and the user agent can verify the authenticity of such a request. The issuance request includes a reference to the contract that describes how the user agent should render the UX and what information Sam needs to provide in order to be given a verifiable alumni credential.

2. After the user agent verifies that the request is genuine, it renders the UX to Sam. Because of the specific requirement that A has for issuing digital alumni cards in our scenario, Sam needs to sign in with Sam's existing ABC University account, which, in turn, will issue a security token to the user agent with claims such as Sam's first name and last name, degree, and graduation date. (Note that during setup above, the issuer can be configured to accept security tokens from any trusted and compliant OpenID Connect identity provider and the user agent will use this identity provider during the issuance process.) Therefore, when the individual presses 'Login to ABC University' on the user agent, the user agent can redirect the individual to authenticate with the IdP, and it is there the individual can perform standard authentication tasks such as entering their username and password, performing Multi-Factor Authentication (MFA), accepting

terms of service, or even paying for their credential. All this activity occurs on the client side via the user agent (e.g., a mobile app). When the user agent finally receives the security token from the IdP, it can pass it along to the issuer which can then extract claims from it, as mentioned above, and inject these as attributes into the resulting verifiable credential, potentially enriching the claims with information obtained from other sources. As well, after the individual authenticates with the IdP, the user agent can display additional input fields that the individual is free to self-select. After the individual has provided all the required information, the user agent can verify that it has all the necessary issuer requirements fulfilled, and it can go ahead and ask if Sam would like to accept the card.

3. In our scenario, when Sam accepts the card, Sam is asked to use a biometric gesture such as a fingerprint scan. This action generates a private/public key pair for Sam's DID whereby the private key is stored on the mobile phone in a secure enclave, and the public key is published to a distributed ledger.

4. Finally, the issuer receives all the required information alongside Sam's DID and issues the digital card to Sam who then receives the verifiable credential, which is a JSON Web Token (JWT) following the W3C standard for verifiable credentials. The JWT includes both the DID of the subject, Sam, and the DID of the issuer, ABC University, as well as the type of the credential, and any attestations such as first name, last name, major, and graduation date. It also contains a way to find out the credential's revocation status in case the credential is later revoked by the issuer - ABC University. This verifiable credential is digitally signed by the issuer's DID.

5. Once the user agent validates the verifiable credential received from ABC University, it inserts this digital card into Sam's digital wallet as a card Sam can now present to other organizations such as Example Insurance.

Verifiable Credential Presentation

1. When Sam visits the Example Insurance website on their mobile phone to receive a discount on their vehicle insurance, Sam presses the 'Verify Credentials' button on the Example website (which is a deep link) or simply scans a QR code generated by Example via their mobile phone. This generates a presentation/verification request for Sam to verify Sam's ABC University alumni status. The request describes the type of card(s) that Sam should present to Example Insurance, such as Sam's digital alumni card from ABC University, and this request is digitally signed by the verifier's DID, which in our case, is Example Insurance. The presentation request can also include Example's terms of service.

2. After the signature of the request is verified by the user agent, Sam is presented with a UI on the user agent indicating that Example Insurance is requesting permission to see

Sam’s ABC University alumni card with a reason as to why Example needs to see it (such as for Sam to be able to receive their discount).

3. After Sam approves the request with a biometric gesture, such as with a fingerprint scan on the mobile phone, the verification response, which is essentially a presentation of a credential response (also known as a verifiable presentation), is sent to Example Insurance. The response is signed by Sam's private key and includes the verifiable credential issued by ABC University to Sam nested inside the JWT payload.

4. Example Insurance attempts to match the person performing the presentation of the credential with the subject of the nested verifiable credential to ensure that it is indeed Sam who is presenting it to Example Insurance, and not anybody else. Therefore, the DID of Sam is present in both the outer JWT payload since Sam is performing the presentation of the credential, as well as inside the nested JWT payload as the subject of the verifiable credential issued by ABC University. Once Example Insurance confirms that the DID in the presentation matches the subject of the issued credential, Sam is both authenticated to the Example Insurance website and authorized to claim Sam’s discount! This is much better than simply possessing a username and password, since, in this mechanism, Example Insurance knows that the person presenting this credential is the same person to whom the card was issued. With a username and password, someone else can use it to impersonate you. In this architecture, however, this is significantly harder to do. Someone else will need to take control of Sam's private key stored on Sam’s phone's secure enclave to be able to accomplish this malevolent task.

5. At last, Example Insurance can extract the data it requires from the verifiable credential such as Sam's first name, last name, major, graduation date, and go ahead and present Sam with Sam’s vehicle insurance discount!

6. The credential verification flow completes when Sam stores a signed receipt by Example Insurance that will be associated with the card in Sam’s wallet. Sam now has a single place where Sam can view all the websites where Sam has presented Sam’s alumni card over time. In our scenario, the receipt includes information about Example Insurance, the reason Example needed to receive the card, Example's terms and conditions, and the date the receipt was generated. This signed receipt is associated with the card in Sam's digital wallet and will always be under Sam's possession.

