Servidor de Autenticación

MEJORA DE LA EXPERIENCIA DE USUARIO PARA LA ADOPCIÓN DE LA WEB3 Y SOLUCIONES CON TECNOLOGÍA BLOCKCHAIN

21 de Mayo 2025

i2cat

Ignasi Oliva

Head of Innovation Blockchain and DLT

Cybersecurity & Blockchain DLT Research Group

Identification

VS

Identity

PRIVACY

STORAGE

i2cat

MANAGEMENT

CONTROL

USE

PRODUCT

CHALLENGES

DATA SECURITY

PRIVACY

USABILITY

Old & New Challengues

Username & Password

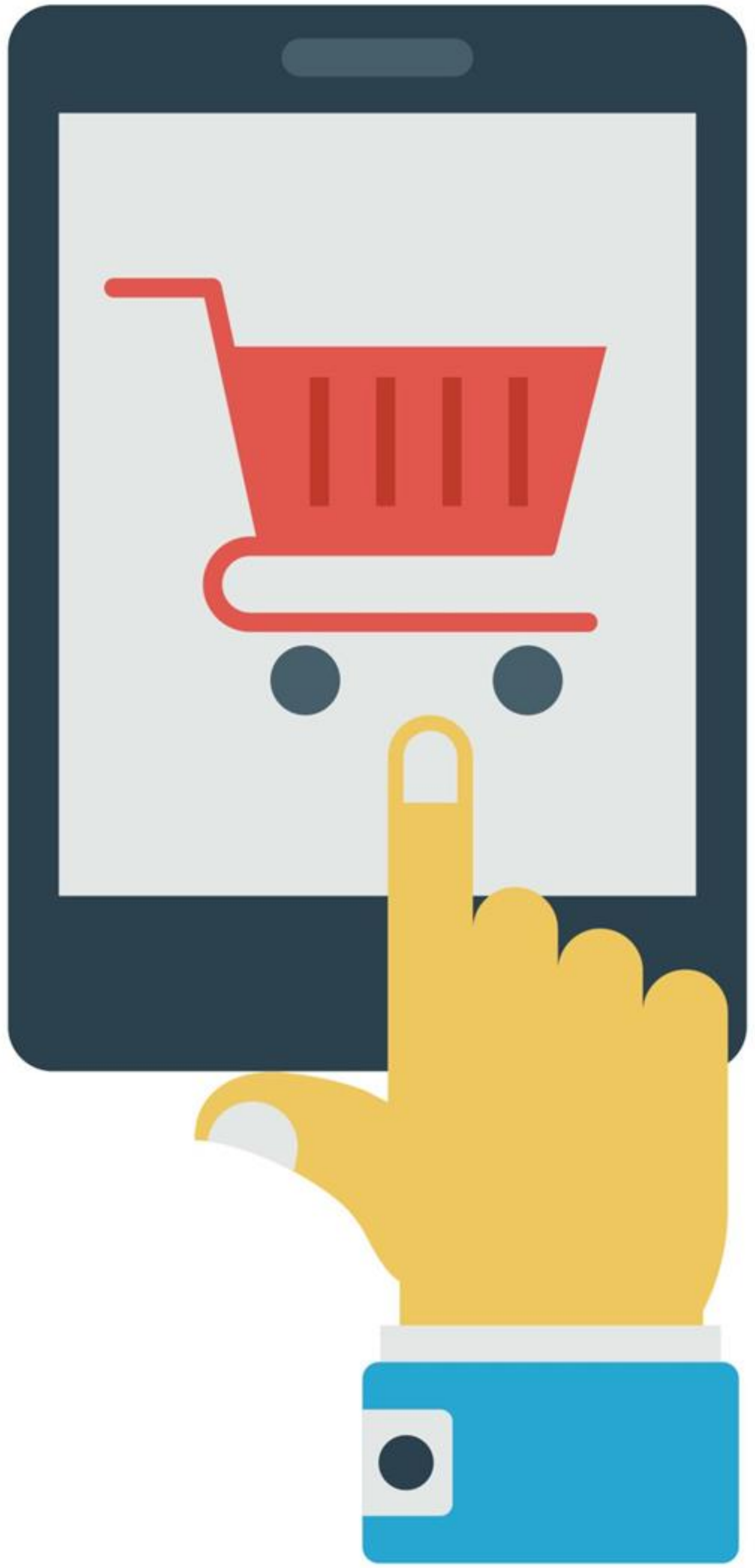
- 1960, initially, passwords were used to protect individual user *access to time-shared mainframe computers*.
- In 1974, Robert Morris developed one-way encryption (hashing) to store passwords securely.
- In 1979, Morris and Ken Thompson coined the term "salt" to describe adding random characters to stored passwords to add difficulty to brute force attacks on database leaks.

