Bitcoin: oro digitale, finanza e tulipani

Intervista a
Ferdinando M. Ametrano
www.ametrano.net/about/

ultimo aggiornamento: 29 novembre 2019
Link permanente: https://goo.gl/eyjDJ2
YouTube: https://bit.ly/381yz1J

Se ne discute molto, ma su bitcoin la divisione è radicale, tra scettici che parlano di bolla ed entusiasti che descrivono una rivoluzione globale. Tra questi ultimi, Ferdinando M. Ametrano è uno degli esperti più controversi ed interessanti: fisico di formazione, per decenni si è occupato di derivati finanziari, fino al 2014 quando scopre bitcoin; oggi guida il Digital Gold Institute ed insegna "*Bitcoin and Blockchain Technology*" in diverse università e principalmente a Milano-Bicocca (del cui Crypto Asset Lab è direttore scientifico). Imprenditore in CheckSig, società di custodia bitcoin per investitori istituzionali e *high-net-worth individuals*, è stato in precedenza *Head of Blockchain and Virtual Currencies* in Intesa Sanpaolo, membro del comitato organizzatore di *Scaling Bitcoin* (la principale conferenza annuale per gli sviluppatori della criptovaluta) e nel 2018 è intervenuto al primo seminario organizzato su bitcoin all'ONU[1]. Lo abbiamo intervistato, accendendo il riflettore sui molteplici aspetti di bitcoin.

1. Oro digitale

Ferdinando, partiamo dalle basi: cos'è bitcoin?
È un bene digitale trasferibile ma non duplicabile, cioè "spendibile" una sola volta (a favore di Tizio) ma non due volte (a favore anche di Caio). Per la prima volta in ambito digitale questa caratteristica è intrinseca al protocollo informatico che definisce bitcoin e non è garantita da una autorità o emittente, come capita invece con un titolo azionario o il saldo di un conto corrente. Inoltre, bitcoin è un bene scarso, la cui emissione è deterministicamente fissata e limitata alla soglia di 21 milioni che verrà raggiunta intorno al 2140: è l'emergere della scarsità in ambito digitale.

Cosa limita i bitcoin a 21 milioni?
Le regole del protocollo informatico che definisce bitcoin. Chiunque può cambiare queste regole e questo limite, ma nel farlo crea tecnicamente qualcosa di diverso rispetto a bitcoin: si esclude quindi automaticamente dal network bitcoin le cui regole sono quelle accettate dalla maggioranza degli utenti economicamente rilevanti. Chi possiede bitcoin ha un incentivo economico a preservarne la scarsità evitando manipolazioni inflazionarie, che per fortuna non possono in alcun modo essere imposte.

[1] https://www.youtube.com/watch?v=VbwUwioZ9F0&t=330s&list=PLrVvuryXHYTezxoQBL7Lw3svQEVd2uTzZ&index=10 (video);
https://www.un.org/development/desa/dpad/2018/seminar-understanding-bitcoin-blockchains-and-the-crypto-economy/ (info);
https://speakerdeck.com/nando1970/bitcoin-as-digital-gold (slide)

Perché la scarsità in ambito digitale dovrebbe essere rilevante?
Perché suggerisce un paragone con la scarsità dell'oro in natura. L'oro è l'unico materiale che luccica sempre perché non arrugginisce, allo stesso modo bitcoin si distingue, "luccica", in ambito digitale perché non può essere duplicato. Entrambi inoltre sono scarsi. Bitcoin, se dimostrerà di reggere alla sfida, potrebbe essere l'equivalente digitale dell'oro. Per questo acquisisce valore e permette interazioni economiche.

Abbiamo già l'oro fisico, perché dovrebbe interessare quello digitale?
Se consideriamo il ruolo dell'oro nella storia della civiltà, della moneta e della finanza, possiamo intuire che l'emergere del suo equivalente digitale, "liquido" come la musica ed i film che consumiamo oggi, potrà essere dirompente nell'attuale civiltà digitale e nel futuro della moneta e della finanza.

È difficile accettare che qualcosa senza valore intrinseco possa avere valore.
Nemmeno l'euro o il dollaro hanno valore intrinseco: dal 1971 nessuna valuta con corso legale è convertibile in oro[2]. In realtà nulla ha davvero valore "intrinseco": le cose hanno valore per gli utilizzi che possiamo farne e l'apprezzamento che ne deriverà in noi o negli altri. Per questo non ci sentiamo ridicoli ad andare in giro con quei foglietti di carta colorata nei nostri portafogli. E se proprio volessimo trovare il valore intrinseco dell'oro è il fatto che luccica (non si ossida) ed è scarso, esattamente come bitcoin in ambito digitale.

Ma qui si tratta di una semplice sequenza alfanumerica digitale...
Oggi spediamo email invece di lettere cartacee, ascoltiamo mp3 invece di LP o CD, le foto le visualizziamo e non le stampiamo quasi più. Abbiamo imparato che il digitale non ha meno valore degli oggetti materiali.

Gli mp3 si ascoltano, le email si leggono, le foto si guardano. Con un bitcoin cosa si può fare?
Si può scambiare con diverse migliaia di dollari statunitensi o l'equivalente in beni e servizi.

Lei parla di oro, ma bitcoin non è una moneta? La chiamano criptovaluta...
Anche l'oro fisico è stato usato a lungo come moneta, analogamente succede oggi con bitcoin. A maggior ragione perché è uno straordinario mezzo di scambio: "leggerissimo", trasferibile in maniera praticamente istantanea, con massima sicurezza e comodità,

[2] https://www.federalreservehistory.org/essays/gold_convertibility_ends

programmabile e divisibile in cento milioni di parti. Ma sebbene sia tecnicamente possibile, può non essere saggio pagare in bitcoin: chi ha speso 10.000 bitcoin per due pizze[3] nel maggio 2010 non ha fatto una scelta ragionevole per il suo patrimonio.

Quindi è una valuta da non utilizzare?
Una valuta è caratterizzata da una politica monetaria elastica, in cui l'offerta di moneta si adegua alla domanda, tentando di tenere stabile il potere di acquisto; nel caso di bitcoin l'offerta è non solo deterministica, ma soprattutto completamente inelastica: non si adegua a variazioni della domanda. Bitcoin è *crypto-commodity* più che *crypto-currency*, bene rifugio più che moneta transazionale.

Veramente sembra più speculazione selvaggia: il prezzo si muove con dinamiche da montagne russe, non da mercati finanziari…
Nel mercato la dinamica del prezzo origina dall'interazione tra acquirenti e venditori e rappresenta il processo di scoperta del valore: al suo debutto nel 1997 Amazon valeva $1.40, arrivò nel 1999 durante la bolla Internet a $113, per poi crollare a $5.51 nel 2001 con una perdita (*peak-to-valley drawdown*) del 95%; oggi vale diverse migliaia di dollari. Qual è la lezione? Quando ci sono dirompenti discontinuità di paradigma la scoperta del valore è un processo dinamico e complesso, con volatilità altissima.

Il business case di Amazon, pur innovativo, si comprendeva con categorie tradizionali: commercio tramite canale digitale. Bitcoin non si capisce esattamente cosa sia…
È l'equivalente digitale dell'oro! Ma a maggior ragione, siccome la novità di bitcoin non è stata ancora compresa bene, non deve stupire se il prezzo di scambio oscilla violentemente. Inoltre essendo l'offerta di bitcoin inelastica, insensibile alle variazioni di domanda, queste si scaricano sul prezzo senza attenuazioni. Il trend è comunque intrinsecamente deflattivo ed a crescita esponenziale: l'offerta è limitata, la domanda aumenta, il prezzo sale. Ovviamente è impossibile che un bene si rivaluti diverse migliaia di volte negli ultimi 7 anni senza rischi proporzionalmente elevatissimi: la massima perdita percentuale del prezzo (*worst drawdown*) è stata del 93%.

I banchieri centrali servono proprio a questo, a rendere stabile il valore di una moneta.
Dalla sua fondazione nel 1913 la Federal Reserve ha accompagnato il dollaro statunitense in un percorso di svalutazione che gli ha fatto perdere ad oggi il 98% del suo potere di acquisto. Secondo Milton Friedman (premio Nobel per l'economia) "nessuna grande istituzione negli Stati Uniti ha registrato performance così mediocri per

[3] https://bitcointalk.org/index.php?topic=137.msg1195#msg1

un periodo così lungo come la Federal Reserve, nonostante questo mantenendo un'alta reputazione pubblica"[4]. In ogni caso bitcoin non è moneta: la sua offerta non è governabile discrezionalmente, esattamente come l'oro. Non esiste per fortuna banchiere centrale o governante che possa per decreto aumentare la quantità di oro in circolazione.

Ma che valore può avere qualcosa che non ha emittente centrale e non è garantito da alcuna autorità?

La moneta non è davvero "garantita", ma imposta dal corso legale: non la si può rifiutare come saldo di un debito, è pretesa nel pagamento delle tasse. Il suo valore deriva da questa costrizione e dalla forza di chi la impone: il dollaro, ad esempio, vale per la rilevanza geopolitica degli Stati Uniti. Bitcoin, invece, non si impone e vale soltanto per la fiducia che possiamo riporre nella sue basi matematiche e crittografiche nonché per l'ecosistema economico e culturale che ne discende. Le caratteristiche di bitcoin possono generare una fiducia almeno pari a quella che accordiamo al banchiere centrale.

Il banchiere centrale ha una flessibilità operativa che la rigidità di un algoritmo non può avere.

Il banchiere centrale esercita in piena indipendenza la discrezionalità garantita al suo mandato, l'algoritmo matematico farà sempre ciò che è previsto, in maniera deterministica e non manipolabile. Ci possono essere giudizi diversi su quale approccio sia più utile in un determinato periodo storico, ma oggi è tecnicamente possibile anche il secondo: il cambio di paradigma dalla fiducia centralizzata a quella decentralizzata. È comunque opportuno ribadire ancora che bitcoin va paragonato all'oro e non ad una valuta regolata da banca centrale: le sue garanzie di affidabilità ed immutabilità sono fornite da un intreccio di teoria economica, crittografia, teoria dei giochi e tecnologia, così come ci sono caratteristiche chimico-fisiche a garantire che l'oro non arrugginisca.

Per l'oro fisico valgono immutabili leggi di natura, l'oro digitale è un'invenzione di alcuni: non può essere altrettanto affidabile, di certo non è immutabile.

È "diversamente" affidabile. Tutti possono modificarlo, essendo codice open-source, ma così facendo creano un protocollo informatico alternativo e si escludono dal network esistente. Le uniche modifiche praticabili sono quelle che ottengono ampia approvazione, un *consenso* sostanzialmente unanime: la correzione di problemi esistenti, funzionalità più efficienti, ecc. La conferma empirica della sua affidabilità è che funziona da più di un decennio: si parla, sia in senso generico che strettamente

[4] https://miltonfriedman.hoover.org/friedman_images/Collections/2016c21/WSJ_04_15_1988.pdf

tecnico, di consenso distribuito e "consensus money". È poco intuitivo, ma la novità e la forza di bitcoin sta proprio nell'allineamento sinergico di interessi ed incentivi che consentono la formazione del consenso all'interno dell'ecosistema.

Esiste una qualche forma di consenso e quindi di *governance*? Lo chiedo perché se c'è sembra anch'essa opaca ed elusiva…
Capisco la difficoltà a comprendere queste dinamiche, perché non siamo di fronte semplicemente ad una nuova tecnologia, ma ad un cambio di paradigma. La governance non è proceduralizzata e centralizzata, ma dinamica e distribuita tra diversi attori: sviluppatori, utilizzatori, investitori, nodi del network, aziende. Ognuno può tentare di orientare bitcoin secondo le sue preferenze, ma tutti sono direttamente o indirettamente incentivati a preservare e far crescere il valore di bitcoin. È un processo fluido e non governato in maniera impositiva: bitcoin è di fatto il consenso attorno a cui si coagula la maggioranza degli attori economicamente significativi dell'ecosistema. Chi si colloca su posizioni minoritarie è marginalizzato e di conseguenza automaticamente penalizzato dal punto di vista economico.

