

— QUADERNO I —

LA CUSTODIA

Self-custody, responsabilità, perdita,
metodo e maturità operativa davanti al valore digitale

— Possedere davvero qualcosa
significa anche poterlo perdere. —



custody://la-custodia

| tomo I

| format ebook breve · 60-80 pagine

F L O R I A N O R I G H E T T I

ESTRATTO GRATUITO | QUADERNO I

La Custodia

Quaderni di Custodia Digitale · Quaderno I

Floriano Righetti

Edizione definitiva · settembre 2026

© 2026 Floriano Righetti

Tutti i diritti riservati.

florianorighetti.ch

Questo quaderno ha finalità culturali e informative. Non costituisce consulenza finanziaria, legale, fiscale o d'investimento. Le indicazioni vanno valutate rispetto agli strumenti e alle circostanze concrete.

Non inserire segreti reali nei modelli del libro. I documenti compilati restano riservati anche quando non contengono credenziali. Le scene narrative sono esempi illustrativi.

Testo e riferimenti verificati il 12 settembre 2026.

ESTRATTO GRATUITO

Prologo: La porta che non si può forzare (pp. 5-8).

Il testo e la numerazione delle pagine riproducono l'edizione integrale. L'indice presenta il libro completo: i capitoli non inclusi in questa anteprima non sono collegati.

La pagina finale rimanda alla scheda del quaderno sul sito dell'autore.

Indice

Nota al lettore.....	4
Prologo	5
1 Che cosa significa custodire	9
2 La chiave e il segreto	16
3 La falsa comodità.....	23
4 La mappa dei rischi	30
5 Mettere distanza.....	39
6 Custodire insieme	47
7 La disciplina del futuro	55
Tre scene di custodia.....	62
Chiusura.....	63
Glossario minimo	65
Appendice operativa.....	69
Fonti e approfondimenti.....	73
Nota di passaggio.....	74

Nota al lettore

Questo quaderno parla di custodia digitale: come mantenere accessibili, protetti e comprensibili nel tempo i beni e gli accessi che contano. Una parte crescente della nostra vita, del nostro lavoro e della nostra memoria passa attraverso sistemi digitali. Se gli accessi vengono persi, compromessi o dimenticati, ciò che credevamo di possedere può diventare irraggiungibile. Le pagine che seguono offrono un linguaggio e un metodo per riconoscere queste dipendenze prima di un incidente.

La custodia digitale non riguarda soltanto le criptovalute. Riguarda un dominio internet, un archivio nel cloud, un account professionale, una libreria di documenti, un wallet, una licenza, una firma elettronica, una prova, una chiave di cifratura, una cartella condivisa, un'identità operativa. Riguarda tutti gli oggetti che non stanno più semplicemente in un luogo, ma dentro relazioni tecniche, contrattuali, procedurali e umane.

Le pagine che seguono hanno un obiettivo culturale e operativo. Vogliono aiutare il lettore a distinguere accesso, possesso, controllo e proprietà. Vogliono mostrare perché una password non è una chiave privata, perché una chiave privata non è un oggetto qualunque, perché un backup non è una decorazione prudente, perché la sicurezza senza trasmissione può diventare un'altra forma di perdita.

Questo testo non è consulenza finanziaria, legale, fiscale o d'investimento. Non suggerisce di acquistare asset digitali, non indica fornitori da usare, non prescrive una configurazione universale e non sostituisce il parere di professionisti qualificati. Dove entrano norme, successioni, fiscalità, obblighi aziendali o patrimoni importanti, serve una verifica specifica. La custodia è concreta proprio perché non vive nel vuoto: vive dentro famiglie, aziende, leggi, dispositivi, abitudini, paure e competenze reali.

La tesi di fondo è semplice e difficile insieme: possedere davvero qualcosa significa anche poterlo perdere. È un invito a riconoscere le conseguenze del controllo, non a preferire il rischio. La possibilità di recuperare un accesso tramite un servizio non cancella i nostri diritti; l'assenza di un intermediario non li crea da sola. Cambiano invece le responsabilità operative: chi conserva le chiavi, chi può intervenire e che cosa resta possibile quando qualcosa va storto.

