



Scan me



# Ethereum Blockchain Talk

07 Giugno 2019 @ Sapienza Università di Roma



Lorenzo Zaccagnini  
Founder @Devoleum



Elisa Romondia  
Founder @Devoleum

# Lorenzo Zaccagnini



- Sviluppatore ed insegnante Blockchain & AI
- Laureato in Psicologia alla Sapienza
- Borse di studio in Blockchain & AI da Facebook, Google, Udacity e ConsenSys
- Blockchain Mentor di Udacity, top company della Silicon Valley che si occupa di formare professionisti nell'ambito delle nuove tecnologie
- Co-founder di Devoleum. Una soluzione Blockchain & AI per la tracciabilità e l'ottimizzazione delle filiere agroalimentari, riconosciuta a livello internazionale (Forbes, Business Insider, Le Figaro)

# Elisa Romondia



- Sviluppatrice ed insegnante Data Analysis & AI
- Laureata in Psicologia alla Sapienza
- Borse di studio in Data Science & Blockchain da Facebook, Google, Udacity e ConsenSys
- Data Analyst Mentor di Udacity, top company della Silicon Valley
- Co-founder di Devoleum. Premiata come:
  - Forbes 60 Women-Led Startups That Are Shaking Up Tech Across The Globe
  - Top50 donne italiane più influenti by InspiringFifty Italia 2018
  - Top10 imprenditrici innovative d'Europa by StartHer @Station F

# Devoleum

Utilizza **Ethereum blockchain** ed **Intelligenza artificiale** per **tracciare ed ottimizzare le filiere agroalimentari**, riconosciuto a livello internazionale. Principali feature:



- Aperto al pubblico, chiunque può provare la simulazione sul nostro sito
- Utilizza **zero proof knowledge (zksnark)**, **oracoli** ed **IPFS** per garantire confidenzialità e compatibilità con il **GDPR**
- Equilibrio tra dati confidenziali delle aziende e trasparenza per i consumatori
- Integra blockchain ed AI per la correttezza dei dati
- Ha un visione a lungo termine sull'automatizzazione e la creazione di filiere sostenibili dal punto di vista economico ed ecologico. Focalizzato sul rispetto della salute psicofisica dei lavoratori ed il riconoscimento dei loro diritti, combattendo in prima linea caporalato e agromafie.

