Market Guide for Decentralized Identity

8 July 2024 - ID G00797492 - 23 min read

By Analyst(s): Michael Kelley, Akif Khan

Initiatives: Identity and Access Management; Build and Optimize Cybersecurity Programs

Security and risk management leaders have long been responsible for identity data that is both centralized and federated, but now need to prepare for the democratization of identity data through decentralization. This Market Guide describes key developments and identifies representative vendors.

Overview

Key Findings

- The market for decentralized identity (DCI) will be driven not by economic models or even collections of functionality, but by opportunity cost on a use-case-by-use-case basis.
- The market for digital identity is evolving as more vendors provide products. These range from digital wallets devoted to payments to offerings that support cryptocurrency and verifiable credentials (VCs) containing identity data.
- Some governments are making significant moves toward developing identity wallets, having begun with implementations to track COVID-19 vaccinations and continued by introducing mobile driver's licenses, national ID cards and digital passports. These developments are culminating in a variety of DCI use cases in the public sector.
- Security and privacy for identity data remain lacking.
- Blockchain-based identity and privacy-preserving protocols are becoming viable alternatives to conventional identity and access management (IAM) approaches by including the ability to comply with regulations like know your customer (KYC) and anti-money-laundering (AML) rules.

Recommendations

Security and risk management (SRM) leaders responsible for IAM should:

This research note is restricted to the personal use of dom.wilkins@gartner.com.

- Examine their digital ecosystems for potential optimization opportunities for DCI by identifying existing use cases that could prove more efficient when converted to DCI.
- Narrow their focus on the portable digital identity market by prioritizing DCI approaches to identity data.
- Explore how starting with government VCs and a government-backed digital identity wallet could shorten the time to value for their DCI use cases by using that government's existing DCI infrastructure.
- Prepare for a chaotic period of vendor consolidation in the DCI market by choosing a vendor with a track record of early success in supporting DCI use cases, and be prepared to quickly switch vendors in the event of a business change.
- Explore how DCI can enable compliance with regulations by tracking early developments in the market for KYC and AML DCI use cases and developments in protocols.

Strategic Planning Assumption

By 2026, at least 500 million smartphone users will be regularly making verifiable claims using a digital identity wallet built on distributed ledger technology.

Market Definition

Decentralized identity (DCI) democratizes digital identity by decentralizing both the storage and the use of identity data. The primary benefits of DCI are privacy, anonymity and user autonomy. DCI tools include a trust fabric, typically a distributed ledger like a blockchain; a digital wallet, which is tied to an entity (user); verifiable credentials (VCs), which represent identity attributes used to prove identity claims; and decentralized identifiers (DIDs), which establish pseudonymous relationships for issuing and verifying claims. DCI systems are delivered via software and SaaS capabilities. Users are primarily humans, but machines and even business entities can be users of DCI.

DCI is used for user verification, identifying and tying a physical person to an identity wallet, and for user authentication and authorization, authenticating that user and authorizing them to access resources and data. Unlike conventional approaches, DCI does not use central stores of identity data, instead decentralizing the identity data, relationships between a user and service provider, and verification.

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Current centralized approaches to managing identity data, for example, a corporation storing identity data for employees, or a credit rating company storing identity data for consumers, struggle to provide benefits in three key areas: user experience, assurance (security) and pseudonymity (privacy).

User experience is achieved through using a DCI wallet, which is typically a simple smartphone application. This approach enables users to easily collect, consent and share VCs (which prove requests for information).

Assurance is provided via the integrity of the identity verification mechanisms used in the process of establishing that identity within the network. Realistically, organizations that have a need to establish an identity for interacting with their services can “outsource” that task to the DCI network.

DCI provides privacy for participants, primarily through consent management and through the use of privacy preserving protocols such as zero-knowledge proofs (ZKPs) which provide pseudonymity.

DCI can help to solve problems related to identity verification, account takeovers, fraud, privacy and security. DCI is driven by verifiable credentials, which represent proofs for claims about identity attributes, like employment status, citizenship, or authorizations to access applications and data. But the process of doing this with DCI, compared with the real world, represents magnitudes of improvement in terms of efficiency, cost and assurance.