Most commonly used and accepted by the average user.

DNS and X.509

- X.509 was originally conceived in the late 1980s, using public key cryptography to issue and verify certificates.
- Linked to DNS to support TLS/SSL, as the basis for HTTPS.
- Managed transparently by corporations and the public sector.
- Essential Components of E-commerce Security.

This complexity is hidden, providing secure browsing without user management.



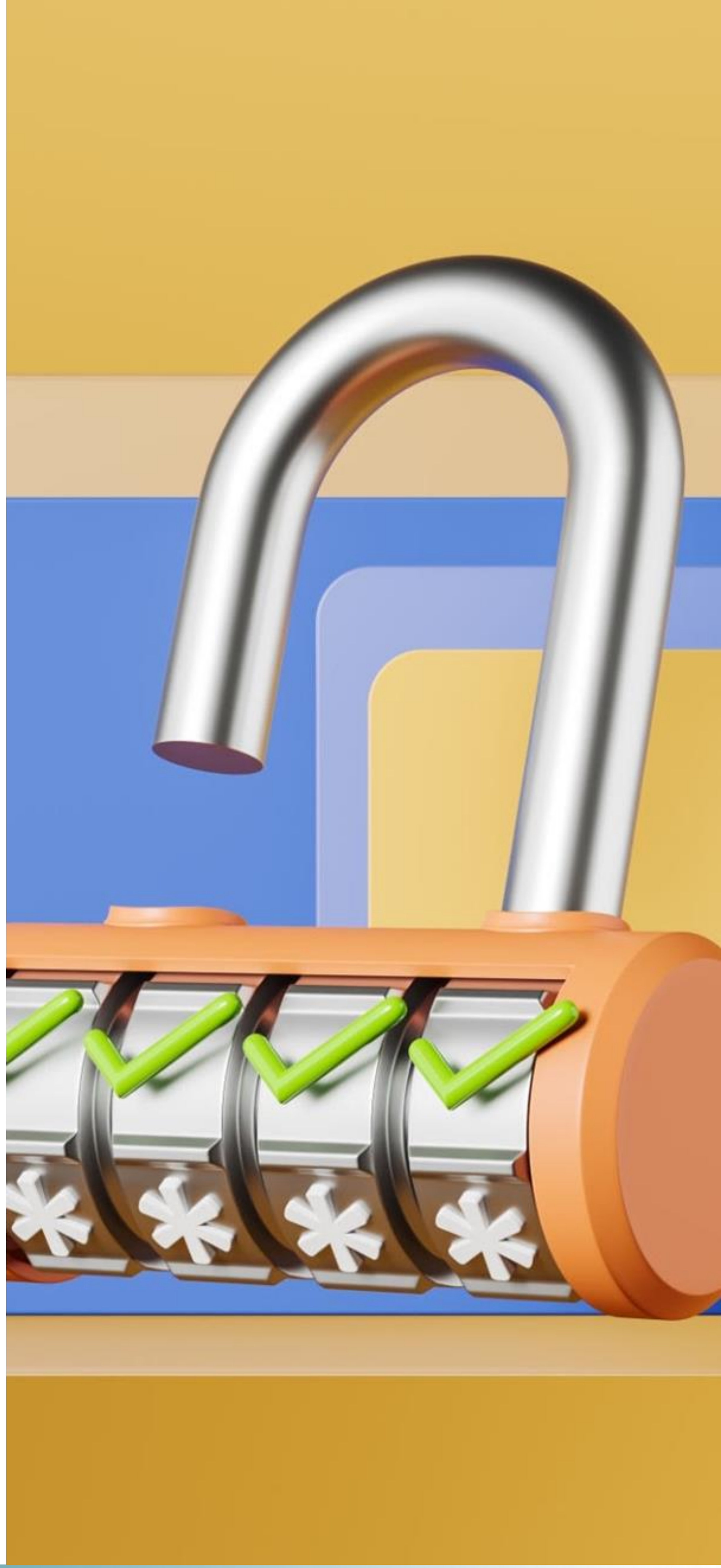
i2cat

Pretty Good Privacy (PGP)

- Developed by Phil Zimmerma**nn** in 1991 as a tool for secure email and file encryption.
- Built on a *"Web of Trust" model*: users manually validate and sign each other’s public keys.
- Emphasized decentralization, user empowerment, and grassroots adoption.

