

Algorand value proposition: incontro col CDTI di Roma del 10 giugno 2020

La Blockchain si riferisce a tante cose assieme e spesso le discussioni che ne seguono fanno perdere di vista l'obiettivo iniziale di coloro che la concepirono diversi anni fa, <https://en.wikipedia.org/wiki/Blockchain>.

Cosa è la Blockchain? Una lista di blocchi in cui ogni blocco è legato crittograficamente al blocco precedente, la scrittura del blocco successivo è effettuata attraverso un protocollo di consenso e la catena evolve seguendo un equilibrio basato sulla teoria dei giochi.

Perché venne concepita la Blockchain? Gli ideatori volevano qualcosa che fosse evocativo di distribuzione, immutabilità, sicurezza e trasparenza per dare a tutti un'assoluta fiducia sui dati presenti nei blocchi.

Quindi la Blockchain ideale è:

- Pubblica
- Permissionless (tutti possono aggiungersi come utente senza un'autorizzazione)
- Decentralizzata (tutti hanno la medesima autorevolezza nella governance della Blockchain).

Se con questi requisiti sembra dubbio poter parlare in maniera corretta di Blockchain private e permissioned, tuttavia ha senso avere dati privati e il poter gestire una struttura dati all'interno di una comunità privata di soggetti. Ciò detto, è da ritenere che l'adozione di Blockchain private anche laddove una Blockchain pubblica sarebbe stata ideale, sia stato anche un compromesso per superare il problema delle prestazioni delle Blockchain basate sul proof of work, una per tutte la Blockchain di Bitcoin, nelle quali il limite inferiore del tempo di latenza (vale a dire la conferma della registrazione irrevocabile di un nuovo blocco) è inaccettabile per lo svolgimento delle transazioni commerciali a cui siamo abituati, richiedendo molti minuti o svariate decine di secondi in quelle più recenti.

Nell'incontro via Web organizzato dal CDTI di Roma il 10 giugno u.s., giustificato dal recente annuncio dei grant da parte di Algorand Foundation (gli interessati possono trovare i dettagli al link seguente <https://algorand.foundation/grants-program>), il dott. Pietro Grassano, Dirigente di Algorand Inc., ha sottolineato le caratteristiche di una Blockchain propriamente detta come è Algorand:

- Open source per la trasparenza dei protocolli e degli algoritmi
- Costi molto bassi di una transazione (un millesimo di Algo, quindi oggi circa 0,00025 US\$)
- Resilienza delle risposte, tempi di latenza trascurabili e throughput elevato (*la rete MainNet funziona in maniera continua da un anno senza problemi 24h/24; ad oggi gestisce 1×10^3 TPS con un tempo di latenza inferiore a 4,2"; e l'obiettivo per fine 2020 è di arrivare a valori molto più alti; inoltre per come è concepita la rete Algorand non ha fork, problema non trascurabile nel proof of work*)
- Scalabilità per poter servire miliardi di utenti e quindi di fatto consentirà di offrire servizi nuovi a nuove fasce di popolazione oggi escluse, ad esempio per quanto riguarda i pagamenti elettronici
- Cifratura molto avanzata ed abbinata ad una assoluta decentralizzazione per una totale sicurezza (in Algorand lavora una squadra di crittografi molto noti, e il fondatore e Presidente, Prof. Silvio Micali del MIT, è un matematico e crittografo di fama mondiale che ha costituito un team di altissimo livello)
- Mantenimento di una relazione di fiducia tra gli utilizzatori e le aziende, tra gli utilizzatori e gli organismi pubblici perché assicura la sovranità dei dati al cittadino nelle applicazioni che lo coinvolgono

- Capacità di poter gestire circostanze diverse e diverse esigenze attraverso l'interconnessione con altre Blockchain (nella roadmap Algorand è incluso il modello della co-chain <https://www.algorand.com/resources/blog/algorand-co-chains>).

Tutti questi requisiti che sono molto stringenti sono possibili nella Blockchain Algorand che il 19 giugno u.s. ha compiuto un anno, perché Algorand è un'azienda giovane, con una tecnologia di nuova concezione e che ha messo a punto tenendo conto delle buone idee, del lavoro svolto nelle precedenti Blockchain e delle sfide in corso. Le slide dell'intervento sono a disposizione nel sito del CDTI cdti.org o possono essere richieste scrivendo al relatore <https://it.linkedin.com/in/pietro-grassano-7a3bb41>, che nella sua relazione ha toccato questi temi:

- Risorse professionali chiave in Algorand Inc. e in Algorand Foundation e relazione tra le due entità;
 - o Algorand Inc. è la società che sviluppa il SW dietro le specifiche della Algorand Foundation a cui spetta la governance della MainNet
- Limiti delle piattaforme pubbliche precedenti, che riguardano:
 - o Compromessi tra decentramento, scalabilità e sicurezza, difficoltà di utilizzo da parte di chi sviluppa software, alti costi di transazione (per quelle basate sul proof of work), prestazioni scarse (per quelle basate sul proof of work), carenze nella sicurezza (nel bonded proof of stake e nel delegated proof of stake); per dettagli vedere al link <https://www.algorand.com/resources/blog/algorands-core-technology-in-a-nutshell>
- Benefici fondamentali di Algorand;
 - o Rendere possibile la vision della Blockchain propriamente detta, attraverso prestazioni eccezionali, elevatissima sicurezza, bassissima capacità computazionale (quindi è una tecnologia green) e la disponibilità di ambienti di sviluppo basati (quindi SDK e reti di test) sugli skill più diffusi nell'informatica (finora Java, Java Script, Go, Python, altri se ne aggiungeranno) per un time to market delle soluzioni aziendali
- Ecosistema di Algorand: crescita in un anno e prime aree di adozione
 - o Alcuni casi di uso
- Novità della Algorand 2.0
 - o A livello 1 sono stati portate applicazioni importanti, quali gli asset fungibili e non, gli atomic swap e alcune categorie di smart contract che implementabili con un linguaggio *not turing complete* (TEAL)
- Cosa c'è all'orizzonte
 - o Co-chain e interoperabilità con altre blockchain pubbliche e private
 - o Cenni alla roadmap sono qui visibili <https://algorand.foundation/roadmap>

Algorand sta evolvendo lungo una direttrice che la renderà molto importante per chi sviluppa software applicativo.

Il webinar è stato preceduto da un'introduzione di Massimo Di Virgilio, Presidente del CDTI di Roma, di Gianluca Duretto, consigliere CDTI e coordinatore del gruppo di lavoro Blockchain del CDTI, e di Sergio Caserta, Algorand Ambassador e consigliere CDTI. Una sessione di Q&A ha completato il webinar di Pietro Grassano, Business Solutions Director Europe.

Sergio Caserta, consigliere del CDTI di Roma, è Algorand Ambassador, responsabile Italia della Vanguard Communications Europe e value maximiser della MirrorWave. Caserta si è laureato in Ingegneria Elettronica nel 1977 a Roma ed è membro ACM; può essere contattato via email s.caserta@cdti.org o via LinkedIn <https://it.linkedin.com/in/sergiocaserta>