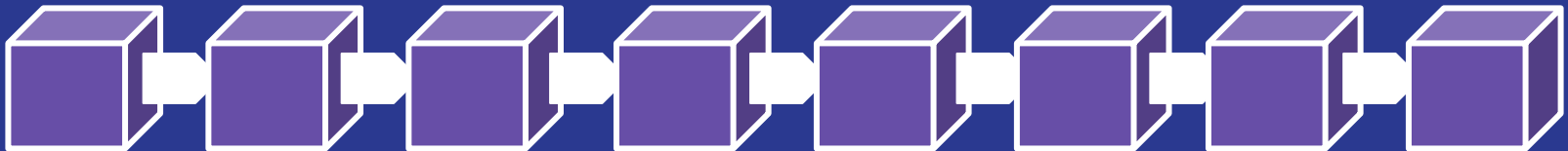
# Introduzione

---

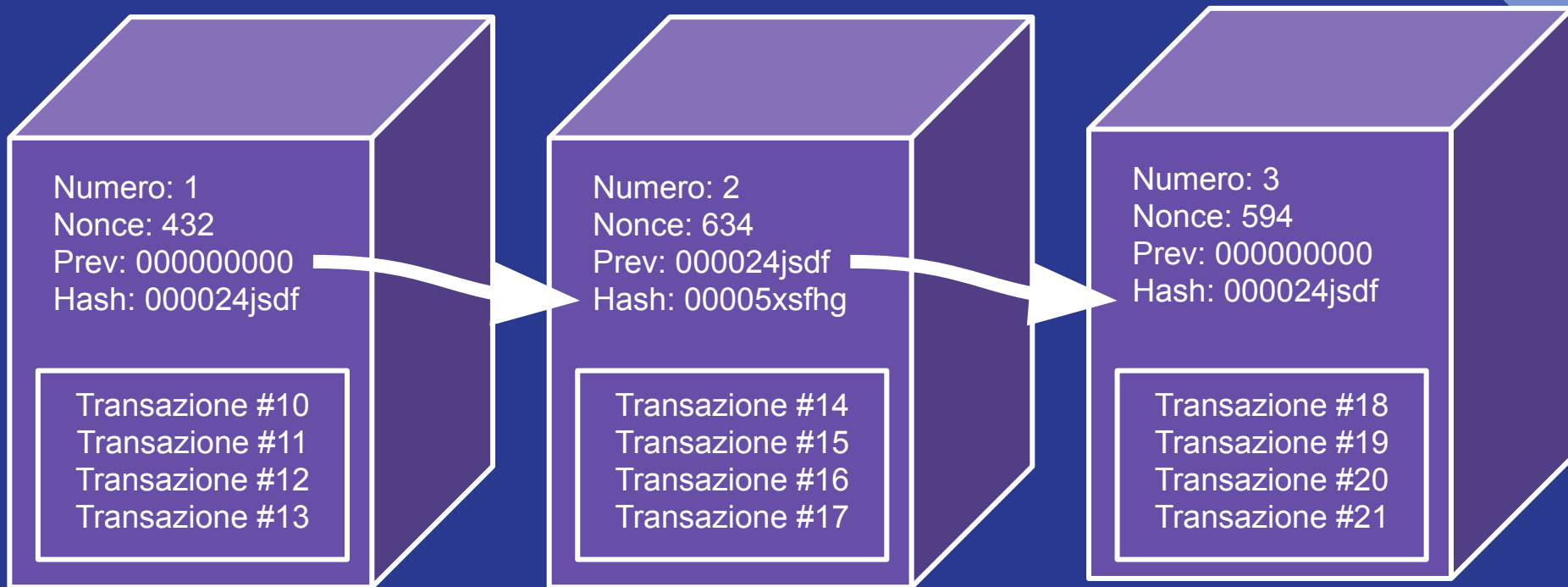
Cos'è Ethereum Blockchain e cos'è uno Smart Contract

# Cos'è una Blockchain

La **Blockchain** è conosciuta per la sua **immutabilità**, una serie di dati vengono criptati ed incapsulati dentro ad un blocco (*block*), l'integrità di ogni blocco è assicurata da una **firma digitale** generata dal suo contenuto (*transazioni*) e da informazioni prese dal blocco precedente, di conseguenza *ogni blocco creato è concatenato a quello precedente (chain)*, ogni dato inserito diventa immutabile e nel caso venissero modificati dei dati in un blocco non ci sarebbe più corrispondenza con il blocco successivo, garantendo la piena **tracciabilità** e **trasparenza** di ogni dato presente nella Blockchain.