Adoption limited by usability challenges and trust management complexity.

i2cat



OAuth 2.0 and OpenID Connect (OIDC)

OpenID Provider
z.B. Yahoo!
Google,
VeriSign,
MySpace,
PayPal, ...
6. Die Daten
2. Die OpenID Erm
OpenID
er Endnutzer wird zum Authentifizieren an den OpenID P
l sich bei der Relying Party anmelden und gibt dazu seinen Ope
Relying Part weiter. Dieser wird mitgeteilt, ob der Anmeld

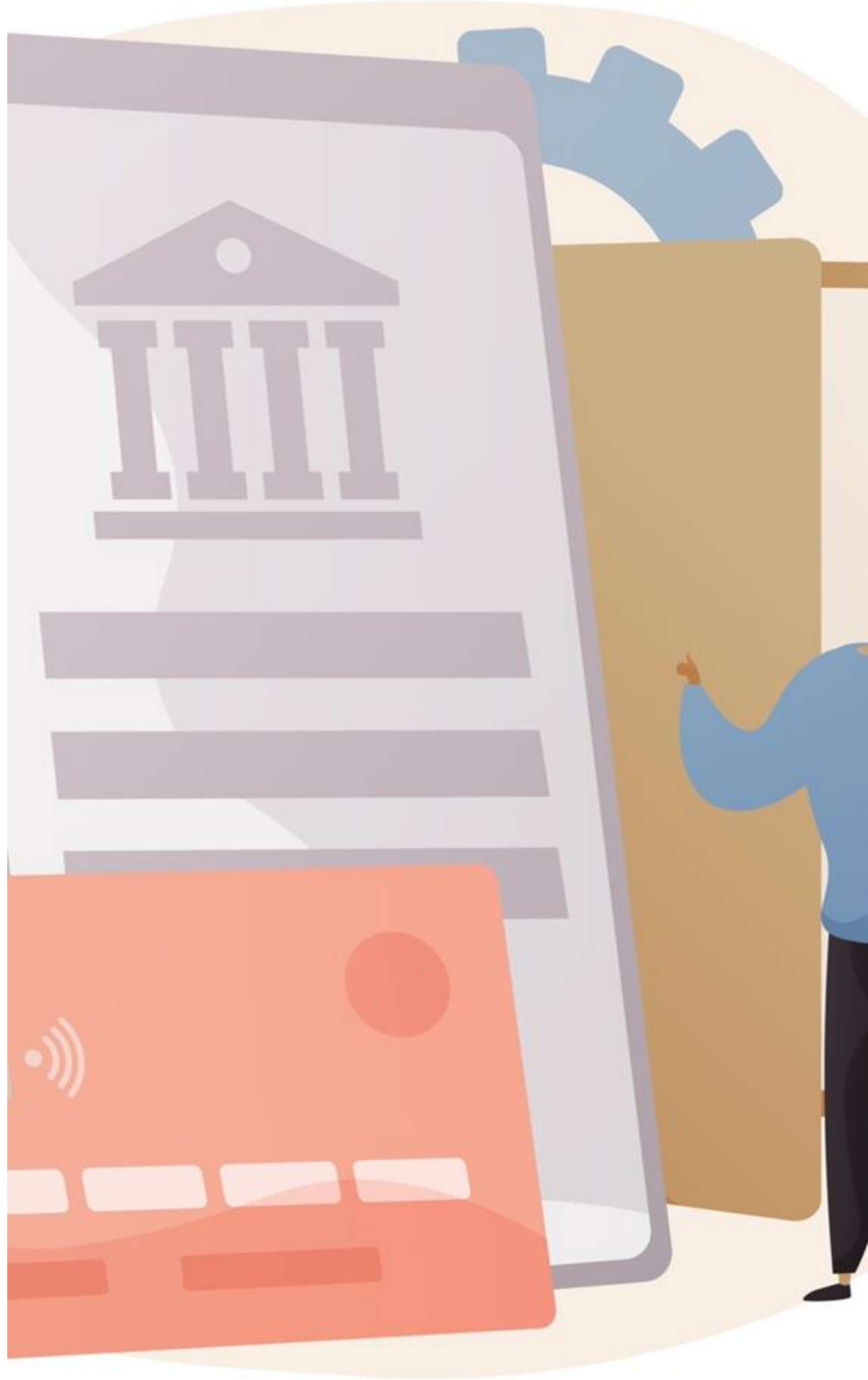
- ❑ OAuth 2.0 - An authorization framework, not originally designed for authentication.
- ❑ OpenID Connect, built on top of OAuth 2.0 to provide authentication capabilities.
- ❑ Identity is managed by a trusted third-party (Identity Provider).
- ❑ Reduces password fatigue and centralizes identity policy enforcement.

