

**BLOCKCHAIN E SMART CONTRACT: IL RUOLO DELLA
CERTIFICAZIONE. L'IMPRESA DIGITALE. UN VALORE
AGGIUNTO.
OPPORTUNITA' E LIMITI ATTUALI**

www.avvocatobruccoleri.it

[Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/](https://www.linkedin.com/in/maria-bruccoleri-648440135/)

COSA E' LA BLOCKCHAIN

- E' il database nel quale confluiscono tutte le transazioni eseguite.
- Non è gestito a livello centralizzato, ma collettivamente dai vari aderenti al network, secondo la strutturazione c.d. **peer to peer**.

IMP: Nozione di “**NODO**”: ogni dispositivo hardware in grado di comunicare con altri dispositivi, che fanno parte della stessa sottorete o della Rete (es. computer, palmari, dispositivi mobili, web TV).



I “nodi” vengono definiti, anche, “*host*” (dall'inglese *to host*, ospitare), poiché dotati di applicazioni che possono essere sia client, sia server.

1. Un'applicazione assume il ruolo di **client** quando è utilizzatrice di servizi messi a disposizione da altre applicazioni.
2. Un'applicazione assume il ruolo di **server**, invece, quando è fornitrice di servizi usati da altre applicazioni.
3. Un'applicazione assume il ruolo di **actor** quando può fungere sia da client sia da server, a seconda dell'operazione richiestagli

BLOCKCHAIN

Nell'architettura peer to peer, gli elaboratori connessi tra loro sono in posizione paritetica e svolgono, a seconda dell'operazione richiesta, il ruolo di client o server.

SISTEMA DISTRIBUITO



1. Le applicazioni, fra loro cooperanti, risiedono su più nodi elaborativi (elaborazione distribuita)
2. Il patrimonio informativo, unitario, è ospitato su più nodi elaborativi (base di dati distribuita)

⇒ È un sistema costituito da più applicazioni che collaborano per il perseguimento di obiettivi comuni, attraverso una infrastruttura di comunicazione hardware e software.

⇒ Garantisce una maggiore flessibilità nell'organizzazione delle attività

www.avvocatobruccoleri.it

[Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/](https://www.linkedin.com/in/maria-bruccoleri-648440135/)

BLOCKCHAIN:

Database decentralizzato che archivia asset e transazioni su una rete di tipo peer to peer protetta, mediante l'uso della crittografia.

I partecipanti alla rete, collettivamente, verificano, approvano e registrano le varie transazioni.

L'informazione, presente in tutti i nodi, diventa immutabile.



La blockchain è un nuovo paradigma per la gestione delle informazioni, il quale permette di garantire la reale immutabilità dei dati e certificarne la storia completa.

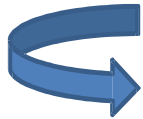
www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

BLOCKCHAIN E BIT COIN

Cenni storici

1991: con l'articolo "*How to time – stamp a digital document*" di Stuart Haber e W. Scott Stornetta, nasceva la Blockchain.



Veniva fornita una soluzione alla certificazione temporale e di autenticità delle operazioni informatiche.

2008: veniva illustrato il progetto di creare una moneta virtuale, basata su di un protocollo Blockchain di tipo "Distributed Ledger (privo di autorità centrale).

Nozione e definizione di Blockchain

- Protocollo strutturato in blocchi, tra loro collegati in rete, in grado di certificare l'ordine cronologico di diverse operazioni, sfruttando una singola catena di algoritmi dove ogni transazione od operazione si lega alle precedenti operazioni.
- I dati della transazione vengono inseriti in blocchi, collegati l'uno all'altro, in modo da creare una catena.
- Ogni blocco include un c.d. hash: funzione algoritmica informatica non invertibile, che identifica il blocco, in modo univoco, e che permette il collegamento con il blocco precedente, tramite la sua identificazione.
- Rete di registri contabili, contenuti in server separati tra loro, ma collegati dal web, all'interno della quale si utilizzano algoritmi, che trattano i dati con tecnologie crittografiche, che scongiurano errori, alterazioni ed accessi agli stessi, da parte di persone non autorizzate, e garantiscono gli utenti dalla commissione di errori o da alterazioni esterne, in assenza di un organo centrale.



