City resident becomes a victim of identity theft

6 loans worth ₹4 lakh taken in his name by a fraudster from three different banks & 3 finance companies

Tampered Aadhaar and PAN cards of Sumit Khanna.

IDENTITY THEFT CASES BECOMING COMMON IN INDIA

NEVER SHARE YOUR IDENTITY PROOFS WITH UNKNOWN PEOPLE

FBI takes down marketplace that sold millions of stolen identities

Seventeen countries took part in the seizure and more than 100 were arrested.

APR 5, 2023

IDENTITY THEFT

- The two women received the cards on the addresses of their bungalows last week
- They were surprised to see photographs of different women and mismatch in dates of birth
- Their names and addresses were correct
- They reported the matter to the cybercrime cell

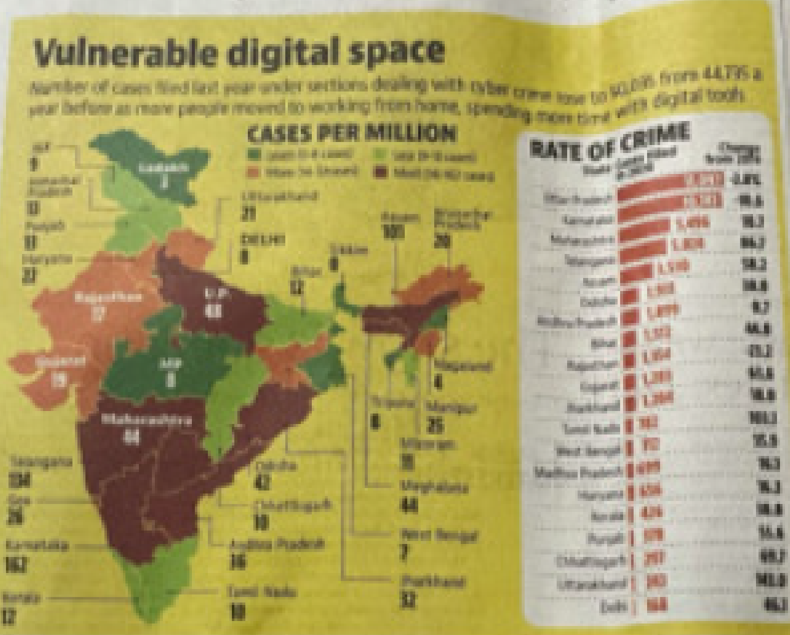
Police found the cards were made at an Aadhaar centre in Junnar

- The police traced the women, whose photos were on the cloned cards
- These women said the suspect had asked them to pose for the photographs

FORGING DOCUMENTS

- The accused made 7,000 illegal Aadhaar card enrolments/ data changes by uploading forged documents
- To carry out enrolments and corrections in Aadhaar cards, the accused procured 6 Aadhaar kits comprising laptops, iris and fingerprint scanners and cameras

Cyber crime registered 11.8% increase last yr: NCRB report



Bank executive held for identity theft, novel fraud

He used fake credentials to siphon money with a credit card

ABOUT ME

GAURAV TODWAL - SDE, MINIORANGE

Cyber Security Reseacher and Identity Management Enthusiast

Passionate in Unraveling Why and How

THE BATTLE AGAINST DIGITAL IDENTITY THEFT

Presented By: Gaurav Todwal, miniOrange

miniOrange

WHAT IS DIGITAL IDENTITY

Digital Identity encompasses the digital representation of individuals, organisations, or entities within the online realm. It comprises a collection of attributes, credentials, and characteristics that uniquely identify and distinguish a user in the digital space.

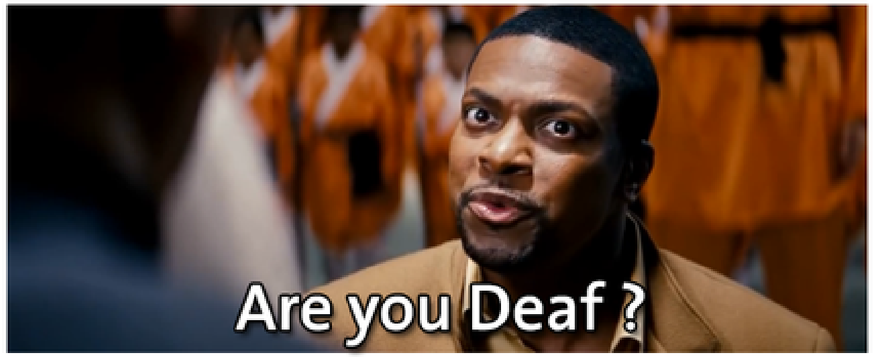
THE SHADOW SELF: UNDERSTANDING DIGITAL IDENTITY THEFT


Who are you ?


2
Yu

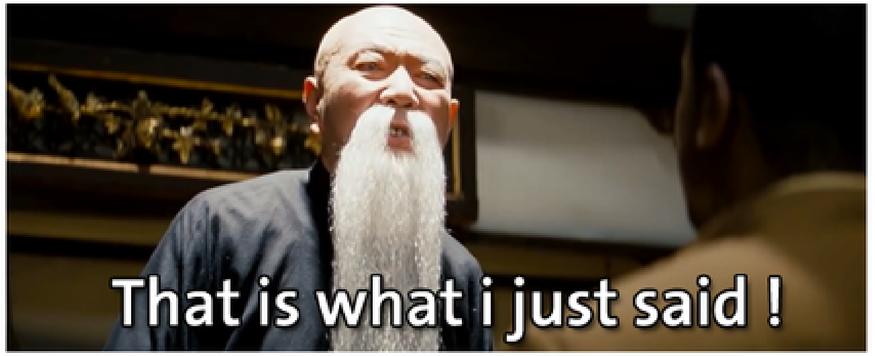

No not me, you !


Yes, i’m Yu


Are you Deaf ?


No, Yu is Blind.


i’m not blind. You Blind.


That is what i just said !

TYPES OF IDENTITY THEFT

Financial

The most common culprit involves stolen personal information (think Social Security numbers, credit card details) used for unauthorized charges or even opening new accounts in your name.

Office

Using your information to secure jobs or claim unemployment benefits can damage your employment history and reputation.

Medical

Stealing your data for medical services or prescriptions in your name creates a nightmare scenario. Inaccurate medical records, denied insurance claims, and financial burdens are just some of the potential harms.

Passport

Stolen passport information can be used for illegal travel or visa applications, putting your identity and safety at risk.

