Privacy e anonimato nelle reti

Tecnologie, rischi e soluzioni nel mondo digitale

A cura di: *Andrea Mazzucato*

Introduzione

Viviamo in una società iperconnessa, dove ogni comunicazione lascia una traccia.
In questa presentazione analizzerò:

- *cosa sono privacy e anonimato nel contesto delle reti;*
- *quali sono le vulnerabilità più comuni;*
- *le soluzioni tecniche più efficaci;*
- *le implicazioni normative;*
- *e infine, come ho affrontato concretamente questi temi progettando FinBlock.*

Privacy e anonimato

Privacy = il diritto a controllare i propri dati personali. È un diritto umano riconosciuto anche dall'art. 8 della Carta dei Diritti UE.

Anonimato = agire in rete senza essere identificabili direttamente.

Attenzione: anonimato non è impunità. Esistono tecniche forensi (come l'analisi dei metadati o delle firme digitali) che permettono di identificare i responsabili in caso di reato.

Come la rete espone i nostri dati

Ogni livello del modello ISO/OSI può rappresentare una minaccia per la privacy:

Livello	*Rischio per la privacy*
Livello 2	*MAC address e probe Wi-Fi → identificazione dispositivi*
Livello 3	*IP address → tracciamento geolocalizzato*
Livello 4	*TCP header → fingerprinting delle connessioni*
Livello 7	*Header HTTP, cookies, DNS → identificazione utenti*

Tecnologie per la difesa della privacy

Tecniche fondamentali:

- *Crittografia (TLS, RSA, AES): protegge dati in transito e a riposo.*
- *VPN: nasconde IP e crittografa il traffico.*
- *DNS-over-HTTPS/TLS: impedisce il tracciamento via DNS.*
- *Browser sicuri: Brave, Firefox (con uBlock, Privacy Badger).*
- *Tor: navigazione anonima basata su rimbalzi criptati.*
- *Autenticazione a 2 o più fattori (2FA, MFA)*

Blockchain: pseudonimia ≠ anonimato

Molti credono che la blockchain sia “anonima”. In realtà è solo pseudonima:

- Ogni wallet è identificato da un indirizzo pubblico.
- Le transazioni sono immutabili e visibili a tutti.
- Se un indirizzo viene collegato a una persona (es. via exchange), tutte le sue operazioni diventano tracciabili per sempre.

FinBlock e il design della privacy (con Web3)

