UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M. FANNO"

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

"Criptovalute e Blockchain: la finanza del futuro è digitale?"

RELATORE:

CH.MO PROF. BERTONI MARCO

LAUREANDO: MANFRIN ANDREA

MATRICOLA N. 1113067

ANNO ACCADEMICO 2017 – 2018

"Intorno al 2005, diverrà chiaro che l'impatto di Internet sull'economia non è stato superiore a quello del fax"

Paul Krugman, 1998

INDICE

Introduzione

Nell'ottobre del 2008, poche settimane dopo la ratifica dell'Emergency Economic Stabilization Act, un'entità nota con lo pseudonimo di Satoshi Nakamoto, di cui non è ancora stata appurata l'identità, introdusse un sistema di pagamento elettronico basato su un network di utenti, invece che sulla fiducia tra le parti, la reputazione o la supervisione di un regolatore esterno, così permettendo a due soggetti di negoziare direttamente tra loro senza la necessità di un intermediario. Lo scopo era di tagliare i costi di transazione e rimuovere la componente umana della funzione di controllo, aumentando la sicurezza degli scambi. La moneta utilizzata negli scambi venne chiamata "bitcoin", la prima e tuttora più famosa criptovaluta.

Il bitcoin si impose come una valuta immateriale e, per le caratteristiche del sistema entro cui veniva scambiata e generata, non controllata da una banca centrale, governo o autorità di alcun tipo, bensì da algoritmi strutturati in maniera tale da rendere ogni transazione sicura e trasparente.

Il suo valore non è regolato dalla solvenza di uno Stato e non può nemmeno essere alterato direttamente da politiche fiscali o monetarie.

Tra entusiasmo e controversie, il Bitcoin (ovvero il sistema che si regge sui bitcoin e che ne permette lo scambio) è divenuto un'industria da decine di miliardi di euro, innescando un processo di imitazione e perfezionamento che ha portato alla creazione di numerose concorrenti; tra queste l'ether (sistema Ethereum), il bitcoin cash (appartenente al Bitcoin Cash) e il litecoin (criptomoneta del Litecoin).

Questo ha consentito alle criptovalute, verso fine 2017, di avere una capitalizzazione di mercato totale di circa 800 miliardi di dollari americani, crollata poi nei primi mesi del 2018 fino a raggiungere circa i 300 miliardi ad aprile e 220 miliardi nei primi giorni di ottobre (coinmarketcap.com).

Tuttavia, l'interesse per le criptovalute e la tecnologia che ne supporta l'utilizzo, nota come Blockchain, rimangono alti, spingendo governi e banche ad indagarne la natura per capire i possibili utilizzi e conseguenti rischi.
"Le monete virtuali, in particolare il bitcoin, hanno catturato l'immaginazione di alcuni, hanno impaurito altri e confuso alla grande il resto di noi, me incluso"; così si esprimeva il Senatore degli Stati Uniti Thomas Carper, Presidente del Comitato della Sicurezza e degli Affari Governativi il 18 novembre 2013.

Lo scopo di questo lavoro è di presentare in maniera introduttiva i diversi aspetti economici delle criptovalute e della Blockchain. Il documento si suddivide in 5 sezioni:

- Nel primo capitolo si illustrano i concetti di criptovaluta e Blockchain, e si descrive il loro funzionamento;
- Nel secondo capitolo viene analizzato l'impatto che le criptovalute potrebbero avere sull'economia, esaminando il loro ruolo di denaro alternativo, il loro rapporto con la criminalità, la regolamentazione che l'UE ha elaborato per controllare questa connessione e gli effetti che potrebbe avere la creazione di una criptovaluta controllata dalla Banca Centrale;
- Nel terzo capitolo si esaminano benefici, applicazioni ed ostacoli al successo della Blockchain, nonché la possibilità che essa non sia veramente innovativa;
- Nel quarto capitolo si tenta di spiegare il successo del mercato delle criptomonete nel 2017, guardando a due fattori che potrebbero giustificare le fluttuazioni di prezzo di questa classe di asset;
- Il quinto capitolo conclude il documento con alcune osservazioni ed ipotesi sul futuro di questa tecnologia.

1. Criptovalute e Blockchain: cosa sono?

Criptovalute

Le criptovalute sono una famiglia, non del tutto omogenea, di valute digitali scambiabili sul web, di cui il bitcoin è il membro più noto ed anziano.

Ci sono infatti anche alcune criptovalute private, soggette a permessi che rappresentano un caso particolare del mercato in quanto non aderiscono all'ideale di decentralizzazione estrema connessa agli esemplari più noti.

Un altro fattore di distinzione è il processo attraverso il quale viene aumentata la quantità di valuta circolante.

In seguito verranno trattate le caratteristiche delle criptomonete pubbliche basate sul modello introdotto dal bitcoin (pur essendo dotate di peculiarità che le differenziano le une dalle altre).

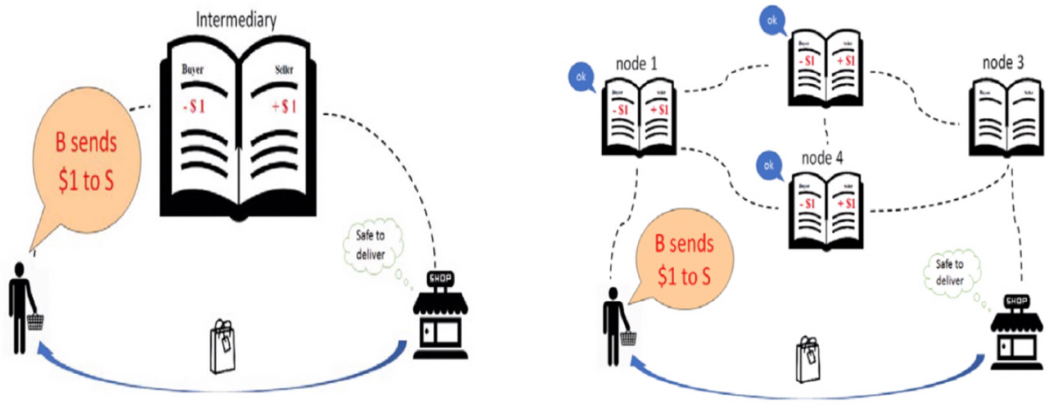
Come spiegato da Satoshi Nakamoto nel documento con il quale aveva introdotto la sua invenzione (Nakamoto 2008), il sistema Bitcoin funziona attraverso il network che viene a formarsi tra i computer di tutti gli utenti connessi. Il Bitcoin, come gli altri sistemi per lo scambio di criptovalute che lo hanno usato come modello, non consiste di banche o società controllate da manager, bensì di sistemi di pagamento internazionali completamente digitalizzati e decentralizzati: software open source che consentono agli utenti di scambiare liberamente le monete digitali, registrando tutte le transazioni avvenute e rendendole pubbliche. Transazioni in moneta virtuale sono possibili in qualsiasi momento e luogo, per l'acquisto di beni reali o virtuali, senza l'intermediazione di una terza parte che assicuri che il denaro utilizzato per i pagamenti non sia già stato speso o che le transazioni vengano alterate ex-post.

La sicurezza è garantita dalla tecnologia che funge da pilastro centrale di questo sistema, la Blockchain: è per mezzo di essa che si effettuano le transazioni.

Per utilizzare le criptovalute bisogna innanzitutto dotarsi di un portafoglio digitale dove immagazzinare le criptomonete, rappresentato da un software o hardware, a seconda delle necessità dell'utente. Le transazioni avvengono poi attraverso la Blockchain. I pagamenti consistono nello spostamento di criptovaluta da un portafoglio digitale all'altro di qualsiasi utente che sia interessato a scambiarle.

Token digitali regolati da intermediario (es. PayPal)

Token digitali in un sistema decentralizzato (es. Bitcoin)



Fonte: (Chiu e Koeppl, 2017, p.4)

Secondo i loro sostenitori, i punti di forza delle criptovalute sono molteplici:

- la possibilità da esse offerta di rimuovere il "middle man" tagliando costi di transazione, come le commissioni richieste dall'intermediario;
- l'aumento del livello di sicurezza del sistema, sostituendo corruttibili e fallibili controllori umani con algoritmi e crittografia capaci di assicurare trasparenza e irreversibilità delle transazioni, richiedendo una quantità di informazioni minore rispetto alle banche
- la possibilità di compiere transazioni che varchino i confini nazionali senza dover richiedere permessi rilasciati da autorità estere;
- la possibilità di usare pseudonimi per proteggere l'identità degli utenti;
- la capacità di integrare (quando non ne fosse già dotata alla nascita) strumenti chiamati smart contracts, di cui si discuterà nel capitolo riservato alla Blockchain, incrementando notevolmente la flessibilità delle contrattazioni tra le parti, risolvendo problemi classici di selezione avversa senza costi aggiuntivi.

Le criptovalute sono al momento deregolamentate in molti stati ed escluse dalla sfera di influenza di politiche fiscali e monetarie. La loro stessa emissione non è regolata dallo Stato, Banca Centrale, società o altra autorità centralizzata, bensì dagli utenti del network attraverso metodi alternativi, a seconda della Blockchain su cui operano. Il più utilizzato, quello dei bitcoin, è il mining: il miner ottiene una certa quantità di criptovaluta "nuova" risolvendo un puzzle di codici prodotto dal sistema stesso, aumentando dunque il numero di bitcoin in circolazione.

Per le sue caratteristiche, la criptovaluta fa appello a tre gruppi distinti di clienti.

Un gruppo è composto da appassionati di tecnologia che adottano i bitcoin per il commercio sulla rete. Poiché sempre più transazioni commerciali di routine migrano online, questi utenti

ritengono che il valore delle criptovalute dovrebbe aumentare a causa della domanda di transazioni e citano anche i loro vantaggi in termini di costi rispetto alle carte di credito e ad altri sistemi di pagamento per la normale vendita al dettaglio.

Un secondo gruppo, con credenze politiche di stampo libertario, trova allettante l'idea di una valuta sconnessa da qualsiasi governo. Alcuni di questi aderenti diffidano apertamente del sistema finanziario mondiale, e la tempistica dell'introduzione di bitcoin, che coincide con la fase più critica della crisi finanziaria globale, ha probabilmente contribuito ad infittire le loro fila. Andreas Antonopoulos, un noto sostenitore del bitcoin e CSO di Blockchain.info (una piattaforma che funge da portafoglio digitale e banca dati con statistiche e informazioni sul mercato critpo), rispondendo alla congettura che il 10% dei bitcoin esistenti a marzo 2014 fosse già stato trafugato da hacker, disse: "… un enorme miglioramento rispetto al resto della nostra economia, dove l'80% è nelle mani dei criminali, e loro possiedono le banche" (Is Bitcoin a Flash in the Pan?, 2014, minuto 8:14).

Il terzo gruppo è composto da individui che vedono nelle criptovalute un espediente per commerciare illegalmente, a causa della protezione della privacy e dunque dell'anonimato che esse, in maniera più o meno efficace, garantiscono, come nel caso del sito di transazioni illegali "Silk Road", di cui si discuterà in seguito nella sezione riservata al riciclaggio di denaro e Deep Web.

Blockchain

La vera fonte di innovazione non deriva però dalle criptovalute, bensì da ciò che consente di utilizzarle per i pagamenti: la Blockchain. Bitcoin ed altcoin (alternative coins, termine che si riferisce ad ogni criptovaluta che non sia il bitcoin) sono soltanto l'ultima forma di denaro dematerializzato, utilizzabile anche attraverso carte di credito e debito, bonifici bancari ecc. I benefici specifici di cui godono le criptomonete dipendono dalle caratteristiche della Blockchain.

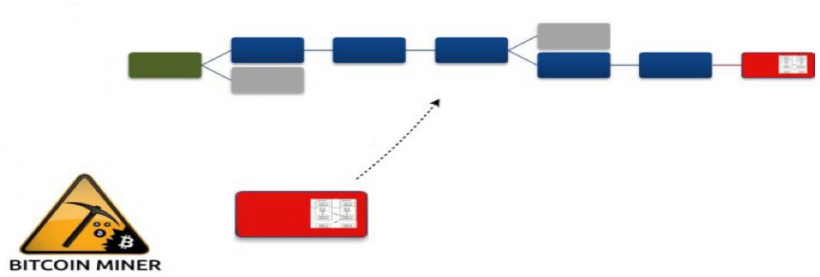
Ma cos'è la Blockchain?