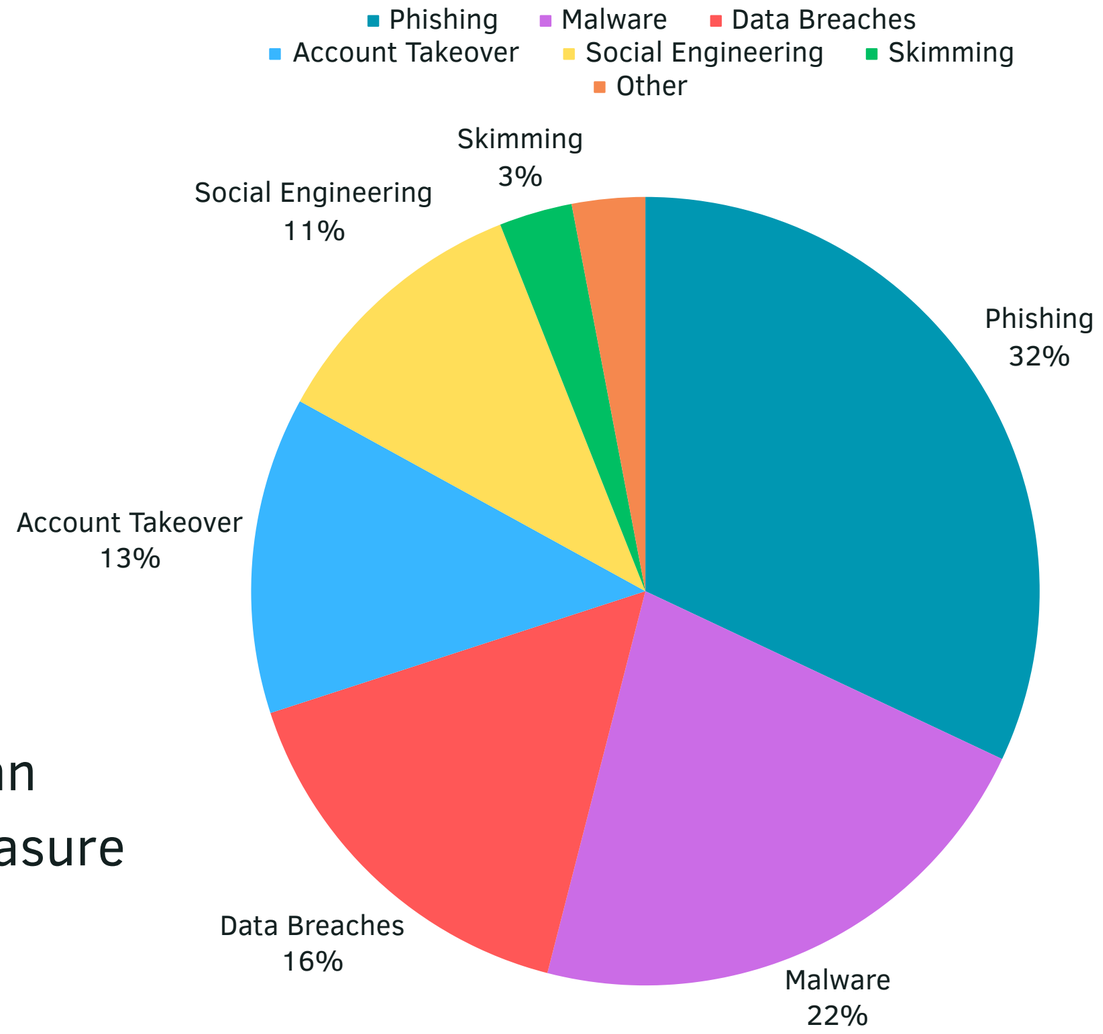
Child

Children are especially vulnerable to identity theft, with stolen information used for opening accounts and causing long-term damage.

HOW ARE IDENTITIES STOLEN?

As of Novemeber 2023

By understanding these **hacking methods**, you can build formidable defenses around your digital treasure chest.



Source: https://www.businesswire.com/news/home/20230530005194/en/New-North-America-Fraud-Statistics-Forced-Verification-and-AIDeepfake-Cases-Multiply-at-Alarming-Rates

miniOrange

HAS YOUR DATA BEEN COMPROMISED?

IdentityShield

Have I Been Pwned: Check if your email has been compromised in a data breach

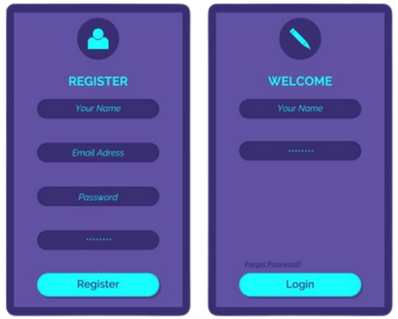
Have I Been Pwned allows you to search across multiple data breaches to see if your email addres...

haveibeenpwned.com

FROM DATA BREACH TO BUILDING DATA FORTRESS

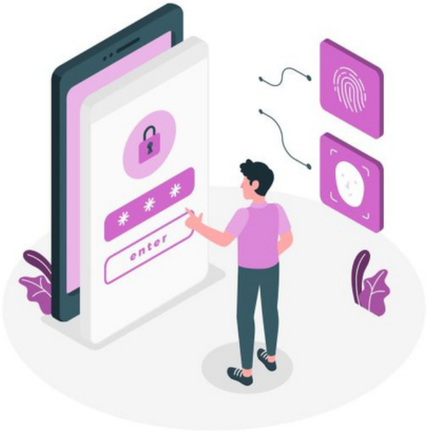
Let‘s understand how we can build the unbreakable fortress to safeguard our identity.

Centralized Identity



- Using the username and password to login into the sites or sites
- The bad player if had access to your password he can access any of your data.
- **Why to shift:** Password vulnerability
- **Where to shift:** Password Vault and Single Sign-On.

Federated Identity



- Arose when Web and Software as a Service were seeing broad adoption and password protection.
- User data is stored with an unknown federated source.
- **Why to shift:** Privacy and data protection
- **Where to shift:** Decentralized sources of authentication.

WHAT IS
DECENTRALIZED IDENTITY (DID)

Let’s Touch the Surface of DID:

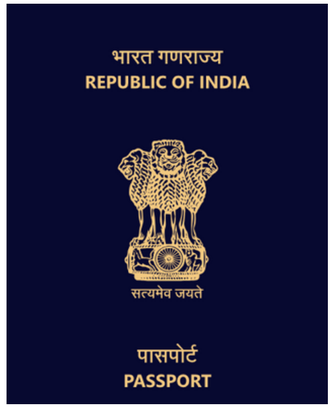
Individual Control and Enabling Trust

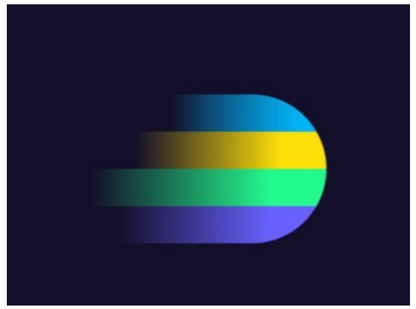
Decentralized identity gives the indiviual control over their own identity, so that they can decide how their personal information is shared and accessed, enabling trusted interactions while preserving privacy.

