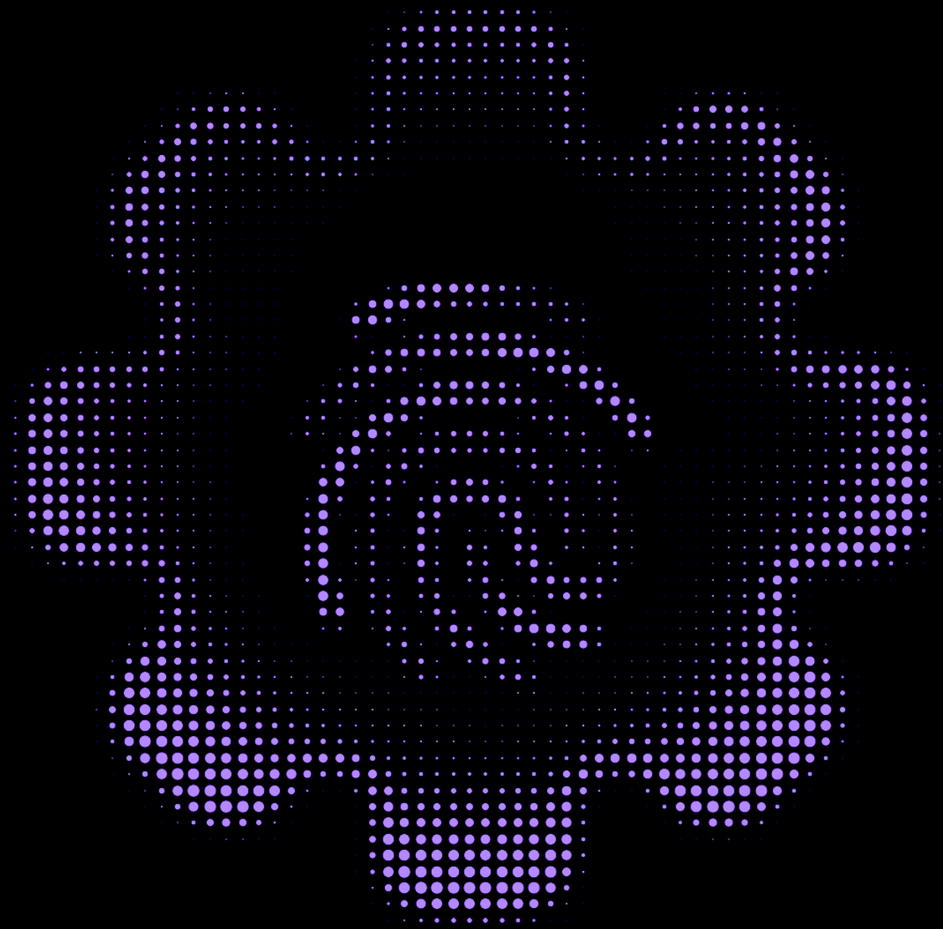
THINK TANK
BY LAB45

Reimagining Business Processes through Decentralized Identity

A Primer



Decentralized Identity, powered by Blockchain, transforms digital interactions, offering users control, privacy, and security. Explore its varied applications across sectors as the technology continues to evolve and find new innovative uses.

WHAT'S INSIDE!

September 2023 | A lab45 Publication

SECTION 01

KYC Process Transformation

Context

The KYC policy is a set of mandatory guidelines implemented by banks and financial institutions to identify customers and comply with international regulations that combat money laundering and terrorist financing, Banks usually incorporate the following four crucial elements into their KYC policies:

- Customer Policy
- Customer Identification Procedures (including data collection, identification, verification, politically exposed person/sanctions list check), also known as the Customer Identification Program (CIP)
- Risk assessment and management (part of the KYC process, which includes due diligence)
- Ongoing monitoring and record-keeping

This procedure involves verifying a customer's identity through documents, including a national ID Document using a document reader and advanced verification software.

