

# Smart contracts

# SMART CONTRACTS



---

## B L O C K C H A I N

---

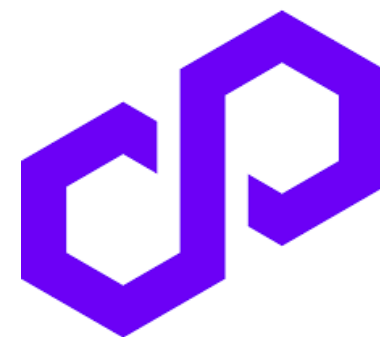




# SMART CONTRACTS



Ethereum



Polygon



Avalanche



Hyperledger



Solana

---

**B L O C K C H A I N**

---



# SMART CONTRACTS

## 1994



 @NickSzabo4

<http://unenumerated.blogspot.com>

A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), **minimize exceptions** both malicious and accidental, and **minimize the need for trusted intermediaries**. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.

**-Nick Szabo “The Idea of Smart Contracts”**





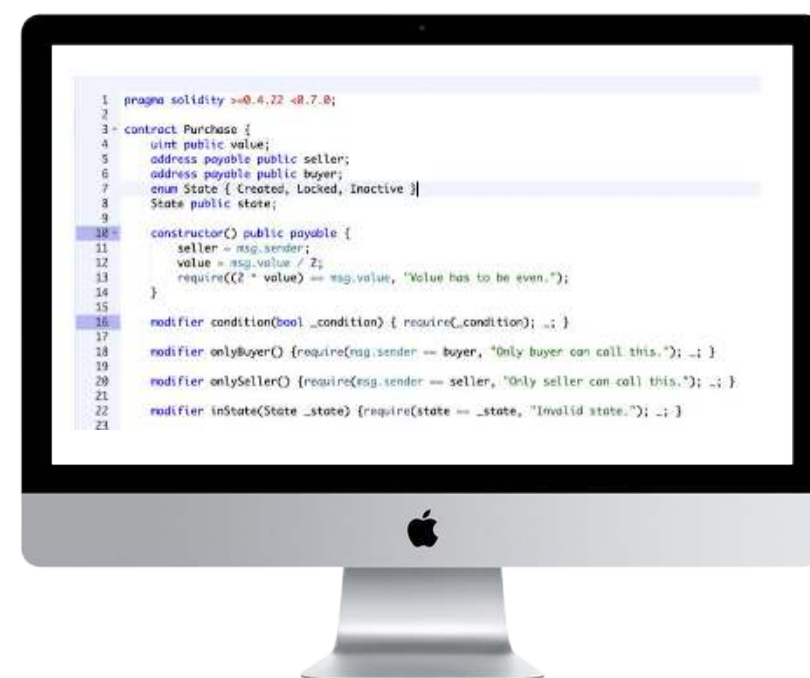




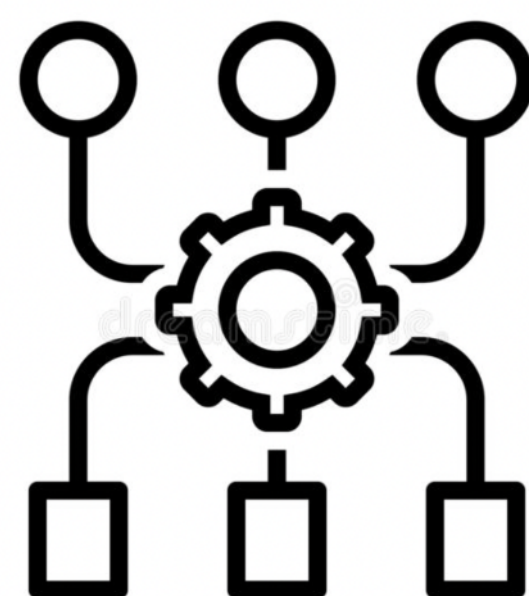
```
1  pragma solidity >=0.4.22 <0.7.0;
2
3  contract Purchase {
4      uint public value;
5      address payable public seller;
6      address payable public buyer;
7      enum State { Created, Locked, Inactive }
8      State public state;
9
10     constructor() public payable {
11         seller = msg.sender;
12         value = msg.value / 2;
13         require((2 * value) == msg.value, "Value has to be even.");
14     }
15
16     modifier condition(bool _condition) { require(_condition); _; }
17
18     modifier onlyBuyer() {require(msg.sender == buyer, "Only buyer can call this."); _; }
19
20     modifier onlySeller() {require(msg.sender == seller, "Only seller can call this."); _; }
21
22     modifier inState(State _state) {require(state == _state, "Invalid state."); _; }
23
24     event Aborted();
25     event PurchaseConfirmed();
26     event ItemReceived();
27
28     function abort()
29         public
30         onlySeller
31         inState(State.Created)
32     {
33         emit Aborted();
34         state = State.Inactive;
35         seller.transfer(address(this).balance);
36     }
37
38     function confirmPurchase()
39         public
40         inState(State.Created)
41         condition(msg.value == (2 * value))
42         payable
43     {
44         emit PurchaseConfirmed();
45         buyer = msg.sender;
46         state = State.Locked;
47     }
48
49     function confirmReceived()
50         public
51         onlyBuyer
52         inState(State.Locked)
53     {
54         emit ItemReceived();
55         state = State.Inactive;
56
57         buyer.transfer(value);
58         seller.transfer(address(this).balance);
59     }
60 }
```



