THINK TANK
BY LAB45

Digital sovereignty rising: The emergence of decentralized identity

A Primer

Digital identity systems, integral to our digital interactions, advance in security and convenience. Yet, challenges persist in securing privacy and data-use consent for identity-holders.

May 2023 | A lab45 Publication

History of Digital Identity & Decentralized Identity

What is Digital Identify?

Digital identity encompasses an individual's personal information, digital information, and digital activity, including behavior, preferences, and reputation. As our lives increasingly move online, managing digital identity becomes crucial for social interactions, financial transactions, and work activities.

> We have watched digital identity evolve from the silo identity model to the federated identity model. We believe the next stage of evolution will be DID.

Evolution Of Digital identity

Silo Identity Model:

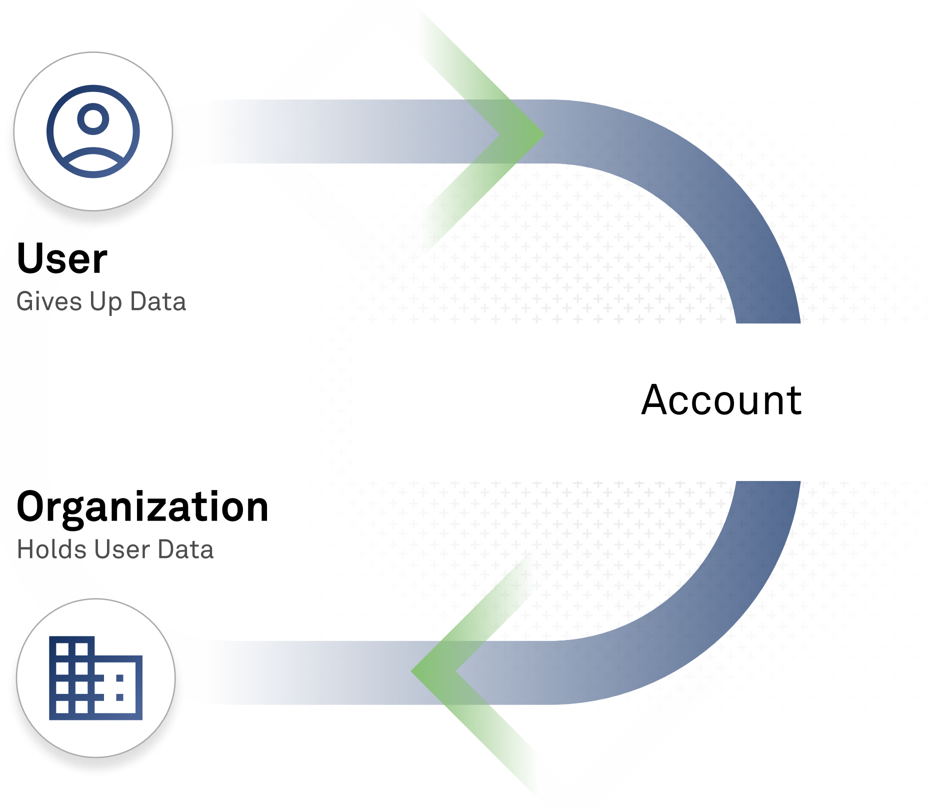
Under the silo model, each service provider (SP) required users to register and create credentials. Credentials usually consisted of a username and password. While functional at early digital stages, this approach faced challenges as the digital world became more mature.

Identity & Data Rights: The SP became the custodian and controller of a user's digital identity and data.

Monotonous Experience: Each SP requires unique credentials. Most users managed using the same set of usernames & passwords across accounts— or laboring to manage numerous unique credentials.

Security: Traditionally, data was stored in large databases. User data stored in large databases attracted hackers. as one breach could grant access to numerous identities, often repeated across multiple silos.

Siloed Identity: Every company is an Identity Provider



Federated Identity Model:

Increased digital services needed a user-friendly solution. The federated identity model improved the user experience by enabling access to multiple services using one credential set, introducing a third-party intermediary between users and providers. Tech giants mostly fill this role.

Identity & Data Rights: The control of user's data shifted from SPs to intermediaries. This still disenfranchises the user.