Malgrado non esista una definizione precisa e globalmente condivisa di Blockchain (Halaburda 2016), quella più ampia e normalmente utilizzata la delinea come un database distribuito (che si appoggia sul menzionato network di utenti), che registra transazioni, diritti di proprietà e descrizioni di asset; nella maggioranza dei casi, non richiede alcun tipo di permesso per l'accesso (esistono Blockchain private), rendendo le informazioni contenute trasparenti e pubbliche, affinché tutti gli utenti possano esaminarle.

È importante sottolineare come la Blockchain non sia un server, cioè una piattaforma che fornisce servizi in mano ad una società o ad un individuo. Non esiste una sala contenente gli hardware che supportano le funzionalità della Blockchain; ciononostante, può lavorare in concomitanza con piattaforme come mercati di scambio di criptovalute o portafogli digitali, pur mantenendo la sua indipendenza e le sue caratteristiche intatte.
La tecnologia Blockchain può teoricamente esistere senza una criptovaluta, tanto che si è arrivati a discutere le potenziali applicazioni della Blockchain al di fuori del contesto criptomonete.
Come si mostrerà nel capitolo riservato alle applicazioni della Blockchain, Google è solo una di molte aziende che sta esplorando il potenziale di questa tecnologia.

All'interno del contesto criptovalute, la Blockchain funge da libro mastro costantemente aggiornato che memorizza le transazioni effettuate e le informazioni che le contraddistinguono: in primis i codici che individuano i portafogli delle due parti, la quantità scambiata, il momento in cui avviene lo scambio. Queste informazioni vengono raccolte in "blocchi" (blocks) che, venendo innestati l'uno dopo l'altro in ordine cronologico, formano una "catena" (chain) estendibile all'infinito.
Il principale pericolo in cui incorre un venditore che accetti moneta virtuale è quello del double-spending: un compratore potrebbe spendere l'intero contenuto del suo portafoglio in più transazioni separate ma effettuate simultaneamente. Un utente dotato di un solo bitcoin, per esempio, potrebbe spenderlo in una moltitudine di acquisti contemporaneamente: di tutti i venditori, solo uno vedrebbe il bitcoin spostarsi nel proprio portafoglio, mentre gli altri perderebbero il loro asset senza ricevere un pagamento. Non esistendo una sorta di autorità centrale o Clearing House che possa sventare il piano del compratore fraudolento o risarcire i venditori danneggiati, si verrebbe a formare una situazione di Moral Hazard in cui nessun utente si sentirebbe al sicuro nell'accettare criptovaluta, causando il collasso del sistema.
La Blockchain è strutturata per affrontare proprio questo tipo di problema.
Come spiega Nakamoto, la Blockchain è costituita da blocchi, ognuno contenente un certo numero di transazioni considerate simultanee dal sistema al momento del loro inserimento nel blocco. Ogni blocco di questa catena viene approvato dai nodi del network attraverso un meccanismo a maggioranza, ovvero attraverso l'approvazione della maggioranza dei computer del network. Quando un nuovo blocco viene approvato, esso diventa l'ultimo anello della Blockchain. Due transazioni contrastanti non possono appartenere allo stesso blocco e una transazione che appartiene ad un blocco successivo ad un altro non può entrare in contrasto con una transazione di quest'ultimo.

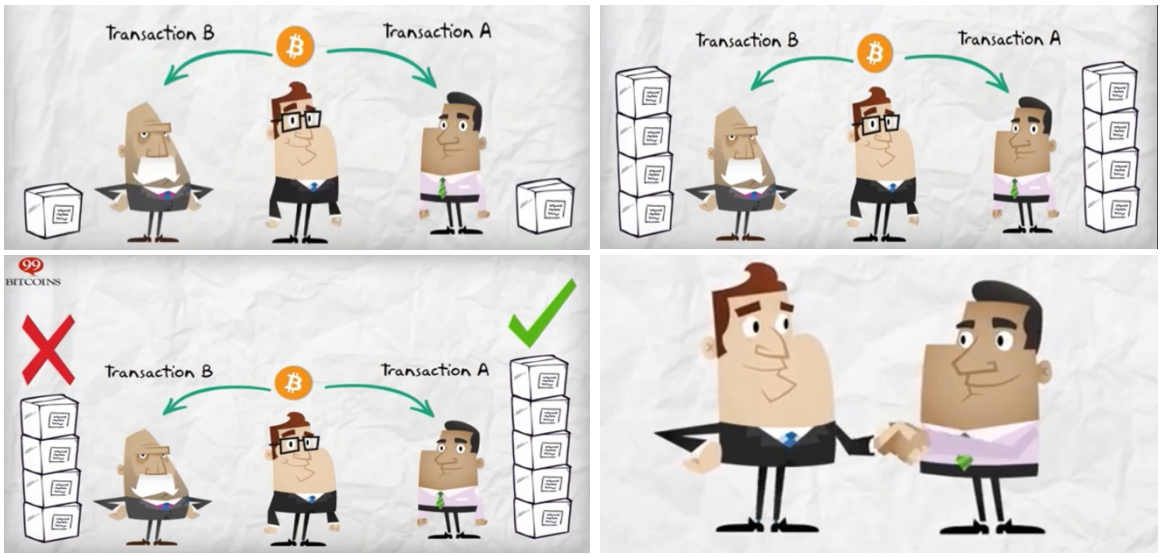
Se più blocchi contenenti diverse transazioni simultanee del cliente fraudolento vengono approvati contemporaneamente, la catena assume tante biforcazioni quanti sono i blocchi, ognuno valido quanto gli altri. A quel punto, inizia la gara per aggiungere il successivo blocco. Poiché il network riconosce (a maggioranza) come valida soltanto la biforcazione più lunga della catena, respingendo le altre, la prima delle biforcazioni a vedere l'aggiunta di un nuovo blocco diventa la catena vera e propria, mentre le altre vengono rigettate e annullate, invalidando dunque i blocchi e le transazioni che li compongono.



Fonte: Instituto Nacional de Ciberseguridad de España S.A. (INCIBE) (2014)

Se più biforcazioni dovessero approvare in contemporanea il secondo blocco, inizierebbe la gara per il terzo, e così via.

Dopo 6 blocchi, la possibilità che si ripresenti il problema, e che quindi si accetti criptovaluta spesa più volte, è pressoché inesistente. (immagini: 99bitcoins.com)



Poiché la Blockchain consente l'uso di smart contracts (strumenti speciali di cui si discuterà capitolo riservata alla Blockchain), un venditore può fissare il momento di alienazione del bene in maniera tale da avere almeno 6 blocchi confermati oltre quello della propria transazione (circa 1 ora, nel sistema Bitcoin).

Meccanismo del consenso

Per approvare i blocchi, la Blockchain implementa un meccanismo del consenso che può variare in base al sistema adottato: il Bitcoin richiede il cosiddetto "proof-of-work", ma esistono numerose alternative, tra cui spicca per popolarità il "proof-of-stake" (che verrà trattato in seguito).

Il più comune meccanismo del consenso, il proof-of-work, è strettamente collegato al mining: ogni transazione, prima di essere raggruppata con altre in un blocco (all'interno del quale tutte le transazioni vengono considerate simultanee), non è confermata, quindi non è immutabile. Per farla diventare parte della Blockchain, occorre che un nuovo blocco venga aggiunto: il "miner" è colui che gareggia con gli altri miner per ottenere il diritto di aggiungere il blocco di transazioni. La "gara" consiste in un lavoro di decrittazione, che si sostanzia nel risolvere un puzzle crittografico generato dal sistema della Blockchain. Risolto il puzzle, il miner può selezionare transazioni (ai suoi occhi tutte uguali) e inserirle nel blocco che sta aggiungendo alla Blockchain.

Alcuni utenti potrebbero legare delle piccole commissioni alle loro transazioni, in modo da invogliare i miner a includerle con priorità. Questo meccanismo rende il tempo di approvazione più lungo, e può portare le transazioni senza commissioni a rimanere prive di conferma per lungo tempo, evidenziando la possibile inadeguatezza del proof-of-work nel sostenere grandi volumi di transazioni. Allo stesso tempo, il proof-of-work garantisce che la modifica della Blockchain sia proibitivamente costosa, scoraggiando gli hacker dall'attaccarla e rendendola virtualmente impossibile da falsificare: il network riconosce come valida soltanto la catena più lunga, cosicché per poter manomettere un blocco (per alterare a proprio vantaggio una transazione) occorre modificare anche tutti quelli successivi, compresi quelli che stanno venendo approvati, generando una catena "fraudolenta" più lunga di quella legittima. Una tale azione richiede grande potere computazionale e implica un notevole dispendio di risorse, in primis energia elettrica.

Il mining può essere effettuato da chiunque abbia una macchina adatta, ma per i suoi costi (installazione delle macchine, energia elettrica e sistema di raffreddamento) e la quantità di lavoro necessaria, spinge i miner a raggrupparsi in pools, dividendo il carico di lavoro e la ricompensa tra i membri.

Il sistema presenta un punto debole, per quanto difficile da sfruttare: controllando la maggior parte della potenza di calcolo sulla rete, un attaccante o un gruppo di aggressori può interferire con il processo di registrazione di nuovi blocchi. Se ad esempio un pool o un singolo utente avessero accesso a più del 50% del potere computazionale del network, potrebbero effettuare un cosiddetto "51% attack": avrebbero il potere di impedire agli altri

minatori di aggiungere i blocchi, monopolizzandone l'aggiunta e guadagnando tutti i premi. Cambiare i blocchi già approvati prima dell'inizio dell'attacco rimarrebbe estremamente difficile anche nel caso di un attacco del 51%, in quanto dovrebbe essere sostituito ogni blocco successivo a quello che si vuole modificare, il che richiederebbe grandi quantità di tempo ed energia. Più le transazioni sono indietro nella catena, più difficile è manometterle.
Il mining pool “ghash.io” superò per breve tempo il 50% della potenza di calcolo del network Bitcoin nel 2014, inducendo i membri ad impegnarsi volontariamente a ridurre la quota, dichiarando in seguito che si sarebbero tenuti al di sotto del 40% della potenza mineraria totale in futuro (Wilhelm 2014).

Il vantaggio della Blockchain, rispetto al sistema tradizionale che si affida ad una autorità centrale, risiede nel taglio dei costi e nella possibilità di ogni utente passato e presente di visionare un database incorruttibile e che non può essere distrutto. Il controllo viene spostato dalla supervisione di banche e intermediari all’automazione di algoritmi noti e al lavoro di un network che trae profitto dal seguire le regole, invece che dal violarle.

2. L’impatto delle criptovalute sull’economia

La criptomoneta è moneta?

Le criptovalute vogliono proporsi come forma innovativa di moneta scambiabile: la valuta digitale per un mercato sempre più digitale. Ma possono davvero essere considerate una forma di denaro?

Come afferma David Yermack (2013), bitcoin e altcoin vanno innanzitutto valutati a livello dei 3 ruoli generalmente assegnati al denaro dagli economisti: riserva di valore, unità di conto e mezzo di scambio.

- Riserva di valore

  In quanto riserva di valore, la criptomoneta affronta due sfide: la sicurezza e la volatilità.

  La sicurezza del portafoglio digitale, dentro cui le criptovalute vengono immagazzinate, non è la stessa di cui gode la Blockchain: per esempio, la catena di Bitcoin non è mai stata violata dal 2009, ma sono avvenuti numerosi furti di criptovaluta dai portafogli digitali dei detentori.

  Uno di questi quello alla piattaforma Coincheck: in una conferenza stampa del 26 Gennaio 2018, i dirigenti hanno ammesso un furto di oltre 500 milioni di NEM (una criptovaluta meno nota), per un valore di circa 530 milioni di dollari (al momento dell'hack), arrivando a superare il record negativo stabilito da Mt.Gox nel 2014, che vide una perdita di circa 850.000 bitcoin, per un valore di circa 450 milioni di dollari americani (in quel momento). (Wilmoth 2018).

  Alcune società che si occupano di questo servizio (indispensabile per trattare criptovalute) hanno contrattato forme grezze di assicurazione con dei terzi: mentre questa formula funziona in teoria, costringe il cliente a sostenere il costo della valutazione della sicurezza della società di portafogli e della compagnia assicurativa.

  Ammettendo di aver trovato un modo sicuro ed economico di conservare i propri bitcoin, bitcoin cash, ether o altra valuta, l’individuo dovrà fare i conti con la notevole volatilità che contraddistingue la categoria.

  Il prezzo delle criptovalute cambia notevolmente nel corso di brevi periodi di tempo, arrivando a variare anche di svariati punti percentuali in sole 24 ore. Su Coinbase, una delle principali piattaforme di scambio di criptovalute, nonché portafoglio digitale (www.coinbase.com), bitcoin crebbe di valore, nel corso del 2017, partendo da meno di 1000 dollari (americani) e arrivando a toccare i 19.400 dollari a metà Dicembre, per poi crollare nel corso dei 2 mesi successivi, arrivando a 6900 dollari il 5 Febbraio. Prima ancora della fine del 2017, il prezzo era sceso a circa 12.250 dollari. Tra il 4 e l’8 Gennaio il prezzo calò da 15.155 a 14.970 dollari, toccando però una punta di 17.135 dollari il 6.