LET'S UNDERSTAND WITH AN EXAMPLE

You, Aadhar and Airport Authority of India

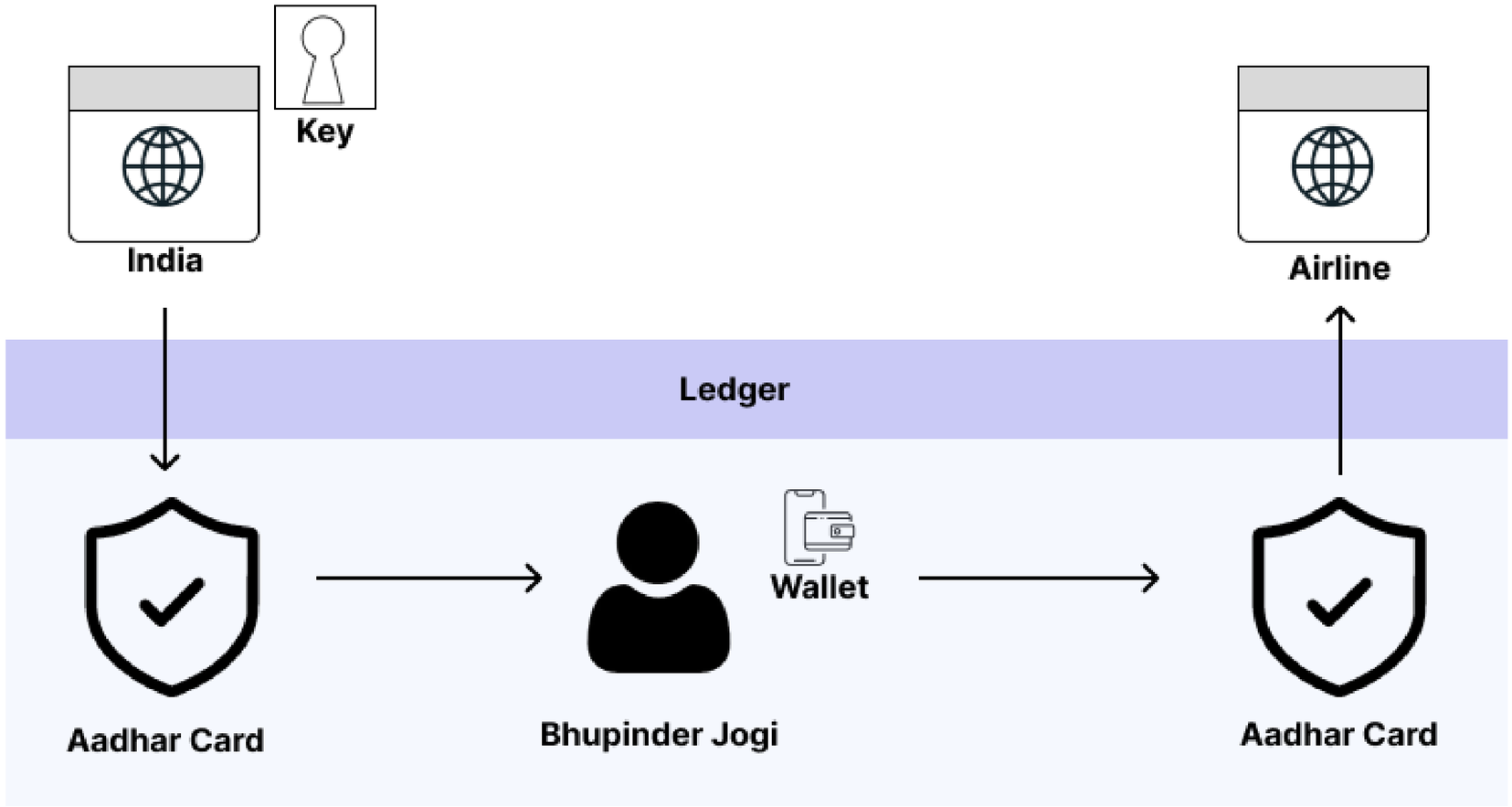
UNDERSTANDING WITH EXAMPLE





Issuer **Holder** **Verifier**

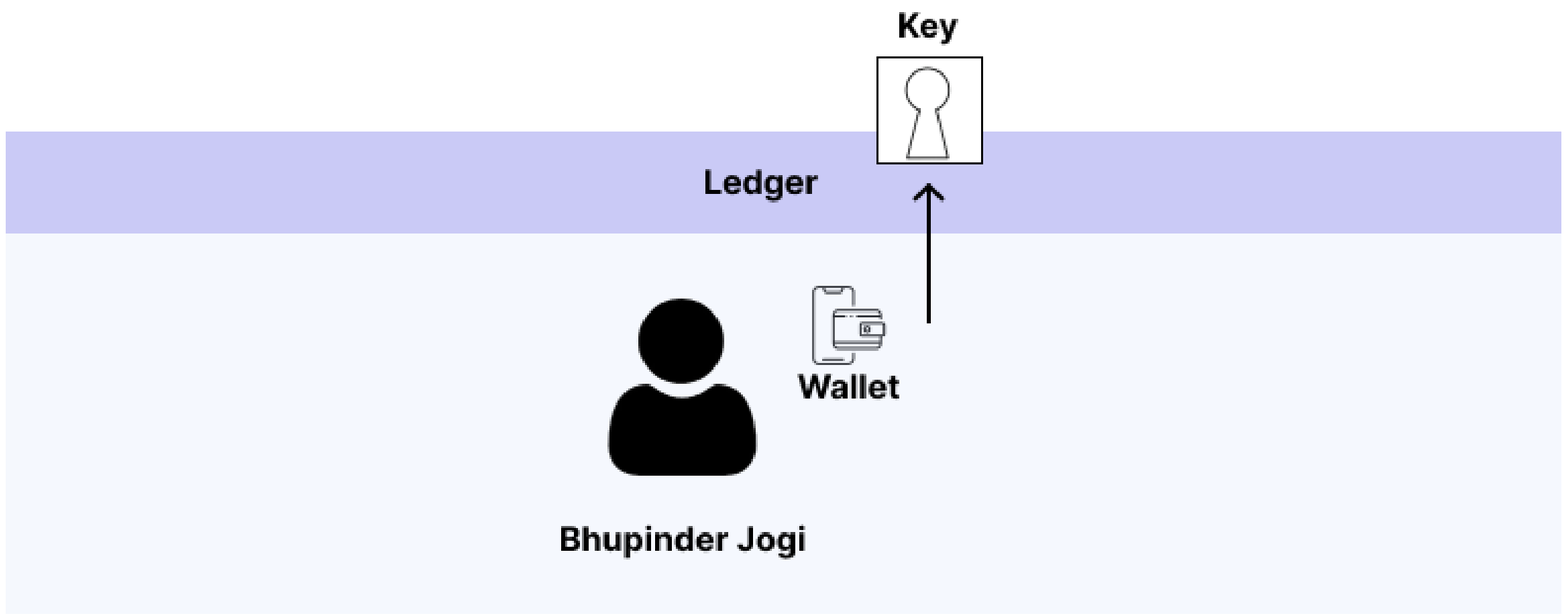
BASIC SETUP



Let's see how Bupinder Jogi, will obtain and user Digital Identity:

- Bupinder Jogi will install the identity wallet.
- He requests for the Identity which will be installed in his wallet.
- Jogi presents his digital identity to any of the Airport Authority.
- Airport Authority befor providing the service will validate the identity and confirm its belonging.