# Cosa c'è dentro un blocco

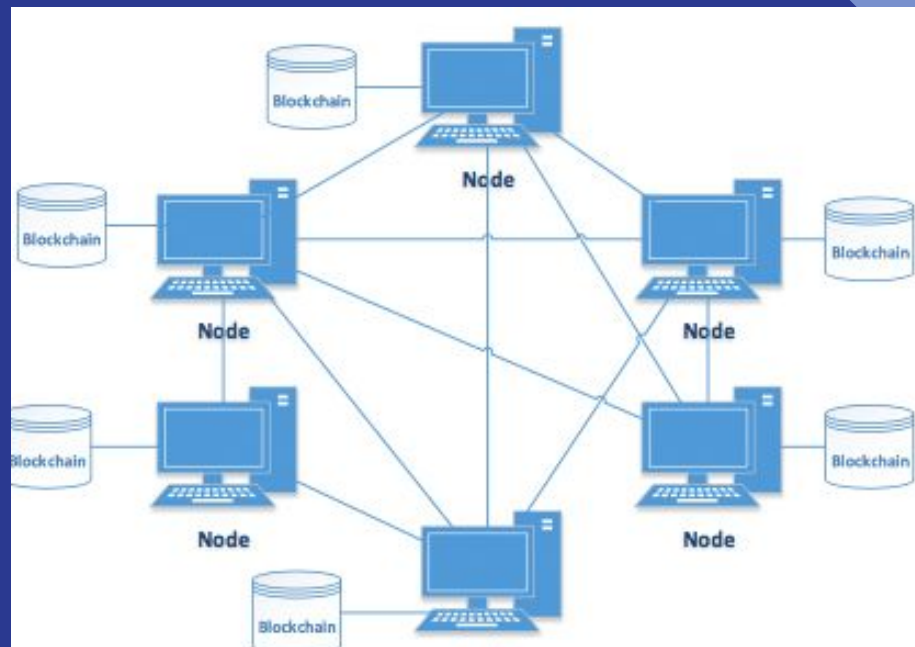


# La rete decentralizzata di Ethereum

## Ethereum blockchain

è composta da più nodi.

Ogni macchina connessa alla blockchain contiene una copia esatta di tutti i blocchi, dal primo all'ultimo creato, quindi **tutti hanno l'esatta replica dell'intera blockchain aggiornata.**





# Cos'è uno Smart Contract

**Ethereum blockchain** è caratterizzata dalla possibilità di creare **Smart Contract (SC)**. Gli SM sono dei **contratti digitali** che gli sviluppatori possono programmare e pubblicare sulla rete di Ethereum. Uno SC, dopo la pubblicazione, non può più essere modificato ed il suo codice resta immutabile, garantendo sicurezza nella sua esecuzione e sui risultati da esso prodotti.

- Questa **immutabilità** apre molti scenari sull'utilizzo degli SC per rendere più trasparenti e sicuri **accordi tra aziende e privati**, specialmente nel caso delle filiere.
- Ogni operazione di scrittura richiede un costo in criptovaluta per evitare loop infiniti e congestionare così la rete.

# Utenti e anonimato

Su Ethereum abbiamo due tipi di account

- ▶ **Externally owned accounts** (controllati dalle persone)
- ▶ **Contract accounts** (controllati dagli smart contract)

**Es: 0x1e9e5c65b98f74406bca2c14c706b4d8f3c68e1**

Entrambi hanno un **bilancio pubblico** e sono **identificati da un codice alfanumerico** (address) che non rivela nulla circa la vera identità del proprietario. Utile per proteggere da censura e persecuzioni ma apre altre problematiche riguardo attività illecite. Per immettere dati su Ethereum pubblica è necessario acquistare **ETH** registrandosi con un documento d'identità presso un exchange.

# Questioni aperte

Una struttura decentralizzata e distribuita come quella di Ethereum Blockchain, dove tutti hanno l'esatta copia dei dati, dal primo all'ultimo blocco, lascia aperte diverse questioni di tipo legale.

*I dati inseriti non si possono cancellare, in caso di immissione di **dati illeciti** (es. materiale pedopornografico), **dati sensibili** o ancora, **dati protetti da copyright**, chi è responsabile e come possiamo proteggere le vittime di queste azioni?*



# **Blockchain e Giurisprudenza**

## **Nuovi orizzonti professionali**

# La nostra esperienza

Con Devoleum, cerchiamo di conciliare aspetti legali e tecnologici per creare un progetto concretamente realizzabile e compatibile con le norme giuridiche riguardo il trattamento dei dati. Per gestire queste problematiche c'è bisogno di una o più **figure professionali con queste competenze**:

- Conoscenza di Ethereum Blockchain
- Diritto digitale
- Presenza online curata ed aggiornata (LinkedIn e pubblicazione articoli su piattaforme come Medium)
- Lingua inglese
- Utilizzo di strumenti per il remote working (Slack, Google Drive, GitHub, Skype, etc.)
- Attivismo e visione a lungo termine su tematiche inerenti la società e l'innovazione tecnologica