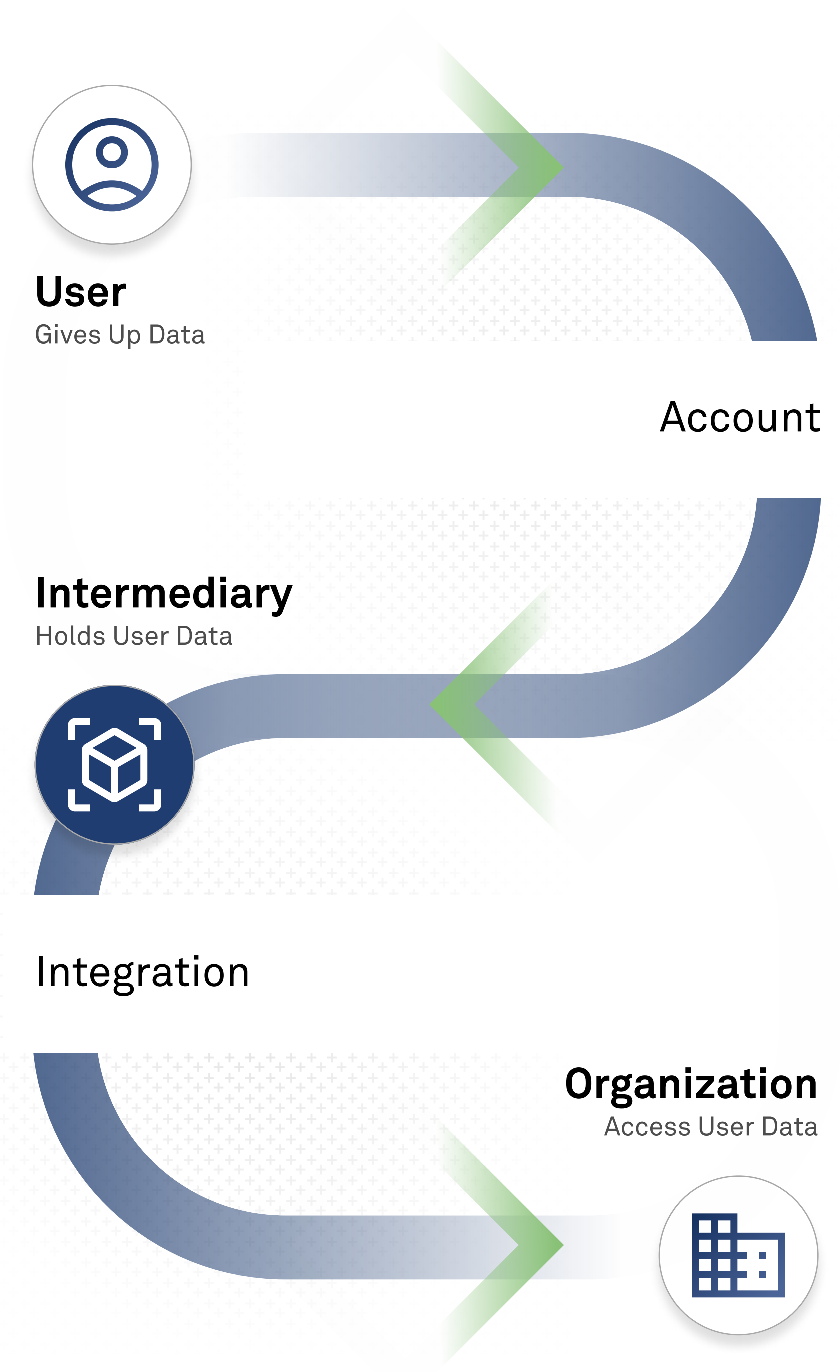
Monetization at the Cost of Privacy: Intermediaries used user identities and data to establish behavioral profiles and targeted advertising and recommendations. Digital identities thus became the product, driving intermediary revenue.

Incomplete Solution: While this model proved useful for consumers, e-retailers, and other industries, most intermediaries are not considered secure enough for highly-sensitive services like banking and healthcare. These services remain reliant on an advanced silo model with improved security.

Broken trust: Due to their widespread use and comprehensive data sets, intermediaries gained high levels of control and influence. This resulted in both breaches of trust and anti-competitive scenarios. One notable example is the 2018 Facebook-Cambridge Analytica scandal.

> **The current system resides at a very low trust level, with over 93% of users distrusting social media platform's digital custodianship.**

Federated Identity: Companies Using 3rd Party Identity Provider



How DID (Decentralized Identity) Solves these Problems?

Self-Sovereign Digital Identities: A New Frontier

With self-sovereign digital identities, the user possesses independent ownership and control of their identity and data. Long-held as a futuristic ideal, DID has the potential to make self-sovereign digital identity a reality.