CREATE IDENTITY



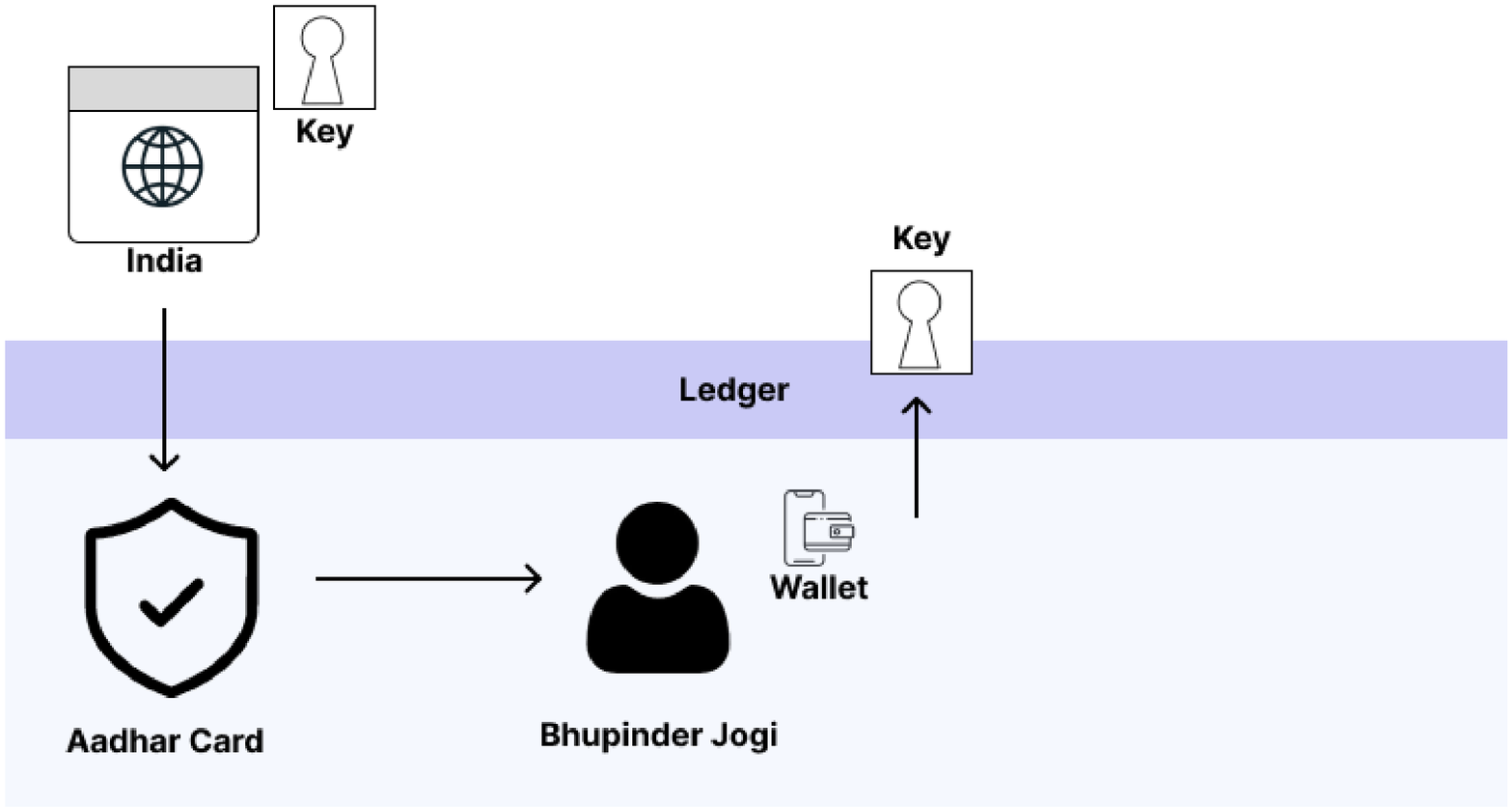
The wallet generates an identifier for Jogi along with key pair that is used to prove ownership of the identifier.

The private key is stored in the wallet and in return, the public key is published to the ledger.

Identifier will be used to identify the Jogi in this Digital Ecosystem.

The key will be used to verify the Jogi's identity.

FETCHING THE DOCUMENT

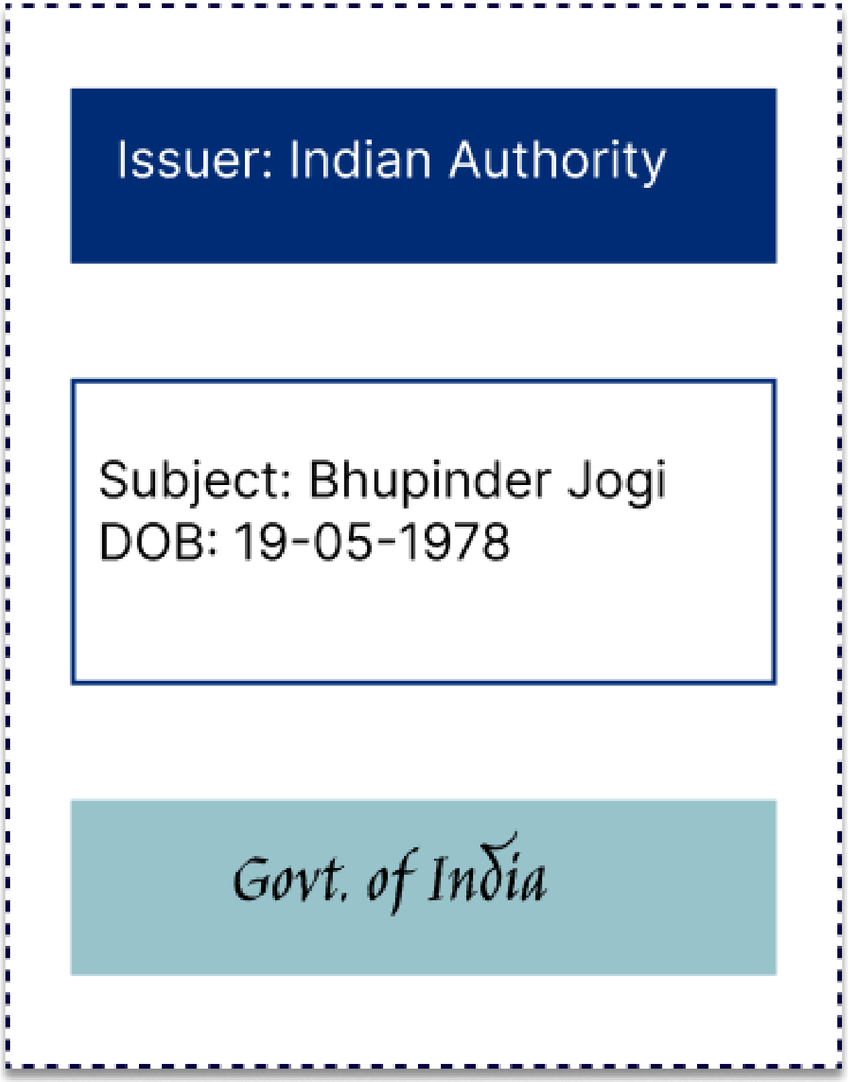


Now that our identity wallet is configured, Jogi request the documents like Aadhar Card, Driving license, etc from the Indian Government.