The Problem

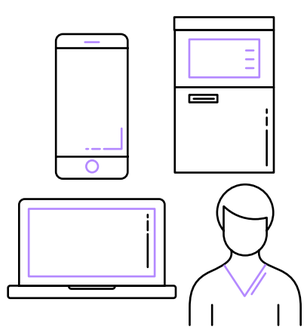
While the KYC regulations provide benefits they come at a cost. Failure to meet regulations can result in hefty fines from regulators. In fact, in the first half of 2021 alone, nearly $1 billion was issued in KYC and AML fines.

- **Cost of Implementation:** As per a white paper by Consult Hyperion a single KYC cost varies from 13$ to 130$, which scales up to an average cost of $60 million per year for a bank.

Decentralized KYC Solution

Decentralized KYC offers customers the ability to a obtain a verifiable credential attesting the fact that the KYC process has been completed by a trusted authority. Verifiable credential then

KYC Process Flow



Identity Verification

01 Identity Document Verification

02 Customer Authentication

03 Risk Assessment

Enrollment Facilitation

04 Identity Verification Report

05 Automatic Form Filling

can be stored on their mobile wallet and verified through cryptography. These verifiable credentials serve as trustworthy and tamper-proof digital identity documents that can be verified by other service providers for authenticity and ownership. KYC Verifiable Credential providers may issue these credentials as part of an existing KYC process or at the customer's request. This solution benefits all parties involved by providing a streamlined customer experience and simplifying and reducing the cost of processes for banks and service providers.

KYC Process Transformation:

A Bank or Financial institution looking to implement a self-sovereign decentralized Identity based KYC solution should use a phased approach:

1) **Target a Single Business Function First:** Consider implementing this for one business stream within your organization. For example, a Savings bank business in a Banking conglomerate can do the KYC using their Target a single business function first regular process. The digital records collected can be stored in the Blockchain and the user issued a Decentralized Identifier. The Savings bank function becomes an issuer of credentials.

2) **Scale this to Other Functions in the Organization:** When a different business within the conglomerate needs to offer services to the same customer, these credentials can be verified using the Identifier and credentials provided by the original business stream without having to perform a detailed KYC, as the Issuer is a trusted source now.

3) **Build a Consortium:** Once this is successful, the conglomerate can consider creating a closed consortium with organizations having similar needs in the sector or even outside.

4) **Execute and Reap Benefits:** In this consortium, every member agrees that credentials issued by one member can be trusted and utilized by other members.

How will it Work?

Here is an example of how this use case might work in practice:

1) A customer visits a financial institution's website and begins the account opening process.

2) During the account opening process, the customer is prompted to provide some personal information, such as their name, address, and date of birth.

3) The financial institution uses this information to verify the customer's identity by performing a KYC (Know Your Customer) check.

4) Instead of asking the customer to upload documents like a passport or utility bill, the financial institution requests a verifiable credential from a trusted third-party provider, such as a government agency or a credit bureau.

5) The customer is redirected to the third-party provider's website to retrieve their verifiable credential.

6) The customer signs in to their account with the third-party provider and retrieves their verifiable credential. This credential contains their verified personal information, such as their name, address, and date of birth.

7) The customer returns to the financial institution's website and submits their verifiable credential.

8) The financial institution validates the verifiable credential using the decentralized identity platform, ensuring that it is authentic and that the information matches the customer's account opening details.

9) The customer's account is approved, and they can access their new account and start using it.

The approved KYC verifiable credential is stored in Customer's digital wallet and in any further transaction or engagement can be reused without initiating the KYC process again. Additionally, KYC VC can also be used across multiple business and services within an organization as well as across the industry.

Conclusion

The potential impact for banks, is quite significant. This presents a unique opportunity to provide customers with higher security and less friction in their transactions. By eliminating intermediaries and returning to trusted, direct relationships, banking processes can become much simpler. Overall, the use of verifiable credentials for KYC can improve the efficiency, accuracy, and customer experience while increasing the security and integrity of the information.

