Usi non finanziari delle principali blockchain pubbliche

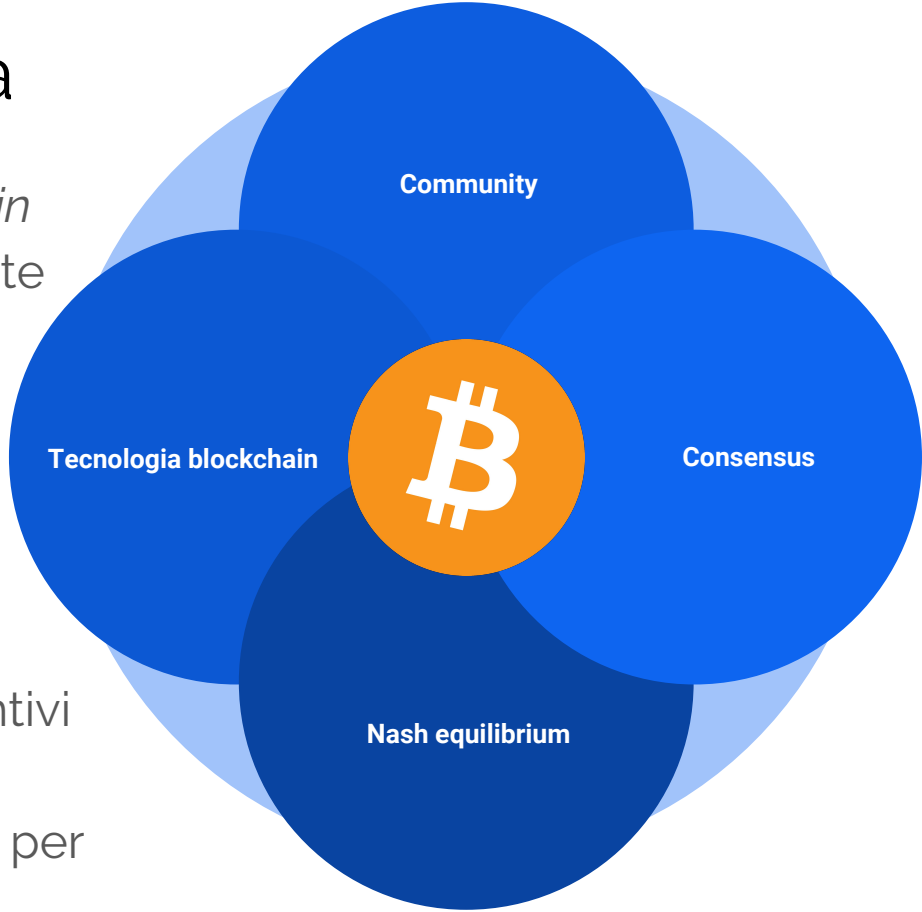
Valerio Vaccaro

Blockchain for Business
Università di Venezia "Ca' Foscari"
20 febbraio 2019

Introduzione terminologica

Correntemente si usa il termine *blockchain* per identificare soluzioni complesse basate su:

- **community**: insieme di sviluppatori, utilizzatori, finanziatori, ...
- **consensus**: regole di funzionamento autosufficienti
- **nash equilibrium**: incentivi e disincentivi economici
- **tecnologia blockchain**: una struttura per salvare liste ordinate di eventi



Agenda

Come è fatta una blockchain?