Must-Have Capabilities

The must-have capabilities for this market include:

- Verifiable credentials
- DIDs, which establish and maintain the relationship between a wallet holder and service provider
- An identity wallet

Standard Capabilities

The standard capabilities for this market include:

- An identity trust fabric, typically a blockchain

This research note is restricted to the personal use of dom.wilkins@gartner.com.

- An interface for issuing verifiable credentials to wallet holders
- An interface for a verifier to validate claims, through verifiable credentials

Optional Capabilities

Some vendors may include optional capabilities like:

- The ability to store and use non-fungible tokens (NFTs), or similar digital documents like smart contracts.
- Identity verification services for initial sign-up and provisioning, as well as recovery services, the ability to recover a wallet and its associated verifiable credentials.
- The ability to store and use mechanisms like educational credentials (e.g., diplomas, degrees), health cards or professional certifications.
- The ability to store and use government-issued mechanisms, such as mobile drivers licenses and digital passports (which aren't verifiable credentials).
- The ability to process payments, or hold and manage cryptocurrency.

- Identity wallets to store VCs.
- Identity trust fabric (almost always a blockchain of some kind), which is used to establish relationships between wallet holders and service providers and to anchor user transactions and interactions.
- Capabilities to issue and verify VCs.
- Support for privacy-preserving protocols such as zero-knowledge proofs (ZKPs) and zero-knowledge claims (ZKCs).

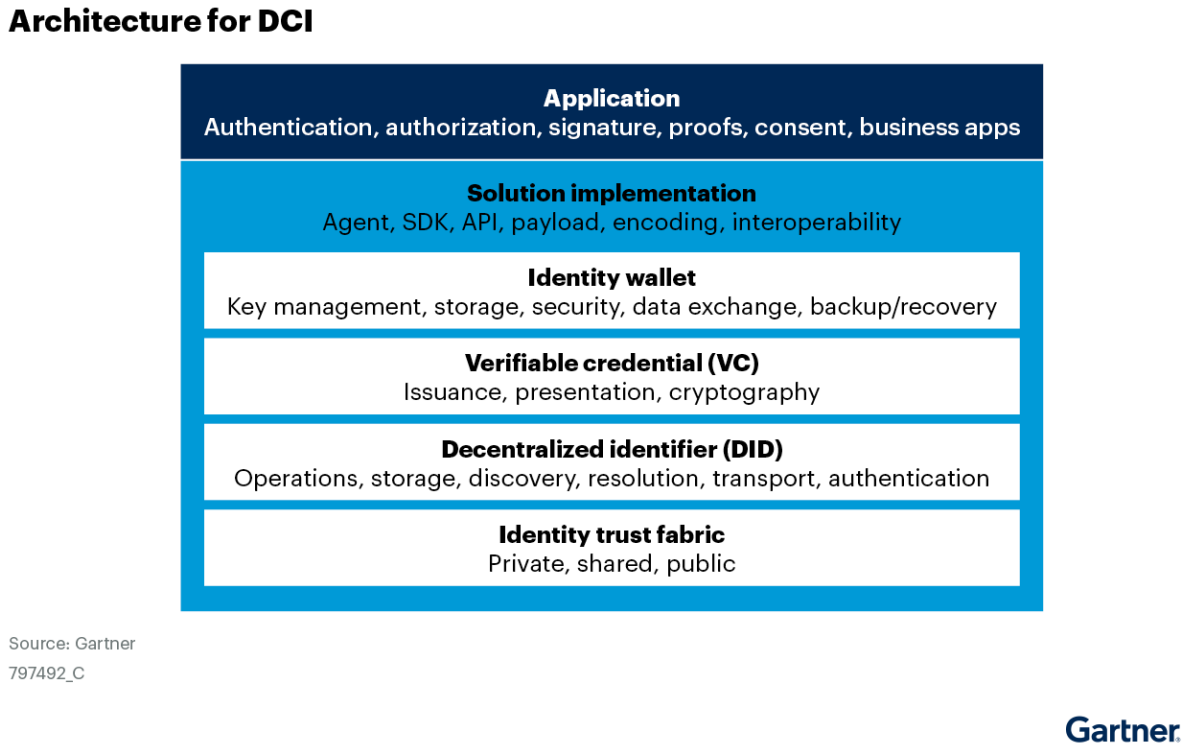
The majority of DCI vendors are still relatively small and focused on trying to address specific use cases and grow their business within specific regions. Several large global vendors have established DCI offerings, but these remain a modest part of their overall product portfolios. As a whole, the DCI market is still young and evolving.

