

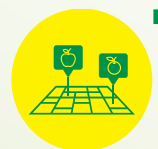
Teoria della Blockchain e applicazioni all'agricoltura

25/6/2020

Dott. Fabio Lecca

CTO - tokenfarm@tokenfarm.it

www.tokenfarm.it



Token farm



Presentazione: Fabio Lecca

- Dal 2017: Portale del Socio Coldiretti – ad oggi 35.000 Soci iscritti ai Servizi Online <https://socio.coldiretti.it>
- Membro del gruppo dei 30 esperti Blockchain del Ministero dello Sviluppo Economico <https://www.mise.gov.it/index.php/it/10-istituzionale/ministero/2039024-blockchain-membri-del-gruppo-di-esperti>
- CTO di TokenFarm: startup innovativa di Coldiretti www.tokenfarm.it
- Membro dell'Associazione Blockchain Italia www.associazioneblockchain.it
– tavolo sulla tracciabilità Agroalimentare



Agenda

- Presentazione
- Blockchain in Italia
- Strategia Nazionale Blockchain
- Teoria della Blockchain
 - Peer to peer e Decentralizzazione
 - Immutabilità dei dati
 - Automatismi («smart contract»)
 - Identità digitale
 - Oracoli
- Applicazioni in agricoltura per filiere, comparti e singole attività
 - Tracciabilità di filiera
 - Applicazioni assicurative
 - Efficiente e trasparente erogazione di contributi
 - Tokenizzazione: nuove forme di accesso al credito

Blockchain in Italia

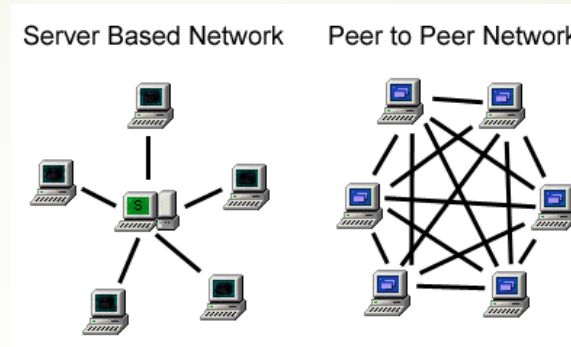
- Fine 2018: ingresso dell'Italia nella EBP European Blockchain Partnership (28 paesi)
- DL Semplificazioni febbraio 2019:
<http://www.senato.it/japp/bgt/showdoc/frame.jsp?tipodoc=Emend&leg=18&id=1097873&idoggetto=1095835>
 - Definizione delle Tecnologie basate su registri distribuiti
 - Definizione di Smart Contract
 - La memorizzazione produce gli «Effetti giuridici della validazione temporale elettronica»
 - Linee guida tecniche a cura di AGID
- EBSI: European Blockchain Systems Infrastructure, infrastruttura europea comune per la realizzazione di servizi pubblici, anche transfrontalieri. Casi d'uso: identità digitale, riconoscimento dei titoli di studio, «notarizzazione», condivisione sicura di dati.
- Strategia nazionale pubblicata il 18 giugno e in consultazione fino al 20 luglio 2020: <https://www.mise.gov.it/index.php/it/consultazione-blockchain>



Strategia Nazionale Blockchain e registri distribuiti


- Documento che fotografa lo stato dell'arte della tecnologia e suggerisce azioni utili per incentivare lo sviluppo economico
- La principale e potenziale caratteristica offerta da questa tecnologia, è quella di ridurre, in alcuni casi anche drasticamente, **il costo della fiducia** necessario al perfezionamento di una transazione, intesa come scambio informativo o di valore, garantendo al tempo stesso certezza della sua esecuzione
- In quei contesti in cui il costo della fiducia è una componente rilevante del costo transazionale, queste tecnologie possono ridurre inefficienze e semplificare i livelli di intermediazione
- La riduzione del costo della fiducia, inoltre, può rendere economicamente conveniente l'esecuzione di micro scambi di valore tra due attori, creando le basi per lo sviluppo di nuovi modelli di business
- Questa tecnologia potrà rivoluzionare il modo con il quale le imprese, i privati, le amministrazioni pubbliche interagiscono