Segue

- La blockchain fornisce garanzia di decentralizzazione, trasparenza, sicurezza e immutabilità dei dati raccolti.



- Database aperto e trasparente per tutti i partecipanti, decentralizzato, distribuito e criptato in grado di garantire l'assoluta immutabilità di tutte le informazioni raccolte.
- È un sistema che segna la fine del monopolio della documentazione da parte di un unico soggetto.



Tutti gli utenti verificano la fattibilità di ogni transazione, autorizzandola mediante un sofisticato meccanismo di decriptazione dei codici

“Database distribuito, che utilizza la tecnologia peer to peer, dove ogni utente è in grado di prelevare dal web, diventando un nodo della rete.



La blockchain, potendo tutelare gli utenti da errori o alterazioni dei dati ed assicurare la genuinità delle informazioni immagazzinate nel sistema, potrebbe essere la chiave di volta per il passaggio epocale a quella che viene chiamata “*sharing economy*”

CARATTERISRICHE DELLA BLOCKCHAIN

- **Sicurezza:** database condiviso, decentralizzato, distribuito e criptato con precise regole di sicurezza.
- **Consenso:** archivio aperto a chiunque voglia partecipare e modificabile solo con il consenso di tutti i partecipanti
- **Immutabilità:** le informazioni contenute nella Blockchain sono imm modificabili ed incorruttibili
- **Trasparenza:** gli utenti possono, in qualsiasi momento, vedere tutto.
- **Assenza di intermediari:** la transazione avviene da individuo ad individuo.

Non vi è interferenza di intermediari, autorità centrali, burocrazia o amministrazioni a ciò preposte.

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

OBIETTIVO DELLA BLOCKCHAIN



- Garantire un sistema che non commetta errori
- Garantire un sistema che non consenta la perdita o alterazione di dati e informazioni
- Blocchi l'accesso alle informazioni di chi non è autorizzato

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

COMPONENTI DELLA BLOCKCHAIN

1. Utenti: o, più precisamente, i loro server, detti “nodi”.
2. Transazioni: dati che rappresentano i valori o servizi scambiati, che necessitano di essere verificate, approvate e catalogate.
3. Blocchi: contengono e confermano le transazioni in attesa.
Ogni nuovo blocco viene aggiunto, in media, ogni 10 minuti (c.d. mining).
4. Conferma: indica che una transazione è stata processata dalla rete ed inclusa in un blocco.
5. Ledger: si tratta di una sorta di “libro mastro” nel quale sono trascritti tutti i blocchi in maniera immutabile e sequenziale.
6. Hash: funzione matematica contenente un codice lungo 64 caratteri formato da lettere e numeri, che identifica il blocco e ne protegge il contenuto

LIMITI DELLA BLOCKCHAIN

- **Limitata velocità:** per potere aggiungere un nuovo blocco occorre decriptare un “rompicapo” che, per motivi di sicurezza, è molto complicato e oneroso da risolvere.
- **Costi elevati:** la soluzione dei rompicapi richiede dei costi non indifferenti: servono computer molto potenti e tanta elettricità.
- **Assenza di privacy:** le informazioni relative alle transazioni sono visibili a tutti gli utenti della rete.
- **Rischio di centralizzazione:** i nodi più piccoli potrebbero rinunciare i rompicapi nell'ipotesi in cui un'entità economicamente potente accedesse alla rete e risolvesse, per prima, gran parte degli algoritmi crittografici.