Convenience vs. Centralization Risk (IdP becomes a critical point of control).

Verifiable credentials, DIDs and web of trust

- W3C Decentralized Identifier & VCs Working Group formed in 2019.
- DIDs are persistent, self-owned identifiers that do not rely on a central authority.
- Digital credentials issued by authorities (e.g., universities, governments) that can be cryptographically verified.

Enables use cases like self-sovereign identity (SSI), cross-border credentials, and privacy-preserving authentication.



i2cat

Wireless Systems

- Radius developed in 1991 originally for dial-up modem authentication. Forms the backbone of 802.1X authentication in enterprise Wi-Fi and wired networks today.
- Cellular authentication relies on shared secret keys stored both on the SIM card (Subscriber Identity Module) and on the carrier’s authentication server (e.g., HLR/HSS in 3G/4G, AUSF in 5G).

RADIUS and cellular network authentication are widely adopted and well-established technologies familiar to both providers and users.

i2cat

Bitcoin, blockchain and beyond

- 2009 Bitcoin Introduces public key cryptography for payments.
- 2015 Ethereum generalizes the concept with Smart Contracts.
- 2016-2018 Emergence of Web3 authentication via wallets.
- Digital Signature Protocol becomes a login method; using eth_sign became a de facto decentralized authentication mechanism.
- EIP-4361- *Off-chain authentication for Ethereum accounts to establish sessions.*

Software wallets like MetaMask simplified crypto authentication, but mainstream adoption still faces usability hurdles.

From mainframe passwords to smart contract wallets.