Peer to peer e decentralizzazione



- Bitcoin: a peer-to-peer electronic cash system del 2008 - introduzione di concetti di economia nel campo del software
- Ogni nodo della rete è paritario rispetto agli altri e agisce sia da client che da server
- Ogni nodo può ricevere Transazioni, validate mediante un «algoritmo di consenso» e raggruppate in «blocchi».
- Es. di algoritmo di consenso: Proof-of-work, che consiste nella risoluzione di un complesso problema matematico che richiede ingenti risorse di calcolo (in cambio si ottiene una ricompensa) : chi lo risolve ha diritto di aggiungere il blocco
- A valle della validazione, un nuovo blocco è scritto su ogni nodo e «concatenato» crittograficamente con il blocco che lo precede

Immutabilità dei dati


DATA  Welcome to Blockchain Demo 2.0!

PREVIOUS HASH 

HASH 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

GENESIS BLOCK on Tue, 17 Oct 2017 19:53:20 GMT 604


▼


DATA 

PREVIOUS HASH 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf


HASH 0004a8229b4c09c42d6d3221682a5f3ebe5e6509511ce403c565ea42d5f1264a

BLOCK #1 on Wed, 24 Jun 2020 21:18:31 GMT 4706


DATA  Welcome to Blockchain Demo 2.0!!

PREVIOUS HASH 

HASH 2a81a5d47560567a689aa51100c8bbbbe91b42a79b95ff9aaa70e110a5264f15


GENESIS BLOCK on Tue, 17 Oct 2017 19:53:20 GMT 

▼

DATA 

PREVIOUS HASH 2a81a5d47560567a689aa51100c8bbbbe91b42a79b95ff9aaa70e110a5264f15

HASH 204a13a80f6b30bac55a859dce5b496e8e3bc34d694256fec008a73de161d1a3

BLOCK #1 on Wed, 24 Jun 2020 21:18:31 GMT 

- Decentralizzazione e sicurezza: occorre prendere il controllo di oltre il 51% dei nodi della rete per poter controllare ciò che viene scritto sulla blockchain
- Per fare ciò serve una enorme potenza di calcolo che rende antieconomica questa operazione

Automatismi e «smart contract»

- Se i dati in una blockchain sono immutabili, allora posso registrarci sopra dei programmi (rappresentati anch'essi come dati) e farli eseguire ad una macchina (intuizione geniale di Vitalik Buterin, al tempo 19enne)
- 2015 : Ethereum: «An Unstoppable World Computer»
- Definizione di «smart contract» del 1997 ad opera di Nick Zsabo
- Ambiente di esecuzione sicura e certificata di programmi software
 - Sicura: le invocazioni dei programmi sono transazioni
 - Certificata: posso verificare una singola computazione a distanza di anni
- Rapporti tra «contratti»





Identità digitale

- Riconoscere con affidabilità gli utenti per abilitare i servizi online
- Utenti «anonimi» e «pseudonimi»
- Utilizzo della crittografia a chiave pubblica (chiave pubblica e privata)
- Self-Sovereign Identity: l'utente ha il controllo dei dati per accedere ai servizi e possiede i dati che lo riguardano – rispetta il GDPR – aderisce agli standard delle credenziali W3C
- eSSIF: european Self Sovereign Identity – con validità legale
- Una blockchain pubblica (ma senza dati personali) con la funzione di «elenco telefonico» delle chiavi pubbliche degli enti che emettono credenziali e delle «liste di revoca»



