BLOCKCHAIN NELLA FILIERA ALIMENTARE: EVOLUZIONE, RIVOLUZIONE O ILLUSIONE?[1]

La tecnologia *blockchain*, apparsa nel 2009 come supporto tecnologico della moneta virtuale bitcoin, è stata classificata negli ultimi anni come la gran rivoluzione che cambierà l'economia e il modo di fare business. Nel 2014, Marc Andreessen, co-fondatore di Netscape e inventore del primo browser web, classificò bitcoin (e la tecnologia di supporto, *blockchain*) come l'invenzione tecnologica più importante dalla creazione di Internet nel 1993. The Economist ha definito *blockchain* come *"la grande catena per essere sicuri delle cose"*[2]*,* affermando che *"la tecnologia che supporta bitcoin consente alle persone che non si conoscono o non si fidano l'un l'altro di costruire un rapporto affidabile, e questo ha implicazioni che vanno ben oltre la criptovaluta*".

PERCHÉ ABBIAMO BISOGNO DI UNA TECNOLOGIA COME BLOCKCHAIN?[3]

Secondo il documento originale che lo descrive[4], *"Bitcoin è un sistema di denaro elettronico che consente di effettuare pagamenti online tra individui (peer-to-peer) senza dover passare attraverso un istituto finanziario"*. In altre parole, bitcoin consente transazioni economiche senza l'intervento di un "intermediario di fiducia". La tecnologia *blockchain* è stata inventata per supportare questa valuta elettronica. Perché è necessaria?

Immaginiamo che, nel mondo del denaro fisico, Mario voglia effettuare il pagamento di un euro a Giulia. Mario consegna la moneta a Giulia e la transazione viene

[1] Caso presentato dai professori Jose Antonio Boccherini Bogert. Per la scrittura del presente caso sono state impiegate informazioni ottenute in giornali, riviste settoriali e studi debitamente citati. Luglio 2022.

[2] "The great chain of being sure about things", The Economist, 31 ottobre 2015, https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things (consultato l'11 febbraio 2019.).

[3] Questa sezione è un adattamento della spiegazione contenuta nel documento "What is blockchain technology?", CB Insights, 11 settembre 2018. Il documento può essere scaricato in https://www.cbinsights.com/research/what-is-blockchain-technology/.

[4] Nakamoto,S., "Bitcoin: a Peer-to-Peer Electronic Cash System", 31 de octubre de 2008, https://bitcoin.org/bitcoin.pdf, consultato l'11 febbraio 2019. Satoshi Nakamoto è uno pseudonimo. Il documento è stato pubblicato su una mailing list da un programmatore o un gruppo di programmatori che operavano sotto quello pseudonimo e rimangono anonimi fino ad oggi.

completata in modo sicuro. Dopo la transazione, Mario non possiede più la moneta, ora la possiede Giulia. Entrambi non hanno bisogno di un intermediario che verifichi la validità della transazione. Inoltre, Mario non potrebbe più dare la stessa moneta a Laura per effettuare un altro pagamento, perché essa non è più in suo possesso. Non è possibile effettuare un doppio pagamento con la stessa moneta e vengono così garantite le condizioni che forniscono valore alla moneta: la sua appartenenza può essere certificata, ma rimane una risorsa scarsa.

Cosa succederebbe se quella moneta non fosse fisica, ma digitale? Mario potrebbe inviare la moneta digitale a Giulia via e-mail (ad esempio) per effettuare il pagamento. Quindi Giulia dovrebbe possedere quella moneta digitale e Mario non dovrebbe più averla. Ma cosa succederebbe se Mario conservasse una copia di quella moneta digitale prima di inviarla a Giulia e la usasse nuovamente per effettuare altri pagamenti? Una moneta digitale, infatti, non è altro che una sequenza di zeri e uno; è quindi facilmente copiabile. Se non si trovasse una soluzione a questo problema, le monete virtuali mancherebbero di valore e utilità.

Se Mario e Giulia sono in possesso della stessa sequenza di zeri e uno, come è possibile sapere chi è il legittimo proprietario della moneta? Una possibile soluzione è utilizzare un registro digitale (un ledger, in inglese) in cui vengono riportate le transazioni e ciò confermerebbe in qualsiasi momento chi è il legittimo proprietario. Quindi, se Mario ha effettuato un pagamento a Giulia, il registro segnalerà che quella moneta ora appartiene a Giulia e non più a Mario.

Ma chi gestisce questo registro? Non può essere Mario, perché potrebbe cancellare la nota della transazione e sostenere di essere ancora il proprietario della moneta. Per ragioni analoghe, non può essere Giulia. Una soluzione potrebbe essere quella di utilizzare un intermediario, una terza parte (chiamiamolo Leonardo), di cui si fidino sia Mario che Giulia, che annoti la transazione e tenga aggiornato il registro.