Valori simili possono delineare il bitcoin come un interessante investimento speculativo, ma scoraggiano un consumatore che cerca stabilità. E il bitcoin non è l'unico caso: tra il primo giorno del 2018 e l'inizio di Febbraio, il costo di un ether aveva toccato punte di 1380 dollari così come fondi sotto gli 850 dollari.
Il 17 Ottobre 2018, alle 14:20, i dati di Coinbase mostravano una variazione del +0,2% del valore in euro del bitcoin rispetto all'ora precedente, +0,28% per ether, -0,09% per litecoin. Il prezzo in euro del bitcoin segnava una diminuzione del 1,23% rispetto alla settimana precedente.

Studi sulla volatilità del prezzo dei bitcoin non sono conclusivi: alcuni delineano una sostanziale prevalenza della componente "bolla" rispetto ai fondamentali, arrivando addirittura a sostenere che il valore intrinseco del bitcoin è nullo (Cheah e Fry 2015); altri, come quello di Kristoufek (2015), riconoscono l'importanza di fondamentali quali uso nelle transazioni e la quantità circolante. In particolare, quest'ultimo studio evidenzia due effetti contrastanti nella correlazione tra il prezzo del bitcoin e il numero di transazioni per cui viene utilizzato: maggiore l'uso dei bitcoin per acquisti di beni e servizi, maggiore la domanda di questa criptovaluta e quindi il prezzo; allo stesso tempo, all'aumentare del prezzo aumenta l'insicurezza rispetto alla criptomoneta e quindi ne diminuisce l'utilizzo. Inoltre, un maggior numero di transazioni rende più costose le commissioni per i miner e più lenta l'approvazione dei pagamenti, riducendo la domanda di bitcoin. Lo studio afferma che l'effetto positivo prevale, anche se si indebolisce col tempo. Tuttavia, il valore del bitcoin è aumentato sensibilmente rispetto al 2015. Lo studio sottolinea inoltre come la correlazione tra prezzo e volume totale delle transazioni continui a variare nel tempo, impedendo di trarre conclusioni.
Lo stesso studio pone inoltre l'attenzione sul prezzo del bitcoin in quanto investimento: poiché è considerato un "investimento sicuro", viene considerata la correlazione tra il suo prezzo e il Financial Stress Index (FSI) in quanto "indice generale di incertezza finanziaria" (Kristoufek 2015, p.10), trovando che non vi è connessione statisticamente rilevante, eccetto nel periodo della crisi finanziaria cipriota del 2012-2013. Anche con il prezzo dell'oro (considerato una efficace riserva di valore di lungo periodo) in franchi svizzeri (scelti per la notevole stabilità di questa valuta) il prezzo del bitcoin non mostra una correlazione.
Jamal Bouoiyour e Refk Selmi (2017) sottolineano, infine, come il mercato cinese abbia riposto al deterioramento del renminbi cinese contro il dollaro americano prestando maggiore interesse nei confronti del bitcoin, che si è apprezzato.

Gli accademici concordano comunque sul fatto che l'interesse degli speculatori ha un notevole effetto sul prezzo del bitcoin.

- Unità di conto

  A causa della loro notevole volatilità, le criptovalute godono di una scarsa performance come unità di conto: un venditore che accettasse, per esempio, bitcoin, dovrebbe costantemente ricalibrare i prezzi in bitcoin in base al fluttuante tasso di scambio con la valuta nazionale. Questa pratica non solo si tradurrebbe in un costo per il business, ma causerebbe notevole disagio ai clienti.

  Il problema diventa evidente quando si esamina il primo acquisto di un bene in bitcoin della storia: le "pizze di Lazlo" (Wallace 2011) acquistate per 10.000 bitcoin nel 2009. A novembre 2010, il tasso di cambio era passato da 0,004 a 0,26 dollari (+6400%): conservare i bitcoin invece che spenderli avrebbe fatto guadagnare all'anonimo compratore circa 2600 dollari. Attualmente, le due pizze hanno un valore di decine di milioni di dollari.

  Un altro fattore da considerare è il costo relativamente elevatissimo di un bitcoin rispetto alla maggior parte dei prodotti e servizi ordinari. Questo problema riguarda soprattutto, ma non soltanto, il bitcoin, in quanto di gran lunga più costoso di qualsiasi altra criptovaluta: al 17/10/2018 circa 32,8 volte più costoso in euro dell'ether e 15 volte più del bitcoin cash, rispettivamente terza e seconda criptovaluta più costosa.

  Al 9/10/2018 il prezzo di un bitcoin su Coinbase è circa 5734 euro (1 euro = 0,000174398 bitcoin); questo implica transazioni nell'ordine di cinque o sei cifre decimali per l'acquisto di beni del valore di pochi centesimi. Il problema aumenterebbe se il prezzo del bitcoin tornasse ai picchi di fine 2017, quando toccò i 16.490 euro. Commerciare in frazioni di bitcoin è possibile fino all'ottava cifra decimale, ma nella pratica sarebbe estremamente confusionario.

- Mezzo di scambio

  In quanto immateriale e non coniata da un'autorità centrale universalmente accettata, la criptovaluta non ha un valore intrinseco: esso dipende dall'utilità che gli utenti della rete le imputano come mezzo di scambio nell'economia.

  È semplice constatare il numero di transazioni effettuate attraverso una criptovaluta popolare come il bitcoin in un determinato periodo di tempo: possiamo ad esempio osservare come venisse scambiato centinaia di migliaia di volte giornalmente nel periodo Dicembre 2017 – Gennaio 2018, arrivando al picco di quasi 500.000 transazioni

giornaliere e di come, il 3-4 Ottobre 2018, sia stato scambiato circa 237.000 volte al giorno (blockchain.com). Notevolmente più complesso, se non impossibile, è individuare quanti di questi movimenti riflettano acquisti di beni e servizi, piuttosto che scambi con denaro tradizionale o altre criptovalute a scopi speculativi, o semplici spostamenti tra portafogli digitali appartenenti allo stesso proprietario.

Si potrebbe guardare al numero di venditori e organizzazioni che accettano bitcoin come forma di pagamento (99bitcoins.com): dal "Coupa Café" a Palo Alto al KFC in Canada, dall'Old Fritzroy (un pub in Australia) a Subway, da ShopJoy alla libreria del MIT, la lista è varia, ma non molto lunga. Il consumatore medio non paga al supermercato o al bar con il portafoglio digitale, né prenota alloggi e viaggi utilizzando criptovaluta.

Non mancano, tuttavia, le eccezioni: il caso più emblematico in Italia è quello della cosiddetta "bitcoin valley", situata nei pressi di Rovereto. Una zona dove un numero insolitamente alto di esercizi e consumatori scambiano bitcoin: merito anche di inbitcoin, azienda italiana che sviluppa prodotti e servizi per l'uso dei bitcoin, che ha promosso l'iniziativa nominata proprio "bitcoin valley" per pubblicizzare e diffondere l'uso di questa criptovaluta nel territorio. La loro mission è quella di fornire servizi e prodotti che si basino sul bitcoin, alle grandi imprese come ai piccoli negozi fisici, per "sfruttare al meglio questa tecnologia dirompente" (inbitcoin.it); la loro vision è che il processo di disintermediazione promosso dal bitcoin stravolgerà la vita di tutti i giorni più di Uber e Bla Bla Car. Nella bitcoin valley vi è oramai una quantità di esercizi che accettano bitcoin per i pagamenti, mentre alcuni lavoratori del bar Mani al Cielo, di Gianpaolo Rossi, chiedono di essere stipendiati, in tutto o in parte, in bitcoin.

"Ci sono anche dei punti fisici, i Compro Euro, che, un po' come i Compro Oro, permettono di cambiare gli euro con i bitcoin grazie a dei bancomat che accettano le banconote e le trasformano in criptovaluta, … Sono anche dei punti di formazione per "diffondere fiducia", dove si possono anche solo fare due chiacchiere con persone in carne ed ossa, fare domande, soddisfare la propria curiosità su cosa sono queste monete un po' criptiche". (Gozzi 2018).

L'ostacolo principale alla diffusione del bitcoin non è tanto l'implementazione di apparecchiature che possano consentirne l'uso nella vendita al dettaglio, bensì la volatilità di questa classe di asset, che scoraggia i commercianti dall'adottarla, soprattutto in seguito alla repentina discesa dopo la crescita sensazionale di Novembre-Dicembre 2017.

Le criptovalute sono tra loro differenti, quindi differenti sono le loro propensioni a diventare moneta universalmente accettata, ma è evidente che una criptomoneta che cercasse di imporsi

dovrebbe risolvere il problema della notevole volatilità comunemente associata a questo genere di asset, espandere la fiducia di cui gode la Blockchain fino ai portafogli digitali (il che richiederebbe anche una maggiore consapevolezza del pubblico riguardo il loro funzionamento), e avere un valore non troppo elevato rispetto a quello dei beni destinati ad essere comprati giornalmente dalla classe media.

Un importante, se non indispensabile aiuto, potrebbe arrivare dal settore bancario e governativo. Un notevole ostacolo alla collaborazione è il problema del riciclo di denaro: mentre è vero che qualsiasi valuta, dall'euro al dollaro americano, digitale o sotto forma di carta stampata, non può dirsi immune da questo rischio, le criptovalute sono particolarmente predisposte a celare e proteggere i proventi di attività illegali.

Criptovalute e criminalità

Rob Wainwright, direttore dell'Europol, ha affermato: "Loro [criptovalute] non sono banche e non sono governate da un'autorità centrale, quindi la polizia non può monitorare tali transazioni. E se le identificano come criminali, non hanno modo di congelare le risorse come nel normale sistema bancario" (Corcoran 2018).

La promessa di un libro mastro decentralizzato con transazioni verificabili in modo indipendente ha un enorme appeal, specialmente in un'epoca in cui la gestione centralizzata suscita preoccupazioni sia per hacking dall'esterno che per la manipolazione interna. Eppure, la maggioranza delle transazioni avvengono su piattaforme centralizzate, come Coinbase o Bitfinex, dove le criptovalute vengono scambiate con denaro tradizionale. Questi scambi operano in gran parte al di fuori della portata delle autorità di regolamentazione finanziaria e offrono livelli variabili di trasparenza limitata.

Limitata trasparenza sembra essere un problema ricorrente: come detto precedentemente, un utente del sistema Bitcoin gode di un certo anonimato, in quanto il pubblico può vedere che in un determinato momento una certa somma viene scambiata, ma non ha a disposizione informazioni che riconducano alla persona coinvolta: "È simile al livello di informazioni diffuse dalle borse, dove il tempo e le dimensioni dei singoli scambi, il "nastro", sono resi pubblici, ma senza dire chi erano le parti" (Nakamoto 2008). Questo pone un notevole problema per i regolatori e, conseguentemente, anche a quelli che sperano in una cooperazione tra criptovalute e mondo della finanza: transazioni "secretate" possono servire a confondere gli investigatori in merito all'origine di fondi, oltre che a semplificare l'evasione fiscale, dato che il fisco non sa chi deve tassare.

È bene specificare che il grado di anonimato di cui gli utenti godono è variabile, spaziando dall'anonimato completo allo pseudo-anonimato (Houben e Snyers 2018): bitcoin (come altcoin con grande capitalizzazione di mercato come ether, bitcoin cash, litecoin e XRP) è pseudo-anonimo, in quanto, con grande utilizzo di risorse e capacità tecniche, è possibile risalire all'identità di un utilizzatore da una transazione. Un esempio di altcoin totalmente anonimo è il dash, che consente di utilizzare una feature denominata PrivateSend, che protegge totalmente la privacy di un utente.

La protezione dell'anonimato, sia essa assoluta o meno, delinea le criptovalute come i "paradisi fiscali del domani", nonché come strumenti per il riciclo di denaro e addirittura finanziamento del terrorismo, come nel caso di Ali Shukri Amin, che spiegò via Twitter come usare Bitcoin per mascherare donazioni all'ISIS (FATF 2015).

Il metodo per rintracciare utilizzatori di criptomonete pseudo-anonime è utile, ma è troppo laborioso per divenire la risposta generale al problema. Il fatto che la Blockchain non sia limitata dai confini nazionali aggrava il pericolo, in quanto il riciclaggio potrebbe avvenire in paesi dotati di un insufficiente apparato per individuare e combattere riciclaggio di denaro e finanziamento del terrorismo.