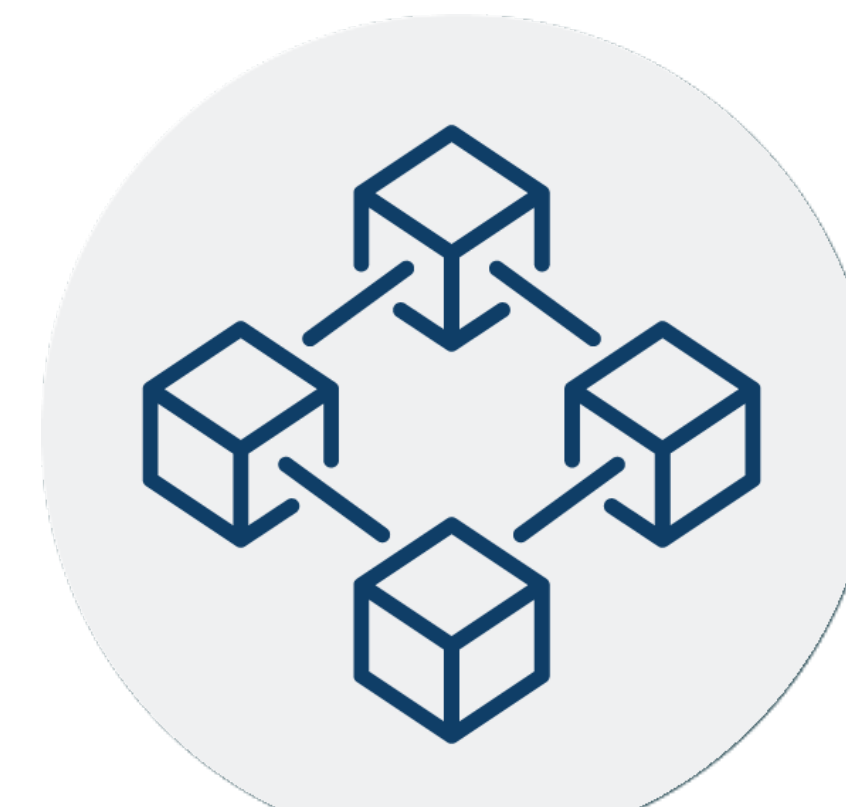
# CICLO DI VITA DI UNO SMART CONTRACT



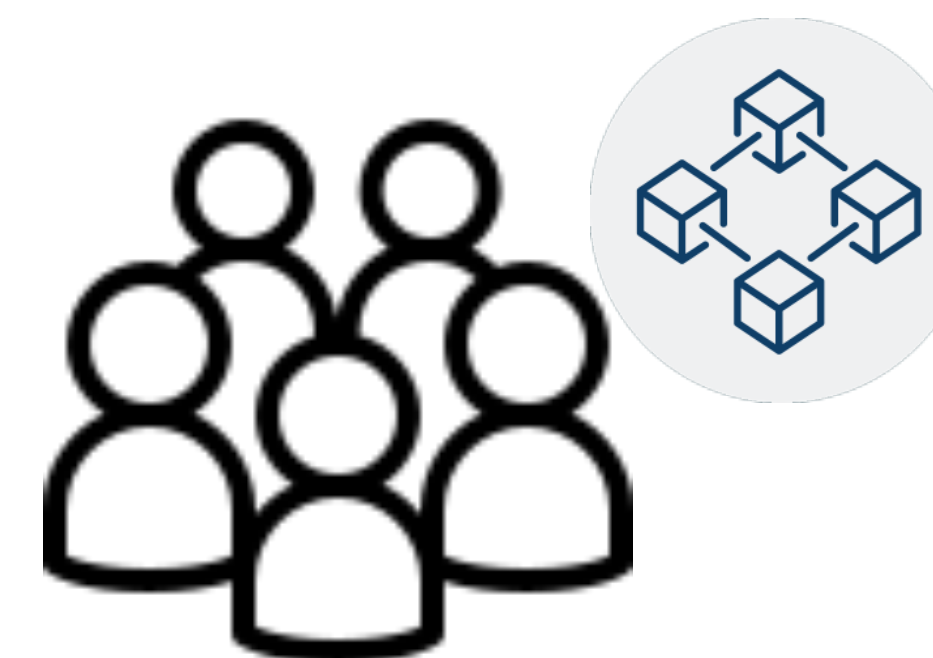
## 1. REDAZIONE CODICE



## 4. IL CONTRATTO VIENE ESEGUITO SULLA BLOCKCHAIN



## 2. ATTESTAZIONE SULLA BLOCKCHAIN



## 3. IL CONTRATTO È ACCESSIBILE SULLA BLOCKCHAIN

## Indirizzo eth Contratto

0x692a70d2e424a56d2c6c27aa97d1a86395877b3a

## Istruzioni codice bytecode

## Memoria volatile

# Stack

## Array

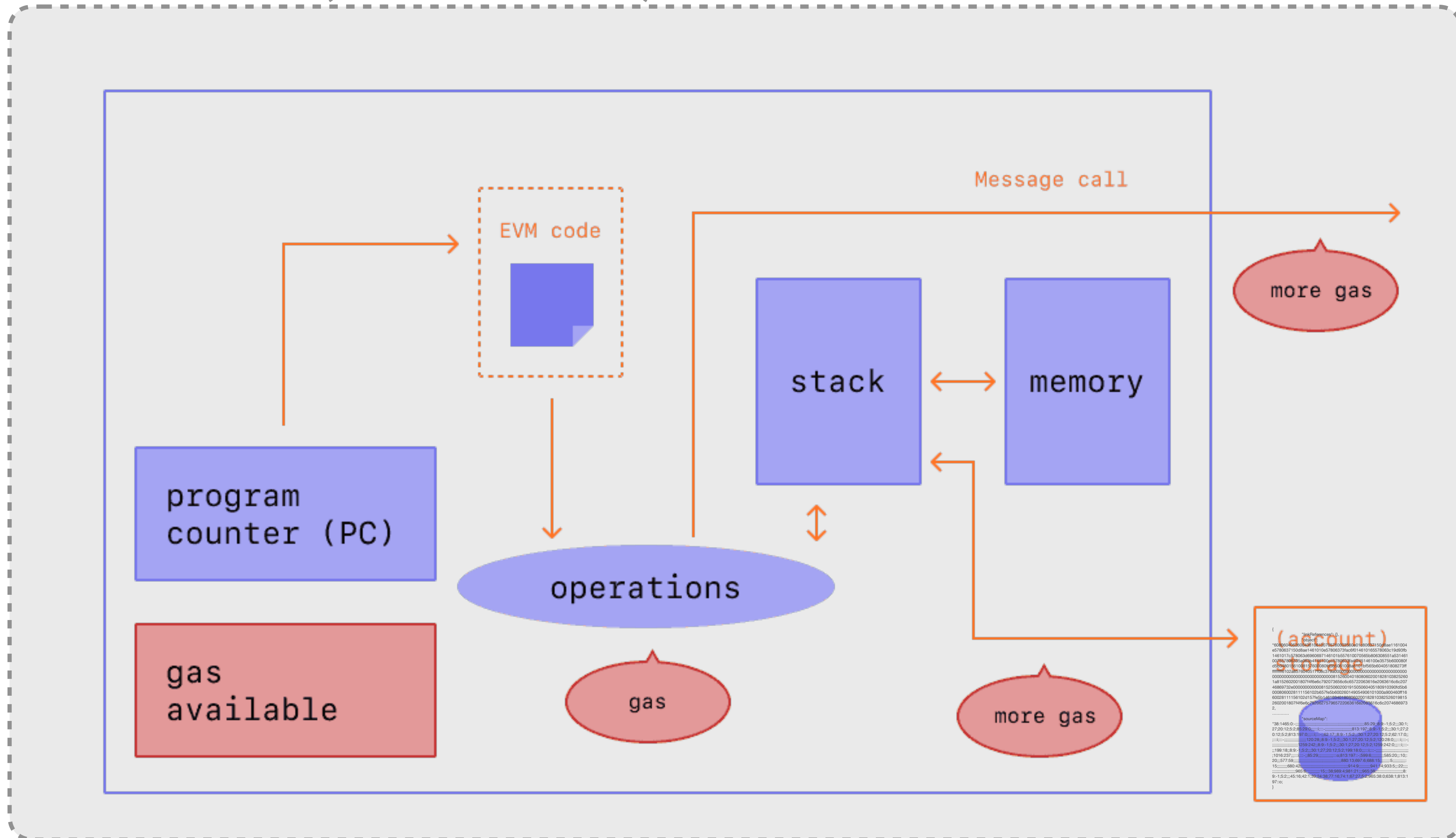
## Memoria permanente

## Storage



# ATTESTAZIONE DEL CONTRATTO SULLA BLOCKCHAIN

## NODO ETHEREUM (ETHEREUM CLIENT)



A stylized, high-contrast black and white illustration of a pair of round-rimmed glasses. The frames are thick and circular, with a simple bridge connecting the two lenses. The temples (sides) are also thick and curve slightly upwards at the ends. The entire graphic is rendered in solid black against a plain white background.

## Attivazione funzione

## Osservazione

## Indirizzo eth Contratto

0x692a70d2e424a56d2c6c27aa97d1a86395877b3a

## Istruzioni codice bytecode

```
{
  "linkReferences": {},
  "object":
    "6080604052600436106100705760003560e01c80637150d8ae1161004e5780637150d8ae1461010e5780
    6373fac6f014610165578063c19d93fb1461017c578063d6960697146101b557610070565b806308551a53
    1461007557806335a063b4146100cc5780633fa4f245146100e3575b600080fd5b34801561008157600080f
    d5b5061008a6101bf565b604051808273ffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffff1681526
    0200191505060405180910390f35b34801561100d857600080fd5b506100e16101e5565b005b3480156100e
    f57600080fd5b506100f8610416565b6040518082815260200191505060405180910390f35b34801561011a
    57600080fd5b5061012361041c565b604051808273ffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffff
    ffff16815260200191505060405180910390f35b34801561017157600080fd5b5061017a610442565b005b34
    801561018857600080fd5b506101916106de565b60405180826002811156101a157fe5b60ff16815260200
    191505060405180910390f35b6101bd6106f1565b005b60016000905490610100a900473fffffffffffffffffffff
    ffffffffffffff1681565b60016000905490610100a900473fffffffffffffffffffff1673fffffffffffffffffffff
    ffffffffff163373fffffffffffffffffffff16146102a8576040517f08c379a0000000000000000000000000000000000
    .....
  "sourceMap":
    "38:1465:0-;.....;85:29;;8:9-1;5:2;;;30:1;27;20;12;5:2;85:29:0;...;.....;
    .....;813:197;;8:9-1;5:2;;;30:1;27;20;12;5:2;813:197:0;...;.....;62:17;;8:9-1;5:2;;;30:1;27;20;12;5:2;62:
    17:0;...;.....;120:28;;8:9-1;5:2;;;30:1;27;20;12;5:2;120:28:0;...;.....;1259:242;;8:9-
    -1;5:2;;;30:1;27;20;12;5:2;1259:242:0;...;.....;199:18;;8:9-1;5:2;;;30:1;27;20;12;5:2;199:18:0;...;.....;
    .....;1016:237;...;.....;85:29;...;.....;813:197;...;.....;599:6;...;.....;585:20;;10;20;577:59;
    .....;880:13;697:6;688:15;...;.....;5;...;.....;15;...;.....;680:42;...;.....;914:9;...;.....;941:1
    4;933:5;;22;...;.....;965:6;...;.....;15;;38;989:4;981:21;;965:38;...;.....;8:9-1;5:2;;45:16;42:1
    ;39;24:38;77:16;74:1;67:27;5:2;965:38:0;638:1;813:197:0;;o;
  }
}
```

## Azione

## Memoria volatile

# Stack

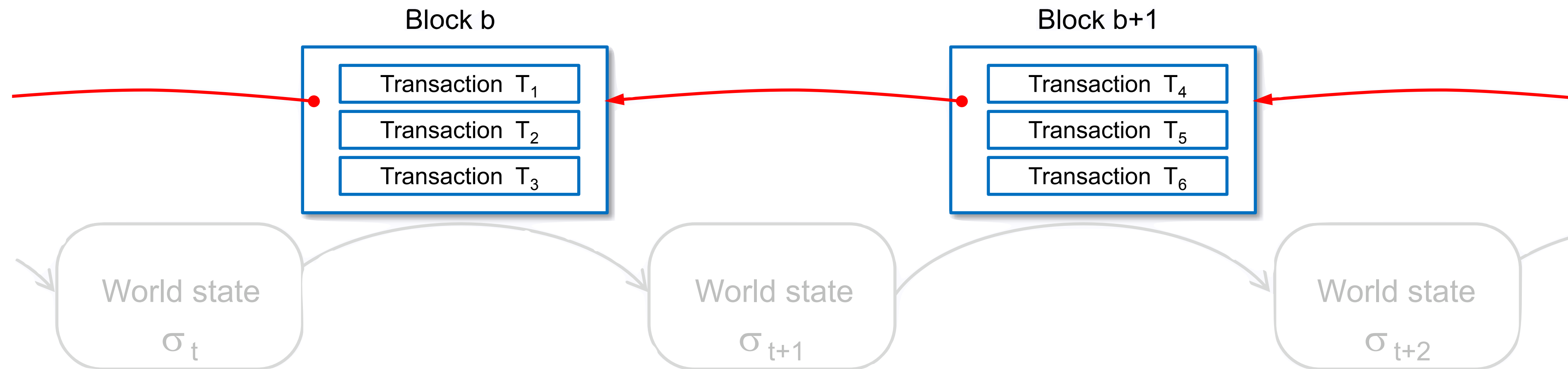
# Array

## Memoria permanente

## Storage

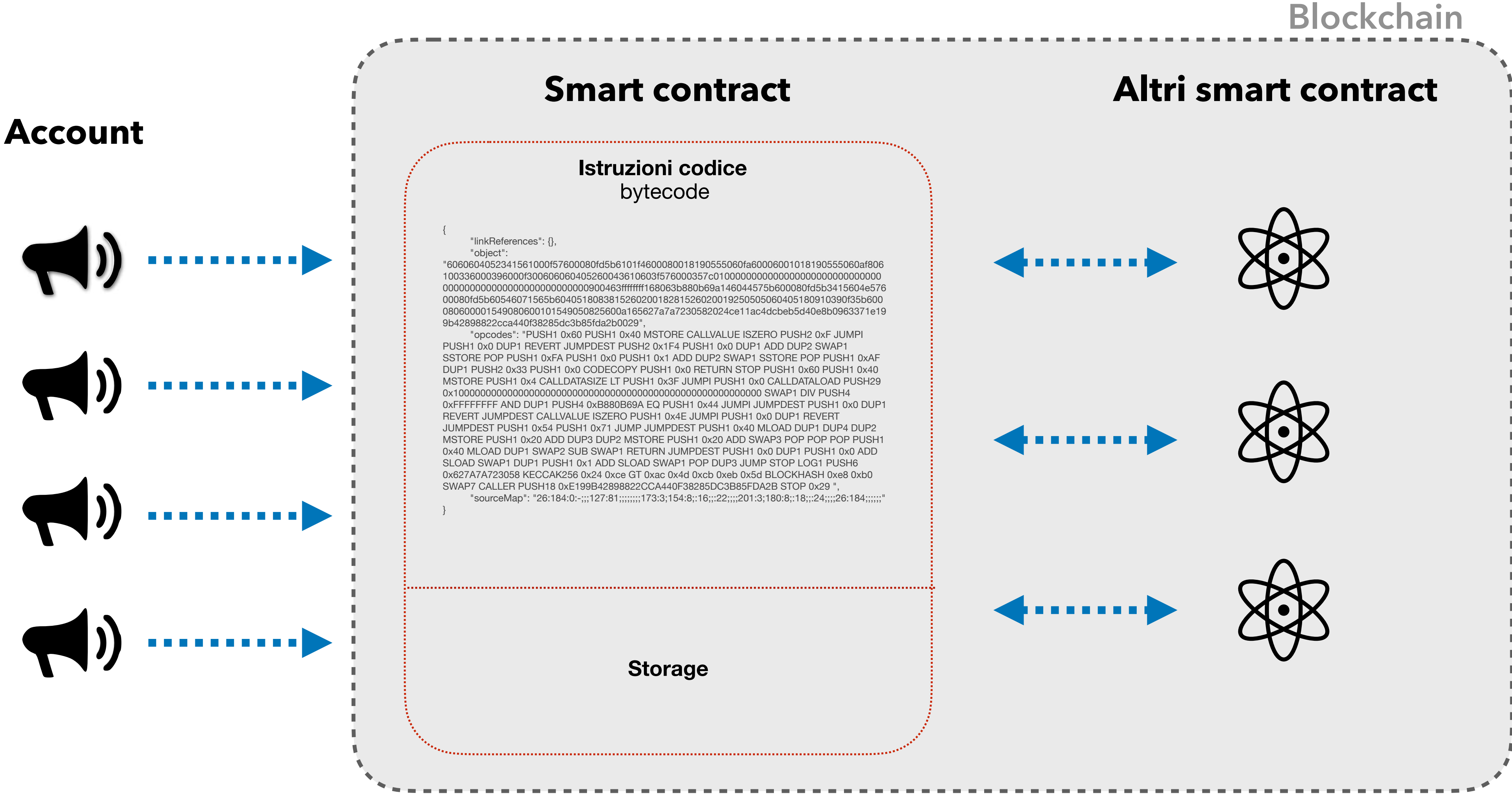


## Chain of blocks: Blockchain



From the viewpoint of the implementation,  
Ethereum can also be seen as a chain of blocks, so it is 'BLOCKCHAIN'.

# L'ECOSISTEMA DELLO SMART CONTRACT





## Perché gli smart contract non si collegano all'esterno

- **Regola uguale per tutti.** Ogni nodo deve rifare gli stessi calcoli e arrivare allo stesso risultato. Se il contratto chiedesse un dato online, i nodi potrebbero ricevere **risposte diverse** → niente accordo comune.
- **Prova e verificabilità.** La blockchain deve poter **verificare domani** ciò che è successo oggi. Una pagina web può cambiare, sparire o dare esiti diversi: **non è prova stabile** dentro la blockchain.
- **Rischio terzi.** Affidarsi a un sito o servizio esterno crea un **single point of failure** e di possibile manipolazione. “Dati sbagliati → esecuzione sbagliata”, spesso **irreversibile**.
- **Regole di sistema.** Per evitare questi rischi, le macchine che eseguono i contratti **bloccano le chiamate di rete**: niente HTTP, niente Internet.

**L'isolamento non è un limite tecnico casuale:** è una garanzia di integrità e consenso.

## Come si porta “il mondo reale” dentro la blockchain

### Soluzione: gli oracoli (un “notaio” digitale)

- Il contratto **chiede** un dato *sulla* blockchain (richiesta registrata).
- Una rete di operatori indipendenti (**oracoli**) raccoglie il dato fuori dalla blockchain.
- Gli oracoli **riportano** il risultato *sulla* blockchain con firme e verifiche.  
Il dato diventa parte dello **stato comune**, quindi **verificabile** e **uguale per tutti**.

### Perché è accettabile anche dal punto di vista legale

- **Trasparenza:** richiesta, fonte e risposta sono registrate on-chain.
- **Affidabilità:** più fonti/operatori riducono il rischio di errore o manipolazione.
- **Accountability:** compensi, penali e reputazione creano **incentivi corretti**.

