Persistent

Persistent Self Sovereign Identity Capability

Digital Identity

Decentralized Verifiable Credentials

Persistent

Centralized Identity

Trust between user and the organization is typically established using shared secrets, usually in the form of a username and a password.

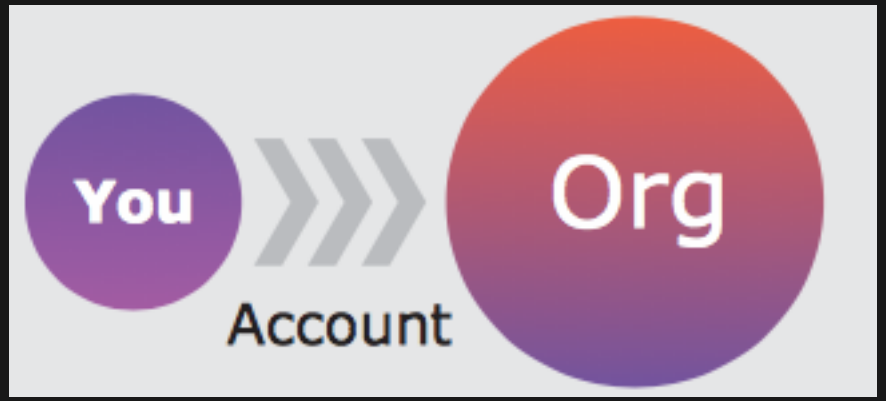
At least some of user's personal data is typically stored within the organization's data "silo", a scenario that repeats for every organization, app, or website user logs into.

Pros

- Widely established, well understood and straightforward to use.
- Helps the organization manage compliance and liability by keeping data in-house.
- Enables pairwise (unique) credentials for each relationship, which enhances both security and privacy..

Cons

- Worst customer experience - forces you to maintain multiple credentials, one for each app, service, or relationship.
- Breach of an organization using siloed identity can be catastrophic.
- Authentication is one-way which is vulnerable to phishing attacks.
- Identity and security experts which can be a challenge to small organizations.



Source:

Federated Identity

The IDP issues the digital credential, providing a single sign-on experience with the IDP which can then be seamlessly used elsewhere, reducing the number of separate credentials you need to maintain.

User logs in to the IDP, which then “federates” your login to the service you’re trying to access using protocols such as OAuth, SAML, or OpenID Connect.

Pros

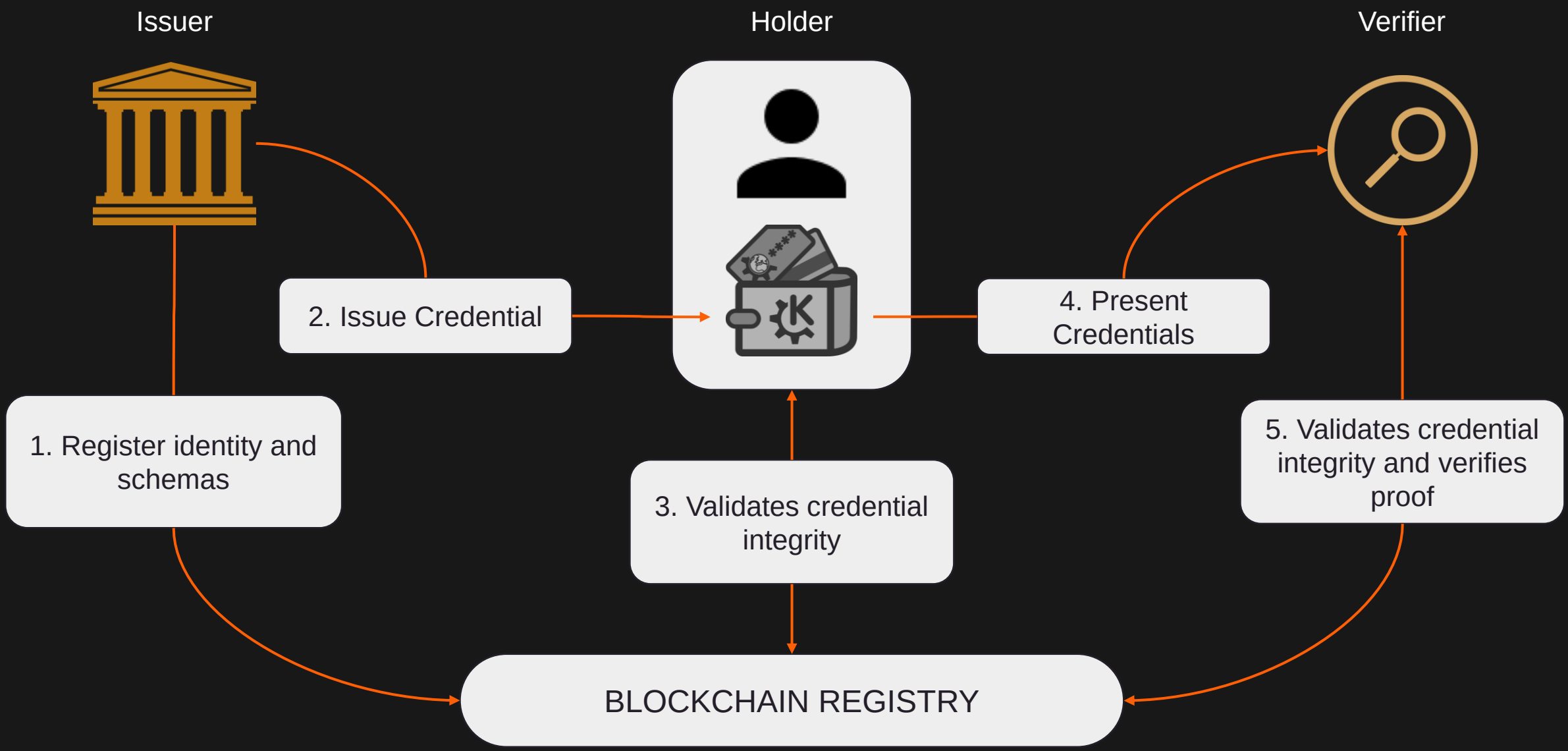
- Improves customer experience by allowing users to access many applications with a single credential.
- Reduces operational cost and complexity. It also makes it easier to ensure the security and privacy of shared information.