Prologo

La porta che non si può forzare

Sul tavolo c'è un telefono che nessuno riesce a sbloccare. Accanto, un portatile spento, un hard disk esterno, una busta con alcune parole scritte a mano, tre chiavette USB senza etichetta e un piccolo dispositivo di plastica che qualcuno riconosce vagamente come un hardware wallet. La stanza è ordinata. Non c'è stata violenza, non c'è stato furto, non c'è stata intrusione. Tutto è ancora lì. Eppure qualcosa è scomparso.

La famiglia sa che attraverso quei dispositivi potrebbe essere raggiungibile qualcosa di importante. Non sa quanto. Non sa dove. Non sa se si tratti di fotografie, documenti, contratti, domini, criptovalute, codici, password, account professionali o semplici copie inutili. Il proprietario non c'è più. Chi resta riceve oggetti fisici, ma non il percorso che li rende leggibili.

Nel mondo materiale, una porta chiusa può essere forzata. Si può chiamare un fabbro, un notaio, un tecnico, un'autorità. Si può rompere una serratura, aprire un cassetto, inventariare una stanza, sollevare un tappeto, svuotare una cassaforte. Il mondo fisico resiste, ma in qualche modo concede una seconda possibilità. Lascia tracce grossolane, spessori, chiavi duplicate, fatture, polvere, impronte, oggetti. Anche quando è protetto, tende a rimanere visibile.

Il digitale è diverso. Una porta chiusa bene può non avere più fabbro. Può non esistere una serratura da rompere, perché la serratura è matematica. Può non esistere un ufficio a cui presentarsi, perché il sistema non riconosce volti, lutti, urgenze o buone intenzioni. Può esistere solo una chiave, e quella chiave può essere una sequenza di parole, un file cifrato, un dispositivo, un secondo fattore, una combinazione di passaggi che nessuno ha mai scritto in modo comprensibile.

Questa immagine riguarda soprattutto chiavi crittografiche e dati cifrati privi di una via di recupero. Un account amministrato da un fornitore può prevedere procedure diverse, anche in caso di morte. Non tutte le porte digitali funzionano allo stesso modo.

È questa la scena originaria della custodia digitale: il valore non sparisce, ma smette di rispondere.

Non sempre la perdita digitale arriva come attacco. La immaginiamo spesso così perché l'attacco ha una forma narrativa comoda. C'è un aggressore, una vittima, una violazione, un colpevole. Ma molte perdite sono più silenziose. Un telefono cade in acqua. Un numero viene disattivato. Un account email viene chiuso. Una seed phrase viene copiata male. Un backup non viene mai testato. Una persona muore senza lasciare istruzioni. Un servizio cambia policy. Un documento resta cifrato in un archivio che nessuno sa più aprire.

La perdita digitale è spesso una sottrazione senza scena. Non si sente il rumore del vetro rotto, non si vede una porta scassinata, non compare una stanza vuota. Il saldo può restare registrato, il file può restare salvato, il token può restare su una blockchain, il dominio può restare in un registro, la cartella può restare su un server. Ciò che viene meno è la relazione tra chi dovrebbe agire e il sistema che permette di agire.

La custodia comincia esattamente lì: nel riconoscere che un bene digitale non coincide con la sua apparenza. Vedere qualcosa su uno schermo non significa controllarlo. Avere un'app installata non significa custodire un wallet. Possedere una password non significa avere una procedura. Sapere che un backup esiste non significa sapere che funzioni. Ricordare di aver scritto una frase non significa che qualcun altro saprà trovarla, capirla e usarla nel momento giusto.

La nostra epoca ha reso l'accesso naturale. Ogni giorno entriamo in sistemi che ci riconoscono senza che li comprendiamo davvero. Il telefono si sblocca con il volto, il browser riempie i campi, il cloud sincronizza, il password manager suggerisce, la banca manda una notifica, il wallet mostra un saldo, il sito resta online, il documento appare dove ci aspettavamo di trovarlo. Questa fluidità è una conquista straordinaria. È anche una forma di anestesia.