# Facebook

Anche Facebook ha recentemente data notizia di sé cercando una figura professionale che unisca competenze inerenti la giurisprudenza e le blockchain

facebook careers

[Jobs](#)

[Areas of Work](#)

[Locations](#)

[Students & Grads](#)

[Facebook Life](#)

[Blog](#)



## MINIMUM QUALIFICATIONS

- ✓ J.D. degree (or foreign equivalent) and membership in at least one U.S. state bar
- ✓ 5+ years of legal experience, including 4+ years working at or for technology companies (either in-house and/or at a law firm)
- ✓ Experience leading contract negotiations
- ✓ Experience advising clients on and managing deals on deadlines with minimal supervision
- ✓ Experience building relationships and collaborating with business teams and other members of the legal team (regulatory, product, privacy, etc.) to ensure business needs are met

## PREFERRED QUALIFICATIONS

- ✓ Experience with blockchain and with the legal issues arising from blockchain applications

# Un dibattito che richiede professionisti

La crescente popolarità delle blockchain sta portando sempre più al centro dell'attenzione gli **aspetti legali** legati alla loro applicazione. Questo ha fatto sì che la figura del **giurista** sia diventata centrale per qualunque progetto che si occupi di questa tecnologia nonché per la **regolamentazione del suo utilizzo**. Specialmente nel caso in cui ci sia lo scambio di **asset tokenizzati** o **dati sensibili**.

## Maryland Creates New Law To Allow Blockchain Record Keeping by Corporations

Posted by Justin Szilard | May 6, 2019 | News | ★★★★★



## Another push for Colorado blockchain law has more than token support

How a failed bill led to a collaboration between local politicians, state regulators and blockchain startups to figure out whether Colorado even needs any new laws

JAN 4, 2019 5:00AM MDT

BUSINESS



Tamara Chuang @gadgetress

[f](#) [t](#) [r](#) [v](#) [w](#) [More](#)

The Colorado Sun — [tamara@coloradosun.com](mailto:tamara@coloradosun.com)

Tech+Business+Economy

[See more](#)

# Gestire grandi flussi dati in sicurezza su Ethereum blockchain

---

Oracoli ed intelligenza artificiale




# Aspetti fondamentali

Un progetto su blockchain per essere utilizzabile deve garantire:

- **Interoperatività:** la connettività con dati ed oggetti all'esterno della blockchain, stabilendo l'autenticità dell'interlocutore
- **Confidenzialità:** possibilità di gestire informazioni confidenziali
- **Scalabilità:** possibilità di gestire dati di diverse dimensioni
- **Correttezza dei dati:** verificare le informazioni con un determinato grado di accuratezza

Attualmente nessuna di queste cose può essere fatta totalmente all'interno della blockchain (Ethereum) in maniera efficiente.



**Un' applicazione concreta della  
blockchain richiede l'uso di  
strumenti esterni**

# Interoperatività | Oracoli

## Il problema

Gli **smart contract** di base **non possono connettersi all'esterno** ma per funzionare hanno bisogno di dati, molte volte questi dati risiedono all'esterno della blockchain, come può capitare per lo stato di una spedizione oppure un tasso di cambio.

## La soluzione

Gli **oracoli** sono degli **agenti che trovano e verificano eventi all'esterno oppure all'interno della blockchain**, permettendo agli smart contract di agire ed interagire con il mondo all'esterno della blockchain.

# Differenti tipi di oracoli

**Software Oracles:** Gestiscono le informazioni disponibili online, come i servizi web (API) delle società. Questi oracoli estraggono le informazioni necessarie e le inseriscono negli smart contract.

**Hardware Oracles:** Alcuni smart contract necessitano di informazioni direttamente dal mondo fisico, ad esempio le scansioni RFID nelle filiere.

**Inbound Oracles:** Il caso d'uso di esempio di questi sarà un ordine di acquisto automatico se l'USD raggiunge un determinato prezzo.