Cons

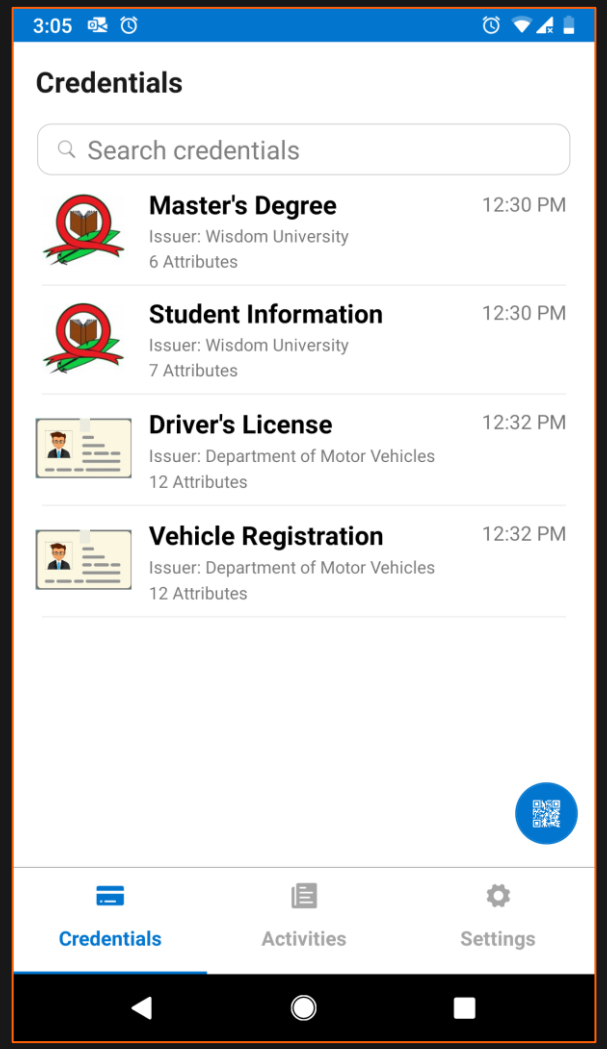
- Forces users to create a new relationship with a potentially unfamiliar IDP, separate from and in addition to the organization with which they’re trying to interact.
- IDP also determines the limitations of data structures and schema and must maintain direct connections with all network participants, inhibiting flexibility and scalability.
- Authentication is one-way which is vulnerable to phishing attacks.

Source:

Verifiable Credentials Workflow



Persistent Digital Identity Wallet



EASY IDENTITY CREATION

Create and manage an identity within seconds. No usernames or passwords to set.

VERIFIABLE CREDENTIALS

Acquire, store and present verifiable digital credentials with the identity wallet.

INSTANT VERIFICATION

Authenticity of credentials can be instantly verified accelerating customer onboarding processes in digital workflows.

SHARE WITH USER-CONSENT

Credentials can only be shared with user-consent and selectively if required. Ensures compliance with privacy laws.

AUTOMATIC SYNC

Identity and credentials are securely backed-up to user-preferred cloud storage.

EASY RECOVERY

Identity and credentials can be restored on a new device from the secure cloud backup.

