Criptoeconomia

Traduzione Italiana di Cryptoeconomics

Eric Voskuil

Traduzione Italiana a cura di *Parsevalbtc* disponibile online:

https://github.com/parsevalbtc/cryptoeconomics-IT-translation

Aggiornata al commit: `30afdfc` - v1.0

Indice

Introduzione alla Traduzione Italiana

I tempi recenti, nella loro straordinarietà, ci offrono l'opportunità, forse addirittura ci impongono, di riflettere attivamente sull'evoluzione sociale, tecnologica ed economica che ci ha condotti fino ad oggi. In questa riflessione non si può non includere Bitcoin, la cui sola definizione ed inquadramento rappresentano già un compito notevole e tutt'altro che semplice. *Un asset digitale scarso spendibile ma non duplicabile? Una riserva di valore? Una moneta? Un fenomeno sociale?* Una combinazione delle precedenti e di numerose altre definizioni apparse nel corso della sua ancora giovane esistenza potrebbe essere sufficiente?

Qualunque persona si avvicini a questo nuovo mondo non necessita solo di un insieme definizioni, talvolta già superate, o di sofisticati modelli predittivi, ma al contrario di un vero e proprio inquadramento economico razionale. L'assiduo lavoro di Eric Voskuil, che ha portato alla stesura di *Cryptoeconomics*, risponde con rigore a questa essenziale necessità. Tra le numerose caratteristiche pressoché uniche di questa raccolta di argomenti di economia, il lettore non potrà non apprezzare l'estrema capacità di razionalizzazione e sintesi dei concetti economici strutturati in capitoli ed espressi in larga parte per "Principi" e "Fallacie". Questo approccio non è limitato al solo inquadramento economico delle proprietà di Bitcoin ma ai più fondamentali principi economici, come la produzione ed il consumo, le proprietà della moneta, la preferenza temporale solo per citarne alcuni, e che necessariamente si intersecano con le proprietà del nuovo bene digitale.

L'opera è pienamente tributaria della grande - ma sfortunatamente ancora troppo poco diffusa - tradizione della Scuola Austriaca di Economia che, partendo da un insieme ristretto di principi primi, applica rigorosamente la logica deduttiva per arrivare a comprendere le conseguenze delle preferenze umane. Tale Scuola Economica è infatti l'unica nel vasto panorama di teorie economiche ad abbracciare senza riserve i principi di libertà e del diritto di proprietà. Con questa premessa viene rigettata ogni forma di supposta "verità" universale di tipo ideologico o politico, supportata dalle più disparate ipotesi aggiuntive; un approccio che sempre, nel corso della storia, è stato foriero dello spreco o del furto di preziose risorse e, troppo spesso, anche delle più nefaste e distruttrici conseguenze per la vita degli individui.

Il mio auspicio, derivato dall'esperienza personale benché differente dall'approccio pressoché opposto dell'autore, è che la lettura di *Cryptoeconomics*, grazie alla sua struttura estremamente flessibile e sintetica, possa essere il punto di partenza per lo studio più approfondito e motivato delle grandi opere della Scuola Austriaca. Mi riferisco in particolare, all'*Azione Umana* di Ludvig Von Mises e a *Man Economy and State* di Murray Rothbard, a più riprese citati nella raccolta, ma che, tuttavia, per monumentalità, complessità e sopratutto tempo richiesto per la loro lettura, scoraggerebbero anche il più motivato lettore senza il forte incentivo di espandere e completare la sua comprensione della conoscenza economica.

Con il corretto inquadramento teorico della Scuola Austriaca, non è possibile non avvertire quanto Bitcoin stesso ed il suo intero sviluppo siano una naturale conseguenza di quegli stessi principi economici: un genuino prodotto della volontà e dell'azione umana sviluppato nel corso di numerosi anni di ricerche e tentativi nei più disparati campi del sapere teorico ed applicativo. Grazie ad un livello di cooperazione senza precedenti che ha portato, e porta tutt'ora, all'incessante scambio di un immenso capitale di conoscenze distribuite, lo sviluppo di Bitcoin sta dando risposta positiva ad una tra le più fondamentali necessità ricercate dall'umanità: un più elevato grado di protezione delle libertà individuali che viene raggiunto attraverso la possibilità di conservare e scambiare valore su base volontaria, per la prima volta in forma digitale. Un genere di libertà che è stato in ogni tempo fortemente limitato e ostacolato.

Ho cercato di procedere con una traduzione il più fedele possibile al testo originale, mantenendo molti termini in lingua inglese poiché ormai entrati nel lessico tecnico e impiegati correntemente anche in italiano; l'utilizzo nel testo del carattere corsivo e i collegamenti al glossario dovrebbero aiutare rispettivamente alla loro individuazione e comprensione. Allo stesso modo anche una parte notevole dei *link* è stata mantenuta in lingua originale perché, o non esistente, o non abbastanza esaustiva in lingua italiana. Spero di riuscire in futuro ad arricchire la raccolta con alcuni commenti e con le correzione ed i suggerimenti che i lettori vorranno segnalare. A questo proposito desidero riportare una definizione contenuta nella raccolta che mi ha particolarmente colpito: la definizione di miner onesto. Benché, come in ogni valutazione del valore, anche l'onestà sia una valutazione soggettiva, credo che questa definizione rappresenti fedelmente lo spirito di tutti coloro che contribuiscono a Bitcoin così come al progresso genuino di molteplici discipline del sapere umano, anche per piccola parte: l'aggiunta del proprio blocco al di sopra dei blocchi costruiti da altri. Quale sarà dunque il prossimo blocco?

Parsevalbtc

Criptoeconomia

Questo progetto è iniziato come un modo per evitare di riscrivere le stesse idee 140 caratteri alla volta. Operando su quel tipo di piattaforma gli argomenti erano stati sviluppati nella maniera più breve ed informale possibile. Non pensavo di scrivere un libro e tuttora non sono nelle condizioni per farlo (n.d.t. non più). La maggior parte degli argomenti (incluso questo) sono stati scritti sul mio telefono a bordo di un aereo, di un treno, o presso un caffé. Molti di questi sono veloci osservazioni che nascono da un'intima conoscenza del codice alla base di Bitcoin o da lungo studio personale ed esperienza in varie discipline.

Nel tempo gli argomenti hanno iniziato a collegarsi reciprocamente; è emersa necessariamente una tassonomia e quello che era stato un processo casuale di osservazione ad hoc è iniziato a diventare un lavoro. Gli argomenti sono stati scritti nella forma più breve possibile e presuppongono una certa conoscenza sia di Bitcoin che dell'economia. Ho cercato di fare uno sforzo genuino per razionalizzare i collegamenti e la terminologia ma la mia attenzione si è concentrata sulla coerenza e sull'espansione della comprensione della materia. Fortunatamente altre persone si sono affiancate per aggiungere le illustrazioni, sistemare l'organizzazione degli argomenti e per la pubblicazione.

Ho impiegato i termini Catallattica e Prasseologia per per descrivere la disciplina sottostante a cui le persone si riferiscono anche con il termine Scuola Austriaca. Ho trovato ognuno di questi termini insoddisfacente; quindi ho iniziato a riferirmi a questa disciplina con il termine "Economia Razionale" (da non confondere con il razionalismo economico) un sistema basato interamente sul ragionamento deduttivo a partire da un insieme di assiomi.

Fu Mises a fondare esplicitamente un sistema economico su base razionale, tuttavia questo approccio non si è diffuso nell'intera Scuola Austriaca (che è antecedente a Mises). Rothbard aggiunge rigore e chiarezza a Mises derivando alcune importanti e nuove conclusioni. Tuttavia Mises (come la maggior parte delle persone) ha commesso degli errori effettivi che purtroppo sono stati portati avanti da Rothbard. Altri errori comunemente amplificati nella Scuola Austriaca sono chiaramente interpretazioni errate di Mises (e di Rothbard).

Ogni volta che Mises commette un errore sta criticando la moneta fiat. In altre parole sembra sacrificare la sua obiettività alla passione. Tuttavia, il suo sistema

razionale, correttamente applicato, mette in luce facilmente tali errori. La moneta di stato è meritoria di critica, e i Bitcoiner raramente perdono l'opportunità per manifestarla. Eppure ciò necessita di una critica *accurata*; ogni cosa al di sotto di tale livello è controproducente. Con una analisi corretta è possibile identificare forze specifiche che governano sia la moneta fiat di monopolio (e.g. il Dollaro) che la moneta fiat di mercato (e.g. il Bitcoin). Un'analisi condotta correttamente può limitare lo spreco di prezioso capitale (n.d.t. di tempo) dietro ad affermazioni irrazionali. Un processo rigorosamente razionale non espone solo gli errori, ma produce anche nuove ed interessanti scoperte e semplificazioni, non solo in Bitcoin, ma nella teoria economica in generale.

Gli argomenti qui presentati formano un grafo sul quale nessun ordinamento completo sembra essere appropriato. L'indice rappresenta un ordine imposto in maniera blanda. Mentre è stato fatto qualche progresso in questo senso, consiglio di leggere gli argomenti per come sono stati scritti, per soddisfare una curiosità.

Testo originale: Cryptoeconomics

Indice

Prefazione di Amir Taaky

La Cripto-anarchia non è una strategia volta ad imporre una qualche egemonia politica o volta a screditare altre possibili attitudini o fini. E' semplicemente un insieme di concetti o idee che possono essere utilizzati tatticamente per realizzare modi alternativi di vivere. La Storia è il risultato della volontà e dell'azione umana, ma ciò ha luogo all'interno di una struttura di convinzioni, credenze e rappresentazione che apportano significato e orientamento per ogni obiettivo. In questo modo, la Cripto-anarchia cerca di dotare l'individuo di potenti strumenti concettuali che gli consentono di costruire le proprie visioni creative.

L'economia riveste un ruolo importante poiché essa è lo studio della meccanica fondamentale delle azioni umane e delle loro conseguenze. L'Economia Razionale analizza l'attività umana accettandone nello stesso tempo le limitazioni imposte dalla conoscenza. A partire da un semplice insieme di assunzioni che includono quelle secondo cui gli uomini agiscono e preferiscono avere le cose prima rispetto ad averle più tardi, i teoremi vengono derivati usando le regole di inferenza. Il risultato è molto potente in quanto esso è necessariamente vero se le assunzioni sono vere. Lo sviluppo di questi teoremi ci permette di dotarci di semplici costrutti che possiamo utilizzare per circoscrivere e analizzare fenomeni più complessi.

Il concetto di Criptovaluta si è sviluppato dalla cripto-anarchia e dall'economia di libero mercato, ma da allora il fenomeno è cresciute ben oltre le sue stesse radici fino a diventate un'entità contemporanea con caratteristiche uniche. Questo ci ha imposto di ritornare sulle nostre stesse idee e assunzioni per comprendere come le varie discipline coinvolte siano collegate tra loro. Questo nuovo campo di studio va sotto il nome di Criptoeconomia.

Criptovalute come il Bitcoin rappresentano un tipo di moneta che, per la prima volta nella storia umana, è contemporaneamente globale, non censurabile e di libero accesso per ciascuno. Ci sono stati notevoli avanzamenti nelle tecnologie di anonimizzazione, non solo per le criptovalute ma anche per altri strumenti finanziari e attività umane. Le Criptovalute sono quindi un fenomeno unico del quale le caratteristiche fondamentali necessitano di studio.

L'importanza dell'economia sta nel fornirci un modo per comprendere le attività degli esseri umani. Questo significa poter fare dei piani su dove applicare le

nostre risorse e la nostra conoscenza tecnica. L'attuale generazione di aziende che operano nel settore *crypto* non comprende la portata strategica di tutto ciò e non sarà pronta a trarre vantaggio dalle nuove tendenze geopolitiche. In questo momento c'è troppa divergenza nella scelta degli obiettivi su cui concentrarsi - l'industria *crypto* non è abbastanza selettiva.

I concetti della teoria dell'evoluzione possono aiutarci a prevedere quali tipi di strategie organizzative risulteranno vincenti nel lungo termine. Ad esempio la Strategia di Selezione r/K afferma che dopo grandi eventi di estinzione i primi organismi che vanno ad occupare le nicchie sono le specie aventi un gran numero di giovani individui che giungono velocemente a maturazione e che hanno a disposizione poche risorse lasciate investite dai genitori per loro (selezione-r). Tuttavia, nel lungo periodo, essi vengono spodestati da organismi che contano un minor numero di individui giovani ma che sono maggiormente specializzati per occupare le nicchie e che richiedono maggiore tempo per arrivare a maturazione (selezione-K). Questi cripto-organismi derivati da selezione-K sono quelli che saranno maggiormente adattati ad avvantaggiarsi delle nuove nicchie economiche che si stanno aprendo.

Un altra ipotesi presa dalla teoria dell'evoluzione è quella della Regina Rossa che spiega come gli organismi siano in una costante battaglia tesa alla loro evoluzione. Ciò significa che dobbiamo costantemente adattarci ed evolvere in un ambiente in continuo cambiamento, con attori in continua evoluzione. Questo avviene attraverso il processo di applicazione della nostra conoscenza al fine di riconoscere schemi e costruire modelli concettuali, modificando tali modelli in maniera retroattiva al fine di migliorarne l'accuratezza o mettere in discussione i paradigmi sottostanti.

L'attuale gruppo di cripto-società perirà abbastanza in fretta. Al suo posto emergerà una nuova generazione di organizzazioni. Queste, in sintonia con le tendenze geopolitiche, avranno un altissimo grado di adattamento e saranno ottimizzate per sopravvivere in uno stato di perenne disequilibrio. Per sostenere queste condizioni questa nuova generazione dovrebbe essere fondata su una sintesi che combini le astuzie della cripto-economia con la stessa cripto-anarchia - che di fatto, nella sua essenza, è una semplice dottrina: il motore del cambiamento storico non è semplicemente innovazione tecnologica, ma concetti, modelli e idee che ci danno il potere sulla realtà materiale.

La mia esperienza con Eric risale al 2013 quanto cominciammo a lavorare su un sistema software Bitcoin che fosse al contempo veloce e scalabile. Eric è uno sviluppatore di alto livello che da solo può svolgere il lavoro di un intero team per la creazione di software a livello produzione - un'abilità estremamente rara. Oltre a ciò, egli vanta un ampio spettro di esperienze di vita avendo volato con gli aerei della Marina degli Stati Uniti e fondato numerose società di successo. Egli combina una forte conoscenza pratica con un altrettanto forte supporto teorico corroborati da un profondo interesse e conoscenza di teoria politica ed economica.

Le singolari intuizioni di Eric sui concetti fondamentali ci forniscono un quadro essenziale per guidare la futura direzione del campo della criptoeconomia. Egli applica rigorosamente la teoria economica razionale alle criptovalute e si avventura al di là del livello finanziario per spiegare come l'attività umana plasmi realmente il futuro a venire.

Titolo originale: Foreword by Amir Taaki

Indice

La *Value Proposition*

Il valore di Bitcoin rispetto alle sue alternative deriva direttamente dal rimuovere il controllo dello stato sia sull'offerta monetaria che sulla censura delle transazioni. I vantaggi includono la libertà dal signoraggio, dal controllo sui cambi e dalla sorveglianza finanziaria. Questi ultimi permettono al denaro di essere trasferito ad ogni persona, in ogni luogo e con qualsiasi tempistica senza la necessità di ottenere il permesso di una terza parte.

Questi vantaggi rappresentano una riduzione di costo ottenuta evitando la tassazione. Il signoraggio è una forma diretta di tassa mentre il controllo sui cambi porta a limitare la sua evasione. Lo stato medesimo, spesso, sostiene la sua indipendenza politica come un obiettivo volto a limitare questo potere di tassazione. La sorveglianza finanziaria limita l'evasione delle tasse in maniera generale. **Nonostante Bitcoin non possa eliminare la tassazione, esso porta a ridurre il suo gettito e rappresenta un cambio nella natura della tassazione.** Ad ogni modo, per coloro che considerano lo stato un bene sociale, l'opzione di finanziarlo volontariamente rimane sempre aperta.

Sarebbe un errore assumere che questi vantaggi derivino dall'esistenza di una tecnologia più efficiente di quella impiegata dalle monete di monopolio. La tecnologia è in realtà molto meno efficiente, tuttavia aiuta la persone a resistere ai controlli dello stato. E' questa caratteristica resistenza ad attribuirgli valore.

Titolo orginale: Value Proposition

Indice

Assioma di Resistenza

Nella logica moderna un assioma è una premessa, non può essere provata. E' una assunzione di partenza attraverso la quale possono essere dimostrate altre proposizioni. Per esempio nella geometria Euclidea non è possibile dimostrare che due linee parallele non si incontrino mai. Questa premessa definisce semplicemente il particolare tipo di geometria.

Provare delle affermazioni su Bitcoin richiede di affidarsi ad un sistema assiomatico specificamente basato su matematica, probabilità, e catallattica; e quindi sulle assunzioni su cui si basano queste discipline. Tuttavia Bitcoin si basa anche su un assioma che non è presente in questi sistemi. Satoshi vi allude in una delle sue prime dichiarazioni:

> Non è possibile trovare una soluzione ai problemi politici nella crittografia.
>
> Ma possiamo vincere una grande battaglia nella corsa agli armamenti e guadagnare una nuova frontiera di libertà per diversi anni.
>
> I governi sono bravi a tagliare le teste delle reti controllate centralmente come Napster, ma le reti puramente P2P come Gnutella e Tor sembrano sopravvivere.

In altre parole, viene fatta l'assunzione che un sistema *possa* resistere al controllo dello stato. Ciò non viene accettato come un fatto compiuto, ma si ritiene che possa essere una assunzione ragionevole basata sul comportamento di sistemi simili.

Chi non accetta l'assioma di resistenza sta prendendo in considerazione un sistema completamente diverso da Bitcoin. Se si assume che un sistema *non possa* resistere al controllo dello stato, le conclusioni non hanno alcun senso nel contesto di Bitcoin - così come le conclusioni della geometria sferica contraddicono quella Euclidea. Come potrebbe funzionare in Bitcoin l'assenza di permesso e la resistenza alla censura senza l'assioma? La contraddizione porta a commettere evidenti errori nel tentativo di dare una spiegazione razionale.

Tra le persone è prassi comune riferirsi cinicamente ad un sistema simile a Bitcoin, che però escluda l'assioma di resistenza, come ad un altro "PayPal"; una

denominazione, invero, non priva di merito. Confinity, originariamente, aveva tentato di creare un sistema con una *value proposition* simile a quella di Bitcoin. Avendo fallito nel tentativo, ha rigettato l'assioma facendo nascere la PayPal che conosciamo oggi.

Titolo originale: Axiom of Resistance

Indice

Tassonomia della Moneta

La moneta fiat non ha valore d'uso. Ha però utilità come moneta solo nella misura in cui le persone sono disposte ad effettuare degli scambi con essa. Spesso tra questi soggetti si trova anche uno stato emittente, sebbene questa non ne sia una caratteristica distintiva. Il nome deriva dal fatto che "ne è dichiarata l'esistenza" come moneta (n.d.t. l'espressione deriva dal latino, ad esempio nella celebre frase biblica "Fiat lux et lux fuit" - "Sia fatta luce, e luce fu") . Tuttavia, anche questa definizione non ne è una caratteristica distintiva. La moneta fiat è semplicemente una moneta che non possiede valore d'uso. Ci si riferisce ad una moneta con valore d'uso con il termine moneta merce (n.d.t. anche moneta commodity).

Essendo il valore soggettivo, cosa che rende impossibile definire il valore d'uso nella pratica, la classificazione è di per sé stessa chiara. Ad esempio, le cartamoneta può essere bruciata per riscaldarsi, ma ciò non è tipicamente considerato un suo valore d'uso reale. Bitcoin può essere utilizzato per il timestamping, ma anche questo non è tipicamente considerato un valore d'uso principale. Si ritiene, al contrario, che oro, argento, rame e altri materiali di conio abbiano un valore d'uso reale. Quando il valore nominale di una moneta merce diventa minore del suo valore come merce, si ha una transizione ad una pura commodity ed essa viene quindi fusa o accumulata.

Un sostituto monetario è una obbligazione contrattuale relativa ad una determinata somma di denaro, rimborsabile a richiesta. Come tale, un sostituto monetario rappresenta un "bene futuro", mentre la moneta rappresenta un "bene presente". La moneta fiat non è un sostituto monetario perché non è riscattabile per nessuna somma definita di denaro, è essa stessa denaro. Il debito è spesso cartolarizzato e garantito dal prestatore come un sostituto monetario, noto come banconota. Essendo il valore soggettivo, non è possibile, allo stesso modo, distinguere se una persona dia valore al rimborso o all'obbligazione del rimborso stesso; ma si assume, in generale, che ad avere valore sia il rimborso vero e proprio e non il documento sul quale tale rimborso è scritturato. Quando un sostituto monetario viene abrogato, ma viene ancora utilizzato negli scambi significa che è passato ad una condizione di moneta fiat.

La moneta rappresentativa viene spesso confusa come un bene presente, tuttavia poiché essa è in realtà una obbligazione (a ciò che essa stessa rappresenta), si tratta di un sostituto monetario. Il Dollaro Statunitense basato sull'oro era un sostituto monetario mentre il Dollaro Statunitense moderno è una moneta fiat. I dollari in giacenza sul conto corrente sono sostituti monetari elettronici, così come lo sono tutti i Bitcoin custoditi da terze parti e quelli scambiati mediante transazioni non confermate. Tutte queste sono promesse di rimborso rispettivamente in dollari o in bitcoin.

I dollari che possono essere tenuti in mano sono vera moneta fiat, così come lo sono i bitcoin che possono essere spesi con la propria chiave privata. Come tale il termine "fiat" non fornisce una distinzione tra Dollaro e Bitcoin. Tuttavia va ricordato che questa distinzione non si è mai resa necessaria prima dell'avvento di Bitcoin. Monete di mercato senza valore d'uso non erano ritenute possibili. Tuttavia vi è, in realtà, una reale distinzione tra questi due tipi di moneta, di cui nessuna delle due possiede valore d'uso. Questo richiede l'impiego di un nuova caratteristica distintiva.

Il Dollaro (come tutte le monete fiat di stato) differisce da Bitcoin a causa della protezione di monopolio esercitata sulla sua produzione. E' il divieto di competere sul mercato che permette allo stato di limitare l'offerta monetaria e quindi di estrarre una rendita di signoraggio.

> Il monopolio è una garanzia di uno speciale privilegio affidato dallo stato che riserva una certa area della produzione ad un particolare individuo o gruppo.

Il monopolio sulla produzione di moneta fiat di stato è creato sotto forma di statuto di anticontraffazione. Una unità di una moneta è considerata invalida a meno che non venga prodotta da un agente autorizzato dello stato. Ciò è differente da quanto avviene in Bitcoin in quanto esso è prodotto dalla competizione di mercato e la contraffazione è preclusa attraverso un accordo basato su registro pubblico. **Con il termine "moneta di monopolio" ci si può ragionevolmente riferire ad una moneta che si difende dalla contraffazione sulla base di uno statuto** (da non confondere con la moneta del Monopoly), e riferirsi a Bitcoin come ad una "moneta di mercato". Quando il valore nominale di una moneta fiat è ridotto fino al suo costo di produzione, essa è passa allo stato di moneta di mercato.

La moneta merce è anch'essa una una moneta di mercato, in quanto essa non dipende da un privilegio di monopolio che restringe la sua offerta. Se l'offerta di una moneta merce è troppo grande, essa smette di essere utile come moneta per mancanza di portabilità. La distinzione tra moneta merce e Bitcoin deriva dai Principi della Criptodinamica. L'offerta di una moneta merce è controllata dalla competizione di mercato che esiste per fornirla come conseguenza della sua domanda di mercato. Non è classificabile come moneta fiat in forza dell'esistenza di un suo presunto valore d'uso.

Sia le monete che i sostituti monetari costituiscono una valuta. Ci si riferisce talvolta alla moneta come ad una base monetaria. Tutte le monete sono soggette ad essere date in prestito e sono quindi sono soggette all'espansione del credito (i.e. in forma di sostituti monetari) che porta ad una corrispondente riserva frazionaria.

Riepilogo

- Valuta
  - Moneta [presente]
    - Merce (Commodity) [valore d'uso]
      - di monopolio
        - Moneta di Dollaro Statunitense
      - di mercato
        - Lingotto
    - Fiat [nessun valore d'uso]
      - di monopolio
        - Banconota di Dollaro Statunitense
    - di mercato
      - Bitcoin
  - Sostituto Monetario [futuro]
    - elettronico [intangibile]
    - rappresentativo [tangibile]
      - Banconota
        - *Silver Certificate* Statunitense

Titolo originale: Money Taxonomy

Indice

Modello di Banca Pura

Il concetto di una banca pura può essere utile nel dimostrare il comportamento generale dell'imprestare il denaro.

Una banca pura fornisce solamente i seguenti servizi:

- prende a prestito denaro (ha un debito con i creditori)
- dà in prestito denaro (vanta un credito nei confronti dei debitori)
- accumula denaro (detiene una riserva)

Le differenze essenziali con una banca reale sono:

- la mancanza di intervento dello stato (regime di *free banking*)
- nessun costo operativo (efficienza perfetta)

La banca è di proprietà dei suoi creditori in proporzione al credito posseduto da ciascuno di essi, cosa che avviene in ogni società. Esistono banche di primaria importanza che sono possedute dai loro correntisti, ad esempio USAA e Vanguard, cosa che non rappresenta una distinzione rispetto ad una banca reale. Né una banca pura né una banca reale possiedono "capitale proprio" da imprestare, in quanto tutto il capitale è preso a prestito dagli investitori in una forma o in un'altra. L'obiettivo dei creditori è quello di massimizzare il loro ritorno sull'investimento. L'obiettivo dei debitori è quello di minimizzare le spese dovute all'interesse.

I conti dei creditori sono dei sostituti monetari. Questo aspetto distingue la banca da un fondo di investimento. I sostituti monetari possono essere sia dei depositi a vista che dei fondi monetari. La distinzione tra i due dipende dal modo con cui vengono trattate le riserve insufficienti (tasso di rendimento negativo), nel primo caso sulla base dell'ordine di arrivo (*first come, first served*), mentre nel secondo attraverso la "rottura della parità con il dollaro" (*breaking the buck*).

La mancanza dell'intervento di stato è assimilata al noto concetto di *free banking*, dove non vi è controllo statuario, assicurazione di stato, finestre di sconto dei tassi, o signoraggio. La banca utilizza una moneta commodity se non specificato diversamente, cosa che semplifica i calcoli eliminando il bisogno di compensare l'inflazione o la deflazione dei prezzi.

Rispetto ad una banca reale, l'ipotesi di efficienza perfetta differisce solo nel tasso di ritorno, in quanto non viene consumato nulla in spese operative. Tutti i ricavi sono conseguenza della preferenza temporale. Viene assunto un tasso di interesse uniforme, in quanto l'arbitraggio tra tassi è una spesa. Il *demurrage* è definito come la spesa dovuta al deposito del denaro. Il rapporto di spesa (inclusivo del *demurrage*) è pari a 1 per la banca pura.

Il capitale riservato è il denaro con cui crediti e debiti vengono finalizzati (con tempo 0 di maturità) (i.e. il processo di *settlement*). La svalutazione rappresenta il costo opportunità dello stesso capitale a non essere investito, anche noto come "*cash drag*". Si assume che le relazioni di interesse valgano per un singolo periodo di interesse composto, avente tasso fissato per quel periodo. Queste semplificazioni, per come sono state presentate, non hanno rilevanze per le relazioni implicate.

Date le precedente definizione di banca pura, le seguenti relazioni valgono in maniera assoluta.

```
[capitale] riservato     = preso-in-prestito - investito
demurrage                = tasso-di-demurrage * riservato
svalutazione             = tasso-di-interesse * riservato
interesse                = tasso-di-interesse * investito
ritorno                  = rapporto-di-spesa * interesse
```

Per la banca pura, il rapporto di riserva determina interamente il rapporto di capitale, il rapporto di debito, il rapporto di risparmio, lo stato patrimoniale e il tasso di rendimento.

Rapporto di Riserva

```
rapporto-di-riserva = riservato / preso-in-prestito
                    = (preso-in-prestito - investito) /  preso-in-prestito
```

Rapporto di Capitale

```
rapporto-di-capitale = riservato / investito
                     = (preso-in-prestito - investito) /  investito
```

Rapporto di Debito

```
rapporto-di-debito = preso-in-prestito / riservato
                   = preso-in-prestito / (preso-in-prestito - investito)
                       = 1 / rapporto-di-riserva
```

Rapporto di Risparmio

```
rapporto-di-risparmio = investito / riservato
                      =  investito / (preso-in-prestito - investito)
```

Stato Patrimoniale

La banca pura non ha fonti di indebitamento (passività) ma solamente capitale sociale apportato dagli azionisti.

