

*Gentile famiglia, ecco il Suo*

# BOLLETTINO UFFICIALE MUNICIPALE

anno 25 | numero 3 | **MARZO** 2018



CITTÀ DI SAN BENEDETTO DEL TRONTO



SANDBEA.RU

# Internet per le nonne

## Qui si batte la moneta

di Antonio Prado\*

**T**utti lo dicono, tutti ne parlano, qualcuno se lo domanda: cos'è *Bitcoin*? I più informati sanno che è una moneta virtuale, cioè, in parole povere, che non si tocca.

Giusto, ma *Bitcoin* è molto di più e tenterò durante le poche righe di questo trafiletto di raccontarne il funzionamento.

Partiamo dal principio, o quasi, cioè da un fatto ormai assodato e universalmente riconosciuto: l'utilità della moneta nel mondo moderno. Chi dimentica le banconote di carta delle nonne (o bisnonne forse), veri e propri lenzuoli di carta da conservare gelosamente ripiegati cento volte nel petto?

Oggi girano meno contanti sostituiti dalle carte di credito, cioè tesserine di plastica in grado di pagare beni e servizi con un addebito diretto sul conto corrente bancario. Già, le banche: aziende che fanno da intermediari tra noi e il denaro e che su questa attività generano profitti.

Detto diversamente, l'euro che abbiamo in sacoccia vale proprio uno; quello che depositiamo in banca non vale più uno, ma poco meno. Accettiamo che l'istituto di credito trattenga la differenza pur di poter fruire di alcuni servizi come la sicurezza dei nostri risparmi, la possibilità di prelevare contanti da qualsiasi sportello del mondo ecc.

Sarebbe un sogno se potessimo fruire di quei servizi togliendo di mezzo l'intermediario, cioè le banche. Oggi, o meglio dal 2009, il sogno si è avverato per opera di tale Satoshi Nakamoto. Nessuno sa se sia un lui o una lei, se sia un singolo o un gruppo, se sia uno scienziato o un imprenditore. È un nome sul quale si è a lungo investigato ma che tuttora rimane sconosciuto. Conosciutissimo invece è il suo studio del 2008 intitolato appunto "*Bitcoin: un sistema di contante elettronico senza intermediari*". Tutto il lavoro presuppone l'esistenza della rete Internet, la diffusione dei calcolatori elettronici e la partecipazione di milioni di internauti.

La base fondante di questa nuova moneta elettronica è un meccanismo chiamato catena a blocchi (*blockchain* in inglese). Immagiamola come una vera e propria catena che, anziché essere costituita di maglie, abbia delle scatole ciascuna delle quali sia incatenata alla precedente e alla seguente attraverso un forte anello di congiunzione.



disegno di Belinda Menzietti

Ora poniamo che nonna Maria voglia regalare 10 soldi a ciascuno dei nipotini Giuseppina, Alessandro, Luca, Marco, Antonio; come potrebbe farlo usando questa diavoleria?

Semplice, scriviamo su un registro (che tutti i ragionieri conoscono): da Maria a Giuseppina 10; da Maria ad Alessandro 10; da Maria a Luca 10 e così via. Alla fine risulterà che ciascun nipote avrà 10 soldi in più e che nonna Maria avrà 50 soldi in meno. Tutti d'accordo firmano la pagina del registro e la infilano nella prima scatola vuota disponibile della catena.

Questa operazione, che chiamiamo transazione, viene contrassegnata da un codice assai complesso e stampigliato sulla scatola di Maria e dei nipoti. Sulla stessa viene però stampato anche il codice complesso della scatola immediatamente precedente. Ovviamente chi riempirà la seguente nella catena dovrà scrivere il codice della scatola di nonna Maria così da averle tutte concatenate l'una all'altra.

Insomma, un libro mastro di migliaia di pagine che contiene tutte le transazioni avvenute, ma proprio tutte tutte, cioè dal 2009 a oggi.

La caratteristica del sistema teorizzato da Nakamoto sta nel fatto che chiunque voglia partecipare all'uso di *Bitcoin* deve disporre di un software (cioè un programma o anche una *app*) che prima di poter essere usato deve avere una copia di tutto il libro mastro. In questi giorni l'intera catena (cioè il registro o libro mastro) contiene un volume di dati pari a circa tre volte l'intero scibile della versione inglese di *Wikipedia*, l'enciclopedia *on-line*.

Dunque, tutta la catena a blocchi viene replicata milioni di volte quanti sono gli utenti della valuta elettronica, sempre uguale a sé stessa e sempre aggiornata e sincronizzata.

Al di là di strampalate manie complottistiche, possiamo concludere che proprio questa catena a blocchi protetta da codici crittografici, distribuita a chiunque, sia la più grande garanzia di trasparenza (le transazioni sono visibili a tutti), affidabilità (perché non governata da un'autorità centrale), convenienza (non ci sono intermediari), solidità (le informazioni sulle transazioni non possono essere modificate con facilità), irrevocabilità (le transazioni non possono essere annullate).

Il meccanismo *blockchain* costituisce il fondamento per altre cosiddette criptovalute come *Bitcoin: Litecoin, Dash, Ether* e molte altre.

Ciascuna ha il proprio portafoglio (software) contraddistinto da un lunghissima stringa di numeri e lettere. Per aprirlo ci vengono date delle chiavi con le quali riceviamo, conserviamo o inviamo denaro.

Ma attenzione a non perdere le chiavi: nessuno ve ne potrà dare una copia e tanto meno nessuno potrà accedere al vostro portafoglio ed eventualmente restituirvi l'unico *Bitcoin* in esso contenuto (che oggi vale poco più di ottomila euro).

Nel prossimo numero vi scriverò di: *Fake news*

\*Giornalista, Chief Digital Officer Servizio Infrastrutture Digitali