After being issued the digital document will be stored inside the wallet.

With just a single click , the document is seemlessly issued and stored in her wallet using the new Web API’s

DIGITAL DOCUMENT



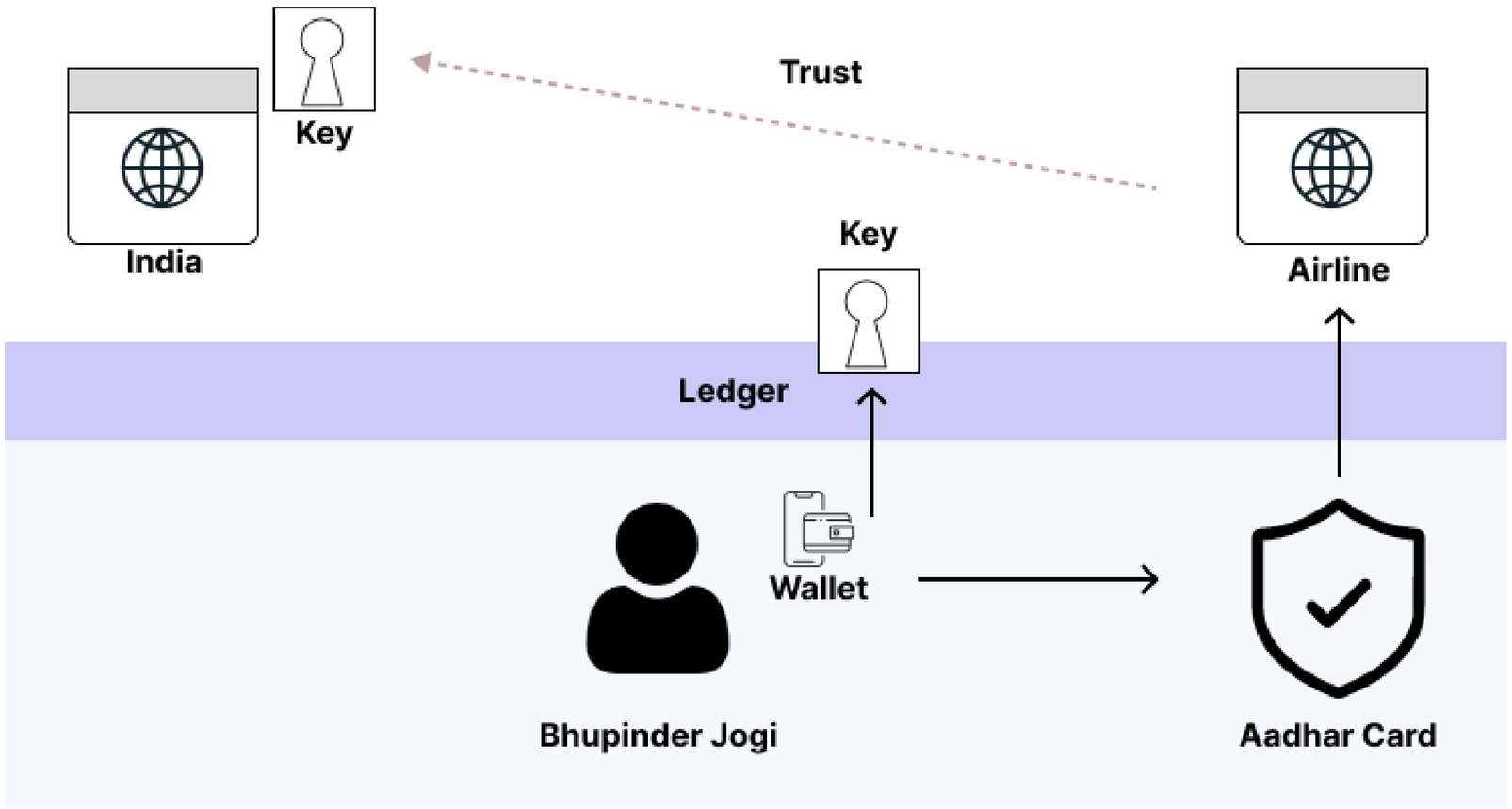
Digital Document Contains three major component:

1. Issuer
2. User claims
3. Signature

The signature can be used to validate the document is issued by trusted source or not.

This signature is equivalent to the anti-tempering measures present in our physical passport.

VERIFYING THE DOCUMENT

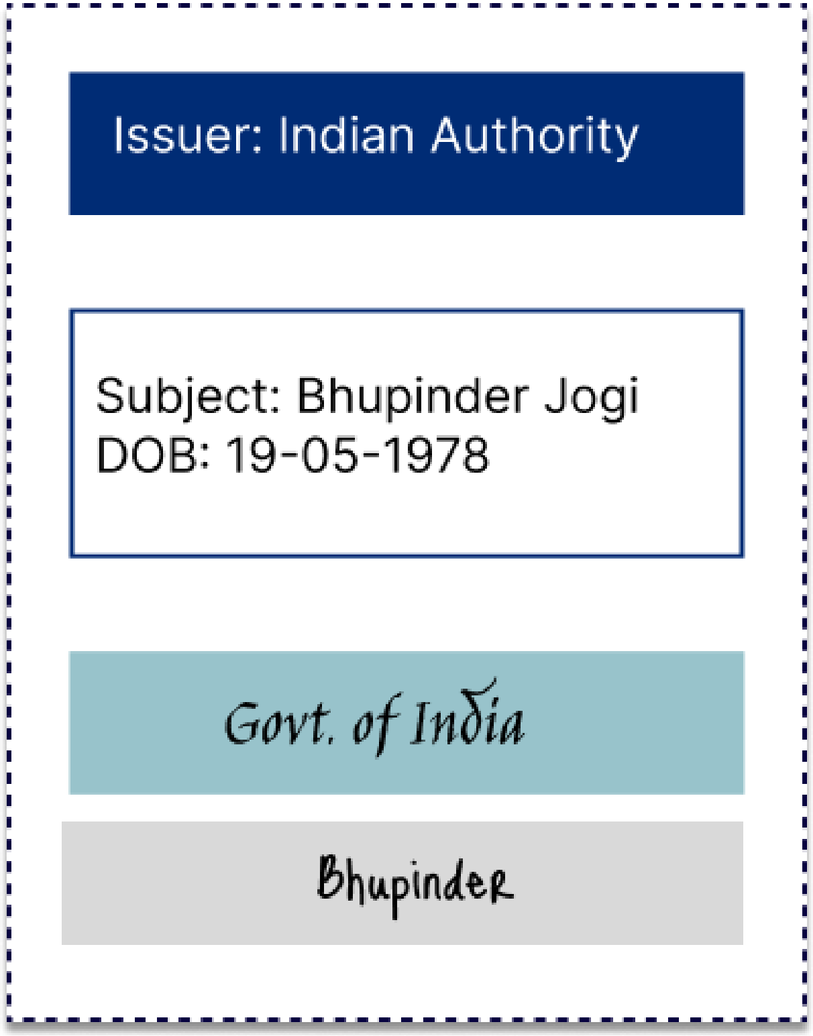


Just as the federated identity (SAML and OAuth) the service provider or verifier had a trust relationship with the Issuer.