Il caso più emblematico e famoso di attività illecite condotte attraverso l'uso di criptovalute è quello di Silk Road: quest'ultimo era il più grande mercato nero del web (Ruiz Cabrera 2016), situato nel Deep Web (una parte della rete inaccessibile per il comune utente, covo di commercio illegale e materiale censurato dal governo), dove si vendevano narcotici, armi e contratti di assassinio. Silk Road fungeva da intermediario tra le parti, che rimanevano anonime ed effettuavano pagamenti esclusivamente in bitcoin. Il sito fu chiuso nell'Ottobre 2013 in seguito all'arresto del fondatore, Ross Ulbricht, colto in fragrante mentre si offriva di pagare 80.000 dollari per l'assassinio di un suo collaboratore, arrestato in precedenza. Per consentire l'arresto fu necessaria la collaborazione tra FBI e Google, una lunga operazione sotto copertura, numerosi errori grossolani da parte di Ulbricht e una certa dose di fortuna nello scoprire l'esistenza del sito, avvenuta quando un agente si imbatté in domande sospette (poste da Ulbricht stesso per farsi pubblicità) su un forum dedicato ai bitcoin.

Nei suoi due anni di attività, Ulbricht aveva guadagnato circa 18 milioni di dollari di commissioni sulle transazioni.

Casi come quello di Silk Road hanno evidenziato la necessità di implementare un sistema di leggi che possa scongiurare l'abuso di questa tecnologia, ma la mancanza di un organismo centrale sul quale focalizzare gli sforzi ha spinto a chiedersi quali attori debbano essere regolamentati e come si possa rimuovere il velo di anonimato che ricopre le transazioni sulla

Blockchain. La possibilità che misure troppo stringenti soffocassero l'innovazione prima ancora che realizzasse il suo pieno potenziale hanno reso ancora più difficile intervenire.

Regolamentazione UE

Negli ultimi anni, i governi della zona europea si sono mobilitati: nel 26 Giugno 2017, la Commissione Europea rilasciò il "Supranational Risk Assessment", che conteneva la raccomandazione agli Stati Membri di inserire le criptovalute nel campo d'azione dell'AMLD4 (Quarta revisione della Direttiva contro il riciclaggio di denaro), aggiungendo le piattaforme di scambio di criptovalute e i fornitori di portafogli digitali alla lista di enti indicata nell'articolo 4. In quest'ultimo sono incluse banche, istituti finanziari, agenzie immobiliari e altre professioni o categorie suscettibili di divenire mezzo per riciclo di denaro o finanziamento del terrorismo. Gli enti che presentano queste caratteristiche sono sottoposti a particolare sorveglianza e tenuti ad una serie di obblighi, tra i quali quello di svolgere la "dovuta diligenza" nello stabilire una relazione d'affari e nell'effettuare una transazione occasionale che ammonta a 15.000 euro o più, indipendentemente da eventuali deroghe o esenzioni. Nel caso si verifichino queste condizioni, l'ente dovrà appurare l'identità del cliente.

In generale, se vi sono sospetti di attività illecite, è obbligatoria la comunicazione all'unità di intelligence finanziaria competente, che ogni Stato Membro deve costituire. Sono previste sanzioni per chi contravviene a queste norme.

La Commissione Europea ha sottolineato alcune potenziali risposte al problema dell'anonimato (Houben e Snyers 2018):

- Registrazione obbligatoria degli utenti.
- Registrazione volontaria degli utenti.
- Forzare le piattaforme di acquisto e vendita di criptovaluta e i fornitori di portafogli digitali ad adibire all'articolo 4 dell'AMLD4.
- Forzare le piattaforme di acquisto e vendita di criptovaluta e i fornitori di portafogli digitali a sottostare alla PSD2 (Seconda revisione della Direttiva sui Servizi di Pagamento), che è più stringente dell'AMLD4 in quanto impone, oltre agli stessi obblighi, anche il rispetto di valori minimi di capitale, dei requisiti di salvaguardia e delle regole per la protezione dei consumatori, nonché il conseguimento di una licenza.

Gli Stati Membri hanno espresso favore nei confronti della terza opzione, mentre hanno rigettato la quarta per paura che ciò avrebbe legittimato, agli occhi del pubblico, le valute

virtuali, inducendo i consumatori a riporre la loro fiducia in strumenti che non vengono ritenuti sicuri e affidabili dai supervisori finanziari.

Sull'onda di queste decisioni, è stata recentemente approvata la AMLD5 (Revisione della sopracitata Anti-Money Laundering Directive 4), la cui effettiva applicazione inizierà il 20 gennaio 2018 che e che racchiude anche regolamentazione specifica in merito alle criptovalute.

"… AMLD5 non ha solo esteso il suo campo d'azione alle piattaforme di scambio di valute virtuali e ai fornitori di portafogli (compresi gli obblighi di registrare presso le autorità nazionali anti-riciclaggio, introdurre controlli con dovuta diligenza dei clienti, monitorare regolarmente le transazioni valutarie virtuali e segnalare attività sospette alle entità governative), ma chiede inoltre che gli Stati Membri creino banche dati centrali comprendenti identità degli utenti di valute virtuali e indirizzi di portafoglio, nonché moduli di auto-dichiarazione presentati da utenti di valuta virtuale." (GSMA 2018, p.13).

La criptovaluta emessa da una Banca Centrale

Immaginiamo che uno Stato decida di abbracciare la criptovaluta e la tecnologia Blockchain: una Banca Centrale dovrebbe innanzitutto analizzare in quali ambiti potrebbe beneficiare dell'introduzione di una criptomoneta. Come sottolineato da Ben S.C. Fung e Hanna Halaburda (2016), potrebbe innanzitutto voler:

- Migliorare l'efficienza dei pagamenti retail e di quelli di grande valore (anche pagamenti interbancari);
- Implementare una risposta adeguata all'introduzione di criptovalute decentralizzate, limitando i loro effetti destabilizzanti ed evitando di perdere il primato sul controllo della valuta circolante;
- Riuscire, potenzialmente, ad introdurre politiche capaci di portare i tassi di interesse sotto lo zero-lower-bound.

Le principali inefficienze del mercato che potrebbero essere risolte dalle criptovalute sono:

- Sicurezza: su internet come attraverso il POS, un venditore disonesto potrebbe abusare dei dati della carta di credito o debito del cliente; un hacker potrebbe attaccare l'account PayPal, avendo accesso a carte di pagamento e perfino all'account bancario.
- Commissioni: specialmente nel caso di transazioni di valore molto ridotto, potrebbero spingere i venditori a non offrire determinati prodotti online. L'assenza di commissioni rappresenterebbe un vantaggio rispetto al POS per il business.

- Costi non monetari: un cliente che dovesse pagare in contante senza averne a sufficienza a portata di mano potrebbe decidere di non portare a termine la transazione; inserire una grande quantità di dati per eseguire una transazione online potrebbe portare via molto tempo, specie se la connessione dovesse interrompersi momentaneamente, azzerando I progressi.

Come visto in precedenza, gli altcoin potrebbero fornire una soluzione ad alcuni di questi problemi: la Blockchain rappresenta una forma molto sicura per scambiare valore, priva di commissioni e in grado di supportare transazioni di qualsiasi portata senza richiedere informazioni sull'utente.
Si è anche visto, però, che le criptovalute non possono assicurare totale sicurezza per quanto riguarda i portafogli, e possono dimostrarsi poco pratiche per transazioni di basso valore, oltre a essere molto volatili.

Anche se i consumatori cominciassero ad adottare le criptovalute in massa, diversificando in base alle proprie preferenze, i competitor oggettivamente migliori non diverrebbero necessariamente i più popolari. Come molti altri mercati, anche quello dei sistemi di pagamento viene influenzato dall'economia di rete: una forma di moneta virtuale potrebbe incontrare una barriera all'entrata invalicabile nella presenza di giganti quali Bitcoin, per il cosiddetto "effetto rinforzo" (Gandal e Halaburda 2014, p.9): più è popolare una valuta, più è utile e dunque attraente per nuovi utenti. Pertanto, ci si potrebbe aspettare che le criptovalute più popolari diventino ancora più popolari, fino a dominare l'intero mercato.

Per arrivare alla soluzione più efficiente potrebbe essere necessario l'intervento delle autorità pubbliche, attraverso la regolamentazione o l'introduzione di una criptovaluta controllata dalla banca centrale dello Stato. Un vantaggio di una CVBC (CriptoValuta della Banca Centrale) sarebbe quello di poter risolvere il problema della volatilità di questi asset, grazie all'impegno della Banca Centrale di fissare il tasso di cambio: questo consentirebbe di utilizzarla come mezzo di pagamento invece che come rischioso investimento.
Se una Banca Centrale debba emettere o meno la propria esclusiva criptovaluta è una questione aperta, che va affrontata in parallelo a quella delle caratteristiche che questa forma di denaro dovrebbe avere.
Innanzitutto, dovrebbe essere consentito scambiare criptovaluta con banconote o depositi in valuta nazionale presso la stessa Banca Centrale. Inoltre dovrebbe essere iscritta, come le altre voci del passivo del bilancio, sotto forma del suo valore corrispettivo in valuta nazionale.

Altre caratteristiche sarebbero determinate dai motivi che spingerebbero all'emissione della CVBC, in quanto nel progettarla, si incontrerebbero una serie di trade-off:

- Il livello di anonimato garantito conforterebbe alcuni utenti, dando un livello di sicurezza simile a quello del denaro contante, ma renderebbe ancora più facile riciclare il denaro o evadere le tasse.
- Mettere un tetto alla quantità di valuta contenuta in un portafoglio in un determinato momento potrebbe mettere al riparo gli utenti dal rischio di furto o di perdita accidentale, oltre che a intralciare eventuali tentativi di riciclaggio; per alcuni utenti potrebbe risultare come un notevole intralcio, tuttavia, poiché renderebbe difficile o impossibile effettuare determinate transazioni.
- La BC dovrebbe prendere la difficile decisione in merito all'affidarsi alla tecnologia Blockchain o fungere da intermediario: nel secondo caso, verrebbe a mancare una delle principali attrattive degli altcoin, mentre nel primo occorrerebbe designare un sistema inespugnabile ed efficiente, soprattutto per quanto riguarda il meccanismo del consenso.
- Nel caso venisse adottata la Blockchain, occorrerebbe regolare la dimensione dei blocchi e il tempo approvazione, caratteristiche che determinano la velocità di elaborazione delle transazioni e la sicurezza (maggiore velocità implica minore potere computazionale necessario, quindi maggiore rischio di sabotaggio). Velocità e sicurezza caratterizzerebbero l'entità delle transazioni che si effettuano su quella Blockchain.

Introdurre una tecnologia così innovativa comporta una varietà di sviluppi difficili da prevedere, ma John Barrdear e Michael Kumhof (2016) anticipano alcuni potenziali effetti collaterali.

- Tassi d'interesse

  L'acquisizione finanziata da CVBC di debito pubblico ridurrebbe la quantità di debito a rischio di default in mano ai privati, abbassando il rischio di credito associato, causando quindi un decremento dei tassi di interesse sul debito pubblico, portando potenzialmente a maggiore accumulo di capitale e dunque crescita economica. Questa ipotesi è però controbilanciata da un rischio strutturale: con l'uso di criptovaluta verrebbe ridotto l'utilizzo dei depositi bancari, il principale strumento con cui le banche finanziano nuovi prestiti. Aumenterebbe dunque il costo del finanziamento del sistema bancario e, di conseguenza, l'entità degli oneri per coloro che prendono a prestito.
- Sviluppo tecnologico

  Adottare un sistema di pagamento decentralizzato, in cui diventare un nodo (verificatore di transazioni, come i miner nel Bitcoin) costa meno che fondare una banca, stimolerebbe

la competizione tra sistemi di verifica, promuovendo il più efficiente. Crescerebbe inoltre la competizione da parte del mercato dei depositi bancari.

- Too Big To Fail

  Una CVBC spoglierebbe le banche della loro aura di insostituibilità, dovuta al loro ruolo chiave nel sistema dei pagamenti, ammortizzando l'impatto sui clienti in caso di fallimento.

In definitiva, molte sono le variabili da considerare nel decidere sull'emissione di una CVBC, e non è certo quale sarebbe il risultato. La complessità e innovatività della tecnologia rendono difficile prevederne gli sviluppi.

"Mentre sembra chiaro che alcuni rischi sarebbero attenuati, altri rischi emergerebbero, e non è certo quale sarebbe maggiore. ... Tuttavia, esiste un rischio di stabilità finanziario molto chiaro, quello di gestire malamente la transizione verso un nuovo ambiente monetario e finanziario non ancora testato" (Barrdear e Kumhof 2016, p.16).