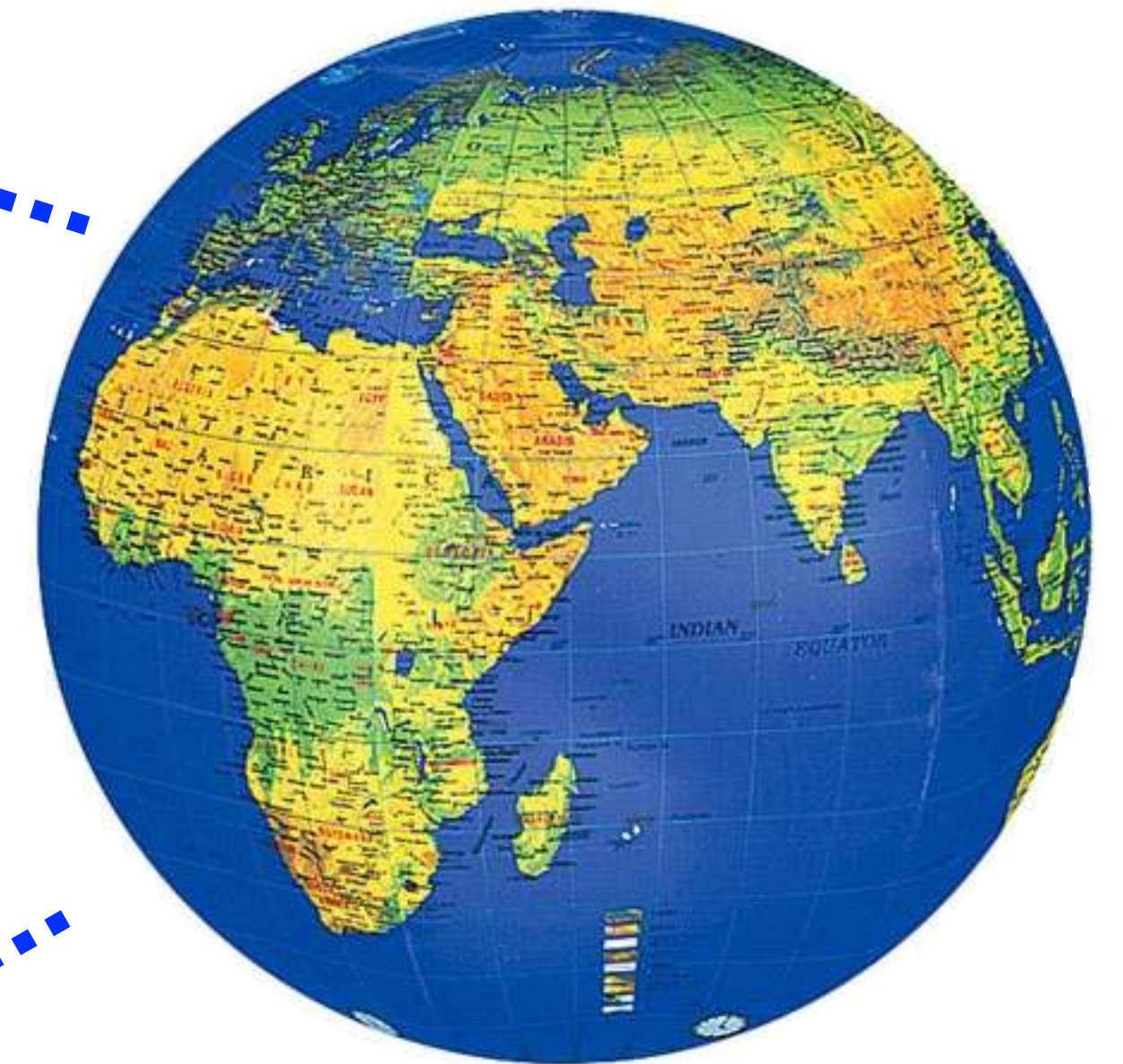
**Gli oracoli non collegano il contratto a Internet:**  
portano Internet nella blockchain in modo controllato e dimostrabile.



## Smart contract

## Storage

# Oracoli





# Blockchain

## Smart contract

```
{
  "linkReferences": {},
  "object":
    "6060604052341561000f57600080fd5b6101f4600080018190555060fa60006001018190
    555060af806100336000396000f300606060405260043610603f576000357c0100000000
    00000000000000000000000000000000000000000000000000000000000000000000
    900463ffffff168063b880b6
    9a146044575b600080fd5b3415604e57600080fd5b60546071565b60405180838152602
    0018281526020019250505060405180910390f35b600080600001549080600101549050
    825600a165627a7a7230582024ce11ac4dcbeb5d40e8b0963371e199b42898822cca440
    f38285dc3b85fda2b0029",
  "opcodes": "PUSH1 0x60 PUSH1 0x40 MSTORE CALLVALUE ISZERO PUSH2 0xF
    JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH2 0x1F4 PUSH1 0x0 DUP1 ADD
    DUP2 SWAP1 SSTORE POP PUSH1 0xFA PUSH1 0x0 PUSH1 0x1 ADD DUP2 SWAP1
    SSTORE POP PUSH1 0xAF DUP1 PUSH2 0x33 PUSH1 0x0 CODECOPY PUSH1 0x0
    RETURN STOP PUSH1 0x60 PUSH1 0x40 MSTORE PUSH1 0x4 CALLDATASIZE LT
    PUSH1 0x3F JUMPI PUSH1 0x0 CALLDATALOAD PUSH29
    0x10000000000000000000000000000000000000000000000000000000000000000000
    SWAP1 DIV
    PUSH4 0xFFFFFFFF AND DUP1 PUSH4 0xB880B69A EQ PUSH1 0x44 JUMPI
    JUMPDEST PUSH1 0x0 DUP1 REVERT JUMPDEST CALLVALUE ISZERO PUSH1 0x4E
    JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH1 0x54 PUSH1 0x71 JUMP
    JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP4 DUP2 MSTORE PUSH1 0x20 ADD
    DUP3 DUP2 MSTORE PUSH1 0x20 ADD SWAP3 POP POP POP PUSH1 0x40 MLOAD
    DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH1 0x0 DUP1 PUSH1 0x0 ADD
    SLOAD SWAP1 DUP1 PUSH1 0x1 ADD SLOAD SWAP1 POP DUP3 JUMP STOP LOG1
    PUSH6 0x627A7A723058 KECCAK256 0x24 0xce GT 0xac 0x4d 0xcb 0xeb 0x5d
    BLOCKHASH 0xe8 0xb0 SWAP7 CALLER PUSH18
    0xE199B42898822CCA440F38285DC3B85FDA2B STOP 0x29 ",
  "sourceMap":
    "26:184:0:-;;;127:81;;;;;173:3;154:8;:16;;;22;;;201:3;180:8;:18;;;24;;;26:184;;;;;"
}
```