Non si capisce…
La scarsità dell'oro fisico è garantita da madre natura, quella digitale è puramente convenzionale, necessita del consenso degli attori interessati. Ma non si tratta di una convenzione fragile o velleitaria; piuttosto siamo di fronte ad una architettura che orienta gli incentivi economici di tutti gli attori coinvolti a vantaggio di immutabilità, incensurabilità e preservazione della scarsità. Adam Smith ci ha insegnato che non è dalla benevolenza del macellaio, del birraio o del panettiere che ci aspettiamo la cena, ma dalla cura che questi hanno per il loro interesse. In questo caso la cena è la sostenibilità dell'esperimento bitcoin.

2. Tra truffa e speculazione

Gli incentivi economici di bitcoin sono spesso paragonati ad uno schema Ponzi: una catena di Sant'Antonio dove i primi si arricchiscono a spese degli ultimi.
Non è uno schema Ponzi: è un esperimento ardito che potrebbe fallire ma culturalmente fondato e tecnologicamente robusto. La sua resilienza sta convincendo un numero crescente di persone che l'esperimento possa aver successo. Il valore è dato, come per qualsiasi bene, dall'incontro di domanda e offerta sul mercato. Siccome l'offerta è limitata e la domanda crescente, il prezzo sale. È lo stesso principio secondo il quale i

biglietti di un evento possono costare anche migliaia di euro: sono limitati e se c'è gente disposta a pagarli tanto, il loro valore sarà quello.

Molti però paragonano bitcoin alla bolla dei tulipani, che secoli fa furono scambiati in Olanda a prezzi esorbitanti per un periodo, dopodiché il valore crollò a zero.

Quella dei tulipani è una bolla durata sei mesi[5] (al massimo tre anni... ma alcuni sostengono addirittura non sia mai davvero accaduta come lo raccontiamo oggi[6]) nell'Olanda del 1637. Trovo intellettualmente disonesto e sconfortante paragonarla con un fenomeno che dura da nove anni nell'economia globale del 2018: l'informazione disponibile oggi è infinitamente superiore, circola con maggiore facilità, il mercato è molto più aperto ed esteso. Bitcoin non è effimero, anzi si sta mostrando straordinariamente resiliente. Su bitcoin c'è una taglia formidabile: chiunque ne rompa il funzionamento può trarne un gigantesco beneficio economico o almeno una straordinaria fama. Nessuno ci è riuscito...

Non negherà che nella crescita di prezzo ci sia una fortissima componente speculativa che certamente danneggia la reputazione bitcoin.

Sono per il libero mercato, non sono preoccupato per la reputazione di bitcoin: ognuno investa quanto e come ritiene opportuno, sperando che prenda rischi finanziari di cui è consapevole. Quando sale tanto gli speculatori che non credono alla sostenibilità nel tempo dell'idea di oro digitale vendono e traggono profitto. Conosco chi ha venduto a diecimila, a mille, a cento. Qualcuno ha venduto anche ad un dollaro nell'aprile 2011, visto che qualche mese prima i bitcoin si regalavano online. Anche gli speculatori corrono i loro rischi...

Premi Nobel come Krugman e Stiglitz criticano severamente la bolla bitcoin.

Del primo ricordo la frase "l'impatto di internet sull'economia non sarà superiore a quello avuto dal fax"[7]. Il secondo stimò la probabilità di fallimento delle agenzie americane *Fannie Mae* e *Freddie Mac* talmente piccola da non essere misurabile[8]: quei fallimenti hanno innescato la crisi finanziaria del 2007 che dura tutt'ora. Vincere un premio Nobel non garantisce una intelligenza assoluta e ineccepibile.

---

[5] https://en.wikipedia.org/wiki/Tulip_mania

[6] https://theconversation.com/tulip-mania-the-classic-story-of-a-dutch-financial-bubble-is-mostly-wrong-91413

[7] http://web.archive.org/web/19980610100009/www.redherring.com/mag/issue55/economics.html

[8] https://www.wsj.com/articles/SB10001424052748704204304574543503520372002

Se qualcosa aumenta di valore 14 volte in un anno e non è una bolla, allora cos'è?
Non credo sia una bolla, piuttosto qualcuno suggerisce potrebbe essere lo spillo che fa scoppiare altre bolle. In primis, quella di un debito pubblico che cresce inesorabilmente. A differenza di quest'ultimo, che costituisce passività, bitcoin è intrinsecamente un attivo: nel momento in cui dovesse prevalere la sfiducia sulla sostenibilità del debito i capitali si riverseranno in bitcoin. Scenari meno drammatici potrebbero invece vedere l'euro e il dollaro intraprendere percorsi virtuosi per l'urgenza della concorrenza bitcoin (e dei nuovi sistemi monetari che ne potranno derivare). Se proprio dobbiamo usare un'immagine per la crescita di valore, bitcoin rappresenta una grande, confusa, magari anche pericolosa, ma sostanzialmente inarrestabile corsa all'oro: un *new wild west* con truffatori, prestigiatori, ubriachi molesti, furfanti da baraccone e fuorilegge; non ci sono mappe e lo sceriffo non è ancora arrivato in città. La confusione è grande, perché tanti non hanno chiarezza sulla natura di bitcoin: ma negare che luccichi non aiuta nessuno. Dopotutto, città straordinarie come San Francisco sono nate proprio dalla corsa all'oro.

Il sistema bitcoin ha avvantaggiato enormemente i primi che lo hanno adottato: non è ingiusto??
È come dire che nella corsa all'oro sono avvantaggiati quelli che arrivano per primi ai giacimenti: è ovvio e non è nemmeno ingiusto, visto che hanno investito tempo e risorse per arrivare "primi".

3. Regolazione

Non sarebbe opportuno regolare bitcoin?
Bitcoin è tecnologia nativamente *permissionless*: come il web, l'email ed i protocolli peer-to-peer sfugge ai tentativi di regolazione. "Regolare bitcoin" suona velleitario: la natura di bitcoin è indifferente alla regolazione tanto quanto lo sono le caratteristiche chimico-fisiche dell'oro. È invece necessario contrastare i criminali che utilizzassero bitcoin, come si fa con quelli che usano l'oro, l'euro o le partecipazioni azionarie. Sono già regolati i punti di contatto tra bitcoin e le monete a corso legale (le borse di scambio, i fornitori di servizi finanziari, ecc.): è inutile tentare di imporre ulteriori vincoli tecnicamente non praticabili o peggio ancora criminalizzarlo.

Bitcoin è entrato più volte nell'agenda del G20.
Ne è stato proposto un esame: un'attività mirata alla comprensione di un fenomeno finora frainteso nelle sue caratteristiche e ambizioni sarebbe effettivamente utile. Quanto a regolarlo: l'approccio non potrebbe che essere a livello globale, ma proprio per

questo sarà difficile raggiungere un consenso chiaro ed univoco. Siamo di fronte a un cambiamento di paradigma culturale, non ad una semplice innovazione tecnologica: per questo molti dei criteri usuali sono inapplicabili. È più probabile che capiremo non per lucidità di analisi, ma per adattamento empirico e non senza scossoni controversi. Normare in maniera inopportuna o prematura sarebbe un grave errore perché rischia di soffocare innovazione e sviluppo.

Quindi evviva il far west, teniamo lo sceriffo lontano?
Come auspicato anche da Fabio Panetta, vicedirettore di Banca d'Italia, per bitcoin "occorre innanzi tutto lavorare sull'informazione, illustrarne caratteristiche e rischi"[9]. Oggi sono già coperti alcuni aspetti regolamentari e legislativi (esenzione IVA, normativa antiriciclaggio): si può proseguire su questa strada con la cautela opportuna per non fermare l'innovazione necessaria in assenza di una comprensione reale della natura di bitcoin. D'altronde se lo paragoniamo ancora alla mania per i tulipani, vuol dire che siamo distanti dall'aver messo a fuoco la vera novità che rappresenta. Cosa vorrebbe dire regolare bitcoin? Proibirlo? Tassarlo?

Le preoccupazioni spaziano dal finanziamento del terrorismo al riciclaggio di denaro sporco. Per il Ministro delle Finanze francese Le Maire bitcoin è una "risorsa speculativa che può dissimulare ogni tipo di attività illegale".
Le preoccupazioni sono per ora grandemente esagerate: il Tesoro inglese nei suoi rapporti sul riciclaggio del 2015 e 2017 ha messo le valute virtuali (come amano chiamare bitcoin ed affini) all'ultimo posto tra i rischi di riciclaggio[10]. Al primo posto ci sono le banche, seguite da studi legali e contabili. L'Europol in un documento del 2016 ha dichiarato che non vi sono evidenze dell'uso di bitcoin per il finanziamento al terrorismo[11]. Inoltre, la trasparenza delle transazioni bitcoin lascia scie elettroniche che facilitano il lavoro d'indagine rispetto al contante, ai diamanti o all'oro fisico. Ovviamente quanto più bitcoin verrà riconosciuto ed accettato, tanto più verrà utilizzato anche dai criminali, i quali peraltro già usano dollari, euro, internet, telefonia cellulare ed aviazione senza che questo susciti scandalo o sorpresa.

---

9 https://www.lastampa.it/2018/01/02/economia/i-nostri-istituti-fuori-gioco-se-non-innovano-amazon-pu-diventare-un-big-del-credito-0sg7dLD8aF6xF9F8qJ5q6O/pagina.html

10 https://www.gov.uk/government/publications/uk-national-risk-assessment-of-money-laundering-and-terrorist-financing

11 https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-terrorist-attacks

Di certo bitcoin viene usato nel dark web per acquisti illeciti e per i riscatti dei virus informatici.
È vero: i piccoli spacciatori online usano bitcoin; il cartello colombiano della droga però preferisce ancora i dollari statunitensi. I riscatti per i virus informatici negli anni novanta si pagavano in dollari presso una casella postale o un conto panamense, oggi in bitcoin perché bitcoin… funziona! Gli usi patologici non possono però essere la chiave con cui si guarda ad un fenomeno nuovo e positivo. Vanno perseguiti i criminali, non demonizzati strumenti utili ed innovativi.

E se bitcoin venisse dichiarato illegale?
Ci sono esempi di dispotismo simile: ad esempio, nel 1933 negli Stati Uniti il possesso dell'oro fisico venne reso illegale[12]. Faccio però notare che i bitcoin sequestrati dalle forze dell'ordine sono stati messi all'asta dal Dipartimento di Giustizia degli Stati Uniti, in molteplici occasioni. Quando si sequestra droga non la si mette all'asta perché illegale; le aste bitcoin hanno quindi creato un precedente significativo in un ordinamento di *common law*: dichiarare illegale bitcoin richiederebbe probabilmente un pronunciamento della Corte Suprema. E comunque conosciamo l'effetto del proibizionismo: che riguardi gli alcolici negli anni venti o la droga oggi, l'effetto è primariamente quello di aumentare il prezzo del bene proibito.

Il proibizionismo riguarda sostanze che si acquistano sul mercato nero per ricavarne un qualche, pur discutibile, piacere o vantaggio. Bitcoin si compra solo per speculazione.
Anche la speculazione finanziaria porta piacere e vantaggi, oltre che fornire il servizio di facilitare la scoperta del valore di un bene. Ma in maniera più sostanziale rispondo sottolineando che bitcoin si usa per contrastare il monopolio governativo della moneta ed innescare processi libertari di concorrenza di mercato: questo procura a molti piacere intellettuale e vantaggi in termini di libertà ed efficienza.

Di certo i governi prenderanno qualche iniziativa di contrasto.
Per un governo come per un hacker, è impossibile spegnere bitcoin perché manca una sede centrale, un amministratore o un server da bloccare. È indubbio che i governi riserveranno a bitcoin lo stesso ostracismo storicamente riservato all'oro fisico, non credo però convenga giungere ad un confronto frontale. Come diceva Gandhi "prima ti ignorano, poi ti deridono, quindi ti combattono, infine hai vinto". Bitcoin potrà avere effetti destabilizzanti e sistemici, ma se il legislatore ed il regolatore sapranno

[12] Executive Order 6102, https://en.wikipedia.org/wiki/Gold_Reserve_Act

interpretare la sfida senza demonizzazioni, potrebbero essere adottati comportamenti virtuosi che farebbero bene all'economia.