Usi finanziari di una blockchain

usi non finanziari di una blockchain

- proof of publication
- trustless timestamping
- single use seal

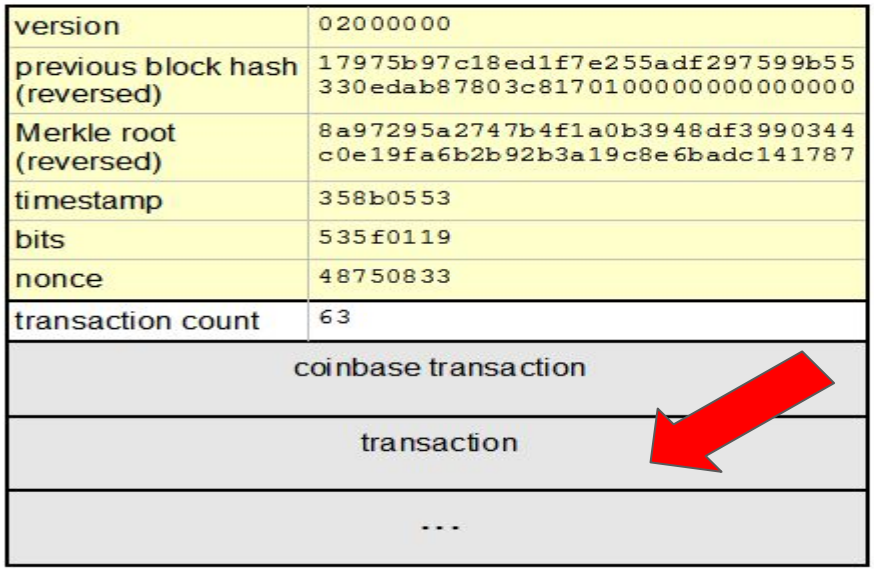
Com'è fatta una blockchain?

Transazione - è il vettore per lo spostamento di valore su blockchain.

- N input (necessariamente transazioni non spese precedenti)
- M output
- Script di autorizzazione e firma (programmabilità)
- Crittografia

version		01 00 00 00
input count		01
input	previous output hash (reversed)	48 4d 40 d4 5b 9e a0 d6 52 fc a8 25 8a b7 ca a4 25 41 eb 52 97 58 57 f9 6f b5 0c d7 32 c8 b4 81
	previous output index	00 00 00 00
	script length	
	scriptSig	script containing signature
	sequence	ff ff ff ff
output count		01
output	value	62 64 01 00 00 00 00 00
	script length	
	scriptPubKey	script containing destination address
block lock time		00 00 00 00

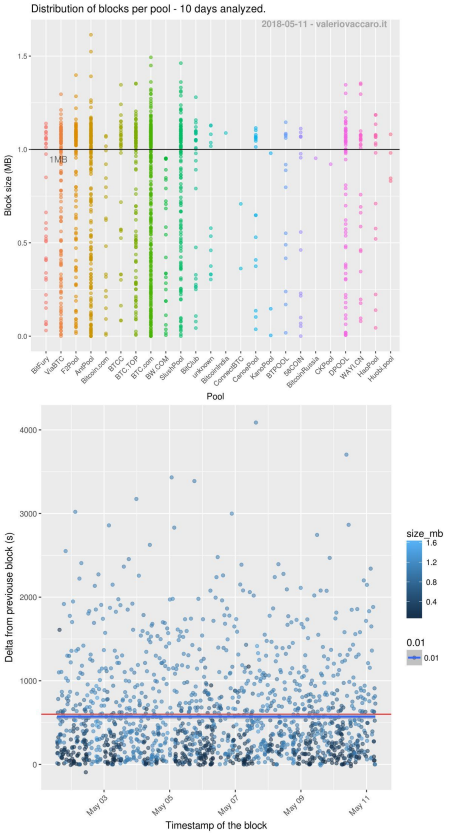
Com'è fatta una blockchain?