7. Some implementations may further enable Sam to go ahead and decide to revoke Example's access to Sam’s ABC University digital alumni card. Example should thus implement the necessary revocation measures to ensure it complies with Sam's request. The verifier should then cease to use the data from the card Sam presented to it. Sam can later prove that Sam issued a revocation request if such a need arises, and this can help with General Data Protection Regulation (GDPR) compliance.

Scenario Summary

In our simple use-case above, the issuer of a verifiable credential was ABC University, but in other contexts, the issuer can be an employer, a government agency, a device, a daemon process, or even the individual. Likewise, a verifier can also be any of the previously mentioned actors. The decentralized identity ecosystem is very broad and the standards allow for opportunities to unlock a more flexible, secure, and privacy-preserving way to perform digital interactions in a myriad of contexts.

The components presented in the flow above are based on open standards. The verifiable credentials issuance and presentation flows depend on the foundational specification of the *W3C Verifiable Credentials Standard*, and the decentralized system, such as blockchains and ledgers, are based on *W3C Decentralized Identifiers* work. The purpose of the decentralized ledger technology is to support a decentralized public key infrastructure (dPKI). The dPKI anchors DIDs and their public keys and thus enables ownership of DIDs to be validated without relying on only a few privileged identity providers or certification authorities.

The Decentralized Identity Foundation is leading the effort on decentralized identity, but more work remains to fully define the space.[iii] For example, the decentralized identity community is discussing how to enable better privacy preservation by empowering Sam to present Sam's age in a privacy-preserving way without unnecessarily disclosing Sam's exact date of birth to the verifier. Another area under discussion is how to empower Sam with performing self-owned key recovery in case Sam loses or damages Sam's phone, so that Sam can more easily retrieve all Sam's previously acquired digital cards back onto a different device or onto a different user agent in a more seamless manner.

Decentralized Identity Limitations

While decentralized identity has the potential to improve an individual's productivity and digitize existing business processes for governments and corporations, it does have known limitations and areas where further research or investigation would be required. A decentralized identity ecosystem can only be successful when it achieves critical mass adoption by governments, businesses, and individuals. When Apple released the first iPhone, it ushered in a new and immediate change in the user experience the moment the purchaser took possession of their new device. In contrast, an individual may not gain much benefit in obtaining a verifiable credential from an issuer unless they can then use that verifiable credential with many verifiers. A digital passport, for example, is only useful to a citizen if it can be used at most airports and border crossings around the world. Organizations may hesitate to be issuers or verifiers of verifiable credentials unless there is already a healthy ecosystem in place, but that ecosystem cannot develop unless there are entities willing to issue and verify these new credentials.

Decentralized identity is a digital identity. Without the necessary technology to hold a digital wallet, such as on a mobile phone or some sort of computing device, it will be very difficult for

the promise of digital identity to be realized by all individuals around the world. If an individual loses their device or decides to share their device with others without proper precautions, it can become a challenge to recover their data onto a different device or to prove who performed a specific interaction. Asking the average person to understand this and to safeguard their private key material remains a significant challenge to decentralized key management.

In most decentralized identity use-cases, the developers assume all parties involved have access to the Internet. That may not be the case. Other scenarios that take the individual away from Internet access leave open the question of how verifiable credentials can be verified in such scenarios. Verifying verifiable credentials requires looking up information on the dPKI, or at the very least, checking if a credential that is being presented has been revoked, and that requires network connectivity. In purely disconnected offline environments this poses a challenge, and a potential hurdle to decentralized identity adoption in specific contexts and situations.

The promise of decentralized identity is to empower individuals to own and control their digital identity and personal data. However, if a person provides a verifiable credential containing personal data to the service provider, the service provider is able to copy this data to its own databases for marketing purposes or to be able to continue providing services to the user. The individual can attempt to revoke access that the service provider has to the verifiable credential but there is no guarantee that the service provider will honor such a request and delete all the data it has stored about the user. This would be a very challenging problem to solve via strictly technological measures and would most likely require legal and policy frameworks in place to ensure everyone's personal data is protected, to ensure audit records are kept, and to establish a documented process for dispute management and resolution.

Final Words

Decentralized identity can enable entirely new business opportunities and empower citizens to be more in control of their identity and personal data. Today, IT administrators need to perform cryptographic key exchange ceremonies to establish trust between two organizational entities. This does not scale when doing business with dozens or perhaps hundreds of other vendors in a more ad-hoc manner. Today, when a bank issues a credit card to a customer, that customer can use that credit card to make purchases with almost any merchant worldwide. In such a scenario, it is not feasible to expect every merchant to exchange cryptographic keys a-priori with every possible bank that issues credit cards. A decentralized identity ecosystem can enable a similar concept to credit card associations by introducing governance authorities and frameworks for many different trust communities in a wide array of industry verticals. As a result, merchants, or other verifiers, can avoid setting up multiple trust federations – they can simply ask the issuer to present additional proofs proving that the issuer is indeed a member of a specific governance authority with which the verifier already has an established trust relationship.