Gli stati troveranno modo di fermare bitcoin.
La natura decentralizzata e distribuita di bitcoin rende praticamente impossibile modificare il protocollo o spegnere il network. Piuttosto credo si monterà una campagna di discredito dipingendo bitcoin come pericoloso. Trovo probabile che, a fronte di incidenti gravi (finanziamento al terrorismo, relazioni con paesi sotto embargo) ci saranno multe altissime verso le banche che offrono servizi finanziari alle borse di scambio; di conseguenza le banche, nella loro discrezionalità, sceglieranno di non operare con le borse rendendo difficile la compravendita di bitcoin per valute tradizionali. Ma in ogni caso sono strategie difficili da coordinare efficacemente a livello globale.

Bisognerà almeno tutelare i risparmiatori?
Non voglio maramaldeggiare ricordando i ricorrenti misfatti che avvengono sui mercati regolati, ma almeno evitiamo paternalismi: chi investe oggi in bitcoin è culturalmente e tecnologicamente evoluto. È indubbio che alcuni siano attirati dalla prospettiva di facili guadagni, ma l'acquisto di bitcoin ha oggi un tecnicismo che lo rende inaccessibile agli sprovveduti, costringe ad un livello di comprensione e consapevolezza superiore rispetto ad altri mercati.

Molti hanno comprato bitcoin su piattaforme semplici da usare ma spesso di dubbia affidabilità, senza avere chiaro cosa sia e come funzioni bitcoin e investendo capitali sproporzionati rispetto alle loro possibilità.
Non c'è modo di salvare gli investitori incoscienti da sé stessi: sapranno sempre trovare modi nuovi con cui farsi del male. Si può solo investire in informazione ed educazione sul tema. Quanto all'affidabilità delle piattaforme: nel 2017 è partita al *Chicago Mercantile Exchange* la contrattazione dei derivati (futures) su bitcoin, mentre la compravendita del sottostante bitcoin (spot) avviene ancora su borse di scambio che non sono istituzioni finanziarie vigilate. Le migliori borse ottemperano già alla normativa su antiriciclaggio, prevenzione del finanziamento al terrorismo e adeguata verifica: bisognerebbe incoraggiarne l'inclusione nel sistema finanziario, marginalizzando banditi e fuorilegge. Il mercato dei bitcoin ha grande volatilità, anche a causa di volumi scambiati relativamente bassi che consentono ancora manipolazioni dei prezzi. Ci sono trader e speculatori che applicano tecniche inapplicabili o addirittura illegali sui mercati tradizionali. Se davvero si vuole difendere il risparmiatore, bisogna consentirgli una semplice e sicura operatività in bitcoin. La responsabilità ultima delle truffe e degli scandali che abbiamo visto nel mondo delle criptovalute è da ascriversi

fondamentalmente al fatto che regolatori ed intermediari finanziari non hanno finora fornito servizi legittimi e qualificati per entrare in questo mondo, lasciando gli investitori alla mercé di tanti ciarlatani.

4. La finanza

In molti sostengono che l'aumento di valore di bitcoin negli ultimi mesi del 2017 sia stato dovuto al lancio dei contratti *futures* sulla piazza di Chicago: perché?

Questi contratti sono regolati in dollari e non in bitcoin: si apre quindi la porta all'investimento in bitcoin per chi era impedito da difficoltà tecnologiche o vincoli regolamentari. Da un lato infatti ci sono difficoltà tecniche per custodire appropriatamente un asset puramente digitale non gestito da emittente centrale: manca esperienza e non sono ancora diffusi processi di sicurezza e custodia adeguati. Dall'altro lato, ricordiamo che l'Autorità Bancaria Europea dissuade le istituzioni finanziarie dal comprare, vendere o possedere bitcoin. Insomma, il *futures* regolato in dollari rende l'esposizione finanziaria a bitcoin semplice e praticabile per molti. Questo ha contribuito alla crescita dei prezzi, perché notevoli capitali premono per investire in bitcoin. D'altronde poi abbiamo visto una correzione significativa dei corsi: facile che oltre alle prese di profitto dei primi investitori, abbia contribuito anche la possibilità di andare *corti* bitcoin tramite il futures, insomma di venderli senza averli. I *futures* in sé sono strumenti neutrali.

Nella storia ogni innovazione è stata inglobata dalla finanza. I *futures* scambiati a Chicago non potrebbero essere la fine di bitcoin come "utopia" libertaria?

A Chicago per 50 anni hanno scambiato il *futures* sulla pancetta di maiale: con lodevole pragmatismo si compra e vende qualsiasi cosa interessi alle persone. Ma per ora mi sembra che siamo ben distanti da un'accettazione del fenomeno bitcoin da parte del mondo finanziario in generale.

La *Fia* (*Futures industry association*) ha scritto alla *Commodity futures trading commission*, l'ente che ha autorizzato il lancio dei futures, criticando la scelta, o almeno i modi.

Wall Street teme che la finanziarizzazione di bitcoin ne rappresenti il definitivo "sdoganamento", un punto di non ritorno. Bitcoin è percepito come nemico perché rappresenta valore che non discende da una autorità costituita e che è trasferibile senza

intermediari. La sua esistenza certifica che un sistema decentralizzato può essere più efficiente e sicuro rispetto agli attuali modelli.

Jamie Dimon, l'amministratore delegato di JP Morgan, considera bitcoin una frode che finirà male. Ha definito stupidi quelli che comprano bitcoin ed ha minacciato di licenziare chiunque nella sua banca lavori con bitcoin.
Il giorno, però, dopo alcuni suoi trader compravano *exchange traded note* legate a bitcoin sulla borsa svedese, sfruttando il calo di prezzo innescato da quelle dichiarazioni. Ma al di là dell'aneddotica, di fronte ai rischi di disintermediazione è vero che molti banker assumono posizioni di sostanziale ostilità, anche se magari le esprimono con minore veemenza. Gli *incumbent* non cercano davvero l'innovazione, anzi la temono: basti pensare a Blockbuster, BlackBerry o Kodak.

L'ostilità delle grandi banche sembra generalizzata.
Non aver compreso bitcoin per tempo ed averlo osteggiato impedisce adesso di riconoscere l'errore. Ed è innegabile che bitcoin sia cresciuto in un ecosistema che non ama il mondo della finanza. Ma l'ostilità, pur generalizzata, non è unanime. Ad esempio, Lloyd Blankfein, ex amministratore delegato di Goldman Sachs, si mostra più possibilista[13]: dice di non essere ancora arrivato ad una conclusione su bitcoin, ricorda che c'era scetticismo anche quando la carta moneta sostituì l'oro; addirittura ipotizza che bitcoin possa rappresentare una naturale progressione: come siamo passati da moneta garantita (redimibile in oro) a moneta fiduciaria (non redimibile), potremmo andare oggi verso "consensus money". L'alternativa miope è quella delle multinazionali musicali che hanno fatto la lotta agli MP3 ed al *file-sharing* col risultato che la musica liquida oggi non la compriamo da loro ma da iTunes, Amazon e Google.

5. Come funziona bitcoin

È vero che le transazioni bitcoin sono anonime?
Bitcoin esiste solo come bene scritturale, transazione registrata su un libro mastro digitale condiviso in modalità *peer-to-peer* tra i nodi di un network. Ogni nodo ha una copia di questo registro contabile pubblico, chiamato *blockchain*, sul quale sono annotati tutti i cambi di proprietà di bitcoin, in maniera totalmente trasparente per chiunque. Non c'è quindi anonimato, ma siccome le controparti di ogni transazione non sono attori identificati si parla di pseudonimato.

[13] https://www.cnbc.com/2017/11/09/cnbc-exclusive-cnbc-transcript-goldman-sachs-ceo-lloyd-blankfein-speaks-with-cnbcs-kayla-tausche-today.html

Se non è nominativamente associato, qual è il titolo di possesso di bitcoin?
I bitcoin appartengono a chi è tecnicamente capace di spenderli, cioè di trasferirli ad altri. Per trasferirli si usa la crittografia asimmetrica basata su chiave privata e chiave pubblica, tipica della firma digitale: chi conosce una chiave privata può firmare con quella una disposizione di trasferimento e la firma è verificabile da tutti i nodi utilizzando la corrispondente chiave pubblica. Siccome i bitcoin sono associati ad indirizzi che derivano univocamente dalle chiavi pubbliche, la chiave pubblica permette anche di constatare se i bitcoin che si vogliono trasferire siano effettivamente nella disponibilità dell'indirizzo corrispondente e quindi ultimamente del detentore della corrispondente chiave privata usata per firmare la transazione. Se la transazione è quindi complessivamente valida, viene registrata sulla blockchain mettendo i bitcoin trasferiti a disposizione di un nuovo indirizzo. Questo nuovo indirizzo deriva anch'esso da una chiave pubblica, la cui corrispondente chiave privata è a quel punto la sola che potrà spenderli ulteriormente. Insomma il possesso della chiave privata è il possesso dei bitcoin associati, perché consente di spenderli.

Chi certifica la spesa, chi aggiorna la blockchain?
Ogni transazione è validata da tutti i nodi della rete, ma la sua finalizzazione avviene quando entra nel registro transazionale chiamato blockchain, cioè catena di blocchi: le transazioni sono infatti accorpate in blocchi concatenati sequenzialmente. I blocchi possono essere creati da qualsiasi nodo (in questo caso chiamato nodo di *mining*, o *miner*), a patto che fornisca la *proof-of-work* prevista dal protocollo, cioè la prova di aver effettuato il lavoro computazionale necessario. È l'accumularsi di questo lavoro che rende sicura la blockchain: un agente malevolo che volesse manipolarla dovrebbe essere in grado di fare più lavoro dell'insieme di tutti i miner onesti.

Cosa motiva i nodi a svolgere questo lavoro computazionale?
Un incentivo economico: il nodo che crea un blocco è ricompensato con l'emissione di nuovi bitcoin, attraverso una transazione speciale (*coinbase*) inclusa nello stesso blocco. Il protocollo bitcoin socializza la rendita di signoraggio (la ricchezza che origina dalla creazione di moneta) per coprire i costi del network. Questa remunerazione è cruciale per incentivare il comportamento onesto dei miner: se un blocco contenesse transazioni invalide (o transazioni "valide" che tentano però di spendere due volte gli stessi bitcoin) verrebbe rigettato dagli altri nodi come invalido, con l'effetto di annullare anche la ricompensa del miner contenuta nel blocco. Si è innescato quindi un circolo virtuoso: i miner competono per la ricompensa di signoraggio ed investono in potenza computazionale; maggiore potenza computazionale rende il network più sicuro;

maggiore sicurezza fa crescere il valore di bitcoin; la remunerazione di signoraggio diventa quindi ancora più appetibile per i miner.

Sembra complicato…
Bitcoin combina in maniera inedita e creativa elementi di crittografia, teoria monetaria ed economica, sistemi distribuiti, teoria dei giochi. È complicato comprenderne la natura sinfonica che amalgama elementi così diversi: per questo spesso se ne colgono (e criticano) aspetti parziali, perdendo di vista l'insieme. Ma bitcoin si può usare in modo semplice, così come per telefonare non è necessario capire come funzioni la rete GSM.

6. Ico, forkcoin e altcoin

A proposito di innovazione finanziaria: nel 2017 e 2018 le Ico hanno raccolto miliardi di dollari. Di cosa si tratta?
Le *Initial coin offering* sono l'equivalente nel mondo delle criptovalute delle offerte pubbliche di acquisto azionarie. Potenzialmente rappresentano la disintermediazione dei Venture Capital: le startup raccolgono capitale in crittovaluta dagli investitori e li ricompensano con l'emissione di *token*, gettoni digitali che vengono quotati ed il cui principale *appeal* è far sognare apprezzamenti simili alla straordinaria rivalutazione di bitcoin. Per discriminare tra frodi e proposizioni legittime servono elementi tecnici e buon senso, ma sono rari in un mondo in cui il rumore mediatico è altissimo e gli esperti di settore preferiscono talvolta silenzi omertosi se non addirittura collusivi.