**Outbound Oracles:** Questi oracoli danno la possibilità agli smart contract di interagire con il mondo esterno, sbloccare una macchina di un servizio di Car sharing quando le condizioni dello smart contract sono soddisfatte.

**Consensus Based Oracles:** I prediction market come Augur e Gnosis si basano molto su oracoli per confermare i risultati futuri. L'utilizzo di una sola fonte di informazioni potrebbe essere inaffidabile. Per avere maggiore sicurezza, è possibile utilizzare una combinazione di diversi oracoli, dove per esempio 3 oracoli su 5 potrebbero determinare il risultato di un evento.

## Blockchain

## Off-Chain



1. Il nostro SC fa una richiesta allo SC dell'Oracolo, la quale viene accettata
2. Una componente esterna alla Blockchain ascolta questo evento, ed invia i dati allo SC dell'Oracolo
3. I dati vengono inviati al nostro SC dallo SC dell'Oracolo

\* SC = Smart Contract

# Confidenzialità

## Il problema

Regolamentazioni come il **GDPR**, mettono serio rischio l'applicazione concreta della blockchain in qualsiasi ambito. Nasce la necessità di avere differenti gradi di confidenzialità e rivelare informazioni solo al momento ed all'interlocutore opportuno, per proteggere i propri clienti e la propria azienda. Immettere all'interno di Ethereum dati confidenziali è rischioso, data la sua natura aperta e decentralizzata, entrando in conflitto specialmente con l'art 17 del GDPR "right to be forgotten"

## La soluzione

**Zero Proof Knowledge**, la possibilità di dimostrare di conoscere un segreto senza rivelarlo. Concetto sviluppato da Silvio Micali ed applicato da Alessandro Chiesa su Zcash (zksnark).

**DATI DELLA FILIERA**

**EMETTE  
CERTIFICATO  
OFF-CHAIN**

## **Blockchain**

**CONTRATTO  
UTENTE**

**SUCCESSO**

**CONTRATTO  
VERIFICATORE**

1. L'operatore o device della filiera emette un certificato per un asset
2. SC verifica il certificato senza l'immissione di dati confidenziali
3. Viene registrato il successo ed abilita la richiesta (es: emissione token)

# Scalabilità

## Il problema

Immettere dati su Ethereum è molto costoso, se parliamo di blockchain pubblica. Fare un servizio di video streaming, immagazzinare foto oppure documenti all'interno della blockchain è proibitivo da un punto di vista economico e legale per via della GDPR.

## La soluzione

Immettendo nella blockchain solamente una referenza anonima, è possibile utilizzare server centralizzati oppure altri servizi decentralizzati, i quali non sono delle blockchain perché hanno una struttura ed un funzionamento differente.



# Scalabilità | Scenario attuale



IPFS <https://ipfs.io/>

Permette di immagazzinare file anche di grosse dimensioni in maniera decentralizzata. Ogni volta che viene immesso un file in IPFS viene prodotta una firma digitale, la quale va a formare un link che può essere inserito come riferimento all'interno dello smart contract.

La firma all'interno dello smart contract è un insieme casuale di caratteri, quindi non fornisce nessun indizio sul file a cui fa riferimento, in caso di modifica del file la firma cambia totalmente e può essere comparata con quella all'interno dello smart contract per rilevare eventuali manipolazioni.

**Server centralizzato:** Garantisce confidenzialità e compatibilità con il GDPR, cancellare il file all'esterno della blockchain garantendo il diritto all'oblio immettendo all'interno della blockchain una referenza anonima (hash).