One of the major hurdles for adopting blockchain today in enterprise scenarios is the lack of a decentralized identity infrastructure. After all, it's not very logical to have a decentralized blockchain network if all the identities on it are still relying on centrally controlled accounts. Furthermore, in a decentralized identity ecosystem, consumers will be more easily able to track which websites they visit online and with whom they transact. You will know which businesses have your personal data, and you will be able to revoke access to it should you so desire. Instead of sharing paper documents or physical cards, you will be able to share digital documents and digital cards in a fully digital, privacy-preserving, and auditable manner. For organizations, this may reduce GDPR-related risk since personal data will be stored in the identity hub under the individual's control, while the organization will only have access to specific data as granted by the user. Furthermore, the individual may have the opportunity to revoke access to their data, and this may simplify the GDPR compliance for an organization as well as streamline such requests for the individual. As well, GDPR compliance may be eased for an organization as it will be able to possess cryptographic proof as evidence that the individual has indeed provided them with specific data.

As discussed, the digital wallet contains a digital agent app with which the user interacts. Such digital or user agents are mostly based on open source software. The individual can download a user agent from a commercial corporation, or perhaps even a government entity. An individual may even develop their own user agent from existing open source software. Conceptually, an individual must trust the user agent and it should be under the individual's control.
While it is extremely challenging to attempt to predict how the decentralized identity landscape will evolve given its nascent state, current trends are indicating government interest to ease the burden on citizens and businesses via government-issued digital IDs. Tailwinds from the unprecedented global COVID-19 pandemic are urging government institutions to streamline citizen and business access to government-provided services. As well, increasingly stringent regulatory compliance requirements and further demand by users for better user experience and increased convenience may further drive demand for digital identity in the form of verifiable credential exchange. Finally, verifiable credentials may prove very useful in situations where the same credential must be presented both online in digital transactions as well as in offline in-person interactions, since this can result in increased business efficiencies for the enterprise and a more consistent and simplified user experience.

Conclusion

Decentralized identity is a conceptual shift from the way the identity and access management community has been approaching identity in the past, yet it is able to co-exist with the account-based identity model that has existed for decades. Decentralized identity can add a lot of value to transactions that require high assurance of trust to make authorization decisions. If an individual continues to authenticate with a website using a traditional "account", it does not preclude the individual from having to present verifiable credentials in order to, say, transfer large sums of money to another individual or organization. This offers the possibility to unlock a myriad of new opportunities for digital commerce and enable consumers, employees, and citizens around the world to transact on the web in a more secure, safe, and privacy-preserving

manner. It may pave the path for a digital wallet with digital cards, like the way we all use a physical wallet and physical cards today. Verifiable credentials are easy to reason over because many of them will simply be digital representations of the physical cards we already carry in our wallets every day.

We are still at the early days of decentralized identity. It is not a technology that a single company can simply release to the market. It requires both standards as well as collaboration between the private and public sector to have a healthy ecosystem of *issuers*, *holders*, and *verifiers*. When we finally reach critical mass adoption, digital experiences may look and feel much different from the experiences of today. Decentralized identity is an exciting development in the identity space, and it has the potential to offer more trustworthy digital experiences and unlock more value for everyone.

Change Log

Date	Change
2020-10-30	V1 published
2022-02-28, 2023-03-31	V2 Editorial changes only (changed example business names to non-Microsoft specific ones; changed A University to ABC University)

Author Bio

Leo Sorokin has over 10+ years of experience in various solution architecture and enterprise architecture roles with large organizations in the financial, manufacturing, and software industries. He is currently a Cloud Solutions Architect at Microsoft helping the largest Canadian organizations adopt cloud technology. Leo has extensive experience with identity, service-oriented architecture, application integration, cloud-native application and hybrid-cloud architecture, as well as security software architecture. Leo is also TOGAF® 9 Certified, a Microsoft Certified Azure Solutions Architect and holds a Computer Science degree from York University. Leo has also taught technology related courses in several educational institutions.

[i] "Verifiable Credentials Data Model 1.0," W3C Recommendation, World Wide Web Consortium (W3C), 19 November 2019, https://www.w3.org/TR/vc-data-model/.

[ii] "Decentralized Identifiers (DIDs) v1.0," W3C Working Draft, World Wide Web Consortium (W3C), 27 October 2020, https://www.w3.org/TR/did-core/.

[iii] Decentralized Identity Foundation (DIF), [Online]. Available: https://identity.foundation/.