Asset della banca - Attività	Capitale Sociale - Passività
investito + riservato	preso-in-prestito

Tasso di Rendimento

Il tasso di rendimento del creditore è, in aggiunta, una funzione del tasso di interesse. Il tasso di rendimento del creditore è inferiore al tasso di interesse del debitore a causa del *cash drag*, la spesa necessaria per sostenere la domanda di prelievo. Per ridurre queste spese sono tipicamente inclusi dei vincoli temporali nei contratti delle banche reali. Ad esempio, per legge ogni prelievo da un conto corrente con interesse degli Stati Uniti può essere ritardato di 7 giorni. Il creditore può eliminare il *cash drag* tenendo il debito in un fondo di investimento (i.e. senza assicurazioni sul *settlement*) rispetto a tenerlo in una banca.

```
tasso-di-rendimento = tasso-di-interesse * (investito / preso-in-prestito)
```

Come mostrato ne la Relazione del Risparmio il rapporto di capitale è il tasso di interesse (n.d.t. la relazione è stata modificata e non ha un tale livello di generalità: questo paragrafo ha subito concordemente delle modifiche - si veda il commento nel capitolo relativo. Ai fini della presente versione l'applicazione della relazione segue la specifica assunzione che il capitale accumulato si deprezzi interamente e venga interamente sostituito dall'interesse ottenuto dall'investimento). Il rapporto di capitale include il deprezzamento dei beni presenti, che nel caso della moneta è il *demurrage*. Il *demurrage* della banca pura è 1, e quindi questo termine scompare dall'espressione. Sostituendo il rapporto di capitale nella formula si ottiene il tasso di rendimento espresso nei termini del capitale preso a prestito ed investito.

```
tasso-di-rendimento = (riservato * demurrage / investito) * (investito / preso-in-prestito)
            = (riservato / preso-in-prestito) * demurrage
            = riservato / presto-in-prestito
```

Il tasso di rendimento di una banca pura è il rapporto di riserva.

Le Banche Reali

I rapporti di capitale stabiliti indipendentemente dalle persone, basati sulla preferenza temporale, determinano il tasso di interesse di mercato. La sostituzione apportata qui sopra per il rapporto di capitale proprio della banca come tasso di interesse, implica che la banca stia fissando il tasso di interesse. Tuttavia, questo è connaturato al concetto di preferenza temporale. Una banca può fissare il tasso di interesse che preferisce. Non vi è assunzione che il mercato possa

imporre un tasso alle banche reali, di conseguenza vengono assunti l'interesse e quindi il rendimento di mercato.

```
tasso-di-rendimento-di-mercato = tasso-di-interesse-di-mercato * (investito / preso-in-prest
                               = rapporto-di-capitale-di-mercato * (investito / preso-in-pre
```

La banca in regime di *free banking* differisce dalla banca pura anche per quanto riguarda le spese operative che riducono direttamente il tasso di rendimento.

```
tasso-di-rendimento-free-banking = tasso-di-rendimento-di-mercato * rapporto-di-spesa
```

A sua volta, la banca reale differisce dalla banca in regime di *free banking* per quanto riguarda la tassazione (inclusiva delle spese regolatorie) che riduce direttamente il tasso di rendimento.

```
tasso-di-rendimento-reale = tasso-di-rendimento-free-banking * rapporto-di-tassazione
```

A sua volta, la banca centrale (di stato) differisce dalla banca reale per quanto riguarda il sussidio fornito dai contribuenti (inclusivo dello sconto applicato ai prestiti ricevuti), cosa che incrementa il tasso di rendimento.

```
tasso-di-rendimento-banca-centrale = tasso-di-rendimento-reale * rapporto-di-sussidio-reddit
```

Ove la tassa includa il signoraggio sulla moneta impiegata dalla banca è necessario utilizzare l'Equazione di Fisher sulle relazioni precedenti per tradurre il tasso di interesse da una tasso nominale ad un tasso reale. Non vi è implicato nessun altro cambiamento oltre alla tassa che è già inclusa nell'esempio della banca reale riportato sopra. Questa tassa è in generale la fonte del sussidio, che è già incluso nell'esempio della banca centrale riportato sopra.

Ogni persona, o società di persone, è una banca reale e lo stato è una banca centrale. Una banca reale garantisce il servizio di fornire liquidità agli investimenti, un bene economico. Il costo di produzione è la svalutazione delle sue riserve. Questo rappresenta il modello di tutta la produzione.

Titolo orginale: Pure Bank

Indice

Produzione e Consumo

Produzione e Consumo sono le due azioni umane complementari volte a produrre e a consumare beni economici. I *ruoli* di produttore e di consumatore che riguardano gli esseri umani non dovrebbero essere confusi con le azioni relative alla produzione e al consumo. Un ruolo si riferisce all'*intento* non all'*azione* sé. Tutti i produttori consumano e tutti i consumatori producono. Il consumo che produce un bene economico è produzione, altrimenti si ha alternativamente un processo di tempo libero o spreco.

La banca pura fornisce il modello per ogni tipo di produzione. Un produttore puro prende a prestito del capitale e lo consumo nella creazione di un prodotto. La frazione consumata in ogni istante è stata *investita* (data in prestito) nella produzione. La frazione non consumata in ogni istante è stata *riservata* sotto forma di liquidità disponibile. Il nuovo prodotto viene venduto, dando luogo ad un *interesse* sulla frazione consumata, e *restituita* sotto forma di dividendo. Poiché la produzione richiede tempo ed è stata assunta la perfetta efficienza, il tasso di riserva scende dal 100% al 0% nel tempo. Il quantitativo messo a riserva rappresenta la stessa necessaria spesa produttiva analoga alla riserva di liquidità della banca pura. **La riserva può venire reintegrata solamente da maggiore capitale preso a prestito, ad esempio quando il dividendo viene reinvestito.**

Un produttore reale converte tempo e capitale in interesse al prezzo di mercato del prodotto realizzato, così come una banca reale ottiene l'interesse al prezzo di mercato. La banca sta semplicemente ottenendo l'interesse di un altro produttore costituendosi come suo investitore. Questo mostra la fondamentale equivalenza dell'investimento sotto forma di debito e di capitale sociale (equity), indipendentemente da distinzioni di tipo statuario (la tassazione).

Un consumatore puro accumula capitale senza *investirlo* nella produzione. Tutto il capitale è *preso in prestito* e *riservato*. Con una riserva del 100% non vi è né *interesse* né rendimento e alla fine si giunge a completa svalutazione. In questo caso il capitale preso a prestito viene considerato un regalo (beneficienza). In aggiunta, un consumatore reale è soggetto alla tassazione e al sussidio che incrementano e diminuiscono rispettivamente il tasso di deprezzamento di quanto accumulato.

Titolo originale: Production and Consumption

Indice

Lavoro e Tempo Libero

Lavoro e tempo libero sono azioni umane complementari che si riferiscono alla produzione e al consumo di beni economici. Il lavoro è il processo di consumo che porta a produrre un bene economico (produzione). Il tempo libero è il processo di consumo che non produce un bene economico. Il consumo senza utilità rappresenta il processo di spreco.

> Il lavoro coinvolge la rinuncia al tempo libero, un bene desiderabile.
>
> Rothbard: Man, Economy and State

Questo sottile errore implica che sia il lavoro che il tempo libero sono beni economici. Tuttavia, solo le azioni creano o consumano i beni](ch012-expression-principle.md). Il lavoro (produzione di beni economici) e il tempo libero (produzione di beni non economici) sono azioni umane che creano e consumano beni nel tempo. Nel più puro senso del termine, la produzione implica il consumo del corpo della persona che agisce, mentre il consumo ne implica la sua produzione.

> In ogni ora egli concentrerà il suo sforzo verso la produzione del bene il cui prodotto marginale è il più alto nella sua scala di valori. Se deve rinunciare ad un'ora di lavoro, egli rinuncerà ad un'unità di quel bene la cui utilità marginale è la più bassa nella sua scala di valori. In ciascun istante egli confronterà l'utilità del prodotto nella sua scala di valori con la disutilità di lavoro ulteriore. Sappiamo che per una persona l'utilità marginale dei beni prodotti dallo sforzo diminuirà all'aumentare dello sforzo speso per essi. D'altro canto, per ogni nuovo sforzo compiuto, la disutilità marginale dello sforzo continua ad aumentare. Pertanto, una persona continuerà a compiere lavoro fino a quando l'utilità marginale relativa al rendimento eccede la disutilità marginale dello sforzo dovuto al lavoro. Una persona smetterà di lavorare quando la disutilità marginale del lavoro sarà più grande dell'utilità marginale dei beni aggiuntivi prodotti dal lavoro stesso.
>
> Successivamente, quando lo sfruttamento del tempo libero aumenta, l'utilità marginale del tempo libero diminuirà, mentre l'utilità marginale dei beni a cui si è rinunciato aumenta, fino al punto in cui

> l'utilità marginale del prodotto a cui si è rinunciato diventa maggiore dell'utilità marginale del tempo libero, e l'attore tornerà di nuovo a lavorare.
>
> Questa analisi delle leggi relative al lavoro sono state dedotte dalle implicazioni dell'assioma dell'azione e dell'assunzione relativa al tempo libero come un bene economico.

Non risulta né corretto né necessario assumere che il tempo libero sia un bene (economico), e facendo questo arrivare all'implicazione che il lavoro sia un "non-bene". Allo stesso modo non è necessario costruire l'artificio dell'utilità negativa ("disutilità"). Il valore è semplicemente una preferenza di una maggiore utilità rispetto ad una più bassa. Sia il lavoro che il tempo libero producono beni di utilità (positiva).

E' la preferenza temporale ad implicare che l'utilità del tempo libero sia maggiore dell'utilità del lavoro. Considerando in maniera appropriata il corpo di una persona come una proprietà, "la preferenza del tempo libero" segue direttamente dalla preferenza temporale. Come implica la citazione riportata sopra, questo è il risultato di uno scambio del tempo passato senza il proprio corpo (tempo speso nel lavoro), al fine di ottenere l'interesse atto a compensare il valore che un individuo attribuisce al tempo speso con il proprio corpo (tempo libero).

Tempo, spazio e beni economici sono *fattori* di ogni produzione, mentre il lavoro è il *processo* della produzione. **Lavoro/tempo libero e produzione sono nomi distinti che indicano la medesima azione umana.** L'atto di produrre è lavoro o tempo libero; l'atto di lavorare o usufruire del tempo libero è produzione. La banca pura fornisce il modello di ogni produzione. Questo ciclo risulta evidente nel caso del lavoro autonomo che è proprio l'esempio della produzione. Nel caso delle persone stipendiate ci sono due produttori, l'impiegato ed il datore di lavoro.

Un puro impiegato stipendiato ottiene capitale *preso a prestito* e così lo scambia per cibo, educazione e attrezzatura richiesta per un lavoro. Una parte del suo capitale è *riservata* e il rimanente è *dato in prestito* al datore di lavoro. Il datore di lavoro paga all'impiegato un interesse (lo stipendio) per la durata di questo "prestito". L'impiegato riscatta il suo "principale" deprezzato e lo stipendio alla fine del lavoro.

Il livello salariale compensa sia la preferenza temporale per il quantitativo (di tempo) dato in prestito (il tasso di interesse nominale) sia la svalutazione del "principale" per tutta la durata del prestito. Il quantitativo di principale e l'interesse, diminuiti della svalutazione della frazione riservata, è *restituita* al creditore del datore di lavoro. Nel caso in cui l'investimento di capitale sia preso a prestito dal suo stesso capitale accumulato, l'impiegato è creditore di sé stesso. Il ritorno può essere accumulato o reinvestito in lavoro futuro (o in altra forma).

Un datore di lavoro ed un impiegato reali ottengono ciascuno un tasso di interesse di mercato. Il tasso di interesse dell'impiegato è il suo livello salariale. Il tasso

di interesse del datore di lavoro è il prezzo ottenuto per il lavoro prodotto per la durata della produzione. La spesa di produzione del datore di lavoro rappresenta il consumo del suo capitale preso a prestito, riservato fino a quel momento, allo stesso modo del suo impiegato. La quantità per la quale l'interesse eccede la svalutazione è l'incremento di ricchezza di entrambe le parti.

Il tasso di interesse ottenuto da ambo le parti è lo stesso. La differenza nei ritorni (dell'investimento) dipende strettamente dal capitale investito, sia nella produzione individuale (per l'impiegato), che nella gestione collettiva della produzione (per il datore di lavoro). La massima valutazione del tempo libero di una persona può essere inferita dallo stipendio che accetta, scontando opportunamente il principale al tasso di interesse di mercato.

```
stipendio = tasso-tempo-libero * (1 + tasso-di-interesse + tasso-svalutazione-corpo)
```

L'impiegato scambia il tempo libero per tempo speso nel lavoro nella misura in cui egli valuta la quantità di interesse più del valore che attribuisce al tempo libero. La preferenza per il tempo libero è una riformulazione della preferenza temporale, dove il corpo di ciascuno è il bene economico che viene dato in prestito alla produzione in cambio di un interesse.

La ricchezza in denaro è generalmente più bassa in giovane età e implica una preferenza temporale più alta per la moneta. Con il passare del tempo la ricchezza viene accumulata e la preferenza temporale si abbassa. Ma è anche vero l'opposto per la preferenza per il tempo libero. Il denaro ed il proprio corpo non sono lo stesso bene e non sono in generale scambiabili. In giovane età un individuo ha la più bassa preferenza temporale per il tempo libero. Poiché il corpo di una persona si svaluta con l'età, il suo equivalente si riduce nonostante la ricchezza in denaro, incrementando la preferenza per il tempo libero. Questo può portare a richiedere un tasso di interesse più elevato di quello del mercato, che porta infine ad optare il pensionamento. La preferenza temporale per il denaro e per il tempo libero si influenzano vicendevolmente in quanto tendono a muoversi in direzioni opposte. Nella misura in cui l'obiettivo del lavoro è quello di incrementare la ricchezza, meno ricchezza abbassa la preferenza temporale del tempo libero mentre più ricchezza la aumenta. Questa circostanza, allo stesso modo, può portare ad optare per il pensionamento.

Titolo originale: Labor and Leisure

Indice

Principio del Rischio di Custodia

Quando un contratto rappresenta un asset, il contratto è un reclamo effettuato sull'asset detenuto dal custode. Questo reclamo è spesso chiamato un titolo (*security*), cosa che implica, in maniera sottintesa, che il reclamo è "garantito" rispetto al possibile diniego, da parte del custode, di scambiare l'asset secondo i termini del contratto. Il valore monetario della *security* è quello dell'asset sottostante al netto dei costi di transazione e di esecuzione del reclamo.

Il rischio di custodia è un aspetto centrale di ogni moneta. L'utilità di una moneta è limitata dall'affidabilità del suo custode. Poiché un custode è un essere umano, la sua affidabilità non può essere garantita. Nel caso di una moneta di stato, l'unico custode è lo stato medesimo. Come mostrato ne il Principio di Riserva la moneta di stato esiste con lo scopo di accumulare una riserva. Questo fornisce un beneficio allo stato solamente perché il suo ruolo di custode può essere abrogato, sia attraverso la liquidazione delle riserva, sia attraverso l'emissione di titoli fraudolenti. In altre parole il default del custode è la ragione dell'esistenza della moneta di stato.

Il valore monetario di un'unità di Bitcoin è strettamente una funzione di ciò che può essere acquistato nello scambio. Se nessun commerciante lo accetta, una sua unità non è utile in alcun modo al suo proprietario. Bitcoin non necessita di custodi (è un asset *non-custodial*) ma, nell'ottica di stabilire un principio generale, è possibile considerare l'insieme di tutti i commercianti come il custode collettivo di Bitcoin. Per come è posto, il rischio di custodia è distribuito attraverso tutta l'economia.

Nel caso di Bitcoin, i commercianti offrono la loro proprietà in cambio di moneta. Come tale, non è implicata nessuna trasformazione della proprietà in un titolo. Un commerciante può smettere di accettare qualsiasi moneta, cosa che porta a ridurre l'utilità della moneta stessa. Questo può essere considerato come un rischio di custodia, ma non come un fallimento in quanto il commerciante non ha accettato alcun obbligo a priori di commerciare in cambio di quella moneta. Come mostrato ne il Principio di Frammentazione, il cambiamento dell'accettazione da parte dei commercianti è la natura di una separazione.

Come mostrato ne la Fallacia della Prova di Proprietà, la "tecnologia blockchain" non può offrire alcuna protezione contro il default del custode. Un asset "tokenizzato" è una *security*. L'opportunità, da parte del custode, di perpetrare una frode o un furto, sia in maniera diretta che sotto la costrizione dello stato, non viene ridotta. **Così come per le monete *commodity* come l'oro, la riduzione del rischio di custodia offerta da Bitcoin non deriva della tecnologia o da una obbligazione contrattuale, ma dalle dimensione della sua economia.** Ironicamente sono le "*security*" ad essere insicure.

Titolo originale: Custodial Risk Principle

Indice

Principio del Costo Dedicato

I costi non necessari che vengono sostenuti dai miner non contribuiscono in alcun modo, né alla resistenza alla doppia spesa, né alla resistenza alla censura. Questi costi costituiscono un vero spreco poiché rappresentano niente più che una misura dell'inefficienza del miner. Ad esempio, se un miner con macchine mal configurate spende una grande quantità di energia senza essere in grado di vincere la ricompensa a causa della cattiva configurazione, ciò non dà alcun contributo alla sicurezza. Ogni costo che non è strettamente richiesto per la generazione ottimale di hash power non è un costo necessario. La cattiva configurazione di un miner non rappresenta un costo per un altro miner.

E' stata formulata una teoria secondo la quale la proof-of-work (PoW) può essere resa più efficiente energeticamente introducendo costi non dedicati alla funzione del mining. Un esempio di questa teoria è l'impiego di capacità computazionale per la scoperta di numeri primi. La ragione per incorporare questi costi deriva dal fatto che i risultati da essi prodotti hanno un presunto valore di mercato. In caso contrario, non ci sarebbe alcun valore nell'aggiungere una ulteriore funzione.

Ogni costo dedicato alla produzione di un valore vendibile indipendentemente può essere compensato attraverso la vendita di quel sottoprodotto. Facendo un'analogia, i produttori di birra possono vendere i sottoprodotti di scarto dei cereali agli agricoltori. Questo migliora la loro efficienza eliminando un costo non necessario. In questo modo, nella misura in cui il sottoprodotto ha valore, la sua produzione non incorre in un costo netto. Ciò nonostante i costi netti necessari devono salire al livello della ricompensa a causa della competizione. Quindi lo stesso risultato sarebbe raggiunto da una semplice PoW che consumi l'intero valore della ricompensa in aggiunta a dei processi energivori indipendenti che generino gli altri prodotti commercializzabili. Per questa ragione la teoria è invalida.

Il *Merged Mining* viene solitamente implementato per risolvere il problema di "bootstrappare" (n.d.t. avviare) una nuova moneta superando le fasi vulnerabili di basso hash rate. Questo tipo di progettazione non riconosce che l'hash rate che non viene dedicato alla nuova moneta non contribuisce alla sua sicurezza.

Poiché l'intero costo dell'hash rate può essere recuperato vendendolo su una catena, non vi è alcun costo nel censurare le altre catene validate tramite *merged mining*.

Titolo originale: Dedicated Cost Principle

Indice

Principio di Svalutazione

La proprietà di un prodotto si trasferisce dal produttore al consumatore (o ad un altro produttore), tuttavia né la produzione né il consumo sono avvenuti in quel momento (n.d.t. il momento dello scambio). Il Produttore tiene da parte il prodotto prima dello scambio e il consumatore lo conserva dopo che esso è avvenuto. Il prodotto esiste e viene infine scambiato tra le persone. I termini "produttore" e "consumatore" sono nomi che definiscono gli *obiettivi* (produzione e tempo libero) dei due principali attori economici. Il produttore *vuole* creare (apprezzare) il capitale, mentre il consumatore vuole distruggerlo (svalutarlo). Un produttore che possiede in maniera esclusiva non produce e un consumatore che non possiede non consuma. Ma la riserva del produttore (il suo inventario) svaluta il prodotto così come lo svaluta il consumatore.

L'utilizzo comune del termine "consumo" confonde l'interesse con la svalutazione. Il realizzarsi della *vendita* di un prodotto rappresenta un interesse per l'investitore, non una svalutazione del prodotto stesso. La svalutazione di un prodotto è consumo *attuale* e può rappresentare per il suo possessore un servizio (utilità) o uno spreco. Lo spreco è una svalutazione sulla quale il possessore non attribuisce alcun valore. Solo la distruzione riflette il consumo presente così come solo la creazione riflette la produzione presente. Solo l'*azione* possiede un significato economico, il nome attribuito ad uno specifico ruolo non ne possiede alcuno. Il ricavo netto di una vendita che va dal produttore al consumatore è l'interesse, anche se esso viene capitalizzato attraverso il reinvestimento.

La ricchezza, definita come capitale accumulato, è la somma dei prodotti. Tutti i prodotti sono accumulati e subiscono svalutazione. La produzione crea prodotti, mentre l'interesse rappresenta sia il costo che il ritorno economico nel fare ciò. Il prezzo di un prodotto è la somma del suo interesse sul ritorno dell'investimento ed il costo di tutti i prodotti consumati nella sua produzione. Ogni prodotto incorporato come componente di un nuovo prodotto è svalutato interamente come prodotto indipendente ed apprezzato nel nuovo prodotto. Poiché la somma dei costi di produzione equivale al principale dell'investimento, l'incremento netto nei prodotti è semplicemente l'interesse.

Il tasso di crescita della ricchezza è la differenza tra il tasso di interesse ed il tasso di svalutazione.

```
tasso-di-crescita = tasso-di-interesse - tasso-di-svalutazione
```

Gli esempi che seguono dimostrano l'effetto della svalutazione sulla crescita:

```
tasso-di-crescita = tasso-di-interesse - tasso-di-svalutazione
  5% = 10% - 5%
-10% = 10% - 20%
```

Il tasso di svalutazione è sempre positivo, poiché tutti i beni si svalutano.

```
tasso-di-svalutazione > 0
tasso-di-interesse - tasso_di_crescita = tasso-di-svalutazione
tasso-di-interesse - tasso_di_crescita > 0
tasso-di-interesse > tasso_di_crescita
```

Ogni bene manifesta svalutazione, il che implica che l'interesse economico è sempre maggiore della crescita economica

L'interesse economico può essere osservato nel tempo come il ritorno sul capitale investito.

> Gli investitori si aspettano dei ritorni del 10.2% assieme ai *millenials* che sperano in rendimenti maggiori.
>
> Shroeders: Global Investor Study

I tassi di svalutazione possono essere derivati dai tassi di interesse e di crescita del capitale.

> La crescita globale nel 2019 è diminuita al 2.6 percento, [...] cosa che riflette scambi commerciali internazionali ed investimenti più deboli del previsto all'inizio dell'anno. Si prevede che la crescita salga gradualmente al 2.8 percento entro il 2021.
>
> World Bank: Global Economic Prospects

In questo caso un tasso di interesse del 10.2% è controbilanciato dal 7.6% di svalutazione che porta al 2.6% di crescita.

```
tasso-di-svalutazione = tasso-di-interesse - tasso_di_crescita
tasso-di-svalutazione = 10.2% - 2.6% = 7.6%
```

Questo dato è consistente con le stime di svalutazione del capitale. Mentre gli edifici ed i macchinati hanno bassi tassi di svalutazione, i veicoli, il corredo da ufficio e le scorte di cibo (ad esempio) ne hanno uno ben più alto.

> Nel periodo 1960-2000, le tre stime per i macchinari e l'attrezzatura sono 5.61%, 5,42%, e 5.68%. Per gli edifici, le stime sono 3.36%, 3.43%, e 3.43%.
>
> OECD: Estimating Depreciation Rates

Nella misura in cui il denaro manifesta valore d'uso, essa si deprezza come ogni bene. Si presume che la moneta fiat, come il Bitcoin o il Dollaro Statunitense,

non abbia valore d'uso. Una moneta *pura* non manifesta alcuna crescita a causa del costo opportunità dell'interesse a cui si rinuncia. In altre parole, l'interesse rappresenta la cattura del valore del tempo ed il deprezzamento della moneta incorpora la mancata cattura di quel valore.

```
tasso-di-crescita-moneta-pura = tasso-di-interesse - tasso-di-interesse
0% = 9% - 9%
```

Il valore di tutte le monete *presenti* subisce anche una svalutazione dovuta al demurrage.

```
tasso-di-crescita-moneta-merce = tasso-di-crescita-moneta-pura - demurrage
-1% = 0% - 1%
```

I tassi di crescita delle monete inflazionarie e deflazionarie sono discussi nella Fallacia della Moneta non Prestabile.

Titolo originale: Principio di Svalutazione

Indice

Principio di Espressione

Le *azioni* umane non devono essere confuse con i *beni*. Non riuscire a distinguere i due concetti, al livello più fondamentale, porta ad errori dalle conseguenze significative. Le azioni sono fondamentalmente delle preferenze dell'essere umano cui viene data *espressione* attraverso i beni che sono oggetto di tale espressione. Senza espressione una preferenza è solamente un pensiero e un bene non fornisce alcun servizio. La catallattica stessa riguarda le preferenze espresse in maniera specifica riguardanti la produzione, lo scambio ed il consumo.

Lo spirito umano è l'attore (la persona). Egli possiede delle preferenze che esprime attraverso il corpo sul quale ha il controllo (che egli possiede). Il corpo è la sua proprietà, un bene. Quando il suo corpo è totalmente svalutato (alla morte), lo spirito cessa di essere attore. Non è necessario contemplare la separazione degli spiriti dai corpi in quanto non è implicata alcuna azione.

La catallattica non riguarda i concetti legali, teologici, o etici dell'umanità. Il Test di Turing è un criterio sufficiente per definire se una entità è umana. La distinzione catallattica è riposta nel modo in cui si formano le preferenze, in maniera indipendente da qualsiasi altro attore. Una persona intesa in questo senso è un decisore e si distingue da una entità che segue delle regole. Una macchina è un bene (n.d.t. economico) che esprime le preferenze di una persona. Una persona esprime le sue preferenze facendole eseguire alla sua macchina.

Uno spirito non può essere una proprietà, mentre un corpo è di proprietà del suo spirito. Solamente lo spirito controlla il corpo e il controllo definisce la proprietà. Nel caso in cui lo spirito è obbligato ad agire attraverso l'aggressione da parte di un altro attore, la preferenza non è espressa indipendentemente. La preferenza espressa (l'azione) è quella dell'aggressore.

La catallattica considera solamente le conseguenze di attori indipendenti. Quando una persona subisce un furto, è la preferenza del ladro a venire espressa, non la propria. Quando una persona paga una tassa, si presume che essa stia esprimendo la preferenza di un'altra persona poiché una tassa non è volontaria per natura. La schiavitù implica l'espressione delle preferenze del padrone, non di quelle dello schiavo. Sostituire la preferenza di qualcuno con quella di un altro è uno scambio non volontario (un furto).

Viene talvolta affermato che il tempo ha valore perché la vita è un fenomeno temporaneo. Questo non rappresenta il fondamento della preferenza temporale. Il fatto che una persona non abbia vita eterna non ha conseguenze sulla catallattica. Una persona può vivere per sempre, tuttavia si presuppone sempre che essa manifesti una preferenza per possedere i beni prima rispetto a possederli più tardi nel tempo. Una vita infinita non implica il mancato desiderio di consumare.

L'azione è l'espressione della preferenza umana attraverso i beni. I processi che vengono controllati dalle persone sono azione mentre i processi che vengono compiuti da macchine sono beni. In altre parole, produzione/lavoro, scambio/furto, e tempo libero/spreco sono azioni, mentre siti web, catene di montaggio e automobili sono beni.

Titolo originale: Expression Principle

Indice

Principio di Inflazione

Si presuppone che una moneta cambi il proprio potere d'acquisto in proporzione alla domanda di beni che essa rappresenta. In altre parole, con un quantità di moneta doppia, ciascuna unità della moneta sarà in grado di scambiare metà del precedente quantitativo di beni, e ciò avviene poiché un aumento del quantitativo di beni implica una minore domanda (n.d.t. relativa) per essi. Si tratta di una relazione di proporzionalità tra l'inflazione monetaria e l'inflazione del prezzo (o deflazione). Questa relazione monetaria è una espressione della legge della domanda e dell'offerta.