## Blockchain

## IPFS

CONTRATTO UTENTE

LINK IPFS FILE:

**QmNi1ZhT4bw73rjrSwLUE6Ep38QMyKznhVewAMAUF5zsDD**

**Spedizione.PDF**

Il link è

<https://ipfs.io/ipfs/QmNi1ZhT4bw73rjrSwLUE6Ep38QMyKznhVewAMAUF5zsDD>

La firma è:

[QmNi1ZhT4bw73rjrSwLUE6Ep38QMyKznhVewAMAUF5zsDD](https://ipfs.io/ipfs/QmNi1ZhT4bw73rjrSwLUE6Ep38QMyKznhVewAMAUF5zsDD)

# Correttezza

## Il problema

Immettere dati errati su Ethereum blockchain può portare ad una catena disastri, essendo immutabili il danno è quasi irreparabile.

## La soluzione

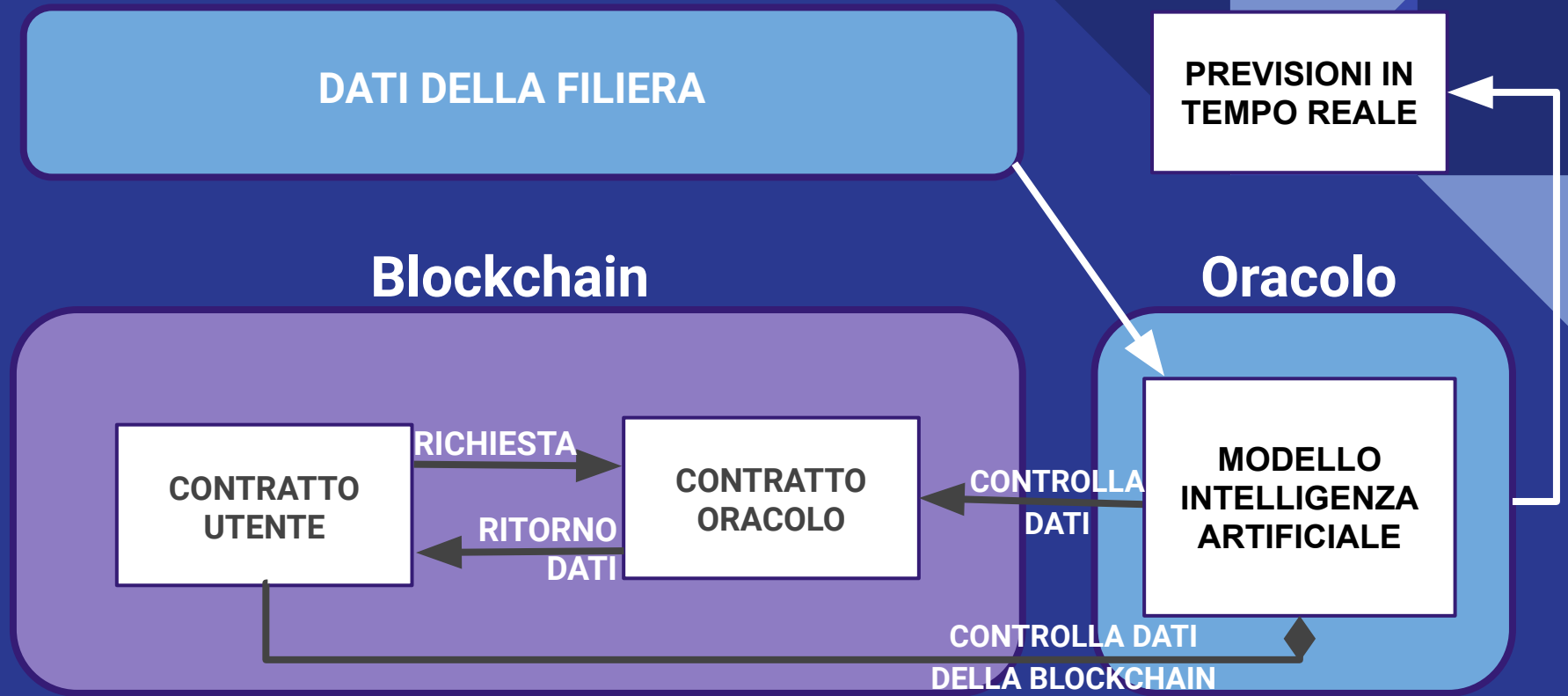
La relazione tra intelligenza artificiale e smart contract è di mutuo beneficio, l'intelligenza artificiale ha bisogno di dati per creare ed allenare modelli efficienti ed accurati, gli smart contract allo stesso modo hanno bisogno di dati per operare decisioni. utilizzando l'insieme avremmo dati sempre più accurati all'interno della blockchain, modelli di intelligenza artificiale sempre migliori e viceversa.