Perché bitcoin è rispettabile mentre questi token sarebbero discutibili?
Questi token non danno praticamente alcun diritto (per sfuggire alla regolazione come strumento di investimento), hanno utilità applicativa spesso trascurabile, possono essere inflazionati a discrezione dell'emittente. Il capitale in crittovaluta raccolto va nella disponibilità diretta dell'imprenditore senza nemmeno entrare nel recinto aziendale, per cui l'azienda può fallire e l'imprenditore godersi gli investimenti ricevuti. Spesso si tratta di schemi *pump&dump*: si *pompa* il prezzo del token con tecniche che su mercati regolati sarebbero reato, allettando investitori ingenui a impiegare quei capitali che poi si dissolveranno nella fase di *scarico* (*dump*), quando l'emittente beneficerà della vendita delle sue quote. Il livello di euforia crescente, innescato dalla rivalutazione delle criptovalute, ha reso talmente appetibili questi token che addirittura già in fase di emissione si registrano vere e proprie corse all'acquisto. In questo caso gli investitori sono spesso operatori di mercato avvertiti, tutt'altro che ingenui: consapevoli dello schema *pump&dump*, contribuiscono ad accelerare il *pump*, facendo schizzare i prezzi già in fase di emissione, per prendere beneficio anche loro in fase di *dump*.

Spesso godono di offerte scontate in fase di pre-emissione. Si tratta di implicite complicità fattuali, se non addirittura di espliciti accordi riservati, tecnicamente facilitati da piattaforme pubbliche di scambio che per incassare le commissioni transazionali non esitano a consentire la compravendita corsara di token improbabili e discutibili.

Nel 2017 abbiamo visto l'esplosione dei fork bitcoin: di cosa si tratta?
Sono derivazioni di bitcoin che tentano di cambiare alcune regole del protocollo; vengono tecnicamente realizzate come per gemmazione: condividono la storia transazionale di bitcoin fino al momento della separazione (*fork*) che, come fosse uno *stock split* o uno stacco dividendi, distribuisce automaticamente il nuovo coin ai possessori di bitcoin (*airdrop*). Di per sé la possibilità per chiunque di *forkare* bitcoin è una garanzia di libertà: nessuno è prigioniero di un determinato gruppo di sviluppatori, è sempre possibile per gli attori economicamente rilevanti coagularsi intorno alla "forma" di bitcoin che meglio rappresenta la loro visione e le loro necessità. Ma i tentativi visti finora hanno perseguito modifiche controverse che sono quindi rimaste minoritarie; si sono inoltre caratterizzati per la progressiva perdita di rilevanza: gli ultimi *forkcoin* hanno addirittura abbandonato qualsiasi finzione di dignità culturale o tecnologica.

Il primo fork, Bitcoin Cash, sembra aver trovato una sua stabilità…
È il tentativo velleitario di modificare bitcoin in chiave di maggiore utilizzabilità transazionale, ma l'espediente tecnico scelto, l'aumento della dimensione del blocco, ottiene solo di centralizzare il network nelle mani di pochi grandi miner e non scala davvero; bitcoin regge circa sei transazioni al secondo, VISA circa 60.000: non si può aumentare la dimensione del blocco di un fattore 10.000! Peraltro, su Bitcoin Cash ci sono oggi meno transazioni rispetto alla rete bitcoin: non interessa sostanzialmente a nessuno tranne che ai suoi supporter. Bitcoin Cash è cresciuto perché economicamente sostenuto da una cordata di imprenditori ostili a bitcoin, ma resterebbe trascurabile se non fosse che tenta insidiosamente di confondere utenti ed investitori che possono scambiarlo per il vero bitcoin.

Oltre a Ico e fork, sono tante le criptovalute ad essere cresciute molto: la leadership di bitcoin è insidiata.
Il successo di bitcoin ha innescato una pletora di tentativi emulativi (*alternative coin*, o più brevemente *altcoin*): il sito CoinMarketCap ne registra migliaia (inclusi token e forkcoin). La quasi totalità di questi cloni non apporta innovazione, manca di sostanza tecnica e meriti funzionali. Molti di questi sono cresciuti semplicemente perché avendo un prezzo basso sono stati percepiti come a maggior potenziale rispetto a bitcoin, un po' come capita con i *penny stock*. Insomma, pensando di aver perso il treno bitcoin, in

tanti cercano nuove opportunità: salgono su convogli merci di incerta destinazione, non hanno capito che il treno ad alta velocità bitcoin è appena partito. Questa, a mio avviso, rischia di essere la vera bolla che scoppierà.

Se bitcoin cresce è ragionevole, se crescono alternative a bitcoin si tratta invece di una bolla?
Lo so che sembra fazioso ed arrogante, ma sinceramente è così. Bisogna discriminare tra oro digitale ed il ciarpame di imitazioni; comprendere l'insensatezza fraudolenta delle Ico. Ognuno svolga le sue analisi, tragga le sue conclusioni e faccia le sue scelte: nel tempo si avvierà un processo di selezione naturale ed i nodi verranno inevitabilmente al pettine. Quando succederà, i capitali in fuga non potranno che approdare alla spiaggia sicura di bitcoin, il bene rifugio per eccellenza.

La sua critica gli altcoin sembra essere una opinione senza prove metodologicamente fondate.
Non è possibile farsi carico di smontare in maniera sistematica e documentata qualsiasi corbelleria venga proposta. Investo il mio tempo su temi e situazioni rilevanti, che altri perdano il loro tempo ed i loro investimenti...

Tra migliaia di cloni qualcosa di interessante deve esserci...
L'emergere di alternative è salutare concorrenza per bitcoin: questi altcoin sperimentano nuove tecniche e si impara dai loro tentativi e dai loro fallimenti. Finora però solo pochi hanno mostrato peculiarità distintive che li hanno resi, con differenti e controversi livelli di qualità, meritevoli di considerazione. Ethereum ha l'ambizione di essere un computer globale piuttosto che oro digitale; Litecoin è talmente simile a bitcoin da avere quasi assunto il ruolo di piattaforma di test dove verificare in anteprima le nuove funzionalità che potrebbero poi essere adottate per bitcoin; Monero e ZCash forniscono vero anonimato transazionale; Ripple incarna la declinazione di queste tecnologie in una chiave più affine al mondo della finanza tradizionale e regolamentata.

Ripple è tra le criptovalute con maggiore capitalizzazione ed ha avuto performance superiori a bitcoin nel 2017.
Immaginiamo che io emetta l'AmetranoCoin, che tutti i 21 milioni di coin appartengano a me, che io ne metta in circolazione solo pochi e poi ricompri un millesimo di coin per un dollaro: difficile sostenere che per questo gli AmetranoCoin abbiano una capitalizzazione di 21 miliardi di dollari. Ripple ha creato una piattaforma multi-asset, dove il coin XRP, a gestione totalmente centralizzata, è usato sia come carburante per transazioni finanziarie, sia come collaterale di garanzia. XRP potrebbe essere utile per le transazioni interbancarie che coinvolgono valute e paesi diversi (*correspondent*

banking), ma quando le banche dovessero riconoscerlo, potrebbero creare un loro equivalente consorzio alternativo. La tecnologia può essere interessante, il coin non lo è ed in ogni caso non è una crittovaluta decentralizzata.

Ethereum però sembra rappresentare una reale alternativa a bitcoin.
Bitcoin è oro digitale per trasferimenti di valore incensurabili; ether, la moneta della piattaforma Ethereum, è il carburante per attività computazionali incensurabili. Ethereum vuole essere un super-computer distribuito, capace di ogni tipo di elaborazione (in gergo tecnico è *Turing-complete*) con memoria persistente globale e ricchezza di possibili stati. Prediletto da quegli informatici che trovano bitcoin noioso nella sua semplicità concettuale, è straordinariamente versatile e permette sofisticati *smart contract*: contratti crittografici i cui termini sono rispettati dall'esecuzione automatica del software che li definisce. Qualcuno sogna di usarli un giorno per il trading di derivati, per ora è una specie di parco giochi che consente la cura dei *cryptokitties*, gattini digitali scambiati in rete per decine di migliaia di dollari. La *killer application* di Ethereum è stata l'aver consentito le Ico: difficile esserne orgogliosi. In realtà la grande ambizione e complessità di Ethereum lo rendono proporzionalmente fragile: lo stesso Vlad Zamfir, ricercatore di punta dell'Ethereum Foundation, lo ha più volte definito "non sicuro né scalabile, un'immatura tecnologia sperimentale: inaffidabile per applicazioni critiche"[14]. Ethereum promette molto ma è per ora fragile: se alla fine dovesse mantenere le promesse potrebbe diventare uno straordinario successo. Io sono scettico, ma potrei sbagliarmi e sono comunque grato di una competizione tecnologica che fa bene anche a bitcoin. Dagli errori di Ethereum stiamo imparando tutti tanto.

Si parla di innovazioni decisive sulla piattaforma Ethereum: lo sharding dovrebbe ridisegnare la tecnologia blockchain, Casper dovrebbe sostituire la dispendiosa proof-of-work, la virtual machine che esegue il codice dovrebbe essere rimpiazzata con una architettura migliore e scalabile.
Il suo elenco mostra come sostanzialmente dell'Ethereum attuale non funzioni praticamente nulla e si stia tentando di cambiare in corsa, senza nemmeno sapere quale sia il processo di governo e controllo, componenti tecnologiche delicatissime. Peraltro, nulla di quello a cui accenna lei è pronto: si tratta di ricerca futuristica e per ora spesso infondata: io sono pessimista sulla tenuta nel tempo di Ethereum.

Non mi dica che apprezza Monero, la crittovaluta che garantisce l'anonimato assoluto nelle transazioni.

[14] https://twitter.com/vladzamfir/status/838006311598030848

Il mio apprezzamento è solo per bitcoin: Monero, come gli altri altcoin, non ha le carte in regola per una sostenibilità futura. Monero però sperimenta tecniche crittografiche di avanguardia (crittografia omomorfa, *ring signature*, *zero-knowledge proof*s) che in futuro potrebbero essere adottate per migliorare la confidenzialità delle transazioni bitcoin.

7. Privacy e futuro della moneta

La confidenzialità delle transazioni finanziarie favorisce i criminali.
Siamo in un mondo in cui la privacy è sempre più minacciata, ma paradossalmente sembra interessare solo i criminali: eppure si tratta di un diritto fondamentale riconosciuto nella Dichiarazione dei Diritti dell'Uomo. Anche la nostra Costituzione sancisce che la "libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili", ma accettiamo che il monitoraggio di massa delle conversazioni (e di quelle conversazioni particolari che sono le transazioni finanziarie) sia la prassi usuale a cui affidiamo la nostra sicurezza.

Le persone oneste non hanno nulla da nascondere.
Le rispondo con una citazione di Edward Snowden: "rinunciare alla privacy perché non si ha niente da nascondere è come rinunciare al diritto di parola perché non si ha niente da dire".

È ragionevole sacrificare la privacy per la sicurezza: durante le guerre alcuni diritti vengono temporaneamente sospesi.
In questo caso però si tratta solo di una pericolosa forma di pigrizia intellettuale e operativa: decentralizzazione e crittografia stanno rendendo comunicazioni e transazioni finanziarie imperscrutabili all'analisi. Il monitoraggio di massa del grande fratello ha quindi inevitabilmente i giorni (magari gli anni) contati: da un lato sarà sempre meno efficace, dall'altro comporta gravi rischi per la privacy di tutti. Insomma, i malintenzionati sfuggono ai controlli, mentre i cittadini onesti subiscono violazione arbitrarie e generalizzate della loro privacy. Sarà meglio prenderne atto e adeguare strumenti d'indagine e criteri del diritto, senza attardarci in battaglie di retroguardia destinate al fallimento. Sono elementi che fanno parte di quel radicale cambio di paradigma che rende obsolescenti molte prassi su cui fondiamo la stabilità del nostro vivere civile.

La sicurezza quindi non la preoccupa?

Mi preoccupo della sicurezza e della libertà. Come cittadini ci propongono di barattare la privacy con la sicurezza, ma non funzionerà e rischia di mettere a repentaglio la libertà nostra e dei nostri figli. Ci lasciamo cullare dalle "magnifiche sorti e progressive" della democrazia ma dimentichiamo le dittature in Cina, Corea del Nord, Myanmar, Venezuela e che 80 anni fa dalle nostre parti c'erano Hitler, Mussolini e Stalin. Dobbiamo temere strumenti di controllo di massa che i regimi totalitari di domani potrebbero usare con efficacia inedita e spaventosa.