Oracoli

- Dati «on-chain» e dati «off-chain»
- es. data e ora corrente: non è «on chain» (possiamo leggere il timestamp dell'ultima transazione osservata, ma ha una certa «risoluzione»)
- Per motivi di sicurezza le blockchain possono soltanto accedere ai dati «on-chain»: come è possibile quindi «accedere al mondo esterno»?
- Gli Oracoli alimentano gli smart contract con i dati del mondo esterno di cui hanno bisogno e quindi «scatenano» le azioni codificate
- Tipologie: Software, Hardware, Inbound, Outbound, Consensus-based



Applicazioni in agricoltura

- benefici per :
 - Filiere
 - Comparti
 - Singole attività
- PoliMi: Agroalimentare è indicato tra i settori chiave per l'utilizzo della blockchain(dopo Finanza e PA), ma:
 - Soffre di basso livello di digitalizzazione

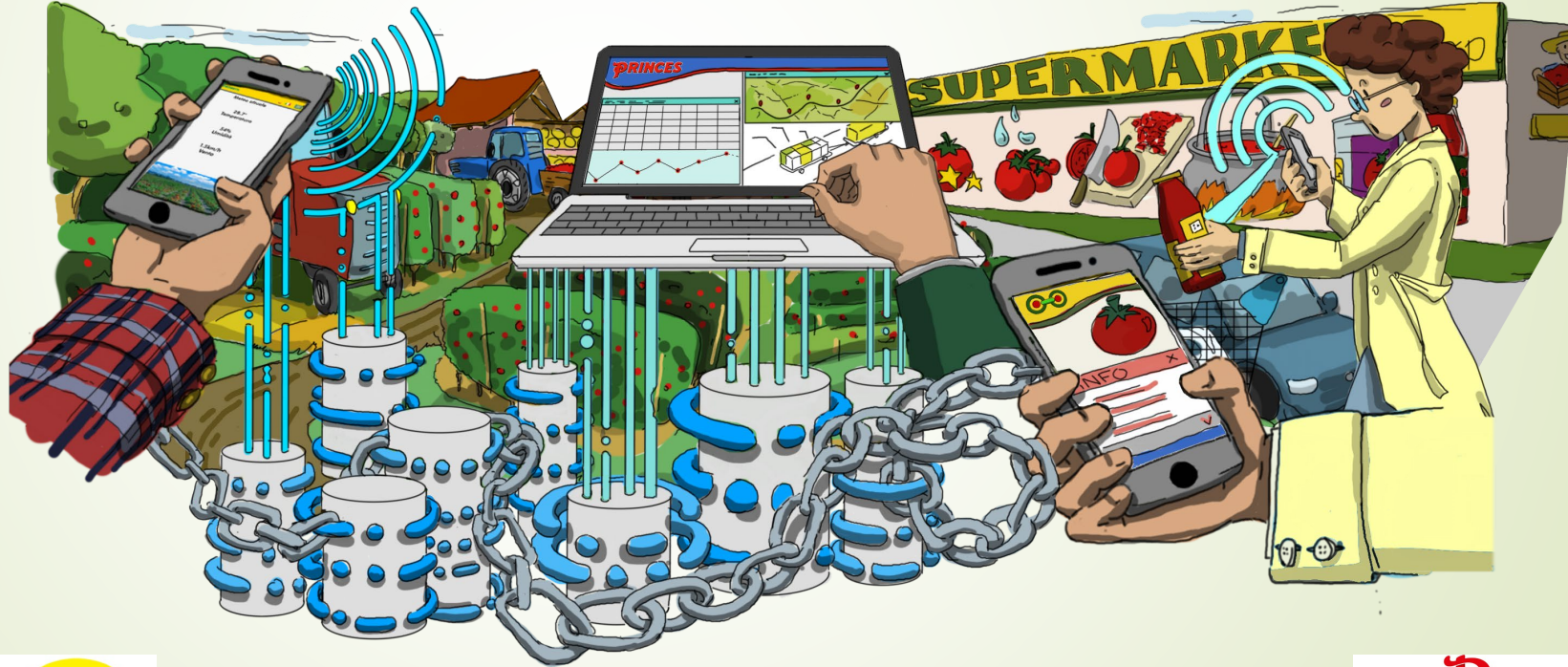


Tracciabilità di filiera

- Nell'attuale mercato agroalimentare, a causa dell'incremento della distanza tra produttore e consumatore, viene a perdersi sia l'identificazione del luogo da cui proviene il prodotto che la conoscenza del soggetto che lo realizza.
- All'aumento della varietà dei prodotti alimentari si contrappone una perdita di contatto tra produttore e consumatore che genera un'inevitabile perdita di **"fiducia"**
- Il grado di **fiducia** aumenta quando è possibile stabilire con ragionevole attendibilità il luogo di origine delle materie prime, osservare il processo di lavorazione, essere informati sulle modalità operative che portano alla realizzazione del prodotto e, soprattutto, conoscere personalmente chi ne garantisce la qualità
- Proprio questa relazione personale con i consumatori è percepita dal produttore come un'ulteriore motivazione rispetto alla sua funzione di fornitore di alimenti di qualità a chi è in grado di apprezzarne l'origine e il significato

Il progetto Pomos

Con 46 milioni di quintali totali raccolti all'anno, l'Italia è il primo produttore in Europa di pomodoro ed il secondo al mondo (dopo la Cina)



Il progetto Pomos: obiettivi



► Tracciabilità

per garantire il rispetto dei requisiti dei singoli prodotti, aumentando sicurezza, efficienza ed automazione dei processi produttivi



► Sostenibilità

- **Sociale:** garantire il rispetto della legalità e dell'eticità nella forza lavoro nei prodotti trasformati
- **Ambientale:** garantire l'utilizzo consapevole delle risorse ambientali e nello smaltimento dei rifiuti
- **Economica:** riconoscere il giusto valore ai prodotti degli agricoltori, sulla base di prezzi stabiliti nell'Accordo nazionale di Filiera