## Storage

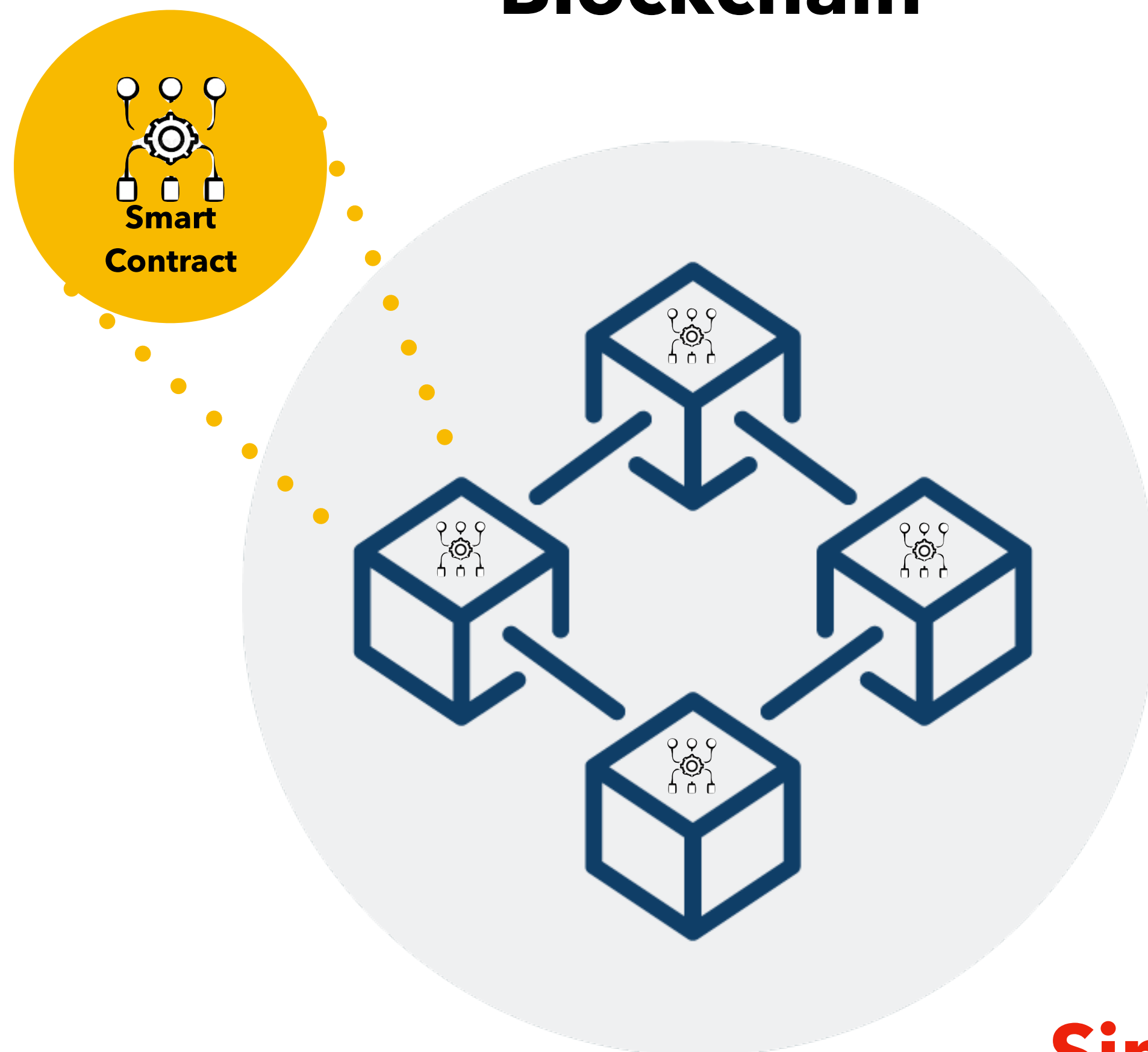
## Oracoli



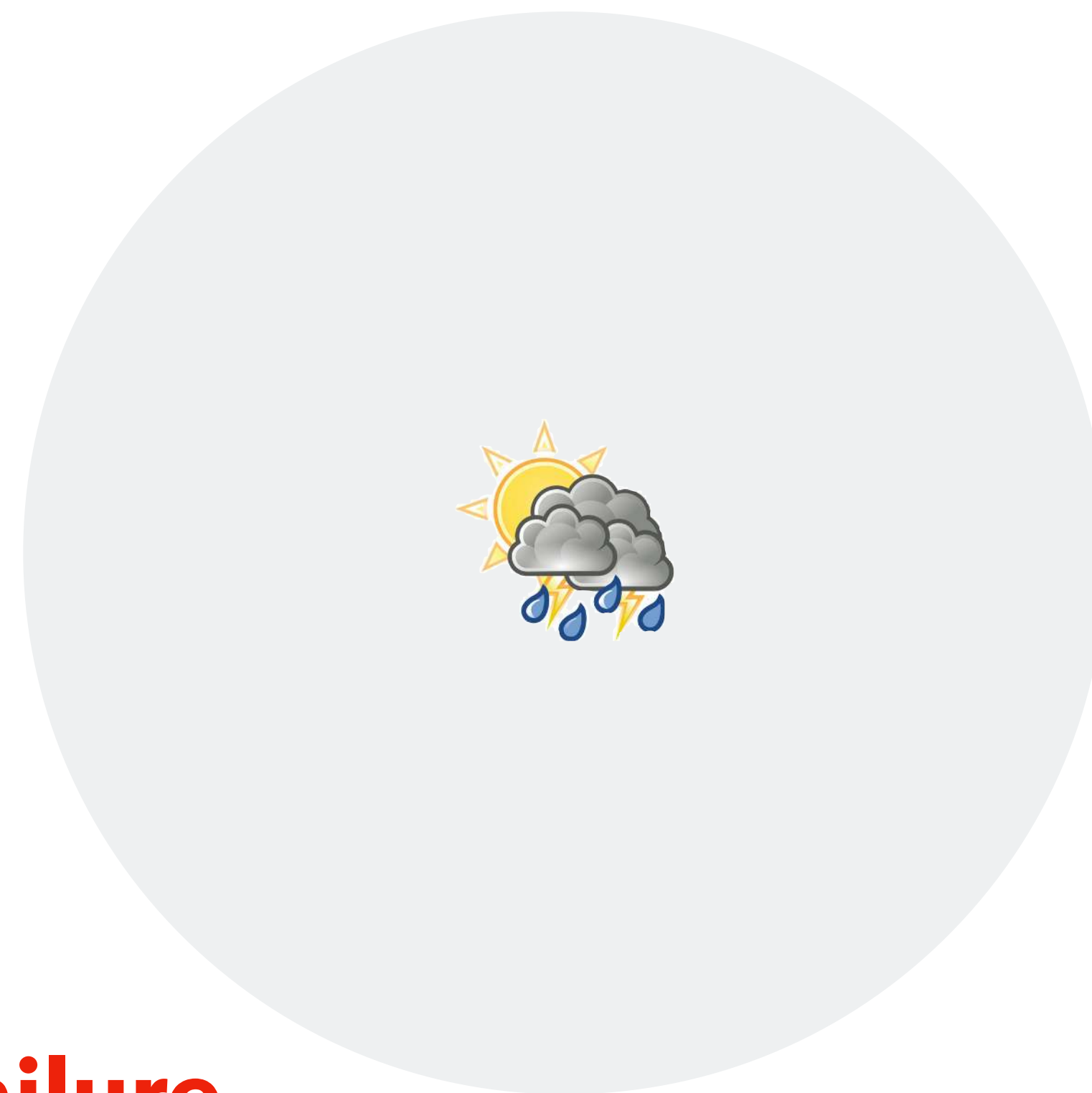




## Blockchain

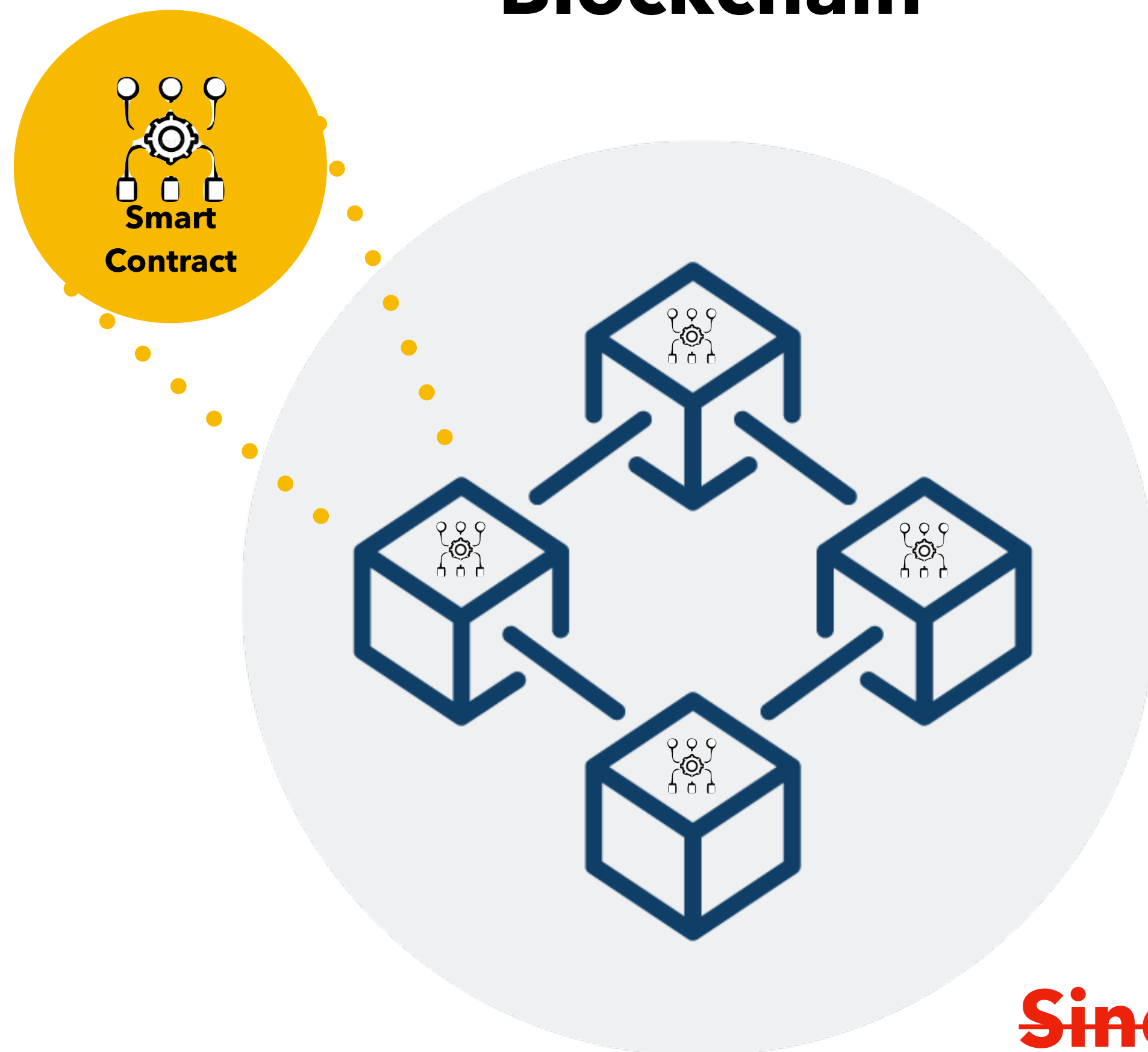


## Oracolo

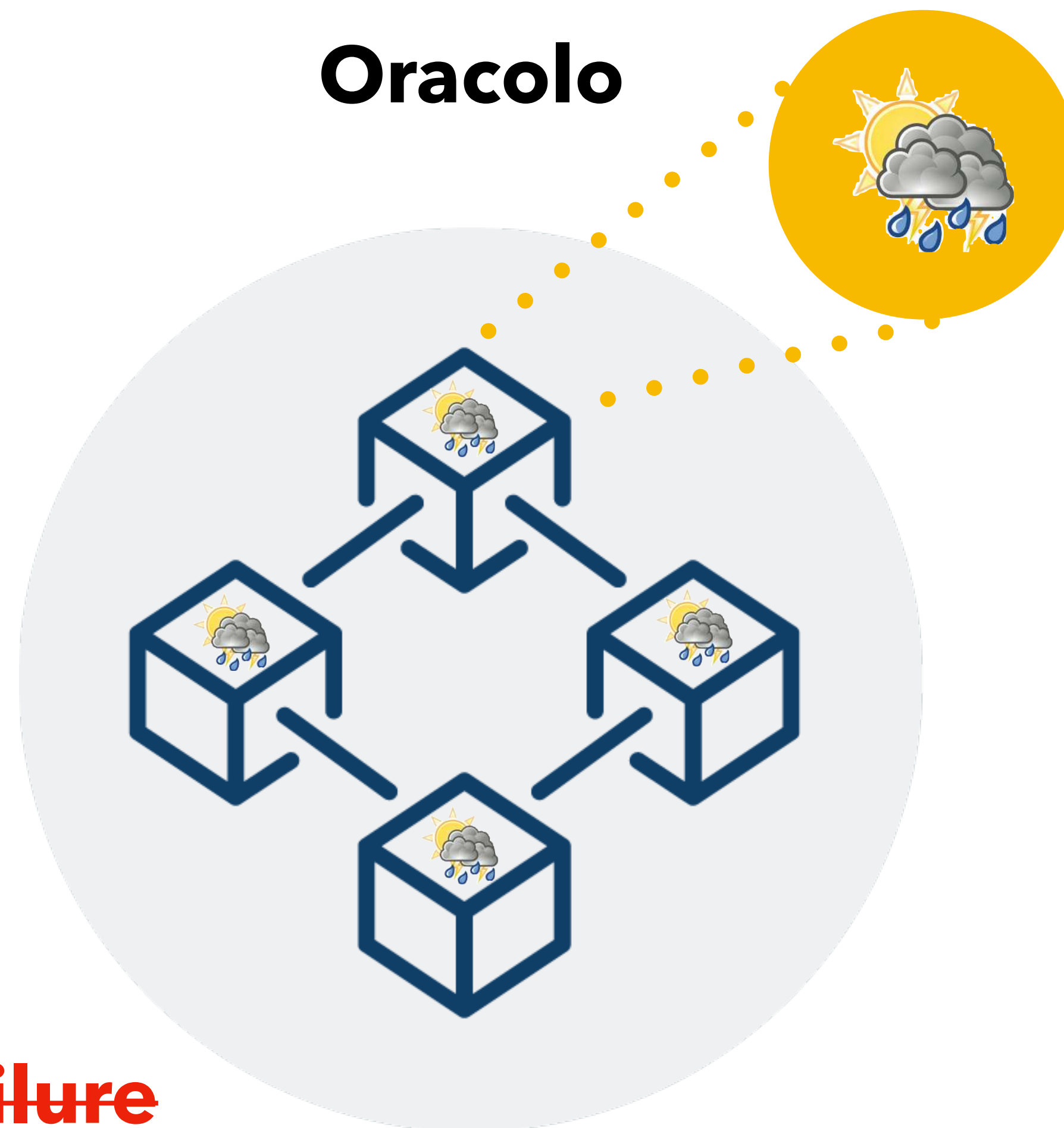


**Single point of failure**

## Blockchain



## Oracolo



~~Single point of failure~~  
**Decentralizzazione**



## Piattaforme Blockchain - Smart Contracts

| <br><b>ETHEREUM</b> | <br><b>POLYGON</b> | <br><b>AVALANCHE</b> | <br><b>HYPERLEDGER</b> | <br><b>SOLANA</b> |
|------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Standard                                                                                             | Costi ridotti                                                                                         | Subnet custom                                                                                           | Permissioned                                                                                              | High throughput                                                                                      |
| Massima sicurezza                                                                                    | EVM compatible                                                                                        | Performance                                                                                             | Enterprise                                                                                                | Costi ridotti                                                                                        |
|                                                                                                      | Enterprise adoption                                                                                   | DeFi focus                                                                                              |                                                                                                           | Rust-based                                                                                           |

## 💡 **Smart Contract: Tipi e Casi d'Uso Pratici** 💡

Una panoramica di come i contratti auto-eseguibili stanno trasformando i processi legali e commerciali.



## Tokenizzazione e Vendita di Beni Digitali (NFT)

Un smart contract gestisce in modo sicuro e automatizzato la compravendita di un asset digitale unico.

- **Come funziona:** il diritto di proprietà di un bene digitale è incorporato in un NFT (Non-Fungible Token).
  - L'**acquirente** paga il corrispettivo allo smart contract.
  - Lo smart contract trasferisce l'**NFT** all'acquirente, che ottiene così il diritto di proprietà.
  - Allo stesso tempo, il contratto rilascia il corrispettivo al **titolare del diritto** (il venditore), che lo incassa.
-  **Esempio:** La vendita di opere d'arte digitali come "Everydays: The First 5,000 Days" di Beeple, venduta da Christie's per 69,3 milioni di dollari. Lo smart contract garantisce lo scambio istantaneo e sicuro tra il pagamento e il token di proprietà.

### **Rilevanza per i professionisti:**

Gestione di nuovi mercati per beni digitali.

Tracciabilità e certificazione della proprietà per fini contabili e fiscali.

Automazione del calcolo e del versamento delle royalties.

## Assicurazioni Parametriche (Smart Insurance)

Gli smart contract creano polizze "intelligenti" che attivano rimborsi automatici al verificarsi di eventi misurabili, eliminando le lunghe attese.