Addirittura bitcoin paladino dei diritti umani?
Bitcoin è già oggi una cartina tornasole della democrazia essendo sostanzialmente avversato in paesi come Cina, Russia e Venezuela. Chi è perseguitato o vive in uno Stato sull'orlo della bancarotta con bitcoin può portare in salvo i suoi risparmi. In quanto oro, bitcoin è un bene rifugio non manipolabile: una "garanzia" per i propri risparmi, al riparo da inflazione o interventi predatori. Se un paese come il Venezuela o la Grecia va in crisi, bitcoin difende la proprietà privata dalle grinfie del Leviatano.

Certo, ma questo aiuta anche la fuga all'estero dei capitali e l'evasione fiscale.
Ritengo che la lotta ad un fisco oppressivo vada condotta a livello politico e non con pratiche illegali, ma queste possibilità tecniche sono come valvole di sfogo che impediscono soprusi eccessivi. Le cito Luigi Einaudi, economista di fama internazionale, Presidente della Repubblica ed uno dei padri della Repubblica Italiana: "Gli esportatori illegali di capitale sono benefattori della Patria, perché i capitali scappano quando i governi dissennati e spendaccioni li dilapidano, e allora portandoli altrove li salvano dallo scempio e li preservano per una futura utilizzazione, quando sarà tornato il buon senso".

Abbattiamo quindi il sistema attuale? È indubbio che bitcoin abbia una caratterizzazione anarchica ed antagonista.
Non mi sbilancio sulle caratterizzazioni politiche, anche perché l'eterogenesi dei fini spesso rende poco rilevanti queste considerazioni. Di certo, dopo millenni in cui Cesare ha avocato a sé il monopolio sulla moneta, ci sembra incomprensibile, perfino rivoluzionario, constatare che tale monopolio non è più tecnicamente necessario. Ma non è necessario per questo sposare la cultura anarchica, io ad esempio ne rifuggo: al Leviatano occorre tagliare le unghie, ma se lo uccidiamo rischiamo di ritrovarci con mostri peggiori, quelli storicamente sconfitti dalla *Rule of Law*. Molto meglio la cultura libertaria della scuola austriaca, quella del premio Nobel per l'economia Friedrich von Hayek: contro il monopolio governativo della moneta, per la competizione di mercato

tra monete a corso legale e monete private[15]. Il libero mercato e la concorrenza permetteranno l'emergere di buone monete e buone prassi monetarie, il monopolio invece ci dà inevitabilmente un prodotto scadente.

Quindi l'obiettivo è far saltare le banche centrali?
No, non condivido posizioni antagoniste. Non penso sia utile far saltare le banche centrali, anche perché le loro monete muoiono da sole: hanno 27 anni di vita media, non tutte sono longeve come la sterlina inglese (che comunque dalla sua nascita nel 1694 ha perso il 99.5% del suo valore). L'obiettivo è piuttosto fornire loro una concorrenza leale ed efficace che inneschi un circolo virtuoso: la competizione di mercato farà bene anche alle monete tradizionali.

Hayek voleva monete tra loro competitive nel garantire la stabilità dei prezzi: non avrebbe amato bitcoin. Inoltre lei si contraddice: aveva detto che bitcoin non è moneta.
Anche l'oro all'inizio è stato utilizzato direttamente come moneta: in seguito monete più evolute ne hanno superato alcuni limiti senza per questo renderlo obsoleto. O meglio: originariamente messo a garanzia della moneta, i governi hanno poi trovato il modo di marginalizzare l'oro per ottenere maggiore libertà in termini di inflazione (ed infatti da quando la convertibilità aurea è stata soppressa il debito pubblico è cresciuto senza freni in tutto il mondo). Bitcoin abilita nuove possibilità di ingegneria monetaria. Nei prossimi anni renderà possibile la creazione di monete digitali fiduciarie e criptovalute decentralizzate con politica monetaria algoritmica ma elastica, entrambe garantite da bitcoin come asset di riserva[16]. Come il *gold standard* un tempo, domani il *bitcoin standard*. Queste monete saranno "pagabili a vista" in bitcoin, garantiranno la stabilità del potere di acquisto rispetto a un paniere, saranno in competizione con le monete a corso legale ma anche tra di loro (soprattutto nella definizione del paniere più ragionevole): le chiamo Hayek Money[17] perché realizzeranno il sogno dell'economista austriaco.

Chi introdurrà queste nuove monete private?
L'iniziativa privata, portata avanti da singoli, gruppi ed organizzazioni, ad esempio Libra proposta da Facebook. Poi, perché no, magari anche da qualche piccolo stato che si voglia giocare una partita geopolitica strategica. Il punto cruciale sarà garantire riserve

[15] *Denationalisation of Money: The Argument Refined*, Friedrich A. Hayek; https://mises.org/library/denationalisation-money-argument-refined
[16] *The Cryptocurrency Frontier in Commodity Monetary Standard*, Ferdinando M. Ametrano; https://ssrn.com/abstract=2508296
[17] *The Cryptocurrency Price Stability Solution*, Ferdinando M. Ametrano; https://ssrn.com/abstract=2425270

affidabili e verificabili: per questo bitcoin è in *pole position* per definire un nuovo *gold standard*.

Il gold standard è stato abbandonato perché aveva chiari limiti.
Nel 1966 Alan Greenspan, non immaginando che sarebbe in futuro diventato chairman della Federal Reserve, scriveva[18]: "la spesa in deficit è semplicemente uno schema per la confisca di ricchezza. L'oro ostacola questo processo insidioso. Si erge come protettore dei diritti di proprietà. Se uno capisce questo, allora non ha difficoltà a comprendere l'antagonismo degli statisti verso il gold standard". In ogni caso, consenta almeno agli ingenui come me di sognare la possibilità che un nuovo bitcoin standard possa competere in un libero mercato con le monete a corso legale. Poi vedremo quale soluzione prevarrà.

8. Libra

Che differenza c'è tra Bitcoin e Libra, il coin proposto da Facebook?
Bitcoin vuole essere l'equivalente digitale dell'oro: scarsità in ambito digitale incensurabile, non controllata da nessuno, decentralizzata. Libra vorrebbe essere, invece, una criptovaluta non speculativa, perché con valore stabile grazie a riserve in valute e titoli di stato. Sfruttando gli oltre due miliardi di utenti Facebook, mira ad essere una moneta globale, utilizzabile per i pagamenti e le rimesse internazionali, integrata anche nei sistemi di messaggistica come WhatsApp e Messenger. È una soluzione centralizzata controllata dalla Libra Association, la no-profit costituita in Svizzera da Facebook ed i suoi partner. Al lancio dell'iniziativa nell'associazione erano presenti tra gli altri: Mastercard, Visa, PayPal, Vodafone, Uber, Spotify, Andreessen Horowitz, Coinbase, Xapo, Stripe; mancavano invece le banche e le grandi aziende tecnologiche che competono con Facebook.

Libra è una criptovaluta?
Utilizza tecniche crittografiche ed un network peer-to-peer, soddisfa quindi i requisiti che il senso comune attribuisce al concetto di criptovaluta. Ha anche l'ambizione di essere *permissionless,* ma il controllo centralizzato avrà molte sfide, sia in termini di governo della piattaforma (cosa succede in caso di contrasti tra i partner) che di requisiti regolamentari (ad esempio, il rispetto della normativa antiriciclaggio e di contrasto al finanziamento del terrorismo). Preoccupa, inoltre, il tema della privacy, su cui già in

[18] *Gold and Economic Freedom*, Alan Greenspan; http://www.constitution.org/mon/greenspan_gold.htm

passato Facebook ha avuto episodi pessimi: è inquietante l'idea che domani possa conoscere anche tutte le nostre transazioni finanziarie.

Quando si potrà utilizzare Libra?
Il lancio era previsto per il primo semestre 2020, ma i governi ed i regolatori internazionali si stanno opponendo decisamente.

Cosa cambierebbe con l'arrivo di Libra?
Potrebbe far superare la diffidenza verso le criptovalute ed in generale le forme digitali e private di trasferimento del valore, ponendo fine al "paleolitico" delle transazioni finanziarie lente (anche oltre due giorni), costose, costrette in definiti confini nazionali o valutari. E questo potrebbe avvantaggiare anche Bitcoin, che di suo aggiunge il non essere inflazionario (non è creato per perdere valore in termini di potere d'acquisto): Libra moneta transazionale, stabile nel potere di acquisto ed utile per i pagamenti, Bitcoin bene rifugio incensurabile, attraente dal punto di vista speculativo. Perdono invece terreno R3, PayPal, SatisPay, le *alt-coin* con ambizioni velleitarie come Bitcoin Cash, Ripple, LiteCoin, ma sopratutto Tether ed i cosiddetti *stablecoin*, cioè quelle criptovalute che puntano come Libra a mantenere la parità di potere d'acquisto con le monete tradizionali. Anche Lightning Network, la soluzione tecnologica di secondo livello basata su Bitcoin che punta a superarne i limiti transazionali, potrebbe soffrire della concorrenza di Libra.

Se arrivasse Libra che bisogno ci sarebbe di Bitcoin?
Oggi Libra non ci sarebbe se la strada non l'avesse aperta Bitcoin dieci anni fa. E di Bitcoin c'è bisogno come e più di prima, se si comprende il suo ruolo nella storia della moneta. Su questo argomento può essere utile il mio intervento TEDx[19]: bitcoin come bene di riserva che si potrà utilizzare a garanzia di nuove monete private. Il punto debole di Libra, oltre alla censurabilità, sono proprio le riserve a garanzia, denominate in valute inflazionarie che perdono valore: qualcuno immagina la possibilità di includere anche Bitcoin nelle riserve per risolvere questo problema.

9. La blockchain oltre bitcoin

L'oro fisico ha una utilità "intrinseca" in gioielleria ed applicazioni industriali, bitcoin non ha alcuna utilità.
Esiste la gioielleria dell'oro digitale, cioè una applicazione non monetaria di bitcoin: è la cosiddetta notarizzazione. L'*hash-value* di una base dati, cioè un identificativo

[19] https://www.youtube.com/watch?v=3XRF9erlMmU

equivalente ad una univoca impronta digitale, viene associato ad una transazione bitcoin, come se venisse scritto nel campo "causale" della transazione. Il sistema di sicurezza che impedisce la manipolazione della transazione bitcoin garantisce anche l'immutabilità e la datazione (marcatura temporale) non ripudiabile dell'*hash-value*. Viene quindi implicitamente certificata l'esistenza di quella base dati, consentendo a tutti di verificarne la mancanza di alterazione e la datazione. Esiste anche un protocollo aperto, *OpenTimestamps*[20], che definisce uno standard di notarizzazione estremamente scalabile che non impatta negativamente sul funzionamento del network bitcoin. La notarizzazione può sembrare banale… in realtà è molto potente poiché nel futuro il mondo potrebbe "parassitare" la sicurezza di bitcoin per mettere in sicurezza tutte le basi dati ed altri sistemi transazionali: ha quindi una applicazione industriale. Se bitcoin è oro digitale, la notarizzazione è l'equivalente della gioielleria: inessenziale per l'oro, ma efficacissima nel mostrarne la bellezza.

Ma la notarizzazione è una applicazione della blockchain, cioè della tecnologia su cui si basa bitcoin. Non serve bitcoin, basta la blockchain.
Falso. Non esiste blockchain senza un asset digitale nativo[21]. La blockchain in sé è solo una struttura dati poco flessibile, disegnata per rendere complicata la sua manipolazione. Rappresenta un "registro condiviso" (nel caso di bitcoin il registro delle transazioni) su cui i nodi della rete raggiungono il consenso. Il consenso distribuito in rete è un problema di *computer science* sostanzialmente irrisolvibile; bitcoin lo risolve con lo stratagemma di teoria dei giochi spiegato prima: un incentivo economico affinché i nodi della rete siano onesti. Questo è possibile solo avendo un asset digitale nativo sulla blockchain, quindi sfruttando la ricchezza che origina dal signoraggio per incentivare l'onestà e coprire i costi del network. È invece un grande *bluff* parlare di "registro condiviso" senza spiegare come si possa raggiungere il consenso sullo stesso.