- La moneta di mercato caratterizzata da incremento dell'offerta, come l'Oro e il Bitcoin delle prime fasi, consuma un valore di beni pari al valore delle nuove unità create - cosa che include il costo opportunità del capitale investito nel fare ciò. Per questa ragione essa non produce alcuna variazione nella proporzionalità e di conseguenza nessuna inflazione di prezzo.
- La moneta di monopolio non è soggetta a competizione nella sua produzione, cosa che permette al produttore di ottenere un premio di monopolio nel momento in cui le nuove unità vengono prezzate. Per questa ragione il produttore è portato ad incrementare la proporzione di moneta rispetto ai beni, cosa che porta all'inflazione del prezzo.
- La moneta di mercato caratterizzata da offerta fissata, come il Bitcoin delle fasi avanzate (n.d.t. quando termina la distribuzione di nuove monete, ovvero quando si esaurisce la componente di sussidio), non crea unità addizionali. Per questa ragione la proporzione di moneta rispetto ai beni decresce con la crescita economica, cosa che porta alla deflazione del prezzo.

La proporzionalità si riferisce ai beni "rappresentati" da una moneta. Se ci fosse solo una moneta, questa sarebbe in relazione diretta con tutti i beni. Tuttavia la relazione deve essere analizzata in presenza di molteplici monete. I beni rappresentati da una moneta sono quelli per i quali essa può essere scambiata. In altre parole, la relazione implica una domanda per i beni denominati in quella moneta.

Tuttavia, la domanda non rimane costante nel caso venga intrapresa la decisione di effettuare attività mineraria (n.d.t. estrattiva). Viene creata una nuova domanda di beni derivante dalle necessità dell'attività estrattiva. Il minatore deve

consumare dei beni "rappresentativi" nella produzione della moneta. La nuova moneta è interamente compensata dall'incremento di domanda rappresentato dai beni consumati e dal costo opportunità (i.e. vi sono meno nuovi beni) nell'impiegarli nell'attività estrattiva. Di conseguenza la proporzionalità è preservata allo stesso modo anche nel caso ci siano molteplici monete. **La crescita economica non è caratterizzata da inflazione di prezzo nel libero mercato.**

> Variazioni nell'offerta di moneta devono necessariamente modificare la disposizione di beni vendibili per come sono posseduti da vari individui e società. La quantità di moneta disponibile nell'intero sistema di mercato non può aumentare o diminuire senza che prima siano aumentate o diminuite le disponibilità di liquidità di certi individui.
>
> Mises: L'azione Umana

Questa affermazione asserisce che la nuova moneta ha effetto prima sulle disponibilità in denaro. Tuttavia ciò non si verifica con la moneta di mercato. La sua creazione *riduce* allo stesso tempo la disponibilità di *beni* e *incrementa* le disponibilità di *denaro*. L'aumento di domanda di moneta è compensato simultaneamente e proporzionalmente dal suo stesso aumento di offerta. Questa riduzione di beni non può essere ignorata nella valutazione della relazione monetaria. L'affermazione infatti confonde la moneta di mercato con la moneta di monopolio poiché la seconda non consuma il suo valore in termini di beni attraverso la produzione. Nella misura in cui i beni sono consumati sostanzialmente nello stesso luogo in cui la moneta viene prodotta, e nello stesso momento, non ha luogo neanche una distribuzione disomogenea della relazione monetaria.

Questo errore persiste nonostante venga esplicitamente riconosciuto che l'attività estrattiva consumi, in termini di beni, il valore che produce come nuova moneta.

> Il fatto che i proprietari di miniere d'oro si basino su degli stabili ricavi annuali dovuti alla loro produzione di oro, ciò non annulla l'effetto della nuova quantità di oro estratta sui prezzi. I proprietari delle miniere prendono dal mercato, in cambio dell'oro prodotto, i beni ed i servizi necessari per l'attività estrattiva [...]. Se essi non avessero prodotto questo quantitativo di oro, i prezzi non ne sarebbero stati influenzati.

Presa letteralmente, l'ultima frase è una tautologia (nessuna creazione implica nessun effetto di prezzo derivante dalla creazione stessa). Dal contesto risulta chiaro il ragionamento di Mises secondo il quale, se l'oro non fosse stato prodotto, i prezzi sarebbero rimasti inalterati. Tuttavia senza un cambio nell'offerta di moneta, se i beni fossero stati consumati in un altra produzione, la crescita economica implicata avrebbe *diminuito* i prezzi; e se i beni fosse stati spesi per il tempo libero, la contrazione economica implicata avrebbe fatto *aumentare* i prezzi. In altre parole, la conclusione riportata sopra è perfettamente capovolta. La relazione monetaria è preservata *a causa* della produzione di moneta e

verrebbe cambiata solo a causa di un mancata produzione. Questo errore va poi a contagiare le teorie da esso dipendenti.

> Contro questo ragionamento si deve prima di tutto osservare che in un regime di economia progressiva in cui il dato di popolazione è in aumento e la divisione del lavoro ed il suo corollario, la specializzazione industriale, vengono perfezionati, prevale una tendenza verso un incremento di domanda della moneta. Un numero addizionale di persone appare sulla scena e vuole dotarsi di disponibilità di contante liquido. La misura della autosufficienza economica, i.e. relativa alla produzione per le necessità domestiche, si restringe e le persone fanno maggiore riferimento al mercato; questo, in linea generale, [p. 415] li spinge ad incrementare le loro disponibilità di denaro.

In altre parole, la sola crescita economica cambia la relazione monetaria - una diretta contraddizione con l'affermazione precedente.

> La tendenza all'aumento dei prezzi derivante da quella che è chiamata la "normale" produzione di oro incontra una tendenza al calo dei prezzi derivante dall'aumento di domanda della disponibilità di denaro. Tuttavia, queste due opposte tendenze non si neutralizzano a vicenda. Entrambi i processi prendono ognuno il proprio corso, ed entrambi portano ad uno scompiglio delle esistenti condizioni sociali, facendo diventare più ricche alcune persone, ed alcune più povere. Entrambi i processi influenzano i prezzi dei vari beni in tempi e misura differenti. E' anche vero che l'incremento di prezzo di alcune commodity causato da uno di questi processi può essere infine compensato dalla caduta causata dell'altro processo. Può accadere che, alla fine, alcuni o un numero significativo di prezzi tornino al loro precedente livello. Ma questo risultato finale non è l'esito di una assenza di movimenti provocati da cambiamenti nella relazione monetaria. E' piuttosto l'esito dell'effetto combinato della coincidenza di due processi indipendenti l'uno dall'altro.

Questa affermazione rappresenta la confutazione dell'idea della creazione di moneta come di uno "stimolo" alla crescita, cosa che è di per sé corretta. Tuttavia, essa assume in maniera scorretta che la domanda di moneta e la sua creazione siano processi indipendenti. Essi sono esplicitamente dipendenti per come viene espressa la relazione monetaria e la legge di domanda da essa richiamata. L'effetto delle relazioni indipendenti è perfettamente invertito in questo ragionamento, in quanto riesce solo a mascherare la relazione monetaria. Lo stimolo rappresenta un'inversione di causa ed effetto correttamente rifiutata, tuttavia è un errore accettare e rifiutare la relazione monetaria allo stesso tempo.

L'errore relativo all'inflazione, come quello commesso sul teorema di regressione, può sorgere da un comprensibile desiderio di spiegare gli effetti avversi della moneta di monopolio. Tuttavia nel puro sistema razionale della catallattica, ogni errore nella deduzione produce inconsistenza, cosa evidente in questo caso.

La moneta di mercato è soggetta ad inflazione monetaria ma non produce inflazione del prezzo. La moneta di monopolio è analogamente soggetta ad inflazione monetaria ma produce inflazione del prezzo - esclusivamente dovuta al monopolio sulla sua produzione. Von Mises generalizza troppo sul fatto che *tutta* l'inflazione monetaria porti ad inflazione del prezzo.

> I prezzi crescono allo stesso modo se [...] la domanda di moneta crolla a causa di una generale tendenza alla diminuzione delle disponibilità liquide di denaro. La moneta spesa in maniera addizionale da questo "disaccumulo" porta ad una tendenza di prezzi più alti alla stessa maniera di ciò che fluisce dalle miniere d'oro [...]. Di converso, i prezzi cadono quando l'offerta di moneta crolla, o [quando] la domanda di moneta aumenta (e.g., attraverso una tendenza all'"accumulo", ovvero detenere un maggiore disponibilità di saldo contante.

Il denaro è sempre posseduto da qualcuno. Assumendo, come esplicitato in precedenza, che non vi sia nessuna creazione di nuova moneta, una maggiore disponibilità di "saldo contante" per una persona implica una minore disponibilità per un'altra. Un maggiore accumulo di denaro implica solamente una minore domanda presente di beni relativa ad una anticipata domanda futura. Un minore accumulo di denaro implica solamente una maggiore domanda di beni nel presente. Non è come se il denaro fosse stato ri-seppellito nella terra. Non vi alcun costo nel "disaccumulare" (scambiare moneta), si tratta di qualcosa di differente rispetto alla moneta "che fluisce dalle miniere d'oro".

Un incremento generale dell'accumulo (di denaro) da l'*impressione* di maggiore ricchezza, ma ciò è illusorio. Per avere valore per le persone, la moneta deve essere scambiata per i beni, momento nel quale l'illusione scompare. A differenza dell'attività estrattiva, l'effetto del disaccumulo non è uniforme. La prima persona che lo applica ottiene il più alto valore di scambio mentre l'ultima ottiene il più basso. La strategia speculativa del "*pump and dump*" sfruttare questa disomogeneità. La ricchezza è trasferita, non creata.

Inoltre, un aumento dell'accumulo implica una più alta preferenza temporale, che è il rapporto tra il capitale accumulato e il capitale dato in prestito (rapporto di capitale), riflesso nel tasso di interesse. Questo porta ad un aumento del costo del tempo, non ad un maggiore valore del capitale. Lo stesso quantitativo di beni (la ricchezza) è presente nel momento in cui aumenta l'accumulo. Tuttavia questa aumentata proporzionalità riduce la produzione a causa del costo più elevato del capitale. Questo crea una *permanente* e composita riduzione della ricchezza poiché il tempo perso nella produzione non è mai recuperato anche a seguito di un successivo disaccumulo. Se tutto il denaro fosse accumulato per un decennio (assumendo che non si faccia ricorso al baratto), le persone, una volta disaccumulato, scoprirebbero che esso avrebbe perso significativamente valore a seguito di una marcata riduzione del quantitativo di beni disponibili.

Indipendentemente dalla crescita economica (o dalla contrazione), la variazione nella domanda per una moneta di mercato implica una variazione proporzionale nella domanda, o nell'offerta dei beni scambiati per quella moneta, in contrapposizione ad un'altra moneta o al baratto. L'offerta di beni è il livello per il quale la moneta è accettata per scambiarli. Una moneta manifesta valore monetario solo per la sua capacità di essere scambiata direttamente o indirettamente per cose caratterizzate da valore d'uso, così come direttamente implicato dalla relazione monetaria stessa. Il valore di una moneta deriva dalle persone che sono disposte ad accettarla ai fini dello scambio. Data la fungibilità della moneta, vendere moneta ad un'altra persona implica che non vi è alcun cambiamento nella sua accettazione.

Per quanto riguarda la moneta merce, questo principio è basato sull'assunzione che il quantitativo di beni richiesto per produrre la moneta rimanga costante. Il prezzo dei beni espressi nella moneta viene quindi mantenuto costante dalla relazione monetaria. Tuttavia, se il quantitativo di beni necessario per produrre una moneta commodity aumenta o diminuisce, viene rispettivamente implicata una decrescita od una crescita dei prezzi espressi in quella moneta. Di conseguenza, indipendentemente dalla domanda, la relazione monetaria è controllata dal tasso di variazione dei fattori di produzione necessari. Si presume che tali cambiamenti non siano predicibili in quanto sono già incorporati nel prezzo. Per questa ragione ciò costituisce un errore speculativo.

Titolo originale: Inflation Principle

Indice

Principio degli *Altri Mezzi*

Bitcoin è un atto di resistenza, un tentativo di "guadagnare un nuovo spazio di libertà". La libertà viene ridotta dalla costante pressione derivante dal finanziamento obbligatorio allo stato. E' un fatto ordinario che la libertà venga conquistata attraverso spargimenti di sangue, con lo specifico obiettivo di ridurre il potere dello stato. Bitcoin non può eliminare la necessità di correre rischi personali nel perseguire questo obiettivo. Tuttavia, attraverso la condivisione del rischio, esso può potenzialmente ridurre la tassa implicata dall'inflazione senza spargimento di sangue. Ciò non eliminerà la tassazione in maniera generale, tuttavia potrà ridurre il potere dello stato rendendo la tassa significativamente più visibile.

Questo conflitto tra stato ed individui per il controllo della moneta passerà, al massimo, attraverso quattro fasi previste dal modello di sicurezza di Bitcoin. Queste fasi possono sovrapporsi e variare in funzione del luogo ma sono, ciascuna, chiaramente identificabili.

1. Luna di miele
2. Mercato nero
3. Competizione
4. Resa

La fase della luna di miele è caratterizzata dal desiderio delle agenzie dello stato di conservare il controllo nella regolazione dei movimenti di moneta e dei titoli mobiliari (*securities*). Per questo fine viene fatta pressione sui punti di aggregazione. All'aumentare della pressione sui miner che si sono raggruppati (*pooled miners*) e sui commercianti centralizzati, il costo aumenta e l'utilità cala. La moneta diventa quindi maggiormente distribuita per evitare queste spese.

Nel momento in cui è evidente che i controlli applicati sui punti di aggregazione risultano insufficienti, ed emerge la consapevolezza che il signoraggio è a rischio, le transazioni ed il mining di bitcoin vengono dichiarati fuorilegge. Poiché gli stati tendono a collaborare al fine di proteggere le loro monete, questa potrebbe diventare una "Guerra al Bitcoin" su scala globale. Ciò potrebbe coincidere con l'adozione di una nuova moneta ufficiale, i.e. la *Fedcoin*. L'obiettivo sarebbe quello di indurre le persone ad adottare una moneta apparentemente "più sicura"

di Bitcoin ma di mantenere nel contempo il signoraggio e i vantaggi portati dalla sorveglianza di una moneta fiat elettronica.

Assumendo una sufficiente resistenza, Bitcoin continua ad esistere indipendentemente dalla *Fedcoin* come una moneta del mercato nero. A questo punto lo stato è indotto a concludere che l'unica tattica efficace è quella di competere come miner. Poiché il mining è una attività necessariamente anonima, non vi è alcun modo di tipo economico per impedire la partecipazione dello stato nel mining. Di conseguenza il Bitcoin entra nella fase di competizione con lo stato che prova a perpetrare un attacco del 51% continuo.

Considerando a parte la continua fase di contrasto al mercato nero, la fase competitiva è caratterizzata da una pacifica battaglia di hash power tra lo stato e gli individui. Lo stato opera in perdita poiché deve escludere le transazioni soggette a censura (n.d.t. nei blocchi da lui minati). Questa perdita è compensata dal gettito fiscale. La pressione dovuta alle fee delle transazioni censurate aumenta fino al punto in cui il sussidio derivante dalla tassa sul mining non è compensato da questo livello di *fee*. **A questo punto le tasse e le commissioni delle transazioni censurate aumentano entrambe fino al punto in cui uno schieramento del conflitto non dichiara la resa.** In questa modo Bitcoin può potenzialmente vincere una guerra per altri mezzi. Non si può assumere, tuttavia, che questa resa sia perpetua. Come implicato ne il Paradosso del livello di Minaccia, è probabile che la situazione possa riportarsi alle fasi precedenti al diminuire della minaccia.

Titolo originale: Other Means Principle

Indice

Principio di Resistenza al Brevetto

A differenza del copyright, il brevetto è una forza anti-mercato. Un vero contratto di copyright è un accordo contrattuale tra il compratore ed il venditore, mentre un brevetto è esclusivamente una concessione di monopolio data dallo stato. Il brevetto non è un "attacco" esercitato dal detentore dello titolo stesso, è una distorsione creata dallo stato sulla pressione di aggregazione.

Il processo di mining è altamente competitivo. La protezione di monopolio nell'uso di un algoritmo di mining efficiente rappresenta una forte pressione di aggregazione anti-mercato. Bitcoin è reso sicuro dalle persone che resistono alle forze anti-mercato. La resistenza affronta un rischio maggiore quando i miner sono fortemente raggruppati e/o non anonimi.

Se le persone non oppongono resistenza a queste forze non vi è sicurezza nella moneta. Quando il livello di minaccia aumenta le conseguenze della violazione di brevetto diventano un rischio di livello pari a quello dello stesso mining. Per questa ragione l'impatto dei brevetti non è irrilevante poiché riguarda la sicurezza della moneta.

Titolo originale: Patent Resistance Principle

Indice

Principio di Condivisione del Rischio

Bitcoin non è protetto dalle blockchain, dall'hash power, dalla validazione, dalla decentralizzazione, dalla crittografia, dall'*open source* o dalla teoria dei giochi - è protetto dalle persone.

La tecnologia non è mai la radice della sicurezza di un sistema. La tecnologia è uno strumento che aiuta le persone a proteggere ciò che ha valore per loro. La sicurezza richiede alle persone di agire. Un server non può essere protetto da un *firewall* se non vi è una serratura sulla porta della stanza in cui esso si trova, la quale, a sua volta, non può proteggere la stanza senza un guardiano che la controlli, il quale, a sua volta, non può proteggere la porta senza correre alcun rischio per la propria incolumità.

Bitcoin non è diverso da tutto ciò, è protetto dalle persone che corrono un rischio personale nell'utilizzarlo. Condividere questo rischio con altre persone è lo scopo della decentralizzazione. Un sistema centralizzato richiede che una sola persona si faccia carico di tutti i rischi ad esso connessi. Un sistema decentralizzato suddivide i rischi tra gli individui che rappresentano la sicurezza del sistema. Coloro che non comprendono il valore della decentralizzazione molto probabilmente non comprendono neanche il ruolo necessario delle persone ai fini della sicurezza.

Bitcoin permette alle persone di condividere il rischio personale di accettare e minare la moneta. E' la sola volontà e abilità di queste persone a resistere che può impedire la coercizione dei loro nodi e la cooptazione dei loro centri di mining, ed in realtà è questo principio ciò che protegge Bitcoin. Se le persone non accettano questi rischi non vi è una sicurezza efficace della moneta. Se un gran numero di persone li accetta, il rischio individuale viene minimizzato. Bitcoin è uno strumento, non è magia.

Titolo originale: Risk Sharing Priciple

Indice

Principio di Riserva

Il termine "riserva" si riferisce al capitale accumulato che si differenzia dalla porzione dei risparmi che viene investita. Sia gli stati che le persone accumulano capitale per rispondere agli attesi requisiti di liquidità. Il termine "valuta di riserva" si riferisce al capitale accumulato dallo stato che si rende necessario per il *settlement* delle partite economiche con gli altri stati. Le riserve di moneta delle persone che vivono in uno stato consistono generalmente della moneta emessa dallo stato stesso - principalmente banconote o moneta fiat e un quantitativo minore in moneta.

Gli stati acquistano moneta di riserva dalle persone usando moneta di monopolio, controllo del cambio estero e tassazione diretta. Usando la loro stessa moneta, essi scontano tali acquisti di un quantitativo pari al signoraggio. Il controllo del cambio estero restringe o proibisce l'uso della valuta di riserva come moneta. Trattando la valuta di riserva come una proprietà ma non come una moneta, lo stato crea una tassa sull'apparente guadagno ottenuto sulla moneta di riserva quando esso svaluta la sua moneta attraverso l'inflazione monetaria. I tassi di cambio ufficiali al di sotto del valore di mercato creano un'altra tassa sull'uso della valuta di riserva.

Un "*gold standard*" rappresenta uno standard per il quale lo stato accumula oro come moneta di riserva, e gli individui tengono a riserva dei titoli di riscossione di un quantitativo "standard" d'oro. Nel 1834 si stabilì che il Dollaro Statunitense potesse essere riscattato al tasso di 20.67 $ per oncia d'oro. Per 100 anni lo stato ha acquistato e venduto oro allo stesso tasso. Nel 1934 il Dollaro venne svalutato del 60% a 35$ per oncia. A questo punto la sua redimibilità (da parte delle persone) fu abrogata e venne reso illegale accumulare o contrattare in oro. Questo divieto alla redimibilità venne esteso anche agli altri stati nel 1971, ponendo ufficialmente fine al gold standard negli Stati Uniti. Non più sotto forma di un debito dello stato, il Dollaro è passato dall'essere una valuta rappresentativa (i.e una banconota) ad una valuta fiat.

La principale riserva estera degli Stati Uniti è l'oro (74.5%) con il rimanente costituito da valuta estera e titoli equivalenti, al contrario dei cittadini la cui riserva principale è il Dollaro. La stesse banconote o monete fiat dello stato non sono generalmente utilizzabili come moneta di riserva estera, in quanto lo stato

può abrogare o svalutare i pagamenti dovuti. Il Tesoro degli Stati Uniti afferma di detenere oltre 8'000 tonnellate metriche di oro dal valore approssimativo di 400'000'000'000 $. Il potere d'acquisto di una banconota di Dollaro Statunitense del 1834 era all'incirca 30 volte superiore al valore del Dollaro Statunitense fiat del 2019.

Lo scopo di una moneta di riserva è quello di tassare. Per prima cosa lo stato acquista moneta di riserva con titoli di credito promissori negoziabili, successivamente emette più titoli di credito rispetto alla quantità di moneta in riserva, poi abroga i titoli di credito e infine mantiene la riserva originale. La svalutazione delle banconote è il risultato della loro emissione eccessiva (signoraggio) e rappresenta una tassa su coloro che le detengono come riserva. Lo stato raccoglie la moneta di riserva e la detiene come un accumulo che rappresenta la solvibilità rispetto ai debiti contratti con gli altri stati. Nonostante le persone possano ancora accumulare moneta di riserva, essa è soggetta a vincoli onerosi così da preservare il beneficio di tassazione derivante dal monopolio di stato sulla moneta. Questi vincoli diventano più restrittivi all'aumentare del livello di tassazione.

L'uso dell'oro come riserva di stato non offre alcun beneficio monetario agli individui che sono comunque costretti ad utilizzare negli scambi la moneta di monopolio. Come mostrato ne la Fallacia della Valuta di Riserva, il Bitcoin come riserva di stato non può rappresentare un miglioramento. Tuttavia, a differenza dell'oro, la definizione di Bitcoin appartiene a coloro che lo accettano nello scambio. Se la maggior parte dei bitcoin fosse in mano allo stato e le persone utilizzassero dei sostituiti monetari negli scambi, nessuna azione potrebbe impedire allo stato di introdurre arbitrariamente sia inflazione che censura.

Titolo originale: Reservation Principle

Indice

Principio di Scalabilità

La scalabilità è l'incremento proporzionale di alcune prestazioni di un sistema quando viene impiegato più hardware. Il *throughput* (n.d.t. capacità di processamento nell'unità di tempo) delle transazioni bitcoin è perfettamente non scalabile in quanto nessun quantitativo di hardware aggiuntivo può incrementarlo.

La regola di consenso relativa limite alla dimensione del blocco stabilisce un compromesso arbitrario tra l'utilità e la sicurezza del sistema. Un aumento della dimensione del blocco incrementa marginalmente il *throughput* delle transazioni e di conseguenza incrementa il costo delle risorse nella validazione delle stesse (i.e. elaborazione, storage, e banda). All'aumentare del costo di validazione, la sicurezza economica è influenzata negativamente da un più elevato rischio di centralizzazione. Poiché il compromesso è arbitrario per natura, non può esistere una dimensione ideale (n.d.t. del blocco).

Per ogni dimensione del blocco adottata, il sistema non è scalabile poiché risulta necessario attendere la finalizzazione delle transazioni attraverso la conferma. Poiché solo un numero finito di transazioni può essere selezionato per l'inclusione in un blocco, altre transazioni potrebbero risultare escluse. Questa esclusione è motivata a livello finanziario dal costo opportunità di non utilizzare il capitale impiegato nel mining e rappresenta la manifestazione della non scalabilità. Questa scarsità intrinseca necessita di un mercato competitivo delle conferme che viene finanziato in proporzione alla domanda di moneta.

L'effettiva capacità di supportare transazioni aggiuntive, e di conseguenza l'utilità, può essere incrementata dal *layering*. Questo rappresenta un compromesso di sicurezza di tipo *locale* e *limitato nel tempo* che si differenzia dal compromesso di sicurezza di tipo *sistemico* e *persistente* che caratterizza l'aumento della dimensione del blocco. Entrambi i compromessi abbassano ma non eliminano la soglia di utilità, cosa che implica la conservazione della proprietà di stabilità.

Di conseguenza la stabilità e la non scalabilità esistono per ogni dimensione del blocco e per ogni livello di *layering*.

Titolo originale: Scalability Principle

Indice

Principio di Inflazione Soggettiva

L'inflazione del prezzo nel libero mercato deriva completamente delle preferenze personali, e pertanto non è riconducibile a nessun altro fattore.

- Il prezzi dei beni sono determinati soggettivamente. [Teoria Soggettiva del Valore]
- La preferenza temporale determina l'espansione del credito sulla moneta. [Assioma di preferenza temporale]
- La creazione di moneta non provoca l'inflazione dei prezzi. [Principio di Inflazione]

Questo principio potrebbe essere ottenuto più semplicemente dalla definizione di libero mercato che è, di per sé, una entità costruita solamente sulle preferenze personali.

Titolo originale: Subjective Inflation Principle

Indice

Principio di Consolidamento

La necessità di scambiare una moneta con un'altra al fine di effettuare degli scambi con dei commercianti rappresenta un costo. Questo costo deve essere non nullo anche se automatizzato in quanto deve consumare spazio e/o tempo. Per questa ragione, una sola moneta è sempre "migliore" (ha maggiore utilità) di due monete, nella misura in cui l'unica moneta risultante non diventi dipendente dal livello delle *fee* come implicato dalla soglia di utilità.

Possiamo ragionevolmente supporre che due monete distinte non possano avere perennemente la stessa utilità. La Legge di Thiers mette in evidenza le conseguenze legate alla migliore moneta in assenza del controllo dello stato. Da questo concludiamo necessariamente che, in assenza del controllo dello stato, **la migliore tra le due monete, alla fine, rimpiazzerà l'altra** . Quando ciò avviene, l'utilità si concentra sulla moneta che sopravvive seguendo una dinamica opposta rispetto a quanto dettagliato ne il Principio di Frammentazione.

Il principio non implica che (altre) nuove monete non possano essere create o esistere durante un significativo lasso di tempo. Esso implica semplicemente che vi è una pressione di mercato che indirizza verso una singola moneta. La migliore moneta in una situazione, può non essere affatto una buona moneta o addirittura una moneta utile in un'altra situazione. Per esempio, l'oro non è una moneta utile per il trasferimento elettronico e bitcoin non è molto utile in assenza di una rete. Una moneta rimpiazza un'altra negli scenari nei quali essa è migliore.

Titolo originale: Consolidation Principle

Indice

Principio di Frammentazione

A differenza del baratto, l'utilità di una moneta deriva direttamente dalla sua abilità di facilitare gli scambi. Se essa non è accettata da *nessun* commerciante allora essa non ha obiettivamente alcuna utilità monetaria. Maggiore è la quantità di beni e servizi (inclusiva della valutazione della loro ubicazione) che può essere acquistata con una moneta in un certo tempo, maggiore è la probabilità che la moneta abbia maggiore utilità per ogni singola persona.

Una separazione implica che zero o più commercianti hanno smesso di accettare la moneta originale e che zero o più commercianti hanno iniziato ad accettare la moneta che si è separata. Una separazione "pulita" è una situazione ipotetica nella quale l'accettazione da parte dei commercianti delle due monete non si sovrappone (n.d.t. ogni commerciante accetta solo una delle due monete) e che non vi sono cambiamenti nell'insieme dei commercianti. Una separazione "pulita" produce due economie dall'insieme originale dei commercianti.

Se assumiamo che le monete siano identiche a parte l'evento relativo alla loro separazione, il Principio di Consolidamento implica che l'utilità delle due monete aggregate è la medesima della moneta originale a cui va sottratto il costo di scambio. Lo scenario qui descritto può essere esteso al fine di includere la sovrapposizione dei commercianti. Ciò non ha effetto sull'utilità della moneta in quanto va a spostare l'incidenza del costo di scambio dall'acquirente al venditore.

Un aumento o una diminuzione del numero di commercianti che accettano una delle due monete rappresenta, rispettivamente, un guadagno netto o una perdita di utilità combinata in quanto ciò implica la rimozione o l'aggiunta del costo di scambio di una terza moneta. In altre parole, l'effetto è proporzionale per ciascuna delle monete coinvolte nella separazione. Questo fattore si riferisce alle caratteristiche specifiche di ciascuna separazione, non al processo di separazione in generale.

