Blockchain & Trust

Una Questione di Fiducia

Introduzione

In questa presentazione analizziamo la complessa relazione tra **Blockchain & Trust**, che implica una controversa declinazione del comune concetto di **"Fiducia"**.

Cos'è la Fiducia?

Quando ci riferiamo al termine "fiducia", diamo per scontato il suo significato

il concetto di fiducia in realtà è strettamente legato al contesto in cui viene utilizzato

Cos'è la Fiducia?

Nel contesto della **tecnologia digitale**, l'uso del significato comune di fiducia può essere fuorviante

Posso riporre negli strumenti digitali la stessa fiducia che ripongo in genitori e amici?

Relazioni di Fiducia

I rapporti di fiducia sono:

✓ **Asimmetrici**: la fiducia potrebbe non essere la stessa da entrambi i lati della relazione;
✓ **Contestuali**: la fiducia può essere diversa nei vari domini;
✓ **Relativi al tempo**: la fiducia può degradarsi nel tempo;

Definizione di Trust

In parole povere, possiamo definire il concetto di "Trust" come:

l'aspettativa che una particolare entità (sia essa umana o digitale) si comporti nel modo previsto;

Fidarsi dei Sistemi Informatici

I computer non possono prendere **decisioni complesse** che implichino relazioni di fiducia;

al contrario, c'è il rischio di presumere che i computer siano affidabili quanto le controparti umane

Fidarsi dei Sistemi Informatici

fidarsi di un S.I. vuol dire che possiamo fidarci:

- ✓ delle prestazioni del computer?
- ✓ delle capacità di archiviazione?
- ✓ dell'integrità dei dati?
- ✓ dell'affidabilità delle transazioni?

La Fiducia può degradarsi nel tempo

La fiducia che possiamo riporre in un S.I. può degradarsi nel tempo, a causa dei cambiamenti nei contesti operativi (es. dalle piattaforme mobili all'IoT), a seconda dello "stato dell'arte" delle contromisure di sicurezza disponibili al momento, le minacce emergenti coinvolte, ecc.

La Fiducia come sinonimo di Agenzia

Fidarsi di un S.I. implica un problema di **agenzia**

Agenzia riguarda l'agire per conto di qualcun altro: ciò implica la necessità di identificare il soggetto (agente) di cui possiamo fidarci;

Fiducia come questione di Sicurezza

Le relazioni di fiducia sono quasi sempre coinvolte quando entra in gioco la Sicurezza:
trattando di cybersecurity dal punto di vista della Trust, occorre mettere in discussione i presupposti di fiducia sottostanti, impliciti o espliciti, nella progettazione dei sistemi;

Fiducia come questione di Sicurezza

facendo emergere in forma esplicita le relazioni di fiducia esistenti nei sistemi, possiamo renderli più resilienti, più utilizzabili e più sicuri.

Come entra in gioco la Sicurezza

Per capire come viene applicata la sicurezza e come è correlata al problema della fiducia, si consideri ad esempio un sistema di sicurezza come un sistema di rilevamento delle minacce (threats detection):

Il Dominio specifico e la Sicurezza

riponiamo la nostra fiducia che il sistema rilevi efficacemente le minacce sulla base della sua implementazione, progettata per lo specifico dominio di sicurezza;

Relazioni di Fiducia implicite

di conseguenza, molte relazioni di fiducia (sia implicite che esplicite) sono coinvolte e incorporate nell'implementazione di un tale sistema di detection;

Esplicitare le relazioni di Trust

le specifiche tecniche generali per affrontare lo scenario di rilevamento delle minacce sono state dichiarate e implementate in anticipo, per riporre la nostra fiducia sulla loro efficacia

Cambiamenti di contesto e Sicurezza

Cosa accade però se il contesto di riferimento cambia?

Potremmo ancora riporre la nostra fiducia nel sistema di rilevamento quando viene distribuito in uno scenario piuttosto diverso?

Cambiamenti di contesto e Sicurezza

Quanto è probabile che quelli che in precedenza consideravamo segnali affidabili si trasformino ora in falsi positivi?