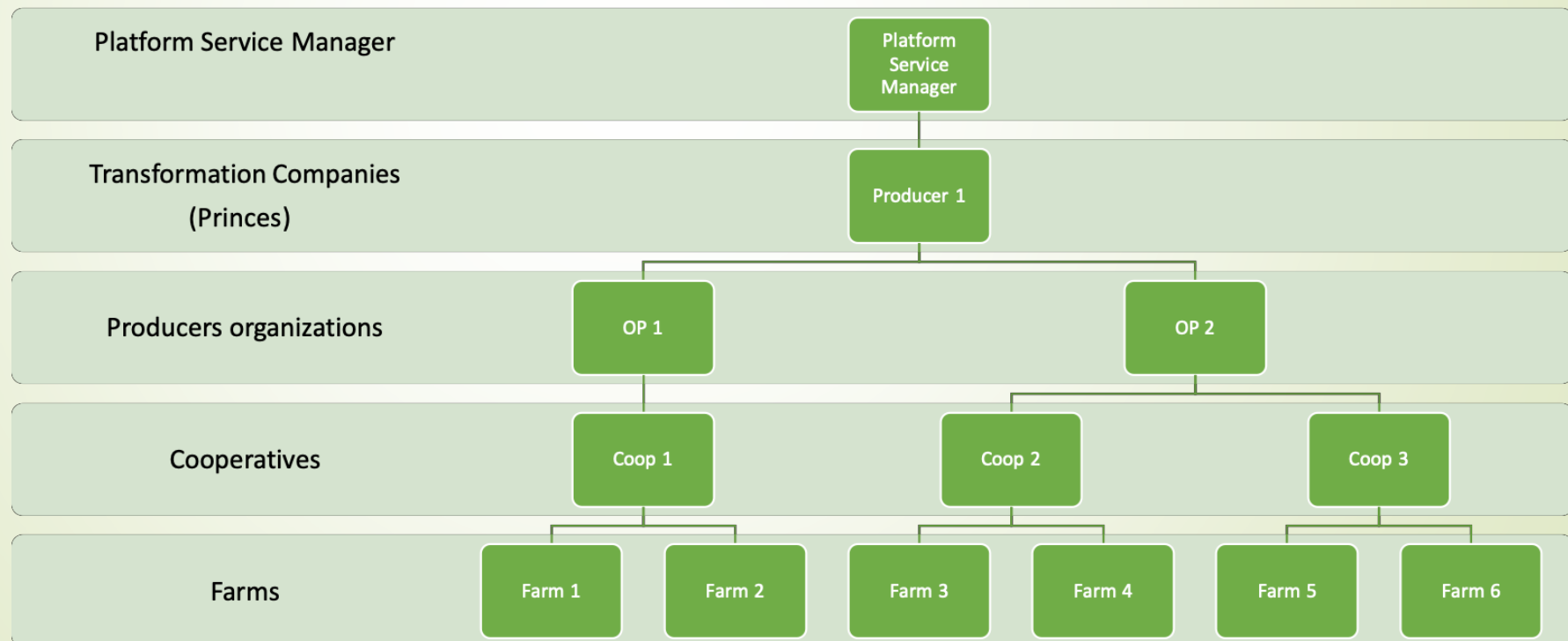


► Qualità

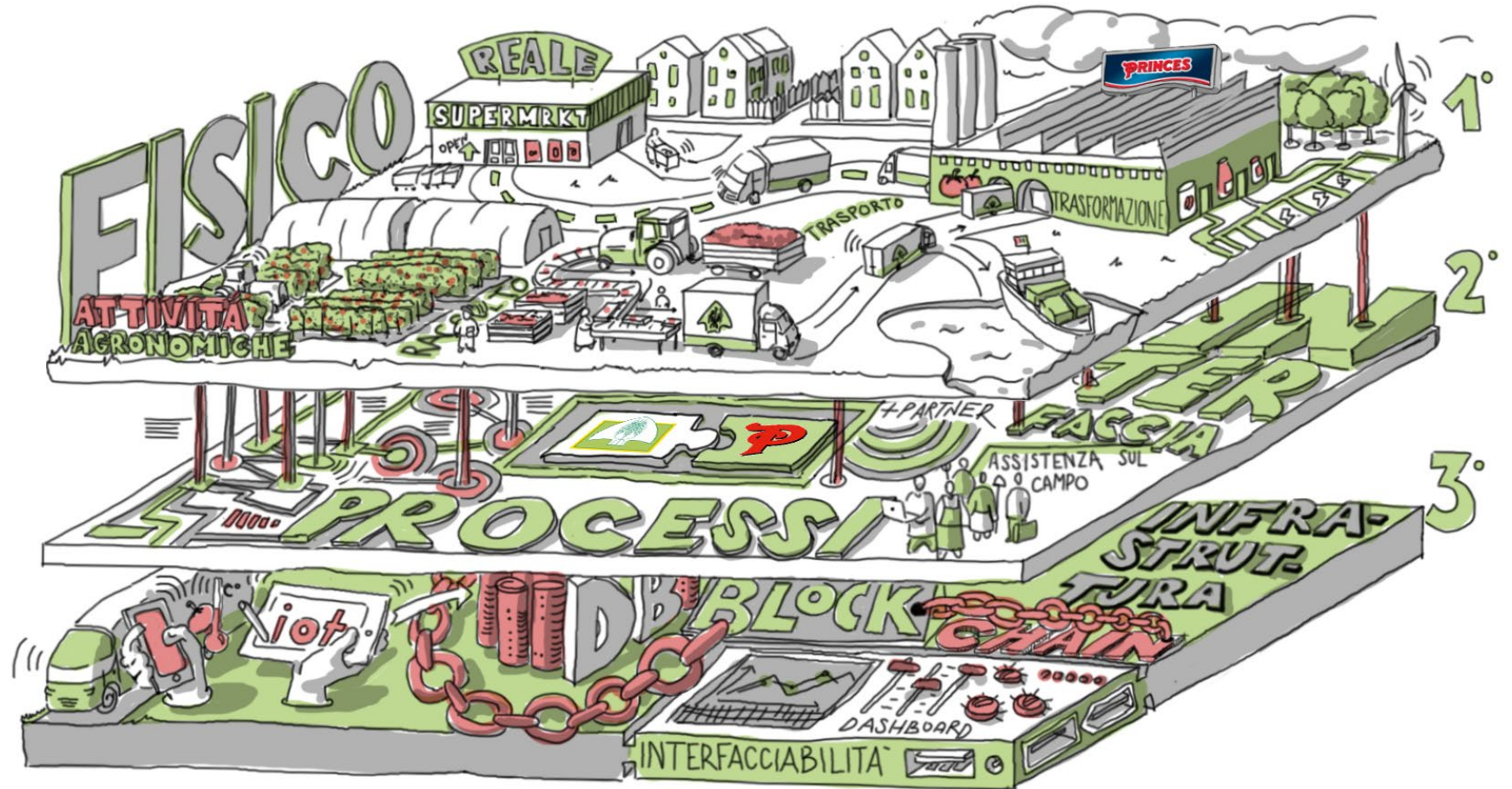
valorizzare la qualità del prodotto e l'identità nazionale del Made in Italy