Di conseguenza, una separazione produce sia uno spostamento che una riduzione di utilità in proporzione alla dimensione relativa delle due economie. Ne la

Fallacia dell'Effetto Network viene spiegato perché la riduzione non sia di natura quadratica, come talvolta si tende a credere.

Sebbene possa sembrare che nello spostamento qualcuno abbia "preso" valore dalla moneta originale, tale valore è tuttavia "andato" a formare la moneta separata. In altre parole, i commercianti sono padroni del valore che essi stessi attribuiscono ad una moneta. Nel momento della separazione un'unità originale si trasforma in due unità ciascuna avente proporzionalmente una diminuita utilità rispetto all'originale. Impiegando una *replay protection* obbligatoria e bidirezionale, ciascuna delle due monete può essere spesa senza costi addizionali. Altrimenti la necessità di protezione da questo evento porta a scontare le unità della(e) catena(e) non protetta(e).

Questa analisi è applicabile anche alle nuove monete. La differenza nel caso di una nuova moneta risiede nel fatto che le unità delle (altre) monete originali non possono essere spese sulla nuova catena. Per questa ragione, la nuova moneta deve affrontare la difficoltà di allocare le sue unità, cosa che richiede lavoro e quindi tempo. Le separazioni avviano automaticamente questo processo suddividendo l'utilità di una catena esistente, nella misura in cui i suoi commercianti sono disposti a fare ciò.

Titolo originale: Fragmentation Principle

Indice

Principio dell'Assenza di Permesso

Bitcoin è stato progettato per operare senza il permesso di alcuna autorità. La sua *value proposition* è interamente basata su questa proprietà.

Dal punto di vista dello stato, un mercato può essere classificato come: dotato di autorizzazione (*permissioned*), o non dotato di autorizzazione (*permissionless*). Per semplicità di terminologia, al primo ci si riferisce spesso con il termine "mercato legale" (*white market*) e al secondo con il termine "mercato nero" (*black market*). Gli scambi del mercato legale, per definizione, richiedono una autorizzazione mentre quelli del mercato nero non la richiedono.

Per una semplice questione di definizione, le operazioni in Bitcoin non possono essere contemporaneamente appartenenti al mercato legale e non dotate di autorizzazione. Ogni persona che opera nel mercato legale necessita di una autorizzazione per fare ciò. Bitcoin è quindi intrinsecamente una moneta del mercato nero. La sua architettura di sicurezza assume necessariamente di operare senza il permesso dello stato.

La sicurezza di Bitcoin non si estende quindi ai sistemi che operano nel mercato legale. **Ogni sistema dipendente dalla *value proposition* di Bitcoin deve anche essere un mercato nero**.

Titolo originale: Permissionless Principle

Indice

Principio dei Dati Pubblici

Dal Principio di Condivisione del Rischio consegue che la sicurezza del sistema dipende dalle attività di mining e di scambio svolte sotto copertura. Una moneta esiste sotto forma di un mercato mutuamente vantaggioso tra i miner e i commercianti basato sulla conferma di transazioni all'interno dei blocchi in cambio di *fee*.

Le attività che avvengono necessariamente sotto copertura sono suddivise per ruolo:

Miner

1. ottenere i blocchi [sui quali aggiungere nuovi blocchi]
2. ottenere transazioni non confermate [da cui guadagnare commissioni]
3. creare e distribuire blocchi [affinché altri possano aggiungere nuovi blocchi sopra di essi]
4. ricevere pagamenti in cambio di conferme [per finanziare le proprie operazioni]

Commercianti

1. ottenere blocchi [per validare i pagamenti dei clienti]
2. ottenere transazioni non confermate (opzionale) [per anticipare pagamenti e *fee*]
3. creare e distribuire transazioni [per ottenere il pagamento dei clienti]
4. effettuare pagamenti in cambio di conferme [per remunerare le conferme]

Se i blocchi non possono essere ottenuti anonimamente il sistema non è sicuro. L'impossibilità di ottenere i blocchi del ramo più forte disponibile ad altre persone rappresenta una partizione della rete e costituisce una falla localizzata nella sicurezza. Tuttavia, né l'anonimità né il suo opposto, l'identità, possono assicurare che un individuo osservi il ramo più forte della catena. In altre parole, ogni sforzo teso a mitigare il partizionamento con l'introduzione dell'identità rappresenta una falsa dicotomia che sacrifica la sicurezza del sistema in cambio della erronea pretesa di garantire la sicurezza in forma localizzata.

Non è essenziale che tutti i miner o i commercianti vedano tutte le transazioni in ogni momento. Tuttavia, un'ampia visibilità è preferibile in quanto produce

la più robusta competizione tra le *fee* e la massima informazione. In altre parole un mercato nel quale ogni partecipante vede tutte le transazioni in ogni momento è un mercato in concorrenza perfetta. Richiedere alla rete transazioni specifiche, rispetto a richiederle tutte (o richiedere informazioni riassuntive di tutte) rappresenta una possibile forma di tracciamento e, come tale, deve essere evitata anche nell'interesse della sicurezza.

La creazione di blocchi e di transazioni non espone in maniera intrinseca l'identità, tuttavia la distribuzione pubblica degli stessi è la fonte principale del tracciamento. Nella misura in cui i miner rivelano apertamente la loro identità, essi stanno facendo affidamento sull'ipotesi di un ambiente a basso livello di minaccia e non contribuiscono alla sicurezza del sistema. Evitare il tracciamento mentre si inoltrano blocchi e transazioni richiede l'uso di una connessione anonima ad un server della comunità (n.d.t. un nodo bitcoin). Questo garantisce che la rete del protocollo peer to peer non abbia mai modo di accedere ad informazioni che portino ad identificazione.

La proof-of-work garantisce l'anonimità dei miner. Infatti, non vi è firma associata al mining e si assume che l'energia sia disponibile in maniera diffusa. Analogamente, l'abilità di pagare anonimamente per ottenere la conferma è la ragione per la quale vengono incluse le *fee* di transazione. E' sufficiente pagare un miner direttamente (off-chain) per avere conferma della transazione, tuttavia questo espone reciprocamente sia il commerciante che il miner e rende più difficile stimare le *fee* in maniera anonima.

Bitcoin è un sistema innovativo perché tutte le transazioni finanziarie possono essere validate a partire da dati pubblici e senza l'uso dell'identità. I sistemi finanziari centralizzati si basano sulla fiducia delle connessioni con altre controparti (attraverso l'identificazione in forma crittografata) o sulla fiducia delle firme (verificabili in maniera crittografica) che accompagnano i dati trasmessi. Questa è l'essenza dei sistemi basati sulla fiducia; alcune autorità hanno dei segreti che gli altri usano per verificare la loro autenticità. **La ragione alla base della validazione è quella di eliminare l'uso dell'identità e di conseguenza quello dell'autorità.**

Titolo originale: Public Data Principle

Indice

Principio del Social Network

Nella terminologia introdotta nell'articolo del 1964 di Paul Baran sui network distribuiti, l'importanza della topologia nella progettazione delle reti risiede nella capacità, da parte delle comunicazioni inviate attraverso di esse, di sopportare la perdita di un certo numero di nodi. Un network centralizzato (a stella) cadrà con la perdita del solo nodo centrale. Un network distribuito (rete *mesh*) è più resiliente. Un ibrido tra i due è considerato un network decentralizzato.

Come moneta, Bitcoin forma un grafo sociale. Solo una persona può decidere di accettare una certa moneta o un'altra in uno scambio. Un insieme di persone che condividono la stessa definizione di una moneta viene chiamato un consenso. L'autorità in un sistema monetario è il potere di definire la moneta. Bitcoin è uno strumento che le persone possono utilizzare per difendersi dalla tendenza verso l'autorità, così da preservare i loro accordi e quindi l'utilità nella moneta.

Nella terminologia dei sistemi distribuiti un "nodo" Bitcoin è una persona e il sistema è la moneta stessa. Non ha importanza quante macchine controlli una persona, la perdita di quella persona equivale alla perdita di un nodo del sistema (che include la perdita di tutte le macchine appartenenti a quella persona). Una moneta centralizzata non può neanche sopportare la perdita di una sola persona. Se quella persona apporta dei cambiamenti alle regole precedentemente in vigore, la moneta originale cessa di esistere. Come mostrato ne il Principio di Condivisione del Rischio, Bitcoin si affida alla decentralizzazione per permettere alle persone di resistere l'autorità. Questo assetto decentralizzato permette alla moneta di essere in grado di sopportare la perdita di numerose persone nell'affrontare gli attacchi dello stato. Una perdita, intesa in questo contesto, rappresenta il rifiuto di una persona di commerciare con quella moneta.

Titolo originale: Social Network Principle

Indice

Principio del Sistema Bancario di Stato

Non esiste un vero e proprio prestatore di ultima istanza nell'ambito del *free banking*, esso implica solamente un altro prestatore soggetto al vincolo dimostrato ne la Fallacia della Creazione dal Nulla. Tuttavia nel sistema bancario di stato questo ruolo è attribuito alla banca centrale con il supporto (n.d.t. consapevole?) dei contribuenti. Lo stato raccoglie le tasse per fornire prestiti a tasso scontato alle banche associate e al tesoro dello stato. Il prestito deve presentare uno sconto rispetto al tasso di mercato altrimenti non costituirebbe un prestito di ultima istanza. Le banche hanno sempre l'opzione di prendere a prestito il denaro da altre banche o da potenziali depositari. La tassazione è necessaria per sostenere lo sconto applicato. Per questa ragione, se il tasso di interesse naturale del mercato è pari al 10%, lo stato può imprestare denaro alle banche associate al 3% e coprire la differenza con le tasse.

Lo stato ha molteplici fonti di introito da tassazione, ma tipicamente le banche centrali sussidiano i tassi di prestito scontati attraverso il signoraggio. E' noto che le banche centrali dichiarino di non "stampare moneta" ma questo è esattamente ciò che fanno. La *Federal Reserve* degli Stati Uniti (la "Fed") ha il potere di ordinare nuova moneta all'Ufficio del Tesoro di Incisione e Stampa degli Stati Uniti. La Fed paga il costo di stampa della "carta" (in realtà della tela) ed il valore nominale per la moneta metallica. Il Tesoro è solamente un appaltatore che svolge il lavoro. Tipicamente la moneta metallica è prodotta in modo da possedere un valore nominale leggermente superiore al valore d'uso in modo da prevenirne la scomparsa dal mercato. Questo valore d'uso deve essere quindi ridotto quando il valore nominale si riduce rispetto ad esso, come risultato della svalutazione della corrispondente moneta fiat.

Questo implica che l'inflazione monetaria della moneta fiat di stato è letteralmente la conseguenza dello stampare la moneta di "carta". Questo processo viene mantenuto in qualche modo nascosto. La Fed, in prima istanza, non stampa la moneta, poi la mette in un caveau, e poi la impresta all'esterno. Questo sarebbe inutile. L'ordine delle operazioni è sostanzialmente invertito. La Fed emette dei prestiti a tasso agevolato con la *pretesa* che nel suo caveau sia presente la moneta

corrispondente. Il processo di *settlment* stabilito dalla Fed tiene traccia di quanta moneta è detenuta nella riserva di ciascuna banca associata. La maggior parte dei *settlement* può essere spesso compensata, ma periodicamente la moneta deve essere fisicamente spostata.

Per ridurre ulteriormente i costi di trasporto viene richiesto che una porzione significativa delle riserve delle banche associate sia detenuta presso lo stesso caveau della Fed. Questo può essere ottenuto attraverso l'acquisto di Titoli del Tesoro (*Treasury*) messi in vendita dalla Fed. Questi sono sostituti monetari considerati adeguati per soddisfare i requisiti di riserva richiesti alle banche associate. I *Treasury* rappresentano del debito emesso dal Tesoro degli Stati Uniti e generalmente acquistato in grande quantità sul mercato aperto dalla Fed. La Fed riduce lo *yeld* dei *Treasury* (i.e. il tasso di interesse pagato dallo stato) fornendo una domanda aumentata. Essa finanzia queste operazione essenzialmente nella stessa maniera con la quale emette i prestiti agevolati alle sue banche associate. La distinzione sta semplicemente nel fatto che questi acquisti rappresentano dei prestiti agevolati allo stato.

La Fed può *fingere* di avere il denaro nel suo caveau e stampare quando ciò viene richiesto dal *settlement*. Questo fatto crea l'illusione che l'inflazione monetaria sia il risultato dall'imprestare il denaro. Ma in verità ciò è dovuto interamente alla capacità della Fed di acquistare moneta a sconto per poi finanziare i prestiti. Quando una banca associata necessita di moneta essa la può acquistare dalla Fed utilizzando i Treasury. Quando la riserva di moneta corrente della Fed non è sufficiente, essa esegue semplicemente un "prelievo" dai contribuenti ordinando nuova moneta dalla stampante.

La Fed paga al Tesoro i seguenti importi per i "tagli di banconote" del dollaro:

Denominazione	Prezzo
1$	5.5 centesimi
2$	5.5 centesimi
5$	11.4 centesimi
10$	11.1 centesimi
20$	11.5 centesimi
50$	11.5 centesimi
100$	14.2 centesimi

Se stampare una banconota da 1$ avesse avuto un costo di 5.5 centesimi nel 1915, oggi avrebbe un costo di 1.40$. Quando il costo di stampare una banconota raggiunge il suo valore nominale essa è passata dall'essere una moneta fiat ad essere una moneta commodity. A questo punto il suo valore di signoraggio è pari a zero. Al continuare della svalutazione la denominazione deve essere quindi interrotta. L'analisi delle banche centrali coinvolte nell'iperinflazione è informativa in quanto le banconote raggiungono il loro costo di stampa in un periodo di tempo molto più breve e le monete tendono a scomparire del

tutto. L'emissione di banconote aventi denominazione più grande permette alla moneta di rimanere fiat mentre la moneta merce viene abbandonata. Il Dollaro dello Zimbabwe ha raggiunto con una banconota la denominazione di 100'000'000'000'000 (n.d.t. centomila miliardi) di unità prima di essere totalmente abbandonata in favore delle valute straniere.

Senza la capacità di creare moneta fiat, la Fed non potrebbe effettuare il *settlement* nei conti correnti; così come qualsiasi altra banca, se essa non disponesse di riserva sufficiente (inclusa quella che potrebbe essere presa a prestito) per coprire i prelievi, dovrebbe dichiarare fallimento. Finché una banca associata non ha necessita di effettuare *settlement* con moneta effettiva, come nel caso dei prelievi agli ATM o agli sportelli fisici, o con le banche non associate o altre istituzioni, non vi è necessità di muovere la moneta corrente, o di stamparla. Tuttavia, senza la capacità di stampare moneta a costo più basso la Fed sarebbe soggetta a fallimento come qualsiasi altra banca.

La quantità totale di Dollari Statunitensi in circolazione viene indicata con la sigla "M0". Questa include tutta la moneta tangibile ("liquidità contante") in aggiunta ai saldi dei conti presso la Federal Reserve. Queste due forme di denaro sono considerati obbligazioni intercambiabili della Fed. Le obbligazioni intangibili sono moneta che viene conteggiata ma che non è ancora stata stampata.

Quando l'attività di presa in prestito da parte delle banche associate viene ridotta, ovvero quando la Fed alza i propri tassi di interesse, le "obbligazioni" della Fed (la moneta) possono essere distrutte con l'effetto opposto della stampa. Quando la Fed ha contratto M0 di quasi il 20% in quattro anni a partire dal suo picco nel 2015, ciò ha rappresentato un costo sulle entrate fiscali. La Fed, infatti, si dipinge come un'organizzazione no profit, ma il guadagno netto derivato dai suoi prestiti viene versato al Tesoro degli Stati Uniti con cadenza annuale.

> La Federal Reserve ha incrementato il target del tasso di interesse dei fondi federali di sette volte tra Dicembre 2015 a Giugno 2018. Questo ha impatto sull'andamento del disavanzo federale e sul debito federale in due modi
>
> - Direttamente attraverso i pagamenti degli interessi netti
> - Indirettamente attraverso le rimesse annuali dalla Fed verso il Dipartimento del Tesoro degli Stati Uniti
>
> Le rimesse annuali al tesoro sono essenzialmente la rimanenza degli introiti della Fed al netto delle spese operative. Per legge, questo gettito addizionale deve essere girato al Tesoro.
>
> Il ricavo mandato al Tesoro ha avuto il picco di 97.7 miliardi di $ nel 2015 ed è costantemente calato da allora. Nel mese di Gennaio la Fed ha inviato al Tesoro 80.2 miliardi di $.

Questa "rimanenza dei ricavi della Fed" è ciò che viene guadagnato, al netto delle spese operative, dai prestiti di denaro stampato dal Tesoro degli Stati Uniti a costo nominale, e garantito dalla sua protezione di monopolio. Così il il risultato

netto di queste operazioni è che il Tesoro stampa nuova moneta e poi la riprende indietro sotto forma di interesse della moneta stampata. Come mostrato sopra, il Tesoro prende anche a prestito moneta a tasso scontato indirettamente finanziato dalla Fed attraverso l'emissione di titoli del Tesoro. **Benché la moneta non sia fisicamente stampata e poi depositata direttamente al Tesoro, il risultato è lo stesso**.

La moneta di monopolio di stato non è creata *ex nihilo* da operazioni bancarie fraudolente. E' letteralmente creata dalla "tela dei vecchi jeans" dallo stato.

La transizione ad un moderna "società senza contante" implica che le banche centrali mantengano la forma esistente di contabilità per la moneta non ancora stampata e che eseguano tutti i *settlement* internamente. Questo elimina i costi di stampa e di trasporto dovuti al *settlement* e garantisce piena capacità di censurare le transazioni della moneta. Un esempio di *Fedcoin*, come la e-Krona in fase sperimentale, richiederebbe alle persone di transare per mezzo della moneta di stato in forma elettronica. Bitcoin serve lo stesso scopo ma senza il controllo dello stato sull'attività di emissione o di conferma delle transazioni. Per queste ragioni non ci si può attendere che Bitcoin diventi una valuta di riserva per il sistema bancario di stato in quanto seguirebbe lo stesso percorso fallimentare del *gold standard*. La *value porposition* di Bitcoin si basa sul non utilizzare la moneta di stato.

Titolo originale: State Banking Principle

Indice

Principio di Sostituzione

Un bene succedaneo è un bene che può essere utilizzato al posto di un altro. Quando il prezzo di un prodotto cresce, ad un certo punto le persone si muovono verso dei beni sostituti o cessano del tutto l'uso del primo bene.

Mentre un bene succedaneo avente lo stesso prezzo del prodotto originale potrebbe essere meno desiderabile, il suo prezzo più basso compensa questa preferenza. In questo modo la presenza dei beni succedanei riduce la domanda del bene originale. I sostituti competono con l'originale nello stesso modo di un incremento di offerta del bene originale.

Data una moneta con una offerta fissa, viene comunemente assunto che nessun incremento dal lato dell'offerta possa ridurre la pressione all'incremento del prezzo. Tuttavia, come mostrato ne la Proprietà di Stabilità, Bitcoin incorpora delle *fee* di transazione che aumentano necessariamente con l'uso. Questa caratteristica, unica nel suo genere, crea una pressione di riduzione del prezzo attraverso una riduzione della domanda. **L'aumento di costo rende i beni sostituti un'opzione percorribile, creando una pressione alla diminuzione del prezzo attraverso un aumento effettivo dell'offerta**.

Non vi è nulla che possa impedire tale evoluzione in molte monete simili. E' possibile che esse esibiscano proprietà monetarie praticamente indistinguibili, minimizzando il *trade-off* della loro sostituzione. Come mostrato ne il Principio di Consolidamento, vi è sempre una pressione verso una singola moneta in quanto essa elimina i costi di scambio. Tuttavia, questa pressione contrasta con i costi crescenti e, ad un certo livello d'uso, essa deve lasciare il posto alla sostituzione (o all'abbandono).

Vi è una teoria secondo la quale, poiché la creazione di una moneta non costa nulla, il principio di sostituzione implichi che Bitcoin debba diventare senza valore a causa della sua illimitata offerta gratuita. Questa teoria ignora il fatto che Bitcoin richieda che le persone paghino per usarlo. Questo è valido per una seconda moneta così come lo è per la prima. Tuttavia l'aumento di offerta riduce la domanda. Ad un certo punto la domanda non è sufficiente per produrre/proteggere un ulteriore quantitativo di offerta e per ciò la teoria è invalida. Questa è la stessa relazione che vale per la monete commodity e, di fatto, per ogni prodotto.

Titolo originale: Substitution Priciple

Indice

Principi della Criptodinamica

Criptodinamica è un termine definito in questa raccolta con lo scopo di riferirsi facilmente ai principi fondamentali di Bitcoin. Ciò è fatto con l'intento sia di aiutare nella comprensione di Bitcoin sia di differenziarlo da altre tecnologie. Questi principi rappresentano il sottoinsieme minimo di principi *criptoeconomici* necessari per raggiungere questo obiettivo.

Benché la scelta del nome non sia essenziale, il razionale sottostante viene sviluppato di seguito.

Cripto

"Una criptovaluta è una moneta che impiega crittografia robusta per proteggere transazioni finanziarie, controllare la creazione di unità addizionali, e verificare il trasferimento [di unità]." - Wikipedia

Dinamica

"La dinamica è quella branca della matematica applicata [...] che si occupa dello studio delle forze [...] e del loro effetto sul moto." - Wikipedia

Cripto + Dinamica

Criptodinamica è l'insieme delle forze che proteggono le transazioni Bitcoin controllando (1) la definizione delle unità, e (2) il trasferimento delle unità.

Principi

La forza della sicurezza è interamente umana in natura. Le personedevono agire per proteggere qualsiasi cosa, incluso Bitcoin. Vista come sistema economico, la sicurezza di Bitcoin prevede che le persone agiscano in una maniera economicamente razionale (proprio interesse). Come tale, le forze di sicurezza di Bitcoin

sono basate interamente sulle azioni di singoli individui a tutela del proprio interesse, specificamente:

- Condivisione del Rischio
- Dissipazione di Energia
- Bilanciamento del Potere

Tali forze dipendono, in quest'ordine, l'una dall'altra. Senza condivisione dei rischi, l'energia non può essere spesa nel sistema per bilanciare il potere di un'entità censurante. Se queste tre forze rimangono integre Bitcoin può essere protetto. In mancanza di una sola di esse una tecnologia non può essere definita Bitcoin.

Data l'esistenza di queste tre forze, non si può assumere che una implementazione di Bitcoin possa essere protetta in senso assoluto. Inoltre, una implementazione potrebbe essere più sicura di un'altra. **L'unico criterio di distinzione è quello secondo il quale una tecnologia è Bitcoin se include queste forze, mentre non è Bitcoin se non le include**.

La possibilità di protezione permessa da queste forze si definisce "sicurezza criptodinamica". Così, ad esempio, una "blockchain *permissioned*" viola il principio di condivisione dei rischi, una tecnologia basata strettamente su proof-of-stake (PoS) viola il principio di dissipazione dell'energia e una moneta che si affida interamente alla componente di sussidio per ricompensare la conferma delle transazioni viola il principio di bilanciamento del potere. Nessuno di questi esempi e criptodinamicamente sicuro.

Titolo originale: Cryptodynamic Principles

Indice

Proprietà di Resistenza alla Censura

La resistenza alla censura è una conseguenza delle *fee* di transazione. L'applicazione della censura è di fatto indistinguibile dall'applicazione di un *soft fork*, dove la maggioranza dell'*hash power* rifiuta i blocchi che non applicano la censura. Senza questo tipo di azione le transazioni sono confermate su base economica razionale, a dispetto della soggettività individuale del singolo miner.

Un miner avente la maggioranza è finanziariamente profittevole. Per questa ragione non sopporta un costo nell'acquisire i mezzi per porre in atto la censura. Poiché il mining è necessariamente una attività anonima, è sempre possibile per ogni potenziale soggetto acquisire e sviluppare la maggioranza dell'*hash power* e controllarla ad ogni istante. Come mostrato ne la Fallacia della Proof of Work, gli *hard fork* non possono essere usati per sconfiggere selettivamente la forza censurante ma, al contrario, accelerano il collasso della moneta.

Nel caso di una censura attiva, le *fee* delle transazioni che non vengono confermate possono essere aumentate. Questo premio sulle *fee* va a creare un maggiore profitto potenziale per i miner che confermano le transazioni censurate. Se portata ad un livello sufficiente, questa opportunità produce una competizione addizionale e quindi un incremento complessivo di *hash rate*.

Se il crescente *hash power* di tipo non censurante eccede quello del censore, il controllo di quest'ultimo fallisce. Il censore si trova quindi di fronte alla scelta di sussidiare le operazioni o di abbandonarle. Solo lo stato può sussidiare perpetuamente le operazioni in quanto può imporre la tassazione e ottenere un guadagno dalla preservazione del suo stesso regime monetario. **Lo stato deve consumare un quantitativo di tasse almeno pari al livello del premio delle *fee* per mantenere il controllo della censura**.

Una moneta senza *fee* integrate ricadrebbe sotto il controllo di un censore o evolverebbe in un mercato parallelo delle *fee*. Come mostrato ne la Fallacia delle *Fee* a Parte non è necessario che le commissioni siano integrate nel protocollo, tuttavia l'integrazione delle stesse rappresenta una importante tecnica di anonimizzazione. In ogni caso, la resistenza alla censura deriva unicamente dal premio

sulle *fee*. La parte di sussidio della ricompensa del blocco non contribuisce alla resistenza alla censura in quanto il censore guadagna lo stesso sussidio degli altri miner.

E' possibile che l'applicazione della censura posso portare ad un collasso del prezzo, causando una perdita alle operazioni del censore. Tuttavia, in questo caso, il suo obiettivo è stato raggiunto, non lasciando alcuna opportunità all'economia di contrapporsi al censore. Questo collasso può essere ottenuto ad un costo irrisorio semplicemente dimostrando l'intenzione di porre in essere la censura. E' anche possibile che un *soft fork* creato per applicare la censura possa portare ad un aumento del prezzo, in quanto le attività del mercato legale si associano a tale misura dello stato. Cionondimeno, affinché la moneta sopravviva, la sua economia deve continuare a generare un premio in termini di *fee* sufficiente a sopraffare il censore.

Non può essere dimostrato che l'economia sia in grado di generare un livello di *fee* sufficiente a sopraffare il censore. In maniera simile, non può essere dimostrato che il censore sia disponibile e capace di sussidiare le proprie operazioni ad ogni livello. Non è quindi possibile dimostrare la resistenza alla censura. Questo è il motivo per cui la resistenza al controllo dello stato è assiomatica.

Titolo originale: Censorship Resistance Property

Indice

Proprietà del Consenso

Generalmente le persone pensano al consenso nel contesto di una appartenenza fissata, come ad esempio a quella di una giuria. In questo modello il consenso implica che tutti i suoi membri siano obbligati a concordare. Ma poiché l'appartenenza a Bitcoin (n.d.t. il suo utilizzo) non necessita di permesso e non è quindi fissata, vi è sempre completo accordo tra i suoi membri, per come implicato da questa definizione di appartenenza. In questo modello il consenso si riferisce alla dimensione dell'appartenenza (l'economia) non ad una condizione dell'accordo.

Un consenso può frammentarsi o consolidarsi. Generalmente un consenso più esteso porta ad una maggiore utilità e ad una maggiore sicurezza data da una maggiore condivisione del rischio.

Titolo originale: Consensus Property

Indice

Proprietà di Stabilità

Il valore è un'entità soggettiva e di conseguenza i prezzi costanti rappresentano una finzione economica. I prezzi di scambio di una moneta sono determinati dalla sua domanda e offerta che, a sua volta, dipende dalla curva domanda di tutte le persone per tutti i prodotti. La stabilità di una moneta non è la tendenza verso un prezzo costante di tutti gli altri beni ma è una relazione di smorzamento tra la domanda di moneta e la sua offerta.

E' possibile classificare le monete in tre categorie di offerta:

- Offerta di Mercato (commodity - moneta merce)
- Offerta di Monopolio (monopolio)
- Offerta fissa (bitcoin)

In ogni moneta, la distruzione di unità diminuisce l'offerta e di conseguenza incrementa il valore delle unità rimanenti. Assumendo che non vi sia incentivo economico nella distruzione di unità, ciò non impatta la stabilità.