Eppure ci sono importanti iniziative industriali che puntano sulla blockchain senza bitcoin.
Non abbiamo ancora visto alcuna applicazione concreta della chimera nota come "blockchain senza bitcoin". Nulla nemmeno da consorzi come R3, HyperLedger o l'Enterprise Ethereum Alliance, che hanno ottenuto investimenti per centinaia di milioni ed hanno tra i partecipanti tutte le principali istituzioni finanziarie, società tecnologiche e di consulenza. Bisogna saper distinguere tra euforiche esagerazioni e la cruda realtà[22]. Al massimo, si può intendere come tecnologia blockchain il possibile

[20] https://opentimestamps.org/
[21] https://www.finextra.com/videoarticle/1241/blockchain-needs-a-native-digital-asset
[22] *Bitcoin, Blockchain, and Distributed Ledgers: Between Hype and Reality*, Ferdinando M. Ametrano; https://goo.gl/Z9OeHt

rafforzamento di processi esistenti con tecniche crittografiche rese popolari da bitcoin: parlo spesso di database con steroidi crittografici. È un po' come se nell'esplosione nucleare di bitcoin, il *fallout* radioattivo sia rappresentato dalla crittografia applicata. Confucio diceva "quando un uomo saggio indica la luna gli stolti guardano il dito": qui la luna è bitcoin e il dito è la blockchain.

Ferdinando, se c'è una cosa su cui tutti sono d'accordo, anche i critici di bitcoin, è proprio la potenzialità della tecnologia blockchain.
Alla fine degli anni novanta, quando Internet conosceva la sua prima ampia diffusione, era letteralmente impossibile immaginare che un giorno sullo *stack* tecnologico TCP/IP sarebbero stati costruiti modelli di business come Amazon, Facebook, Google. Allo stesso modo oggi fatichiamo ad immaginare quali innovative potenzialità sapranno realizzarsi su bitcoin, cioè sullo *stack* tecnologico del TCP/IP del valore. Ma saranno iniziative che sfruttano la scarsità digitale, la possibilità di trasferire valore senza intermediari ed eventualmente la resilienza del sottostante registro contabile blockchain, non certo i generici miglioramenti di processi tradizionali ottenuti attraverso la taumaturgica evocazione di una indefinita tecnologia blockchain.

Lei torna sempre alla centralità della scarsità digitale rispetto alla tecnologia.
Sì, questo è il cuore del fenomeno bitcoin e blockchain, perché crea valore e permette interazioni economiche. Internet oggi è fondamentalmente la possibilità di comunicare senza censure accoppiata alla capacità di distribuire e consumare contenuti liberamente: quello che mancava era la possibilità di transazioni economiche senza intermediari. Bitcoin abilita questo aspetto completando la vera *agorà* elettronica, la piazza principale della nostra *polis* digitale, la realizzazione del sogno *cypherpunk*.

Ma i sistemi di pagamento attuali sono già piuttosto efficienti.
Per ora non direi lo siano davvero. Siamo in un mondo dove l'enciclopedia si è trasformata in Wikipedia, la musica ed i film sono diventati liquidi, la posta si è fatta elettronica; inoltre l'accesso a queste risorse è continuo, la comunicazione istantanea: c'è quindi l'aspettativa che una evoluzione simile avvenga per il sistema finanziario e bancario. Con un numero di telefono o un email possiamo trasferire istantaneamente quantità rilevanti di dati a costo marginale nullo, ma se vogliamo trasmettere i pochi byte che rappresentano la nostra ricchezza possiamo farlo tipicamente solo dalle 9 alle 5, dal lunedì al venerdì, pagando una commissione e sopportando due giorni di ritardo nell'esecuzione. Le cose stanno lentamente cambiando, ma per ora i costi sono alti e l'efficienza scarsa: tra dieci anni guarderemo indietro e la situazione attuale ci sembrerà ridicola.

Un po' tutte le banche centrali stanno sperimentando con queste tecnologie: vedremo monete a corso legale sulla blockchain?

Bisogna capire bene di cosa parliamo. Se ci riferiamo a moneta di banca centrale, noi semplici cittadini vi accediamo solo nella forma di banconote e monete metalliche. I saldi dei nostri conti correnti sono moneta di banca commerciale, cioè la promessa che quando ci presenteremo allo sportello ci verrà dato quel corrispettivo in moneta di banca centrale. L'importante è non presentarci tutti assieme allo sportello, perché le banche commerciali tutta quella moneta di banca centrale non ce l'hanno davvero. Se avessimo accesso diretto a moneta di banca centrale in forma elettronica, è evidente che le banche commerciali non riuscirebbero più a fare raccolta: tutti infatti preferirebbero detenere la liquidità in moneta elettronica di banca centrale, cioè di una banca che per definizione non può fallire perché quella moneta la stampa a piacimento. Questo concetto è stato espresso chiaramente nel 2016 da Mike Carney[23], Governatore di Bank of England, e nel 2017 da Jens Weidmann[24] di Bundesbank. Quanto alle banche commerciali, accedono già a moneta di banca centrale in forma elettronica: non hanno quindi bisogno della blockchain.

Niente blockchain per le banche centrali?

Si può tentare la digitalizzazione del contante, cioè la creazione di moneta di banca centrale al portatore e non tracciata, che sostituisca il contante per le piccole spese. Per questo scopo tecnologie distribuite come la blockchain, seppur in questo caso sostanzialmente centralizzate, possono essere utili. Ho collaborato a progetti con questa ambizione: potrebbe essere un'opportunità storica, ma l'impressione è che l'ossessione del controllo di qualsiasi transazione finanziaria, quel mostro pericoloso e oppressivo chiamato *cashless society*, sia oggi dominante. L'effetto sarà che perderemo anche questa opportunità a vantaggio di criptovalute private, aggravando quei rischi sistemici che vorremmo controllare abolendo il contante.

A quali rischi si riferisce?

Quello di accelerare in maniera disordinata e pericolosa la pur benefica progressiva riduzione del ruolo dei governi e della loro capacità di tassare. Se le valute con corso legale non daranno una esperienza di pagamento semplice, istantanea, transnazionale, multivaluta, accessibile anche a non bancarizzati, rischiano di trovarsi superate da bitcoin e soprattutto da quelle nuove monete stabili nel potere di acquisto rese possibili dalla redimibilità in bitcoin di cui abbiamo parlato prima. Lo aveva previsto Milton

[23] http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech914.pdf
[24] https://www.bundesbank.de/Redaktion/EN/Reden/2017/2017_06_14_weidmann.html

Friedman, anche lui premio Nobel per l'economia, quando nel 1999 profetizzò bitcoin[25]: "Una fonte di ottimismo affidabile è la crescita di Internet, tra i cui principali effetti ci sarà la riduzione della capacità dei governi di raccogliere le tasse. [...] Internet sarà una delle forze principali nel ridurre il ruolo dei governi. L'unica cosa che manca, ma che verrà sviluppata presto, è un contante digitale elettronico affidabile, un metodo che permetta di trasferire valore attraverso Internet da A a B senza che A e B si conoscano; così come posso dare un biglietto da $20, non c'è traccia della sua provenienza e non c'è bisogno che io sia conosciuto".

Christine Lagarde del Fondo Monetario Internazionale si è mostrata aperta all'adozione di queste tecnologie: non sarebbe naturale immaginare un oro digitale targato Fondo Monetario Internazionale?

Sarebbe certamente ragionevole! Ma anche qui ci sono difficoltà oggettive e miopie strategiche che frenano. Il Fondo Monetario Internazionale (FMI) è dal 1969 che promuove i Diritti Speciali di Prelievo (DSP): un bene sintetico proposto come bene di riserva al posto dell'oro, ma focalizzato anche a ridurre il ruolo di predominio del dollaro statunitense come bene di riserva. Questi DSP hanno ottenuto un successo solo moderato, perché a livello geopolitico gli Stati Uniti non vogliono rinunciare al privilegio, economicamente decisivo, di avere la loro moneta come bene di riserva per eccellenza. Un oro digitale promosso dal FMI incontrerebbe le stesse resistenze. Inoltre è difficile immaginare che il FMI possa creare un oro digitale al portatore, non tracciato, messo in sicurezza da una potenza computazionale non controllata, rinunciando anche solo in parte alle rendite di signoraggio.

Maduro in Venezuela propone il Petro, la Russia pare abbia studiato il criptorublo: ci sono giochi geopolitici attorno alle criptovalute?

Per ora si tratta di enunciazioni velleitarie: una crittovaluta governativa è un ossimoro, a maggior ragione quando si tratta di dittature che non vogliono realizzare qualcosa di decentralizzato e incensurabile. Maduro vorrebbe rifarsi una verginità deflattiva, ma non sarà il travestimento da crittovaluta a dargliela. La Russia vuole probabilmente familiarizzare con la tecnologia, per imparare a reprimere ed eventualmente ad attaccare con queste armi. C'è la Corea del Nord che accumula bitcoin, anche con attacchi predatori e terroristici. Le criptovalute saranno davvero strumenti di posizionamento geopolitico: ci sono potenze economiche che potrebbero considerare nuove valute, garantite da bitcoin come asset di riserva, per portare sfide epocali sullo scenario monetario internazionale.

[25] https://www.youtube.com/watch?v=onn34J74dnU

10. I punti deboli di bitcoin

Bitcoin vanta di essere decentralizzato, ma la maggioranza della rete è in Cina.
La maggioranza dei nodi della rete non è in Cina: in Cina si è concentrato negli ultimi anni il 70-80% della potenza computazionale della rete bitcoin, il cosiddetto mining. Il mining è quella cruciale attività dei nodi della rete che, finalizzando le transazioni, impedisce che un bitcoin possa essere speso due volte. Questa attività è profittevole solo con hardware ottimizzato per le particolari operazioni computazionali richieste e su ampie economie di scala; sono quindi nate *mining farm* e *mining pool* intrinsecamente oligopolistici. Ma non esistono barriere all'ingresso e nel tempo gli oligopolisti sono cambiati. Ma soprattutto il mining non è il cuore del consenso distribuito che caratterizza bitcoin, la cui incensurabilità è garantita dagli oltre diecimila nodi che non fanno attività di mining e sono distribuiti in tutto il mondo, concentrati particolarmente in Europa e negli Stati Uniti.

Ma si parla sempre dell'attacco del 51%, non è una eventualità pericolosa?
Il 51% del mining non può validare una transazione invalida, né rubare o confiscare bitcoin a proprio vantaggio: la crittografia lo impedisce. Potrebbe però effettuare una doppia spesa: una transazione validata viene ricompensata con un bene o servizio, ma viene poi cancellata, sostituendola con una transazione alternativa dove i fondi sono tolti al destinatario "legittimo". Un attacco del 51% potrebbe anche censurare sistematicamente alcune transazioni, o persino tutte le transazioni. In tutti questi casi l'affidabilità del network verrebbe danneggiata gravemente, con conseguente perdita del valore di bitcoin. Insomma i miner ucciderebbero la gallina dalle uova d'oro che li remunera con l'emissione di nuovi bitcoin: essendo agenti economici razionali, è molto difficile che si lancino in un simile attacco. Ed infatti quando in passato una *mining pool* ha raggiunto il 51%, ha invitato i suoi associati a collegarsi con pool alternativi per ridurre la posizione di dominanza.

Quindi la centralizzazione del mining non la preoccupa?
La centralizzazione del mining è di per sé una preoccupazione legittima, ma bitcoin ha dimostrato sul campo di resistere anche all'oligopolio del mining: a novembre 2017 i miner cinesi, d'accordo con alcune delle principali aziende dell'ecosistema bitcoin, hanno tentato unilateralmente di cambiare le regole del protocollo, per consentire un maggior numero di transazioni al secondo, ma hanno dovuto abbandonare l'iniziativa e registrare un sonoro fallimento.

Perché hanno fallito?
Il *futures* sul coin da loro promosso, il cosiddetto *bitcoin2x*, aveva una quotazione di mercato pari ad un decimo del bitcoin tradizionale. Insomma il mercato ha mostrato di non apprezzare il bitcoin modificato: per i miner, la cui attività sarebbe stata retribuita con quel coin, andare avanti diventava economicamente folle. Il protocollo bitcoin ha dimostrato ancora una volta di essere robusto: i suoi incentivi economici lo rendono resiliente a tentativi di manipolazione.