DID is made possible by the technologies of blockchain, verifiable credentials, and decentralized identifiers. It has the following capabilities:

Selective Disclosure: Selectively share information with service providers without requiring new credentials.

Zero Knowledge Proof: Prove identity claims without sharing further information.

Automated Validation: Automatically validates identity and actions, for convenience.

Instant Verification: Can instantly verify identity.

Cryptographically-established Ownership: Fortifies security through advanced cryptography.

Web3.0 and A New Digital Identity

Web3.0, the internet's next evolution, aims for a decentralized, interconnected, and intelligent web. It aims for decentralized, peer-to-peer networks for secure, trustless transactions— without intermediaries. Unlike today's static web that does not adapt to the needs of its users, Web 3.0 will be dynamic and interactive, leveraging AI and blockchain to personalize, adapt, and democratize the internet. As user identity is crucial in Web3, DID will be foundational.

Ecosystem of Decentralized Identity

In a DID-based identity system, three players—User, Issuer, and Verifier—interact using Verifiable Credentials. Shared over a distributed-ledger technology (DLT)-based immutable P2P network, these credentials enable P2P pairwise interactions. See Appendix for a travel use case.

Issuer: In DID systems, issuers grant Verifiable Credentials (VC) with a digital signature for authenticity, allowing users to claim their identity or eligibility.

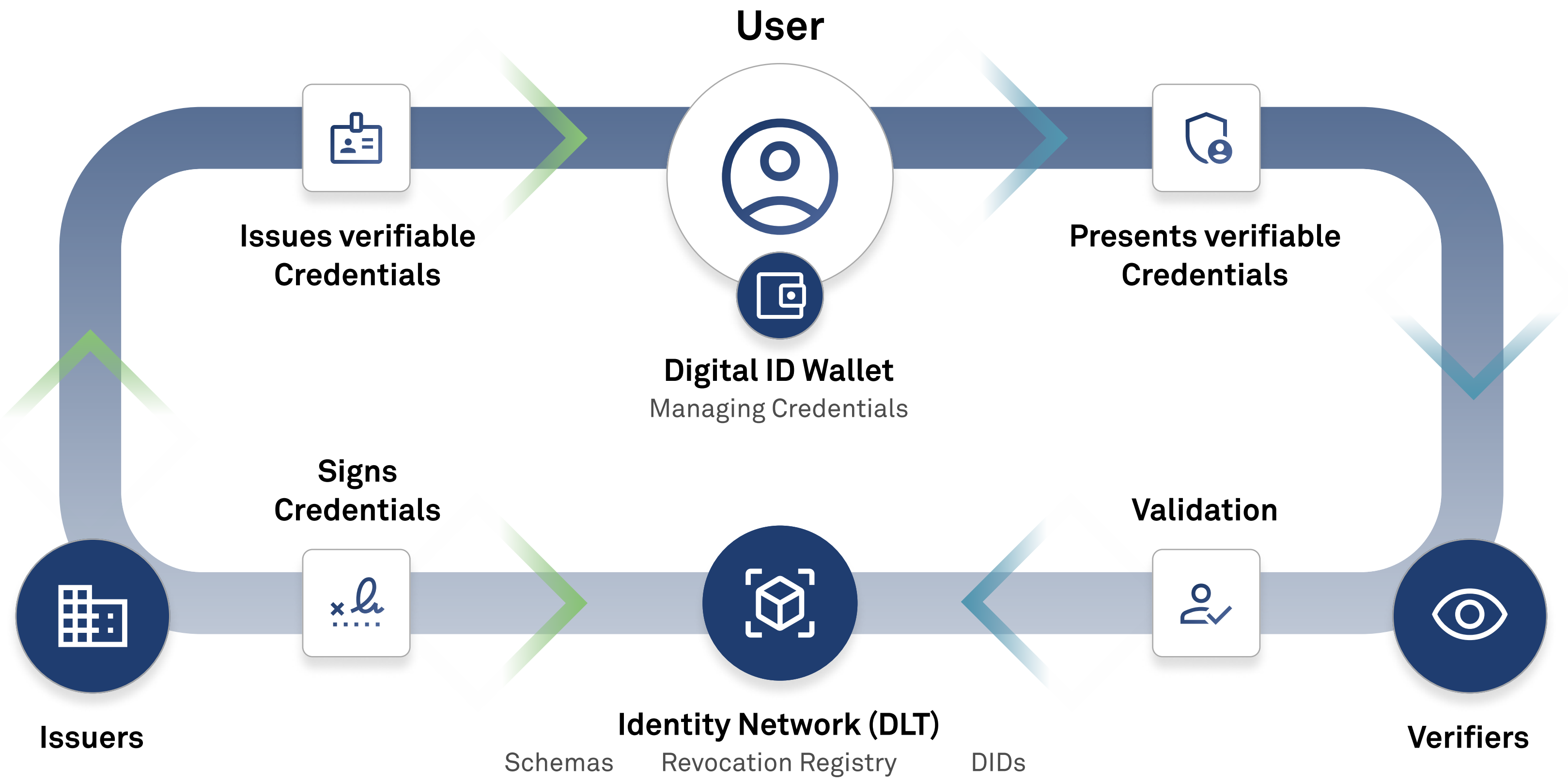
Verifier: Entities requesting user credentials for service provision are Verifiers.

