Nexa Center for Internet & Society
Politecnico di Torino

Blockchain e Privacy:
un binomio impossibile?

88° Nexa Lunch Seminar – 26 maggio 2021

Dott. Giacomo Conti

Breve introduzione alla Blockchain

- **Una nuova concezione di tenuta orizzontale dei dati, sicura e a potere diffuso.**
  Ogni *record* contiene in sé lo storico di tutti i *records* precedenti, criptato.

- **Due fattori essenziali:**
  1) Estrema difficoltà nell'alterare il dato
  2) «I dati verificano se stessi», in un sistema decentralizzato, superando la dicotomia client-server tradizionale

SICUREZZA E VELOCITÀ PER TUTTI A BASSO COSTO!

1) **Eliminati alla radice i rischi di compromissione del server centrale**
2) **Transazioni rapide e costi di gestione bassissimi**
3) **Storico inappuntabile delle informazioni**

Ma non è tutto oro quel che luccica.

- **Immodificabilità non significa veridicità.**

- **Il progresso tecnologico è stato più repentino del progresso legislativo.**

- **Le norme in materia di privacy (GDPR in primis) sono incompatibili con la tecnologia della blockchain, quand'essa è usata per trattare dati personali.**

INCOMPATIBILITÀ FONDAMENTALI

1) **Impossibilità di individuare un *data controller* univoco**

2) **Impossibilità di ottenere modifica o cancellazione dei dati (16,17)**

1. Trattare dati personali vuol dire eseguire su di essi "qualsiasi tipo di operazioni", tra le quali figura anche la semplice archiviazione.

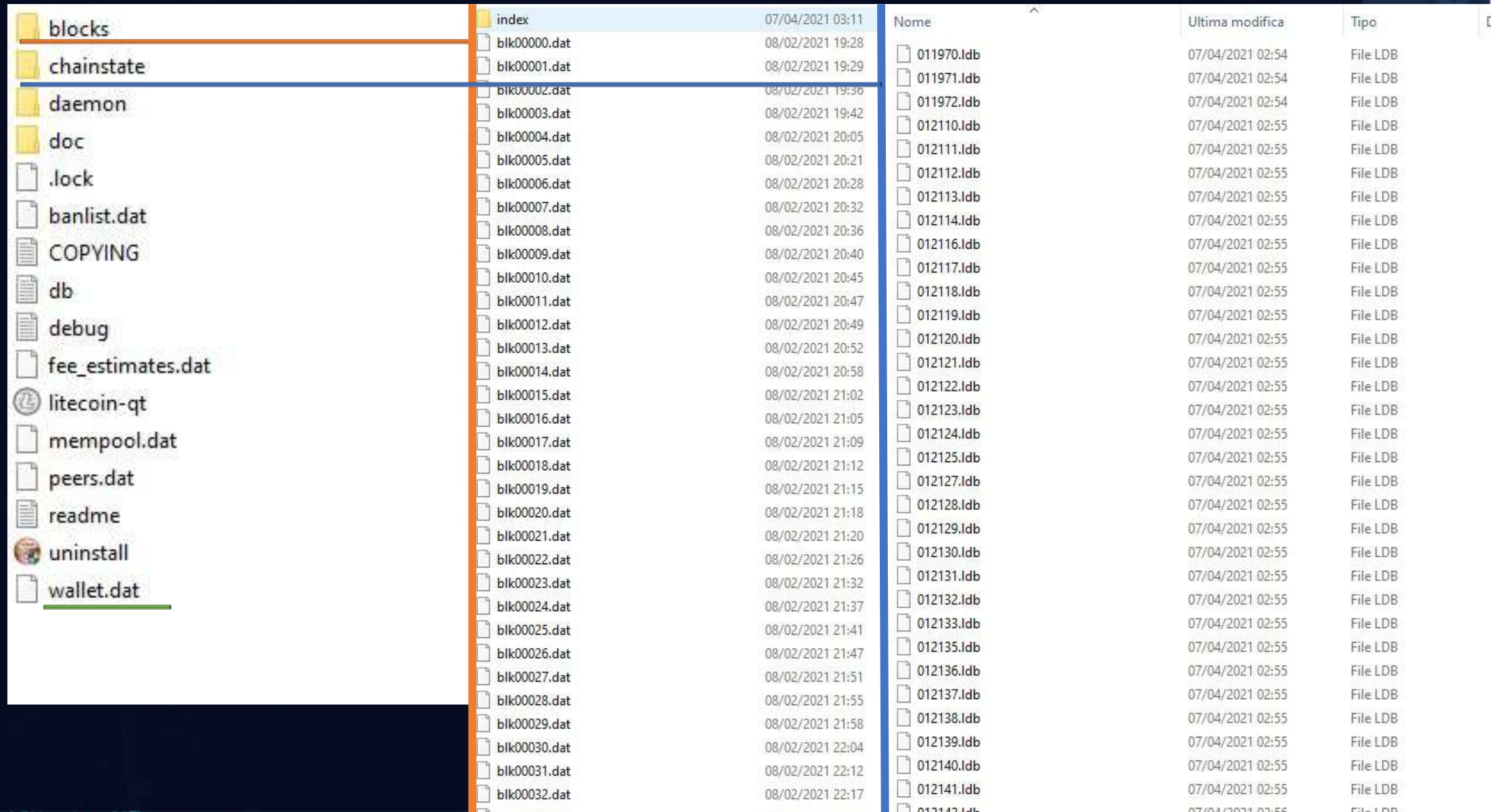
Affidereste mai i vostri risparmi ad uno così?