L'offerta di una moneta merce aumenta grazie all'incentivo finanziario di produrne in quantità maggiore quando ci si attende che il suo prezzo sia pari o superiore al prezzo di produzione (inclusivo del costo del capitale). Questa relazione tra prezzo e offerta è prevedibile nonostante il prezzo (e quindi l'offerta) non lo sia. Poiché il prezzo non è prevedibile, questo tipo di inflazione monetaria non può essere capitalizzato. Di conseguenza tutti i possessori della moneta soffrono di una riduzione del valore dato dall'incremento di offerta. La competizione garantisce che questa produzione, finanziata dai possessori esistenti, è limitata dal prezzo corrente. La retroazione data dalla diminuzione di valore dovuta all'aumento di offerta riduce l'incentivo a produrre, creando quindi stabilità.

L'offerta di una moneta di monopolio viene incrementata arbitrariamente (quindi tassata sotto forma di *demurrage*) dal "sovrano" in ragione della ricompensa finanziaria derivante dal signoraggio. Quando questa inflazione monetaria diventa prevedibile essa può essere capitalizzata, andando a scontare il ritorno sul signoraggio. Per questa ragione i cambiamenti nell'offerta non vengono spesso pubblicati. A causa della protezione di monopolio di stato (i.e. la produzione non autorizzata rappresenta il crimine di contraffazione), la competizione non può effettivamente limitare i rendimenti. Il profitto (la tassa) del sovrano è la

ricompensa del signoraggio ed è la ragion d'essere della moneta di monopolio. La protezione di monopolio è la sola distinzione economica tra la moneta merce e la moneta di monopolio. L'incremento di offerta causato dal signoraggio è mitigato solamente dall'instabilità politica dovuta alle persone che resistono alla conseguente diminuzione del valore. Questa tensione si manifesta inizialmente attraverso la fuga di capitali che viene contrastata con il controllo del cambio estero.

L'offerta di Bitcoin è indipendente dal prezzo. Poiché il sussidio è una quantità prevedibile, esso viene capitalizzato e non ha effetto sul prezzo nel corso del tempo. Il suo scopo è quello di distribuire razionalmente le unità e viene quindi poi progressivamente eliminato. Poiché le *fee* crescono necessariamente con la domanda, la soglia di utilità va ad eliminare la domanda di transazioni aventi valore al di sotto di tale soglia. Più in generale, il livello delle *fee* cresce al punto in cui i sostituti monetari sono più economici per una dato valore della transazione. **Quindi la stabilità deriva dal limitare direttamente la domanda al posto di affidarsi ad un incremento di offerta per ottenerla**. La stabilità implica che il prezzo venga limitato, ma esso può salire all'aumentare della capacità di sostenere più transazioni da parte della moneta e con un incremento di utilità rispetto ai sostituti.

Titolo originale: Stability Property

Indice

Proprietà della Soglia di Utilità

L'utilità viene espressa come la preferenza di una moneta rispetto ai sostituti (n.d.t. monetari) per trasferimenti di valore confrontabile. Un'utilità più elevata implica un livello di *fee* più elevato, sotto l'ipotesi che vi sia un più elevato volume di transazioni. La competizione per la conferma porta ad aumentare le *fee*. Poiché nel corso del tempo si assiste a delle differenze nel mercato del prezzo delle *fee*, un individuo può offrire una *fee* non competitiva nell'aspettativa di attendere un tempo più lungo per ottenere la conferma della sua transazione. Altri individui non transeranno sulla catena affidandosi invece ai sostituti monetari.

La più elevata utilità, quindi, implica l'aumento del valore medio transato in quanto le *fee* crescenti porterebbero il costo del trasferimento ad eccedere il valore trasferito. Una maggiore profondità (n.d.t. delle transazioni "sepolte" dentro la catena) implica una maggiore sicurezza della conferma. Di conseguenza è possibile scambiare del tempo in cambio di una *maggiore* sicurezza contro la doppia spesa. Tuttavia, il tempo non può essere ridotto al di sotto del periodo di un blocco al fine di ottenere la più *bassa* sicurezza possibile. I più bassi livelli di sicurezza sono rispettivamente: nessuna sicurezza (come transazione non confermata) e sicurezza minima (una conferma). Non può essere effettuato nessuno scambio tra questi due livelli.

Fee più elevate implicano un *hash rate* più elevato, cosa che mitiga la necessita di aumentare la profondità di conferma per valori di trasferimento più elevati. **Poiché non vi è modo di ridurre la sicurezza per valori di trasferimento più piccoli, il più piccolo valore di trasferimento utile cresce assieme all'utilità**. Il mancato supporto ai trasferimenti in un certo intervallo di valori implica che i sostituti sono meno cari in quell'intervallo di valori. Questo implica la possibilità che coesistano differenti monete al fine di servire distinti intervalli di valore. Tuttavia tutti i tipi di Bitcoin (n.d.t intesi come sistemi di protocollo monetario analoghi - inclusivi dei più celebri fork) possiedono intrinsecamente questa proprietà.

Differenze nelle regole in termini di periodo o dimensione dei blocchi non cambiano questa relazione. L'effetto di queste variazioni tra monete è strettamente

proporzionale. Anche un sistema con blocchi di dimensione illimitata deve produrre dei livelli di *fee* che portano fuori mercato i trasferimenti di basso valore.

Titolo originale: Utility Threshold Property

Indice

Proprietà del Gioco a Somma Zero

Il mining di Bitcoin è un gioco a somma zero. In media la catena cresce di un blocco ogni 10 minuti, dove il totale della ricompensa viene controllato dal miner che lo ha trovato. Tenendo da parte la pressioni al raggruppamento (pooling), i miner competono per ottenere la ricompensa e ciascuno totalizzerà, in media, una ricompensa proporzionale al suo *hash power*. Per un miner la differenza tra il costo e la ricompensa nel tempo rappresenta il suo tasso di rendimento (ritorno) sul capitale investito nel suo centro di mining.

Vi sono due aspetti da considerare nella proprietà del gioco a somma zero:

- Nell'intervallo di tempo compreso tra due organizzazioni, un miner guadagna una ricompensa e tutti gli altri miner non ne guadagnano nessuna. Né il prezzo, né *l'hash rate*, né la difficoltà, né l'inflazione, né le *fee*, o qualsiasi altro fattore ha alcun effetto su questa proprietà.
- L'entità della ricompensa, misurata in unità della moneta (n.d.t. minata) o nel prezzo di scambio, non ha effetto sul tasso di rendimento del capitale. (n.d.t. si vedano i capitoli Modello di Business del Miner e Fallacia della Preferenza Temporale per una spiegazione dettagliata sul perché - cosa assolutamente non scontata - il tasso di rendimento (i.e. il tasso di interesse) derivi dalla preferenza temporale delle persone ed influenzi tutte le attività di produzione, non solo del mining)

Visto in maniera *idealizzata* il mining di Bitcoin è un sistema chiuso. Il ritorno sul capitale varia relativamente ad altri centri di mining ed è dovuto ai difetti del protocollo quali il premio di prossimità e lo sconto di varianza, così come alle economie di scala e all'efficienza degli operatori. Tuttavia, poiché questi fattori impattano sul costo relativo dell'*hash power*, è la proporzionalità dei tassi di rendimento ad essere influenzata, non il rendimento globale.

Il Bitcoin *nella realtà* non è un sistema chiuso. Le pressioni all'aggregazione a mercato e anti-mercato dovute rispettivamente alla variazione (dei costi di mining) e alla distorsione sono di tipo esterno. A livello fondamentale, Bitcoin

esiste per difendere i mercati mettendo necessariamente in conflitto la distorsione con la variazione (o con la sua mancanza).

Quando la distorsione è applicata ad un miner in questo gioco a somma zero, tutti gli altri miner ne sono affetti. Per esempio, un sussidio (da non confondersi con la componente di sussidio prevista dal consenso) dato ad un miner agisce come una tassa su tutti gli altri e, viceversa, una tassa su un miner agisce come un sussidio su tutti gli altri. Il miner sussidiato opera ad un costo più basso per lo stesso *hash rate*, oppure ha un maggiore *hash rate* effettivo per lo stesso costo. Il miner tassato opera ad un costo più elevato per lo stesso *hash rate*, oppure possiede un *hash rate* più basso allo stesso costo.

Un'entità che eroga sussidi non si attende alcun ritorno del capitale, altrimenti essa sarebbe considerata un investitore. L'investimento è una forza di mercato attraverso la quale un miner paga un prezzo di mercato per il capitale. Con un tasso di rendimento effettivo più elevato il miner sussidiato attrae più capitale degli altri miner, continuando ad espandere l'*hash power* finché non rimane un unico miner. L'obiettivo dell'entità sussidiante è, in ultima istanza, quello di controllare il centro di mining sussidiato.

Una tassa sul mining ha l'effetto di muovere tutto l'*hash power* verso i centri di mining non tassati, al di fuori della giurisdizione dell'autorità tassante, come conseguenza della necessità per il capitale di trovare rendimenti a mercato. Se applicata in maniera estesa, questa tassa può portare il controllo dell'autorità sulle sue stesse operazioni di mining. In altre parole, l'autorità può sopprimere la competizione. Questo obiettivo può essere raggiunto anche attraverso una tassa del 100% per la quale l'autorità coopta i centri di mining. L'effetto è lo stesso, il centro di mining tassato viene fatto fallire ed i ricavi della tassa vengono utilizzati per le attività di controllo.

Le conseguenze del gioco a somma zero nel mining combinate con l'intrinseca pressione al raggruppamento (pooling) vengono approfondite ne il Paradosso del Livello di Minaccia.

Titolo originale: Zero Sum Property

Indice

Paradosso del Livello di Minaccia

Come implicato dalla Proprietà del Gioco a Somma Zero, presumibilmente, l'unico modo per sconfiggere un incentivo esterno è quello di minare in perdita rispetto al ritorno a mercato sul capitale. In maniera simile, sembra che l'unico modo per sconfiggere una tassa, compresa una tassa del 100% (un divieto), sia quello di minare al di fuori della giurisdizione dell'autorità tassante, ad esempio in segreto. Come in tutti i mercati neri vi è un costo maggiore nel condurre un mining di tipo sovversivo. Competere contro un mining sussidiato ne aggrava il costo.

Accettando l'assioma di resistenza, è necessario assumere che sia la tassazione sia gli incentivi saranno usati per ridurre il costo del controllo di Bitcoin. Usando il potere di incentivare il mining (con il gettito fiscale), gli stati possono indurre il fenomeno del raggruppamento nella regione dove viene applicato l'incentivo. Una volta che la maggioranza dell'*hash power* è stata raggruppata, lo stato può usare il suo potere di tassazione (regolatorio) sulla regione per applicare la censura.

Quindi per godere dei benefici di una moneta robusta, sembrerebbe che le persone siano sostanzialmente costrette a minare in perdita. Tuttavia la censura crea l'opportunità per altri soggetti di minare in maniera profittevole nella misura in cui le persone (n.d.t. che utilizzano Bitcoin) siano intenzionate a compensare tale costo con le *fee*. Questo mercato nero è l'applicazione della resistenza alla censura in Bitcoin. Le persone pagano un prezzo più elevato per certe transazioni, e, al fine di mantenere quel prezzo elevato, lo stato deve subire allo stesso modo delle spese a discapito della loro inefficacia.

Paradossalmente, questo tipo di strumento funziona bene quando la moneta è sotto attacco mentre funziona poco bene in altre situazioni. Se non vi fosse pressione al raggruppamento interna queste situazioni si bilancerebbero reciprocamente. Tuttavia la distribuzione dei rischi è essenziale per il mining sovversivo e la pressione al raggruppamento lavora *contro* tale distribuzione. Quindi vi è una superficie di attacco in continua espansione senza che vi sia alcuna pressione alla sua contrazione, a meno che delle efficaci alternative monetarie non siano già state soppresse. La soppressione delle alternative

aumenta l'utilità della ricompensa al miner nella regione dove ha luogo tale azione coercitiva. Il Paradosso si applica anche alle pressioni alla centralizzazione.

La conseguenza attesa di questo fenomeno è che Bitcoin non sarà ben *preparato* agli attacchi in quanto la preparazione delle difese è finanziariamente svantaggiosa per le persone che vivono in un ambiente caratterizzato da un basso livello di minaccia.

Titolo originale:

Indice

Modello di Business del Miner

I miner conducono un gioco a somma zero all'interno di una economia a somma positiva. Essi competono tra di loro, non con l'economia. L'utilità crescente riflette una somma positiva che è una conseguenza naturale dello scambio commerciale.

E' stato affermato che i blocchi minati in un periodo di prezzi crescenti produca dei ritorni estremamente elevati per i miner, almeno fino a quando non avviene l'aggiustamento. Questa idea è basata sulla diffusa incapacità di comprendere che i prezzi di mercato non sono prevedibili. Le scommesse sul cambiamento di prezzo sono speculative per natura. Non vi è ragione di presumere che la *speculazione* su Bitcoin sia più o meno efficace di qualsiasi altro tipo di speculazione. Tuttavia se un aumento di prezzo fosse stato prevedibile allora l'allocazione di capitale avrebbe riflesso tale circostanza allo stesso modo, quindi cancellando la possibilità di ritorni elevati.

D'altra parte, l'*investimento* nel mining di Bitcoin è basato sulla relazione prevedibile tra il profitto e la competizione nel corso del tempo. Questa relazione predice che in media tutta l'attività di mining si avvicina al tasso di interesse di mercato. Come avviene in tutti i mercati, il prezzo è imprevedibile nel breve periodo, mentre nel lungo periodo si avvicina ai ritorni di mercato. Fondamentalmente, è la preferenza temporale a controllare il mercato dei tassi di ritorno sull'investimento.

Allora come fa un miner a conseguire dei ritorni elevati? Ciò non può essere ottenuto attraverso un accordo a parte sulle *fee*. Vi è solo un modo di conseguire tassi di ritorno più elevati del mercato, ed è quello di avere un costo dell'*hash power* relativo ad una moneta inferiore alla media. Questo obiettivo è raggiunto, sia traendo vantaggio dalla pressione al raggruppamento oppure attraverso una maggiore efficienza operativa. A causa della proprietà del gioco a somma zero, questi miner sono controbilanciati dai tassi di ritorno più bassi rispetto al mercato che ottengono gli altri miner. Di conseguenza per un miner onesto il premio diminuisce quando esso possiede più del 50% di *hash power* fino ad annullarsi quando esso ne possiede il 100%.

Tuttavia altri miner potrebbero ritirarsi dal business del mining in quanto il loro capitale andrebbe alla ricerca di ritorni a mercato. Questo lascerebbe un solo miner legato ai ritorni a mercato. In altre parole, conseguire ritorni più elevati del mercato richiede che vi sia qualcuno dal quale possano essere "catturati". Il più elevato ritorno che può essere sostenuto è funzione del più elevato costo opportunità che altri sono disponibili a sostenere. Questo è a sua volta funzione dell'utilità della ricompensa in termini differenziali così come discusso ne il Paradosso del Livello di Minaccia.

Limitando i dividendi ai tassi di ritorno a mercato e reinvestendo tutta la ricompensa rimanente, un miner può mantenere un *hash power* costante e quindi ottenere ritorni a mercato su una base proporzionale alla capitalizzazione di Bitcoin. I dispositivi di mining vengono liquidati spegnendoli ogni qual volta ciascuno di essi va in perdita netta oppure scontando i ritorni futuri attraverso la vendita del dispositivo stesso.

Il tasso di ritorno del miner sul capitale dipende solamente dalla preferenza temporale. La relazione tra l'economia ed i miner viene sviluppata ulteriormente ne la Fallacia del Bilanciamento dei Poteri.

Titolo originale: Miner Business Model

Indice

Modello di Sicurezza Qualitativo

Modello di Decentralizzazione

Ne il Principio del Social Network è stato mostrato come Bitcoin sia una rete di relazioni umane. Questa rete può essere modellizzata come un grafo diretto dove ogni vertice rappresenta un commerciante e ogni lato rappresenta uno scambio che coinvolge bitcoin. I lati indicano la direzione verso cui si muove la moneta e ne viene data quantificazione attraverso il numero di unità scambiate. Si presume che tutti i possessori siano stati commercianti quando la moneta è stata ricevuta, anche in qualità di miner (che vendono conferme) e come percettori di beneficenza (che vendono valore intangibile).

Se una persona non accetta personalmente la moneta o non valida di persona la moneta accettata, questa persona non può rigettare le moneta invalida (n.d.t. falsa). La persona in questione sta affidando questo compito ad una autorità centralizzata. Tutte le persone che usano la stessa entità delegata vengono ridotte al solo vertice che la rappresenta.

Per ciascun periodo di tempo la sicurezza economica è funzione del numero dei commercianti e della somiglianza degli importi transati. L'economia più forte verrebbe ottenuta se tutte le persone del mondo si scambiassero lo stesso quantitativo di unità in un determinato periodo, una situazione ideale che può essere chiamata un'economia "distribuita" (o completamente decentralizzata). L'economia più debole si avrebbe se una sola entità delegata accettasse tutte le unità in scambio in un determinato periodo, che risulterebbe essere una economia "centralizzata".

Più specificamente, il sistema più decentralizzato economicamente è quello che ha il maggior numero di vertici (i commercianti) con il più basso coefficiente di variazione relativo ai lati in arrivo (i pagamenti). Definendo una *funzione di distribuzione* come l'inverso del coefficiente di variazione otteniamo:

```
decentralizzazione-economica = distribuzione(pagamenti) * commercianti
```

In maniera simile alla sicurezza economica, la sicurezza delle conferme può essere modellizzata come un grafo nullo. Ciascun miner è rappresentato da un vertice sul grafo. Un operatore di un dispositivo di mining non è un miner in quanto egli non ha capacità di scelta e solamente il miner può essere quindi rappresentato. L'*hash power* totale impiegato da un miner costituisce il peso del vertice.

In ogni periodo di tempo la sicurezza delle conferme è funzione del numero di miner e della somiglianza dell'*hash power* che essi controllano. La più elevata resistenza alla censura verrebbe ottenuta se tutte le persone nel mondo minassero con lo stesso *hash power* in un dato periodo, una situazione ideale che può essere chiamata sistema di conferma "distribuito" (o completamente decentralizzato). Il sistema più debole sarebbe quello nel quale un solo miner controllasse il 100% dell'hash power che equivarrebbe ad un sistema "centralizzato" di conferma.

Più specificamente, il sistema più decentralizzato nella conferma è quello avente il maggior numero di vertici (miner) con la più alta distribuzione in peso (hash power):

```
decentralizzazione-nella-conferma = distribuzione(hash-powe) * miner
```

Modello di Sicurezza

La sola decentralizzazione non è sinonimo di sicurezza. **La sicurezza è il prodotto dell'attività (n.d.t. dell'azione umana), della distribuzione di tale attività e della frazione di umanità che vi partecipa.**

```
sicurezza = attività * distribuzione * partecipazione
```

Poiché non vi è limite al numero di esseri umani, al numero di scambi o al livello di computazione, il livello di sicurezza è illimitato in ciascun asse. La sicurezza è illimitata anche con una distribuzione perfetta (i.e. infinita decentralizzazione). Un livello minimo pari a zero viene raggiunto sia con nessuna partecipazione sia con nessuna attività. La sicurezza economica e della conferma possono essere quindi definite come:

```
sicrezza-economica = pagamenti * distribuzione(pagamenti) * [commercianti / umanità]
sicurezza-nella-conferma = hash-power * distribuzione(hash-power) * [miner / umanità]
```

Limiti del Modello

Queste relazioni non dicono nulla sulla assoluta efficacia rappresentata da ciascun valore, o sull'efficacia relativa di ciascuna coppia di valori, tranne per il fatto che un valore maggiore rappresenta una maggiore efficacia. Ciò non è dovuto ad una carenza nel modello. I fattori includono le persone, ed in maniera specifica l'efficacia della loro abilità individuale a resistere e la loro percezione del valore nella moneta. Tutti coloro che validano o che minano offrono un certo livello di resistenza ma non vi è sottintesa continuità. Ci si riferisce infatti ad un "livello" di sicurezza e non ad un "quantitativo" di sicurezza.

Come mostrato ne il Principio dei Dati Pubblici, l'anonimità è uno strumento che aiuta a difendere la possibilità di ciascuno di commerciare e/o minare. Come tale, il livello di decentralizzazione non può essere mai misurato; il modello rappresenta un aiuto a livello concettuale. Come mostrato nella Fallacia del Bilanciamento del Potere, la sicurezza che viene dedicata da ciascuno dei due sotto-gruppi è complementare ed indipendente da quella dell'altro. Mentre le persone possono decidere di commerciare e/o minare indipendentemente in futuro, la Fallacia dello Scarafaggio mostra che essi non stanno contribuendo alla sicurezza finché non lo fanno (n.d.t. in maniera attiva). Questo modello è rappresentativo della sicurezza finché essa è presente in un certo periodo tempo.

Titolo originale: Qualitative Security Model

Indice

Difetto del Premio di Prossimità

La latenza è il tempo richiesto per eseguire una comunicazione. L'informazione si muove ad una velocità non superiore alla velocità della luce e di conseguenza la latenza è un fattore che non può essere eliminato.

Le differenti distanze reciproche trai i miner implicano che gli annunci saranno noti ad alcuni più tardi rispetto ad altri. Quando un miner non è consapevole di un annuncio (n.d.t. non lo ha ricevuto) sta sprecando capitale lavorando su un candidato debole. Più tempo passa e più diventa esponenzialmente meno probabile che un miner sia ricompensato per tale blocco candidato. Quindi i miner competono per vedere gli annunci prima degli altri miner, in quanto ciò ne riduce il costo opportunità.

Se fossimo in condizione di disporre dei miner con pari *hash rate* a punti equidistanti intorno alla terra, essi sperimenterebbero lo stesso livello medio di latenza. Tuttavia, a causa dai benefici finanziari derivanti da una latenza ridotta, essi tenderebbero a spostarsi reciprocamente più vicino. Questa forza è la pressione al raggruppamento, e si manifesta in diversi modi.

La pressione al raggruppamento basata sulla prossimità è una conseguenza della struttura in sequenza della catena richiesta dalle regole di consenso. **Bitcoin stabilisce un ordine basato sul principio del "vincitore prende tutto" che produce un costo opportunità sproporzionato**. Lo sconto dovuto alla varianza è un altra pressione al raggruppamento causata dal consenso.

La difesa che Bitcoin *intende* sollevare è la difesa del mercato contro le forze anti-mercato. Per fare ciò è necessario distribuire hash power tra le persone in maniera diffusa in modo che esso sia difficile da cooptare. Tuttavia la pressione al raggruppamento intrinseca al consenso lavora contro questo obiettivo. Questo è il motivo per il quale questa caratteristica è definita un difetto.

Titolo originale: Proximity Premium Flaw

Indice

Difetto dello Sconto di Varianza

La varianza è la frequenza variabile con la quale viene ottenuta una ricompensa. La varianza è intrinseca alla natura probabilistica del mining e non può essere eliminata.

Per come è strutturato il consenso, differenti *hash power* tra i miner implicano che le ricompense verranno guadagnate da alcuni di essi con maggiore frequenza di altri. Con il 10% di *hash power* ci si aspetterebbe di essere ricompensati 10 volte più frequentemente di coloro che hanno l'1%, sebbene il fattore moltiplicativo sia in realtà più elevato a causa del premio di prossimità. Tuttavia, i risultati effettivi non sono predicibili e possono variare significativamente. Per la presente discussione è tuttavia sufficiente assumere in ambo i casi una relazione di proporzionalità. In questo esempio, un miner riceve una ricompensa ogni 100 minuti e l'altro ogni 1000 minuti. Assumendo la stessa ricompensa per ogni blocco, la grandezza della ricompensa è anch'essa proporzionale all'*hash power*.

Va considerato inoltre che un miner di piccole dimensione potrebbe dover attendere anni prima di ricevere una ricompensa. Nonostante un miner di dimensioni più piccole sia remunerato in maniera proporzionale egli deve affrontare questo difetto rispetto ad un miner di dimensioni maggiori. Egli può tuttavia migliorare il suo flusso di cassa ricevendo una frazione della ricompensa più frequentemente. Vi è anche la possibilità che un centro di mining non sia ben configurato e che non pervenga mai ad un risultato positivo. Per queste ragioni i miner sono portati a scontare la varianza elevata. I miner di dimensioni più piccole convertiranno i loro centri di mining in un insieme di singoli dispositivi di mining e pagheranno un miner aggregatore per ottenere una varianza ridotta. Questo è il fondamento logico che sta alla base di P2Pool ma poiché la riduzione di varianza ottenuta da questo sistema è meno efficiente, la pressione al raggruppamento rimane.

La pressione al raggruppamento basata sulla varianza è dovuta dell'unico livello di difficoltà della rete previsto dalle regole di consenso. **Nonostante possiedano un basso *hash power* , i piccoli miner devono competere ad una difficoltà più elevata che amplifica intrinsecamente la varianza**. Il

premio di prossimità rappresenta un'altra pressione al raggruppamento causata dal consenso.

La difesa che Bitcoin *intende* fornire è la difesa del mercato contro le forze anti-mercato. Per fare ciò è necessario distribuire l'*hash power* in maniera estesa tra le persone in modo che esso sia difficile da cooptare. Tuttavia la pressione al raggruppamento intrinseca al consenso lavora contro questo obiettivo. Questo è il motivo per il quale questa caratteristica è definita un difetto.

Titolo originale: Variance Discount Flaw

Indice

Rischio di Centralizzazione

La debolezza di Bitcoin deriva dalla centralizzazione e dal ragguppamento. Le forze che producono il mining in forma aggregata sono chiamate pressioni al raggruppamento. Mentre il raggruppamento indebolisce la sicurezza delle conferma, la centralizzazione indebolisce la sicurezza delle regole di consenso. La debolezza è dovuta al minor numero di persone con le quali condividere il rischio.

Il rischio del consenso è condiviso solo tra i commercianti attivi, in quanto essi sono le persone che hanno la possibilità di rifiutare uno scambio di proprietà con unità che non sono conformi alle loro regole. Le forze di natura finanziaria che riducono il numero di commercianti sono chiamate pressioni alla centralizzazione. Il problema della delega è che essa è di solito collegata alla centralizzazione, come avviene tipicamente nei *web wallet*. Il wallet non ha la sola funzione di detenere le unità risparmiate, ma tipicamente controlla anche la validazione delle unità ricevute in uno scambio. **L'ultima funzione riduce il potere sulle regole di consenso ad una sola persona per tutti i wallet ricompresi nel medesimo servizio**.

La pressione alla centralizzazione include:

- La difficoltà nell'applicare degli sconti ai valori di scambio.
- L'applicazione di sconti nel *settlement on-chain*.

Se uno scambio è difficile per un cliente, il commerciante deve scontare la merce in modo da accettare la moneta. Se lo scambio è difficile per il commerciante si incorre in un costo addizionale. Se per il pagamento ci si appoggia ad una terza parte fidata, essa porta a ridurre la dimensione dello sconto e/o del costo e di conseguenza il ritorno sul capitale (n.d.t del commerciante) viene aumentato.

Il trasferimento comporta delle *fee* che richiedono anch'esse lo sconto della merce da parte di un commerciante. Se viene impiegato un intermediario fidato per finalizzare i trasferimenti *off-chain* le *fee* vengono ridotte e conseguentemente viene ridotto lo sconto aumentando il ritorno sul capitale (n.d.t. del commerciante).

La centralizzazione di manifesta sotto forma di:

- Fornitori di servizi di pagamento.

- *Wallet di tipo web* e intermediari fiduciari.
- *Hosted API* per monitorare la catena.

In un ambiente a basso livello di minaccia il commerciante ha un ridotto incentivo finanziario a sussidiare la sicurezza di Bitcoin. Quando il costo delle alternative aumenta lo sconto diventa inevitabile. A quel punto, o il cliente decide di pagare un prezzo più elevato oppure il commerciante chiude la sua attività in quanto il suo capitale va alla ricerca di tassi di ritorno a livello di mercato.

Titolo originale: Centralization Risk

Indice

Rischio della Pressione al Raggruppamento

La pressione al raggruppamento è un insieme di incentivi di natura finanziaria volti all'aggregazione dell'*hash rate*, specificamente:

- Premio di Prossimità
- Sconto di Varianza
- Variazioni di Mercato
- Distorsioni di Mercato
- Economie di Scala

Nonostante la latenza e la varianza siano dei fattori inevitabili, le regole di consenso *creano* effettivamente i primi due incentivi finanziari. La variazione è una conseguenza della variabilità dei prezzi di mercato delle risorse per il mining. La distorsione è una conseguenza della variabilità dei costi non a mercato che includono le tasse, la regolazione, il sussidio ed il brevetto; forze contro le quali Bitcoin è stato concepito per resistere. In un ambiente ad elevato livello di minaccia, le economie di scala potrebbero diventare negative a causa dei costi associati alla maggiore visibilità ma potrebbero essere altrimenti positive.