Basterebbe solo mettere a punto il sistema, o dovremmo considerare la sua completa reingegnerizzazione?

Cambiamenti di contesto e Sicurezza

quando si tratta di porre in essere **reazioni flessibili** per adattarsi ai cambiamenti di contesto, niente può battere la creatività umana (almeno fino ad ora...)

Algoritmi e Dominio applicativo

Macchine e algoritmi operano in contesti di dominio specifici per i quali sono stati progettati e programmati;

Pregiudizi codificati dalle macchine

questo va sotto il nome di **bias codificato programmaticamente**, per il fatto che in fase di progettazione sono stati considerati solo contesti specifici, il che comporta una scarsa flessibilità intrinseca del sistema;

Software e problemi di Agenzia

Secondo la definizione di Agenzia, i computer agiscono per conto di qualcun altro; questo vale anche nel caso di conseguenze non desiderate, dovute ad esempio a software dannosi o difettosi;

Rapporti di Fiducia inadeguati

in quanto tale, il rischio di porre i sistemi informatici in **rapporti di fiducia inadeguati** può diventare reale, soprattutto se impiegati al di fuori dei domini per i quali sono stati originariamente progettati;

Le "proxy" della Sicurezza

un altro grave rischio è quello di **confondere la mappa per il territorio**: cioè adottare concetti legati alla sicurezza come **possibili alternative** alla Fiducia;

Misure "proxy" della Sicurezza

tali concetti "proxy" sono:

- ✓ Autorizzazione;
- ✓ Riservatezza
- ✓ Integrità;
- ✓ Disponibilità;

I rischi dell'antropomorfismo

in quanto esseri umani, cadiamo facilmente nell'errore dell'Antropomorfismo, cioè attribuire caratteristiche umane a manufatti non umani;

I rischi dell'antropomorfismo

con l'ampia adozione di strumenti potenziati dall'IA, aumenta il rischio di attribuire capacità cognitive ai tool digitali; così come il rischio di fidarsi di essi come partner affidabili che imitano relazioni umane;

Confondere Agenzia con Intenzionalità

L'intenzionalità specifica **da cosa o da chi** dovrebbero essere progettate le azioni di sistema;

in quanto tale, l'intenzionalità consente di implementare correttamente le **funzioni di agenzia** in un sistema:

Confondere Agenzia con Intenzionalità

specificando l'intenzionalità, è possibile introdurre una descrizione ben definita delle **relazioni di fiducia** coinvolte in un sistema;

Confondere Agenzia con Intenzionalità

Nella definizione delle relazioni di fiducia con i sistemi informatici, le **questioni di agenzia** diventano preminenti per gli esseri umani:

Confondere Agenzia con Intenzionalità

gli umani possono fidarsi di entità non umane semplicemente perché le vedono agire come esseri umani, non avendo la capacità di distinguere le azioni reali dalle simulazioni della macchina;

Confondere Agenzia con Intenzionalità

Di conseguenza, il pericolo di introdurre **assunzioni implicite** che portano a relazioni di fiducia implicite, incorporate nel sistema, diventa reale;

Confondere Agenzia con Intenzionalità

l'introduzione di fiducia implicita in un sistema può essere dannosa, poiché non può essere facilmente valutata nei suoi effetti;

Confondere Identità con Fiducia

Nonostante **l'identità** debba essere valutata in modo attendibile quando si instaura un rapporto fiduciario, essa non è l'unico fattore chiave:
vi sono infatti casi in cui **l'anonimato** è ritenuto invece quanto mai necessario per instaurare la rapporto di fiducia:

Confondere Identità con Fiducia

in quanto tale, occorre tenere adeguatamente conto di come un sistema digitale sia dotato di funzioni di agenzia, per fornire il presupposto corretto per raggiungere gli obiettivi prefissi;

Lo Zen della Zero Trust

Così come gli esseri umani, anche i sistemi informatici non sempre fanno ciò che promettono, né sono sempre coerenti (a causa di codici malware o bug), quindi non dovremmo sempre riporre la nostra fiducia su di loro;

Lo Zen della Zero Trust

pertanto dovremmo seguire il motto:

Fidati ma verifica: se avere fiducia è spesso utile, verificarne i presupposti è la chiave per farla rispettare

La Fiducia non è una proprietà di un Sistema

In quanto tale, la Fiducia non può essere considerata una proprietà interna del sistema;

La Fiducia non è una proprietà di un Sistema

la Fiducia deve essere valutata sull'esperienza e condivisa tra le persone, dopo essere stata testata in base a requisiti particolari su come ci si aspetta che il sistema si comporti;

La Fede nella Matematica

siamo indotti a confidare nella matematica perché essa sembra offrirci certezze:
ci aspettiamo che essa dia una risposta deterministica alle nostre domande, soprattutto quando si tratta di sicurezza;

La Fede nella Matematica

La crittografia, in particolare, ci assicura sull'integrità dei dati sensibili e sull'identità del suo proprietario;

essa può farlo a condizione che siano rispettati alcuni presupposti rigorosi, come ad esempio:

La Fede nella Matematica

Requisisti indispensabili:

✓ le chiavi di sicurezza siano adeguatamente protette;
✓ i principi matematici sottostanti valgono ancora nel tempo;
✓ l'implementazione del sw è coerente;

La Fede nella Matematica

La complessità della crittografia amplifica l'effetto di eventuali bachi nel codice, nel senso che errori minori nell'implementazione possono portare a guasti catastrofici

I Limiti della verifica formale

per affrontare tali vulnerabilità nell'implementazione, è stata introdotta una verifica formale che imita la prova matematica sul codice:

I Limiti della verifica formale

sfortunatamente, l'applicazione pratica dei metodi di verifica formale al software è limitata e non può fornire le garanzie che ci aspettiamo;

I Limiti della verifica formale

tra le carenze delle tecniche standard nella verifica formale vi sono:

✓ la capacità limitata di fornire asserzioni a livello di sistema;
✓ la ridotta scalabilità di modelli grandi e complessi;

I Limiti della verifica formale

secondo Ken Thompson:

> "Non puoi fidarti del codice che non hai creato completamente tu stesso. Nessuna quantità di verifica o controllo a livello di fonte ti proteggerà dall'utilizzo di codice non attendibile".

Necessità dell'ispezione del codice sorgente

di conseguenza, bisognerebbe ispezionare il codice sorgente di tutti i livelli software e hardware, per potersi fidare di sistemi digitali di terze parti, nonostante l'effettuazione di verifiche formali;

Contratti legali come alternativa alla Fiducia

tra le alternative alla istituzione di rapporti di fiducia per fronteggiare i rischi, si possono citare i **contratti legali**;

Contratti legali come alternativa alla Fiducia

I contratti legali sono un meccanismo per mitigare il rischio quando i rapporti di fiducia sono insufficienti, a causa di **informazioni imperfette o incomplete**;

Contratti legali come alternativa alla Fiducia

il principale svantaggio dei contratti legali è che dobbiamo introdurre **terze parti in funzione di autorità** per far rispettare i contratti e punire le parti inaffidabili coinvolte nel contratto;

La Sfiducia è facilmente verificabile, la Fiducia no

il problema con la fiducia risiede nella sua asimmetria intrinseca:
mentre un comportamento inaffidabile può essere facilmente rilevato e provato, non è altrettanto vero il contrario;

La Sfiducia è facilmente verificabile, la Fiducia no

in realtà, il punto centrale della costruzione di una relazione di fiducia è garantire che le azioni vengano eseguite come previsto; a volte ciò che conta di più è la prestazione prevista delle azioni, piuttosto che le azioni stesse

Blockchain alla riscossa?

Secondo gli esperti di tecnologia, Blockchain rappresenta la **soluzione definitiva** a tutte le questioni relative alla fiducia e alla sicurezza;

Blockchain alla riscossa?

le blockchain forniscono un'alternativa ingegnosa alle autorità centrali nel far rispettare la fiducia, sostituendole con una rete distribuita di operatori peer che risolvono difficili enigmi matematici;

Davvero la Blockchain può fare a meno della Fiducia?

secondo il famoso paper di Nakamoto su Bitcoin:

> "Blockchain offre un sistema per le transazioni elettroniche senza fare affidamento sulla fiducia".

ma è davvero così?