3. La Blockchain può cambiare il futuro?

Se l'impatto delle criptovalute sull'economia è incerto, occorre chiedersi se l'adozione di una parte di questo sistema, la Blockchain, potrebbe invece produrre risultati prevedibili ed eventualmente positivi.

Come detto in precedenza, la Blockchain è considerata la parte veramente innovativa del sistema Bitcoin (e dei competitori): in quanto tale, si potrebbe pensare di sviluppare la tecnologia separatamente dalle criptovalute che l'hanno resa famosa.

I benefici

È complesso discutere dei vantaggi della Blockchain in generale, in quanto ne esistono svariati esemplari diversi, ma si può sottolineare una serie di benefici che la categoria di Blockchain pubbliche nella sua interezza porta con sé (Natarajan, Krause e Gradstein 2017).

La già menzionata decentralizzazione dovrebbe ridurre i costi di intermediazione, nell'esecuzione delle transazioni, nella stipula dei contratti e nella risoluzione di dispute, dove ridurrebbe il tempo necessario per riconciliare le due parti. Infatti la transazione è trasparente e già approvata dal network, senza bisogno di un elemento che prenda ulteriori decisioni e le comunichi agli altri. Le caratteristiche tecniche della Blockchain (crittografia, smart contract) consentono inoltre di elaborare contratti molto complessi e flessibili, le cui clausole verrebbero implementate automaticamente dal sistema, e che risultano a prova di hack.

Il fulcro della popolarità della Blockchain risiede dunque nel potenziale della "verifica distribuita e senza costi": "Con blockchain, invece, Internet può anche fungere da canale di sicurezza tra terze parti non fidate … una criptovaluta può creare un mercato senza la necessità di intermediari tradizionali. Ad esempio, Bitcoin può imitare la funzionalità di base delle reti finanziarie SWIFT o ACH senza utilizzare banche o istituti controllati o nodi affidabili" (Catalini e Gans 2016, p.4).

La Blockchain gode di alcune proprietà che le consentono di conseguire la verifica distribuita a costo zero:

- Atomicità

  Una delle proprietà riconosciute ad una transazione (Gray 1981), esige che tutti i passaggi logici di un'operazione siano eseguiti, pena l'annullamento di tutti gli altri: per esempio, uno spostamento di fondi che rispetti questa proprietà esige che la somma venga sottratta da un account e aggiunta ad un altro, affinché l'operazione complessiva venga portata a termine.

L’atomicità è parte integrante del sistema, che può anche essere supportato con smart contracts: programmi computerizzati che implementano automaticamente le clausole contrattuali approvate dai contraenti, senza bisogno di intervento umano.

Gli smart contracts sono uno degli elementi più promettenti della tecnologia Blockchain, aprendo la strada ad una varietà di contratti flessibili: i contraenti potrebbero accordarsi sull’usare software o hardware (oracoli) connessi a smart contracts per risolvere le dispute: per esempio, si potrebbe stipulare un accordo che regola i cash flow tra le due parti in base alle condizioni meteorologiche ad una data futura in un determinato luogo, usando un programma che, alla data stabilita, sincronizza i dati di diversi canali meteo per decidere il risultato, piuttosto che un singolo macchinario che registri fisicamente le condizioni sul luogo prescelto alla data prescelta.

- Protezione della privacy e gestione delle informazioni

  Vi è un rischio nell’affidare le proprie informazioni a intermediari: questi potrebbero venderle o inavvertitamente lasciare che vengano rubate. La tecnologia Blockchain può ridurre questo rischio consentendo l'autenticazione senza divulgazione di informazioni sensibili.

  Allo stesso modo in cui può essere usata per tracciare gli attributi delle transazioni finanziarie, questa tecnologia può anche memorizzare le modifiche dello status o delle credenziali di un individuo: informazioni su di una persona potrebbero essere registrate su una Blockchain e richieste, quando necessario, da una terza parte, magari dietro pagamento. Ancora, potrebbe essere dato un accesso temporaneo alle proprie informazioni. Aumenterebbe dunque la sicurezza, oltre che a crearsi lo spazio per nuovi modelli di business fondati su domanda e offerta di informazioni.

Applicazioni al di fuori del contesto delle criptovalute

Che sia attraverso la progettazione di Blockchain private (non del tutto aperte) o la creazione di strumenti che sfruttino quelle già esistenti e prive di permessi, numerose aziende stanno progettando soluzioni che si basino sulla Blockchain.

In particolare, il settore finanziario ha cominciato a sperimentare le potenzialità di questa tecnologia (Natarajan, Krause e Gradstein 2017):

- NASDAQ, NYSE, LSE e borse valori in tutto il mondo stanno testando la capacità della Blockchain di rendere più efficiente il trading.

- Nel mese di dicembre 2015, la US Securities Exchange Commission ha approvato la proposta di Overstock.com di emettere azioni della società tramite la Blockchain del Bitcoin.
- La banca centrale tedesca e la società per la gestione di titoli azionari “Deutsche Börse” hanno ideato un nuovo esemplare di Blockchain per il commercio di beni digitali. Lo scopo della ricerca era quello di dimostrare che fosse possibile condurre su una Blockchain un ciclo completo di emissione di titoli, effettuazione di operazioni societarie e riscatto, nonché di portare a termine trasferimenti di denaro tra i partecipanti. Secondo Cointelegraph (Berman 2018), all'interno del resoconto sono stati evidenziati i principali vantaggi e svantaggi della tecnologia Blockchain. Tra i punti deboli sono stati evidenziati i lunghi tempi di latenza e l'alto utilizzo di potenza di calcolo per portare a termine alcune operazioni; la robustezza dell'ecosistema e i costi ridotti sono stati invece menzionati tra i maggiori benefici.

  Al termine della fase di sperimentazione, Deutsche Bundesbank e Deutsche Börse sono arrivate alla conclusione che le soluzioni decentralizzate dovrebbero essere adattate per andare incontro alle necessità dei mercati finanziari. A tal proposito, le due istituzioni hanno notato che gli sviluppatori di numerose soluzioni decentralizzate hanno recentemente migliorato le proprie offerte, personalizzando le Blockchain così da offrire risposte a problemi specifici.
- La Borsa di Tokyo e IBM stanno testando la blockchain per registrare negoziazioni.
- La borsa valori della Corea del Sud ha lanciato, nel novembre 2016, un mercato basato su blockchain per azioni di startup, denominato Korea Startup Market, in partnership con la start-up Blocko. L'amministratore delegato di Blocko ha descritto questo come il "primo esempio" di come la Blockchain potrebbe essere utilizzata.

Un’altra potenziale applicazione della Blockchain potrebbe stabilire un nuovo standard per la protezione dei dati personali: mantenere le informazioni in modo decentralizzato rende più difficile collegare le informazioni alla persona a cui si riferiscono.
Tra le più interessanti applicazioni pratiche del connubio tra immagazzinamento di dati personali e Blockchain troviamo due prodotti:

- ShoCard: emessa da una società di Palo Alto, è una carta d'identità digitale, ottimizzata per dispositivi mobili, che memorizza le informazioni ID sulla Blockchain Bitcoin. La società sta sviluppando soluzioni per casi d'uso come: verifica dell'identità negli aeroporti e nei call center, credenziali di servizi finanziari, registrazioni automatizzate per acquisti online, prova di età e indirizzo (ad es. alle fermate della polizia).

Carte d'identità, passaporti, patenti o singole tessere che svolgano tutte queste funzioni contemporaneamente e che si connettono direttamente alla Blockchain potrebbero rendere obsoleti i documenti cartacei, più facilmente falsificabili ed esposti al furto.

- BanQu: La società Blockchain BanQu fornisce una "identità economica" alle persone memorizzando l'identità e altre informazioni critiche, inclusi dati biometrici, sulla Blockchain di Ethereum. BanQu presta particolare attenzione ai paesi in via di sviluppo, e sta testando l'identità digitale in un certo numero di progetti, tra cui quello di fornire un'identità digitale ai rifugiati siriani ad Amman, implementare assicurazioni sulle micro-colture attraverso smart contracts e compensare le falle nella supply chain della fornitura di farmaci e vaccini.

La Blockchain può anche rendere più efficiente la supply chain di un'impresa: i dati riguardanti l'origine dei beni, la loro attuale posizione e le loro caratteristiche sarebbero localizzati sulla catena, alla portata di tutti, godendo di trasparenza, rintracciabilità e accessibilità in misura superiore agli odierni sistemi, le cui inefficienze derivano dal distacco tra database di proprietà dei fornitori e quelli dei clienti. Anche nel caso di un'impresa integrata verticalmente, potrebbe risultare ottimale poter condividere con consumatori finali e partner le informazioni.

La possibilità di registrare e rendere trasparenti i diritti di proprietà di azioni societarie nelle Blockchain con un organismo centrale consentirebbe di "personalizzare" la quantità di informazioni che i membri possono visionare e che sono costretti a condividere col pubblico, in modo da creare un equilibrio tra gli azionisti che desiderano restare anonimi e quelli che vorrebbero più trasparenza. (Yermack 2015) Una compagnia potrebbe decidere di essere presente su diverse Blockchain, attirando investitori con diverse preferenze in fatto di trasparenza.

I sistemi fondati su Blockchain forniscono una piattaforma che consente agli smart contracts, scritti in codice informatico, di controllare effettivamente le risorse del mondo reale, come proprietà immobiliari, azioni, titoli di terra o impegni, senza la necessità di una terza parte che controlli il rilascio dell'asset come broker, amministratori di titoli fondiari o agenti di deposito a garanzia.
Grazie a questi contratti intelligenti, le clausole contrattuali possono essere fatte valere automaticamente con maggiore rapidità e minori costi:

- In un contratto di leasing di un'auto si potrebbe collegare la chiave del mezzo allo smart contract, cosicché se l'utilizzatore salta un pagamento al concedente, la chiave viene automaticamente "bloccata", impedendo di usare il mezzo.
- Un utente potrebbe essere pagato automaticamente via Blockchain per l'esecuzione di piccoli incarichi, come rispondere ad un questionario o scrivere una recensione. Sarebbe possibile regolare il pagamento in base a dei criteri, come i voti dati alla recensione dai lettori.
- Un'altra applicazione potrebbe essere distribuire smartphone con una capacità, seppur piccola, di mining, affinché l'utente possa ripagare il proprio stesso piano telefonico fornendo automaticamente potere computazionale all'operatore.
- In uno scenario futuristico, una vettura a guida autonoma potrebbe acquistare in tempo reale spazio su un'autostrada per acquisire priorità rispetto agli altri veicoli.

Risulta evidente come la Blockchain apra dunque la strada alla nascita di nuovi contratti e nuovi modelli di business, caratterizzati flessibilità e trasparenza, ma anche sicurezza, senza però richiedere aumenti di costi, talvolta addirittura riducendoli.

Le sfide

La Blockchain è una tecnologia innovativa, e come tale deve affrontare degli ostacoli per affermarsi:

- Integrazione

  Le Blockchain devono integrarsi l'una con l'altra, oltre che con altri sistemi già esistenti, per potersi affermare sul sistema finanziario. Questo richiede interoperabilità tra Blockchain con caratteristiche diverse, in primis per quanto riguarda il meccanismo del consenso (come menzionato in precedenza, il mining è il più popolare ma non è l'unico); occorre ammantare l'efficacia degli smart contracts di validità legale (ciò che è tecnicamente eseguibile non è automaticamente riconosciuto come legittimo a livello giuridico, basti pensare alle criptovalute stesse); è necessario fornire un portale attraverso il quale i regolatori possano acquisire informazioni più approfondite su determinate transazioni.

- Governance

  La Blockchain potrebbe sollevare problemi di governance nelle organizzazioni che la implementano (Yermack 2015):

- Una modifica alla Blockchain del bitcoin o di simili criptovalute può essere effettuata semplicemente attraverso l'adozione di più di metà degli utenti (ponderata per il loro potere computazionale), cosa che consente di rigettare proposte dannose per il sistema, ma che potrebbe consentire ad un malintenzionato di ingannare il network, proponendo una modifica che venga intesa come benigna dalla maggior parte dei partecipanti, per poi rivelarsi maligna. La mancanza di un regolatore aumenta questo tipo di rischio di sabotaggio.
- Non è chiaro a chi spetti il potere decisionale in caso di situazioni di emergenza. Anche nel caso di una Blockchain dotata di permessi (quindi non del tutto aperta), l'amministratore potrebbe non avere i mezzi tecnici per applicare efficacemente il suo volere ai nodi del network.
- Anche ammettendo che si trovasse un regolatore centrale dotato di ampi poteri, verrebbe tradito l'intento di rendere obsolete queste figure e i rischi ad esse associate (comportamenti scorretti, possibili errori non correggibili dal network), ovvero il motivo per cui Nakamoto (2008) aveva elaborato la Blockchain.