Il progetto Pomos: attori

- Avviato nel maggio 2019 a seguito della firma dell'accordo di filiera
- 300 agricoltori della Puglia - 10000 ettari coltivati - 2,5 milioni di quintali di pomodori all'anno
- Trasformatore : Princes (5% produzione nazionale)



Il progetto Pomos: i 3 livelli



Il progetto Pomos: i dataset

Attività agronomiche →

Semina/Trapianto
Quaderno di Campagna Digitale
Analisi terreno e piante
Fertilizzazioni, Concimazioni, Pesticidi
Consumo energetico, Consumo acqua
Misurazioni ambientali/meteo
Sensori
Manutenzione e taratura macchinari
Operatori e lavoro etico

Raccolta →

Tipologia raccolta (meccanica/manuale)
Dati meteo
Geolocalizzazione macchinari (IoT)
Quantità raccolta
Ora inizio – fine
Controllo qualità e caratteristiche prodotto
Macchinari e manutenzione
Sensori
Consumo energetico
Operatori e lavoro etico

Trasporto →

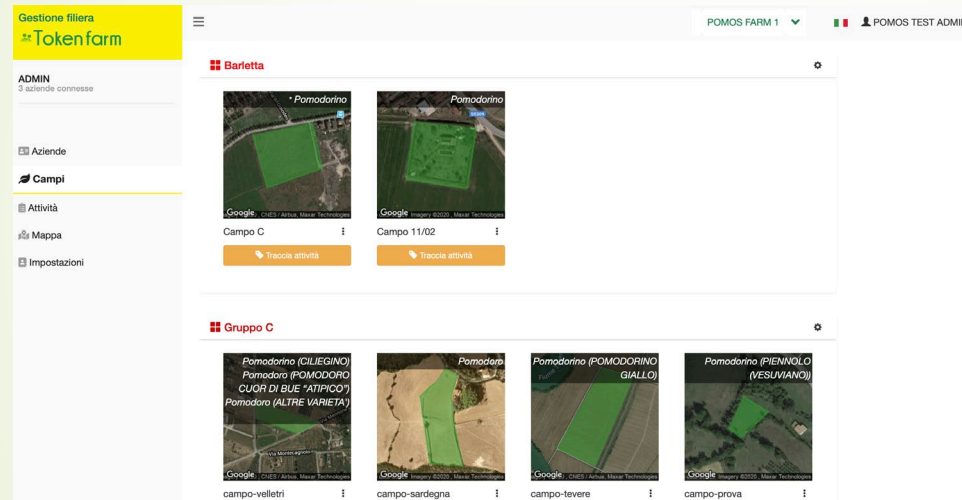
Tipologia e caratteristiche mezzo
Consumo energetico
DDT
Autista e lavoro etico
Tracciabilità: origine, quantità, caratteristiche, destinazione
Creazione Identità digitale del lotto/bins/trasporto
Tag prodotto grezzo

