Smart Contract

Una overview tecnica

Novembre 2025 - Giampaolo Murabito - https://giampa.site

Chi sono

Mi occupo di Information Technology dal 2002, erogo consulenze come business strategy, startup, architetture fiscali on-shore/off-shore, compliance VASP AML/CFT.

Spesso (forse troppo spesso) entro in partecipazione azionaria con le startup a cui presto la mia opera.

2010 - sviluppo ScontrinoSicuro: sistema installato su migliaia di registratori di cassa in Italia

2013 - architetto e realizzo GutenberNext: sistema di firma grafometrica in ambito assicurativo (credo che ancora funzioni dentro Groupama Assicurazioni)

2016/2018 - ETH Genesis Wallet: contribuisco col Prof. Ateniese al password recovery di un wallet Ethereum con 20.000 ETH e ETC. Scrivo un trading system crypto con performance simili agli HFT (High Frequency Trading)

2019 - costruisco da zero una mining farm a Sofia, Bulgaria, con ASIC Innosilicon minando LTC

2020 - apro il mio piccolo AIF (Fondo di Investimento Alternativo)

2022 - rilevo Treedefi.com

2023 - ottengo una licenza finanziaria per un CEX (Centralized EXchange) crypto-fiat a Vilnius/Lituania

2024 - co-fondo su Telegram YesCoin (14 Mln di Utenti), Wydon.io e torno sul web con OraPrima.com

2025 - in pubblicazione “The Italian Way: An unofficial guide to becoming one of us”

Smart Contract

“Uno smart contract è un insieme di promesse, specificate in forma digitale,che include i protocolli attraverso i quali le parti adempiono a tali promesse.

L’idea di base degli smart contract è che molti tipi di clausole contrattuali (come garanzie, obblighi, delimitazione dei diritti di proprietà, ecc.) possano essere incorporati nell’hardware e nel software con cui interagiamo,in modo tale da rendere una violazione del contratto costosa — e, se lo si desidera, talvolta proibitivamente costosa — per chi la commette.”

Nick Szabo, Smart Contracts: Building Blocks for Digital Markets (1996)

Agenda

1. Cos’è uno Smart Contract
2. Caratteristiche degli Smart Contract
3. Comprendere gli Smart Contract
4. Blockchain e DLT
5. Contesto operativo
6. Benefici Potenziali
7. Esempi di Logica Auto-Esecutiva
    a. Applicazione: Assicurazioni
    b. Applicazione: Noleggio Operativo
    c. Applicazione: CDS - Credit Default Swap
    d. Altre applicazioni
8. Proviamo!
9. Domande

Cos’è uno Smart Contract

Uno smart contract è un codice informatico che:

- Include gli elementi di un contratto vincolante *(ad esempio: offerta, accettazione e controprestazione)*

- Compie azioni in base al verificarsi di un evento *(ad esempio: la consegna di un bene, una determinata condizione meteorologica o la variazione di un tasso di riferimento)*

- E’ generalmente decentralizzato, viene verificato ed eseguito simultaneamente su più nodi di una blockchain/DLT *(Permissioned/Permissionless)*

Caratteristiche degli Smart Contract

Il termine “smart contract” può essere un ossimoro, infatti non è necessariamente:

- **Intelligente**, il suo funzionamento è tanto “intelligente” quanto il codice che lo rappresenta! *(Cfr. The DAO, Poly Network, Axie Infinity)*

- **Vincolante,** può rappresentare una donazione o costituire solo una parte di un contratto più ampio. La validità giuridica NON è contemplata, ovviamente, dalla tecnologia.

Comprendere gli Smart Contract

Utilizzano firme digitali e crittografia a chiave pubblica e verificano la partecipazione e l'accettazione delle condizioni concordate.

Autentica gli elementi della transazione

- Le identità delle controparti
- La proprietà degli asset e dei diritti correlati

Accede a informazioni esterne (API)

- Oracoli concordati tra le parti *(ad es. prezzi, dati meteorologici, tassi, etc...)*

Automatizza esecuzione

- Compie automaticamente le azioni programmate senza alcun intervento ulteriore da parte delle controparti *(a*d es. dividendi, innaffiamento, attivazione assicurativa, attività meccaniche)

Blockchain e DLT

Gli smart contract sono eseguiti su una blockchain o un DLT.

- Decentralizzati: lo smart contract viene replicato su tutti i nodi della rete, impedendo qualsiasi modifica non autorizzata o non concordata tra le parti

- Blockchain/DLT: è un mastrino immutabile composto da blocchi di registrazioni e collegati tramite crittografia con una unità di conto attraverso un algoritmo di consenso generato da uno sforzo computazionale (PoW)* o di deposito (PoS)*:
  - Coin -> Bitcoin
  - Token -> Ethereum, BNB , Tron
  - NFT -> Non-Fungible Token
  - Standard -> ERC20, BEP20, TRC20

**PoW - Proof of Work, PoS - Proof of Stake*

Contesto operativo

L’automazione è sempre più presente nella vita quotidiana, attraverso strumenti come:

- Il bancomat (ATM)
- I pagamenti automatici delle bollette
- I sistemi contactless (touch-to-pay)
- Le app per trasferimenti di denaro istantanei

Gli smart contract rappresentano l’estensione logica di questa tendenza: automatizzano il mondo fisico e centralizzato verso quello digitale e decentralizzato.