- **Come funziona:** La logica è basata su una semplice condizione "se... allora...".
  - L'**assicurato** paga il premio.
  - L'**assicuratore** mette a disposizione dello smart contract la provvista per il risarcimento.
  - Lo smart contract **monitora il verificarsi del sinistro** tramite dati esterni (es. dati meteo, stato di un volo).
  - Se l'evento si verifica ("sì"), il contratto **paga automaticamente il risarcimento**. In caso contrario ("NO"), il contratto si chiude.

### **Rilevanza per i professionisti:**

Automatizzazione dei processi di incasso e liquidazione dei sinistri.

Impatti contabili immediati e certi al verificarsi dell'evento.

Nuovi modelli di consulenza per la valutazione del rischio automatizzato.



## **RWA Tokenization (Real-World Asset)**

La tokenizzazione trasforma i diritti su beni reali (immobili, beni mobili, opere d'arte, crediti) in token digitali su blockchain, gestiti da smart contract.

- **Come funziona:**

- Un bene del mondo reale (Real-World Asset) viene rappresentato legalmente da un token digitale.
- Lo smart contract ne gestisce l'emissione, il trasferimento e gli eventuali rendimenti in modo automatico e trasparente.

-  **Esempio:** Un immobile può essere frazionato in migliaia di token. Lo smart contract raccoglie gli affitti e li distribuisce automaticamente come dividendi ai possessori dei token, in proporzione alla loro quota. Lo smart contract può anche monitorare la regolarità del pagamento dei canoni e in caso di inadempimento inibire l'accesso al conduttore.

### **Rilevanza per i professionisti:**

Maggiore trasparenza nei flussi di capitale e nella proprietà degli asset.

Registrazioni contabili automatiche dei trasferimenti e dei rendimenti.

Consulenza fiscale e legale su nuove forme di investimento e gestione patrimoniale.

## **Compravendita di Beni Fisici con Escrow**

Per i beni fisici, uno smart contract può funzionare come una piattaforma di negoziazione digitale, con la funzione di escrow (deposito fiduciario) digitale, trattenendo il pagamento finché dopo il perfezionamento dell'acquisto un'azione nel mondo reale non viene confermata.

- **Come funziona:** Il processo automatizza le fasi chiave della vendita.
  - i. Il **venditore** pone il bene in vendita.
  - ii. L'**acquirente** paga il corrispettivo allo smart contract.
  - iii. Il contratto **verifica il pagamento**, registra il trasferimento del diritto di proprietà e **trasmette l'ordine di consegna** del bene.
  - iv. Il contratto **accredita il corrispettivo** al venditore, che lo incassa.

### **Rilevanza per i professionisti:**

Garanzia della corrispondenza tra flusso finanziario (pagamento) e flusso fisico (consegna).

Tracciabilità completa delle transazioni per audit e revisioni contabili.

Riduzione del rischio di controparte e delle relative controversie.

## Supply Chain e Tracciabilità

Gli smart contract garantiscono trasparenza e automazione lungo l'intera catena di fornitura.

- **Come funziona:**

- Ogni passaggio di un prodotto (dalla produzione alla consegna) viene registrato in modo immutabile su blockchain.
- Gli smart contract si attivano automaticamente per sbloccare pagamenti o emettere certificazioni quando un prodotto raggiunge una determinata fase.

-  **Esempio:** In una filiera agroalimentare, lo smart contract può rilasciare automaticamente il pagamento al contadino non appena il corriere registra la consegna della merce al magazzino, certificandone allo stesso tempo l'origine.

### **Rilevanza per i professionisti:**

Supporto per audit e certificazioni di sostenibilità (ESG).

Contabilizzazione automatica e in tempo reale delle transazioni di filiera.

Validazione di processi di tracciabilità come nuovo campo di consulenza.



## **Notarizzazione e Archiviazione Documentale**

La blockchain, tramite smart contract, può offrire un servizio di "notarizzazione" digitale per garantire data certa e integrità a qualsiasi documento.

- **Come funziona:**
  - Un documento viene caricato su un sistema che ne calcola l'impronta digitale (hash).
  - Questa impronta viene registrata in modo permanente sulla blockchain, associata a una marca temporale (timestamp) intrinseca nell'*altezza del blocco*.
  - Chiunque potrà verificare in futuro che quel documento esisteva in quella data e non è mai stato modificato.
-  **Esempio:** Registrare su blockchain l'hash di un bilancio d'esercizio o di un contratto per certificarne l'esistenza e l'immodificabilità a una data certa.

### **Rilevanza per i professionisti:**

Creazione di prove con data certa e valore legale opponibile in giudizio.  
Evoluzione verso libri contabili e registri aziendali digitali e immodificabili.  
Garanzia crittografica dell'integrità dei documenti per revisioni e certificazioni.

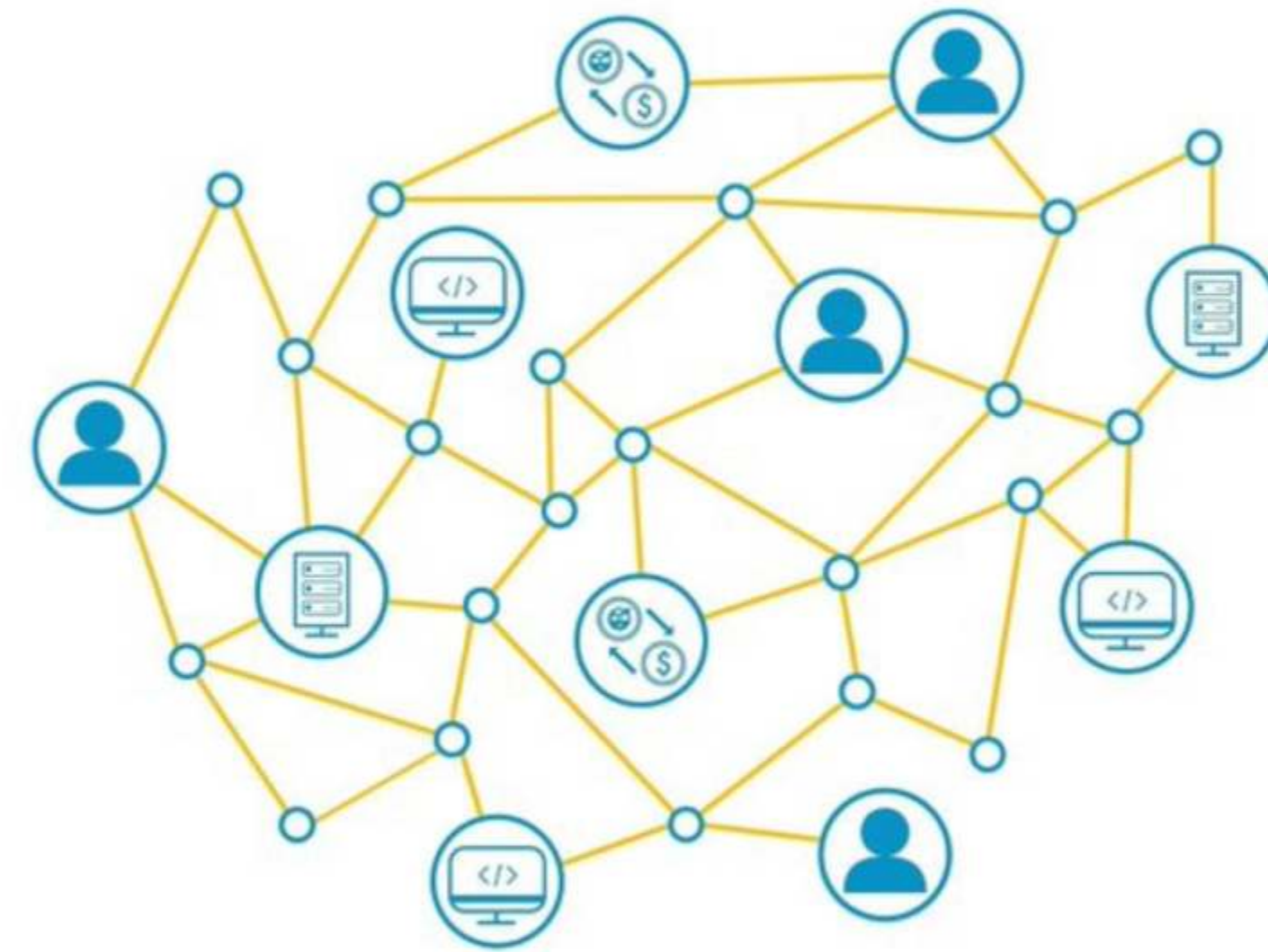
# Dalle Organizzazioni Tradizionali alle DAO

## Organizzazione Tradizionale Centralizzata



- Struttura gerarchica.
- Autorità decisionale al vertice.
- Le regole sono definite da statuti e policy interne.

## Decentralized Autonomous Organization (DAO)



- Struttura distribuita in una rete.
- Il potere decisionale è della community.
- Le regole sono scritte nel codice di uno smart contract.



## Organizzazioni Autonome Decentralizzate (DAO)

Una DAO è una modalità di organizzazione e collaborazione tra utenti gestita da smart contract, priva di un'entità centrale di controllo.

- **Come funziona:**

- Eredita dalla blockchain le proprietà di decentralizzazione, automazione e resistenza alla censura.
- Può simulare organizzazioni tradizionali come società o associazioni, o creare forme di collaborazione completamente nuove.
- Tutte le funzioni (raccolta capitali, proposte, modalità di voto) sono regolate dallo smart contract che ne costituisce l'ossatura.

-  **Esempio:** Un gruppo di investitori crea una DAO per gestire un fondo di venture capital. Le proposte di investimento vengono avanzate dai membri e votate dalla community. Se una proposta è approvata, lo smart contract esegue automaticamente l'investimento trasferendo i fondi.

### Rilevanza per i professionisti:

Nascita di nuove forme di governance societaria e diritto commerciale.  
Consulenza sulla strutturazione legale e fiscale di queste nuove entità collaborative.  
Revisione e audit degli smart contract che definiscono lo "statuto" digitale dell'organizzazione.



# Smart contracts

**Totalmente autoeseguibili**



**Es: trasferimento  
asset digitale**

**Con obbligazioni che richiedono  
cooperazione delle parti**



**Es: contratto fornitura  
bene fisico**

# **GLI SMART CONTRACT NELL'ORDINAMENTO**

# ORDINAMENTO

DL.135.2018

## Art. 8-ter Tecnologie basate su registri distribuiti e smart contract

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.



