AMMINISTRAZIONE CENTRALE
AREA COMUNICAZIONE E MARKETING
SETTORE **UFFICIO STAMPA**
Via VIII febbraio, 2 – 35122 Padova
stampa@unipd.it
http://www.unipd.it/comunicati
tel. 049-8273066/3041

UNIVERSITÀ DEGLI STUDI DI PADOVA

Padova, 6 febbraio 2019

BLOCKCHAIN, NON SOLO CRIPTOVALUTE
SICUREZZA E RIVOLUZIONE DI UNA TECNOLOGIA

La tecnologia della Blockchain, nata nel 2008, nell'immaginario collettivo è legata al concetto di criptovaluta. Una criptovaluta altro non è che una serie numerica concatenata in maniera immutabile sotto forma di blocchi di bit all'interno di una catena (Blockchain). La Blockchain ha anche una seconda caratteristica: è gestita "democraticamente" tra utenti che partecipano al processo. Ma questa è solamente una delle applicazioni possibili.

La Blockchain fa già parte del nostro tessuto sociale: è stato infatti creato un team di esperti afferenti al Ministero dello Sviluppo Economico (MiSE) e con un decreto legge approvato dal Senato viene finalmente riconosciuta la validità giuridica delle "tecnologie basate su registri distribuiti". Le commissioni Affari costituzionali e Lavori pubblici hanno accolto formalmente nella legislazione due concetti: Blockchain e Smart contract. Per Blockchain si intendono "le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili". Smart contract è invece 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".

Ma quanto sono effettivamente sicure queste tecnologie? Cosa vuol dire sviluppare un progetto ex-novo basato su Blockchain e che sfrutti a pieno il potenziale degli smart contract?

In un recente incontro tenutosi all'Università di Padova dal titolo "Blockchain: le sfide della sicurezza nell'era di Bitcoin", il Professor **Mauro Conti**, coordinatore del gruppo SPRITZ - Security and Privacy Research Group e membro del team di esperti del MISE, **ha detto** che «queste tecnologie sono giunte a una maturità sufficiente per poter essere impiegate con

successo non solo in ambito accademico, ma anche in quello aziendale e della pubblica amministrazione. Le tecnologie basate su registri distribuiti permettono di disegnare servizi nuovi e rendere più efficienti e completi quelli attuali, nonché semplificare molti aspetti della vita delle persone e delle aziende, permettendo allo stesso tempo di mantenere elevati standard di sicurezza».

Tra i benefici che tale tecnologia porterebbe alle aziende troviamo la possibilità di fornire ai propri clienti un registro immutabile a loro disposizione per tenere traccia della creazione, modifica e condivisione di documenti sensibili. Dall'altro non bisogna sottovalutare le possibili minacce di sicurezza come il *flooding* di messaggi ai nodi partecipanti, in sostanza l'invio a grande velocità di una serie di messaggi che ricorda, nella terminologia inglese, un effetto di "allagamento". Non solo, il team dell'Università di Padova si è particolarmente concentrato nello studio dei *ransomware* in ambito Blockchain. Si tratta dei *malware* che limitano l'accesso del dispositivo che infettano, richiedendo poi un riscatto (*ransom*) da pagare per rimuovere la limitazione: questa tipologia di virus ha sfruttato l'anonimato dei circuiti monetari per poter facilmente estorcere soldi.

Nell'ultimo anno forti speculazioni economiche hanno fortemente scosso la solidità delle cripto valute. Dall'incontro è emerso che bisognerebbe separare il concetto di tecnologia da quello dei suoi usi: le aziende che investono in Blockchain, non in criptovalute, hanno potenzialità di sviluppo maggiori. E la stessa cosa si può dire per la ricerca: la tendenza futura in ambito accademico è quella di utilizzare il "sistema Blockchain" al fine di fondere le sue caratteristiche di libro mastro (*ledger*) condiviso e immutabile con un gran numero di approfondimenti tra i diversi campi di studio.

Hanno partecipato all'incontro Mauro Conti dell'Università di Padova, Giovanni Maria Martingano e Fabio Canevarolo, Ifin Sistemi, Ankit Gangwal, Stefano Cecconello e Chhagan Lal, ricercatori del gruppo SPRITZ, Michele Todero. La giornata di studio è stata organizzata da SPRITZ group dell'Università degli Studi di Padova, specializzato in sicurezza informatica e privacy, e dall'azienda Ifin Sistemi di Padova, dal 1981 nel mercato nazionale dei servizi digitali, e che opera nell'ambito della Blockchain.