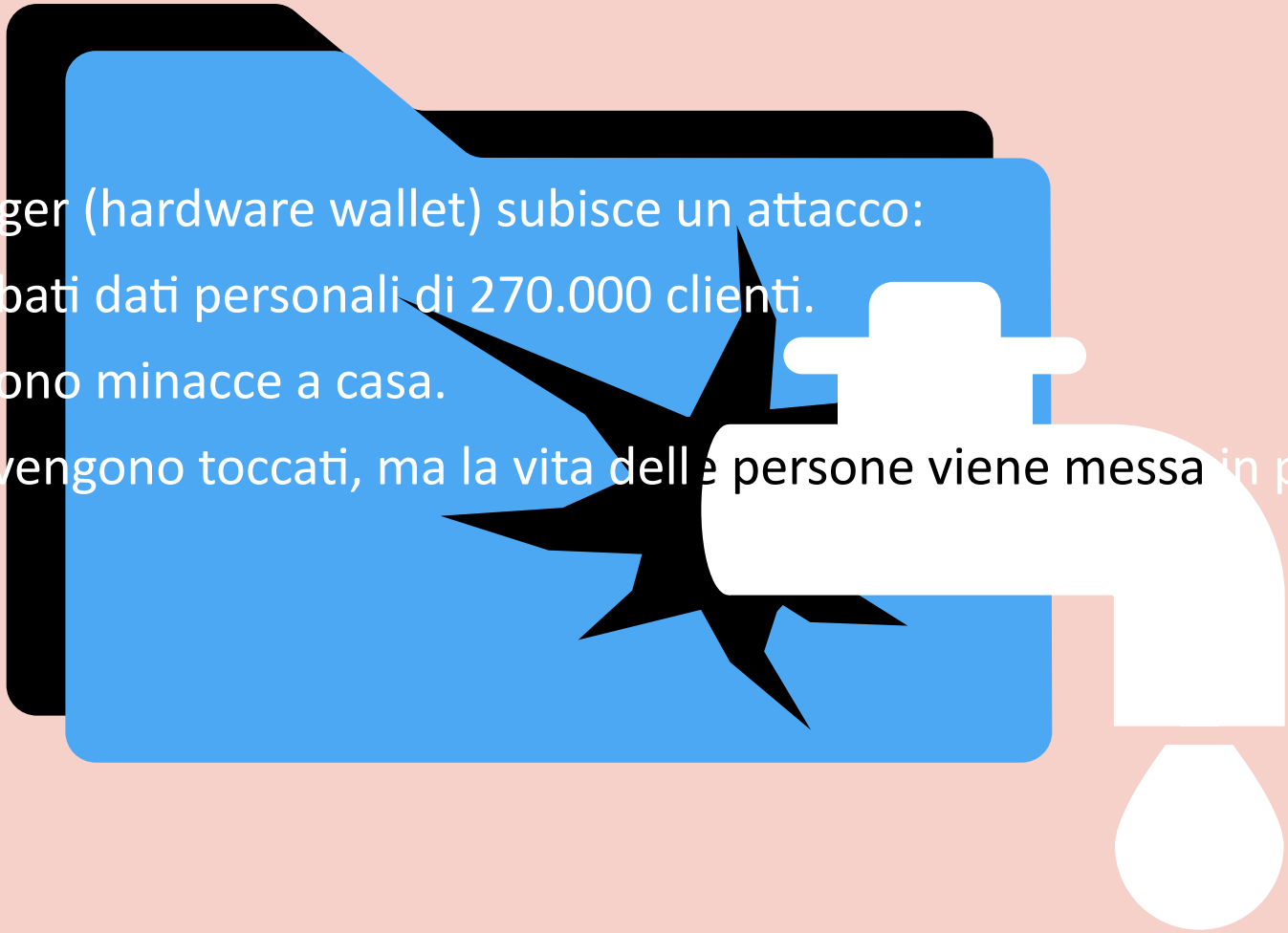
Nel progettare FinBlock, ho applicato i principi del "privacy by design":

- *Data minimization: niente nomi, email o indirizzi.*
- *Pseudonimizzazione: ogni utente è identificato da un codice interno.*
- *Dati sensibili crittografati e salvati off-chain, non sulla blockchain.*

Accesso tramite Web3:

- *L'utente si collega tramite il proprio wallet decentralizzato (es. MetaMask).*
- *Il sistema invia una richiesta crittografica → firmata dall'utente.*
- *Non c'è bisogno di password né registrazione.*
- *Nessun database centrale: l'identità è gestita in modo distribuito e sicuro.*
- *Web3 login = meno rischi, più controllo per l'utente.*

Caso reale: il data leak di Ledger



Nel 2020, Ledger (hardware wallet) subisce un attacco:

- Vengono rubati dati personali di 270.000 clienti.
- Alcuni ricevono minacce a casa.
- I fondi non vengono toccati, ma la vita delle persone viene messa in pericolo.

GDPR: la normativa europea

Il GDPR impone:

- Privacy by design / by default
- Data minimization
- Diritto all'oblio, rettifica, portabilità
- Consenso informato e revocabile

In FinBlock:

- Non raccogliamo dati inutili.
- Tutti i dati off-chain sono crittografati.
- L’utente ha accesso tramite dashboard per modificarli o cancellarli.

Schema tecnico semplificato

1. L’utente accede tramite Web3 wallet → nessun login tradizionale.
2. Firma una richiesta crittografica → autenticazione.
3. Il sistema genera un ID pseudonimo (non collegabile al nome reale).
4. Dati sensibili (tipo asset/token posseduti) → archiviati off-chain, cifrati.
5. Blockchain = solo hash verificabili, firma digitale, log della transazione.

Così abbiamo trasparenza, tracciabilità, ma anche privacy.

Conclusioni

La privacy non è un optional: è una condizione minima per essere liberi.

Il Web non dimentica. La blockchain nemmeno.

La vera innovazione è quella che rispetta le persone.