The trust relationship configures the information about where the public key is stored

The public key is used to verify signature and verfiy the authority of the document

AADHAR PRESENTATION:



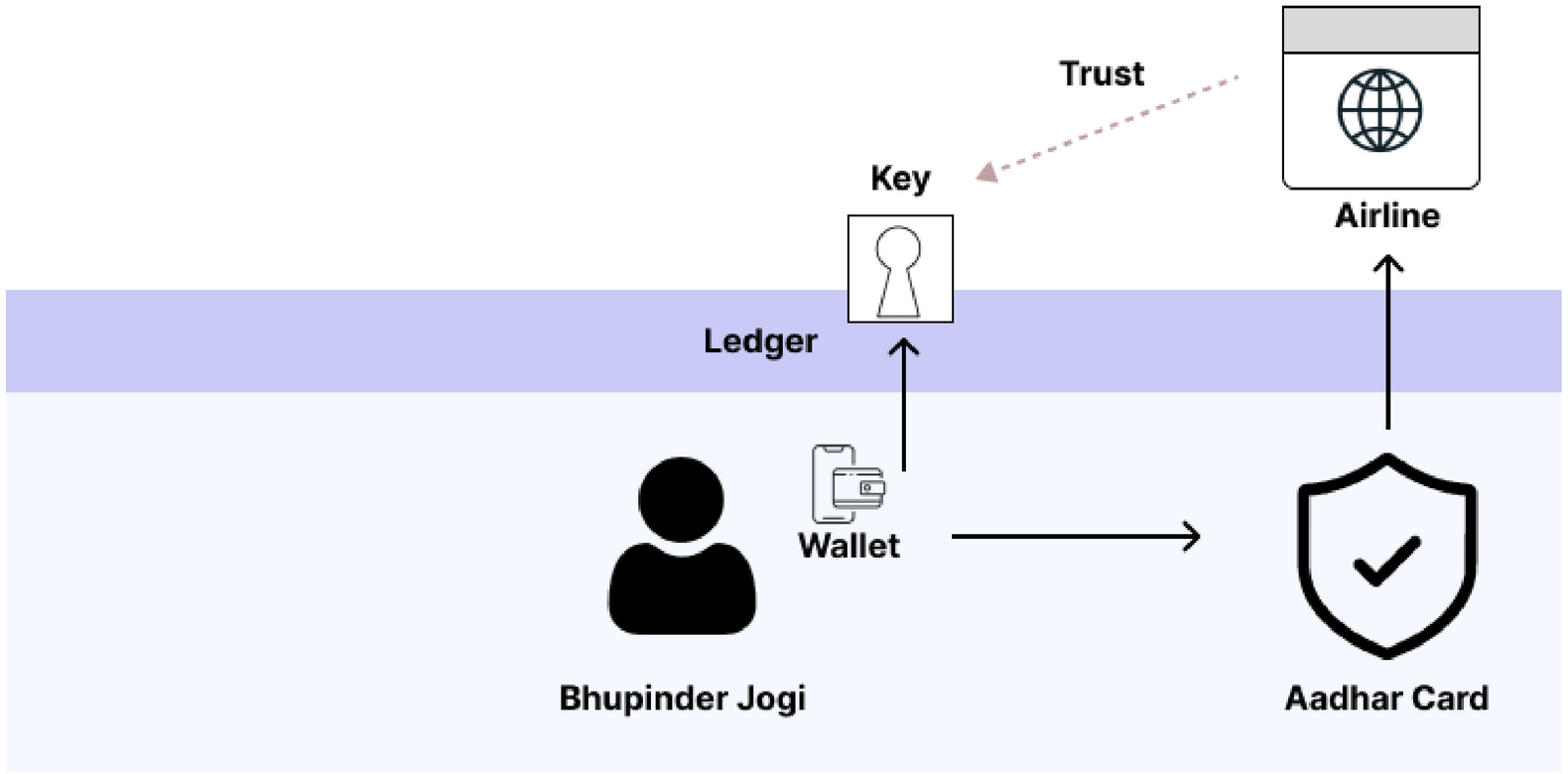
The Aadhar itself is encompassed by another digital signature from the wallet.

This will allow the service provider to verify two things:

1. The ID is issued from the correct authority
2. The person presenting the ID is the legit person or not

Verifying the holder signature will require the holder's public key

VERIFYING HOLDER



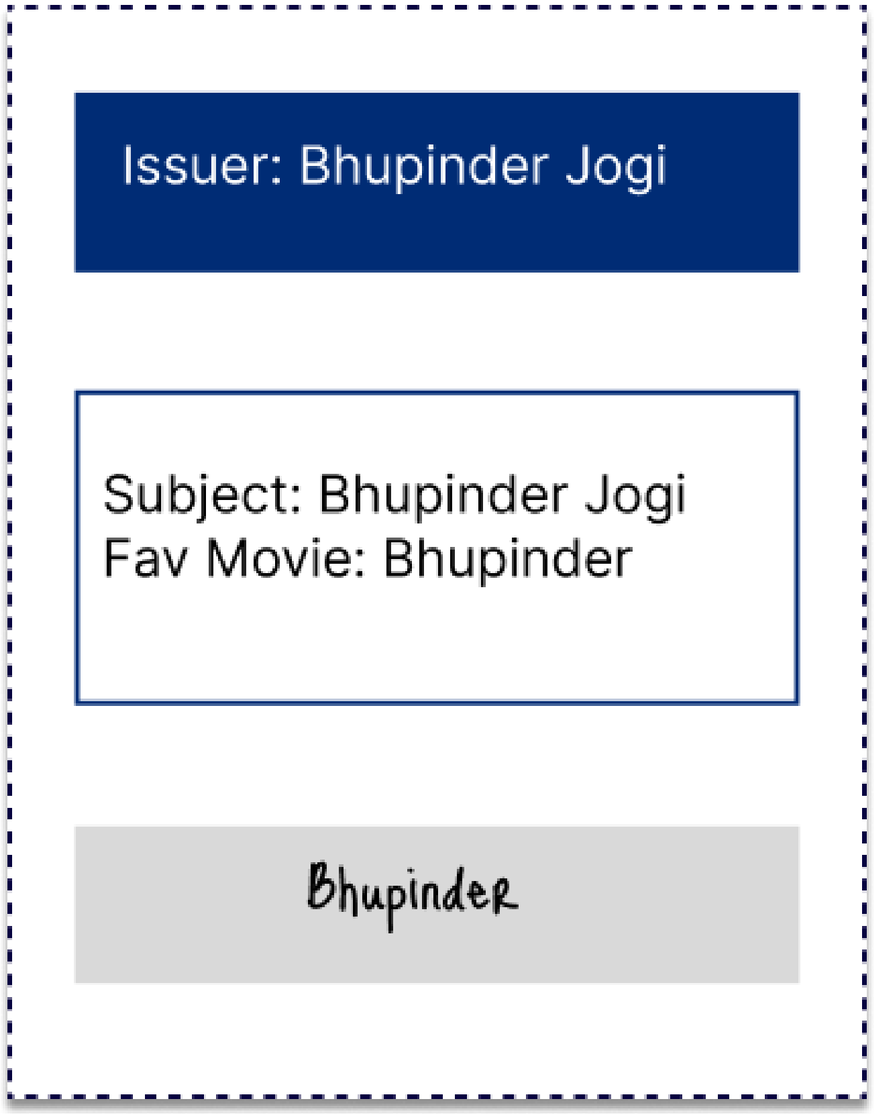
This bring us to the end of this Digital System ecosystem.