Ci sono numerose manifestazioni del fenomeno del raggruppamento. Una è di natura geografica, per la quale miner indipendenti si avvicinano fisicamente. Un'altra è di tipo cooperativo, per la quale dei miner, in precedenza indipendenti, uniscono le forze e installano nello stesso luogo i dispositivi di mining. Un'altra è di tipo virtuale, per la quale i miner diventano dei meri operatori di dispositivi di mining e aggregano il loro *hash rate* presso un singolo miner remoto. Un'altra manifestazione è data dall'esistenza dei propagatori, che aggregano l'*hash power* dei miner. Un'altra manifestazione ancora è data dal flusso di cassa in quanto il più elavato *hash rate* associato con il più elevato utilizzo di capitale rappresenta una forma di co-locazione.

Mantenendo una continua pressione al raggruppamento la selezione delle transazioni si ridurrà, alla fine, al controllo di una sola persona. E' possibile che ciò stia già avvenendo. Il rischio per Bitcoin è che una singola persona rappresenti la sola difesa della sua utilità, rendendo inevitabile il successo

nella cooptazione. Questo rischio non può essere mitigato all'intero dell'economia stessa.

La pressione all'aggregazione è l'equivalente in Bitcoin del Sistema della *Federal Reserve* degli Stati Uniti. Il sistema era stato progettato in modo da facilitare la tassazione attraverso la svalutazione di una moneta debole. Esso offriva il supporto dello stato ad una delega monetaria in cambio di moneta solida. Questa combinazione era disegnata per creare una *pressione* alla raccolta di moneta solida presso l'autorità centrale. Una volta che la raccolta fu sufficiente, lo stato eliminò del tutto il pretesto e sequestrò la rimanente moneta solida. Tutti gli stati hanno sistemi simili e cooperano per difenderli.

Questo fatto non implica che il mining vada contro Bitcoin. Seguendo la stessa analogia, il *free banking* non si oppone all'uso dell'oro. Il mining rappresenta una parte *necessaria* di Bitcoin. Il raggruppamento rappresenta un rischio a dispetto del fatto che la pressione che lo caratterizza non sia creata dai miner, ma dovuta ai difetti di Bitcoin stesso.

Titolo originale: Pooling Pressure Risk

Indice

Fallacia del Monopolio degli ASIC

Vi è una teoria secondo la quale il prezzo degli ASIC per minare Bitcoin sia controllato da un cartello di miner che creano uno sproporzionato vantaggio ai centri di mining partecipanti al cartello.

A livello economico non vi è differenza tra un cartello ed una singola organizzazione. A livello organizzativo, cambiare la dimensione di una società è un esito del libero mercato che è osservabile quando il capitale va alla ricerca di economie di scala ottimali. Se i partecipanti al cartello ricevono gli ASIC ad un prezzo che produce un ritorno sul capitale al di sotto del valore di mercato, ciò si configura come un sussidio tra i partecipanti. Lo stesso fenomeno si verifica per un prezzo che produce dei ritorni sul capitale al di sopra del livello di mercato, con il sussidio che opera nella direzione opposta. Per questa ragione, non vi è alcun vantaggio netto nell'applicare questo sconto tra i partecipanti.

La produzione è generalmente impostata ad un livello che mira a produrre il massimo tasso di ritorno sul capitale. L'unica maniera economicamente razionale per innalzare i prezzi è quella di limitare la produzione al di sotto di quel livello ottimo. Altrimenti i prezzi più alti si tradurrebbero in un inventario invenduto portando a ritorni netti più bassi. Questo significa che la produzione deve essere limitata dal cartello per aumentare il prezzo unitario per i non-membri.

Limitare la produzione lascia l'opportunità ad altri produttori di attrarre i clienti con una più bassa utilità marginale per il prodotto, in quanto questi clienti rimarrebbero altrimenti non serviti. Quindi, la competizione abbassa il prezzo finché il mercato non si equilibra. Un libero mercato ricerca il prezzo di equilibrio che produce un ritorno pari al ritorno sul capitale globale (n.d.t. presente in media negli altri mercati). Un prezzo corrente al di sopra di questo livello di prezzo incrementa la produzione mentre un livello al di sotto la diminuisce. E' la preferenza temporale a determinare il tasso di ritorno sul capitale.

A meno che la produzione non sia soggetta in maniera sproporzionata alle forze anti-mercato quali la tassazione o il sussidio (n.d.t. condizioni, ahinoi, quasi inevitabili dei nostri tempi) ciascuno può godere della stessa opportunità di

aumentare il capitale e competere nella produzione. Se ciò non avviene, significa che i ritorni su questa linea di attività sono compatibili con i ritorni medi di mercato. La tassazione ed il sussidio creano delle distorsioni a livello regionale ma non eliminano la competizione. **In altre parole, il prezzo di monopolio è solamente il prodotto dalla concessione del potere di monopolio da parte dello stato**.

Una teoria collegata alla precedente afferma che l'acquisto di ASIC da questo cartello porti ad incrementare il suo stesso *hash power*. Quest'ultima è invalida sulla base della spiegazione illustrata precedentemente sul prezzo di monopolio. Il capitale del produttore andrà sempre alla ricerca dello stesso ritorno in qualsiasi linea di business o di investimento. Non vi è alcuna ragione di credere che il ritorno sia sproporzionato relativamente ai soli ASIC.

Un'ulteriore teoria collegata afferma che l'algoritmo di *proof of work* di Bitcoin produce una pressione al raggruppamento come conseguenza del supposto fenomeno di cartellizzazione. Se le persone credono sinceramente che gli ASIC siano sovra-prezzati la risposta razionale è quella di raccogliere capitale e mettersi a produrre ASIC. Ma in ogni caso, solo le sole forze di mercato e anti-mercato controllano la produzione dei chip e come tale ciò non costituisce una pressione al raggruppamento basata sul protocollo.

Titolo originale: ASIC Monopoly Fallacy

Indice

Fallacia della Verificabilità

La solvibilità di un custode di Bitcoin non può essere verificata. Un custode è una persona che ha discrezione sia nella restituzione di un asset sia nell'emissione di un titolo che lo rappresenti. Se entrambe le operazioni di restituzione dell'asset e di emissione del titolo rappresentativo associato sono controllate da regole di consenso allora la relazione intrattenuta, in realtà, non è una relazione di custodia. Questa è la distinzione che si configura tra una riserva ed un *layer*. Un *layer* soggiace all'applicazione del protocollo (non ad una custodia) e di conseguenza non necessita di verifica.

La verifica della solvibilità richiede la prova di esistenza contemporanea (atomica) sia dell'intero quantitativo dell'asset detenuto dal custode sia dei titoli emessi a sua rappresentazione. In caso di una riserva nazionale di Bitcoin questo richiederebbe la prova completa di tutto il rappresentativo fiat (e.g. il titolo) emesso a valere sulla riserva sia la prova del quantitativo Bitcoin detenuto in riserva. Anche qualora il titolo rappresentativo venga emesso su una catena distinta di tipo pubblico il requisito di atomicità non risulta soddisfatto.

In alcuni casi risulterebbe sufficiente rinunciare al requisito di atomicità accettando la non correttezza del sistema sotto l'ipotesi che deviazioni materiali nel suo funzionamento verrebbero alla fine scoperte. Tuttavia nel caso del sistema bancario di stato non è sufficiente rivelare una deviazione. Storicamente non è stato difficile scoprire queste deviazioni. La difficoltà risiede (n.d.t. interamente) nel porre fine ad esse.

Titolo originale: Auditability Fallacy

Indice

Fallacia del Bilanciamento del Potere

In Bitcoin il potere è riposto nelle mani dei miner e dei commercianti. Tuttavia questi due poteri non sono "bilanciati" tra di loro, come in una sorta di sistema di controlli e contrappesi. Il potere dei miner è ortogonale a quello dei commercianti. I miner controllano la selezione delle transazioni, i commercianti ne controllano la validità e nessuno dei due può controllare l'altro. Non è una sorpresa infatti che nella descrizione e nell'implementazione originali questi ruoli fossero combinati assieme.

Il potere non è la stessa cosa dalla capacità di influenzare. I commercianti possono influenzare i miner non comprando il servizio da loro offerto. In maniera simile, i miner possono influenzare i commercianti non fornendo loro il servizio. Queste scelte si manifestano come separazioni e stalli. Tuttavia la natura del potere (spesso messa in pratica) è quella di poter ignorare l'influenza. Lo stato detiene il potere; può applicare la coercizione e la cooptazione ignorando al contempo le forze di influenza. I commercianti e i miner *assieme* hanno il potere di difendersi contro queste aggressioni, ma nessuno dei due può farlo senza il supporto dell'altra entità.

Il bilanciamento del *potere* in Bitcoin è tra gli individui e lo stato. Anche gli stessi stati creano dei sistemi che provano a isolare le loro monete dal controllo politico. Bitcoin non è differente in tale contesto avendo incorporato l'assioma di resistenza. Gli individui possono scegliere di essere sia miner sia commercianti. Con una distribuzione diffusa di queste attività diventa difficile per gli attori statali censurare questo mercato. **L'idea che i miner e i commercianti operino in posizioni contrapposte evidenzia l'incapacità di comprendere il modello di sicurezza di Bitcoin**.

I commercianti acquistano un servizio dai miner e come tale i due soggetti sono coinvolti in uno scambio. I commercianti acquistano dei servizi di mining che sono conformi alle loro regole in cambio di una *fee* soddisfacente. Essi sono liberi di separare la catena e a loro volta i miner sono liberi di non minare affatto o di non selezionare transazioni particolari per qualsiasi ragione essi ritengano opportuna. Lo scambio non è mai una attività di contrapposizione o di natura

asimmetrica, è un'attività volontaria e mutualmente soddisfacente dove tutte le tensioni vengono risolte nel prezzo.

Questa mancata comprensione del fenomeno porta le persone a credere che il mining può essere raggruppato in maniera centralizzata a patto che i commercianti non operino una validazione centralizzata, cosa che porterebbe l'economia a controllare il comportamento del mining, rendendo il sistema sicuro. Questa convinzione è scorretta ma sfortunatamente le persone stanno traendo queste conclusione errate a partire dagli eventi recenti. Una fallacia strettamente collegata a quest'ultima è la convinzione che un *fork* della *proof of work* da parte dei commercianti possa controllare il comportamento dei miner.

Titolo originale: Balance of Power Fallacy

Indice

Fallacia del Sottoprodotto nel Mining

Vi è una teoria secondo la quale, nella misura in cui il mining di Bitcoin possa consumare un necessario quanto altrimenti non commerciabile sottoprodotto della produzione (i.e. uno scarto), è implicata una riduzione nel consumo netto di energia. Gli esempi includono gas naturale e memoria computazionale inutilizzati.

Dato un nuovo mercato del sottoprodotto in questione, non avvantaggiarsi del suo ipotetico prezzo più basso rappresenta un costo opportunità per ciascun miner. La competizione per il sottoprodotto di scarto incrementa il suo prezzo, potenzialmente ad un livello tale per cui il costo opportunità viene eliminato. Temporaneamente questo rappresenta un'opportunità di profitto nel mining.

Il ridotto costo del mining deve portare necessariamente ad un incremento dell'attività di mining così da portare il suo costo al livello originale. Paradossalmente ogni riduzione di costo porta ad un consumo *maggiore*. In caso contrario, tuttavia, il sottoprodotto è altrimenti "consumato" come uno scarto. Così il suo consumo nel mining, anche in una misura maggiore, non rappresenta un aumento del suo consumo complessivo.

Quando il mining si sposta dall'utilizzare il prodotto primario ad utilizzare il sottoprodotto di scarto viene incrementata o l'offerta a mercato (e.g. l'energia) o l'utilità (e.g. la memoria computazionale) del prodotto primario. Assumendo che la domanda rimanente resti invariata, questi cambiamenti rispettivamente di offerta o di domanda portano ad un abbassamento del prezzo del prodotto primario.

Bitcoin richiede il consumo di risorse impiegate in maniera diffusa come caratteristica della sua sicurezza. Ad esempio, l'energia è un fattore di ogni produzione, assieme al tempo e al lavoro. La domanda per queste risorse tende ad aumentare a fronte di una riduzione del loro prezzo. Inoltre, poiché l'energia è un fattore di ogni produzione, il costo di altri prodotti (e.g. la memoria computazionale) si riduce ad energia, tempo e lavoro - con il lavoro che a sua volta rappresenta un costo energetico (e.g. la produzione di cibo).

Così, data la riduzione di prezzo, la produzione tende ad espandersi di conseguenza (facendo accrescere il capitale e rendendo quindi le persone complessivamente più ricche). La stabilità di prezzo è una caratteristica generale di tutte le *commodity*. **Per quando qui presentato, non è possibile assumere una riduzione nel consumo complessivo di energia derivante dall'utilizzo di un sottoprodotto nel il mining**, invalidando di conseguenza la teoria.

Titolo originale: Byproduct Mining Fallacy

Indice

Fallacia della Causazione

Vi è una teoria secondo la quale il mining "segua" il prezzo, o più specificamente il valore della ricompensa. L'implicazione naturale è che il mining sia schiavo del prezzo poiché viene a mancare qualsiasi fattore di dipendenza nell'utilità della moneta.

Si consideri il miner che risponde solamente ai valori della ricompensa su base storica. Questa persona non può essere il primo miner perché la ricompensa a quel tempo non ha valori storici. Nessun prezzo può essere stabilito in quanto non è ancora avvenuto alcuno scambio. Il miner potrebbe aver ricevuto la notizia che un certo numero di unità non confermate abbia acquistato una pizza, ma magari le stesse unità hanno subito una doppia spesa. Egli deve anticipare un certo livello di ritorno netto futuro sul capitale che non è determinabile finché esso si materializza o non si materializza. Questa è la natura del rischio imprenditoriale. Il rischio deve essere preso prima che il prodotto possa esistere. Si può credere che tale rischio possa essere spostato sul consumatore attraverso un ordine anticipato del prodotto. Ma a quel punto il consumatore è diventato l'imprenditore, fornendo il capitale e assumendosi il rischio della produzione.

E' certamente possibile per un miner rispondere solamente ai valori di ricompensa storici una volta che la storia è stata stabilita da qualcun altro che si sia assunto tale rischio. Ma qual è la finestra temporale ed il metodo di applicazione della media che predice i futuri valori di ricompensa? L'abilità, unica nel suo genere, di predire i prezzi di scambio fornirebbe al miner ricchezze illimitate. Se ciò potesse essere fatto in maniera generalizzata, il prezzo non cambierebbe mai, in quanto tutti i cambiamenti potenziali sarebbero già scontati alla prima emissione. Per questa ragione, o il prezzo cambia imprevedibilmente, o non cambia affatto. In altre parole, ogni miner affronta la stessa situazione del primo. Non esistono prezzi storici che possano predire prezzi futuri.

Assumendo generalmente un ritorno medio a mercato sul capitale investito nel mining, sia la sovrastima che la sottostima del valore della ricompensa implica una perdita in relazione al costo del capitale. Data la natura della competizione, i profitti e le perdite (rispettivamente al di sopra o al di sotto del ritorno a mercato sul capitale) incontrano una costante pressione negativa di tipo esistenziale. In altre parole, il mercato prova ad eliminare questi errori. Ma data la natura

imprevedibile del prezzo, in realtà, questo compito non può mai essere portato a termine. La produzione non ricerca mai il soddisfacimento della domanda esistente che è di tipo storico per natura, ma va alla ricerca della domanda che essa stessa anticipa. **La produzione prova ad indovinare continuamente il consumo futuro e facendo ciò crea l'opportunità per il consumo stesso** (o non crea assolutamente nulla).

E' possibile affermare che i miner convergano ad un ritorno sul capitale a mercato anticipando i più alti valori delle *fee*. Ma i commercianti, in maniera simile, convergono ad un ritorno sul capitale a mercato dei miner ricercando il più basso valore delle *fee*. Ciò nonostante, i miner devono anticipare i commercianti e rischiare nell'attività del mining prima che venga creata alcuna utilità. Così nella misura in cui vi è una asimmetria, il mining precede l'attività di effettuare transazioni, così come ogni produzione deve precedere il consumo. Fare assunzioni differenti è un fraintendimento tra la direzione che prende il mercato con il modo in cui avviene questo processo.

Titolo originale: Causation Fallacy

Indice

Fallacia dello Scarafaggio

Vi è una teoria secondo la quale l'aggregazione non riduca materialmente la sicurezza offerta dalla condivisione del rischio, in quanto i miner e l'economia si disperderanno quando necessario, in maniera simile agli scarafaggi che si sparpagliano quando vengono disturbati dalla luce. **La teoria implica, irrazionalmente, che la sicurezza *effettivamente* esista perché *può* esistere**. Si tratta essenzialmente di un rifiuto nell'accettare il Paradosso del Livello di Minaccia, il quale suggerisce che la sicurezza, sottoposta ad una minaccia persistente, evolva nel tempo.

La teoria in questione poggia sulla mutevole fedeltà degli operatori dei dispositivi di mining rispetto al loro miner aggregatore. Questa a sua volta è basata sulla Fallacia del Bilanciamento del Potere che assume, in maniera scorretta, che siano i miner ad essere la minaccia. Un cambiamento di *hash power* da un centro-di-mining ad un altro non riduce il raggruppamento ed il rischio ad esso associato. Il rischio è che lo stato coopti grandi quantità di *hash power*, riducendo sostanzialmente il costo dell'attacco. E' un errore pensare che gli stati non collaborino in difesa del signoraggio.

> Il Fondo Monetario Internazionale è una organizzazione formata da 189 paesi che lavora per favorire la cooperazione monetaria globale...

Per questa ragione non è possibile assumere che tutti i grossi centri di mining possano operare al di fuori del controllo dello stato. Una riduzione del raggruppamento richiede un aumento del numero di miner, specificamente di quelli che sono disponibili ed hanno le capacità per operare sotto copertura. Questo richiede che questi operatori soffrano l'incremento di costo associato al loro ridotto raggruppamento. Tuttavia, non ci si può aspettare che le persone lavorino contro i propri stessi interessi finanziari. Affinché la condivisione del rischio aumenti, la pressione finanziaria contro di essa deve cambiare direzione. Assumere il contrario è irrazionale dal punto di vista economico.

La teoria, inoltre, ignora la centralizzazione e la delegazione economiche. E' un errore assumere che l'economia possa decentralizzarsi rapidamente, e inoltre, sarebbe molto probabilmente infattibile annullare i rapporti di delega in essere nel caso di un attacco da parte dello stato poiché, solitamente, il controllo dei cambi limita i trasferimenti.

Titolo originale: Cockroach Fallacy

Indice

Fallacia dell'Espansione del Credito

L'espansione del credito è la moltiplicazione del credito stesso rispetto alla moneta derivante dall'attività di prestito. Quando viene perfezionato un prestito il prestatore ed il debitore detengono la stessa quantità di denaro. A causa dell'apparente natura inflazionistica dell'espansione del credito, essa è trattata come un effetto avverso sulle persone che possiedono la moneta. Poiché le banche rappresentano la categoria di prestatori più importante, questo effetto è spesso attribuito all'attività bancaria in sé. A questo riguardo vi è una teoria secondo la quale Bitcoin possa eliminare gli effetti del sistema bancario basato su riserva frazionaria e quindi eliminare l'espansione del credito.

Il risparmio comprende le attività di accumulo ed investimento. Accumulare implica l'azione di una ininterrotta svalutazione che rappresenta un consumo presente. Investire significa dare in prestito alla produzione e ciò implica che non vi è alcuna svalutazione, poiché i prodotti devono esistere prima che possano effettivamente svalutarsi. L'investimento include sia i contratti di debito che di compartecipazione societaria in quanto la distinzione è prettamente finanziaria, non avendo significatività economica.

La distinzione tra accumulare ed investire è fondamentale per giungere alla comprensione dell'espansione del credito. La moneta accumulata è sotto il controllo del suo possessore, ovvero messa in una camera di sicurezza, sepolta in giardino o messa sotto al materasso. Ciò è intrinseco al significato di proprietà. Il prestatore di moneta non è più il possessore della moneta stessa, anche se il dare in prestito viene considerato una forma di risparmio.

Un prestatore necessita di liquidità per operare, e, come tale, deve accumulare una certa frazione di risparmi. Quando viene acceso il prestito, il debitore possiede l'ammontare dato in prestito. Il debitore, a sua volta, necessita di liquidità, e così accumula una certa parte del prestito stesso. Ogni rimanenza del prestito è necessariamente investita. Questo significa che il debitore, a sua volta, è diventato un prestatore. Il processo continua fino al punto in cui tutto il capitale esistente viene accumulato.

Talvolta ci si riferisce al quantitativo accumulato come alla "riserva" del proprietario, ma più appropriatamente esso è l'accumulo del suo proprietario, una frazione dei risparmi totali del proprietario. Questo utilizzo della parola *riserva* non dovrebbe essere confuso con l'utilizzo che se ne fa nel contesto della moneta di stato come valuta di riserva (i.e. la riserva estera). Il termine "sistema bancario a riserva frazionaria" è un riferimento al rapporto che vi è tra quanto accumulato dalla banca ed il credito emesso dalla stessa (i conti bancari).

Ci si riferisce all'ammontare totale dei Dollari Statunitensi in circolazione con la sigla "M0". Questo include tutta la valuta tangibile ("cassa contante") in aggiunta ai bilanci bancari intangibili dei conti presso la Federal Reserve. Queste due forme di credito vengono considerati titoli d'obbligo intercambiabili della Fed. I titoli d'obbligo intangibili sono moneta che è stata messa a bilancio ma non ancora stampata. Come riportato dalla Fed, il totale dei Dollari Statunitensi è così suddiviso:

Dollari	Quantitativo (2019)
Tangibile	1'738'984'000'000 $
intangibile	1'535'857'000'000 $
Moneta totale (M0)	3'274'841'000'000 $

La quantità M0 sommata a tutta la moneta (n.d.t. in realtà credito bancario - si veda la tabella sottostante) dei conti bancari viene chiamata "M3". Questo dato non è più pubblicato dalla Fed, ma viene stimato essere pari a 17'682'335'000'000 $. Il quantitativo totale del credito denominato in Dollari Statunitensi può essere stimato dalla somma dei seguenti categorie denominate in Dollari: conti bancari, titoli obbligazionari, titoli azionari pubblici e privati.

Credito in Dollari	Quantitativo (2019)
Bancario (M3 - M0)	14'407'494'000'000 $
Titoli Obbligazionari	41'000'000'000'000 $
Titoli Azionari Pubblici	32'891'169'631'125 $
Titoli Azionari Privati	6'426'333'525'358 $
Credito Totale	94'724'997'156'483 $

- Il rapporto totale della moneta rispetto al suo credito è intorno al 3.46% o equivalentemente **l'espansione del credito è 29.9 volte la moneta sottostante**.
- Le riserve bancarie pari a 1,400,949,000,000 $ indicano un rapporto di riserva pari a circa l'11.11% sul credito, o equivalentemente **una espansione del credito di 9.0 volte la moneta sottostante**. Questo dato è leggermente superiore al requisito di riserva che non è mai superiore al 10% (n.d.t. si noti che l'affermazione riflette la situazione alla stesura del

capitolo nel corso del 2019, a partire dal 2020 il requisito di riserva negli Stati Uniti è stato abolito (0%) *ex lege*, sic!) .
- La Riserva relativa alla moneta rimanente (i.e. che esclude le riserve bancarie) rispetto ai titoli obbligazionari ed azionari (i.e. il rapporto tra M0 meno le riserve bancarie e la somma di obbligazioni ed azioni) è pari a circa il 2.08%, ovvero **una espansione del credito di 48.0 volte la moneta**.

L'eliminazione dell'espansione del credito richiede l'eliminazione del credito e di conseguenza della produzione. Tutto il credito è soggetto a default. Tuttavia la teoria afferma che il credito bancario è differente presumendo che esso sia "*risk free*". Questa presunzione deriva dall'esistenza di una assicurazione dei contribuenti di tale credito. Questo fatto non è una conseguenza del sistema bancario ma dell'intervento dello stato nel sistema bancario. Nella misura in cui questa presunzione è attribuita al *free banking*, la teoria è invalida. Tutte le categorie di impresa sono soggette a fallimento e non essendo diverso da esse il *free banking* elimina questa errata percezione.

La distinzione tra un Fondo di Investimento Monetario (Money Market Fund - MMF) e un Conto di Deposito Monetario (Money Market Account - MMA) è istruttiva. Entrambi sono concepiti per mantenere una equivalenza 1 a 1 con la moneta tuttavia entrambi vengono scontati rispetto alla moneta stessa a causa dei costi di *settlement* e di rischio (e.g. alcune persone accettano solo moneta contante rifiutando i costi più elevati delle transazioni con carta di credito e assegni). La distinzione tra i due (a parte l'assicurazione dei contribuenti garantita al secondo) è dovuta al modo in cui viene trattato il rischio di investimento e la riserva insufficiente.

Nel caso di un MMF, il default dell'investimento viene riflesso nel prezzo unitario. Poiché il fondo prova a mantenere un sufficiente Valore Netto dell'Asset (Net Asset Value - NAV) per permettere lo scambio di un'unità del fondo con un'unità della moneta, un calo sufficiente del NAV si rifletterà sul prezzo unitario. Nel caso di un MMA, queste perdite sono assorbite dalle riserve monetarie. Se non vi sono riserve sufficienti, o a causa di un inatteso livello di prelievi o a causa di perdite negli investimenti, il MMA va in default. Il fallimento di un MMA si manifesta sotto forma di una corsa agli sportelli, dove alcune persone vengono rimborsate mentre altre non lo sono. Un NAV insufficiente in un MMF si manifesta invece come un calo uniforme del prezzo unitario.

Il vantaggio del MMA è che le sue unità sono più fungibili sebbene vengano scontate rispetto alla moneta sottostante. Il vantaggio del MMF è che le perdite vengono distribuite uniformemente. Non è quindi inaspettato che i MMA sono tipicamente assicurati dai contribuenti, regolati più strettamente dalla stato, e considerati come fossero credito bancario. E' raro per un MMF "rompere la parità con il dollaro" (*break the buck*), ma naturalmente ciò può accadere e avviene nella realtà. Anche i fallimenti bancari hanno luogo ma sono nascosti dall'assicurazione dei contribuenti.

Il credito bancario non è veramente fungibile. Ciò può essere osservato nell'uso quotidiano di carte di credito e assegni. Vi è un rischio materiale che entrambi gli strumenti falliscano il *settlement* a loro associato. Sebbene questo rischio è generalmente associato al correntista (e.g. nel caso di un MMA) non vi è differenza per la persona che accetta il credito. Ci si potrebbe immaginare quindi che accettare carte di credito e assegni appoggiati ad un MMF venga trattato nella stessa maniera. Il credito circolerebbe come un equivalente in moneta e inoltre distribuirebbe il rischio più uniformemente tra coloro che beneficiano del ritorno sull'investimento derivante da esso. Il *free banking* ha la possibilità di adottare entrambi i modelli in qualsiasi misura le persone lo desiderino ma in ogni caso il credito si espanderebbe rispetto alla moneta sottostante, il rischio esisterebbe e i sostituti monetari esisterebbero comunque.

La decisione di accumulare rispetto ad investire è basata interamente sulla preferenza temporale di ciascun individuo. La preferenza temporale non è derivabile da nessun altro fattore. Come dice il nome, essa è una preferenza dell'uomo. Le preferenze dell'uomo sono soggette a cambiamento e allo stesso modo lo è la preferenza temporale. La preferenza temporale determina il tasso di interesse economico che può essere anche considerato come il costo del capitale. Un incremento nel costo del capitale dovuto ad un aumento della preferenza temporale causa una contrazione del credito disponibile, viceversa una sua diminuzione porta all'effetto opposto. Con una preferenza temporale infinita tutto il capitale sarebbe accumulato per essere consumato, ponendo fine di ogni produzione.

Non importa se ci si riferisce al prestatore come ad una "banca", tutti gli investimenti sottintendono lo stesso comportamento. Se le banche operassero con un accumulo del 100% esse non sarebbero dei creditori. Questo non implica alcuna riduzione nell'imprestare denaro, in quanto il tasso del denaro imprestato è determinato solamente dalla preferenza temporale. **Bitcoin può essere imprestato e non contribuisce in alcun modo a limitare l'espansione del credito**. La teoria è di conseguenza invalida.