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Nevertheless, degrees of specialization are apparent. Some vendors, for example, focus on building identity trust fabric or individual identity wallets. However, this Market Guide examines only vendors that offer a complete DCI solution with all components (see Note 1). The only possible exceptions to this rule are vendors that build their DCI products on large public-permissioned blockchains, rather than building identity trust fabric entirely on their own; our definition of the DCI market does not exclude them.

Figure 1 shows how key components relate to one another to form an overall DCI architecture.

Figure 1: Architecture for Decentralized Identity



The use cases for which DCI can add value today are broad and varied, ranging from government-citizen to business-customer and employer-workforce interactions. DCI solutions can be used across the typical identity life cycle. Vendors have built solutions that can deliver the benefits of DCI, and are focused on getting traction and multiplying their production deployments.

This research note is restricted to the personal use of dom.wilkins@gartner.com.

DCI or SSI?

The most common descriptors of this technology are self-sovereign identity (SSI) and decentralized identity (DCI). SSI was one of the earliest descriptions of a decentralized approach to identifying and managing identity data. However, user sovereignty is more accurately a benefit of a technology than a description of one. Hence, Gartner uses the term DCI to describe this market and its technologies and products, which provide the benefits of self-sovereignty, privacy, security and autonomy.

Market Description

Vendors in the DCI market are building technology to support the components of a DCI ecosystem, namely:

Market Direction

A Growing Vendor Ecosystem

Several years ago, the DCI market was largely characterized by development activity, with little real-world application. It remains nascent, but is evolving, with interest in DCI's utility fueling the growth of a thriving vendor ecosystem.

At one end of the spectrum are large vendors such as IBM, Microsoft and Ping Identity. At the other end are small vendors with a strong regional focus, such as Nuggets in the U.K. and Hopae in South Korea. Some vendors use open-source alternatives, including Hyperledger Fabric and Hyperledger Indy (donated to the public domain by Evernym).

This range of vendors is indicative of a market with growing investment and a diversified vendor ecosystem that is positioning itself to meet a variety of client needs.

Investment in DCI startups is still small, compared with other markets, however. The startups tracked by Gartner together attract investment of less than $500 million annually. This poses a potential risk to these vendors, given the significant resources available to established IAM companies.

Still, the DCI market's potential is significant. Gartner estimates it will be worth $3.3 billion by 2031 (see Emerging Tech: Revenue Opportunity Projection of Decentralized Identity).

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Use Cases Gaining Traction

Demonstrable production deployments of DCI solutions for a range of use cases are fueling interest in DCI as a way to solve real-world business problems. Examples include the following (note that much of this list derives from media releases by the organizations in question):

- **Government-citizen:**
  - The government of Buenos Aires, Argentina, is offering DCI for citizens, enabling them to use VCs to verify birth and marriage certificates, along with income and academic qualifications.
  - The government of Zug, Switzerland, is using uPort technology to offer DCI for citizen use cases, including signing up for city services.
  - Finland is funding the Findynet Cooperative to build a pilot environment for a DCI network.
- **Business-customer:**
  - Verizon ID is an application for mobile phone users built on 1Kosmos BlockID.
  - To secure transactions and relationships for renters and landlords, Domi Labs is rolling out a DCI platform that uses VCs for interactions.
  - Support for users of training applications is available from organizations like Learning Economy and the Trusted Learner Network.
- **Employer-workforce:**
  - Condatis and Sitekit have used Microsoft Entra Verified ID to create a digital staff passport that is used by hospitals in the U.K. to facilitate ease of movement for medical staff.
  - Microsoft Entra Verified ID is also used by LinkedIn to provide a VC that validates employment status.

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Standards Need to Mature

Immature and inconsistent standards and protocols will negatively impact DCI adoption in the short term, beyond niche use cases. Whereas standards that define DIDs and VCs are on their second and third iterations, newer standards like OpenID for VCs and CBOR (an alternate approach to JSON interactions) are still at the draft stage.