Verifiable Credentials (VC): These provide proof and user details. They offer four key pieces of information without issuer interaction: issuing entity, presenting entity, tamper evidence, and credential validity. The issued verifiable Credentials are stored in User's Digital ID wallet, with user being the sole controller.

Identity Networks: Built on DLT, these underpin the DID ecosystem and store signatures and revocation registries. The tamper-evident immutability of the networks leads them to be free of personal identifiable information (PII), as any information written on DLT will remain forever.

Revocation Registries: DLT-based records ensure VC validity and authentication, even if the issuing institute ceases to exist.

Decentralized Identifiers: Decentralized identifiers refer to unique Uniform Resource Identifiers (URIs) linked to entities, directing to documents with verification details like cryptographic keys, service records, and interactions.



Functionality of DID Networks

Pairwise peer-to-peer connection: Established between users and issuers or users and verifiers, these private, point-to-point connections enable secure communication and transactions.

Credential processes: Issuers grant VCs to user wallets, storing verification signatures on DLT. Verifiers request credentials, with wallet and issuer verification performed via DLT.

User & Organizational Benefits

User Benefits

- ✓ **Credential forgery prevention:** The immutability of blockchain-based DID ensures VC authenticity, eliminating forgery risks.
- ✓ **Password-free authentication:** Digital VCs replace cumbersome password and multi-factor authentication, with tamper-detection built into DID wallets ensuring much higher levels of security than traditional password-based systems.
- ✓ **Spam prevention:** DID only allows user- authorized data access. No data footprint is left unless authorized by the user — allowing no unauthorized data access to third party advertisers. Users will be able to browse Web3.0 virtually spam-free, leaving no trace.
- ✓ **Phishing prevention:** DID's P2P pairwise communication, when paired with validated decentralized identifiers, thwarts counterfeit websites.
- ✓ **Dramatically reduced wait times:** Instant verification speeds up processes like international travel checkpoints, employee onboarding, and banking KYC.
- ✓ **Data Monetization:** Unlike the existing model where intermediaries control and monetize user data for third parties, in a self-sovereign DID system, users will be able to demand and receive a portion of monetization benefits from intermediary data usage.

Organizational Benefits

- ✓ **Operational Efficiency & Verification Cost:** Current verification methods demand hiring third- party services or internal teams, resulting in slow, costly processes. KYC costs banks $13-$130 per user, totaling around $60M annually, excluding regulatory penalties. DID provides instant, error- proof verification without external reliance.
- ✓ **IT & Cybersecurity Cost:** DID helps manage rising IT costs for enhancing as-needed traditional silo system security. It can also reduce system interoperability costs.
- ✓ **Enhanced User Experience:** DID improves customer experience with a seamless, efficient, secure process, distinguishing it from non-DID systems.
- ✓ **Enhanced Brand:** The privacy, security, and user- control aspects establish organizations as trusted brands.

How can Organizations Implement DID?

We recommend the following approach:

1. **Start Small:** Start with a simple, isolated POC—ideally replacing a silo function— to avoid impacting other functions. Apply lessons learned to broader areas.
2. **Internal Buy-in:** Engage finance teams, management, and employees before pilot implementation. Build a business case based on the pilot, along with a larger implementation plan.
3. **Select Platform & Partner:** Choose a fitting platform and a trusted partner for both pilot and larger implementations. Ideally, the pilot partner and the larger partner will be identical.
4. **Customer & Partner Onboarding:** Establish processes to minimize disruptions. Implement phased rollouts for reduced disturbance and improved learning and iterative opportunities.

DID Obstacles to Adoption

Siloed Implementation

Obstacle

DID can enable a highly interoperable ecosystem, but it requires organizations and governments, as verifiers and issuers, to participate. Successful scaling hinges on onboarding these parties, especially governments as major ID issuers.