Struttura di un Wallet di criptomoneta

blocks	22/08/2020 19:15	Cartella di file	
chainstate	22/08/2020 19:15	Cartella di file	
daemon	22/08/2020 19:15	Cartella di file	
doc	22/08/2020 19:15	Cartella di file	
.lock	11/12/2017 21:32	File LOCK	0 KB
banlist.dat	11/12/2017 21:32	File DAT	1 KB
COPYING	25/07/2017 05:11	Documento di testo	2 KB
db	11/12/2017 21:32	Documento di testo	0 KB
debug	16/12/2017 22:25	Documento di testo	10.527 KB
fee_estimates.dat	16/12/2017 22:25	File DAT	11 KB
litecoin-qt	25/07/2017 05:11	Applicazione	31.325 KB
mempool.dat	16/12/2017 22:25	File DAT	82 KB
peers.dat	16/12/2017 22:25	File DAT	2.331 KB
readme	25/07/2017 05:11	Documento di testo	1 KB
uninstall	11/12/2017 21:51	Applicazione	148 KB
wallet.dat	16/12/2017 22:25	File DAT	72 KB

dei dati (16,17)

Struttura di un Wallet di criptomoneta



Le Tavole della Legge (o: cosa richiede il GDPR)

1) NON AVRAI ALTRO RESPONSABILE ALL'INFUORI DI ME

Che sia creata la figura del titolare del trat.; possibile anche la creazione di *joint controllers*

2) NON TRATTARE I DATI INVANO

Che i dati siano trattati per finalità specifiche e determinate, e per un tempo predeterminato.

3) RICORDA DI SANTIFICARE LE CARTE

Che il titolare del trattamento informi correttamente l'interessato tramite un'*informativa*

4) ONORA L'INTERESSATO E L'INTERESSATA

Che si consenta all'interessato un diritto di accesso, modifica e cancellazione dei propri dati

5) DESIDERA LA PRIVACY D'ALTRI

***By design*, i sistemi di trattamento devono essere conformi allo stato dell'arte in tema di privacy e sicurezza (nei limiti del possibile)**

6) DESIDERA LA SECURITY D'ALTRI

***By design*, i sistemi di trattamento devono essere conformi allo stato dell'arte in tema di privacy e**

Le Tavole della Legge (o: cosa richiede il GDPR)

1) NON AVRAI ALTRO RESPONSABILE ALL'INFUORI DI ME

INCOMPATIBILE

Che sia creata la figura del titolare del trat.; possibile anche la creazione di *joint controllers*

2) NON TRATTARE I DATI INVANO

INCOMPATIBILE

Che i dati siano trattati per finalità specifiche e determinate, e per un tempo predeterminato.

3) RICORDA DI SANTIFICARE LE CARTE

COMPATIBILE

Che il titolare del trattamento informi correttamente l'interessato tramite un'*informativa*

4) ONORA L'INTERESSATO E L'INTERESSATA

INCOMPATIBILE

Che si consenta all'interessato un diritto di accesso, modifica e cancellazione dei propri dati

5) DESIDERA LA PRIVACY D'ALTRI

SEMICOMPATIBILI

***By design*, i sistemi di trattamento devono essere conformi allo stato dell'arte in tema di privacy e sicurezza (nei limiti del possibile)**

6) DESIDERA LA SECURITY D'ALTRI

***By design*, i sistemi di trattamento devono essere conformi allo stato dell'arte in tema di privacy e**

E SE I DATI NON FOSSERO PERSONALI?

Obiettivo: rendere il dato personale il più «anonimizzato» possibile

CRIPTAZIONE

Nascondere le informazioni dietro un codice.
La chiave di criptazione diventa «elemento ulteriore»: i dati personali criptati rimangono dati personali.

FUNZIONI DI HASH

Criptazione tramite algoritmo che distorce e confonde un dato di partenza, in modo predeterminato.
L'algoritmo diventa l'«elemento ulteriore».

CONSERVAZIONE DEI DATI EXTRA BLOCKCHAIN

I dati personali criptati sono conservati fuori dalla blockchain, e sono collegati ai dati di transazione dentro la blockchain.
Il GDPR è rispettato: c'è data controller e possibilità di modificare/cancellare i dati.