# smart contract

**programma per elaboratore**

la cui

**esecuzione**

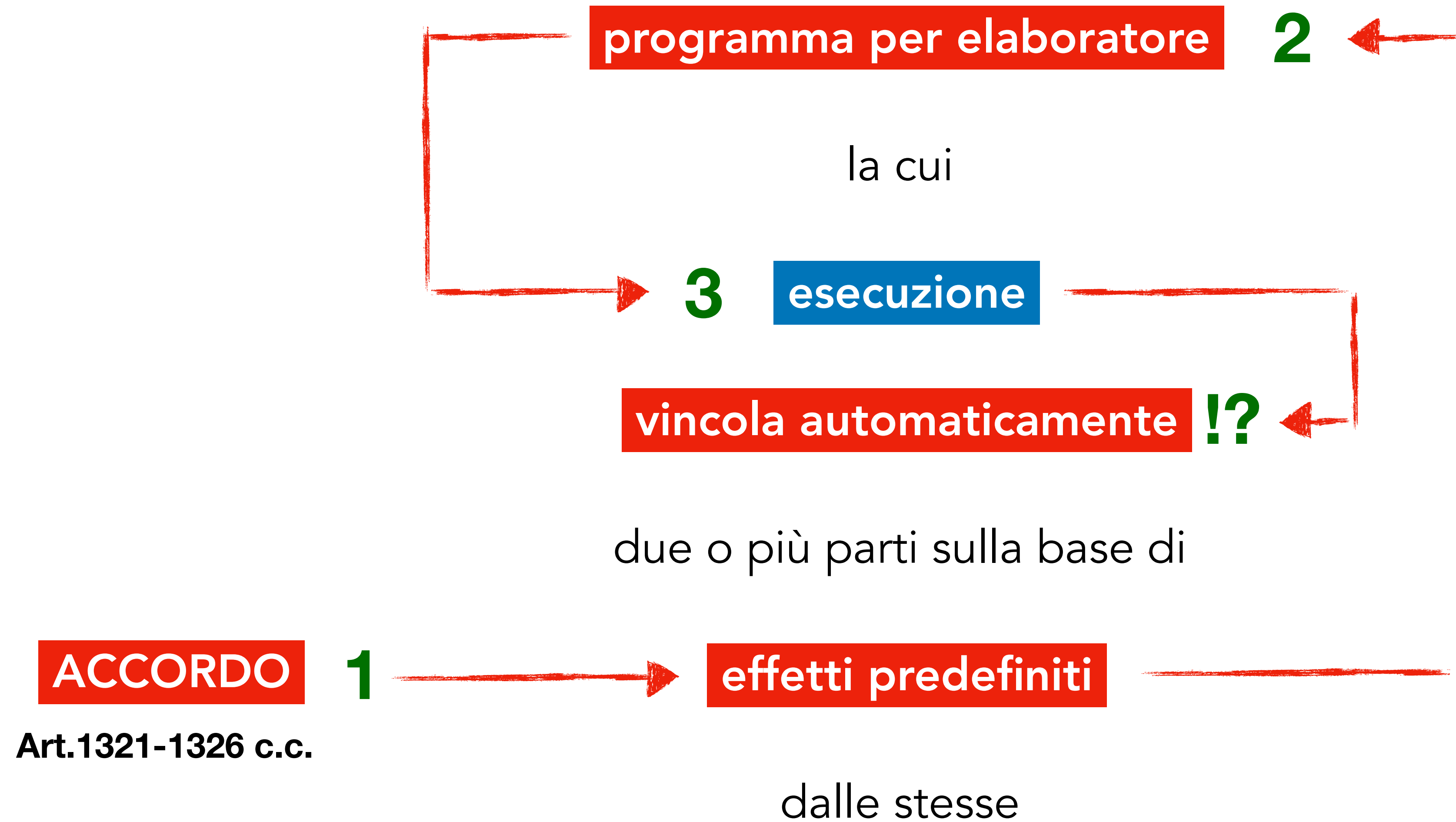
**vincola automaticamente**

due o più parti sulla base di

**effetti predefiniti**

dalle stesse

# smart contract



# smart contract

**VINCOLO AUTOMATICO**



**Totalmente autoeseguibili**

ogni clausola è codificata

la fase attuativa è automatizzata

non è richiesto l'intervento umano

non è ipotizzabile un inadempimento

non è possibile inibire il funzionamento



# ORDINAMENTO

DL.135.2018

## Art. 8-ter Tecnologie basate su registri distribuiti e smart contract

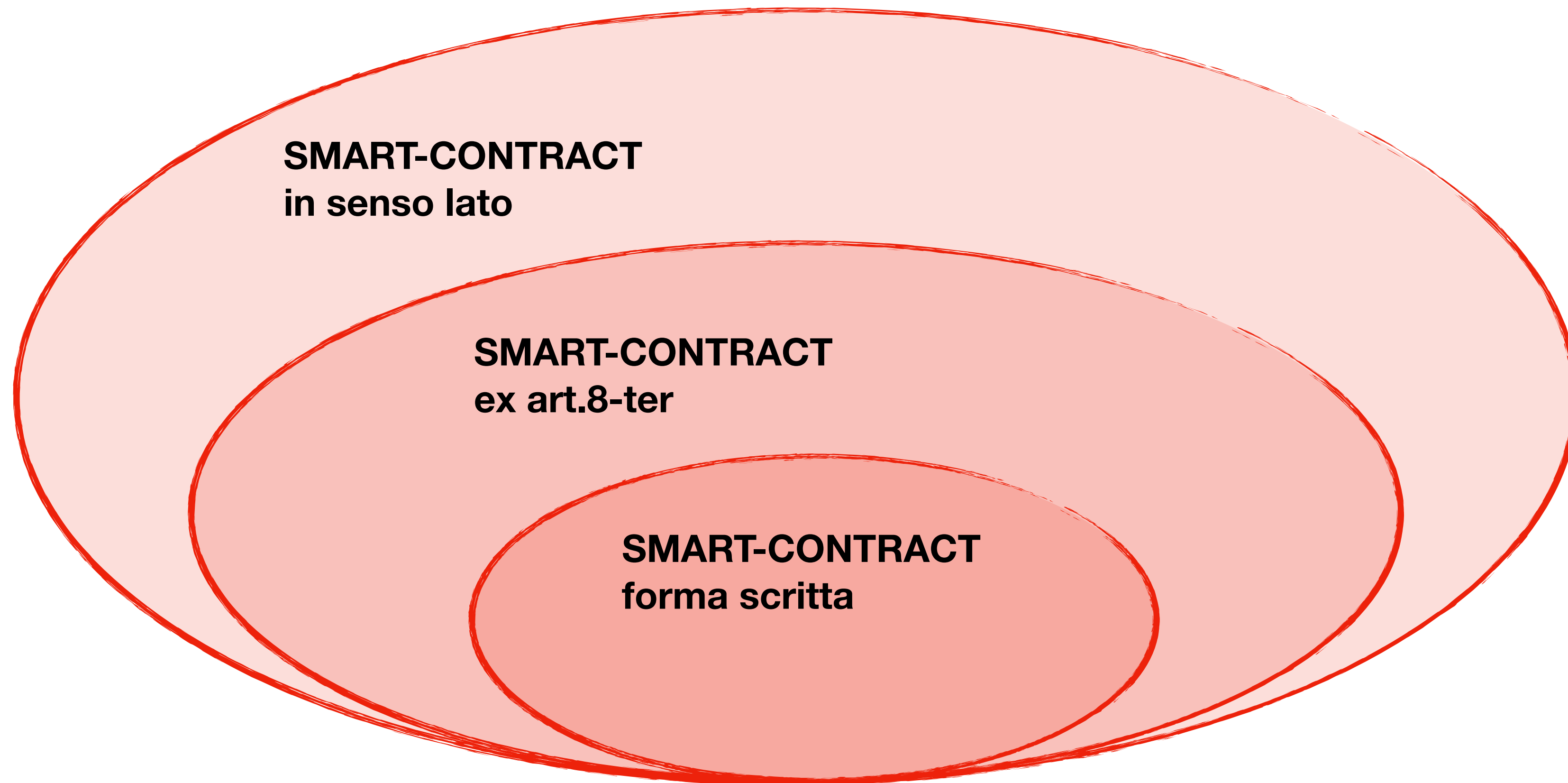
2. ... Gli smart contract soddisfano il requisito della **forma scritta** **previa identificazione informatica delle parti interessate**, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con **linee guida** da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.

# ORDINAMENTO

## **Art. 1350 CC - Atti che devono farsi per iscritto**

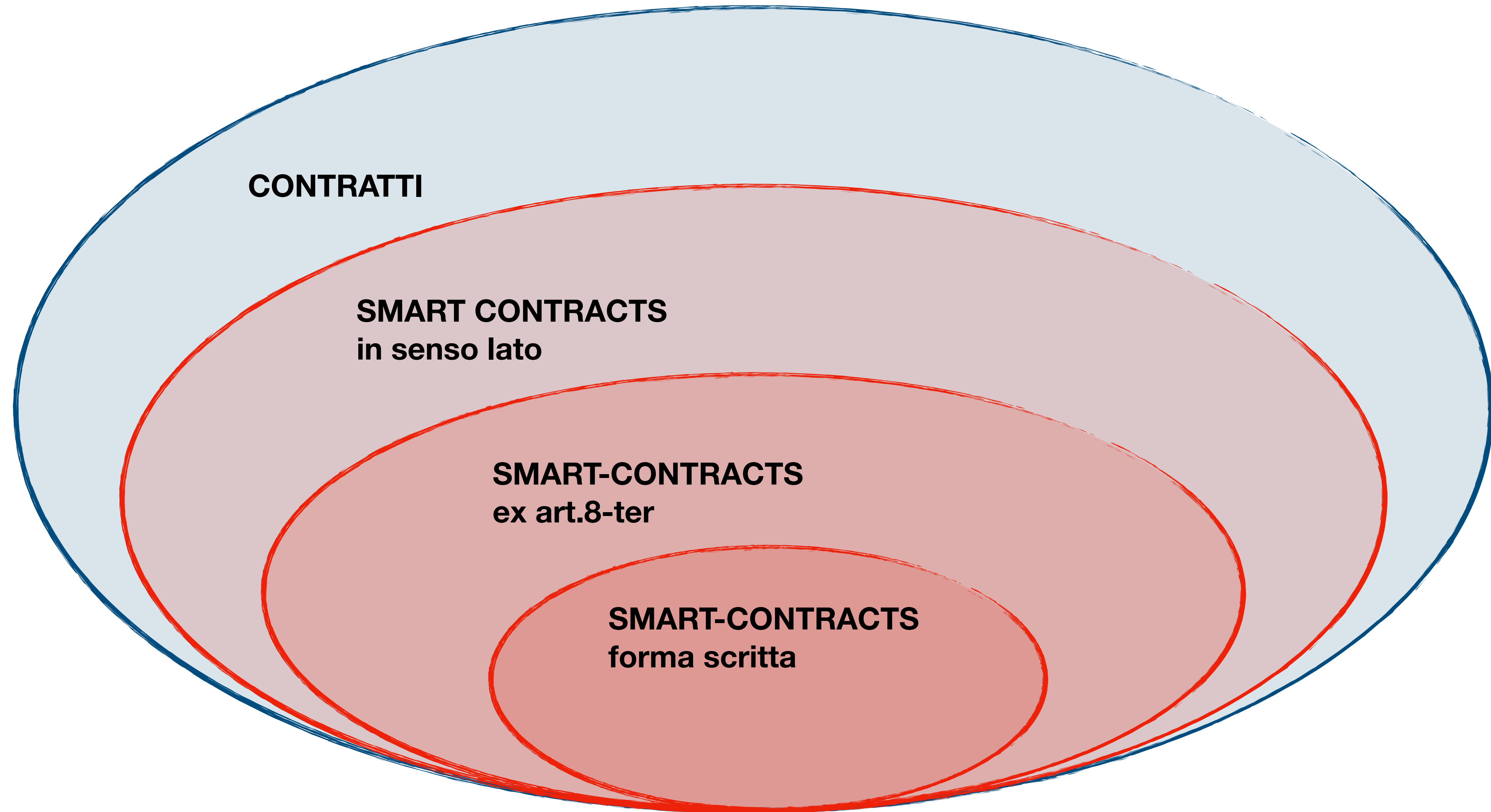
- 1) i contratti che trasferiscono la proprietà di beni immobili;
- 2) i contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili, il diritto di superficie, il diritto del concedente e dell'enfiteuta;
- 3) i contratti che costituiscono la comunione di diritti indicati dai numeri precedenti;
- 4) i contratti che costituiscono o modificano le servitù prediali, il diritto di uso su beni immobili e il diritto di abitazione;
- 5) gli atti di rinuncia ai diritti indicati dai numeri precedenti
- 6) i contratti di affrancazione del fondo enfiteutico;
- 7) i contratti di anticresi;
- 8) i contratti di locazione di beni immobili per una durata superiore a nove anni;
- 9) i contratti di società o di associazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo indeterminato;
- 10) gli atti che costituiscono rendite perpetue o vitalizie, salve le disposizioni relative alle rendite dello Stato;
- 11) gli atti di divisione di beni immobili e di altri diritti reali immobiliari;
- 12) le transazioni che hanno per oggetto controversie relative ai rapporti giuridici menzionati nei numeri precedenti;
- 13) gli altri atti specialmente indicati dalla legge.