IL DNA DELLA BLOCKCHAIN

Processo di identificazione



Necessario per uscire dalla spirale della
incertezza



La Blockchain ci “regala” la piattaforma per trasporre, nel mondo digitale, il concetto di DNA e univocità certa di identificazione

www.avvocatobruccoleri.it

LinkedIn: www.linkedin.com/in/maria-bruccoleri-648440135/

IL DNA DELLA BLOCKCHAIN

- ✓ **Codice univoco:** la piattaforma utilizza Token per l'identificazione univoca e permette di interagire direttamente, l'uno con l'altro, grazie ad algoritmi quali, ad esempio, gli Smart Contract.
- ✓ **Piattaforma decentralizzata:** per la distribuzione dei dati e per la esecuzione delle DAPP (software applicativo che opera in ambiente Peer to peer).

www.avvocatobruccoleri.it

[Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/](https://www.linkedin.com/in/maria-bruccoleri-648440135/)

IL DNA DELLA BLOCKCHAIN

- La Blockchain intesa come pubblica e permission-less crea trasparenza ed un sistema trust-less, dove non dobbiamo fidarci di qualcuno, bensì ci fidiamo del software che è open-source.
- Grazie alla piattaforma si crea consenso, senza necessità di intermediazione o di un organo istituzionale.
- La tecnologia Blockchain modifica il modo di applicare il diritto e tutto il sistema giuridico



Riduzione delle controversie poiché i requisiti necessari ad accordi, tra le parti, sono resi certi dalla stessa piattaforma, e gli Smart Contract prevedono sistemi di salvaguardia delle parti.

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

IL DNA DELLA BLOCKCHAIN

- La legge deve deregolamentare ed agevolare l'introduzione dei software, senza creare ostacoli.
- E' l'uomo stesso capace di immaginare un mondo diverso.
- L'armonia nella Blockchain è la naturale evoluzione dell'umanità.



È stata definita:

“L’armonizzazione di entità “danzanti” che convivono in perfetta sintesi”

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

WEB & TECH: BLOCKCHAIN E SMART CONTRACT

Le novità previste dal Decreto
semplificazioni

Art. 8 Ter

(D.L. 14 Dicembre, n. 135, convertito in legge con L. 11 febbraio 2019, n. 12)

Comma 1

“Si definiscono «tecnologie basate su registri distribuiti» le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturealmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili”.

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

WEB & TECH: BLOCKCHAIN E SMART CONTRACT

Le novità previste dal Decreto semplificazioni

Art. 8 Ter

(D.L. 14 Dicembre, n. 135, convertito in legge con L. 11 febbraio 2019, n. 12)

Comma 2

“Si definisce «smart contract» un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall’Agenzia per l’Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto”.

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

WEB & TECH: BLOCKCHAIN E SMART CONTRACT

Le novità previste dal Decreto semplificazioni

Art. 8 Ter

(D.L. 14 Dicembre, n. 135, convertito in legge con L. 11 febbraio 2019, n. 12)

Comma 3

“La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014”.

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

WEB & TECH: BLOCKCHAIN E SMART CONTRACT

Le novità previste dal Decreto semplificazioni

Art. 8 Ter

(D.L. 14 Dicembre, n. 135, convertito in legge con L. 11 febbraio 2019, n. 12)

Comma 4

“Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l’Agenzia per l’Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3”.

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

WEB & TECH: BLOCKCHAIN E SMART CONTRACT

Le novità previste dal Decreto semplificazioni

Art. 8 Ter

- L'Italia ha fornito una definizione di “tecnologie basate su registri distribuiti” e di “smart contract”, disegnando la disciplina generale degli effetti giuridici connessi all'utilizzo di tali tecnologie.
- La normativa ha il pregio di porsi all'avanguardia nella regolamentazione della tecnologia blockchain oltre gli aspetti prettamente finanziari connessi ai fenomeni delle criptovalute e della tokenizzazione.
- La formulazione normativa lascia spazio ad alcuni dubbi interpretativi, in parte risolvibili, in sede di predisposizione delle linee guida, che l'AgiD dovrà adottare nel tempo, in conformità a quanto indicato nel medesimo Decreto Semplificazioni e ai suoi necessari aggiornamenti.