In un certo senso, questo è ciò che accade oggi con la maggior parte dei pagamenti effettuati tramite bonifico bancario. Il denaro è un registro contabile, ed è quindi digitale. Un bonifico è semplicemente una transazione elettronica che sottrae un importo dal conto della persona che paga e lo aggiunge al conto della persona che riceve. La transazione viene effettuata da una terza parte di fiducia (la banca), che attesta che il saldo di entrambi i conti è corretto. Al giorno d'oggi, la maggior parte delle persone in paesi con sistemi bancari sviluppati ripone in esse la propria fiducia.

Ma Leonardo (l'intermediario di fiducia tra Mario e Giulia) potrebbe iniziare a far pagare una commissione per il suo lavoro che né Giulia né Mario sono disposti a pagare; oppure Mario potrebbe ricattare Leonardo per cancellare la transazione e recuperare così la sua moneta digitale; o ancora, Leonardo potrebbe non essere affidabile e rubare la moneta, aggiungendo una falsa transazione al registro per fingere che Mario gli abbia dato la moneta.

In altre parole, che cosa succederebbe se Mario e Giulia non volessero pagare commissioni all'intermediario o non si fidassero di lui? Una possibile soluzione sarebbe

quella di distribuire copie del registro a più amici, decentralizzando la fiducia. Dato che il registro è digitale, tutte le copie dovrebbero essere sincronizzate e ogni nuova transazione dovrebbe essere aggiornata in tutte le copie contemporaneamente. Se una maggioranza semplice dei partecipanti dichiara che la transazione è valida (ovvero che Mario è il legittimo proprietario della moneta con cui vuole pagare Giulia), essa viene approvata e aggiunta al registro.

Ciò viene chiamato registro distribuito (distributed ledger, in inglese). Se Mario o Giulia volessero falsificare una transazione, dovrebbero ricattare la maggior parte dei partecipanti o modificare la maggior parte delle copie del registro, il che risulterebbe molto complicato. E Leonardo avrebbe solo una delle copie del registro; se lo modificasse per cercare di rubare la moneta, il registro non risulterebbe sincronizzato con le altre copie e la falsificazione verrebbe rilevata.

Più sono “le persone di fiducia” che possiedono una copia del registro, più esso sarà sicuro e affidabile. Questo sistema, quindi, consente di instaurare un rapporto di fiducia tra parti che non si conoscono e che non sono necessariamente affidabili individualmente. Se più della metà dei partecipanti sono onesti e affidabili, la sicurezza è assoluta. Ma anche se non lo fossero, falsificare la registrazione in modo che la contraffazione risulti coerente nella maggior parte delle copie del registro e venga considerata valida sarebbe difficile per chiunque ci provasse.

Nell'esempio precedente, i partecipanti che conservavano una copia del documento erano "amici" e, perciò, relativamente affidabili. In bitcoin, invece, il registro è completamente pubblico e chiunque può partecipare e conservare una copia. Pertanto, il rischio di partecipanti malintenzionati e transazioni false è maggiore.

La soluzione offerta da bitcoin è quella di premiare i partecipanti onesti e punire i malintenzionati. Alcuni partecipanti alla rete bitcoin (chiamati "minatori") ricevono incentivi per fare il "lavoro sporco" al fine di garantire la validità del registro. Quando viene aggiunta una nuova transazione, i minatori competono per adattare la transazione nella struttura del registro, risolvendo un puzzle matematico volutamente complesso che richiede un enorme sforzo di calcolo. Il primo che risolve il problema riceve una ricompensa in bitcoin, a seguito della verifica e dell’approvazione da parte di almeno il 51% dei restanti minatori. Dato il prezzo che i bitcoin hanno raggiunto, questo è un grande incentivo. In questo modo, i contraffattori sono scoraggiati, perché registrare una transazione falsa richiederebbe un enorme sforzo di calcolo, un enorme dispendio di elettricità e, quindi, tanti soldi (molto più di quanto si otterrebbe con la contraffazione). Ma anche se la rete bitcoin fosse falsificata in modo accettabile, il risultato sarebbe il più grande disincentivo: il valore della valuta finirebbe per crollare bruscamente e, di conseguenza, la possibile ricompensa dei contraffattori svanirebbe.

CHE COS'È LA TECNOLOGIA BLOCKCHAIN?

Blockchain (catena di blocchi), la tecnologia che supporta bitcoin, ha molte potenziali applicazioni oltre alla criptovaluta. Essa permette la creazione di registri digitali di