Blocco - contiene le transazioni da confermare

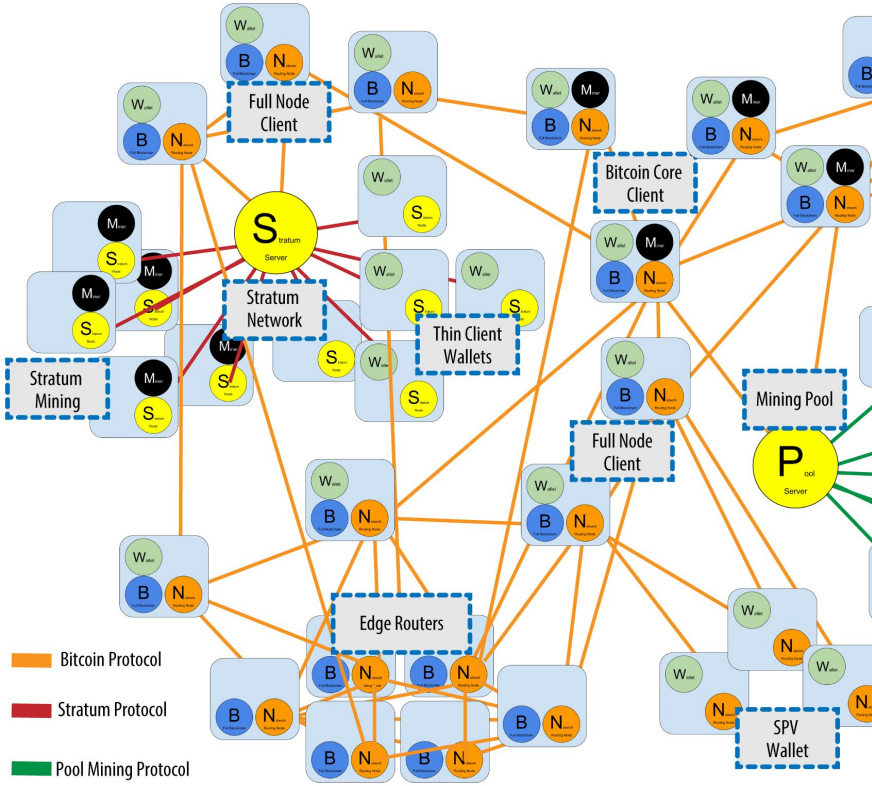
- Può essere scritto sulla blockchain da chi risolve un certo problema matematico computazionalmente rilevante (PoW)
- Contiene un premio per chi trova la soluzione
- La difficoltà è adattata in funzione delle condizioni della rete

Com'è fatta una blockchain?



Mining e rete

Consensus



* statistiche disponibili su http://vaccaro.tech:3838/bitcoin

Usi finanziari

- Strumenti di pagamento
- Store of value
- Denaro programmabile
- Creazione e movimentazione di asset (Token, coloured coins, ...)
- Base per 2nd layer e sidechain
- Simulazione e realizzazione di sistemi complessi di pagamento (atomic swap, ...)

Usi non finanziari

Effettuazione di una transazione che muove informazioni oltre che valore*:

- Proof of Publication
- Trustless Timestamping
- Single use seal

* spesso non è desiderato muovere informazioni importanti e valore in una medesima transazione, occorre comunque pagare le fee di transazione.

Proof of Publication

Scrivo un testo direttamente sulla blockchain (in chiaro o meno)

Uso di un comando specifico per la scrittura di un testo (nel caso di Bitcoin derivati OP_RETURN).

Massimo 80 caratteri per transazione (nel caso di Bitcoin)

Posso provare:

- proprietà del testo (la transazione è firmata con la mia chiave privata),
- data di pubblicazione,
- unicità,
- sequenzialità.

Proof of publication

Non scala!

https://gitlab.com/valerio-vaccaro/writeonchain

Timestamping

Il timestamping è l'atto di dare una data ad un documento, il primo e più comune esempio è il **timbro postale**

- Alice scrive a Bob, la data della comunicazione è apposto da terzi, nè Alice nè Bob possono contraffarlo facilmente
- Attenzione: deve essere apposto sul documento e non sulla busta!

