Sicurezza e validità internazionale delle Blockchain

Le criptovalute come Bitcoin, Ethereum, Litecoin, Ripple e molte altre ancora, si basano sulla condivisione delle informazioni delle loro transazioni in rete peer-to-peer che ne regola l'esistenza e l'attendibilità. Nel 1998 un matematico economista Mr. Wei Dai ha reso pubblica l'idea rivoluzionaria di creare una valuta che non fosse soggetta ad un ente centralizzato, bensì facesse uso della crittografia per controllare la creazione e il trasferimento di denaro. Prende così vita il primo progetto di criptovaluta dal nome Bitcoin. Nel 2008 un anonimo dietro lo pseudonimo di Satoshi Nakamoto riprende con determinazione le idee di Mr. Wei Dai e ne scrive le prime linee guida: da quel momento il Bitcoin diventa tra le criptovalute più note al mondo. Il primo mercato di cambio ufficiale ha inizio nel 2010, il 6 Febbraio, con l'apertura del Bitcoin Market, seguito in Luglio da MTGox.

Il Bitcoin, come le altre criptovalute, si basa sulla distribuzione delle informazioni in rete oltre che su sistemi di gestione informatica Open Source. Pertanto si è reso necessario regolare e legittimare una moneta virtuale che di fatto, almeno sulla carta, è possibile creare dal nulla salvo la conoscenza di alcuni principi informatici non particolarmente complessi.

Essendo impossibile controllare la rete né tantomeno verificare le eventuali attività scorrette nella gestione delle transazioni economiche decentralizzate, come nella natura delle criptovalute, si sono intraprese tecniche digitali di sicurezza e di certificazione molto solide che con il tempo hanno dato legittimità ad un mercato finanziario extra bancario.

Le banche vigilano sui nostri conti correnti e, nel caso in cui il conto si prosciugasse per una qualsiasi ragione, l'istituto di credito interviene bloccando le spese, le uscite e garantendo quindi che quel conto non liquidi pagamenti per i quali non siano disponibili quattrini.

Nei Bitcoin non c'è un istituto di credito che vigila o controlla e legittima, si è dovuto quindi trovare un'altro metodo per impedire ai "furbi" di spendere valuta già spesa. Quest'altro metodo o sistema è fondato sul meccanismo delle timestamp o marche temporali, che identificano ogni transazione con un proprio codice unico sequenziale, rafforzato da un protocollo digitale di conferme. Ogni transazione viene identificata con una marca temporale e inserita in un insieme di dati chiamato blocco. La transazione economica si avvia come in attesa di convalida e cambia stato, solo quando viene trovato un riscontro in un elenco di marche temporali (timestamp) gestito collettivamente dalla rete peer-to-peer in cui sono contenute tutte le transazioni delle criptovalute. Questo registro (libro mastro), enorme,

condiviso pubblicamente e garantito tramite crittografia, è conosciuto con il temine Blockchain o catena dei blocchi e fa sì che la criptovaluta sia legittima e consistente, così da garantirne l'uso e consentire i pagamenti.

Nella sostanza, nell'estesissimo libro mastro sono indicate informazioni come: l'emissione della valuta, il relativo controvalore con soldi fisici, chi ne era il proprietario, chi ne è diventato il nuovo a seguito di una transazione, garantendone l'anonimato, e molte altre. Il libro mastro, quindi i blocchi o le Blockchain, rappresentano la certezza del dato e la sostenibilità che internazionalmente è stata riconosciuta alle monete come il Bitcoin. Con la nostra app abbiamo implementato delle soluzioni che ci permettono di far parte di questo enorme libro mastro. L'adozione delle Blockchain rende il "sigillo" posto al documento che si intende conservare probatorio ed opponibile come deve essere un documento digitale conservato a norma.