- Problema del meccanismo del consenso

  Come detto in precedenza, il Bitcoin utilizza il lavoro dei miner per aggiungere nuovi blocchi alla Blockchain. Il processo è sicuro, ma comporta degli inconvenienti: la ridotta dimensione dei blocchi fa sì che il numero di transazioni elaborate in un singolo secondo sia particolarmente limitato. Bitcoin, tra le Blockchain più lente, è in grado di processare al massimo 7 transazioni in un secondo (Natarajan, Krause e Gradstein 2017), mentre l'approvazione di un blocco richiede in media circa 10 minuti.

  Come se non bastasse, è noto che le criptovalute hanno un limite massimo di unità circolanti: i bitcoin, per esempio, non possono superare i 21 milioni. Anche se il raggiungimento del limite massimo per una determinata criptovaluta è molto distante nel futuro, quando questo dovesse arrivare non sarebbe più possibile creare nuove unità. I miner, dunque, dovrebbero essere ricompensati per il loro lavoro con le commissioni che gli utenti annettono alle loro transazioni. Quando il sistema era agli inizi, il numero ridotto di pagamenti rendeva queste commissioni superflue ma, all'aumentare degli acquisti, gli utenti hanno cominciato a sentire sempre più il bisogno di pagare per vedere approvate il prima possibile le proprie transazioni, fermentando una crescita del valore delle commissioni stesse.

  Questo problema, denominato "scaling problem", risulta particolarmente evidente se si confronta il bitcoin con Visa, capace di elaborare fino a 45.000 transazioni al secondo.

Un utente potrebbe garantire la velocità delle proprie transazioni con le commissioni per i miner, ma con l'aumento della popolarità del bitcoin crescerebbe anche il costo di tale approccio, eliminando il vantaggio di costo che la Blockchain vanta sui sistemi centralizzati.

Alcuni altcoin hanno implementato delle modifiche progettate per risolvere questi problemi, aumentando la dimensione dei blocchi e adottando meccanismi del consenso alternativi al proof-of-work. Il più comune è il cosiddetto proof-of-stake.
L'obiettivo di qualsiasi consenso blockchain è finalizzare i blocchi di transazioni (Moindrot e Bournhonesque 2017). I blocchi finalizzati appartengono tutti alla catena principale e formano una struttura lineare: non ci può essere alcuna biforcazione, il che significa che due blocchi in conflitto non possono mai essere entrambi finalizzati. Nel proof-of-work la finalizzazione del blocco si concretizza con l'aggiunta dei blocchi successivi, rendendo sconveniente la manomissione. Nel proof-of-stake, invece, la convalida dei blocchi si basa su votazioni da parte dei nodi del network in merito a quale blocco è valido e meritevole di diventare parte della Blockchain, senza il dispendio di energie del mining (Seang e Torre 2018).
Esistono numerose varianti del proof-of-stake, anche molto diverse tra loro. Il meccanismo di base risiede nel voto da parte dei "controllori" del network, che decidono quali blocchi sono legittimi: un individuo diventa un "controllore" acquistando sulla Blockchain una certa quantità di criptovaluta. L'entità della quantità detenuta, il deposito, è lo "stake" (interesse, puntata) del controllore. A seconda della variante del proof-of-stake adottata, il valore del deposito implica un proporzionale peso del voto del controllore (come per le azioni in una s.p.a.) o una maggiore probabilità di diventare il membro estratto in modo aleatorio per convalidare il blocco successivo.
Nella variante del "protocollo Casper", adottata dal sistema Ethereum recentemente, si accetta di poter perdere l'intero ammontare depositato nel caso si venga ritenuti controllori fraudolenti da una maggioranza (ponderata in base agli stake) di 2/3 dei nodi o si violino le regole di voto (in tal caso è il sistema che automaticamente distrugge il deposito), scoraggiando la votazione di due blocchi diversi in contemporanea.
In alcune varianti come la Casper, i controllori ricevono compensi in criptovaluta per ogni checkpoint raggiunto, che consiste in un numero prestabilito di blocchi approvati dal sistema, mentre in altri tipi di proof-of-stake si trae profitto dalle commissioni che gli utenti annettono alle singole transazioni affinché abbiano la precedenza sulle altre.

Ethereum, che usa il protocollo Casper, riesce ad aggiungere un blocco alla catena ogni 14-15 secondi, contro i 10 minuti del bitcoin.

I punti deboli del proof-of-stake risiedono nella necessità di minare il totale della criptovaluta in circolazione all'inizio dell'adozione del sistema (in quanto non vi è mining, quindi non vi è creazione di nuova valuta): questo crea la possibilità di una distribuzione iniqua di criptomoneta, in cui un utente particolarmente ricco ottiene maggiore influenza sul voto e diventa ancora più ricco, creando un circolo vizioso.

Seppur più veloce, il proof-of-stake è ritenuto più vulnerabile del proof-of-work, specie nei casi di Blockchain con molti nodi (che rendono difficile effettuare un 51% attack) e un numero limitato di criptovalute circolanti (aumentando il rischio che si accentri il potere di voto in un individuo). Inoltre, nei proof-of-stake che non premiano i controllori con criptovaluta, il problema del costo delle transazioni rimane. Il proof-of-stake, infine, poggia il suo funzionamento sull'assunzione che molti nodi siano costantemente online: se questo non dovesse accadere, il sistema sarebbe molto vulnerabile alla "simulazione a costo zero", detta anche "attacco dalla lunga distanza", (Gaˇzi, Kiayias e Russell 201, p2) dove una minoranza di nodi sfrutta l'assenza di mining per ricreare una nuova Blockchain, alternativa a quella reale, a partire dalla prima transazione. I nodi che entrassero a far parte della Blockchain dopo questo attacco non avrebbero modo di distinguere la catena fraudolenta da quella autentica, col rischio di votare per l'approvazione della Blockchain sbagliata.

È dunque evidente che anche il meccanismo proof-of-stake presenta debolezze, che richiedono di essere superate prima che il sistema possa imporsi come alternativa agli attuali sistemi centralizzati che regolano i pagamenti internazionali.

Blockchain: davvero indispensabile?

La sfida maggiore che la Blockchain potrebbe dover affrontare non sono i monumentali costi del proof-of-work, la difficoltà tecnica nel conciliare sistemi diversi o la sicurezza, bensì il fatto che, malgrado i benefici che porta con sé, questa tecnologia potrebbe non essere necessaria per conseguirli. Questo apparentemente paradossale sviluppo deriva dal fatto che l'innovatività della Blockchain potrebbe essere sopravvalutata.

Nel suo "Blockchain revolution without the Blockchain" (2018), Hanna Halaburda accusa la Blockchain di essere soltanto un agglomerato di strumenti utili, che possono però esistere autonomamente e che non sono stati introdotti da Nakamoto.

La Blockchain viene comunemente considerata un “libro mastro distribuito” o “database distribuito”, che si avvale di smart contracts e crittografia. Questo ha confuso il pubblico portandolo a pensare che queste 3 componenti (smart contracts, crittografia e database distribuito) siano le caratteristiche fondamentali e inscindibili che rendono la Blockchain quello che è, mentre invece smart contracts e crittografia possono, ma non devono, appoggiarsi ad essa.

Gli smart contracts sono programmi computerizzati che implementano automaticamente le condizioni poste dai contraenti, senza bisogno di intervento umano. La loro velocità e ridotta fallibilità (rispetto ad un controllore umano) si traduce in una maggiore efficienza.
Molte Blockchain utilizzano gli smart contracts: alcune sono state progettate puntando principalmente a facilitarne l’utilizzo, come nel caso Ethereum (ethereum.org). Tuttavia, la Blockchain non ha introdotto il concetto: il termine “smart contract” deriva da un articolo di N. Szabo, “Formalizing and Securing Relationships on Public Networks” (1997). Non è nemmeno possibile sostenere che la Blockchain sia indispensabile per l’esistenza di smart contracts, in quanto anche un sistema centralizzato può implementarli (si pensi ad un RID bancario).

La crittografia si basa sull’utilizzo di codici per proteggere le informazioni. Può rappresentare indubbiamente una fonte di risparmio se sviluppata. Un beneficio della Blockchain è stato quello di attrarre su di essa l’attenzione delle imprese, fomentando un rinnovato interesse per le sue applicazioni.
Alcuni business, come Goldman Sachs (Chavez, discorso del 2017), stanno implementando nuovi strumenti crittografici per assicurare maggiore protezione ai loro dati attraverso un sistema che protegga l’informazione dovunque essa sia immagazzinata. I sistemi attuali mirano a rendere più complesso l’acceso al singolo terminale ma, una volta superate le barriere, è possibile accedere alle informazioni.
Questi sviluppi, come nel caso di Goldman Sachs, non richiedono l’utilizzo della Blockchain.

In quanto database distribuito, la Blockchain potrebbe teoricamente fungere da raccoglitore di qualsiasi tipo di informazioni, superando il ruolo da essa concepito di libro mastro digitalizzato. Un meccanismo decentralizzato simile porta maggiori benefici dove maggiore è il costo di risolvere conflitto tra le parti, anche se l’archiviazione dello stesso libro mastro in più posizioni potrebbe aumentare in modo significativo il costo computazionale e di archiviazione. “Ad oggi, non è stato chiaramente dimostrato in quali casi i benefici derivanti

dall'impiego di un libro mastro distribuito superino il costo dei ritardi temporali e dello spazio di archiviazione duplicato." (Halaburda 2018).

Una caratteristica fondamentale delle Blockchain fino ad ora utilizzate, come quella di Bitcoin, Ripple ed Ethereum, è che esse si basano su di un token nativo al sistema: mentre la Blockchain è virtualmente immutabile quando si tratta di criptovalute e delle loro transazioni, lo stesso non si può dire di una Blockchain designata per altri scopi. Questa "debolezza" deriva dal fatto che la protezione offerta dalla Blockchain non si basa soltanto sulla crittografia, bensì anche sul sistema di incentivi promosso dall'adozione di una valuta specifica alla Blockchain. In mancanza di un cosiddetto "token nativo", la catena incorre in dei problemi:

- Gateway problem

  Mentre è possibile scambiare asset diversi dalle criptovalute sulla catena, non è scontato accertare l'esistenza di questi asset. Per scambiare due oggetti occorre prima accertarsi che essi esistano, e che vengano considerati proprietà dei due utenti dal sistema. Mentre la Blockchain può gestire senza interventi esterni le transazioni, una tale verifica deve essere fatta da un terzo individuo. Il gateway problem non sussiste soltanto nel caso di un token digitale, in quanto creato sulla Blockchain e immediatamente riconosciuto da essa.
- Incentivi

  Il mining è necessario non solo per creare nuova criptovaluta, ma anche per rendere sicura la catena, rendendo i tentativi di falsificarla troppo costosi per essere profittevoli. Senza un meccanismo come il proof-of-work (o le alternative proposte come il proof-of-stake, non altrettanto sicure), basato su premi in criptovaluta per i miner, gli utenti hanno bisogno di un incentivo esterno per aggiungere blocchi, e per farlo in maniera non fraudolenta.

Una soluzione a questi problemi sarebbe inserire dei permessi nella Blockchain e centralizzare parte delle funzioni: questo, tuttavia, stravolgerebbe il concetto di innovazione proposto dagli altcoin, reintroducendo il "middle man" che la Blockchain avrebbe dovuto rendere obsoleto.

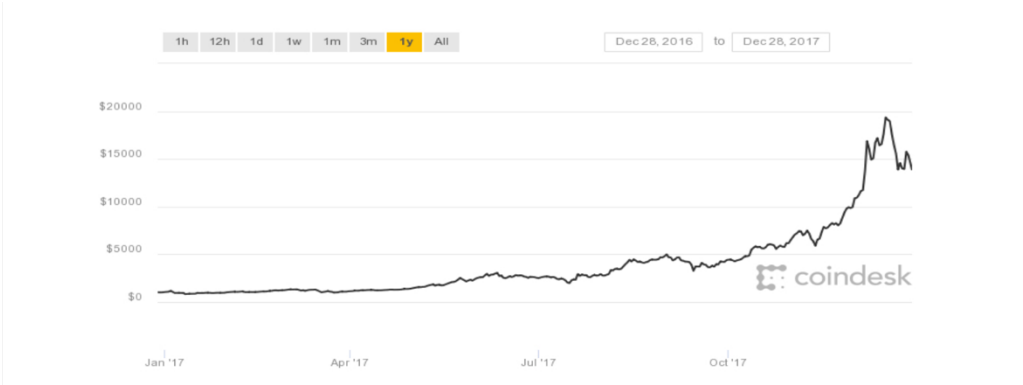
Non secondario è il fatto che, una volta introdotto un supervisore nella Blockchain, si conseguirebbe uno spreco inutile nell'optare di memorizzare l'intera storia delle transazioni invece che una bilancia dei saldi tra i vari utenti.