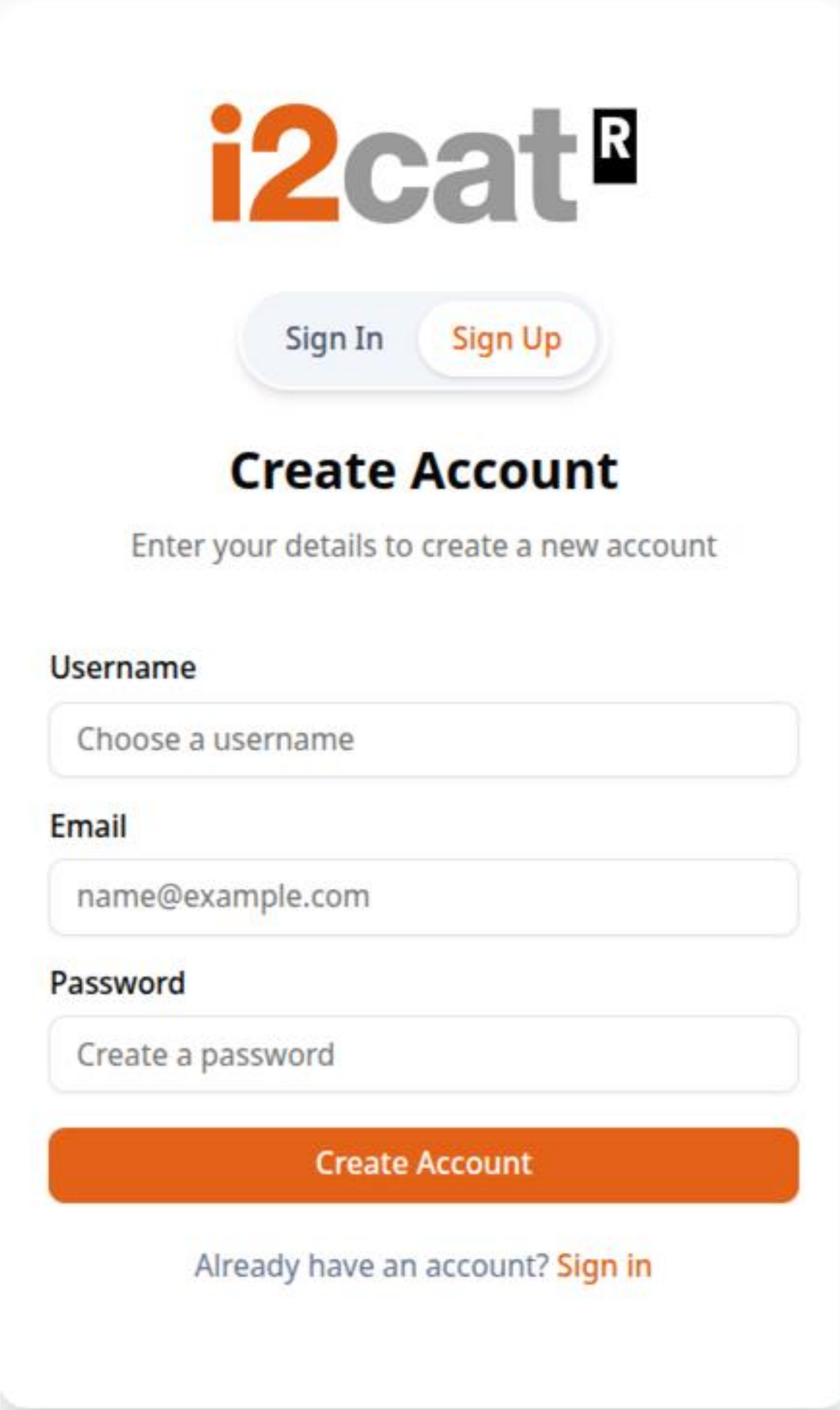
Account abstraction (ERC-4337)

Enables smart contract wallets to support familiar logins, bridging legacy authentication models with decentralized asset management.

i2cat

Demo

- i2CAT has participated in numerous R&D projects involving identity and access management, from classic user-password models to federated identity systems and telco-grade protocols.
- Hands-on work with OAuth2, OpenID Connect, RADIUS, SIM-based and federated authentication has shaped our understanding of interoperable identity systems.
- The blockchain team identified the need to consolidate internal expertise and tools to support diverse authentication use cases, from Web2 to Web3.
- We developed a flexible internal stack bridging traditional password-based login with Ethereum account abstraction (ERC-4337), enabling seamless identity integration.
- The demo showcases a simple local password login system linked to smart contract-based asset management — illustrating how users can onboard Web3 without wallets or seed phrases.



Create Account

Enter your details to create a new account

Username

Choose a username

Email

name@example.com

Password

Create a password

Already have an account? Sign in

Q&A