Finché tutto funziona, non distinguiamo più il bene dall'infrastruttura che lo rende raggiungibile. Non distinguiamo il file dal provider, il saldo dall'account, il token dalla chiave, il dominio dal registrar, il ricordo dall'archivio, la firma dall'identità che la autorizza. Il digitale ci abitua a pensare in termini di presenza immediata: se lo vedo, c'è; se si apre, lo possiedo; se posso usarlo oggi, sarà disponibile anche domani.

Non si tratta di diventare sospettosi verso tutto. Non si tratta di rifiutare i servizi, le piattaforme, il cloud o gli intermediari. La delega è spesso utile, a volte necessaria, in molti casi più sicura dell'autogestione improvvisata. Il problema non è delegare. Il problema è non sapere di aver delegato. Il problema è credere di possedere quando stiamo solo accedendo. Il problema è chiamare sicurezza ciò che è soltanto comodità, e chiamare autonomia ciò che è soltanto isolamento.

Ogni sistema di custodia risponde a una domanda: chi può agire quando serve? Da questa domanda ne nascono altre. Chi sa dove sono le chiavi? Chi può recuperare un accesso? Chi può bloccare un trasferimento? Chi può firmare? Chi può dimostrare un diritto? Chi può aiutare senza poter rubare? Chi può sapere che esiste un valore senza conoscere il modo per spostarlo? Chi può entrare quando il proprietario non può più parlare?

Un bene irraggiungibile per chi è autorizzato può restare intatto e tuttavia essere perso sul piano operativo. Un accesso aperto a chiunque espone il bene; un accesso noto a una sola persona ne concentra la fragilità. Coinvolgere più persone aiuta soltanto se i loro ruoli sono chiari. La custodia vive nel punto difficile tra segreto e trasmissione.

Il piccolo dispositivo sul tavolo, la busta con le parole, il telefono bloccato e il portatile spento sono oggetti poveri se presi da soli. Non contengono magia. Non parlano. Non spiegano a chi resta che cosa siano, perché siano importanti, quali rischi comportino, quali passi vadano eseguiti e quali errori vadano evitati. Senza una procedura, perfino gli strumenti migliori diventano reperti.

Ecco perché custodire non significa semplicemente nascondere. Significa mantenere leggibile. Significa fare in modo che il valore non dipenda solo da una memoria privata, da un'abitudine, da un dispositivo, da un momento di lucidità o da una piattaforma. Significa costruire una relazione tra accesso, controllo, prova e trasmissione.

Il digitale non perdona sempre, ma può essere preparato. La differenza è culturale prima ancora che tecnica. Una persona può comprare lo strumento più sicuro e usarlo nel modo più fragile. Può avere un hardware wallet e fotografare la seed phrase. Può avere un sistema multisignature e non sapere chi conserva che cosa. Può avere un backup in cassaforte e non averlo mai verificato. Può avere tutto sotto controllo e non aver lasciato nessuna istruzione a chi dovrà gestire il dopo.

Questo quaderno comincia da una porta che non si può forzare perché ogni discorso serio sulla custodia deve partire dalla perdita. Non dalla perdita come catastrofe, ma dalla perdita come possibilità strutturale. La proprietà digitale ha bisogno di questa serietà. Non per spaventare, ma per diventare adulta.

Il resto del percorso sarà una mappa. Prima capiremo che cosa significa davvero custodire. Poi entreremo nella chiave, nel segreto, nella falsa comodità, nei rischi, nella distanza, nella custodia condivisa e nella manutenzione del futuro. Ma tutto nasce qui, davanti a una scrivania ordinata, dove nulla è stato rubato e tuttavia qualcosa non è più raggiungibile.

Non tutto ciò che è protetto è custodito. A volte è solo sepolto.

La lettura continua

La Custodia

Floriano Righetti · Quaderno I

Hai letto un estratto dell'edizione definitiva di settembre 2026. Nella scheda del quaderno trovi la presentazione del volume e gli aggiornamenti sulla sua disponibilità.

SCOPRI IL QUADERNO

florianorighetti.ch/it/quaderni/la-custodia

Sette quaderni, un percorso

Custodia, proprietà digitale, eredità, chiavi private, wallet, cold storage e fiducia.

[Esplora la collana completa](#)