WEB & TECH: BLOCKCHAIN E SMART CONTRACT

Tecnologie basate su registri distribuiti



Sono “*le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetaturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati, sia in chiaro che ulteriormente protetti da crittografia, verificabili da ciascun partecipante, non alterabili e non modificabili”.*

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

WEB & TECH: BLOCKCHAIN E SMART CONTRACT

Dubbi interpretativi

1. Anche le Blockchain più conosciute possono essere alterate, con il consenso della maggioranza dei nodi ed esposte ai c.d. attacchi del 51%.
2. **L'art. 8 non valorizza gli elementi del protocollo del consenso e dell'incentivo economico.**

WEB & TECH: BLOCKCHAIN E SMART CONTRACT

Smart Contract

“Programma per elaboratore che opera su tecnologie
basate su registri distribuiti
la cui esecuzione vincola automaticamente
due o più parti sulla base di effetti predefiniti dalle stesse”.

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

WEB & TECH: BLOCKCHAIN E SMART CONTRACT

SMART CONTRACT ELEMENTI DI DEFINIZIONI

- Riconosciuto il requisito della forma scritta, attraverso un processo avente i requisiti fissati dall'AGID, con le sue linee guida.
- Documento informatico che contiene la rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti che soddisfa il requisito della forma scritta.
- Ha l'efficacia prevista dall'art. 2702 cc quando è formato attraverso un processo avente i requisiti fissati dall'AGID, con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento, nonché, la sua riconducibilità all'autore.

WEB & TECH: BLOCKCHAIN E SMART CONTRACT

SMART CONTRACT QUALCHE LIMITE ANCORA:

- Il Decreto Semplificazioni non indica le modalità con le quali lo Smart Contract possa ottenere, oltre alla forma scritta, lo status di scrittura privata ex art. 2702 cc.
- Lo Smart Contract potrebbe avere la forma scritta senza, tuttavia, rientrare nel novero delle scritture private, con la conseguenza che il relativo valore probatorio sarebbe “liberamente valutabile in giudizio”, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità.
- In caso di valutazione negativa, da parte del giudice, si giungerebbe al risultato paradossale di confinare lo Smart Contract nell'alveo dei documenti non sottoscritti, che non hanno “valore giuridico formale e non producono effetti sostanziali e probatori (Cfr. Corte di Cassazione, sentenza n. 30948/2018).

SMART CONTRACTS CHE COSA SONO E COME FUNZIONANO

Tuttavia, uno smart contract è un protocollo informatico usato per facilitare, applicare o verificare digitalmente lo scambio o esecuzione di un contratto. Gli smart contracts permettono di fare transazioni senza l'utilizzo di intermediari o terze parti.

Lo smart contract usa la tecnologia Blockchain.



Uno degli aspetti più importanti della **blockchain** è che, in quanto esiste un network decentralizzato tra le parti autorizzate, non è necessario pagare intermediari. Ciò consente di risparmiare tempo, evitando eventuali conflitti. La tecnologia **blockchain**, nonostante abbia alcuni svantaggi, è considerata **estremamente più veloce**, **più economica** e **sicura** rispetto ai sistemi **tradizionali**. Questo è uno dei motivi che sta spingendo sempre più banche e governi ad iniziare gradualmente ad abbracciare questa tecnologia.

STORIA DEGLI SMART CONTRACTS

Nel 1994, Nick Szabo, crittografo e legale, scoprì che il registro (ledger) decentralizzato poteva essere impiegato per gli smart contracts. Questo tipo di contratti erano al tempo chiamati *contratti auto-eseguibili* oppure *contratti digitali*.



In questo modo, i contratti sarebbero potuti essere tradotti in codice di programmazione, archiviati, replicati sul sistema e supervisionati dalla rete di computer che esegue la blockchain.

Questo avrebbe consentito un “feedback” dal ledger: come per esempio il trasferimento di denaro e la **conseguente ricezione del prodotto o del servizio.**

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

STORIA DEGLI SMART CONTRACTS

NEL 2018 UN RAPPORTO DEL SENATO DEGLI STATI UNITI AFFERMÒ:



“Mentre i contratti intelligenti potrebbero sembrare nuovi, il concetto è radicato nel diritto contrattuale di base. Di solito, il sistema giudiziario giudica le controversie contrattuali e applica termini, ma è anche comune avere un altro metodo di arbitrato, in particolare per le transazioni internazionali. Con contratti intelligenti, un programma applica il contratto integrato nel codice.”