ALTRE SOLUZIONI

- **Dimostrazioni a conoscenza zero**
- **Indirizzi *stealth***
- **Aggiunta di rumore**

Il Problema del Data Controller

- «Tensione inversa»: non è la blockchain incompatibile con il GDPR, ma il GDPR incompatibile con la blockchain

- Trattare dati personali implica un data controller: chi è il data controller?

Non esiste alcun data controller	Tutti sono data controller
Incompatibilità totale con il GDPR: impossibilità di tenere i dati su blockchain	Suggestione interessante: del resto il GDPR espressamente prende in considerazione l'esistenza di «contitolari del trattamento» o *joint controllers*.

- Malgrado la soluzione dei *joint controllers* possa preservare una natura diffusa e decentralizzata, le soluzioni sono entrambe insoddisfacenti: occorre agire tecnicamente sulla blockchain

Quattro tipi di blockchain

- **Riguardo alle *responsabilità* e all'*accesso*, si possono categorizzare quattro tipi di blockchain:**

- ***Permissionless* Pubbliche**
- ***Permissioned* Pubbliche**
- ***Permissionless* Private**
- ***Permissioned* Private**

Blockchain Pubbliche

Permissionless

- La blockchain «tradizionale»
- Nessuna autorizzazione necessaria per accedere alla rete o eseguire in essa transazioni
- Chi assume il ruolo di data controller?
  1) Sviluppatori del software
  2) I miners stessi
  3) Gli utenti della blockchain
- Forse la 3) è la soluzione migliore: gli utenti sono *data controller* per i loro dati personali e *data processors** («responsabili del trattamento») per i dati altrui.

Permissioned

- Chiunque può accedere in lettura alle informazioni e alle transazioni
- È necessario un permesso per aggiungere nuovi dati
- Data controller può essere solo quel ristretto numero di soggetti che sono in grado di aggiungere dati alla catena.
- Promettente tecnologia per la diffusione di informazioni presso il pubblico.

*Il responsabile del trattamento tratta dati personali per conto del titolare del trattamento.
Il responsabile del trattamento è di solito un terzo rispetto all'impresa o

Blockchain Private

Permissionless

- **Tutte le operazioni sono limitate ad una cerchia ristretta di utenti.**
- **Tali utenti possono sia accedere al database, sia aggiornarlo.**
- **Sono come le blockchain permissionless pubbliche, ma valgono soltanto per una rete isolata (LAN)**
- **Stessi problemi della pubblica per l'individuazione del data controller, ma possono essere arginati tramite l'autoregolazione interna aziendale.**

Permissioned

- **Un'autorità centrale determina chi può accedere alla blockchain.**
- **Tale autorità è determinata precisamente, e assume il ruolo di *data controller*.**
- **Di fatto, non è più una blockchain.**
- **Favorita dal CNIL Francese per la tenuta di database privati, anche attraverso la creazione di *joint controllers*.**

Cosa riserva il futuro? Suggestioni Europee

Il proclama della Commissione Europea:

1) Le nuove tecnologie devono "lavorare per le persone"

2) Esse devono dare spunti per una economia equa e competitiva

3) Da ciò deve derivare una società democratica e sostenibile

E quindi, nel concreto?

1) **Creazione di un framework europeo che consenta l'accesso ai dati ed il loro uso in maniera comune presso tutta l'UE. Creazione di autorità e strutture nazionali compatibili tra loro. *Open Data Directive.***
2) **Potenziamento dei sistemi *cloud* europei per la tenuta dei dati (2021-2027 *High Impact Project)***
3) **Educazione degli individui (*Data Education Action Plan*, ancora in divenire)**
4) **Creazione di uno *spazio-dati comune* per tutta l'UE nei settori di interesse pubblico.**

Situazione a maggio 2021: *Pre-Commercial Procurement:* settori pubblici selezionati ricevono in anteprima nuove tecnologie e know-how per ottenere rapida implementazione e feedback.

Quale futuro per la blockchain?

- **La tenuta di dati personali attraverso tecnologie di blockchain non è semplice.**

- **Può verificarsi soltanto se vengono messi in piedi metodi e soluzioni che arginino le criticità connaturate in esse:**

a. La possibilità per gli interessati di accedere ai propri dati

b. La possibilità per gli interessati di ottenere modifica o cancellazione dei propri dati

c. L'individuazione di un titolare del trattamento

d. La realizzazione di un sistema che renda sicuri i dati degli interessati

e. La cancellazione dei dati degli utenti al termine del periodo di trattamento specificato

Blockchain: un modello «concettuale»

- **Più promettente di tutti sembra essere vedere la blockchain come modello: un concetto a cui ispirarsi nella tenuta di dati.**

- **Essa può essere determinante nell'istituzione di *data marketplaces* nei quali i dati vengono scambiati celermente e a basso costo, nonché in sicurezza.**

- **Decentralizzazione, sicurezza e capacità di gestire agilmente numerose transazioni sono infine i punti di forza fondamentali della tecnologia.**