In definitiva, dunque, la Blockchain contiene elementi innovativi che potrebbero cambiare il mondo della finanza e dell'economia in generale, ma poiché questi elementi possono esistere separati da essa (smart contracts e crittografia), o proprio perché ne sono parte integrante e

fondamentale (token nativi), risulta dubbio l'impatto che questa invenzione potrebbe avere al di fuori del contesto delle criptovalute.

4. La scalata al successo delle criptovalute

Al di là dei ruoli che le criptovalute potrebbero assumere nel sistema di pagamento, o dell'impatto che la Blockchain potrebbe avere su sicurezza, governance e taglio dei costi, la fonte principale della popolarità che questo settore ha ottenuto recentemente tra il pubblico è l'incredibile crescita che ha visto nel corso del 2017, in particolare tra settembre e dicembre, e la successiva decrescita.



La scalata è stata talmente repentina da far gridare alla bolla diversi analisti prima ancora che essa effettivamente scoppiasse.

La crescita esponenziale del prezzo del bitcoin negli ultimi due anni ha fatto sì che i banchieri e tutti i tipi di investitori dimenticassero lo scopo per cui è stato creato e si concentrassero sull'opportunità di investimento che rappresenta.

La crescita nel 2017 è stata, per l'intera classe di asset, di oltre il 1200% (Houben e Snyers 2018). Il bitcoin, più di ogni altcoin, ha invaso la vita non soltanto di coloro che lavorano nel mondo della finanza, nei sistemi giuridici che la regolano e dei tecnici che potrebbero interessarsi ai risvolti tecnologici della Blockchain, ma anche della gente comune. La copertura mediatica è passato attraverso internet, TV e perfino la radio. Le peculiarità dei sistemi di criptovalute e le sottigliezze che ne regolano il funzionamento e che ne contraddistinguono la pur scheletrica regolamentazione potrebbero non essere alla portata di tutti, mentre l'impennata del prezzo del bitcoin è stata notata dal mondo intero. L'entusiasmo prodotto da questa improvvisa scalata del bitcoin è stato tale da causare iscrizioni nell'ordine dei 50.000 nuovi utenti giornalieri soltanto per Coinbase (Kharif 2018): è ironico come una piattaforma centralizzata riesca a beneficiare a tal punto da un sistema che si pone come baluardo della decentralizzazione.

Quali fattori potrebbero aver alimentato una tale crescita in questo mercato?

Il già citato effetto rinforzo è sicuramente una delle cause: la crescita del bitcoin e degli altri top player come l'ether, il litecoin e il bitcoin cash hanno fatto sì che più persone venissero a

conoscenza di questo mondo, e hanno aumentato la sicurezza di chi già ne era entrato in contatto. Il conseguente aumento del numero di adottanti ha causato un aumento del numero di transazioni e della fiducia nel settore, spingendo il prezzo più in alto e aumentando ulteriormente la visibilità delle criptomonete.

L'effetto rinforzo, però, rappresenta solo parte della risposta.

Irrazionalità del mercato

"Una bolla. Il valore di cose come il bitcoin è quello che le persone pensano varrà domani, quello che varrà domani è quello che pensano varrà il giorno dopo … Quella che stiamo vedendo è l'ennesima dimostrazione dell'irrazionalità dei mercati" (Stiglitz 2017).

Il prezzo di azioni, titoli, valute e derivati sono influenzati non soltanto dai fondamentali, ma anche da una serie di fattori correlati alla componente psicologica degli investitori. Questa irrazionalità, che non può essere totalmente prevista o compresa, contribuisce alla formazione di bolle, come nel caso della dot.com bubble.

Le notizie (a volte apparentemente sconnesse dal contesto in cui si è investito) possono spingere gli investitori ad eccessi di timore o fiducia nei confronti dei loro investimenti, generando rispettivamente un sell-off (e con esso un deprezzamento) o una frenesia immotivata che porti a picchi nei prezzi degli asset.

Se questi meccanismi valgono per attività dotate di un qualche valore intrinseco, ancor maggiore è la loro importanza in fatto di criptovalute, sconnesse da qualsiasi cash flow.

Fonte: 99bitcoins

In numerosi casi il prezzo del bitcoin è drasticamente calato dopo notizie quali la decisione di Facebook di vietare la pubblicità di criptovalute, mentre segnali di accettazione del bitcoin quale asset valido, invece che come schema di Ponzi digitale, come l'istituzione di future sul bitcoin alla CBOE, sembrano aver alimentato apprezzamenti.

Considerato che il bitcoin e gli altcoin non hanno un ruolo di base se non quello di essere denaro digitale, è legittimo pensare che la fiducia degli utenti vari in base ai segnali che le istituzioni e il web mandano riguardo alla loro volontà di adottare le criptovalute come mezzi di pagamento. Il bitcoin non è l'unico caso, ma essendo la criptovaluta più nota è la più esposta alla copertura mediatica (positiva o negativa) e alle paure ed entusiasmi degli investitori.

In generale, notizie che gettano dubbi sulla stabilità politica di un paese e sulla sua valuta, come il referendum per la Brexit o l'elezione di Donald Trump, sembrano alimentare un apprezzamento del bitcoin, mentre la possibilità di interventi governativi nel settore criptovalute creano FUD (fear, doubt, uncertainty).

Il fatto che le criptovalute si siano imposte a livello di piccoli investitori e gente comune, prima ancora che tra le banche e le grandi aziende, spiega la notevole irrazionalità del mercato e la volatilità che, di conseguenza, affligge i prezzi di questi asset.

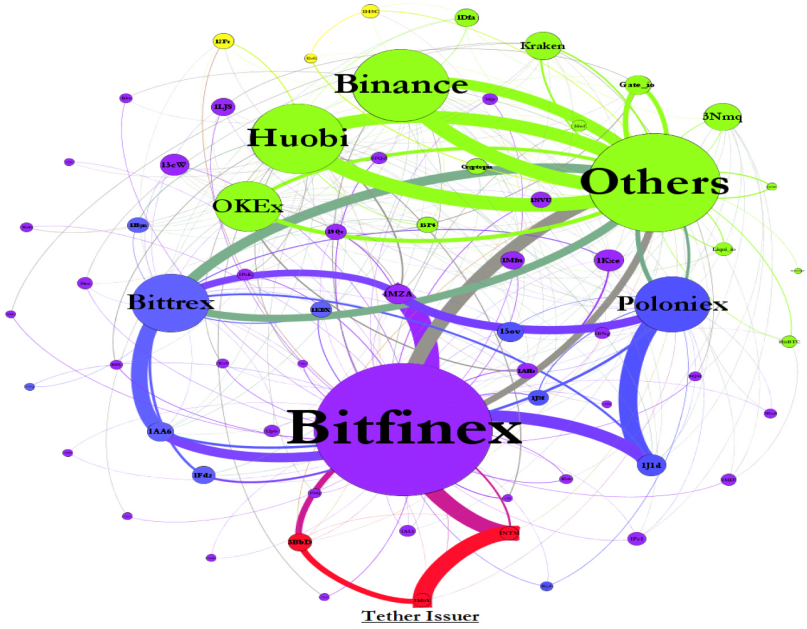
Manipolazione del mercato

Nel loro "Is Bitcoin Really Un-Tethered?" (2018) John M. Griffin e Amin Shams accusano theter, una criptovaluta, di essere stata utilizzata per compiere grandi acquisti di bitcoin, sostenendo il mercato artificialmente ed effettivamente manipolandolo.

L'obiettivo di Tether è facilitare le transazioni tra le piattaforme di scambio di criptomonete grazie alla caratteristica di avere un valore ancorato al dollaro statunitense. Permette di eseguire trasferimenti di capitale ad alta velocità senza ricorrere a vie bancarie. Anche se questo potrebbe verificarsi anche con la moneta tradizionale, Tether è vantaggioso dal momento che molte piattaforme hanno difficoltà a stabilire relazioni con le banche. Tether Limited, l'ente che ha ideato questa criptovaluta e che ha il monopolio dell'emissione di nuove quantità, afferma che le valute sono sostenute al 100% da attività in valuta nel loro conto di riserva. Tuttavia, la stessa Tether Limited ha creato ambiguità intorno a questa affermazione sostenendo che non garantisce il diritto di riscatto.

Inoltre, se è vero che, come andremo a vedere, l'emissione di tether è supply-driven e non motivata dalla domanda di investitori, le riserve di Tether Limited potrebbero non essere commisurate alla quantità di tether circolanti.

I movimenti del tether vengono illustrati nello studio con il seguente schema:



I tether vengono emessi da Tether Limited, l'azienda che li ha creati, per poi transitare attraverso la piattaforma di scambio Bitfinex alle due gemelle Bittrex e Poloniex.

Secondo i due studiosi, i creatori di tether, come molti della categoria, potrebbero essere bull nei confronti del bitcoin (puntare su di un apprezzamento), e questo darebbe loro modo di trarre vantaggio dall'emissione di grandi quantità di tether: invece di piazzarlo tra gli utenti, lo avrebbero utilizzato per comprare grandi quantità di bitcoin, in modo da sostenerne artificiosamente la domanda, mantenendo alto l'ottimismo del mercato e dunque il prezzo. I bitcoin acquistati sarebbero poi stati rivenduti più lentamente o in altre piattaforme non trasparenti, in modo da ridurre il più possibile il deprezzamento causato dall'alienazione.

Questo metodo presenta somiglianze con lo spoofing dei mercati finanziari: un trader piazza grandi quantità di offerte di acquisto intorno ad un particolare titolo (di cui già possiede una certa quantità) con l'intenzione di cancellarle prima che vengano effettuate, suscitando nel frattempo la reazione automatica degli HFT (High-Frequency Traders, che funzionano con algoritmi che consentono di analizzare il mercato e muovere offerte in frazioni di secondo). Gli HFT recepiscono istantaneamente la crescente domanda, muovendo offerte verso quello stesso titolo e alimentando un aumento di prezzo ingiustificato. Lo spoofer riesce così a vendere a prezzi irrazionalmente alti i titoli per cui ha mostrato falso interesse, cancellando le offerte "fraudolente" che avevano alimentato il picco di domanda immediatamente dopo. Lo spoofing è illegale, in quanto tecnica per la manipolazione del mercato, e il primo condannato per tale reato (Michael Coscia, nel 2016) ha visto la sua sentenza confermata nel 2018 (Stohr 2018).

A sostenere la propria tesi, Griffin e Shams portano prove di movimenti sospetti di tether corrispondenti a momenti chiave della fluttuazione del prezzo del bitcoin tra marzo 2017 e marzo 2018: dopo periodi di ritorno negativo per il bitcoin, vi sono ingenti flussi di tether tra le tre principali piattaforme per lo scambio di questa criptovaluta (Bitfinex, Poloniex e Bittrex) verso altre per l'acquisto di bitcoin. Questi flussi inter-piattaforme coincidono con forti apprezzamenti del bitcoin, e sono presenti solo dopo periodi in cui quest'ultimo vede un deprezzamento e tether una nuova emissione nel sistema, ovvero quando è probabile un eccesso di offerta di tether. Dai dati delle Blockchain Tether e Bitcoin risulta che questi flussi di valuta sono strettamente correlati.

Inoltre, non si sono presentati flussi opposti per il tether quando il prezzo del bitcoin è aumentato, cioè il tether viene venduto in grandi quantità per acquistare bitcoin quando questi presentano prezzi bassi, ma non vengono ricomprati quando il prezzo del bitcoin è alto. Questo fenomeno suggerisce fortemente che il bitcoin sia stato protetto dalle emissioni di tether.

I casi studiati sono le 87 ore con maggiori movimenti combinati sulle Blockchain di Tether e Bitcoin, che ammontano a meno dell'1% del periodo preso in esame, ma sono associate al 50% dei profitti totali dei bull di bitcoin e al 64% dei rendimenti su sei altre grandi criptovalute (nei sistemi Dash, Ethereum Classic, Ethereum, Litecoin, Monero e Zcash): gli autori dello studio precisano tuttavia che queste percentuali sono stime che potrebbero sottovalutare o sopravvalutare l'impatto di questi flussi, in quanto non tengono conto delle parzialmente ignote meccaniche di prezzo che connettono il prezzo di una criptovaluta all'altra, il successo di una piattaforma su quella o questa criptomoneta e in generale la risposta dell'intero mercato ad un certo movimento.