Protocols and standards are needed for nearly every aspect of DCI infrastructure, starting with the "fuel" that runs the "engine" of DCI, DIDs and VCs:

- A standard must be adopted that defines how the market can know that the issuer of a VC is authoritative for that information — for example, a university for an educational credential or a business for validation of employment. One approach might be to use the burgeoning Verifiable Legal Entity Identifier (vLEI) standard, which is gaining limited adoption outside financial sector applications.
- Standards for how VCs are used in traditional IAM applications need to be matured — for example, by using VCs to track authorizations to applications or data. OpenID for Verifiable Credentials has shown promise for some of these use cases.
- No one wallet standard yet exists, which will impede more universal use cases coming to market.
- In government use cases, the EU has jumped ahead with its Electronic Identification and Trust Services (eIDAS) 2.0 standard, ratified in March 2024. eIDAS 2.0 is a wide-ranging piece of legislation that requires digital wallets, VCs and interoperability for all EU countries — features that are uniquely enabled by DCI products.
- Some governments have adopted vendors' approaches to DCI without defining all-encompassing government standards. As noted in the previous section, cities like Buenos Aires and countries like Finland have DCI use cases available.
- VC-like mechanisms are popping up for use in digital wallets. The Mobile Driver's License (MdL) standard, for example, is experiencing increased adoption. The Digital Product Passport (DPP) is another standard that would benefit from being compatible with a DCI wallet. Also, although the craze about non-fungible tokens (NFTs) appears to have given way to the craze about generative AI, NFTs are interesting products that could complement or encapsulate VCs for DCI use cases.

For a representative list of DCI standards, protocols and standards organizations, see Note 2.

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Market Analysis

Use-Case-Driven Growth

The DCI market is not being driven in the way traditional IAM markets have.

The privileged access management (PAM) market, for example, has traditionally been driven by security, audit and compliance concerns, and cybersecurity insurers have recently begun introducing PAM requirements for their customers. The access management market, for its part, is driven by user experience and optimizations.

By contrast, the DCI market is being driven by hundreds of use cases. For these, the approach that DCI offers is based on opportunity cost, and is simpler, quicker, and more secure or more private than the established approach.

The economics of the DCI market are driven by the addition of optimizations and efficiencies to current processes, as opposed to defined IAM projects.

Much as the economics of the cloud drove adoption of software as a service, platform as a service and infrastructure as a service, DCI is largely being driven by the opportunity cost principle of economics.

Consider the use case of validation of employment. Employees need to provide validation of employment in order to request, for example, a line of credit for an automobile or a home loan. This use case has traditionally been addressed using a patchwork of automated and manual systems for answering questions about employment status. Now, however, LinkedIn, working with the Microsoft Entra Verified ID product, offers employers a way to create VCs that employees can request, download to their digital wallets, and provide to an organization seeking to verify their employment — all without the verifier needing to contact the employer. In this way, DCI saves significant amounts of both time and money.

The benefits that DCI promises fall into three categories: privacy, security and autonomy. These benefits are why organizations are interested in DCI solutions, but the favorable economics are why they are investing in them (for a fuller explanation of drivers, see Note 3).

This research note is restricted to the personal use of dom.wilkins@gartner.com.

However, there will be instability in the DCI market. Gartner has identified several hundred vendors that are attracting investment, beyond large, well-known companies like IBM, Microsoft and Ping Identity. As more use cases lead to product sales and implementations, we expect consolidation, with many acquisitions in the next three to five years and some companies, especially newer startups, going out of business entirely. SRM leaders will need to choose a partner carefully for any DCI project, and be prepared to change partners quickly in the event of a major business change.

Banking Regulations: Know Your Customer and Anti-Money-Laundering

Among the earliest challenges for the DCI market, beyond the question of how it can make money selling DCI products, is the regulatory challenge. For DCI to be viable in the financial services industry, it must be able to comply with KYC and AML regulations.

A significant number of vendors claim to have the functionality within their DCI solution to comply with KYC and AML regulations. DCI vendors see this as crucial for making KYC and AML compliance processes more efficient. However, Gartner's view is that, at this time, banks cannot make a good business case for transitioning away from their traditional compliance process, regardless of its inherent challenges. We are aware of, and are tracking, only one experimental use of a DCI solution for compliance in a production environment: HSBC Labs is piloting a DID solution from Polygon ID. To open an account, the bank executes a KYC function and based on that, creates a VC that is issued to the user. This VC can be used for a number of transactions between the wallet holder and HSBC, such as logging in, making a purchase and applying for a loan.