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

SMART CONTRACT: CHE COSA SONO?

*Gli smart contract, o in italiano **contratti intelligenti** o **contratti smart**, hanno la funzione principale di scambiare denaro, azioni o beni di qualsiasi altro tipo in **modalità trasparente senza l'utilizzo di un intermediario.***

*Attualmente, il modo migliore per spiegare come funzionano i contratti intelligenti è quello di fare l'esempio di un **distributore automatico di documenti.** Per ottenere dei documenti è necessario recarsi dal commercialista, pagare ed attendere la consegna del documento. Attraverso i contratti intelligenti invece, è sufficiente effettuare un pagamento in criptovaluta al distributore ed il documento verrà **istantaneamente trasferito nel proprio conto.***

*I **vantaggi dei contratti intelligenti non finiscono qua.** Questi contratti non solo sono in grado di definire le regole e possibili sanzioni di un accordo (proprio come avviene in un contratto classico) ma **applicano automaticamente tali regole.***

VITALIK BUTERIN E GLI SMART CONTRACTS

Vitalik Buterin, inventore di Ethereum, è colui che ha coniato e reso popolare il termine Smart Contracts (o Contratti Smart).

Una parola che è ormai diventata un sinonimo di criptovalute come l'Ethereum.



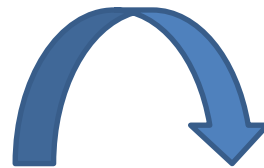
“Un contratto intelligente è un programma per computer che controlla direttamente una risorsa digitale ... L’approccio del contratto intelligente prevede che un contratto legale, trasferisca immediatamente la risorsa digitale in un programma, il programma eseguirà poi automaticamente il codice, convaliderà una condizione e determinerà se il bene dovrà andare a una persona o tornare all’altra persona, o se debba essere immediatamente rimborsato alla persona che lo ha inviato, o una sua combinazione. ” (Vitalik Buterin)

www.avvocatobruccoleri.it

[Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/](https://www.linkedin.com/in/maria-bruccoleri-648440135/)

VITALIK BUTERIN E GLI SMART CONTRACTS

A proposito del progetto **Ethereum**, Buterin ha dichiarato:



“Sono veramente grato di avere l’opportunità di lavorare in una simile area industriale interessante e interdisciplinare, dove ho la possibilità di interagire con crittografi, matematici ed economisti importanti nei loro campi, per aiutare a costruire software e strumenti che già interessano a decine di migliaia di persone in tutto il mondo e lavorare su problemi avanzati in informatica, economia e filosofia ogni settimana”

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

ETHEREUM: LA CRIPTOVALUTA CON GLI SMART CONTRACTS

La criptovaluta più celebre ad incorporare una versione completa dei contratti smart è l'Ethereum.

Vitalik Buterin propose questa criptovaluta nel 2013 come “una blockchain progettata specificatamente per i contratti smart”. Ethereum è un network di computer che fa rispettare, esegue e valida gli smart contracts.



La validazione delle transazioni viene ottenuta attraverso un network decentralizzato di migliaia e migliaia di nodi Ethereum sparsi in tutto il mondo. La struttura del network consente alle applicazioni decentralizzate (DApps) di essere eseguite senza blocchi o disservizi, censure, o interferenze di terze parti. Questo consente alle applicazioni che funzionano attraverso questa tecnologia di risultare immutabili e a prova di hacking.

www.avvocatobruccoleri.it

[Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/](https://www.linkedin.com/in/maria-bruccoleri-648440135/)

ETHEREUM: LA CRIPTOVALUTA CON GLI SMART CONTRACTS

➤ Ethereum può essere, per esempio, utilizzato per creare un sito Web di crowdfunding decentralizzato senza intermediari, come IndieGoGo.

Gli utenti di Ethereum possono investire in un'idea di business inviando denaro a un indirizzo di portafoglio intelligente di Ethereum.