Ma un attaccante malevolo capace di spendere le risorse necessarie a raggiungere il 51% della potenza computazionale, senza doverne ricavare profitto direttamente, non potrebbe fermare bitcoin?
Un simile attaccante, forte della maggioranza del potere computazionale, potrebbe secondo le regole del protocollo bitcoin sopraffare gli altri miner ed aggiornare una blockchain con blocchi vuoti, censurando le transazioni e rendendo il network non funzionale. Ma questo blackout non durerebbe: i nodi degli agenti economicamente significativi si coordinerebbero per un cambio di protocollo che possa rendere obsoleto l'hardware dell'attaccante (cambiando la tipologia di problema computazionale sottostante la proof-of-work) o comunque invalidare gli aggiornamenti censurati del registro transazionale a vantaggio di aggiornamenti legittimi. Un cambiamento di protocollo quasi impossibile da concordare nella normalità operativa, ma che verrebbe eseguito certamente in una situazione di attacco.

Ci sono allarmi per il consumo energetico legato al mining ed alla proof-of-work. Già oggi è comparabile al consumo dell'intera Irlanda o Danimarca e continua ad aumentare: in molti lo trovano irresponsabile.
Stime del 2018 identificavano per bitcoin un consumo di circa 8 TWh: se guardiamo agli Stati Uniti si tratta di un ottavo di quanto consumano i data-center, lo 0.21% dei consumi totali. È un consumo inferiore agli 11 TWh impiegati a livello globale per la produzione di banconote e monete metalliche; è decisamente inferiore ai 132 TWh legati all'attività estrattiva delle miniere di oro[26]. E sappiamo dall'esperienza dei data-center che i consumi non aumentano linearmente con la crescita della potenza computazionale, perché subentrano sempre maggiori efficienze: lo stesso accadrà per le mining farm. Ma possiamo fare considerazioni ancora più radicali. In Cina nel 2016 la rete idroelettrica Yunnan ha dissipato 95 TWh, per impossibilità tecnica di consumare quell'energia[27]: di fatto il mining ha finora prosperato in Cina principalmente perché usa queste risorse,

[26] https://www.bloomberg.com/view/articles/2017-12-07/bitcoin-is-greener-than-its-critics-think
[27] https://www.thethirdpole.net/en/2017/04/28/hydropower-boom-in-china-and-along-asias-rivers-outpaces-regional-electricity-demand/

sfruttando le inefficienze del sistema di produzione. California, Canada e Germania sperimentano surplus di produzione (rispettivamente da solare, idroelettrico ed eolico) che portano a prezzi negativi dell'energia. In futuro non è impossibile immaginare che il mining proof-of-work potrebbe semplicemente assorbire il surplus energetico globale, che crescerà con la nostra capacità di estrarre energia da fonti rinnovabili.

Non si potrebbero usare metodologie alternative per la sicurezza di bitcoin?
Sono allo studio forme di consenso distribuito che non siano costose come la proof-of-work, la più famosa è probabilmente *proof-of-stake*. Ma si tratta per ora di lavori teorici, non applicabili per mettere in sicurezza un network che oggi vale centinaia di miliardi di dollari. Non basta che un'idea funzioni su carta, in laboratorio o in ambiti produttivi economicamente trascurabili: nuove forme di consenso distribuito potranno affermarsi solo se dimostreranno di difendere significativi capitali economici per lungo tempo in un contesto *adversarial*, cioè dove agenti malevoli abbiano forti incentivi ad attaccare. Per farlo dovranno essere investite non solo notevoli energie di ricerca teorica, ma occorrerà mettere a rischio rilevanti capitali e validare empiricamente su un lungo periodo di tempo.

Quando l'emissione di Bitcoin finirà per il raggiungimento dei 21 milioni, come saranno remunerati i miner?
L'evento è previsto intorno al 2140… mi dispiace darle una cattiva notizia, ma io e lei in quella data saremo defunti da un pezzo. Scherzi a parte, la domanda è intellettualmente legittima. Stiamo già osservando che le commissioni transazionali acquisiscono un peso sempre maggiore nella remunerazione dei miner, potrebbero soppiantare completamente la retribuzione proveniente dall'emissione di nuovi bitcoin. Se così non fosse, ci sono circa 120 anni per mettere a fuoco gli incentivi che possano garantire la sostenibilità dell'esperimento Bitcoin: se Bitcoin sarà ancora rilevante nel 2140, è facile prevedere che l'interesse economico di preservarne piena funzionalità sarà enorme.

L'avvento dei computer quantistici permette di ricavare la chiave privata dalla chiave pubblica: minaccia quindi le criptovalute, potendone violare la sicurezza.
L'avvento di reali computer quantistici violerebbe la stessa crittografia che garantisce la sicurezza del sistema finanziario e dell'arsenale nucleare. Non è quindi un problema solo di bitcoin. In realtà si tratta di preoccupazioni esagerate, sia perché siamo ancora molto lontani da computer quantistici (quelli di oggi sono limitatissimi simulatori), sia perché c'è una promettente ricerca nell'ambito di tecniche crittografiche *quantum-resistant*.

Non la inquieta che l'inventore di bitcoin si sia celato dietro lo pseudonimo Satoshi Nakamoto e sia poi scomparso dalla scena?
Nakamoto potrebbe essere una singola persona ma anche un ristretto gruppo. Non sappiamo che fine abbia fatto, ma non è scomparso all'improvviso: ha progressivamente e volutamente abbandonato la scena. Possiamo stimare possegga circa un milione di bitcoin e non li ha mai spesi. Qualcuno vorrebbe candidarlo al Nobel per l'Economia, ma se non rivela la sua identità non è possibile farlo. Chiunque sia, ha mostrato di credere in questa idea rivoluzionaria senza cercare alcun tornaconto. Il suo essere scomparso rafforza bitcoin perché elimina l'autorevolezza di uno scomodo "padre nobile" che potrebbe essere manipolato, ricattato o anche semplicemente avere la tentazione di "governare" l'evoluzione del protocollo: lo sviluppo di bitcoin è meglio sia guidato da criteri meritocratici e considerazioni strettamente tecniche.

Perché le transazioni in Bitcoin non sono più gratuite?
Non lo sono mai state, ma per ora hanno di solito un costo talmente basso da essere trascurabile. Un blocco di transazioni, prodotto ogni circa dieci minuti, ha una capienza limitata: entrano nel blocco le transazioni che pagano le commissioni maggiori, come se fosse un'asta. C'è stato un periodo a fine 2017 in cui il costo è salito moltissimo perché la rete era intasata, fondamentalmente da transazioni fittizie che attaccavano il network. La capacità transazionale di bitcoin non può scalare in modo semplice o arbitrario: è indubbio che, andando avanti, transare sulla rete più sicura al mondo avrà un costo sempre più elevato.

Bitcoin regge poche transazioni al secondo: se, come lei dice, avrà anche costi transazionali crescenti, allora non decollerà mai come metodo di pagamento.
L'oro digitale permette trasferimenti di valore semplici e veloci, con costi transazionali proporzionali alla straordinaria sicurezza ed efficienza offerta. Bitcoin permette circa sei transazioni al secondo, consentendo una operatività giornaliera paragonabile a quella di una grande banca centrale. La blockchain di bitcoin è come se fosse un *real-time gross settlement system*: ha senso che regoli solo transazioni finanziariamente significative. Le limitazioni alla scalabilità che derivano dal contenimento della dimensione del blocco e dal consenso basato su proof-of-work non sono scelte accidentali, ma fondamentali per avere un sistema sicuro e stabile. Peraltro, ogni transazione viene validata due volte da tutti i nodi del network: la prima volta quando la transazione viene resa pubblica e diffusa, la seconda volta quando entra nel blocco di transazioni finalizzate: è evidentemente un livello di sicurezza eccessivo per piccoli importi.

C'è chi non concorda con la visione di oro digitale e vorrebbe bitcoin come mezzo di pagamento.

Per raggiungere capacità transazionali più alte sono in test soluzioni di secondo livello, ad esempio Lightning Network, dove la transazione viene validata solo dalle controparti interessate, che eventualmente ricorrono alla blockchain di bitcoin come garante nel caso uno degli interessati non cooperi; queste soluzioni possono permettere milioni, forse persino miliardi, di transazioni al secondo. È un passo in avanti decisivo per la versatilità e scalabilità di bitcoin e consentirà i micropagamenti, rendendo l'oro digitale ancora più "liquido"; non credo però che per questo bitcoin diventerà un mezzo di pagamento diffuso: il punto qui non è tecnico, ma riguarda l'impossibilità di adeguare l'offerta di bitcoin alla domanda, con la conseguente impossibilità di stabilizzarne il potere di acquisto.

È tutto oro quel che luccica? Ad ascoltare lei sembra che bitcoin non abbia limiti né difetti…

Il difetto principale è la sua mancanza di fungibilità: la trasparenza della blockchain rende bitcoin tracciabile e per questo non tutti i bitcoin sono uguali. Gli atomi d'oro non raccontano nulla della loro storia, sono indistinguibili gli uni dagli altri: se anche un atomo d'oro della vera nuziale di mia moglie fosse stato coinvolto in un crimine sanguinoso 300 anni fa, mia moglie non ne saprebbe nulla e sarebbe tranquilla nel portare la vera al dito. Per questo molti lavorano al miglioramento della confidenzialità transazionale di bitcoin, cioè a ridurre la trasparenza della blockchain. Non si tratta di lavorare per i criminali, ma di rendere sostenibile nel tempo la proposizione di oro digitale. Ci sono nuovi paradigmi crittografici estremamente promettenti, come Mimblewimble, che oggi non sono applicabili direttamente a bitcoin, ma potrebbero essere adattati in futuro.

Possiamo immaginare alternative evolutive a bitcoin che lo soppiantino un domani? Magari un coin Mimblewimble?

È possibile, ma lo reputo improbabile per tre ragioni. La prima è metodologica: la tecnologia ci insegna che le evoluzioni avvengono per stratificazioni successive; ad esempio, il protocollo TCP/IP non è ottimale per lo streaming, applicazione per cui non è stato disegnato, ma nessuno si sogna di sostituirlo: è troppo radicato nella nostra infrastruttura tecnologica. Piuttosto abbiamo migliorato le tecniche di compressione dati ed aumentato la banda di trasmissione per ovviare ai suoi limiti. Similmente, Bitcoin si è affermato come internet del valore e potrebbe essere già tardi per sostituirlo: troppo rischioso, meglio risolvere i suoi limiti con protocolli di secondo livello. La seconda ragione è pragmatica: le competenze professionali e la genialità di intelligenza necessarie per lavorare su questi argomenti sono rarissime; la stragrande maggioranza

dei migliori sviluppatori ha investimenti significativi (intellettuali ed economici) in bitcoin ed è quindi incentivata al suo successo: praticamente impossibile orientarla verso alternative. L'ultima ragione è quasi ontologica: se arrugginisse per obsolescenza il primo tentativo di oro digitale decentralizzato, cosa garantirebbe la sostenibilità di un secondo tentativo?

11. Investire in bitcoin

Perché si dovrebbe investire oggi in bitcoin? È cresciuto talmente tanto che è difficile immaginare possa ancora apprezzarsi, c'è solo il rischio di perdere il capitale investito.
Ovviamente l'esperimento bitcoin è giovane e potrebbe non resistere alla prova del tempo: per questo è importante investire una percentuale limitata del proprio patrimonio. Ed è evidente che se bitcoin ha realizzato rendimenti così esorbitanti, lo ha fatto con rischi altrettanto eccezionali. Ci sono però investitori che hanno appetito per un investimento simile, anche solo in logica di diversificazione del portafoglio. Le criptovalute sono infatti una nuova asset class con correlazione nulla rispetto alle asset class tradizionali.