European banking clients are closely watching, and engaging with, the EU's digital wallet program and its implications for KYC and client onboarding. It seems that EU member states may also allow, or ask, private players, banks, telco providers and consortiums to issue wallets.

We are also tracking developments at the Decentralized Identity Foundation (DIF), a standards organization that is developing new DCI schemas for basic KYC and AML.

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Government Involvement

One of the biggest challenges to widespread adoption of DCI is the need to assure the authenticity of a VC by ensuring that the issuer is authoritative for that information. In lieu of concrete approaches and standards for this, governments can provide a shortcut. By default, governments are authoritative for a significant number of identity attributes that might be found in a VC. For example, proof of citizenship supports access to government benefits. Government projects are revealing faster time to value when government agencies represent authoritative sources for specific identity data attributes, providing a kick start to the process of establishing a useful digital identity wallet.

One of the most significant developments is the EU's ratification of eIDAS 2.0. This regulation defines legal requirements for digital identity for EU member states, as well as guardrails and checks and balances. It has been in development for years, during which time vendors have built DCI products in anticipation of the ratification. We expect to see new DCI vendors — who have spent the past few years defining early use cases — involved in eIDAS 2.0 implementations.

Governments could also help the DCI market by virtue of their infrastructure's scale, which could potentially enable a substantial number of use cases. Examples could include identifying emergency responders, providing secure access to benefits, and issuing safe and secure credentials for automobile or home ownership.

DCI for Machines

Although DCI is primarily known for providing benefits to humans, there is also a good case to be made for how it could benefit machines. Traditionally, IAM for machines has suffered from a lack of comprehensive solutions for identification, authentication and authorization. Use of certificates to identify machines has become the de facto standard approach, though other methods do exist. However, using a digital wallet to identify a machine, and using VCs in that wallet to identify, authenticate and authorize the machine for use cases, is a growing use case for DCI. Companies like Peaq Foundation have developed DCI tools for machines to use wallets and VCs.

Looking ahead, other use cases for both the Internet of Things and operational technology (OT) are in sight, as are use cases associated with smart cars, smart houses and manufacturing applications like digital twins. In addition, the EU has developed legislation for DPPs for tracking the product life cycle, and a company called Filancore has developed a management approach to OT environments based on DCI and VCs. All require the ability to effectively identify, authorize and authenticate machine identities, and, at least for newer devices, DCI represents a viable alternative to existing approaches.

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

The listed vendors range from well-established providers with a significant presence in the DCI market, and vendors often mentioned by clients during interactions with Gartner, to smaller, less-often-cited vendors, especially those with fresh approaches to meeting clients' requirements.

Vendor Selection

Table 1: Representative Vendors in Decentralized Identity

(Enlarged table in Appendix)

Vendor Name	Product Name
1Kosmos	BlockID
ATB Ventures	Oliu
Avast	Digital trust
Civic Technologies	Civic ID
Condatis	Condatis Credential Gateway
Digital Bazaar	Veres One
Extrimian	QuarkID
Filancore	Identity Gateway
Finema	thai.ID
Fractal ID	Fractal ID
Gataca	Gataca Wallet
Hopae	DCX
IBM	Hyperledger Fabric
IdRamp	Integrated Identity Service Platform
Indicio	Indicio Proven
InfoCert	eID
Interac (formerly SecureKey)	Interac Verified
Liquid Avatar Technologies	Liquid Avatar Verifiable Credentials Ecosystem (LAVCE)
Lissi	Lissi Identity Wallet
Microsoft	Microsoft Entra Verified ID
Nuggets	Nuggets
NuID	NuID
PARAMETA (formerly ICONLOOP)	MyID
Peaq Foundation	peaq ID
Ping Identity	PingOne Neo
Regov Technologies	myBID
Scytáles	Scytáles Digital Identity Wallet
Sitekit	Sitekit Digital Passport
Sovrin Foundation	Sovrin Network
Spherity	Enterprise Identity Wallet
SpruceID	Digital IDs
Thales	Trusted Digital Identity
UniquID	UniquID
Validated ID	VIDidentity
Veramo (formerly uPort)	Veramo Agent
Veridas	Veridas Nexus ID Wallet
Wipro	Decentralized Identity platform
Wise Security	Definitive ID