# ORDINAMENTO





# ORDINAMENTO



## Data Act e Smart Contract

**Fonte:** Reg. (UE) 2023/2854, 13 dicembre 2023  
(*"Data Act"* – G.U. L 22.12.2023)

### ◆ **Articolo 30 – Smart Contract per la condivisione dei dati**

- Definizione: **programmi informatici utilizzati per l'esecuzione automatica di accordi di condivisione dei dati**
- Ambito: strumenti tecnici che automatizzano accesso, messa a disposizione e trasferimento dei dati (B2B / B2C)
- **Non tutti gli smart contract, ma solo quelli funzionali alla data economy**

### **Requisiti essenziali (art. 30, §3)**

1. **Robustezza** e possibilità di interruzione sicura
2. **Logging** e tracciabilità delle operazioni
3. Tutela di **dati personali** e **segreti commerciali**
4. Conformità a **standard tecnici europei** (CEN, CENELEC, ETSI)

# Ambito di applicazione del Data Act

## Oggetto

- Norme armonizzate sull'**accesso equo ai dati** e sul loro **utilizzo**

## Ambito materiale

- Prodotti e servizi connessi (IoT, cloud, piattaforme dati)
- Rapporti **B2B**, **B2C** e **enti pubblici**
- Interoperabilità e portabilità dei dati
- Smart contract come **strumenti di esecuzione automatica**

## Rilevanza giuridica

- Gli smart contract **non creano obbligazioni autonome**
- Sono strumenti per l'**esecuzione automatizzata di accordi di data sharing**
- Introducono **obblighi di progettazione sicura** → responsabilità tecnica
- Costituiscono il **primo riconoscimento normativo UE** degli smart contract



# Markets in Crypto-Assets (MiCA)

## Regolamento (UE) 2023/1114

**Adozione:** 31 maggio 2023

**Entrata in vigore:** 29 giugno 2023

**Applicazione parziale:** dal **30 giugno 2024** (per emittenti di *stablecoins*)

**Applicazione piena:** dal **30 dicembre 2024**

### Finalità

Regolamentare in modo unitario i **mercati delle crypto-attività** nell'Unione Europea, fornendo certezza giuridica a operatori e investitori.



## ✚ Rilevanza per gli *smart contracts*

- Il MiCA **non disciplina direttamente gli smart contracts**, ma riguarda gli **asset** che possono esservi rappresentati o trasferiti (*crypto-assets*).
- Gli smart contracts assumono rilievo **solo se automatizzano operazioni su token rientranti nel campo di applicazione del MiCA**.
- In tali casi, si applicano i principi di:
  - **trasparenza e responsabilità** dell'emittente,
  - **tracciabilità e sicurezza** del registro DLT,
  - **rispetto delle norme di tutela degli investitori e antiriciclaggio**.

💡 **In sintesi:** il MiCA **non vieta** né regola gli smart contracts in sé, ma **impone obblighi e cautele** quando essi gestiscono o scambiano cripto-attività regolamentate.

# DLT Pilot Regime

## Regolamento (UE) 2022/858 — *DLT Pilot Regime*

**Adozione:** 30 maggio 2022

**Entrata in vigore:** 23 marzo 2023

**Applicazione:** dal **23 marzo 2023** per una **durata iniziale di 6 anni**

### Finalità

Sperimentare, in un **ambiente regolamentato e controllato**, l'uso di **tecnologie di registro distribuito (DLT)** per la negoziazione e regolamento di strumenti finanziari "tokenizzati".



## ✚ Rilevanza per gli *smart contracts*

- Gli smart contracts sono **strumenti funzionali** alla gestione automatica di operazioni DLT (es. *clearing, settlement, delivery-versus-payment*).
- Il regime pilota consente di **testare in deroga** ad alcune regole MiFID e CSDR sistemi che impiegano smart contracts per:
  - esecuzione automatica delle transazioni,
  - gestione dei diritti sugli strumenti finanziari tokenizzati,
  - tracciabilità e trasparenza delle operazioni.

💡 **In sintesi:** il DLT Pilot Regime crea un **laboratorio normativo** dove gli *smart contracts* possono essere sperimentati **in contesto vigilato**, anticipando future integrazioni normative strutturali.

# CODE IS LAW

WAL IS CODE  
LAW IS CODE



# Smart contracts

spunti di approfondimento



## ⚙️ Approfondimenti tecnici — Smart Contract e piattaforme

### ◆ Ecosistemi di riferimento

- **Ethereum (EVM)**

Linguaggio *Solidity*, compilazione in *bytecode*, uso di *storage*, *stack* e *memory*.

👉 Documentazione: [ethereum.org/en/developers/docs](https://ethereum.org/en/developers/docs)

👉 *Ethereum EVM Illustrated* – Takenobu T.

- **Hyperledger Fabric**

Framework *permissioned* (Go/JavaScript), ideale per contesti aziendali e istituzionali.

👉 [hyperledger-fabric.readthedocs.io](https://hyperledger-fabric.readthedocs.io)

- **Polygon / Avalanche / Solana**

Soluzioni *scalable* compatibili con EVM o con VM proprietarie.

👉 [polygon.technology](https://polygon.technology)

👉 [avax.network](https://avax.network)

👉 [solana.com/developers](https://solana.com/developers)

## ◆ Aspetti implementativi

- **Ciclo di vita dello smart contract**
  - i. Redazione del codice
  - ii. Attestazione su blockchain (*deploy*)
  - iii. Accessibilità pubblica e immutabilità
  - iv. Esecuzione automatica
- **Concetti chiave**
  - *Bytecode, ABI, gas cost, oracoli esterni*
  - *Single point of failure* → importanza della decentralizzazione
  - *Audit e formal verification* per affidabilità del codice

## Approfondimenti normativi — Quadro nazionale e europeo

### Quadro nazionale

- **Riferimento normativo:** *art. 8-ter D.L. 135/2018*, conv. in *L. 12/2019* (cd. “Decreto Semplificazioni”)
- **Definizione legale:** lo *smart contract* è un programma per elaboratore che vincola automaticamente due o più parti su tecnologie basate su registri distribuiti.
- **Effetti giuridici:**
  - Gli *smart contract* soddisfano il requisito della **forma scritta** se le parti sono identificate informaticamente.
  - L'**AgID** definisce i requisiti tecnici di sicurezza e identificazione.
- **Rilevanza pratica:**
  - Digitalizzazione dell'accordo contrattuale
  - Garanzia di autenticità e tracciabilità
  - Coordinamento con le discipline europee (Data Act, DLT Pilot, AI Act)



## Quadro europeo

- **Regolamento (UE) 2023/2854 – “Data Act”**

Introduce la categoria di *smart contract per la condivisione dei dati*: programmi informatici che automatizzano l’accesso o la trasmissione di dati.

→ Requisiti: sicurezza, interruzione controllata, logging, tutela dei dati, interoperabilità.

- **Regolamento (UE) 2022/858 – “DLT Pilot Regime”**

Promuove l’uso di infrastrutture DLT nei mercati finanziari con obblighi di trasparenza e sicurezza.

- **AI Act (2024)**

Introduce principi di trasparenza e controllo umano per sistemi automatizzati.

- **European Blockchain Regulatory Sandbox**

Spazio di sperimentazione regolatoria con autorità e operatori.



# Dall'implementazione alla norma



## Relazione tecnica → giuridica

| Livello tecnico                                        | Livello giuridico                                                      |
|--------------------------------------------------------|------------------------------------------------------------------------|
| Codice <i>Solidity</i> , <i>bytecode</i> , logiche EVM | Riconoscimento legale dello “smart contract” come programma vincolante |
| Deploy su blockchain (Ethereum, Polygon, ecc.)         | Forma scritta e validità giuridica se identità digitale verificata     |
| Funzioni automatizzate e oracoli                       | Requisiti di sicurezza, logging e interruzione (Data Act, art. 30)     |
| Decentralizzazione e trasparenza                       | Responsabilità, tutela dei dati e interoperabilità                     |
| Audit e validazione del codice                         | Conformità agli standard tecnici e normativi UE                        |

## Sintesi

- L'infrastruttura tecnica determina **l'affidabilità e la validità operativa** dello smart contract.
- La normativa europea e nazionale stabilisce **requisiti di sicurezza, trasparenza e controllo**.
- L'obiettivo comune è un ecosistema in cui **codice e diritto** siano coerenti e verificabili.



# Smart contracts

contenuti aggiuntivi

# **SMART CONTRACT E STRUMENTI DI RISOLUZIONE DEI CONFLITTI**

# TUTELA GIURISDIZIONALE

**Totalmente autoeseguibili**

**La tutela giurisdizionale  
non può essere esclusa**

Tutela giudiziale ai  
fini dell'esecuzione del contratto



... ma per altri rimedi?

- nullità
- annullamento
- rescissione
- risoluzione per eccessiva onerosità



Rimedi  
restitutori

Inibizione del  
funzionamento  
del contratto



# TUTELA GIURISDIZIONALE

Con obbligazioni che richiedono  
cooperazione delle parti

**Tutela giurisdizionale  
identica a quelli degli  
altri contratti**

# Software o contratto?

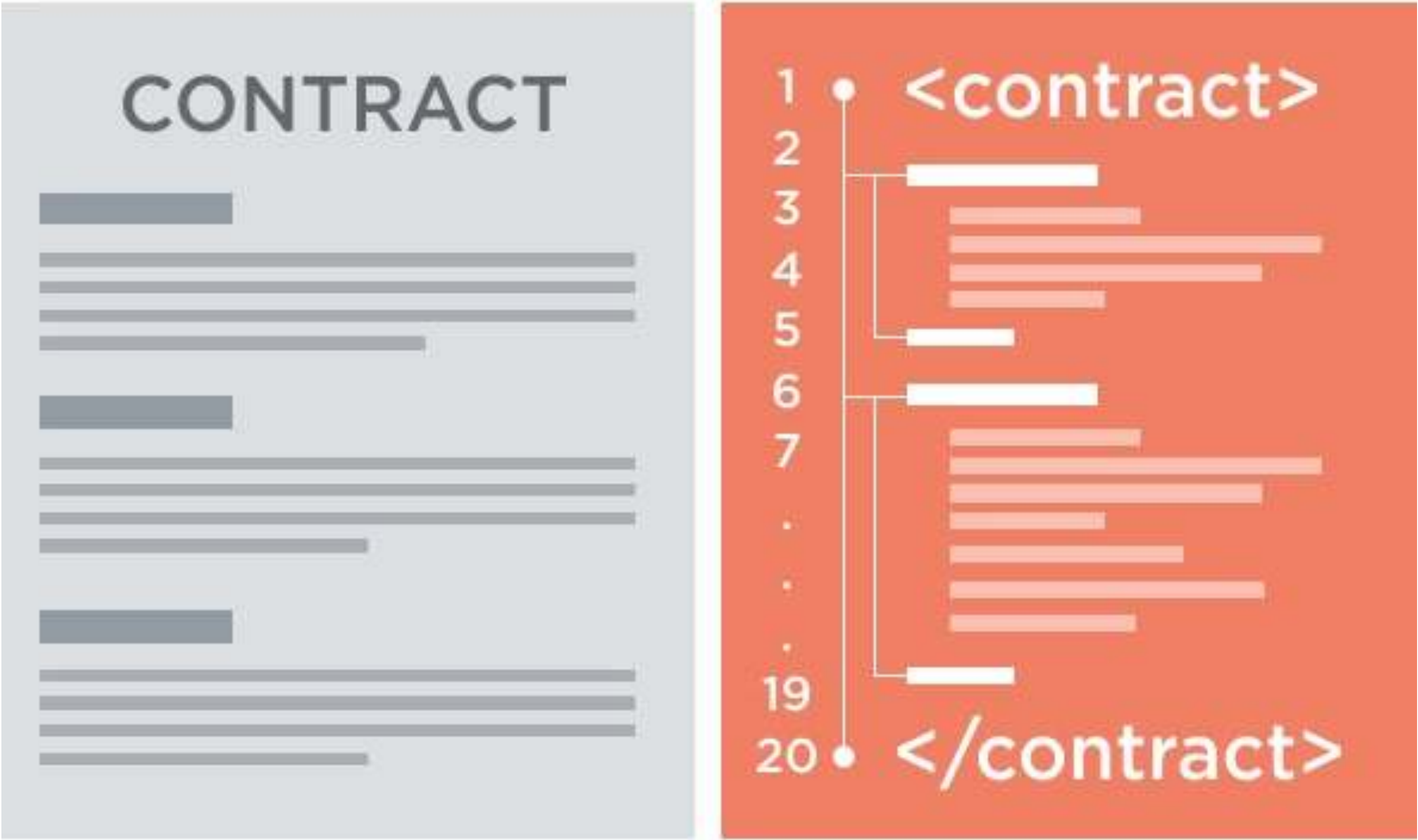


→ **ACCORDO**



**IDENTIFICAZIONE DELLE PARTI**  
**VALIDITÀ DEL CONSENSO**  
**DATI ESTERNI (ORACOLI)**  
**GIURISDIZIONE**  
**LEGGE APPLICABILE**