Benefici potenziali

Offrono vantaggi in tutte le fasi di una transazione economica:

- **Standardizzazione:** l'uso di codice e procedure comuni riduce i costi e semplifica i rapporti tra le parti.
- **Innovazione:** l'automazione favorisce nuovi modelli più efficienti e trasparenti.
- **Sicurezza:** transazioni integre, pseudonime e tracciabili
- **Economia:** riduzione di tempi e processi
- **Certezza:** l'esecuzione automatica limita i rischi
- **Innovazione:** consente conformità non ripudiabile.

Gli Smart Contract sono strumenti chiave della trasformazione digitale dell'economia e della finanza.

Esempi di Logica Auto-Esecutiva

Un distributore automatico propone termini predefiniti, secondo i quali il venditore si impegna a fornire immediatamente al compratore un prodotto al momento del pagamento dell'importo indicato.

Se il pagamento (Pag) è ricevuto e l'articolo (A) selezionato è disponibile, allora:

se Pag ≥ prezzo(A), eroga l'articolo A

se Pag > prezzo(A), eroga anche il resto

altrimenti, emetti un segnale acustico e attendi

"un sistema che esegue automaticamente un'azione (erogare un prodotto) solo quando si verifica una determinata condizione (pagamento corretto):"

Applicazione: Assicurazioni

Business: Il Sig. Del Monte acquista una piantagione di ananas alle Hawaii.

- Rischio: le condizioni meteorologiche
- Assicurazione: PineSafe propone polizza tramite uno smart contract
- Smart Contract: Del Monte e PineSafe lo firmano con un Wallet
- Deployment: Lo Smart Contract viene “deployato” sulla blockchain

Funzionamento dello Smart Contract:

1. Lo smart contract automatizza i pagamenti mensili da Del Monte verso PineSafe.
2. Ogni giorno, il contratto verifica i dati meteorologici forniti da un’autorità terza*
3. Se accade un evento di gelo il contratto esegue automaticamente il pagamento del risarcimento

**L’autorità terza, che fornisce i dati esterni e certifica l’evento, è chiamata oracolo.*

Applicazione: Noleggio Operativo

Business: Stefania utilizza uno smart contract per noleggiare una bicicletta.

- Deposito Cauzionale: lo smart contract sblocca automaticamente la bici.
- Rischio: Lo Smart Contract monitora velocità e distanza via RTS (Ride Tracking Service).
- Status: Stefania ferma la bici in un punto di noleggio diverso dalla partenza.
- Lo smart contract trasferisce automaticamente i fondi alla società RentCo e blocca nuovamente la bici.

Funzionamento dello Smart Contract:

1. Traccia e gestisce tariffe, penali, pagamenti e rimborsi.
2. Avvisa RentCo se Stefania esce dall'area di servizio.
3. Blocca o sblocca il mezzo in base allo stato del noleggio
4. Registra tutte le operazioni sulla blockchain

Applicazione: CDS - Credit Default Swap

Business: Banca stipula un CDS

- Ogni trimestre: calcolo del premio dovuto e trasferimento del pagamento dalla banca al dealer
- Debitore Insolvente: Il contratto verifica tramite un oracolo se si è verificato un evento di default.
- Se il debitore risulta insolvente, lo smart contract calcola l'importo dovuto e trasferisce automaticamente il pagamento dal dealer alla banca.

Funzionamento dello Smart Contract:

1. Automatizza i pagamenti trimestrali della banca verso il dealer.
2. Controlla quotidianamente i dati provenienti da un servizio di informazione finanziaria per verificare eventuali eventi di insolvenza.
3. In caso di default, attiva immediatamente il pagamento del risarcimento alla banca.

Altre applicazioni

Derivati: semplificano i processi post-contrattuali, permettono valutazioni in tempo reale e margin call automatiche.

MultiSignature Wallet: portafogli digitali che richiedono più firme (chiavi) per autorizzare una transazione, aumentando sicurezza e controllo condiviso.

Escrow & Supply chain: tracciano il movimento dei prodotti, semplificano i pagamenti e favoriscono liquidità e credito.

Con l'Internet of Things (IoT), anche veicoli, abitazioni o aziende agricole possono eseguire richieste di risarcimento automatiche.

Real World Assets: si trasformano crediti o attività in titoli finanziari da vendere agli investitori con mercato primario e secondario.

Crowdfunding:

- **ICO (Initial Coin Offering):** raccolta fondi tramite vendita di token direttamente al pubblico.
- **IEO (Initial Exchange Offering):** raccolta fondi gestita da un exchange, che verifica e distribuisce i token.
- **STO (Security Token Offering):** emissione di token regolamentati che rappresentano valori mobiliari o diritti finanziari reali

Non resta che provare!

1. Apriamo due wallet
2. Scambiamo dei fondi
3. Leggiamo la transazione su blockchain

Opzionale (ossia se c'è tempo): facciamo un multi-sig!

Domande

Tecnologia: Token, Coin & Standard

- Criptovalute, Blockchain, Bitcoin, Ethereum, BNB, Tron, USDT, etc...

Applicazioni

- Finanza, assicurazione, crowdfunding, etc...

Sicurezza & Legalità

- Audit e performance analysis, Chain Analysis

Dove e come usarli

- Legislazioni, Framework normativi, MICAR, CNMA, VASP

Grazie :-)

Email: giampaolo.murabito@gmail.com

Telegram: @giampetterson

Web: https://giampa.site