➤ Se l'imprenditore non è in grado di raccogliere un certo importo di finanziamento entro un determinato periodo di tempo, il contratto intelligente può restituire automaticamente a tutti gli investitori i propri soldi.

ESEMPIO:

➤ Invece di pagare il 5% a IndieGoGo, dovranno solo pagare una commissione di 5 centesimi alla rete Ethereum per elaborare la transazione attraverso il **contratto intelligente**. Se la società **raccoglie 10 milioni di euro con Ethereum**, sarà in grado di **risparmiare mezzo milione di euro in commissioni**

AZIENDE CHE UTILIZZANO GLI SMART CONTRACTS (CONTRATTI SMART)

Facendo una **ricerca sul web** è possibile notare la presenza di svariati progetti che stanno **implementando gli smart contracts** attraverso la **blockchain**. **Ethereum è uno degli esempi più celebri**, ma segnaliamo la presenza di **numerose altre aziende** che stanno sfruttando nel migliore dei modi la potenza dei contratti digitali automatici.

Ecco i principali:

- Dash
- Ethereum
- Dfinity
- Etherisc
- EOS
- Polkadot

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

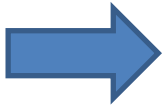
LE TRUFFE DEGLI SMART CONTRACT

- Sin dall'introduzione di questa tecnologia, si stima che oltre 2 miliardi di euro siano stati congelati, rubati, distrutti o comunque compromessi a causa di attacchi informatici.
- Le due maggiori criptovalute, in termini di capitalizzazione di mercato, hanno registrato perdite per circa 2 milioni di BTC e 5 milioni di ETH negli ultimi sette anni.
- Tra glie errori più grandi che si sono verificati nell'ecosistema di Ethereum si includono l'hack DAO e l'hack del portafoglio Parity.

LE TRUFFE DEGLI SMART CONTRACT

DAO

Il DAO era un contratto smart che venne lanciato nella rete Ethereum nel maggio del 2016. Con oltre 162 milioni di dollari equivalenti in Ether, divenne il crowdfunding più grande di sempre nel mondo delle criptovalute.



Tuttavia, il 17 giugno 2016, un hacker riuscì ad entrare all'interno della rete DAO sfruttando una bug nel suo software. Ciò gli consentì di rubare i fondi dal pool di token Ethereum di proprietà della rete DAO. 3,6 milioni di token ETH vennero rubati nelle prime due ore dell'attacco.


Il team e la community dietro Ethereum si affrettarono a sistemare il bug e molto presto risposero alla situazione, presentando molteplici proposte su come affrontare l'attacco.

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

LE TRUFFE DEGLI SMART CONTRACT

DAO



A causa dell'architettura del DAO, i fondi rubati sotto forma di Ethereum vennero segregati in un altro DAO (Child DAO), un ulteriore contratto intelligente, che richiedeva un periodo di detenzione di 28 giorni prima che l'hacker potesse ritirare e riciclare tutti i fondi. Ciò diede al team di Ethereum il tempo sufficiente per decidere come muoversi.

Vitalik Buterin, il creatore di Ethereum, si rese conto della gravità della violazione e rilasciò una dichiarazione subito dopo assicurando a tutti gli investitori che i loro fondi erano al momento sicuri.

La comunità di Ethereum, quindi, decise di eseguire il rendering di qualsiasi transazione, proveniente dall'account degli aggressori, con l'hash del codice come invalido, scongiurando quindi che l'hacker potesse prelevare i fondi, anche, dopo il periodo di detenzione di 28 giorni.

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

LE TRUFFE DEGLI SMART CONTRACT

Il team di Ethereum prese la decisione controversa e difficilissima, in termini aziendali, di rilasciare una nuova versione del software Ethereum che non includeva le transazioni hackerata. Il team, “riavvolse” la blockchain di Ethereum in modo da rimuovere le transazioni dell’hacker, creando quindi un hard fork.