Per importanti documenti deve essere posta da pubblico ufficiale, il notaio

- Ad esempio per il rogito della casa

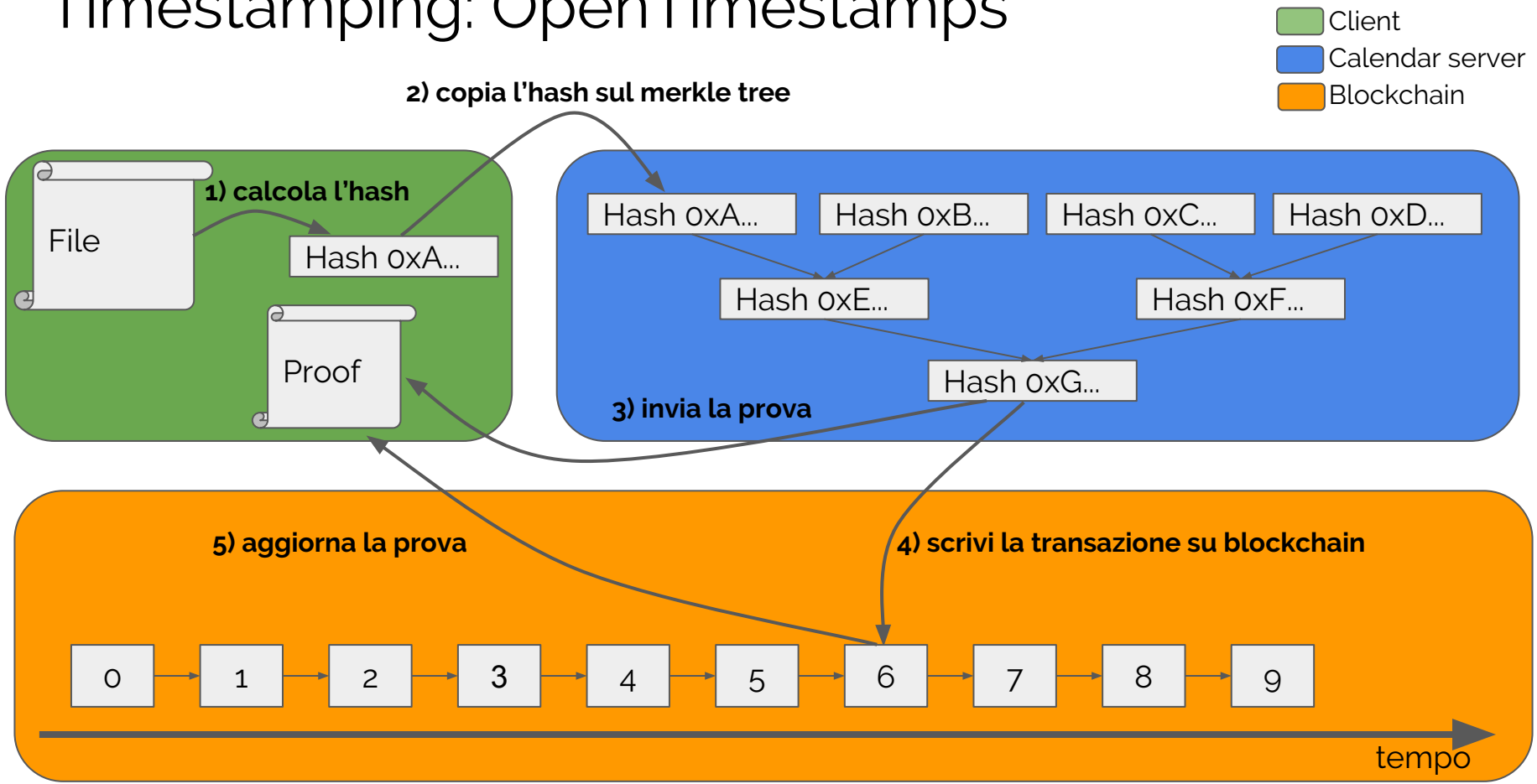
E per i documenti digitali?

