PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4362 di Venerdì 30 novembre 2018

Una innovativa tecnologia di sicurezza: la blockchain

Uno studio del National Istitute of standard and technology- NIST, dell'ottobre 2018, permette anche agli inesperti di prendere confidenza con questa innovativa tecnologia di sicurezza e protezione dei dati.

In allegato a questo breve documento, i lettori troveranno il testo completo del documento, pubblicato nell'ottobre 2018, dal NIST. Il documento passa in esame, con un linguaggio facilmente comprensibile anche per non addetti ai lavori, come funziona la tecnologia blockchain, che comincia ormai a essere inserita nell'arsenale degli strumenti di protezione informatica.

Anche se una delle applicazioni più diffuse di questa tecnologia fa riferimento alla movimentazione delle cripto valute, in realtà essa può essere applicabile ai numerosi altri casi, come i lettori potranno vedere in questa breve presentazione.

Ricordo che la blockchain costituisce un registro digitale a prova di manomissione o che mette in evidenza una possibile manomissione, attuato in una maniera distribuita, vale a dire senza che esista un archivio centrale. Inoltre questa tecnologia non è gestita da un'autorità centrale, o come una banca o un governo, ma è gestita dagli utenti stessi.

A livello di base, questa tecnologia consente a un gruppo di utenti di registrare delle transazioni su un libro mastro, gestito all'interno di questa comunità, operando in modo tale che in condizioni normali non sia possibile modificare una transazione, una volta registrata sul libro mastro. Il documento citato offre una analisi di ottimo livello di questa tecnologia, per facilitare i lettori la comprensione dei pregi che essa presenta.

Nel 2008, la tecnologia blockchain è stata combinata con altre tecnologie, per creare la ormai famosa cripto valuta, che permette lo scambio di cripto valute in maniera sicura e senza fare riferimento ad un'autorità centrale di controllo. La prima cripto valuta basata su questa tecnologia è stata chiamata bitcoin.

Applicando questa tecnologia, le informazioni riferite alla valuta elettronica sono collegate a un indirizzo digitale. Gli utenti di bitcoin possono firmare digitalmente e trasferire i diritti su questa informazione a un altro utente; la tecnologia blockchain registra pubblicamente questo trasferimento di proprietà, consentendo a tutti i partecipanti alla rete di verificare, in modo indipendente, la validità della transazione. La catena dei controlli viene memorizzata, mantenuta e gestita in maniera collaborativa da un gruppo di partecipanti, che possono trovarsi in qualunque parte del mondo. Questo accorgimento, insieme ad alcuni meccanismi criptografici, fa sì che la tecnologia possa resistere a tentativi di modificare il libro mastro, ad esempio modificando i blocchi o contraffacendo delle transazioni.

Il documento riportato in allegato permette al lettore, che conosca la lingua inglese, di comprendere i fondamenti di questa tecnologia e imparare ad utilizzarla correttamente. Questa tecnologia non ha nulla di magico, come invece viene riportato su documentazioni del settore, ma presenta delle indubbie caratteristiche oltremodo attraenti.

Come ho accennato prima, la tecnologia blockchain è il fondamento delle cripto valute attuali, così chiamate perché fanno ampio uso di funzioni criptografiche. Gli utenti utilizzano chiavi pubbliche e private per firmare digitalmente e garantire una valida transazione, all'interno del sistema.

Un'azienda che desideri attuare questa tecnologia deve capire gli elementi fondamentali ad essa correlati. Ad esempio, cosa accade quando un'azienda mette in piedi una rete blockchain e quindi decide di modificare i dati in essa archiviati? Quando si usa un database, la modifica del dato archiviato è relativamente semplice, ma in una tecnologia blockchain quest'operazione può essere molto difficile, proprio perché tale tecnologia è nata per impedire queste modifiche.

Un altro aspetto critico della tecnologia blockchain fa riferimento a come i partecipanti si mettono d'accordo circa il fatto che una specifica transazione sia valida. Quest'operazione, che viene chiamata "raggiungimento del consenso", può essere realizzata in molti modi, con aspetti positivi e negativi.

È importante quindi capire che la tecnologia blockchain è solo una parte della soluzione.

Oggi questa tecnologia viene utilizzata non soltanto per lo scambio di cripto valute, ma anche per distribuire software ad aziende acquirenti, con la garanzia che il software non sia stato modificato in transito.

In linea generale, esistono due grandi categorie di approccio alla tecnologia blockchain, vale a dire le tecnologie senza permesso e quelle con permesso. In una rete senza permesso, chiunque può leggere e scrivere nella catena blockchain senza autorizzazione. Per contro, le reti con permesso limitano la partecipazione a soggetti specifici e consentono quindi un controllo più accurato. È importante conoscere la differenza tra queste due categorie, per vedere quale può essere più utile per soddisfare le esigenze di un'azienda.

Anche se esistono numerose variazioni delle reti blockchain, vi sono alcuni elementi comuni.

Questa catena è costituita da un libro mastro distribuito, composto da blocchi. Ogni blocco è composto di un blocco iniziale, che contiene i metadati riferiti al blocco, e un blocco di dati che contiene gli elementi della transazione ed altri dati correlati. Ogni blocco iniziale, ad eccezione evidentemente del primo, contiene un collegamento criptografico al precedente blocco iniziale. Ogni transazione coinvolge uno o più utenti della rete blockchain e registra quanto è accaduto, firmando il tutto da parte dell'utente che ha avviato la transazione. Ecco perché questa tecnologia sfrutta tecnologie già esistenti, che vengono però combinate in un innovativo contesto.

È bene anche ricordare che la tecnologia blockchain non è in grado di risolvere tutti i problemi e vi sono temi che devono essere affrontati, come ad esempio la gestione di utenti con intenti criminosi, come sono applicati i controlli e i limiti di attuazione della tecnologia.

Ad esempio, in una rete in cui l'accesso è consentito solo a particolari utenti, occorre stabilire delle regole per vedere quale sia la autorità che consente agli utenti di accedere.

Nell'ambito della protezione dei dati personali, il valore di questa tecnologia non consiste tanto nel mascheramento dei dati, che in realtà non avviene, quanto nel fatto che è garantito un elevato livello di protezione dalla alterazione o cancellazione dei dati stessi.

Mi auguro che con il passare del tempo i lettori comprenderanno sempre meglio il funzionamento di questa tecnologia e potranno sfruttare al meglio i suoi indubbi pregi.

Il documento (pdf)

Adalberto Biasiotti

www.puntosicuro.it