# Software o contratto?

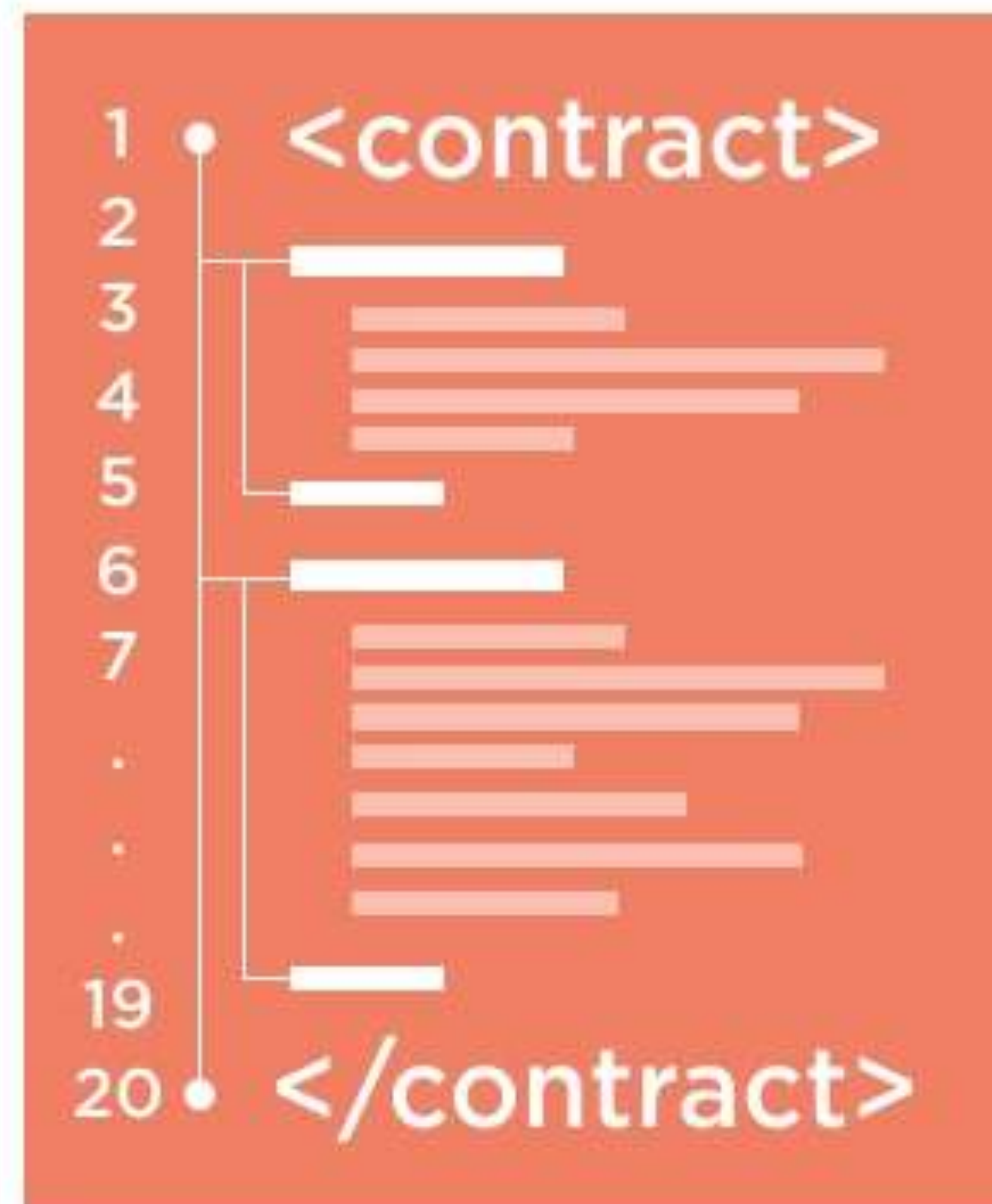




# SMART CONTRACT E ORDINAMENTO



GIUSTIZIA ORDINARIA



# SMART CONTRACT E ORDINAMENTO





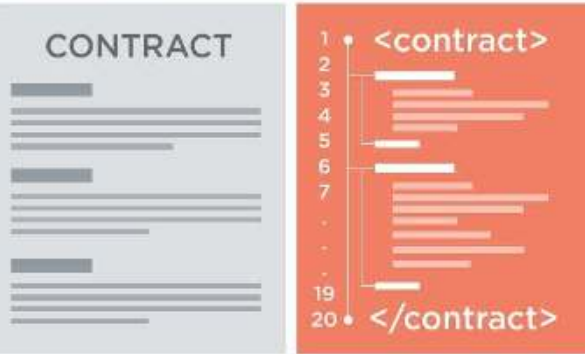
# PIATTAFORME ARBITRALI DATA DRIVEN



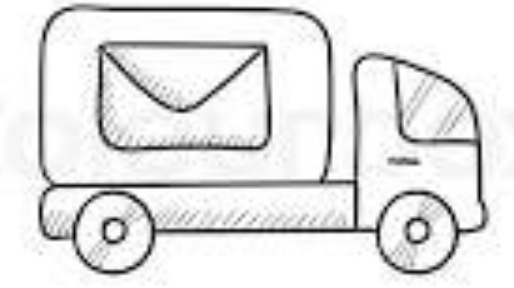
PIATTAFORME ARBITRALI  
DATA DRIVEN



# PIATTAFORME ARBITRALI DATA DRIVEN



Stipula



Consegna



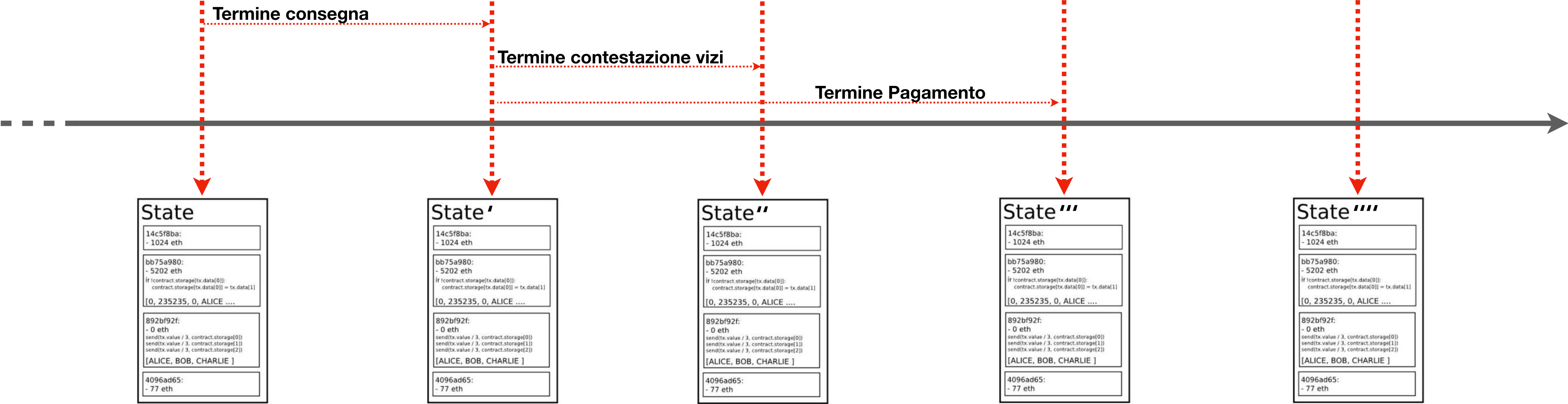
Contestazione vizi

€ ?!

Termine pagamento



Controversia





# PIATTAFORME ARBITRALI DATA DRIVEN

## Blockchain

### Smart contract

Istruzioni codice  
bytecode

```
{
  "linkReferences": {},
  "object":
    "6060604052341561000f57600080fd5b6101f4600080018190555060fa60006001018190555060af806
    100336000396000f300606060405260043610603f576000357c0100000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
    00080fd5b60546071565b604051808381526020018281526020019250505060405180910390f35b600
    080600001549080600101549050825600a165627a7a7230582024ce11ac4dcbeb5d40e8b0963371e19
    9b42898822cca440f38285dc3b85fda2b0029",
  "opcodes": "PUSH1 0x60 PUSH1 0x40 MSTORE CALLVALUE ISZERO PUSH2 0xf JUMPI
    PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH2 0x1f4 PUSH1 0x0 DUP1 ADD DUP2 SWAP1
    SSTORE POP PUSH1 0xfa PUSH1 0x0 PUSH1 0x1 ADD DUP2 SWAP1 SSTORE POP PUSH1 0xaf
    DUP1 PUSH2 0x33 PUSH1 0x0 CODECOPY PUSH1 0x0 RETURN STOP PUSH1 0x60 PUSH1 0x40
    MSTORE PUSH1 0x4 CALLDATASIZE LT PUSH1 0x3f JUMPI PUSH1 0x0 CALLDATALOAD PUSH29
    0x10000000000000000000000000000000000000000000000000000000000000000000000000000000000000
    0x0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
    0xffffffff AND DUP1 PUSH4 0xb880b69a EQ PUSH1 0x44 JUMPI JUMPDEST PUSH1 0x0 DUP1
    REVERT JUMPDEST CALLVALUE ISZERO PUSH1 0x4e JUMPI PUSH1 0x0 DUP1 REVERT
    JUMPDEST PUSH1 0x54 PUSH1 0x71 JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP4 DUP2
    MSTORE PUSH1 0x20 ADD DUP3 DUP2 MSTORE PUSH1 0x20 ADD SWAP3 POP POP POP PUSH1
    0x40 MLOAD DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH1 0x0 DUP1 PUSH1 0x0 ADD
    SLOAD SWAP1 DUP1 PUSH1 0x1 ADD SLOAD SWAP1 POP DUP3 JUMP STOP LOG1 PUSH6
    0x627a7a723058 KECCAK256 0x24 0xce 0xac 0x4d 0xcb 0xeb 0x5d BLOCKHASH 0xe8 0xb0
    SWAP7 CALLER PUSH18 0xe199b42898822cca440f38285dc3b85fda2b STOP 0x29 ",
  "sourceMap": "26:184:0-;;;127:81;;;;;;;;;173:3;154:8;;16;;;22;;;;;201:3;180:8;;18;;;24;;;;;26:184;;;;;"
}
```

### Storage

Stipula

Consegna

Contestazione

Pagamento

## ARBITRO



## ATTORE

CONTRADDITTORIO

## CONVENUTO

# PIATTAFORME ARBITRALI DATA DRIVEN

**ARBITRATO RITUALE**



**DEPOSITO ed  
ESECUTIVITÀ DEL  
LODO  
ART. 825 CPC**

## c.p.c. art. 825. Deposito del lodo

La parte che intende fare eseguire il lodo nel territorio della Repubblica ne propone istanza depositando il lodo in originale, o in copia conforme, **insieme con l'atto contenente la convenzione di arbitrato**, in originale o in copia conforme, nella cancelleria del tribunale nel cui circondario è la sede dell'arbitrato. Il tribunale, accertata la regolarità formale del lodo, lo dichiara esecutivo con decreto. Il lodo reso esecutivo è soggetto a trascrizione o annotazione, in tutti i casi nei quali sarebbe soggetta a trascrizione o annotazione la sentenza avente il medesimo contenuto.

...

# PIATTAFORME ARBITRALI DATA DRIVEN

**PROCEDURA DETTAGLIATA o  
ARBITRATO AMMINISTRATO**



**ART. 816 bis / ART. 832 CPC**

**CONTRADDITTORIO**

**c.p.c. art. 816-bis. Svolgimento del procedimento.**

Le parti possono stabilire nella convenzione d'arbitrato, o con atto scritto separato, purché anteriore all'inizio del giudizio arbitrale, le norme che gli arbitri debbono osservare nel procedimento e la lingua dell'arbitrato. In mancanza di tali norme gli arbitri hanno facoltà di regolare lo svolgimento del giudizio e determinare la lingua dell'arbitrato nel modo che ritengono più opportuno. Essi debbono in ogni caso attuare il principio del contraddittorio, concedendo alle parti ragionevoli ed equivalenti possibilità di difesa.

...



# PIATTAFORME ARBITRALI DATA DRIVEN

**CONVENZIONI PROBATORIE**



**ART. 2698 CC**

c.c. art. 2698. Patti relativi all'onere della prova.

Sono nulli i patti con i quali è invertito ovvero è **modificato l'onere della prova**, quando si tratta di **diritti di cui le parti non possono disporre** o quando l'inversione o la modificazione ha per effetto di rendere a una delle parti **eccessivamente difficile l'esercizio del diritto**.

**MEZZI DI PROVA** ..... **DATI RACCOLTI DALLO SMART CONTRACT**

# Smart contracts