Timestamping: OpenTimestamps

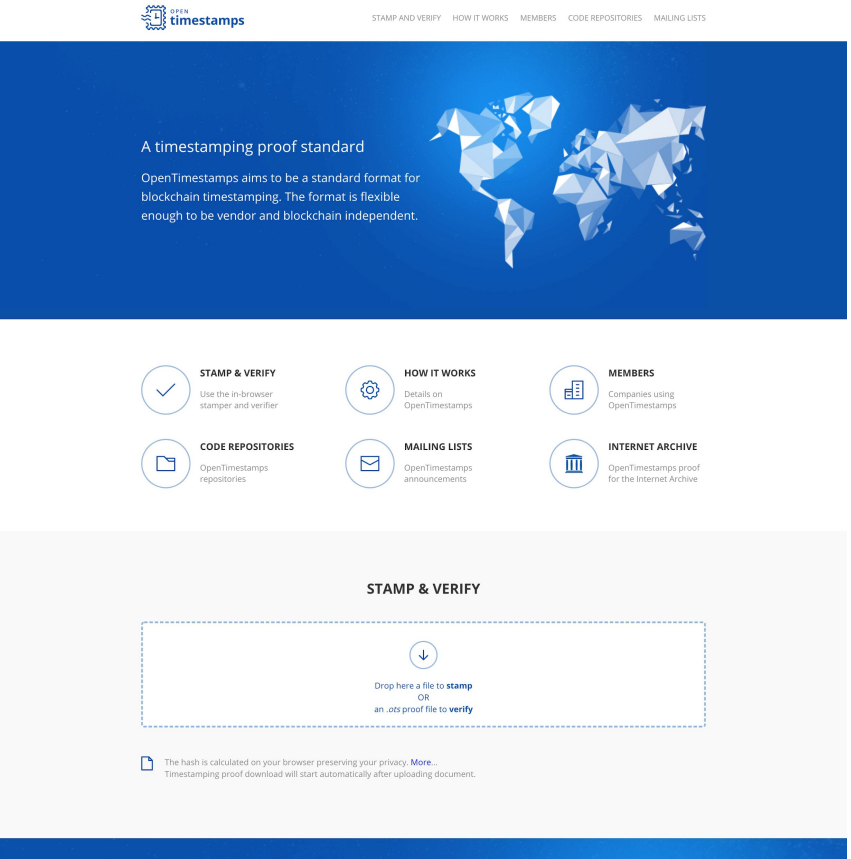
OpenTimestamps è un protocollo standard per la notarizzazione di qualsiasi informazione digitale con le seguenti caratteristiche:

- **Trust** - OTS usa la blockchain bitcoin risultando decentralizzato, pubblicamente verificabile e rimuovendo la necessità di una certification authority,
- **Cost** - OTS può condensare un numero illimitato di timestamps in una singola transazione,
- **Convenience** - OTS genera un timestamp verificabile direttamente da una terza parte in un solo secondo.

Timestamping: OpenTimestamps



Timestamping: OpenTimestamps



E' possibile timestampare un documento direttamente dal sito https://opentimestamps.org/

- Trascina il file sullo spazio **STAMP&VERIFY**
- Il sito calcolerà automaticamente l'hash e manderà una richiesta ai calendar server
- Il risposta verrà fornito un file .ots contenete la prova (parziale) del timestamping

Timestamping: OpenTimestamps

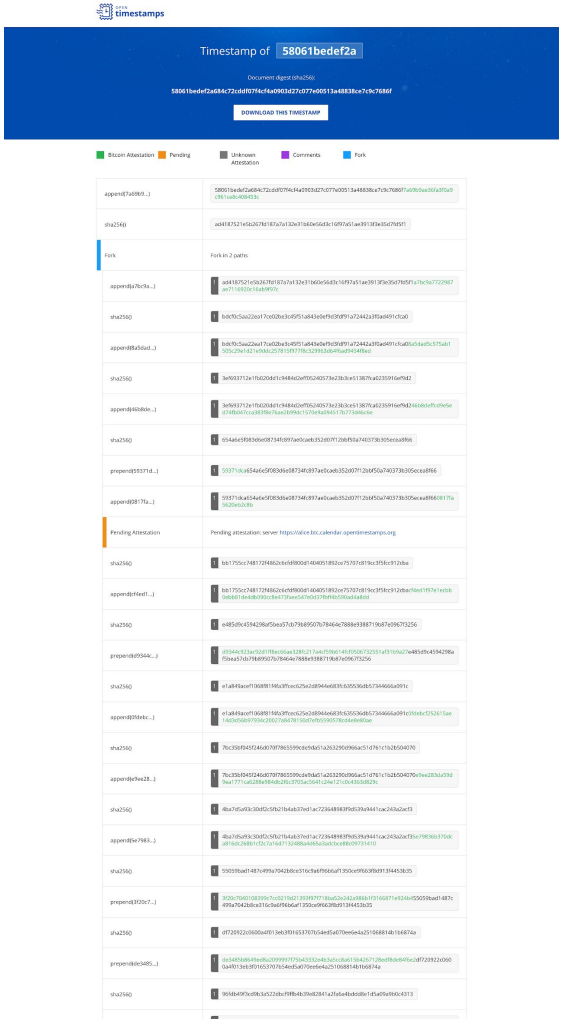
Tutto il software di OpenTimestamps è open source e già disponibile su github.

https://github.com/opentimestamps

Client e Server sono disponibili per installazioni personali e sono già sviluppate le librerie per:

- Python
- Javascript
- Java
- Rust
- Node-RED

Esistono dei **server pubblici** e **gratuiti** che consentono di essere già operativi! Da ora!