Source: Gartner (July 2024)

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Market Recommendations

- The uncertainty about how authoritative issuers of VCs will be validated means that SRM leaders should explore use cases for which governments are the issuers. There is significant activity among governing bodies, which are exploring or developing DCI use cases for citizens. Companies should start their DCI journey by examining what viable government infrastructure exists for DCI, and what initial use cases, provided by governing bodies, can be pursued to shorten their DCI journey. They should also keep track of developments in the field of organizational credentials, such as the vLEI standard from the Global Legal Entity Identifier Foundation (GLEIF), which might solve part of the problem of identifying authoritative issuers of VCs.
- When exploring use cases for DCI, SRM leaders should consider use cases with high levels of opportunity cost — for example, something that currently takes longer, costs more money, and involves more people than would be the case if that use case were addressed by DCI. Examples include validation of employment, remote onboarding, provision of evidence of educational or professional credentials, and validation of the qualifications of people in specific situations (such as first responders and law enforcement personnel at accidents and other crises). Leaders should examine their digital ecosystems for potential use cases for DCI by applying this lens.
- The DCI market is likely to be chaotic for some time, with significant merger-and-acquisition activity, new vendors appearing frequently, and vendors exiting the market unexpectedly. SRM leaders should expect to spend more time vetting potential DCI vendors and proactively charting strategies for pivoting away from failed or merged DCI vendors to maintain progress on DCI projects. They should explore what established vendors in areas like access management have to offer, or have on their roadmaps, in terms of DCI.
- Although regulations were initially expected to erect barriers to the adoption of DCI in heavily regulated industries like financial services, new DCI use cases allow organizations to comply with them. SRM leaders should explore how DCI can enable them to comply with regulations more easily, privately, and securely than conventional means.

Evidence

Over 400 client inquiries and vendor briefings in 2023.

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Note 1: Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.

Note 2: DCI Standards, Protocols and Standards Organizations

Note that the following list is representative, not comprehensive, and that the protocols and standards involved in DCI are still in a state of flux (for a reference source for all current protocols and standards, see Ecosystem Overview, Decentralized Identity):

- Credential Handler API (CHAPI)
- Data Integrity BBS Cryptosuites v1.0, W3C
- Decentralized Identifiers (DIDs) v1.0, W3C
- Decentralized Identity Foundation (DIF)
- Digital Product Passport (EU)
- eIDAS 2.0
- Global Legal Entity Identifier Foundation (GLEIF)
- Interoperability
- JavaScript Object Notation (JSON)
- JSON Web Tokens (JWTs)
- Key Event Receipt Infrastructure (KERI)
- LEI Worldwide (Legal Entity Identifier)
- Linked Data Proofs
- Mobile Driver's License (mDL - ISO 18013)
- Non-fungible tokens (NFTs)
- OpenID for Verifiable Credential Issuance - draft 13 (OpenID4VCI)
- OpenWallet Foundation
- Privacy-preserving protocols (ZKPs and ZKCs)

This research note is restricted to the personal use of dom.wilkins@gartner.com.

- RDF Dataset normalization
- RFC 8949 Concise Binary Object Representation (CBOR)
- Sovrin Foundation
- Trust Over IP Foundation
- Verifiable Credentials Data Model v1.1, W3C
- Verifiable Credentials Status List (VCs)
- WebKMS v0.7

Note 3: Drivers of the DCI Market (Expanded)

The benefits of privacy, security and autonomy drive the growth of the DCI market.

Privacy

Privacy enables consumers to be confident that, even if their personal data were to be released into the world, it could not be used to harm their reputation or financial status. At the heart of DCI are verifiable claims, built on privacy-preserving protocols such as ZKP and ZKC, that ensure only required information can be exposed, such as a person's age. Ensuring a person is of the required age is important in multiple situations (see Emerging Tech: Security — Age Verification and Consent Tracking). A request to verify age typically focuses on validating a minimum age for consuming alcohol, attending a movie with an R14 rating, or playing a game geared to an older audience, for example.

The conventional means of proving minimum age is to expose a document that provides proof of a birthday, such as a birth certificate, driver's license or passport. The verifier uses the birthday and the current date to calculate the person's age. However, this approach exposes far more personal data than is required to prove age.