The public key registered on the ledger will be required to verify the holder's identity.

After being verified, the service provider can now allow the holder to access the service.

HOW WE ARE CONTROLLING OUR IDENTITY?

SELF-SIGNED CREDENTIALS



Users can now choose to issue Self-Signed credentials about themselves that don't need to be made by the third party

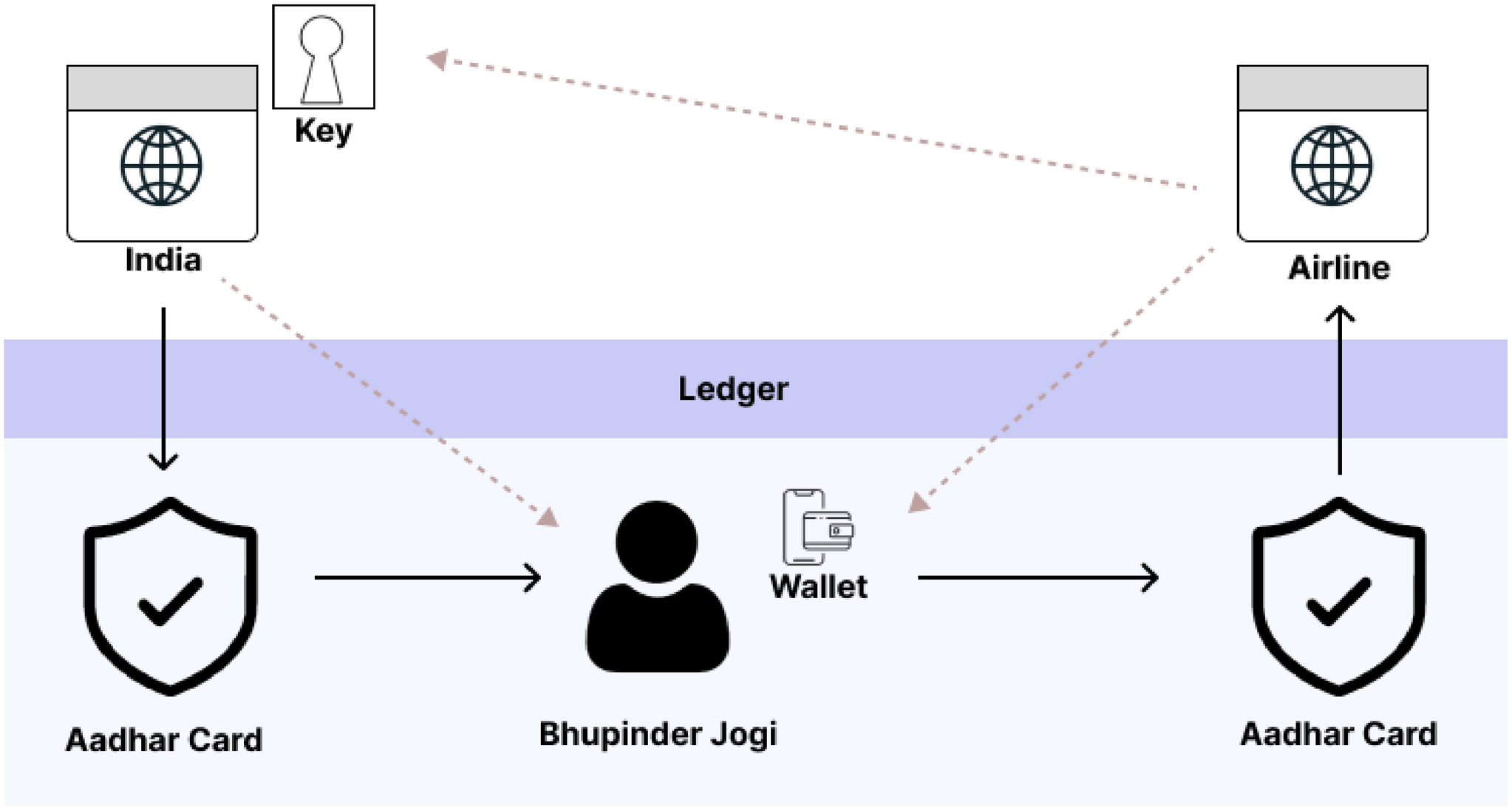
This functionality was unavailable in the Federated Identity system because the user has no cryptographic keys only the website does.

The cryptographic keys are the major requirement to generate the Verifiable credentials.

This notion of the self-signed credentials give the rise to the term Self-Soverign Identity

Transfer of the credentials is in control of the holder who is showcasing the identity