Quindi un investimento solo per istituzionali e grandi patrimoni?
No, per tutti! Oggi sarebbe irrazionale non investire in bitcoin quella parte di capitale di cui si possa sopportare senza troppi rimpianti l'eventuale perdita. Siamo di fronte a una svolta storica: se davvero bitcoin rappresenta l'oro digitale, allora il suo potenziale è persino sottovalutato e dovrà apprezzarsi decine di volte; se invece dovessero emergere elementi critici che oggi sfuggono alle analisi, allora il suo valore è destinato ad azzerarsi.

Apprezzarsi decine di volte? Non le sembra di esagerare?
Se bitcoin è oro digitale, sottolineando la parola "se" perché ci possono essere ancora legittimi dubbi, allora è ampiamente sottovalutato. Facciamo qualche valutazione grossolana. A livello globale i patrimoni gestiti sono circa 100 trilioni di dollari: quando il 2% investisse in bitcoin, anche solo a scopo di diversificazione, questo implicherebbe un prezzo per bitcoin di 100.000 dollari. La capitalizzazione dell'oro fisico è di 8 trilioni: per raggiungere un livello comparabile bitcoin dovrebbe arrivare a 400.000 dollari. La legge di Metcalfe dice che il valore di un network è proporzionale al quadrato del numero dei suoi utenti: oggi si stimano 50 milioni di investitori bitcoin, se proiettiamo a 350 milioni di investitori la capitalizzazione di bitcoin dovrebbe crescere di 50 volte.

Insomma lei propone un azzardo: fate la vostra puntata al casinò bitcoin e se esce "oro digitale" il capitale si moltiplicherà.
Non si tratta di azzardo, ma di aver compreso il potenziale dirompente di bitcoin. Investire in questo momento è al tempo stesso una operazione di esplorazione tecnologica e culturale, una diversificazione del proprio patrimonio ed una scommessa razionale. D'altronde la nostra conoscenza è sempre imperfetta, anche riguardo le cose di cui siamo relativamente più certi: non mi sembra esistano investimenti sicuri al 100%.

Quindi tutti a fare trading, col miraggio di profitti straordinari?
Non ho mai consigliato il trading: persino su mercati regolati il trading dei piccoli investitori è quasi sempre azzardo; nel mercato bitcoin, dove sono correntemente praticate tutte le possibili manipolazioni, il trading è praticamente la somma di incoscienza ed azzardo. Hanno realizzato profitti rilevanti solo quelli che hanno creduto in bitcoin e non lo hanno liquidato ai primi rialzi. È famoso il caso dei gemelli Winklevoss che avevano conteso a Mark Zuckerberg la proprietà intellettuale di Facebook vincendo una causa da 65 milioni di dollari: 11 milioni li avevano investiti in bitcoin quando quotava $120 ed oggi sono miliardari. Tanti di quelli che hanno investito in bitcoin anni fa, ancora non liquidano le loro posizioni perché percepiscono che bitcoin possa avere ancora ampi margini di apprezzamento.

Lei ha certamente investito in bitcoin: c'è un oggettivo conflitto di interessi tra la sua posizione culturale ed i suoi interessi economici.
Su bitcoin sto rischiando molto di più a livello reputazionale che non economicamente. Anche perché faccio quello che dico ed ho investito una piccola somma: è diventata significativa nel mio portafoglio complessivo, ma non sono cifre rilevanti. Nelle cose in cui credo investo sempre tempo, energie, intelligenza, reputazione e soldi: non è la posizione intellettuale che si adegua agli investimenti, piuttosto il contrario. Anzi, per dirla tutta, la penso come Nassim Taleb[28]: se non c'è la propria "pelle in gioco", se non si è personalmente coinvolti in qualcosa, le opinioni che si esprimono non sono davvero affidabili.

Per investire è necessario aprire un conto presso una borsa di scambio, ma queste borse sono state ripetutamente coinvolte in truffe, fallimenti ed incidenti operativi, oltre a sospetti di collusione col mondo del riciclaggio.
Molte borse sono nate in modo hobbistico: Mt Gox, che all'epoca del famoso fallimento nel 2014 era la prima borsa dollaro/bitcoin, era nata come *Magic The Gathering Online*

[28] Nassim Nicholas Taleb, *Skin in the Game: Hidden Asymmetries in Daily Life* (2018)

eXchange, un sito di scambio per carte da gioco. È un mercato giovane, non ci sono borse con tradizioni decennali, tutte hanno finora gestito una liquidità ed un numero di clienti limitato. A tratti hanno funzionato male anche perché non erano attrezzate per una crescita così esplosiva e quindi faticano talvolta a tenere il passo. Le borse più serie sono giustamente preoccupate per il rischio di acquisire clienti problematici e tentano di essere inappuntabili nei controlli.

L'ecosistema bitcoin punta ad eliminare gli intermediari, eppure borse centralizzate ne intermediano gli scambi: non è paradossale?

Gli intermediari sono indispensabili per gli scambi tra bitcoin e valute tradizionali: per gli scambi tra bitcoin ed altre criptovalute ad esempio non sarebbero tecnicamente necessari. In ogni caso la loro utilità è proprio centralizzare ed aggregare domanda ed offerta per aumentare l'efficienza e la liquidità del mercato, ma non vedo contraddizioni significative. Abbiamo altri esempi di protocolli aperti e decentralizzati, ad esempio la posta elettronica, dove esistono servizi centralizzati e fiduciari come Gmail: a fine anni 90 io avevo il mio SMTP server per la gestione della posta elettronica; oggi uso i server di Gmail e della mia università sapendo che se censurassero i miei messaggi potrei semplicemente ripristinare il mio server di posta indipendente ed autonomo.

Ci sono ampie differenze di quotazione del prezzo bitcoin tra le diverse borse, la formazione del prezzo è quantomeno opaca.

Gli arbitraggi tra borse (cioè acquistare dove il prezzo è basso per rivendere dove è più alto) dovrebbero tenere i prezzi allineati ovunque. Ma non è tecnicamente semplice effettuare questi arbitraggi, specialmente in momenti di alta volatilità, sia per i limiti delle piattaforme di scambio che per i tempi di conferma intrinseci di una transazione bitcoin. Inoltre non tutte le borse di scambio hanno la stessa affidabilità, per cui un bitcoin detenuto presso due borse ha diverse probabilità di poter essere riscosso in sicurezza: anche da questa osservazione possono originare prezzi diversi in momenti turbolenti di mercato. In ogni caso parlare oggi di opacità è fuori tempo massimo: il prezzo rilevato sui mercati di riferimento è considerato talmente liquido e trasparente che da dicembre 2017 è stato ritenuto possibile utilizzarlo per fare il fixing giornaliero dei futures quotati a Chicago.

Quali sono questi mercati di riferimento?

Bitstamp, Coinbase Pro, Gemini, ItBit, Kraken. A questi aggiungerei l'italiana TheRockTrading: nel mondo è la più vecchia borsa bitcoin tutt'ora funzionante; non si sono fatti bucare da hacker, non sono scappati con i soldi dei clienti: credenziali minimali, ma nel *new wild west* di bitcoin sono le migliori che si possano esibire. Ovviamente bisogna assolutamente evitare di custodire i propri bitcoin presso una

borsa, che potrebbe fallire o essere violata, ma bisogna gestirli attraverso un proprio *software wallet*, come ad esempio Electrum, a cui altri non possano accedere: bitcoin nasce per non doversi fidare di intermediari.

Comprare un bitcoin è però, ai corsi attuali, un investimento impegnativo non alla portata di tutti. E con il tetto a 21 milioni i potenziali investitori sono limitati nel numero.
Ogni bitcoin è divisibile in 100 milioni di parti, quindi è possibile acquistare o detenere una frazione di bitcoin. Il limite complessivo a 21 milioni è ciò che garantisce che bitcoin non possa essere arbitrariamente inflazionato perdendo valore.

Chi investe in crittomonete deve pagare le tasse?
La risoluzione dell'Agenzia delle Entrate 72/E del 2016 dichiara che "per [..] persone fisiche che detengono bitcoin al di fuori dell'attività di impresa, si ricorda che le operazioni a pronti (acquisti e vendite) di valuta non generano redditi imponibili mancando la finalità speculativa". Tale parere è però criticato nel merito da molti commercialisti, i quali sottolineano anche che il pronunciamento dell'Agenzia non ha rilevanza normativa. L'Agenzia è quindi recentemente intervenuta con ulteriori precisazioni, ma io non sono esperto di temi fiscali e non ho elementi di chiarimento da aggiungere.

12. Tra divulgazione e università

Quando parla di bitcoin tutti le riconoscono chiarezza, qualcuno le rimprovera un tono propagandistico, altri la criticano per supponenza e scontrosità.
Tanti giornalisti ed opinionisti si stanno occupando di bitcoin: la maggioranza degli interventi è un mix di errori fattuali, illazioni infondate e leggende metropolitane. Bitcoin è un terreno scivoloso e può capitare di scrivere inesattezze… ma non si può insistere su bolle, tulipani e gossip tecnologico blockchain. Capita di potersi entusiasmare per un Carlo Lottieri[29] che scrive sull'argomento in maniera semplice ed intelligente, ma a parte queste rarissime eccezioni bitcoin viene sempre dipinto a tinte fosche, senza alcun approfondimento sulla sua rilevanza in questo momento storico e culturale. Serve un dibattito di respiro più alto: tentare di capire cosa stia succedendo nella storia della moneta e se la privacy sia ancora un diritto umano riconosciuto e tutelato. Dal canto mio, tento di contribuire qualche elemento di chiarezza, avendo

[29] http://www.ilgiornale.it/news/cronache/bitcoin-boom-rivoluzione-denaro-non-virtuale-1473289.html

imparato con fatica personale che bitcoin è complesso e richiede un significativo lavoro di comprensione.

Il suo corso *Bitcoin and Blockchain Technology*[30] è una trovata di marketing delle università con cui collabora?
Un corso simile c'è a Stanford, MIT e Princeton: all'Università di Milano-Bicocca va riconosciuta la lungimiranza ed apertura mentale di aver fatto da pioniere in Italia: le lezioni più divulgative dell'anno accademico 2016/2017 sono disponibili su YouTube[31], a disposizione di chiunque voglia approfondire. Inoltre, il corso è stato proposto per tre anni all'interno dell'insegnamento "Computational Finance" di Ingegneria Matematica al Politecnico di Milano, nel 2019 è entrato nel programma della facoltà di Matematica dell'Università degli Studi di Milano.

Come è visto l'argomento dal punto di vista accademico?
Siamo ancora distanti dal pieno riconoscimento della rilevanza di questi temi e c'è molto da lavorare in termini di multidisciplinarietà. Ma su entrambi gli aspetti ci sono segnali incoraggianti: su tutti indicherei il Crypto Asset Lab[32] di Milano-Bicocca, che si distingue per la qualità e la multidisciplinarietà della sua *faculty* e il livello del suo *advisory board*.

Dei molteplici aspetti di bitcoin cosa la appassiona?
Bitcoin è Hayek che incontra il *cypherpunk*: la scuola austriaca dell'economia ed in generale la cultura libertaria sono storicamente minoritarie, ma la crittografia è un potente strumento di libertà, la fionda tecnologica con cui Davide può sconfiggere Golia. Mi interessano quindi i temi di ingegneria monetaria: quelle monete di seconda generazione che chiamo Hayek Money, anche se i tempi non sono ancora maturi dal punto di vista tecnologico e politico. Mi appassionano infine didattica e divulgazione: sto collaborando con BapuFilm al documentario su bitcoin "The Digital Rush"[33], il trailer è su YouTube.

La corsa all'oro digitale?
Sì, alla fine quello è il cuore della faccenda: è stato scoperto l'oro digitale, un numero crescente di persone ne comprende il luccichio inossidabile e il potenziale come asset di investimento. La corsa all'oro apre sentieri in territori ancora selvaggi. È un ecosistema dove, al fianco di esploratori e guide serie, c'è un pullulare di furfanti ed imbroglioni. Ma

[30] https://www.ametrano.net/bbt/
[31] https://www.youtube.com/playlist?list=PLrVvuryXHYTdzvtpzrj4wvYEhCwF6G82b
[32] https://cryptoassetlab.diseade.unimib.it/
[33] http://www.the-digital-rush.com/

per chi saprà arrivare in fondo, senza farsi frodare e avendo chiaro l'orizzonte, il premio esiste: bitcoin, oro digitale a 24 carati.