Single use seal*

Sfrutta le proprietà di singola spesa delle transazioni delle blockchain per “bloccare” l’aggiornamento di un contenuto*.

Il contenuto risulta valido ed aggiornato solo se esiste una “storia” plausibile dello stato del contenuto e se l’ultimo step contiene una transazione non ancora spesa.

La modifica dello stato può essere effettuata solo da chi possiede le chiavi private capaci di spendere l’ultima transazione.

All’atto dell’aggiornamento del contenuto occorre esplicitare chi potrà effettuare la modifica successiva (inserendo i riferimenti di una transazione non spesa).

* E’ una fortissima semplificazione di un concetto molto più ampio e complesso.
https://petertodd.org/2016/commitments-and-single-use-seals

Single use seal: Eonpass

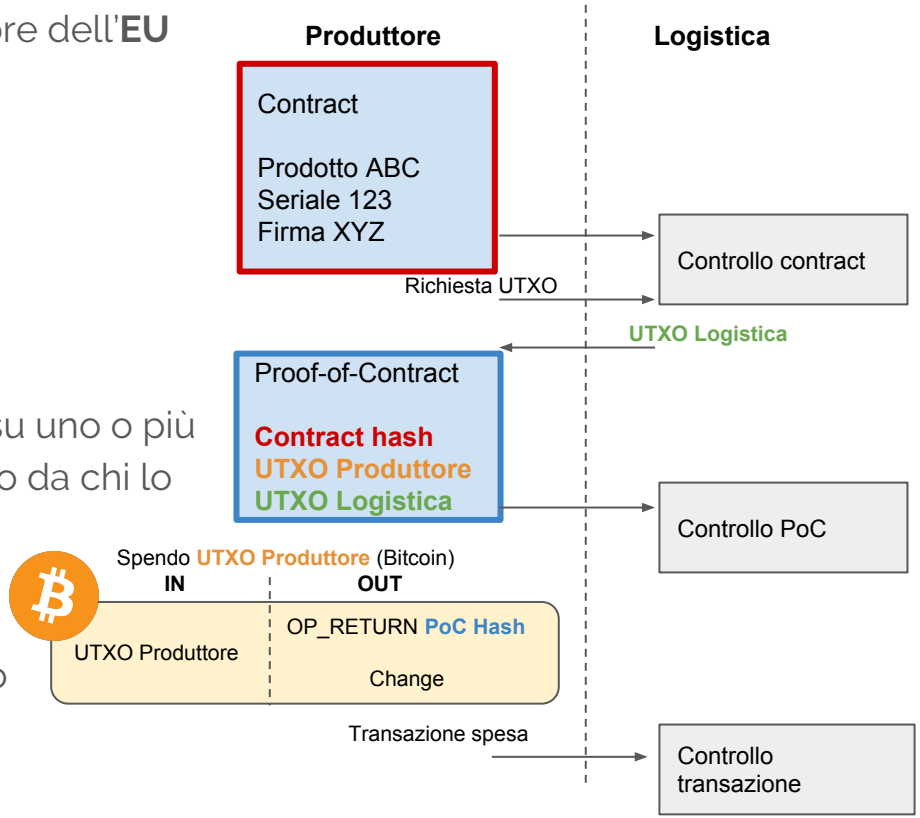
EONPASS™
SUPPLY CHAIN SECURED

Protocollo per l'anticontraffazione di prodotto vincitore dell'**EU Blockathon 2018**

- ID agnostic
- Implementazioni open-source
- Multi-blockchain (anche contemporanee)
- GDPR friendly