SECTION 02

Decentralized IoT Integrated supply-chain for Food/Perishables

Context

The global food traceability market is predicted to grow at a CAGR of 9.0%,(2022-2029) with a value of USD 18.15 billion in 2021. While making it a prospective market, the report primarily focus on centralized solutions with use of Barcodes, RFID, GPS etc., it does not take into consideration the Blockchain based decentralized solutions, which solves for data privacy and trust issues faced by technology under consideration. In comparison the market for Blockchain in Food Supply chain, has much smaller footprint as of today with USD 285 million in 2022 but with more aggressive growth of 43.76% CAGR for 2023-2031 period.

The global IoT market for supply chain is anticipated to be worth $34.81 billion by 2027, growing at a CAGR of 12.7%. making IoT one of the biggest drivers of productivity and growth in the next decade. In case of Food supply the application of IoT can provide real-time data and insights, devices are helping companies to streamline their operations, reduce costs. Furthermore, on customer front it can reduce customer concerns regarding food safety, such as food-borne illnesses and adulteration.

Problems on IoT Front

The current IoT supply chain is complex and inefficient due to the lack of information exchange among multiple parties. Due to this it faces significant challenges:

1) **Security Risks:** IoT devices can be vulnerable to identity spoofing attacks if they do not have a unique and verifiable identity. An attacker could manipulate the identity of a device to gain unauthorized access to sensitive data or control of the device, which can compromise the security of the supply chain. For many organizations concerns about security remain

a significant barrier and are hindering the adoption of IoT devices (see Figure 1).

2) **Interoperability:** There are numerous IoT devices and platforms available in the market, and ensuring interoperability between different devices and systems can be challenging. This leads to compatibility issues, which can hinder the smooth functioning of the supply chain. World Economic Forum cites 67% respondents balk at implementing IoT because of challenges to connect legacy equipment due to lack of interoperability.

3) **Data Silos:** Without a common and interoperable identity infrastructure, IoT devices can create data silos that hinder collaboration and data sharing among different stakeholders in the supply chain. Cisco estimates factories worldwide contain 60 million machines, with 90% of these machines residing in unconnected silos and 70% more than 15 years old.

Problems on Food Supply Chain Front

Supply Chain Complexity & Product Recall

Managing a food supply chain is significantly more challenging than a non-perishable product due to additional aspects that have to be monitored and maintained throughout the supply chain from temperature, humidity to avoiding any contamination. Additionally, each consignment also needs to be cleared for multiple Quality Assurance tests conducted at multiple nodes from farmer to a retails shelf. Any failures along this leads to product recalls, financial loss, regulatory fines, and brand dilution.

According to FDA report for 2022, the product recalls have shot up by 700% in 2022 YoY when measured for “Units”(individual retail packages).

Consumer Awareness: Increased consumer demand about information associated with products like

- Ingredients and their responsible sourcing
- Certification of sustainable production and packaging standards, are shaping their purchasing decisions more than ever.

According to survey conducted by L.E.K Consulting, about 20% of US consumer spend for F&B(Food & Beverage) is on Sustainable products. Additionally, 54% are ready to switch their preferred choice for an alternative sustainable product.

Public Health Impact: Any failure to maintain the standards also has impact on public health.

Figure 1

Security Remains the Leading Barrier for IoT Adoption

Top barrier for investment in the Internet of Things

Source: Bain 2018 IoT customer survey (n=521)

According to the World Health Organization, approximately 600 million people, or roughly one in ten individuals worldwide, fall sick every year due to consuming contaminated food. This leads to a loss of approximately 33 million healthy man-days. In addition, low- and middle-income countries experience an estimated loss of USD 110 billion in productivity and medical expenses each year due to unsafe food consumption.

Decentralized Traceability Solution

Decentralized food supply chain traceability solution proposes the integration of

- Decentralized identifiers (DIDs)
- Verifiable credentials (VCs)
- On board IoT for Logistics

The Solution will Enable

a) Issuance and verification of produce information for stakeholders across the supply chain.

b) Trace each crate of produce along the supply chain providing accurate and trustworthy information about the ambient conditions, quality, and source of produce to each stakeholder.

c) In case of any contamination, this will also help reduce the fallout as each of affected produce can be traced back with accuracy to ensure that no other consignment is affected containing the recall impact.