Eliminare l'espansione del credito è equivalente alla condizione di preferenza temporale infinita, cui corrisponde un tasso di interesse infinito, nessun capitale disponibile per la produzione e nessun prodotto disponibile per il consumo. Negli stati dove il credito è limitato per legge (dalle leggi sull'usura) gli investimenti vanno verso gli strumenti azionari, i prestiti predatori o viene posto fine alla produzione.

Titolo originale: Credit Expansion Fallacy

Indice

Fallacia del *Loop* del Debito

Vi è una teoria secondo la quale la moneta, in realtà, non esista nel moderno sistema della valuta di stato . Al suo posto, ciò che viene definito moneta "fiat" è in realtà un sostituto monetario (e.g. un titolo per reclamare legalmente della moneta). Un sostituto monetario è un obbligo a redimere la moneta presa a prestito che il titolo stesso rappresenta, così che, anche a livello definitorio, ciò rappresenta un problema - che sta alla base del termine "loop". La teoria si basa sull'osservazione che lo stato, allo stesso tempo, emette e accetta la valuta, presupponendo un obbligo nel fare ciò, come ad esempio nella cancellazione del debito verso lo stato (e.g. attraverso le tasse). Per questa ragione la pretesa all'emissione è un credito a compensazione di un futuro *settlement* in termini di tasse, etc. (i.e. moneta presente).

Tuttavia, i sostituti monetari sono dei diritti a reclamare un ammontare definito di moneta, in quanto, altrimenti, non sarebbero fungibili. L'ammontare di un debito d'imposta rappresentato da una banconota da $100, quantificabile in 100$ di tasse, è definito in termini di sé stesso (i.e. la fallacia logica del ragionamento circolare). Tale ammontare, infatti, è controbilanciato da qualunque cosa lo stato desideri scambiare per esso. Questo comprende potenzialmente ogni moneta, che include 100 once d'oro o 100 unità di moneta fiat. **La moneta non rappresenta alcun ammontare di un determinato bene, ma rappresenta qualsiasi cosa possa essere scambiata per essa**.

Lo stato non incorre in alcun debito nel dichiarare che accetterà una moneta, sia essa l'oro o moneta fiat. In maniera simile un'attività commerciale che dichiari l'accettazione di una particolare moneta non incorrerà in alcun debito nel fare ciò. Il debito sotteso ad una moneta rappresentativa (una forma di sostituto monetario), come un certificato d'oro, è espresso nello scambio dell'oro con il diritto vantato dal possessore del certificato stesso. L'emissione di moneta non cambia questo fatto. Sia lo stato che un'attività commerciale possono certamente emettere oro in uno scambio senza che l'oro venga considerato un debito. La moneta fiat di stato gode della protezione di monopolio sull'emissione, garantendo allo stato un profitto nel farlo. Ma questo non rileva alla questione se la moneta fiat sia moneta o debito.

Nessuna moneta ha valore intrinseco. La moneta fiat si distingue dalla moneta merce, come l'oro, in base alla presunzione che essa non possieda valore d'uso. Ma poiché il valore è soggettivo, questa non è una distinzione essenziale. In realtà non si tratta neanche di una distinzione reale, in quanto la cartamoneta può essere bruciata per riscaldarsi. Se lo stato estraesse, emettesse e accettasse oro o bitcoin, la teoria dovrebbe considerare le unità d'oro e di bitcoin come debito in base agli stessi criteri che vengono applicati alla moneta fiat.

La teoria rappresenta una errata comprensione della natura dei sostituti monetari. Un diritto non può essere un diritto a riscattare sé stesso. In questo scenario, il diritto da riscattare si finalizzerebbe in sé stesso. In altre parole, se 100 $ rappresentano un diritto vantato su 100 $ in valore di qualsiasi cosa, detenere tale diritto porta a soddisfare il diritto stesso. Non sarebbe un diritto sotto nessuna forma, sarebbe una moneta. Per questa ragione la teoria è invalida.

Il passaggio da diritto negoziabil a moneta fiat avviene quando la moneta rappresentativa è abrogata dal suo emittente. Il Dollaro Statunitense venne monetizzato nel 1934 quando la possibilità di riscattarlo venne cancellata. Le persone vennero obbligate a scambiare dollari redimibili per dollari irredimibili. Nella misura in cui i dollari precedentemente redimibili rimangono in circolazione, come avviene ancora oggigiorno, essi vengono convertiti quando la *Federal Reserve* entra in loro possesso. Mantenere la dicitura "Federal Reserve Note" su un dollaro irredimibile è anacronistico.

Ogni moneta possiede dei sostituti monetari come conseguenza dell'attività di prestito. Possiamo classificare quattro ipotetici scenari in cui ricadono i sostituti monetari in termini di regressione del debito, dove ogni passo nella regressione è costituito da un titolo promissorio (n.d.t. una cambiale).

- nessuna regressione (moneta)
- singola regressione (moneta rappresentativa)
- regressione finita (sostituto monetario)
- regressione infinita (moneta impossibile)

Un titolo potrebbe costituire un diritto su un altro tipo di diritto, ma non riferito a sé stesso (i.e. a qualunque cosa possa essere scambiata per esso). In caso contrario, non vi è alcuna regressione reale e ciò che si supponeva essere un diritto *è* moneta. Questo vale nel caso il diritto reclamabile sia direttamente o indirettamente circolare, come implicato dal termine "*loop*", in quanto il titolo relativo a tale diritto si finalizza in sé stesso. Così il termine "*loop* del debito" è un altro termine descrittivo del termine "moneta". Esempi di questo includono Oro, Bitcoin ed e l'irredimibile (moderno) Dollaro Statunitense.

Un titolo diretto (singola regressione) contro moneta è la moneta rappresentativa, sebbene questo termine è generalmente riservato per la banconota tangibile che rappresenta la moneta merce. La banconota *rappresenta* direttamente la moneta. Il Dollaro Statunitense redimibile era una moneta rappresentativa.

Un titolo indiretto rappresenta ogni progressione finita di diritti su altri diritti. Quando tutti i diritti sono finalizzati, la moneta è nelle mani del suo legittimo proprietario ove tutti gli altri diritti sono estinti e ogni diritto circolare è interamente compensato. Si noti che se il diritto è totalmente circolare non vi è nulla da finalizzare (i.e. il titolo è moneta).

Una regressione infinita di diritti non può esistere. Si consideri un ipotetico titolo emesso dal tesoro di stato riscattabile sotto forma di compensazione del debito di imposta dovuto allo stato.

- 1 $ finalizza il debito d'imposta su 10 $ di introiti.
- 10 $ finalizzano il debito d'imposta su 100 $ di introiti.
- 100 $ finalizzano il debito d'imposta su 1000 $ di introiti.
- e così via...

Nonostante il titolo non rappresenti sé stesso, la sua regressione è infinita. Un diritto può essere reclamato a fronte di un numero finito di altri titoli rappresentanti diritti. In ogni caso, ogni strumento di questo genere non è un titolo e può essere scambiato solo come moneta.

Titolo originale: Debt Loop Fallacy

Indice

Fallacia del Mining Disaccoppiato

Vi è una teoria secondo la quale la sicurezza nel mining raggruppato (*pooling*) viene incrementata disaccoppiando la ricompensa dalla selezione delle transazione. La teoria ritiene che attraverso la condivisione della sola ricompensa, il controllo sulla selezione delle transazioni si sposti sui miner con minore *hash power*. Questo implica una riduzione nello sconto di varianza e di conseguenza un incremento nella competitività dei centri di mining più piccoli. Poiché i centri di mining più piccoli possono presumibilmente operare in maniera più coperta di quelle più grandi, questo a propria volta implicherebbe che la resistenza alla censura ne risulterebbe incrementata.

La teoria non riconosce che il controllo sulla selezione delle transazioni rimane in capo all'operatore della *pool*, ed è quindi invalida. L'unico beneficio consiste nella riduzione della varianza, ma questo si registra solo quando il pagamento viene ricevuto. Poiché il pagamento è discrezionale, ad esso può essere teoricamente associato ogni tipo di condizione. Le condizioni potrebbero includere la censura e l'identità. I membri possono ricorrere all'abbandono della *pool* in favore di un'altra, così come potrebbero ricorrenre al raggruppamento con condizione di accoppiamento. Per questa ragione le *pool* disaccoppiate e quelle accoppiate sono egualmente soggette alla cooptazione.

Vi è una teoria correlata secondo la quale la trasparenza di una *pool* che impiega il disaccoppiamento è maggiore di quella di una *pool* che usa l'accoppiamento, cosa che facilita la fuga dei suoi membri verso le *pool* che non adottano la censura, limitando quindi la dominanza delle *pool* che adottano censura. Anche accettando generosamente le assunzioni di maggiore trasparenza e il fatto che miner indipendenti agiscano contro il proprio stesso interesse finanziario, la questione della cooptazione rimane comunque irrisolta. Lo stato può sempre riservare a sé stesso l'abilità di operare con i vantaggi finanziari del raggruppamento e la teoria è quindi invalida.

Questa fallacia è simile alla Fallacia della Propagazione che sostiene che tutti i vantaggi finanziari dipendono da miner altrimenti indipendenti che affidano ad

una singola persona il controllo di quello specifico vantaggio.

Titolo originale: Decoupled Mining Fallacy

Indice

Fallacia del *Dumping*

Vi è una teoria secondo la quale vendere le unità di una parte di una moneta separata per le unità dell'altra parte riduce l'utilità relativa della moneta venduta. Tuttavia ogni vendita richiede l'esistenza di un acquirente. Trattandosi di un fenomeno di scambio, l'azione è simmetrica e quindi la teoria è invalida.

Vi è una teoria collegata secondo la quale scambiare unità da un solo lato di una moneta separata costituisce un'azione di *dumping* della moneta stessa, cosa che riduce la sua utilità. La teoria rappresenta semplicemente in modo errato il concetto di *dumping*. Il dumping è una forma di sussidio di stato (da non confondersi con la componente di sussidio di Bitcoin) applicato ad un prodotto venduto ad un altro stato. Si tratta di una imposizione messa in capo al contribuente dello stato sussidiante, applicata tipicamente per ottenere delle quote di mercato sul prodotto in questione. Nel caso la domanda sia elastica, il sussidio incrementa il volume delle vendite del prodotto riducendo il prezzo rispetto a quello che sarebbe altrimenti il prezzo di mercato. Il prezzo ridotto incrementa la domanda richiamando acquirenti con una più bassa utilità marginale per il prodotto finché il mercato non raggiunge l'equilibrio. A differenza di quanto avviene con il *dumping*, scambiare beni a prezzo di mercato non ne riduce il prezzo perché esso non è sussidiato.

Infine, vi è una teoria collegata secondo la quale la riduzione dell'accumulo riduce generalmente i prezzi di scambio del bene accumulato. Ciò è vero, tuttavia un trasferimento non rappresenta una riduzione del livelli di accumulo a meno che l'acquirente della proprietà accumulata, successivamente, non la accumuli in maniera minore rispetto al venditore. E' un errore assumere che tale ipotesi si applichi in questo caso.

Titolo originale: Dumping Fallacy

Indice

Fallacia del Blocco Vuoto

Esiste una teoria secondo la quale minare blocchi vuoti rappresenti un attacco. Tra le ipotesi, la teoria non richiede che i blocchi siano minati su un ramo debole nel tentativo di permettere la doppia spesa e non specifica quale persona venga attaccata.

Si prendano in considerazione i seguenti punti:

- Il termine "attacco" implica il furto. Il *whitepaper* di Bitcoin, ad esempio, utilizza il termine solamente per descrivere i tentativi di doppia spesa.
- Una ricompensa di un blocco è costituita dalle *fee* per le transazioni e da un sussidio. Il miner che rinuncia alle *fee* delle transazioni non includendole (n.d.t. in un blocco) non è remunerato da esse.
- L'*hash power* del miner contribuisce in maniera proporzionale alla sicurezza del network. Il sussidio rappresenta la compensazione per la sicurezza durante la fase inflazionaria. Lo scopo dell'inflazione è quello di distribuire razionalmente le unità. La distribuzione razionale è scambiata specificamente in cambio di *hash power*, non al fine di includere transazioni.
- La conferma di transazioni non è garantita. Le *fee* sono l'*incentivo* per la conferma. La mancanza di conferme implica in maniera obiettiva l'insufficienza delle *fee*.
- I blocchi vuoti sono totalemnte compatibili con regole del consenso e non possono essere ragionevolmente impedite da una nuova regola.

Per queste ragioni la teoria è invalida. Tuttavia risulta utile investigare la causa della fallacia. A causa della Proprietà del Gioco a Somma Zero si potrebbe teoricamente assumere che minare un blocco vuoto "slealmente" possa togliere la possibilità alle transazioni di essere confermate.

Gli altri miner mantengono sempre la capacità di confermare transazioni in proporzione al loro *hash power*. Se il 10% dell'*hash power* mina blocchi vuoti, le conferme richiederanno in media il 10% in più del tempo. Tuttavia se un miner rimuove il 10% dell'*hash power* totale, le conferme richiederanno sempre il 10% in più del tempo in media, fino al successivo aggiustamento della difficoltà. Tuttavia rimuovere il proprio *hash power* non è generalmente considerato un attacco.

Un miner impegna del capitale per minare, producendo, in ritorno, dell'*hash power*. Tenendo da parte gli effetti del raggruppamento, il miner viene sovvenzionato in proporzione all'*hash power* prodotto. Senza questo *hash power* altri miner produrrebbero lo stesso numero medio di blocchi ad una difficoltà proporzionalmente minore. In altre parole, un attacco *reale* sarebbe proporzionalmente meno costoso. Così, nonostante il miner non venga remunerato per includere transazioni, egli sta rendendo sicure le transazioni precedentemente confermate.

Poiché il costo marginale di includere una transazione è al di sotto dei livello medio delle *fee*, il miner che mina un blocco vuoto sta subendo un costo opportunità. Tale costo rappresenta il livello al quale il miner sta sussidiando la sicurezza della catena. Nonostante questo comportamento sembri economicamente irrazionale nel limitato contesto della moneta, esso può considerarsi razionale a causa del costo opportunità insito nell'aspettare a minare su un blocco candidato non vuoto in seguito ad un annuncio (n.d.t. in pratica si procede a minare un blocco vuoto nell'attesa di costruire - o più frequentemente ricevere dalla pool - su un *template* candidato valido e non vuoto).

Nonostante un certo miner possa considerare vantaggioso minare blocchi vuoti, è nel potere di qualsiasi altra persona fare altrimenti. E' la facoltà di esercitare questa opportunità che rende sicura la moneta, anche contro attacchi *reali*. **Criticare queste azioni dettate dal proprio interesse è del tutto inefficace e controproducente**.

Titolo originale: Empty Block Fallacy

Indice

Fallacia dell'Esaurimento dell'Energia

Esiste una teoria secondo la quale la *proof-of-work* (PoW) potrebbe esaurire tutta l'energia disponibile per le persone. La PoW converte l'energia in una barriera contro la doppia spesa che crescente monotonamente per ogni data transazione. Questo è confrontabile con l'energia spesa nel rendere sicura qualsiasi moneta dalla contraffazione (dal suo stesso ente emittente o in altra forma).

Lo scopo di ogni misura di sicurezza è quello di creare un costo necessario a superare tale misura; i.e. una barriera finanziaria. Bitcoin crea la sua barriera alla doppia spesa obbligando l'attaccante a sostituire il ramo della transazione bersaglio con un ramo avente probabilisticamente maggior lavoro. Curiosamente, se la sostituzione ha successo, la barriera per i successivi attaccanti viene elevata in misura ancora maggiore. **L'energia spesa non è un fattore indipendentemente importante dal processo, la barriera eretta è l'onere *finanziario* che l'attaccante deve necessariamente affrontare**.

La barriera di sicurezza (S) di un blocco è il prodotto del costo unitario di un hash (C), dell'*hash rate* (H) e del periodo di tempo (T).

```
S = C * H * T
```

L'aggiustamento porta alla variazione dell'*hash rate* necessario per mantenere un periodo costante per un dato livello del costo di un hash e di sicurezza.

```
T = S / (C * H)
```

Un periodo costante implica che l'*hash rate* è inversamente proporzionale al costo per un dato livello di sicurezza.

```
H ~ S / C
```

Quando l'approvvigionamento di energia viene ridotto il suo prezzo deve aumentare, cosa che riduce il quantitativo speso per un dato livello di sicurezza. Di conseguenza l'energia non può essere esaurita dal mining e la teoria è invalida.

Titolo originale: Energy Exhaustion Fallacy

Indice

Fallacia dello Stoccaggio di Energia

Vi è una teoria secondo la quale il valore dell'energia spesa nella proof-of-work è convertito in valore della moneta, "immagazzinando" effettivamente il valore per un consumo successivo. Nella misura in cui l'energia ha un valore, il lavoro sottostante è venduto in cambio di bitcoin e la moneta è una riserva di valore, tale affermazione è corretta.

Tuttavia la teoria è errata quando implica che il valore dell'energia speso nel mining è unico nel suo contributo al valore. I miner scambiano energia in cambio di unità. Tuttavia tutti i commercianti scambiano qualcosa in cambio di unità. Tutte le cose offerte in uno scambio rappresentano la domanda. **Fatta salva la grandezza, una fonte di domanda non può essere considerata arbitrariamente un fattore più determinante del valore rispetto ad un altra fonte di domanda**. Per questa ragione la teoria è invalida.

Titolo originale: Energy Store Fallacy

Indice

Fallacia dello Spreco di Energia

Esiste una teoria secondo la quale la *proof-of-work* (PoW) rappresenti uno spreco di energia. Questo implica che il livello di sicurezza fornito è maggiore del necessario o che lo stesso livello di sicurezza possa essere fornito da un altro tipo di prova esternalizzata ad un minore costo energetico. Una prova di tipo internalizzato, specificamente la *proof-of-stake* (PoS), rappresenta un altro modello di sicurezza che non viene preso qui ulteriormente in considerazione.

L'*hash power* totale è una funzione della ricompensa, che è funzione delle *fee*, che a loro volta sono determinate dal mercato delle conferme. Se una persona considera il corrente *hash power* insufficiente a proteggere uno scambio di un certo valore contro la doppia spesa allora il requisito di profondità richiesto aumenta. Inoltre, come mostrato ne la Proprietà della Soglia di Utilità, le transazioni con un insufficiente valore per avere anche una sola conferma hanno un prezzo che non le fa includere nella catena.

Questi limiti di sicurezza, rispettivamente superiore ed inferiore, dipendono dal costo di conferma e sono quindi indipendenti dalla tecnica impiegata dalla prova. **Non vi è alcun livello di sicurezza *necessario* ma solo una profondità di conferma soggettiva ed un'utilità minima**.

La sicurezza nella conferma aumenta all'aumentare del costo per generare ciascun blocco. La doppia spesa di una transazione richiede che il suo ramo sia sostituito da un altro avente un maggior costo probabilistico. Così, il solo modo in cui può essere ridotto il costo energetico è quello di spendere lo stesso costo medio per blocco con una minore componente di energia.

La PoW è costituita da differenti forme di costo che includono lavoro, hardware, servizi, terreno, etc. Qualsiasi altra prova di tipo esternalizzato consuma le stesse risorse, sebbene potenzialmente in diverse proporzioni. La questione della riduzione del costo energetico si riduce allo stabilire se una componente energetica del costo della prova può essere sostituita da un altra risorsa componente allo stesso costo. Tuttavia il costo della risorsa sostitutiva include tutti i suoi costi di

produzione che devono necessariamente ricondursi all'energia. La teoria è quindi invalida.

Inoltre, garantire la sicurezza di una moneta rappresenta un costo per i commercianti. Per questa ragione, il fatto che essa venga usata implica che essa sia preferita rispetto alle alternative. Questo implica che le alternative sono essenzialmente più costose. Poiché tutti i costi si riducono fondamentalmente al consumo di energia, segue che la moneta in uso è quella maggiormente efficiente dal punto di vista energetico.

Titolo originale: Energy Waste Fallacy

Indice

Fallacia del recupero della *fee*

Esiste una teoria secondo la quale i miner ricavino un vantaggio finanziario su altri miner quando minano le loro stesse transazioni e quindi "recuperano" le loro stesse *fee*.

La teoria ignora il costo opportunità di occupare lo spazio del blocco senza incassare un pagamento. Il pagamento di una *fee* verso sé stessi è un non-evento finanziario. Non incassare una *fee* rappresenta un costo reale sull'importo a cui si è rinunciato, in quanto il costo del mining per quella porzione del blocco non viene ricompensato. **Il risultato che si ottiene è un più basso ritorno sul capitale rispetto ai miner che vendono effettivamente il loro spazio del blocco**. Data la natura di gioco a somma zero del mining questa disparità consente ai miner più razionali di aumentare il loro *hash power* reinvestendo il loro più alto ritorno del capitale.

Un volume più alto di transazione che competono per avere conferme implica un aumento del livello medio delle *fee*. Questo fatto influenza tutti i miner allo stesso modo, tuttavia un incremento del livello delle *fee* dà luogo a maggiore competizione, non ad un incremento del tasso di ritorno sul capitale. Al contrario, tutti i miner risentono di una ridotta utilità causata dall'aumento di domanda e di conseguenza dal livello delle *fee* (che è stato finanziato completamente dai miner che non sono stati ricompensati). In altre parole la conseguenza è l'opposto di quella proposta, e ciò rende la teoria invalida.

Vi è una teoria correlata secondo la quale gli strumenti di stima delle *fee* possano essere ingannati nel raccomandare delle *fee* più alte di quanto sia effettivamente necessario. Come mostrato ne la Fallacia della *Fee* a Parte questo implica sia una relazione tra il valore storico ed il valore futuro delle *fee* - relazione che non esiste, sia che tutte le *fee* siano visibili *on-chain*, circostanza altrettanto non verificabile.

Titolo originale: Fee Recovery Fallacy

Indice

Fallacia della Purezza Genetica

Esiste una teoria secondo la quale una moneta è più forte quando tutta la validazione è svolta da una singola implementazione comune. Secondo questa teoria, la complessità nell'implementare le regole di consenso implica la possibilità che molteplici implementazioni divergano reciprocamente portando ad una separazione involontaria della catena. La separazione implica una perdita finanziaria per le persone che si trovano sul lato più debole della catena. In aggiunta alla divergenza, una singola implementazione corre il rischio di uno stallo globale del network. La minaccia di una perdita finanziaria implica una più bassa utilità e quindi una più bassa sicurezza del sistema.

Basandosi sull'ipotesi di elevata complessità, ciascun aggiornamento "dell'unico ed autentico *client*" porta ad avere la stessa probabilità di divergenza. Analogamente, la dipendenza su librerie esterne aggiornate indipendentemente ha lo stesso effetto. In altre parole *non è possibile che ci sia una sola implementazione per esse*. Nel caso dell'implementazione iniziale di Bitcoin sia l'aggiornamento del client che l'aggiornamento di una dipendenza esterna hanno portato a separazioni involontarie della catena e ad una perdita finanziaria consistente. Inoltre, in questa implementazione sono state pubblicate delle vulnerabilità del giorno zero che avrebbero potuto portare ad uno stallo globale.

Una singola implementazione produrrebbe una debolezza direttamente confrontabile con quella delle specie viventi aventi uniformità genetica. Nel caso di una singola implementazione, sia gli aggiornamenti interni che esterni influenzano l'economia rapidamente ed in profondità. L'impatto finanziario di una separazione è quindi più importante di quello causato da una implementazione meno adottata a grande scala. In uno scenario dove dieci implementazioni che supportano ciascuna la stessa frazione di economia, verrebbe messo a rischio al massimo il 10% dell'economia per ogni dato aggiornamento, mentre l'aggiornamento di una singola implementazione adottata universalmente raggiunge il massimo rischio di separazione del 50%. La teoria non è quindi solo invalida ma esprime esattamente il comportamento opposto di quanto accadrebbe in realtà.

Titolo originale: Genetic Purity Fallacy

Indice

Fallacia della Riserva Intera

Esiste una teoria secondo la quale il sistema bancario a riserva frazionaria sia una frode che permette alle banche di creare moneta "dal nulla". La teoria suggerisce che l'attività bancaria debba essere a riserva intera.

Questa teoria è incardinata sulla definizione della parola "banca". Rothbard sviluppa questo argomento in "*Man, Economy and State*", ma limita esplicitamente la sua definizione di banca a quella di "deposito" di moneta.

> Quando una persona deposita dei beni in un deposito, le viene consegnata una ricevuta ed essa paga il proprietario del deposito una certa somma per il servizio di custodia. La persona conserva sempre la proprietà del bene depositato; il proprietario del deposito la sta semplicemente custodendo per conto suo. Quando la ricevuta del deposito viene presentata, il proprietario è obbligato a restituire il bene depositato. Un deposito specializzato nel custodire moneta è noto come "banca".

Le banche offrono un servizio di deposito che va sotto il nome di cassetta di sicurezza. Ma le banche non sono definite in maniera così letterale. Esse offrono generalmente conti con interesse come conti di risparmio e depositi a termine. Rothbard impiega l'aspettativa di interesse per distinguere tra l'immagazzinamento di moneta in un deposito e l'attività di dare in prestito:

> La proprietà di qualcun altro è prelevata dal deposito ed usata per i propri scopi finanziari. Non è presa a prestito poiché non viene pagato alcun interesse per l'utilizzo di quella moneta.

In altre parole, il suo appello per la riserva intera non si applica ai conti che hanno un interesse. Tuttavia egli tralascia di far notare che l'interesse guadagnato sulla moneta rappresentata dai depositi può legittimamente compensare le commissioni di tenuta del conto altrimenti necessarie. Le banche spesso offrono dei conti di deposito a vista (e.g. conto corrente) senza interesse. Il fatto che esista un rendimento positivo sul conto non rappresenta un fattore distintivo tra tenuta a deposito ed investimento, anche a partire dalla sua stessa definizione. Laddove un conto bancario renda il 5% ed il livello delle commissioni sia del 6%, non vi è distinzione tra quest'ultimo e un rendimento dello 0% accompagnato da un tasso

di commissioni dell'1%. La distinzione è contenuta nell'accordo contrattuale tra il depositante e la banca.

> Poiché è conveniente scambiare dei titoli di carta al posto di trasportare oro, i depositi di moneta (o banche) che si costruiscono una reputazione pubblica scopriranno che poche persone riscatteranno i loro certificati.

I certificati di moneta che rappresentano moneta depositata sono moneta rappresentativa, una forma di sostituto monetario. Negli Stati Uniti le banche di stato e anche quelle di altra tipologia emettevano già questi certificati. Alla fine questi ultimi vennero rimpiazzati dai certificati di deposito d'oro e d'argento emessi dalla banca centrale.

> Le banche saranno particolarmente soggette alla tentazione di commettere una frode ed emettere pseudo-certificati di moneta che andranno in circolazione a fianco dei certificati di moneta genuini come sostituti monetari accettabili. Il fatto che la moneta sia un bene omogeneo significa che alle persone non importa se la moneta che essi riscattano è la moneta originale che hanno depositato. Questo rende le frodi bancarie più facili da compiere.

Nella misura in cui i certificati della banca centrale abbiano mai rappresentato tutta la moneta depositata (e.g. i rispettivi quantitativi di oro e di argento), essi, alla fine, seguirono il percorso descritto da Rothbard. Poiché la quantità di tutti i certificati divenne troppo grande per supportare rimborso, essi vennero abrogati e le persone vennero obbligate a convertirli in valuta fiat. Queste frodi su larga scala avvennero durante la vita sia di Rothbard che del suo precursore von Mises, e vennero perpetrate dallo stato e dalle banche centrali sotto la protezione della legge (i.e. dello stato).

La teoria proposta da Rothbard non si limita a condannare la frode nell'attività bancaria di deposito (la cassetta di sicurezza), essa si estende in generale anche all'onesta attività di prestito dei depositi delle banche che include i depositi a vista, i depositi di risparmio e spesso anche i depositi a termine. Per come presentata la teoria è invalida. Inoltre, essa implica una condanna all'attività di prestito e di investimento in generale. E, come fa notare lo stesso Rothbard, l'attività di prestito non è distinta da quella di investimento:

> Che il capitale risparmiato sia investito attraverso azioni o prestiti, ciò non ha importanza. La sola differenza sta nei tecnicismi di tipo legale. Infatti, anche la differenza legale tra creditore e proprietario (n.d.t. ovvero tra chi impresta capitale ad una società o chi ne detiene delle quote) è trascurabile.

Tutte le forme di prestito hanno origine dal capitale accumulato da una persona, che esso sia depositato in banca o sotto altra forma. Nell'attività di prestito non vi è altra origine dei fondi al di fuori dei risparmi depositati. Vi è una teoria

collegata secondo la quale le persone sono troppo stupide per comprendere i termini contrattuali del deposito.