Digital Identity & Verifiable Credentials

Solutions

\ Mobile app will provide features to

- Acquire, store and present verifiable credentials
- Identity creation, management and key rotation
- User-consent, select attribute sharing
- Privacy and zero-knowledge proofs
- Credential backup and recovery
- Security and Biometrics
- Seamless mobility to new devices.

\ Web SDK will provide features to

- Credential definition, issuance, revocation
- Instant credential verification.

Outcomes

W3C Identity Standard

Built on W3C Decentralized Identity and W3C Verifiable Credentials Standard

Flexible 3rd Party Integrations

Eased integration with identity and identity document verification services providers

Digital Interactions

Blockchain brings the security, immutability, transparency, provenance

Easy customer onboarding

Digitization, provenance, immutability helps a faster and efficient user onboarding

Success Stories

Telecom provider (QA)

Automate workflows end-to-end with digital identity & verifiable credentials

Telecom provider (IN)

Automate customer onboarding in digital workflows and cut costs across the entire digital ecosystem

Insurance Provider (EU)

Cut costs significantly by lowering manual intervention using password-less sign-ins.

Technologies and/or Partners **Hyperledger Indy, Android and iOS libraries, React Native, Javascript, NodeJS, Java**

Usecases

KYC

- SSI enables a reusable KYC concept that offers a much more seamless way of ID verification.
- Disrupt and digitally transform the corporate KYC landscape
- Enables rapid onboarding and delivers a frictionless experience