To ensure decentralized data authorization, the framework utilizes blockchain technology to act as a bridge between the disconnected IoT data silos. Smart Contracts are used to define the terms of data sharing and access control, which are enforced automatically by the blockchain.

How will it Work?

Let's consider the example of a temperature sensor in a refrigerated truck that is transporting perishable goods. The following is a brief explanation of the sensor's lifecycle within the Decentralized framework

1) **Device Integration:** IoT devices such as sensors and trackers are integrated into various stages of the food supply chain to collect data on temperature, humidity, location, and other relevant parameters for ensuring food quality and safety.

> **Linking emerging technology like Blockchain & IoT with agriculture research should create a sustainable ecosystem, transforming the food sector.**

2) **Decentralized Identity Creation:** Each participant in the supply chain, including farmers, processors, distributors, and retailers, create their own Decentralized Identifiers (DIDs) and associated public-private key pairs. These DIDs serve as unique and verifiable identities for each participant.

3) **Registration on a Decentralized Ledger:** The created DIDs and public keys are registered on a decentralized ledger or registry that supports Decentralized Identity. This step ensures the immutability and integrity of the identity information.

4) **Verifiable Credentials Issuance:** Participants, such as farmers or processors, issue

verifiable credentials to provide proof of specific attributes or qualifications related to their role in the supply chain. These credentials can include certifications, licenses, or audit reports.

5) **Data Collection and Validation:** IoT devices collect real-time data from various stages of the food supply chain, which is then validated and signed using the participant's private key associated with their DID. The collected data can be linked to specific verifiable credentials for added context and trustworthiness.

6) **Verifiable Credentials Presentation:** When sharing data or participating in transactions, participants can present relevant verifiable credentials along with the data to prove their qualifications, certifications, or compliance. This enables trusted data exchange and establishes credibility.

7) **Data Sharing and Access Control:** Participants selectively share collected data and associated verifiable credentials with other authorized parties using their DIDs. Access control mechanisms ensure that only the necessary data and credentials are shared with specific recipients, maintaining privacy and security.

> **Collecting, documenting, and applying reliable and verifiable information throughout the supply chain, from origin to farm to fork, ensures food safety and quality for consumers and stakeholders**

8) **Traceability and Transparency:** The integration of IoT data, Decentralized Identity, and verifiable credentials enhances traceability and transparency in the food supply chain. Each data point is linked to the corresponding participant's DID and can be validated through associated verifiable credentials, enabling a comprehensive audit trail.

9) **Verification and Trust:** The authenticity, integrity, and relevance of the collected data and presented verifiable credentials can be verified by validating the signatures associated with the DIDs and credentials. This verification process builds trust among supply chain participants and ensures data integrity.

10) **Consumer Engagement:** The integrated system provides consumers with access to transparent and trustworthy information about the food products they purchase. Through verifiable credentials, consumers can verify certifications, origin claims, or other attributes, enabling informed purchasing decisions.

11) **IoT Sensor End of Life:** When the temperature sensor reaches the end of its lifecycle, its DID can be revoked, ensuring that it cannot communicate with any other devices or the network.

Conclusion

Overall, using DID and verifiable credentials in food/perishable supply chain can provide a tamper-proof and auditable record of a product's journey, from its origin to its destination. Solution will have lasting impact not only for controlling quality and expense for organization but will also have impact on public nutrition, health, and sustainability.

SECTION 03

Decentralized EHR (Electronic Health Records)

Context

The emergence of information technologies, including electronic health records (EHR), is revolutionizing the delivery of healthcare and enhancing patient care. These technologies are significantly enhancing health outcomes by facilitating better decision-making, improving public health, and reducing costs.

In 2022, the estimated value of the global market for electronic health records was USD 28.1 billion. It is predicted that this market will experience a compound annual growth rate (CAGR) of 4.1% from 2023 to 2030. In comparison, the market size of blockchain technology in healthcare globally was USD 1.97 billion in 2022 and is predicted to grow at a CAGR of 68.40% between 2023 and 2030.