La Fiducia non può essere facilmente evitata

la verità è che abbiamo ancora bisogno di costruire relazioni di fiducia, specialmente nelle applicazioni basate su blockchain:

Più relazioni di Fiducia, non meno

utilizzando criptovalute come bitcoin, abbiamo in realtà bisogno di stabilire molte più relazioni di fiducia

Più relazioni di Fiducia, non meno

Blockchain coinvolge molte relazioni di fiducia implicite/esplicite con:

- ✓ i concetti matematici e computazionali;
- ✓ firme digitali a fondamento della non ripudiabilità;
- ✓ affidabilità dei wallet manager;

e così via...

La Fiducia è spostata, non eliminata

invece di essere eliminate le relazioni di fiducia vengono spostate nell'implementazione del software alla base della tecnologia Blockchain;

La Fiducia sta nell'implementazione

l'implementazione del software in particolare, gioca un ruolo chiave quando si tratta di crittografia: come abbiamo affermato in precedenza, anche un piccolo difetto nell'implementazione degli algoritmi può portare a conseguenze catastrofiche;

La Fiducia sta nell'implementazione

per non parlare delle minacce emergenti poste dall'avvento del Quantum Computing sugli attuali fondamenti della matematica della crittografia...

La Fiducia e i "Protocolli di Consenso"

lo stesso si può dire sui **protocolli di consenso** utilizzati per approvare le transazioni blockchain:

La Fiducia e i "Protocolli di Consenso"

per raggiungere l'accordo della rete sui protocolli di consenso, gli utenti dovrebbero essere in grado di guardare gli elementi del sistema e verificarne la corretta attuazione;

Smart Contracts e Trust

la situazione diventa più dannosa a causa dell'introduzione degli **smart contract**, dove la parola "smart" è altamente fuorviante:

Smart Contracts e Trust

gli smart contract infatti non sono né "smart", in quanto non comportano algoritmi AI/ML, né "contratti" in senso giuridico

Smart Contracts e Trust

in realtà, gli smart contracts sono transazioni che vengono attivate automaticamente al verificarsi di condizioni specifiche:

Smart Contracts e Trust

in quanto tale, dobbiamo fidarci degli implementatori sw nella corretta e appropriata **traduzione digitale di tali condizioni**, insieme all'implementazione sicura delle funzionalità dello smart contract;

Smart Contracts e Trust

la verità è che

non ogni condizione, né ogni reale transazione, può essere attendibilmente tradotta in termini digitali, per la natura deterministica dei presupposti tecnici sottostanti;

Smart Contracts e Trust

quando si tratta di decidere se sottoscrivere o meno uno smart contract, dovremmo chiederci:

> cosa dobbiamo sapere per prendere una decisione del genere?

Smart Contracts e Trust

la risposta è che dobbiamo fidarci non solo dello smart contract per agire come previsto, ma anche delle altre entità coinvolte;

Smart Contracts e Trust

tra questi entità vi sono:

- ✓ l'architettura della blockchain;
- ✓ il codice dello smart contract;
- ✓ l'interprete dello smart contract;
- ✓ il soggetto che fornisce l'informazione relativa alla condizione scatenante (detta anche “oracolo”);

Oracoli come "Single Point of Failure"

in particolare, gli oracoli rischiano di diventare l'anello critico in tali transazioni automatizzate, minando così il rapporto di fiducia esistente con il contratto;

Blockchain come architettura di fiducia distribuita

in un certo senso:

Blockchain non è un sistema "trust-less", quanto piuttosto un'architettura in cui la fiducia viene trasferita in diverse entità, ognuna delle quali implica il proprio livello di fiducia;

Rischio più grande, Fiducia più ampia

di conseguenza, questo **trasferimento di fiducia** può rendere difficile la **valutazione affidabile** dei **rischi** associati, poiché riduce la capacità di utenti, sviluppatori e designer di comprendere e dichiarare correttamente tutta la fiducia relazioni coinvolte, che si diffondono nel sistema...

Per saperne di più

Visita il nostro Sito