# Correttezza | Scenario attuale

## Oracoli

Attualmente il metodo più efficiente per integrare l'intelligenza artificiale con Ethereum blockchain è quella di utilizzare gli oracoli. Le iterazioni necessarie per modellare una intelligenza artificiale richiedono attualmente troppe risorse per essere inseriti direttamente all'interno della blockchain. Utilizzando l'AI all'interno degli oracoli, possiamo analizzare i dati in entrata per la correttezza, in uscita per fare previsioni in tempo reale su dati autentici ed accurati, senza andare a pesare sulla blockchain.

- Combinando tutti gli aspetti precedenti, confidenzialità, interoperabilità, scalabilità ed in questo caso la correttezza, possiamo esprimere il massimo potenziale delle due tecnologie più promettenti attualmente, intelligenza artificiale e blockchain.



1. L'operatore o device della filiera tenta di immettere dati nella blockchain
2. L'oracolo contenente l'AI controlla i dati, se corretti vengono immessi
3. I dati della blockchain possono essere usati per previsioni in tempo reale



# Blockchain e Giurisprudenza

## Casi di utilizzo

# OpenLaw, a free legal repository

Progetto ideato da un docente di legge, Aaron Wright e da David Roon, consente di modellare tutti o parte degli accordi legali utilizzando il codice (Smart Contract), riducendo il costo ed i rischi della creazione e della protezione di accordi giuridici vincolanti.

La loro soluzione consente di superare agilmente il gap di competenze necessarie per la creazione di questi contratti dinamici e intelligenti in un modo che sia applicabile e comprensibile ad un professionista legale.

<https://www.openlaw.io/>



## OPENLAW PROTOCOL

OpenLaw is building the following technology stack to help power next generation smart legal agreements.

AI Assembly / Chatbots / Legal Analytics

Decentralized Storage / Execution  
(Blockchain, IPFS)

Legal markup

Legal scripting

Legal markdown

# Agrello, a digital ecosystem

Progetto ideato in Estonia da un poll di esperti del tech e della giurisprudenza.

Utilizza Ethereum Blockchain e IPFS per la creazione e la verifica di documenti digitali. Le operazioni sono garantite dalla creazione di un'identità digitale su Blockchain supportata da documenti governativi (es. passaporto).

<https://www.agrello.io/>





# Documentum

Documentum consente di archiviare e verificare documenti su Ethereum blockchain.

Gli hash dei file agiscono come firma, altri utenti possono successivamente confrontare gli hash dei file con gli hash nello SC, ciò consente con precisione al 100% di vedere se due file sono identici.

<https://www.documentum.nanadevs.com/>

## Connect MetaMask to Rinkeby

Document name:

Nessun file selezionato

No File, no hash :)

## Examples to compare

1. [DECLARATION OF THE RIGHTS OF THE CHILD](#)
2. [Universal Declaration of Human Rights](#)

## List of documents



### DECLARATION OF THE RIGHTS OF THE CHILD

5e75787532e528df9445b1ddd34e38b8b4c437d56c402b31bc90b2e794495329

5/9/2018

**Verify Document**

Nessun file selezionato



# Grazie per l'attenzione

---

**Devoleum:** <https://www.devoleum.com/>

**LinkedIn:** <https://www.linkedin.com/in/lorenzo-zaccagnini/>  
<https://www.linkedin.com/in/elisa-romondia/>

**Twitter:** [@LorenzoZcg](https://twitter.com/LorenzoZcg) [@elisaromondia](https://twitter.com/elisaromondia)