A CAGR growth difference of about 16x, is primarily fueled by the challenges to address the escalating cases of information leaks and data breaches, along with the necessity to mitigate these concerns.

The Problem

Privacy & Security Concerns: Maintaining patient privacy and compliance with regulations, such as HIPAA, is crucial when validating electronic requests for patient information. It can be challenging for healthcare providers to ensure that their EHR solution has adequate controls in place to protect Personal health Information (PHI), especially if they have existing legacy systems. Breaches of PHI can result in hefty fines and reputational damage, so protecting patient information is of utmost importance.

The data breaches in the healthcare sector have been a major issue with 51% organizations reporting increase in data breaches since 2019.

Interoperability: In the US, an estimated two-thirds of older Americans have multiple chronic conditions, which account for 66% of healthcare costs. As populations age and life expectancy increases, healthcare providers need to prioritize interoperability and data sharing. Seamless data sharing and interoperability are essential to improving patient outcomes, reducing costs, and delivering high-quality care to older Americans.

Decentralized Traceability Solution

Decentralized identity solutions provide an effective way to address privacy, security, and interoperability concerns in electronic health record (EHR) management. Decentralized Identity technology enables patients to maintain control over their health information, determining who can access it and under what conditions. This ensures that sensitive patient data remains private and secure, reducing the risk of data breaches or unauthorized access.

By using a Decentralized Identity solution, patients are issued a unique digital credential that verifies their identity and can be used to grant or deny access to their EHR. This eliminates the need for centralized identity management systems, which can be prone to security breaches and hacks. Decentralized Identity solutions can also enhance interoperability by enabling seamless data sharing between healthcare providers, without the need for complex data exchange agreements.

How Will it Work?

Here is an example of how verifiable credentials could be used in the context of electronic health records (EHR)

1) A patient visits a healthcare provider and provides their personal information, including their name, date of birth, and contact details.

2) The healthcare provider creates an electronic health record (EHR) for the patient and issues a verifiable credential attesting to the patient's identity.

3) The patient can use their verifiable credential to securely and quickly authenticate themselves to other healthcare providers, insurance companies, or government agencies, who can access their EHR and relevant medical information based on patient's permission.

4) If the patient needs to share their EHR with a new healthcare provider, they can do so without having to provide their personal information repeatedly, thus reducing the risk of identity theft.

5) The verifiable credential also allows the patient to control access to their EHR by specifying which healthcare providers, insurance companies, or government agencies can access it and for what purpose.

6) If the patient moves or changes healthcare providers, they can easily transfer their EHR to their new healthcare provider using their verifiable credential, without the need for complicated and time-consuming data transfers.

7) Overall, the use of verifiable credentials in EHRs can improve the security, efficiency, and privacy of medical information exchange, while empowering patients to have greater control over their own health data.

Advantages of Using DID and VC in EHR

For Consumers

- Improved control and ownership of their health information through the use of a decentralized identifier and verifiable credentials
- Increased privacy and security of their sensitive health information due to the tamper-proof nature of the decentralized ledger

For Hospitals

- Reduced administrative burden and costs associated with maintaining and verifying patient identity and health information
- Improved efficiency and accuracy in accessing and sharing patient health information with other providers

For Insurance

- Improved accuracy and reliability of patient health information leading to better risk assessments and insurance pricing
- Reduction in fraudulent claims due to the tamper-proof nature of the decentralized ledger.

Conclusion

Overall, Decentralized Identity solutions offer a secure and privacy-enhancing way to manage EHRs, while improving interoperability and reducing administrative overhead. By providing patients with greater control over their health information, Decentralized Identity solutions can enhance trust and confidence in the healthcare system, leading to better health outcomes.

Authors@lab45 **Abhigyan Malik** **Sujay Shivram**

Ambitions Realized.

Wipro Limited
Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India
Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
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.

For more information,please write to us at info@wipro.com