Solution

The involvement of governments and organizations would boost verifier interest, encourage legislative changes, and promote collaboration in consortiums. There is already some positive movement in this direction— governments in Estonia, Dubai, El Salvador, and others have been making efforts to establish blockchain identity solutions.

Lack of Regulatory Standards

Obstacle

Regulatory controls struggle to keep pace with technological advancements, including blockchain. The absence of clear rules creates uncertainty and mistrust.

Solution

Although W3C announced Decentralized Identifiers as a web standard in July '22, it's a starting point and must mature for seamless cross-platform operations.

Limited Education

Obstacle

DID, mainly driven by the open- source community, has limited awareness among users and organizations due to its complexity.

Solution

As industry use cases increase and Identity and Access Management (IAM) leaders' products mature, the education gap will close. This primer aims to help bridge that gap.

Lost Wallets or Private Keys

Obstacle

Presently, blockchain wallets rely entirely on private keys for authentication and access, risking data and financial loss if misplaced.

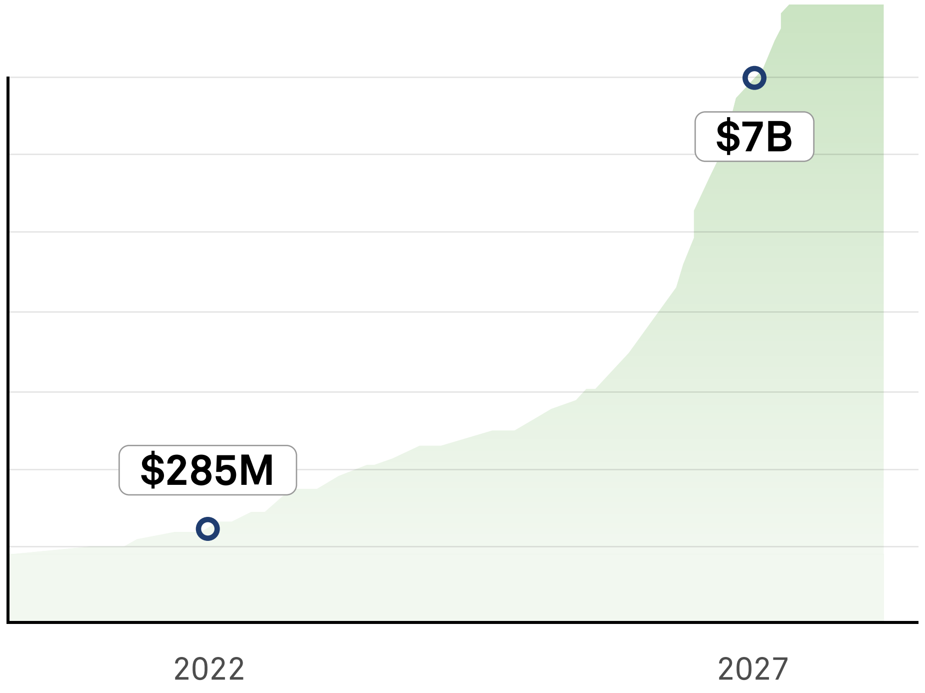
Solution

Some ongoing efforts aim to address this by revoking device authorization or invalidating VCs. However, a robust and streamlined solution remains to be seen.

Market and Product Outlook

Market Outlook and Forecast

According to Markets and Markets, the global decentralized identity market was valued at $285 million in 2022 and is expected to grow at a CAGR of 88.7% over the next 5 years. The market will likely flourish as businesses increasingly adopt decentralized identity solutions to enhance access and identity management systems.



Product Outlook

wipro

In February 2022, Wipro's lab45 launched DICE ID, a decentralized identity platform empowering users to control and share personal data online, quickly and safely. Adopted by Ed-tech, Fintech, and Health-tech industries, it enables:

- Automated validation and verification
- Cryptographic credential ownership
- Selective disclosure
- Self-sovereign user identity control

Microsoft

In March 2022, Microsoft introduced Entra, a new identity and access management portfolio, to implement decentralized identity within the Azure AD and Cloud Infrastructure Entitlement Management (CIEM) systems. Entra aims to help security teams manage permissions, protect digital identities end-to-end in multi-cloud environments, and prevent unauthorized access to apps or resources.