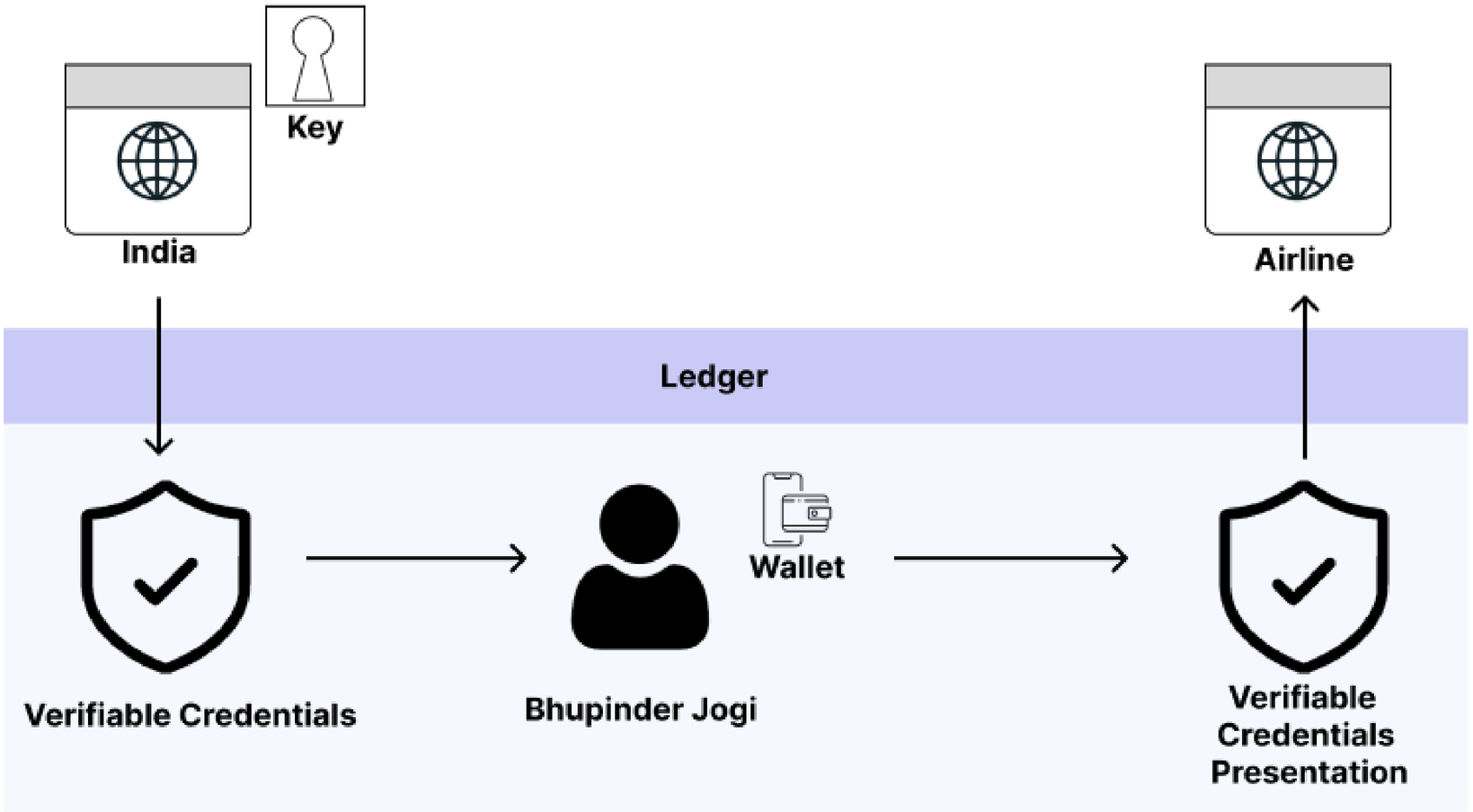
TRUST TRIANGLE



LET’S DIG DEEP INTO DECENTRALIZED IDENTITY ECOSYSTEM

miniOrange

THE ECOSYTEM



The major actors in the Decentralized Identity Ecosystem are:

1. Wallet
2. Ledger
3. Verifiable Credentials

DIGITAL WALLET

Wallet are the application which allows the user to manage and control there identity.

The main function of the wallet is to manage the identifiers and cryptographic key associated with those identifiers.

Wallet also manages the keys and information published on the distributed ledger.

Exchanging of the verifiable credentials with issuer and verifier is managed through the wallet.

miniOrange

IdentityShield

DECENTRALIZED IDENTIFIERS

did:ethr:dfv-gtak-pab7-jen7-p4e

Decentralized Identifiers are globally unique and don’t require any central registeries.

DID contains three major part:

1. Preffix
2. Method (Ledger)
3. Identifier

DID is resolvable and its ownership can be proven with the public key cryptography.

miniOrange

LEDGERS

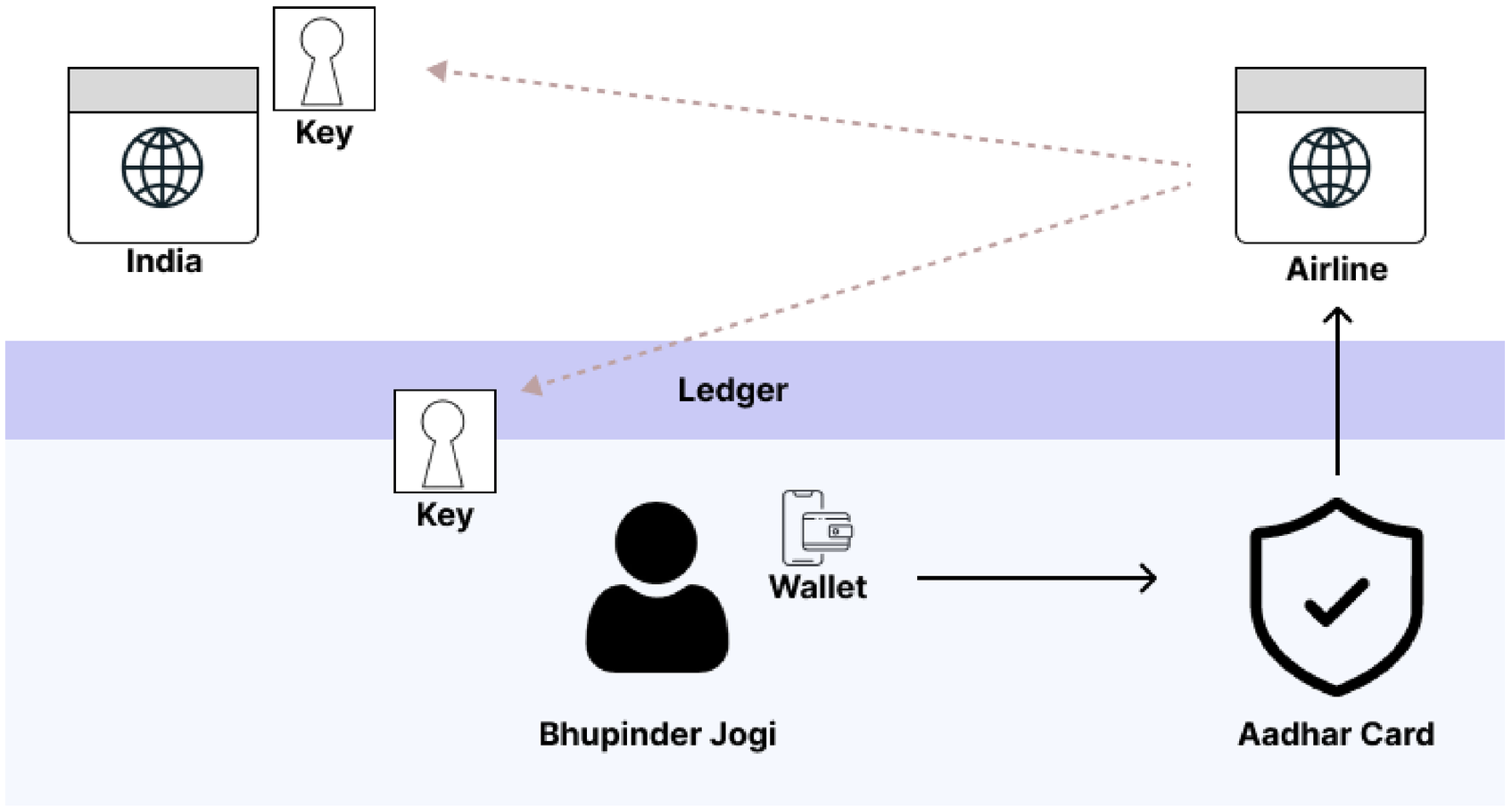
Wallet, in addition of storing credentials, keys and secrets also publishes an indiviual public keys to the ledger.

Legers helps in making the decentralized ecosystem network centric.

The method contained in DID will specify how to publish, update and deactivate the identifier on the ledger.

Create, Update and Delete functionality is performed by indiviual thriough the wallet.

VERIFYING CREDENTIALS



Verifying a credentials requries a public key, need to validate the digital signature on the credential

WHAT'S NEXT ?

TAKE AWAY:

WE VALUE YOUR FEEDBACK

Connect with me.

+91 8949461981

gaurav.todwal@xecurify.com

gauravtodwal