A supportare la tesi dello studio vi è inoltre il fatto che il bitcoin ha visto numerose e forti inversioni di prezzo successive a periodi di ribasso, che non avvenivano prima dell'affermarsi di tether sul mercato e che hanno smesso di presentarsi nel periodo in cui tether ha smesso di essere emesso. Come se non bastasse, sono evidenti grandi acquisti di bitcoin in numeri multipli di 500 da parte di Bitfinex a seguito di larghe emissioni di tether. Infine, si osservano ritorni negativi anormali a fine mese per i detentori di bitcoin in concomitanza a forti emissioni di tether. Secondo gli studiosi, queste perdite derivano dall'alienazione in massa dei bitcoin comprati da Tether Limited, che in quei mesi doveva emettere dei rendiconti per dimostrare di avere sufficienti riserve.

Se la tesi si rivelasse vera, non solo verrebbe spiegata l'enorme crescita del mercato nel 2017, caratterizzata da continui oscillamenti di prezzo, ma verrebbe messa in dubbio la legittimità di

ogni criptovaluta: non solo il denaro tradizionale, ma anche le criptomonete, nonostante siano state create per realizzare un apparato finanziario decentralizzato, sono passibili di accentramento del controllo in alcuni grandi player, che potrebbero commettere frodi senza dover sottostare allo stesso regime di regolamentazione e responsabilità delle istituzioni tradizionali.

5. Conclusioni

Il futuro delle criptovalute, come quello di altre invenzioni all'alba del loro sviluppo, è incerto. Malgrado i recenti sforzi di regolamentare i maggiori operatori del settore, le criptovalute sembrano essere più un asset adatto alla speculazione che una valida moneta di scambio: molti sono i rischi associati al detenerle e scambiarle, e il conseguimento dell'obiettivo per cui sono state create è inficiato dalle falle tecniche tipiche di questa tecnologia, nonché da frodi e crescenti costi di commissione che avvicinano questo sistema a quello tradizionale, che Satoshi Nakamoto si era ripromesso di rendere obsoleto.

Se le criptovalute diventassero di uso comune il panorama economico cambierebbe, dal modo di condurre business tra le grandi multinazionali all'acquisto di beni e servizi da parte del consumatore medio. Le istituzioni finanziarie non scomparirebbero, ma il loro ruolo verrebbe ridimensionato, mentre alcune delle loro funzioni verrebbero spostate alle piattaforme di scambio di criptomonete. Tuttavia, se i problemi di bitcoin e altcoin esposti nei capitoli precedenti non venissero risolti, si assisterebbe ad una semplice smaterializzazione del denaro, non accompagnata da una sensibile trasformazione dei canali di circolazione. Esiste ancora la possibilità che lo Stato adotti una propria criptovaluta: in tal caso l'impatto sulla società, anche se certo, sarebbe di minori dimensioni rispetto a quello prospettato dai sostenitori delle Blockchain aperte e prive di permessi.

Quanto alla Blockchain, dato che le grandi aziende hanno deciso di testare le sue applicazioni in contesti separati da quello delle criptovalute, essa potrebbe sopravvivere alla classe di asset che ne hanno favorito la notorietà. Naturalmente, la natura più o meno competitiva dei mercati preesistenti ne influenzerebbe la diffusione, in quanto la Blockchain ha maggiori probabilità di giustificare la propria adozione in contesti in cui il costo della verifica è attualmente elevato a causa della regolamentazione o della particolare infrastruttura.

Le scelte del governo in diverse giurisdizioni saranno un altro fattore chiave che definirà dove potremmo vedere per prima una criptovaluta promossa dallo Stato, un sistema di pagamenti meno costoso che funziona su un registro distribuito o una sperimentazione con forme più complesse di risoluzione e riconciliazione.

È quindi ancora troppo presto per decidere se l'eredità di Satoshi Nakamoto cambierà il sistema dei pagamenti come i social network hanno cambiato il modo in cui le persone si connettono, oppure se si risolverà in un nulla di fatto, soffocata dalle regolamentazioni e dalla perdita di fiducia o, infine, se sopravviverà come realtà di nicchia, troppo piccola per rappresentare una seria svolta per la società ma troppo affascinante per scomparire del tutto.

Bibliografia

99BITCOINS [online]. Disponibile su https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/ [Data di accesso: 24/10/2018]

99BITCOINS. [online]. Disponibile su https://99bitcoins.com/price-chart-history/ [Data di accesso: 25/10/2018]

BARRDEAR, J. e KUMHOF M., 2016. *The macroeconomics of central bank issued digital currencies*. Bank of England, Londra.

BEIGEL, O., 2018. What is Double Spending. *99Bitcoins* [online], Disponibile su: https://99bitcoins.com/double-spending/ [Data di accesso: 19/10/2018]

BERMAN, A., 2018. La banca centrale tedesca ha completato il testing per una soluzione di pagamento basata su blockchain. *Cointelegraph* [online], Disponibile su https://it.cointelegraph.com/news/german-central-bank-and-deutsche-boerse-successfully-complete-blockchain-settlement-trial [Data di accesso: 24/10/2018]

BLOCKCHAIN.COM [online]. Disponibile su https://www.blockchain.com/it/charts/n-transactions [Data di accesso: 20/10/2018]

BOUOIYOUR, J. e SELMI, R., 2017. *The Bitcoin price formation: Beyond the fundamental sources.*

CARPER, T., 2013. Discorso di apertura di "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies". Comitato della Sicurezza e degli Affari Governativi, Senato degli Stati Uniti. [online] Disponibile su https://m.youtube.com/watch?v=x8Y71IXEK8w [Data di accesso: 12/10/2018]

CATALINI, C. e GANS, S. J., 2016. *Some Simple Economics of the Blockchain*. National Bureau of Economic Research, Massachusetts.

CHAVEZ, R. M., 2017. *Data, Computing, and Transformation in the Financial Industry*. Discorso al simposio Data, Dollars and Algorithms: The Computational Economy. Harvard

Institute for Applied Computational Science. Disponibile su https://m.youtube.com/watch?v=VF6DrX9H0Ug [Data di accesso: 26/10/2018]

CHEAH, E. e FRY, J., 2015. *Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin*. Economics Letters.

CHIU, J. e KOEPPL, T., 2017. *The Economics of Cryptocurrencies – Bitcoin and Beyond*. Bank of Canada.

COINBASE. [online]. Disponibile su https://www.coinbase.com/about [Data di accesso: 17/10/2018]

COINMARKETCAP. [online]. Disponibile su https://coinmarketcap.com/charts/ [Data di accesso: 15/15/2018]

CORCORAN, K., 2018, Criminals in Europe are laundering $5.5 billion of illegal cash through cryptocurrency, according to Europol. *Business Insider* [online], Disponibile su https://www.businessinsider.com/europol-criminals-using-cryptocurrency-to-launder-55-billion-2018-2?IR=T [Data di accesso: 11/10/2018]

ETHEREUM.ORG. [online]. Disponibile su https://www.ethereum.org [Data di accesso: 25/10/2018]

FATF, 2015. *Emerging Terrorist Financing Risks*. FATF, Parigi.

FUNG, S., C., B. e HALABURDA, H., 2016. *Central Bank Digital Currencies: A Framework for Assessing Why and How*. Currency Department, Bank of Canada.

GANDAL, N. e HALABURDA, H., 2014. *Competition in the Cryptocurrency Market*. Currency Department, Bank of Canada.

GAˇZI, P., KIAYIAS, A. e RUSSELL, A., 2018. Stake-Bleeding Attacks on Proof-of-Stake Blockchains. In: *2018 Crypto Valley Conference*, p.2.

GOZZI, A., 2018, Rovereto e la rivoluzione bitcoin, dal dentista al caffè qui si paga in criptovaluta. *Quotidiano.Net* [online], Disponibile su https://www.quotidiano.net/economia/rovereto-bitcoin-1.3824236 [Data di accesso: 16/10/2018]

GRAY, J., 1981. *The Transaction Concept: Virtues and Limitations*. Seventh International Conference on Very Large Databases.

GRIFFIN, M., J. e SHAMS, A., 2018. *Is Bitcoin Really Un-Tethered?*
HALABURDA, H., 2018. *Blockchain Revolution Without the Blockchain*. Currency Department, Bank of Canada.

GSMA, 2018. *Distributed Ledger Technology, Blockchains and Identity: A Regulatory Overview*.

HOUBEN, R. e SNYERS, A., 2018. *Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion*. Studio richiesto dalla commissione speciale TAX3, Parlamento Europeo, Bruxelles.

INBITCOIN [online]. Disponibile su https://inbitcoin.it [Data di accesso: 14/10/2018]

Instituto Nacional de Ciberseguridad de España S.A. (INCIBE) (2014) In: RUIZ CABRERA, S., 2016. *HOW DO YOU DO MONEY LAUNDERING THROUGH BITCOIN?*. Relazione finale Accounting and Finance Degree, Facultad de Ciencias Jurídicas y Económicas - Universitat Jaume I.

"*Is Bitcoin a flash in the pan? - Coinsumm.it*", YouTube video, 45:57. Postato da "CoinSummit," 26 Marzo 2014, Disponibile su: https://m.youtube.com/watch?v=rEtrIjzsceM [Data di accesso 12\10\2018]

KHARIF, O., 2018. Coinbase Says It Was Signing Up 50,000 Users a Day. *Bloomberg*, Disponibile su https://www.bloomberg.com/news/articles/2018-08-14/in-crypto-downturn-coinbase-still-signing-up-50-000-users-a-day [Data di accesso: 23/10/2018]

KRISTOUFEK, L., 2015. *What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis.*

MOINDROT, O. e BOURNHONESQUE, C., 2017. *Proof of Stake Made Simple with Casper*. ICME, Stanford University.

NAKAMOTO, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*.

NATARAJAN, H., KRAUSE, S. e GRADSTEIN, H., 2017. *Distributed Ledger Technology (DLT) and Blockchain*. World Bank, Washington DC.

RUIZ CABRERA, S., 2016. *HOW DO YOU DO MONEY LAUNDERING THROUGH BITCOIN?*. Relazione finale Accounting and Finance Degree, Facultad de Ciencias Jurídicas y Económicas - Universitat Jaume I.

SEANG, S. e TORRE, D., 2018. *Proof of Work and Proof of Stake consensus protocols: a blockchain application for local complementary currencies*. Université Côte d'Azur.

STIGLITZ, J. Intervistato da GAMM, S., 2017. Nobel Prize Winning Economist Joseph Stiglitz: Bitcoin Is a Bubble. *TheStreet*, [online] Disponibile su https://www.thestreet.com/video/14405586/nobel-prize-winning-economist-joseph-stiglitz-bitcoin-is-a-bubble.html [Data di accesso 23/10/2018]

STOHR, G., 2018. Anti-Spoofing Law Survives as U.S. Supreme Court Rejects Trader. *Bloomberg*, [online] Disponibile su https://www.bloomberg.com/news/articles/2018-05-14/anti-spoofing-law-survives-as-u-s-supreme-court-rejects-trader [Data di accesso: 25/10/2018]

SZABO, N., 1997. Formalizing and Securing Relationships on Public Networks. *First Monday*, Disponibile su https://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First [Data di accesso: 28/10/2018]

WALLACE, B., 2011, The Rise and Fall of Bitcoin. *Wired* [online], Disponibile su https://www.wired.com/2011/11/mf-bitcoin/ [Data di accesso: 18/10/2018]

WILHELM, A., 2014. Popular Bitcoin Mining Pool Promises To Restrict Its Compute Power To Prevent Feared '51%' Fiasco. *TechCrunch* [online], Disponibile su https://techcrunch.com/2014/07/16/popular-bitcoin-mining-pool-promises-to-restrict-its-compute-power-to-prevent-feared-51-fiasco/ [Data di accesso: 17/10/2018]

WILMOTH, J., 2018. 'The Biggest Theft in History': What We Know So Far About the $530 Million Coincheck Hack. *CCN* [online], Disponibile su https://www.ccn.com/biggest-theft-history-know-far-530-million-coincheck-hack/ [Data di accesso: 18/10/2018]

YERMACK, D., 2013. *Is Bitcoin a Real Currency? An economic appraisal*. National Bureau of Economic Research, Massachusetts.

YERMACK, D., 2015. *Corporate Governance and Blockchains*. National Bureau of Economic Research, Massachusetts.

1

[1] 12714 Parole + Bibliografia