DCI's privacy-preserving protocols provide proofs for claims about identity attributes, including age. In this case, a query could be sent to a digital wallet holder asking if the holder is at least 21 years old. The subsequent answer, assuming the claim is true, would be a simple affirmation, without providing birth date, address or other details (such as hair color). In this way, privacy of personal identity attributes is both protected and utilized to prove claims about identity.

Security

This research note is restricted to the personal use of dom.wilkins@gartner.com.

The easiest way to understand the security aspects of DCI is to compare how a cryptocurrency, such as Bitcoin, works, with traditional banking. Traditional, central banking systems manage the financial assets of hundreds of thousands of customers. These assets are tracked separately, but treated as a whole, becoming part of the overall assets of a bank, which it can invest. Even if people decided to store their money under the mattress, the value of their money would still be dependent on a central banking system — in the case of the U.S., the Federal Reserve System. By contrast, with cryptocurrency, there is no central banking system, and the value of the currency is intrinsic, it is based on an attribute of the currency (similar to precious metals); that value is based on rarity, not a central banking system.

For DCI, the security and privacy value is based on VCs. These are encrypted artifacts that retain their value based not on a central store of identity data (although they may have derived from such a store originally), but on the ability to function as a discrete mechanism that can prove an identity attribute fully independently of any central system.

Autonomy

DCI delivers autonomy for its users. Without DCI, a driver's license can be checked with a state issuer to ensure validity, and a passport can be checked with a federal governing body to determine authenticity. However, with DCI, no such checks are required. Almost universally based on distributed ledger technology (DLT), DCI derives this benefit from the unique immutability of DLTs. Note that personal data is never stored on a blockchain; the immutability aspect and the derived benefit of autonomy derive from tracking not personal information but relationships and transactions.

If a person were to claim they held an accounting diploma from a university, for example, validating that information without DCI would typically require contact with the university. With DCI, a blockchain stores the record of a transaction between the university and the wallet holder, and reflects the fact that the university has authority to issue the VC that represents the diploma. Because of this unique approach, verifiers of university degrees can accept that the existence of the VC provides verification of the diploma. Because of this feature, DCI wallet holders enjoy a wide degree of latitude in terms of when, and how, they can use credentials to verify claims, and they can do so within the confines of a DCI product.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Portable Digital Identity: Definition and Approaches

Guidance for Decentralized Identity and Verifiable Credentials

Predicts 2023: Users Take Back Control of Their Identities With Web3 Blockchain

Top Trend in Government: Digital Identity Ecosystems

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Table 1: Representative Vendors in Decentralized Identity

Vendor Name	*Product Name*
1Kosmos	BlockID
ATB Ventures	Oliu
Avast	Digital trust
Civic Technologies	Civic ID
Condatis	Condatis Credential Gateway
Digital Bazaar	Veres One
Extrimian	QuarkID
Filancore	Identity Gateway
Finema	thai.ID
Fractal ID	Fractal ID
Gataca	Gataca Wallet
Hopae	DCX
IBM	Hyperledger Fabric
IdRamp	Integrated Identity Service Platform

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Vendor Name	*Product Name*
Indicio	Indicio Proven
InfoCert	eID
Interac (formerly SecureKey)	Interac Verified
Liquid Avatar Technologies	Liquid Avatar Verifiable Credentials Ecosystem (LAVCE)
Lissi	Lissi Identity Wallet
Microsoft	Microsoft Entra Verified ID
Nuggets	Nuggets
NuID	NuID
PARAMETA (formerly ICONLOOP)	MyID
Peaq Foundation	peaq ID
Ping Identity	PingOne Neo
Regov Technologies	myBID
Scytáles	Scytáles Digital Identity Wallet
Sitekit	Sitekit Digital Passport
Sovrin Foundation	Sovrin Network
Spherity	Enterprise Identity Wallet

This research note is restricted to the personal use of dom.wilkins@gartner.com.

Vendor Name	*Product Name*
SpruceID	Digital IDs
Thales	Trusted Digital Identity
UniquID	UniquID
Validated ID	VIDidentity
Veramo (formerly uPort)	Veramo Agent
Veridas	Veridas Nexus ID Wallet
Wipro	Decentralized Identity platform
Wise Security	Definitive ID

Source: Gartner (July 2024)

This research note is restricted to the personal use of dom.wilkins@gartner.com.