Scopri come Blockchain e GDPR sono correlati tra loro

di **Amministratore Sito**
28 Maggio 2020 – 3:28



Il GDPR è stato creato per “regolare” la gestione della privacy legata all’utilizzo dei dati degli utenti sul Web, app e social media da parte di società Web e dei media che stanno cercando di costruire il proprio vantaggio competitivo sulla profilazione degli utenti. Il GDPR può essere “interpretato” come una “carta dei diritti digitali” delle persone.

Le possibili relazioni tra GDPR e blockchain

Il regolamento GDPR ha un impatto su una serie di aree relative alle caratteristiche specifiche della Blockchain:

Accesso e visibilità dei dati: i dati inseriti nella blockchain sono pubblici e accessibili a chiunque partecipi alla catena
Eliminazione dei dati: i dati memorizzati in una blockchain sono a prova di manomissione, pertanto la loro eliminazione non sarà possibile dopo l’inserimento di tali dati nella catena distribuita;
Immutabilità dei dati nel tempo: i dati presenti nella blockchain sono mantenuti illimitati e non possono essere modificati, manomessi o eliminati.
Controllo distribuito dei dati: la blockchain è distribuita, pertanto il controllo sui dati non può essere centralizzato ed è responsabilità di tutti i partecipanti alla blockchain (è difficile identificare le cifre del responsabile della protezione dei dati richieste dal GDPR);
Processi decisionali automatizzati – con Smart Contracts, devono essere considerati anche

i processi decisionali automatizzati o un nuovo tipo di gestione dei dati

Blockchain e GDPR per una sicurezza in base alla progettazione

Blockchain e GDPR consentono di creare soluzioni di "sicurezza progettuale" garantendo la pseudonimizzazione (disaccoppiamento dei dati dall'identità individuale) e la minimizzazione dei dati (condivisione dei soli punti di dati assolutamente necessari).

Con questa impostazione è impossibile ricostruire il contenuto di una transazione dall'hash crittografico unidirezionale. E a meno che una delle parti della transazione non decida di collegare una chiave pubblica a un'identità nota, non è possibile mappare e collegare le transazioni a individui o organizzazioni. Ciò significa che anche se la blockchain è "pubblica" (dove chiunque può vedere tutte le transazioni su di essa), nessuna informazione personale viene resa pubblica.

Blockchain, GDPR e questioni legislative

Il GDPR introduce alcune regole che potrebbero non essere sempre rispettate dalla blockchain.

GDPR e il Data Protection Officer (responsabile della protezione dei dati)- Il GDPR introduce la figura del responsabile della protezione dei dati, un esperto di legislazione e pratiche sulla protezione dei dati che deve assistere la persona che li controlla o li gestisce al fine di verificare la conformità interna al regolamento. Il responsabile della protezione dei dati deve essere una persona con una buona padronanza dei processi IT, della sicurezza dei dati e di altre questioni di coerenza aziendale relative alla manutenzione e al trattamento dei dati personali e sensibili.

"Quando è necessario nominare un responsabile del trattamento dei dati personali? Nel GDPR, il responsabile del trattamento deve essere nominato nel caso in cui le principali attività di trattamento richiedano un monitoraggio regolare e sistematico degli interessati su larga scala, se le attività comprendono il trattamento su larga scala di particolari categorie di dati personali o di dati relativi a condanne penali e reati, sempre quando il trattamento è effettuato da un'autorità pubblica o da un ente pubblico. "

Quale giurisdizione applicare per la legge di quale paese – In caso di controversie, quali leggi devono essere applicate e allin1bitcoins?

In una blockchain (specialmente se è pubblica) i dati vengono conservati su ciascun nodo della rete – accessibili al pubblico a chiunque – indipendentemente dallo scopo originale per cui tali dati sono stati immessi ed elaborati nella blockchain. In che modo questa tipica funzionalità blockchain si adatta a un contesto normativo che richiede che gli scopi specifici per i quali i dati personali vengono elaborati debbano essere specificati, espliciti e legittimi e che i dati personali debbano essere adeguati, pertinenti e limitati agli scopi per i quali vengono trattati.

L'identità di un utente (e quindi i suoi dati sensibili) è protetta da un codice che rappresenta la chiave pubblica per accedere alla rete distribuita. Da un punto di vista normativo, è necessario capire cosa siano i "dati personali" in un contesto blockchain: le chiavi pubbliche devono essere considerate dati personali? Sebbene una chiave pubblica appaia come dati pseudonimizzati, questi non rappresentano dati anonimi e sono spesso associati a persone fisiche specifiche.

Pertanto, è anche necessario affrontare la legislazione su come gestire il problema del “diritto all’oblio” all’interno di una blockchain.