Trasformazione →

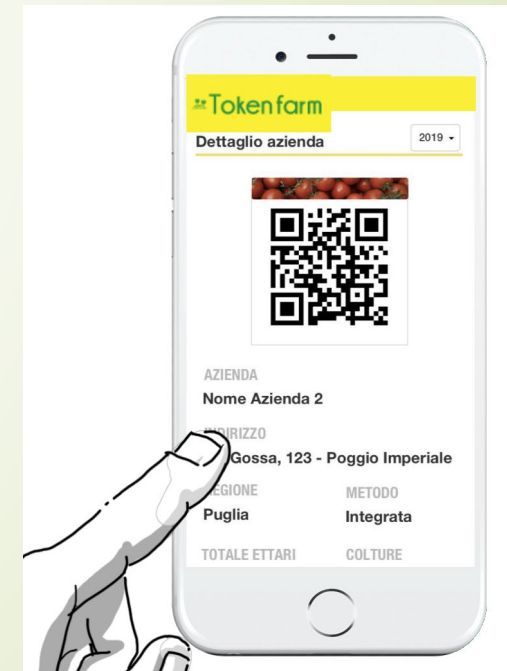
Produzione
Consumi
Personale
Qualità
Creazione Identità digitale prodotto finito
Tag di prodotto finito

Il progetto Pomos: risultati

- 3 App responsive per: agricoltori, trasformatore e gestori della piattaforma



- Clienti finali:
scansione QR Code e visualizzazione dettagli
- È solo l'inizio di un processo molto lungo



Applicazioni assicurative «smart»

- Posso sottoscrivere automaticamente un'assicurazione che prevede un risarcimento in caso di eventi meteorologici avversi (precipitazioni eccessive, gelate, temperature fuori norma in determinati periodi)
- Anche il funzionamento è automatico: un «oracolo» che scrive i dati attendibili provenienti da una fonte concordata (es. Meteo Aeronautica Militare)
- Lo «smart contract» al verificarsi degli eventi secondo i parametri indicati dalla polizza, procede ad effettuare il rimborso al cliente
- Costo del premio più basso





Erogazione di contributi

- Trasparenza ed efficienza dei processi amministrativi
- Integrazione tra fonti dati: Fascicolo Aziendale, registri di carico/scarico, ...
- Invio domanda di contributi agricoli (es Domanda Pac)
- Gli smart contract possono erogare automaticamente i contributi..
 - Controlli più snelli
 - Tempi minori per ottenere i contributi



Tokenizzazione

- Concetto di «moneta programmabile»: le applicazioni possono trasferire informazioni oppure effettuare scambi di valore
- Token: la registrazione di un asset (fisico o digitale) su blockchain in modo che si possa sempre determinare la proprietà, senza dispute
- Nuove forme di accesso al credito: possibilità di «granularizzare» asset che fino a poco tempo fa risultavano indivisibili
 - Opere d'arte
 - Magazzino di prodotti es. forme di Parmigiano Reggiano



Conclusioni

- Blockchain come «macchina per la **fiducia**»
- Tecnologia che spinge alla **collaborazione** piuttosto che alla **competizione**
- Consente **trasparenza** e **affidabilità** nella **gestione dei dati** e nell'**esecuzione dei programmi** (PoliMI: Finanza, PA, Agrifood)
- Principali criticità:
 - Scalabilità e sostenibilità (già in corso di risoluzione)
 - Problema del «minimo ecosistema sostenibile»: bisogna usarla tutti insieme
 - Mancanza di formazione e di competenze