IBM

A decentralized identity solution based on W3C standards, IBM's digital credential offers users digital wallets for secure, selective disclosure, while empowering organizations worldwide to transform identity systems with verifiable credential issuance and verification. Applied in vaccine certification for COVID regulations and for certain skill certifications.

polygon ID

Founded in 2017, Polygon targets Web3.0 implementation across various industries, including retail, social media, entertainment, and finance. Their DID solution, Polygon ID, offers interoperable digital wallets and verifiable credentials for issuers and verifiers. Polygon is among the first to generate zero-knowledge proofs using VCs.

Decentralized Identity Market Size, Trends, Drivers & Opportunities | MarketsandMarkets
IATA Travel Pass: Getting Started - Evernym
Polygon ID | Identity infrastructure for Web3
Research and Markets

Self-Sovereign Identity - the good, the bad and the ugly; May 2019 | TNO Consult Hyperion
whitepaper: Know your compliance costs | Mitek (miteksystems.com)
Wipro Lab45 launched DICE ID

Example Use Case

Keeping up with the rise of international travel

As international travel continues to rise in popularity across developing economies, governments, airlines, and airports face increasing demands. According to Christoph Wolff of the World Economic Forum, passenger numbers may rise 50% from 2016 to 1.8 billion by 2030. To manage this large rise in passenger count, governments, airlines, and airports must implement more efficient processes.

Why DID for Travel?

DID is ideal for travel, particularly international journeys, as the industry requires users to prove their identity and eligibility to various stakeholders for regulatory, national security, and immigration purposes— and DID can do so conveniently and securely. The numerous parties involved and multi- organization interoperability needs make DID a perfect solution, enhancing security, user experience, and efficiency—typically considered opposing goals.

> **When stored as VCs on the blockchain and presented with ease and immediacy—trips to the airport will become less stressful and much easier.**

What will Travel be like, with DID?

Currently relevant issuers and Verifiable Credentials (VCs):

1. **Ministry of External Affairs or Equivalent:** Internationally recognised ID i.e., Passport
2. **Destination Country Embassy:** Accessibility Permit to their Country i.e., Visa, Resident Permit etc.
3. **Airline:** Permit to access flight i.e., Ticket, Boarding Pass and Luggage Tags
4. **Additional Travel Requirement:** COVID Vaccine Certification

Presently, validation of each of the above documents is a manual and tedious process to a large extent.

Transforming passports, visas, check-ins, and health/vaccine certificates into Verifiable Credentials (VCs) streamlines the verification process.

Presenting VCs at check-in, immigration, and departure/arrival stages reduces human intervention and creates a seamless experience.

Verifiers in the process that can easily be verified simply by VC at the entrance to the airport include:

1. **Airport Security:** Safety assurances ensuring airport access
2. **Airlines:** Confirming travel eligibility
3. **Immigration/Homeland Security:** Granting entry to the destination country
4. **Embassy:** Verifying travel documents and passports for visa issuance

Authors @lab45

Abhigyan Malik
Strategy Consultant
in

Sujay Shivram
Principal Strategy Consultant
in

Contributors @lab45

Hitarshi Buch
Chief Architect, Blockchain Platforms
in

lab45

Lab45 is a visionary space developing ground-breaking solutions to foster and accelerate ideation throughout Wipro.

At Lab45, engineers, research analysts, and scientists come together to infuse creative ways of incubating solutions for customers that will transform the future. It is a space filled with ambition at the vanguard of far-reaching research across cutting-edge technologies.

Established with the Silicon Valley culture of free-flowing creativity, Lab45's goal is to make bold ideas a reality and to invent the future of enterprise. So come, collaborate, and see what happens when ideas are left unbound.

Feedback

It will take less than a minute!

Click to Know More

Disclaimer: This report was created using various sources such as expert interviews, internet reports, website research and media releases. This information is collated in good faith and used on an as is and as available basis by us. Our reports should only be construed as guidance. We assert that any business or investment decisions should not be based purely on the information presented in our reports. information included in the reports. We do not guarantee or take responsibility for the accuracy, completeness, reliability and usefulness of any information. The opinion expressed in the reports is our current opinion based on the prevailing market trends and is subject to change.

Ambitions Realized.

Wipro Limited

Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India

Tel: +91 (80) 2844 0011

wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading technology services and consulting company focused on building innovative solutions that address clients' most complex digital transformation needs. Leveraging our holistic portfolio of capabilities in consulting, design, engineering, and operations, we help clients realize their boldest ambitions and build future-ready, sustainable businesses. With over 250,000 employees and business partners across 66 countries, we deliver, on the promise of helping our customers, colleagues, and communities thrive in an ever-changing world.