La vecchia blockchain prese il nome di **Ethereum Classic**, mentre quella nuova adottò il nome Ethereum.

www.avvocatobruccoleri.it

[Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/](https://www.linkedin.com/in/maria-bruccoleri-648440135/)

INVESTIRE NELLE CRIPTOVALUTE SENZA TRUFFE

Con il **rialzo delle criptovalute** si sono presentate **molte opportunità di guadagno per gli investitori**. Come abbiamo visto, il mondo delle criptovalute è stato **contrassegnato da truffe e hacking** di ogni tipo **negli ultimi anni**.



Del resto, questo asset è nato come uno **strumento finanziario completamente decentralizzato**. Non è presente, ancora, un'autorità centrale, in grado di vigilare l'operato delle piattaforme e dei network e quindi il lavoro dei truffatori è facilitato

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

INVESTIRE NELLE CRIPTOVALUTE SENZA TRUFFE

Durante gli ultimi anni sono nati anche molti sistemi truffaldini come Bitcoin Future, Bitcoin Code e Bitcoin Evolution, metodi che promettono soldi facili con le criptovalute, senza fare assolutamente nulla. Nessuno di questi sistema funziona e tutti i fondi investiti verranno irrimediabilmente persi. Questo significa che investire sulle criptovalute è pericoloso? Assolutamente no, ma per operare in questo settore è necessario utilizzare piattaforme sicure.



Oltre che sicure, le piattaforme dovrebbero essere regolamentate ed autorizzate. Le migliori piattaforme infatti, rispettano le varie normative per la protezione degli investitori, come la direttiva dell'Unione europea 2004/39/CE (MIFID) che, per esempio, impone una protezione sui depositi fino a 20 mila euro.

www.avvocatobruccoleri.it

Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

INVESTIRE NELLE CRIPTOVALUTE SENZA TRUFFE

Qua sotto puoi trovare le **lista delle migliori soluzioni per investire oggi sulle criptovalute**. Tutte queste società consentono di **investire sulle criptovalute** che si basano sui **contratti smart come Ethereum e Qtum** ma anche **Bitcoin, Ripple, Litecoin** e molte altre crypto ancora.

Piattaforma: etoro Deposito Minimo: 200€ Licenza: Cysec	Copy Trading Adatto Per Principianti	Piattaforma: trade Deposito Minimo: 100€ Licenza: Cysec	Specialista A Disposizione Metatrader 4	Piattaforma: iqoption Deposito Minimo: 10€ Licenza: Cysec	Deposito Min: 10eur Conto Demo Gratuito
Piattaforma: forextrading Deposito Minimo: 250€ Licenza: Cysec	Ebook Gratuito Segnali Di Trading	Piattaforma: plus500 Deposito Minimo: 100€ Licenza: Cysec	Piattaforma Professionale Demo Gratis	Piattaforma: avatrading Deposito Minimo: 250€ Licenza: Cysec	Copy Trading Attivo Dal 2006

www.avvocatobruccoleri.it

[Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/](https://www.linkedin.com/in/maria-bruccoleri-648440135/)

CONSIDERAZIONI FINALI

Abbiamo visto che cosa sono e come funzionano i **Contratti Smart**, analizzando la loro complessità e potenzialità.

Questa tecnologia ha la possibilità di cambiare il modo di fare business per sempre, in quanto utilizzandolo, i governi e le aziende possono diminuire i costi, **automatizzare l'esecuzione del contratto e fornire una traccia verificabile di controllo.**

www.avvocatobruccoleri.it

[Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/](https://www.linkedin.com/in/maria-bruccoleri-648440135/)

Piazza A. Diaz, 6
Milano, 20123
Cell 328 8871062
E-mail: studiolegalebruccoleri@gmail.com

STUDIO LEGALE
BRUCCOLERI & PARTNERS
Tributario e Penale

Via Gioacchino di Marzo 5
Palermo, 90144 Tel. 091 309131
PEC: avvmariabruccoleri@legamail.it
Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/

GRAZIE PER L'ATTENZIONE

www.avvocatobruccoleri.it
Linkedin: www.linkedin.com/in/maria-bruccoleri-648440135/