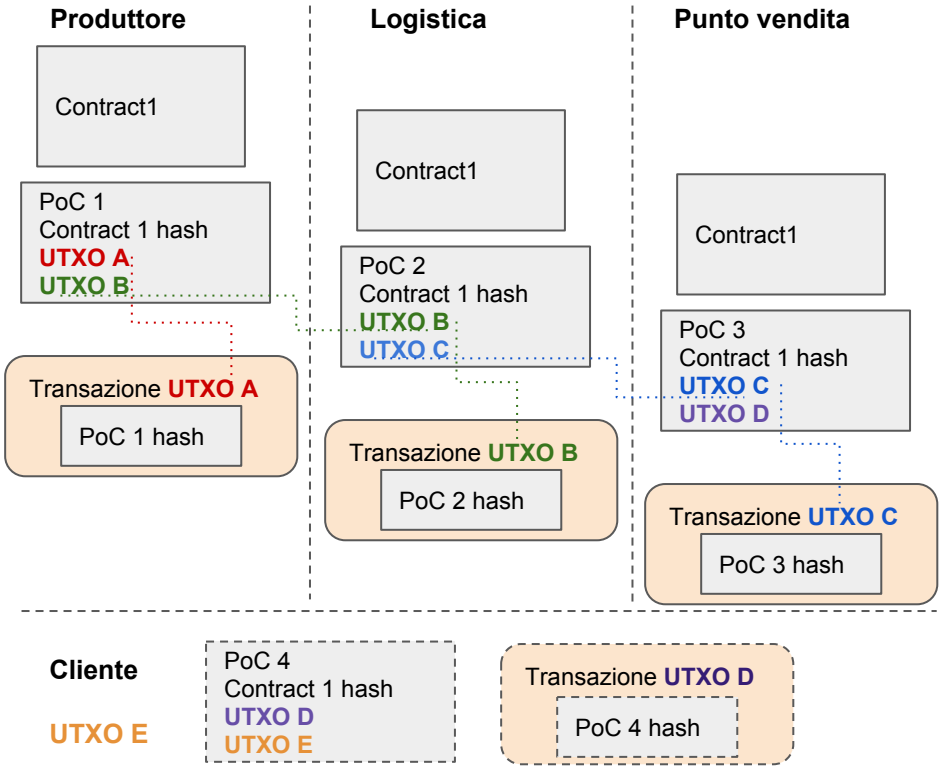
Una contratto è un file che contiene le informazioni su uno o più prodotti non necessariamente omogenei ed è firmato da chi lo redige.

Un Proof-of-contract è l'atto con cui viene dichiarato l'aggiornamento di un contratto e l'eventuale cambio di permessi.



* https://gitlab.com/Eonpass/specs

Single use seal: Eonpass



* https://gitlab.com/Eonpass/specs

Il controllo può essere fatto navigando tutta la storia, il PoC 3 è valido se:

- esiste una storia valida da PoC 1 a PoC 3
- UTXO A, UTXO B e UTXO C risultano spese con un commitment a PoC 1, PoC 2 e PoC 3 rispettivamente
- UTXO D è non spesa

L'acquisto da un Cliente è confermato dalla creazione di un PoC 4 con la transazione non spesa del cliente (UTXO E) e dalla spesa di UTXO D con un commitment al PoC 4 creato.

Sono previsti meccanismi di split e merge dei contratti.

Fonti

- **Mastering Bitcoin** - https://github.com/bitcoinbook/bitcoinbook
- **Opentimestamps** - https://petertodd.org/2016/opentimestamps-announcement
- **Single use seal** - https://petertodd.org/2016/commitments-and-single-use-seals
- **Blockchain and (I)IoT** - https://medium.com/@valerio.vaccaro/blockchain-and-i-iot-a9ec599e0df1
- **Eonpass** - https://gitlab.com/Eonpass/specs/

Valerio Vaccaro
email: valerio.vaccaro@gmail.com
twitter: @Tulipan81
linkedin: https://www.linkedin.com/in/valeriovaccaro/
github: https://github.com/valerio-vaccaro
gitlab: https://gitlab.com/valerio-vaccaro