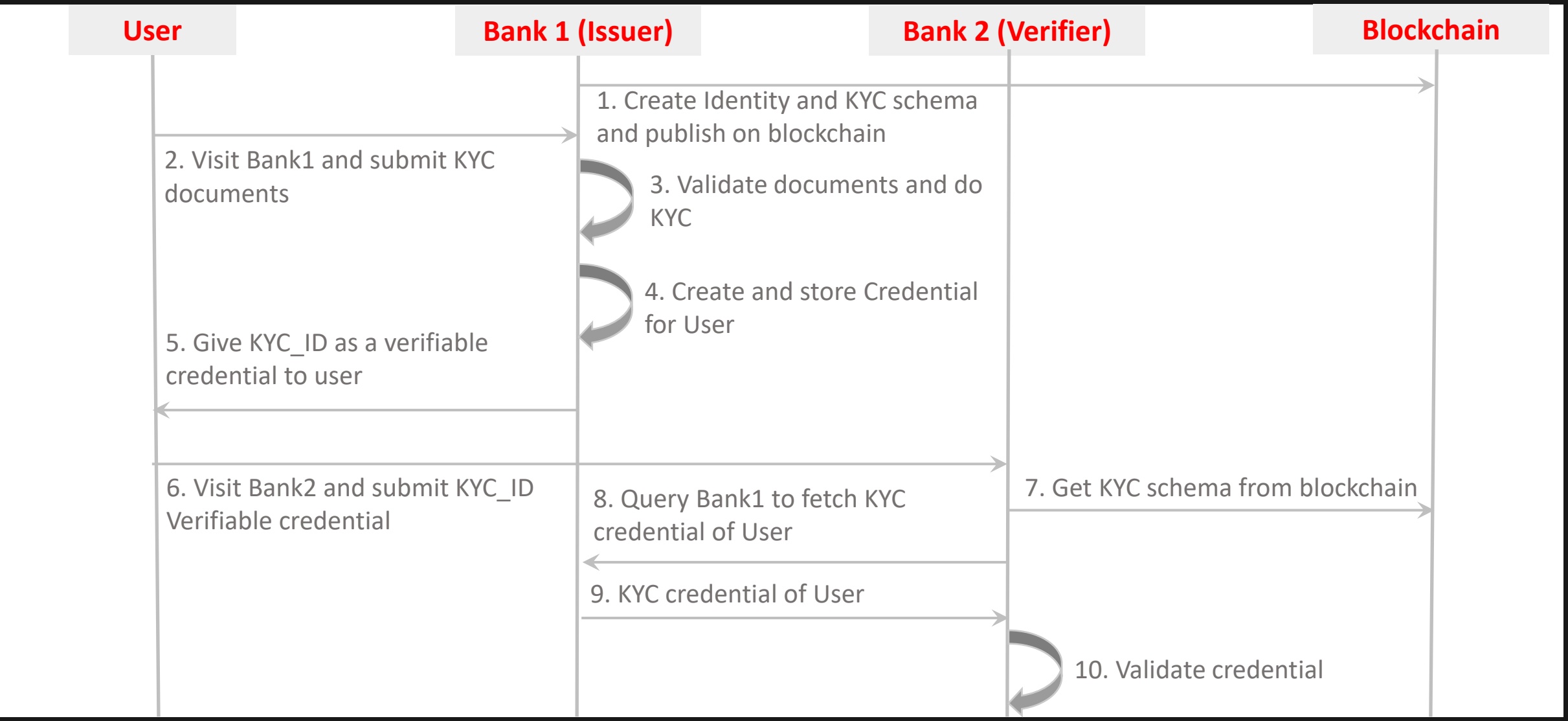
BFSI

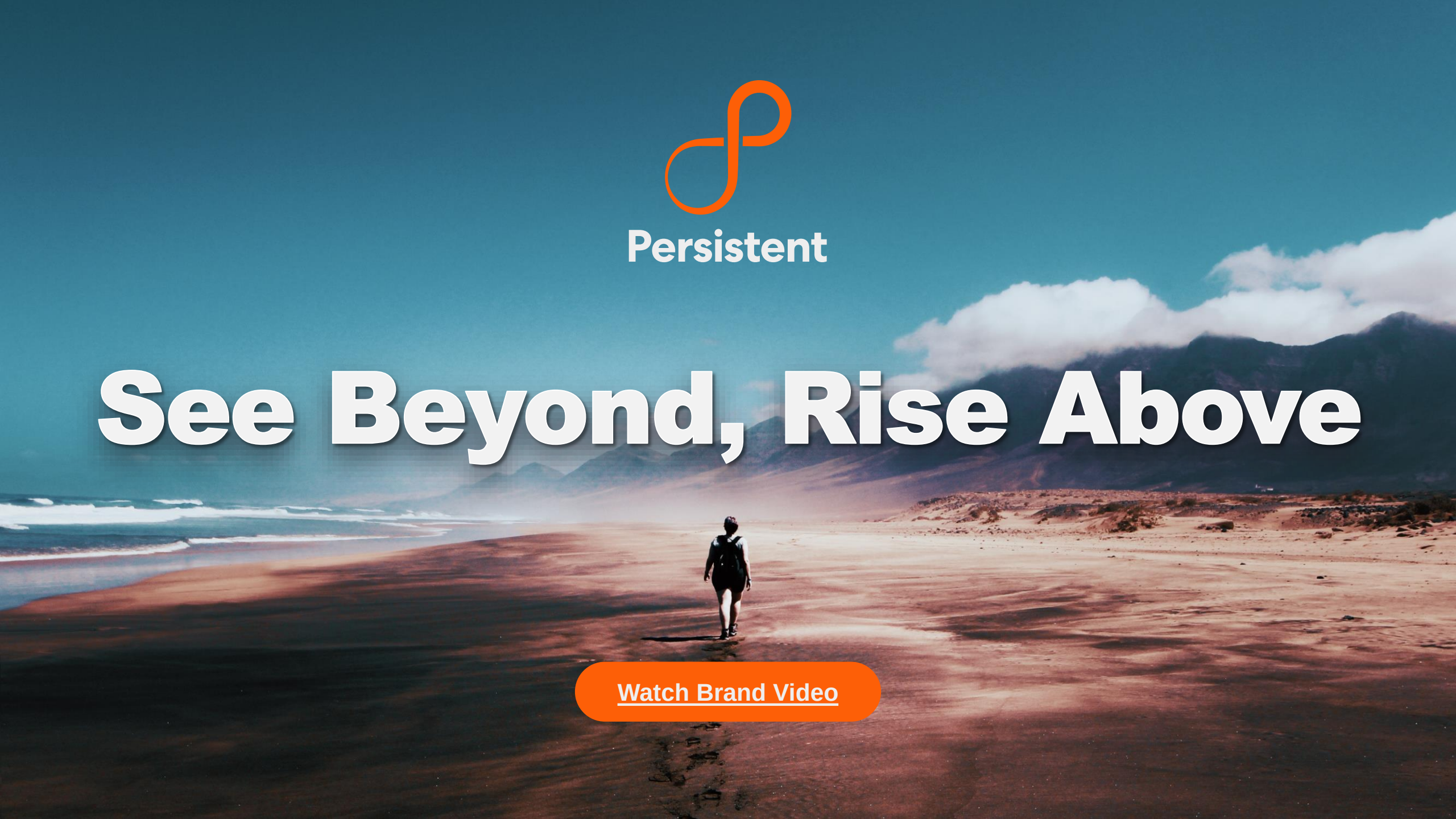
- Banks and Insurance sectors can automate customer onboarding with digital identity and expand customer base rapidly.
- Automate workflows end-to-end with digital identity & verifiable credentials
- Streamline KYC and AML processes to improve customer experience
- Cut costs significantly by lowering manual intervention.

Supply Chain Finance

- SSI enables more efficient and effective track and trace for real-world supply chains.
- SSI can be implemented to manage participants' data and store distributed files with decentralized access control.

KYC use case sequence diagram with SSI




Persistent
See Beyond, Rise Above
Watch Brand Video