> Huerta de Soto considera la possibilità che un certo gruppo di clienti bancari (o, seguendo il suo ragionamento, la totalità di essi) sottoscrivano un contratto di deposito in maniera consapevole e accettando totalmente il fatto che le banche investiranno (o daranno in prestito, etc.) una grande porzione del denaro che essi depositano". In questo caso, obietta Huerta de Soto,"l'ipotetica autorizzazione dal depositante manca di validità legale" in quanto pochi persone tra i non addetti ai lavori comprendono l'instabilità intrinseca dell'attività bancaria a riserva frazionaria: essi credono che il deposito sia garantito, cosa che Huerta de Soto considera un (quasi universale) fraintendimento.

Tuttavia coloro che supportano questo argomento si reputano capaci di comprenderlo. Per questo la teoria è invalida. Riconoscendo il principio morale della non aggressione, ogni individuo ha il diritto di contrattare con un altro volontariamente. Impedire l'esercizio di questo diritto costituirebbe un crimine. Generalmente, i riferimenti agli "*unbanked*" presuppongono che un consistente numero di persone non abbia "accesso" ai servizi bancari. Questo non accade in generale, poiché l'accesso all'attività bancaria è ampiamente disponibile in tutto il mondo. Al contrario, queste sono le persone che comprendono tali rischi e decidono di non correrli.

Una teoria collegata è quella secondo la quale i sostituti monetari vengono scambiati allo stesso valore della moneta sottostante, dando luogo ad una frode. Nella misura in cui i sostituti monetari (e.g. i conti di deposito) vengono assicurati dai contribuenti, lo sconto applicato alla moneta che essi sostituiscono è più basso. Tuttavia, anche disponendo di una assicurazione totale sul loro valore, è un errore assumere che essi vengano scambiati alla pari contro moneta. I sostituti monetari si presentano sotto forma di conti di deposito e vengono transati elettronicamente. Il *settlement* dei conti richiede tempo, denaro e costi dovuti al rischio. Le frodi delle carte di credito e degli assegni sono un fenomeno dilagante, e questo costo viene reso visibile nelle commissioni applicate alle transazioni ed ai conti. Il *settlement* può richiedere giorni se non mesi. I commercianti sono necessariamente portati a scontare i sostituti monetari rispetto alla moneta. Anche il trasferimento elettronico diretto tra banche richiede dei concreti costi di *settlement*:

> Alle banche viene addebitata una commissione lorda di 0.82 $ per ogni transazione, tuttavia esiste un sistema a tre livelli di sconto, che porta le commissioni reali a costare tra 0.034 $ e 0.82 $ per transazione in funzione del volume delle stesse.

Questo è il motivo per cui molte attività commerciali accettano "solo contanti", altre non accettano assegni, altre ancora applicano un premio per compensare lo sconto, ed è anche il motivo per cui ci sono le commissioni agli ATM, etc. Per questa ragione, l'affermazione che i sostituti monetari non siano scontati è

confutata da un sacco di esempi che provano il contrario. In maniera ancora più significativa, è comprovato che questo sconto sia necessario, invalidando quindi la teoria.

Un'altra teoria collegata afferma che il prestito bancario crei l'inflazione dei prezzi come conseguenza dell'espansione del credito. Poiché l'attività di prestito e la moneta sono necessariamente evolute assieme, non può esistere un momento in cui la stessa espansione del credito cambi il livello dei sostituti monetari. Questo richiede che avvenga o un'espansione dell'offerta di moneta o una riduzione della preferenza temporale che viene riflessa nel tasso di interesse economico. L'espansione del credito è una funzione che dipende strettamente da questi due fattori, non dall'attività di prestito stessa. Per questa ragione la teoria è invalida.

Un'altra teoria collegata afferma che le banche possano legittimamente imprestare solamente il denaro "di loro proprietà". Tutto il capitale dato in prestito deriva dai risparmi di qualcuno. Se ogni persona può gestire una banca (i.e prendere a prestito i propri risparmi e darli in prestito ad altri) allora questa è una distinzione solo in apparenza. Aggregare i risparmi con quelli di altre persone (e.g. attraverso depositi bancari) non da luogo ad alcuna significativa distinzione. Per queste ragioni la teoria è invalida.

Un'altra teoria collegata afferma che le banche potrebbero legittimamente imprestare solamente attraverso depositi a tempo. Non vi è distinzione economica tra depositi a tempo e depositi a vista, in quanto entrambi implicano riserva frazionaria. La natura del deposito, anche quello nelle cassette di sicurezza, implica che il tempo e altri tipi di vincolo (e.g. l'identificazione) sono richiesti per il ritiro del deposito stesso. Anche i conti correnti e di risparmio assicurati dai contribuenti sono effettivamente depositi a tempo.

> Per tutti i conti di risparmio e tutti i conti correnti personali con interesse, ci riserviamo il diritto di richiedere una richiesta scritta con un anticipo di sette giorni sulla data del ritiro.
>
> Chase Bank: Accordo di Deposito

Il rischio di fallimento e l'espansione del credito rimangono sempre presenti nonostante la scadenza del deposito. Per questo la teoria è invalida. L'unico vero deposito a vista è quello del non depositare (danaro), e naturalmente le persone hanno a disposizione quest'ultimo ed il deposito a tempo nella misura in cui esse preferiscono.

Un'altra teoria collegata afferma che le banche possano legittimamente imprestare solamente i depositi completamente assicurati. Tuttavia l'unico vero rendimento *risk free* è quello di non avere alcun rendimento. Questo è il motivo per cui solo i contribuenti possono assicurare i prestiti (i.e. perché vengono obbligati a farlo). L'assicurazione completa è equivalente, in termini economici, a non avere alcun prestito in assoluto, rendendo la teoria contraddittoria e quindi invalida.

Un'ulteriore teoria collegata afferma che il *free banking* ha intrinsecamente l'abilità di creare denaro dal nulla. Tuttavia se ciò fosse vero allora ognuno

potrebbe farlo, poiché il *free banking* non conferisce poteri speciali alle persone che definiscono sé stessi come un'entità bancaria. Se la moneta potesse essere creata senza costi non rappresenterebbe una proprietà. Per questa ragione la teoria è invalida. Anche la moneta fiat di stato è soggetta ad un costo di produzione, un costo atto a mantenere il suo monopolio sulla produzione, e un costo politico dovuto all'inflazione monetaria. Il *free banking*, che si applica all'oro o a Bitcoin, beneficia dell'assenza del privilegio di signoraggio dovuto alla natura della competizione.

Infine, accade spesso che le persone che sostengono l'imprestare denaro a riserva intera sono le stesse persone che sostengono una più bassa preferenza temporale. Questa è una contraddizione diretta, in quanto il primo punto che essi sostengono (n.d.t. la riserva intera) implica una preferenza temporale infinita.

Titolo originale: Full Reserve Fallacy

Indice

Fallacia dell'*Halving*

Le regole di consenso in Bitcoin danno luogo ad un tasso prevedibile di inflazione monetaria. Questo tasso viene ridotto periodicamente in un punto del tempo chiamato *halving*. Ci sono differenti funzioni a gradino in Bitcoin. L'*halving* avviene ogni 210'000 blocchi del ramo forte, l'aggiustamento della difficoltà ogni 2016 blocchi del ramo forte e le organizzazioni della catena approssimativamente ogni 10 minuti. I valori numerici che controllano questi intervalli sono arbitrari ma la discontinuità risulta necessaria in quanto essa è dovuta alla natura discreta degli intervalli richiesti dalla *proof-of-work*. Esiste una teoria secondo la quale l'*halving* crei una barriera finanziaria per i miner che potrebbe portare ad uno stallo perpetuo. La teoria è basata sull'azione contemporanea di due funzioni a gradino (quella dell'*halving* e quella della difficoltà) che porterebbero il tempo di una successiva organizzazione ad aumentare sensibilmente a causa della simultanea riduzione dei profitti dei miner.

La teoria presuppone che l'aggiustamento della difficoltà porti a zero il profitto economico medio dei miner, permettendo solamente alla prima metà dei miner (in ordine di profittabilità) di sopravvivere, riducendo quindi l'attività di mining a pochi miner. In altre parole, l'aggiustamento della difficoltà viene considerato una pressione positiva al raggruppamento. Tuttavia, non vi è ragione di credere che l'aggiustamento riduca il profitto di *ogni* miner a zero. Le conseguenza dell'assunzione precedente provocata dal solo aggiustamento della difficoltà, non sarebbe quella di avere *pochi* miner, ma di non averne *nessuno*. In realtà il fenomeno dell'aggiustamento non ha alcuna influenza sulla regolazione del profitto dei miner, esso controlla solamente il periodo di organizzazione. Senza aggiustamento, il profitto rimarrebbe inalterato mentre il periodo di organizzazione e quindi la varianza risponderebbero all'*hash rate* totale. E' la preferenza temporale, che determina il ritorno sul capitale a mercato, a regolare i profitti dei miner come in qualsiasi altro mercato.

Si consideri il caso in cui non vi sia cambiamento di prezzo. In questo caso non vi è ragione di attendersi un cambiamento nell'*hash rate* totale, né di aggiustamenti della difficoltà, e si può concludere che il miner medio generi un ritorno sul capitale a mercato. In altre parole qualsiasi numero di miner indipendenti *può* competere indefinitamente (ipotizzando l'assenza *effettiva* di pressioni al raggruppamento).

Si consideri anche il caso di cambiamenti di prezzo, sia gli aggiustamenti nella difficoltà che le fluttuazioni nella ricompensa influenzano la profittabilità del miner alla stessa maniera. Un aggiustamento della difficoltà e/o un *halving* non sono quindi più importanti per un miner rispetto ad una equivalente fluttuazione di prezzo, e inoltre esibiscono una maggiore prevedibilità. **Ci si attende che i ritorni dei miner eguaglino sempre, in media, i tassi di ritorno sul capitale a mercato**. Di conseguenza la teoria è costruita su una assunzione invalida.

La teoria prende inoltre in considerazione l'eventualità che la ricompensa possa essere insufficiente per remunerare i miner per il livello di difficoltà subito dopo un *halving*. Per questo motivo essi potrebbero optare per ridurre l'*hash rate*, quindi estendendo il tempo delle conferme finché, le *fee* non siano cresciute, il prezzo aumenti e/o la difficoltà si aggiusti verso il basso. Tuttavia le *fee* ed il prezzo sono determinate su un mercato e possono certamente crescere a qualsiasi livello le persone siano disposte a spendere. Non vi è modo di sapere quale livelli il mercato sosterrà. Tuttavia i primi due più importanti eventi di *halving* sono passati senza interruzioni (n.t.d. così come il terzo halving). Le *fee* ed il prezzo sono saliti entrambi, spingendo un significativo incremento dell'*hash rate* totale. Poiché i prossimi *halving* daranno luogo all'equivalente di un riduzione esponenzialmente *più piccola* della ricompensa, non vi è ragione di credere che gli eventi futuri saranno più interessanti di quelli passati.

Titolo originale: Halving Fallacy

Indice

Fallacia dell'Accumulo

Esiste una teoria secondo la quale un maggiore livello di accumulo produca un maggiore livello di sicurezza in una moneta. Questa teoria è simile a quella descritta ne la Fallacia del *Dumping* ma non è necessariamente basata su un evento di separazione.

Il supposto beneficio in termini di sicurezza dato da un più elevato livello di accumulo deriva dalla teoria secondo la quale un possessore possa influenzare la validazione e possa agire in modo da impedire all'economia di accettare ciò che i possessori stessi, collettivamente, considerano moneta invalida. Tuttavia i possessori non agiscono fino a quando non scambiano unità per un qualche bene e, in questo caso, è il commerciante ad applicare le regole di consenso. **La possibilità che i possessori agiscano all'unisono non aumenta questo livello di controllo minimo**. La teoria è quindi invalida.

Un incremento può essere descritto solamente se riferito a qualche livello base. Se una persona è convinta che un più elevato livello di sicurezza derivi da un maggiore accumulo collettivo, la teoria afferma che la persona possa decidere di accumulare più di ciò che altrimenti sarebbe definito ottimale per loro (i.e. il livello base di accumulo di quella persona). Questo modo di agire si configura come un costo individuale a fronte di un presupposto beneficio socializzato. In altre parole la teoria dipende da un comportamento economicamente irrazionale, anche nel caso in cui il beneficio sia reale in termini di sicurezza, ed è per ciò invalida.

La teoria implica che un numero minori di scambi effettuati con la moneta produca un maggiore sicurezza. Ciò è il contrario di quanto avviene in realtà. Come mostrato nel Modello di Sicurrezza Qualitativo, l'applicazione delle regole di consenso richiede degli scambi continui. Il prezzo di un'unità della moneta sotto forma di un altro bene o moneta è arbitrario, ma può salire temporaneamente se gli individui sono indotti a perseguire nella fallacia. Il beneficio di questo aumento va a favore dei proprietari già esistenti. La teoria secondo la quale il prezzo possa solamente salire è collegata ad un errore di tipo speculativo affrontato nella Fallacia Lunare. Anche un dimostrabile e perpetuo aumento generale del prezzo non porterebbe a confermare questa teoria, in quanto essa è

collegata solamente ad un fenomeno di aumento relativo e temporaneo causato da decisioni finanziarie individuali sub-ottimali.

Titolo originale: Hoarding Fallacy

Indice

Fallacia del Mining Ibrido

Esiste una teoria secondo la quale la combinazione di *proof-of-work* (PoW) e di *proof-of-stake* (PoS) nel mining offra un maggiore livello di sicurezza rispetto alla sola PoW. La teoria implica che una maggioranza di possessori di moneta possa mitigare "i cattivi comportamenti" dei miner PoW.

In mancanza di un miner che detenga la maggioranza dell'*hash power*, non vi è nulla da mitigare. Quindi la teoria si fonda sull'aumentare il costo per contenere un regime di censura. Questa considerazione si basa sull'assunzione, di per sé insostenibile, che i miner PoW non siano anche miner PoS.

Il costo del mining ibrido è il costo combinato del lavoro e dello *staking*, inclusivi del costo del capitale. Il ritorno sull'investimento nel mining eguaglia necessariamente il costo del capitale, come conseguenza della competizione. Quando il mining è profittevole, il costo del capitale non contribuisce alla sicurezza. **Realizzare uno *stake* maggioritario non è più costoso di ottenere una maggioranza dell'*hash power***. La teoria è quindi invalida.

In un modello nel quale un detentore di una quota maggioritaria di *stake* può impedire la conferma di blocchi costruiti con PoW altrimenti validi, il censore, una volta che tale maggioranza è raggiunta, non può essere destituito. Questo sistema è fondamentalmente una moneta basata su PoS che manca di resistenza alla censura e dove la parte di PoW non fornisce alcuna sicurezza addizionale.

Titolo originale: Hybrid Mining Fallacy

Indice

Fallacia della Moneta Ideale

E' stata avanzata una proposta secondo la quale l'esistenza di un "indice di valore" internazionale e non politico (i.e. di tipo obiettivo) porterebbe le persone ad obbligare gli stati ad "agganciare" le loro monete all'indice, eliminando quindi l'inflazione di prezzo. E' stato anche suggerito che Bitcoin rappresenti questo tipo di indice e che accelererebbe il processo verso questo scenario.

Il tipo di leva immaginata in questo contesto è rappresentato dalla possibilità di abbandonare certe monete di stato in favore di altre. Si creerebbe uno spostamento dalle monete a più elevata inflazione a quelle a più bassa inflazione basandosi sul confronto con l'indice. Ne consegue che gli stati dovrebbero allineare via via in misura maggiore i loro tassi di inflazione all'indice. Il risultato è che le monete di stato raggiungerebbero "asintoticamente" la condizione di Moneta Ideale rappresentata dall'indice.

La Moneta Ideale è la moneta di stato avente un tasso di inflazione di prezzo pari a zero:

> ... non esiste un tasso di inflazione ideale che dovrebbe essere selezionato e scelto come obiettivo ma piuttosto il concetto ideale sarebbe quello che contempli necessariamente un tasso nullo di ciò che è chiamato inflazione.

La formulazione della teoria è sia variegata che limitata (la prova è lasciata al lettore). Tuttavia il riassunto riportato sopra contiene tutti gli elementi fondamentali. Data la presenza di queste limitazioni può essere utile cominciare l'analisi con assunzioni generose. Assumiamo che esista una moneta che possa esprimere un valore oggettivo (si veda per confronto la teoria soggettiva del valore), che Bitcoin sia tale moneta e che le persone siano generalmente in grado di confrontare il valore di Bitcoin con quello della altre più importanti monete di stato. Assumiamo anche che, nonostante l'apparente contraddizione, le persone usino Bitcoin negli scambi (la fonte dell'indice) *e* che preferiscano contemporaneamente l'uso delle monete di stato (una premessa necessaria).

Se assumiamo anche che le persone non siano vincolate dalle leggi sul corso legale e che l'uso di monete tra loro in competizione abbia successo nel forzare gli stati ad "agganciare il valore obiettivo" di Bitcoin, allora il signoraggio verrebbe

eliminato. Tuttavia, come mostrato nella Proprietà di Stabilità, lo scopo della moneta di stato (fiat) è quello di raccogliere la rendita di signoraggio che è una tassa a tutti gli effetti. Dando per valide le assunzioni riportate sopra, la Moneta Ideale rappresenta il superamento della moneta di stato. **La proposta, quindi, non prende in considerazione la ragione per cui la moneta fiat di stato esiste in primo luogo**.

Si riconsiderino ora le assunzioni. La moneta fiat (n.d.t. di stato) necessita dell'esistenza delle leggi sul corso legale e per questo la Legge di Gresham governa sempre tale ambito:

> Questi esempi mostrano che, in assenza leggi efficaci a tutela del corso legale, la Legge di Gresham funziona al contrario. Se viene data la scelta di quale moneta accettare, le persone transeranno con la moneta che essi ritengono di maggior valore nel lungo termine. Tuttavia, se non viene data loro la possibilità di scegliere e viene loro imposto di accettare tutte le monete, buone o cattive che siano, essi tenderanno a tenere in loro possesso la moneta di maggior valore percepito e spendere la moneta cattiva verso qualcun altro. In breve, in assenza di leggi sul corso legale, il venditore non accetterà altro che moneta di un certo valore (buona moneta), mentre l'esistenza di leggi sul corso legale faranno sì che il compratore offra solo moneta con il più basso valore-merce (moneta cattiva) in quanto il creditore è obbligato ad accettare questa moneta al valore nominale.

La proposta assume scorrettamente che si applichi la Legge di Thiers. Se ciò fosse vero le persone non userebbero la moneta fiat (di stato). Essa inoltre ignora l'esistenza del controllo sul cambio in valute estere, che esiste specificamente per evitare la fuga di capitali. Tale controllo si acuisce all'aumentare della fuga di capitali in modo da preservare il gettito fiscale. Infine, tale controllo limita materialmente il processo di scoperta del prezzo dell'indice stesso, rendendolo meno utile di quanto immaginato nella costruzione della proposta.

La proposta non offre alcuna spiegazione razionale su come le persone saranno in grado di spostarsi tra le monete di stato a fronte di tali controlli. Essa assume inoltre che le persone saranno maggiormente in grado di *riconoscere* la tassa del signoraggio grazie alla presenza dell'indice e della loro abilità nell'effettuare comparazioni, e che quindi saranno in grado di controllare efficacemente l'appetito dello stato nei confronti di questa tassa. Dato l'utilizzo universale dell'oro come indice obiettivo confrontabile prima dell'evoluzione su scala globale della moneta fiat, non è chiaro come le valute fiat abbiano potuto prendere piede se assumiamo che le persone possano reagire secondo le modalità descritte.

Esiste un'ipotesi secondo la quale il Bitcoin sia un indice obiettivo mentre l'oro non lo sia. Questa considerazione è basata sull'offerta di tipo inflazionario dell'oro al contrario dell'offerta fissa di Bitcoin. Questo fatto, a sua volta, presume che l'inflazione monetaria implichi una moneta instabile mentre una offerta fissa implichi una moneta stabile. Come mostrato nella Proprietà di Stabilità,

entrambe le monete sono stabili. Il ragionamento non riesce a riconoscere che il valore, per come indicato dall'indice, è influenzato sia dall'offerta che dalla dalla domanda. La domanda di oro è stabilizzata dall'inflazione e la domanda di Bitcoin è stabilizzata dalle *fee*.

Questa teoria è di conseguenza invalida. O le monete fiat di stato cesseranno di esistere o permetteranno sempre la riscossione della tassa di signoraggio implicata dalla loro esistenza. Gli stati rinunceranno alla tassa solo sotto estrema pressione e, in tal caso, solo per breve tempo. Al limite, la "moneta ideale" sarà Bitcoin e non potrà essere scambiata liberamente con le monete di stato (nel caso esse rimanessero in circolazione).

Titolo originale: Ideal Money Fallacy

Indice

Fallacia del Mining Impotente

Esiste una teoria secondo la quale i miner non detengano alcun potere. Tale argomentazione è distinta rispetto alla Fallacia della Proof of Work ad essa strettamente collegata. La teoria si basa sull'assunzione secondo la quale i miner sono soggetti a differenti pressioni economiche che impediscono loro di sostenere attacchi efficaci. Questa teoria porta le persone a credere che il mining possa esistere in forma fortemente raggruppata fino a quando i commercianti non vengano centralizzati, ovvero fino a quando l'economia può controllare il mining e rendendo quindi il sistema sicuro. La conseguenza di questa teoria invalida è che essa non da importanza all'insicurezza causata dal raggruppamento.

La teoria ritiene che, se la maggioranza dell'*hash power* praticasse una doppia spesa, allora necessariamente i commercianti aumenterebbero la profondità di conferma richiesta, aumentando il costo degli attacchi successivi. Ad un certo punto verrebbe raggiunto un equilibrio secondo il quale una più grande profondità sarebbe sufficiente per effettuare in sicurezza uno scambio. Poiché questo comportamento precluderebbe la doppia spesa in termini complessivi, sempre secondo la teoria, non ci sarebbe alcun vantaggio a sostenere questo tipo di attacco. La teoria ammette che tali attacchi possano avvenire, ma non abbastanza frequentemente per ridurre sostanzialmente l'utilità.

La teoria afferma inoltre che un miner non può non selezionare le transazioni con le *fee* più elevate, in quanto ciò ridurrebbe la relativa ricompensa, arricchendo gli altri miner. Questo si presume possa portare ad una perdita della maggioranza dell'*hash power* e quindi all'impossibilità di continuare l'attività di mining. Questo aspetto della teoria implica che i miner non possano effettivamente mettere in atto azioni di censura.

La teoria considera anche che il *selfish* mining da parte della maggioranza dell'*hash power* sia un'azione perseguibile, ma che in assenza di doppia spesa e di azioni di censura, non ci siano conseguenze avverse per l'economia. In questo caso, tale maggioranza diventa semplicemente il solo ed unico miner in quanto gli altri non sono in grado di ottenere le ricompense. Nonostante l'assenza di

competizione, l'*hash rate* ed il livello delle *fee* vengono mantenuti dalla sempre incombente *possibilità* di competizione.

Tuttavia i miner ed i commercianti sono partner commerciali impegnati volontariamente in una attività mutualmente vantaggiosa. Come esplorato nella Fallacia del Bilanciamento del Potere, nessuno dei due soggetti può controllare l'altro ed il prezzo rappresenta la risoluzione di tutte le preferenze. Ciò sembrerebbe dare supporto alla teoria, tuttavia la teoria stessa è in realtà un ragionamento ingannevole in quanto **non affronta in alcun modo la minaccia**. Bitcoin è stato progettato per difendersi da forze *non* di mercato, in particolare dallo stato. Le forze di mercato non rappresentano mai una minaccia per il mercato stesso.

Il raggruppamento di hash power porta a ridurre fortemente la sicurezza in quanto gli stati possono semplicemente cooptare tale aggregazione. Ma gli stati possono anche costruire i loro centri di mining per ottenere lo stesso effetto. Di conseguenza Bitcoin richiede sia di una significativa quantità di hash power *sia* che tale forma di potere sia distribuita tra le persone che sono disponibili e capaci a correre il rischio del controllo dello stato.

Lo stato è un attore economicamente razionale. L'inflazione è profittevole per l'autorità emittente della valuta. L'uso diffuso di Bitcoin impedirebbe agli stati di riscuotere efficacemente la tassa dell'inflazione. Gli attacchi condotti dallo stato rappresentano quindi un fenomeno atteso, e attacchi di tipo analogo sono di fatto ordinari. E' praticamente inevitabile che lo stato vada a sussidiare questi attacchi, ma anche la sola possibilità di tale circostanza porta ad invalidare la teoria.

Titolo originale: Impotent Mining Fallacy

Indice

Fallacia dell'Inflazione

Le regole di consenso di Bitcoin hanno dato luogo ad un periodo di inflazione monetaria. Esiste una teoria secondo la quale ciò causerebbe la perdita di potere d'acquisto della moneta stessa. Come mostrato nel Principio di Inflazione, **nessun cambiamento del potere d'acquisto si può verificare dall'aumento di offerta** di una moneta di mercato. La teoria è quindi invalida.

Il fatto che Bitcoin non sia inflazionario in termini di prezzo implica che i possessori non "sussidiano" il mining. Il capitale consumato dai miner è di loro stessa proprietà (rappresenta un investimento), la moneta creata è il loro prodotto ed il ritorno sull'investimento (l'interesse) è conseguenza dell'aumento di domanda che loro stessi provvedono a soddisfare - compensando il costo opportunità di impegnare il loro capitale nel tempo.

Titolo originale: Inflation Fallacy

Indice

Fallacia della Qualità dell'Inflazione

Esiste una teoria secondo la quale l'inflazione dei prezzi causata dal signoraggio porti alla produzione di beni di "qualità" più bassa e/o meno durevoli. La durevolezza è uno dei numerosi tipi di qualità cui una persona può attribuire valore confrontando un bene con un altro. **La teoria dà necessariamente per scontato che il valore sia oggettivo contraddicendo quindi la teoria soggettiva del valore**. Per questa ragione la teoria non è valida.

Non esiste infatti una relazione verificabile tra il numero di unità di una moneta richieste per scambiare un bene e le qualità di un bene che una persona possa preferire. Maggiore *ricchezza* (che dipende dalla percezione individuale, in quanto il valore è soggettivo) implica una più bassa preferenza temporale, come previsto dalla teoria dell'utilità marginale. Tuttavia, ipotizzando una errata percezione di un aumento di ricchezza, la più bassa preferenza temporale non implica una preferenza per beni di "qualità" più bassa. Essa implica solamente una maggiore inclinazione a dare in prestito una più grande porzione del proprio capitale.

Rothbard commette questo spiacevole errore in "Cosa ha fatto lo Stato ai nostri Soldi", un errore che continua ad essere perpetuato.

> La qualità del lavoro diminuirà a causa dell'inflazione per una ragione più sottile: le persone si appassioneranno agli schemi di "arricchimento facile", apparentemente comprendendoli come caratteristici del periodo di prezzi sempre crescenti, e spesso disprezzando l'onesto sforzo (n.d.t. impiegato nel lavoro).

Si presume, e ciò viene fatto sicuramente anche da Rothbard, che le persone preferiscano *sempre* diventare ricche prima che più tardi, come implicato dall'assioma della preferenza temporale. E, come mostrato nell'ipotesi di Fisher, nella misura in cui l'inflazione di prezzo è predicibile, questa viene compensata nel tasso di interesse reale. Nella misura in cui ciò non sia predicibile la congettura di Rothbard non può essere applicata.

Il signoraggio è una tassa e questo rende le persone più povere. Essere poveri *aumenta* la preferenza temporale, l'effetto opposto rispetto a quello descritto

nella teoria. Tutte le tasse - per come è strutturato il loro reale funzionamento ed obiettivo - trasferiscono, senza consenso, la proprietà di alcune persone ad altre persone. Come Rothbard stesso, approfondisce nel suo più formale "*Man, Economy and State*", la struttura di una tassa è economicamente irrilevante.

> Per tutte queste ragioni, l'obiettivo di uniformità della tassazione è impossibile da raggiungere. Non è semplicemente difficile da ottenere in pratica; è concettualmente impossibile e auto-contraddittorio.

Di conseguenza non può essere mostrato che il signoraggio stesso renda le persone più povere di altri tipi di tasse alle quali potrebbe presumibilmente sostituirsi. Solamente un incremento netto della tassazione porta ad una riduzione della ricchezza.

Titolo originale: Inflationary Quality Fallacy

Indice

Fallacia dell'Arbitraggio Giurisdizionale

Esiste una teoria secondo la quale, poiché è improbabile che tutti gli stati si uniscano in una messa al bando di Bitcoin, la moneta sopravviverebbe grazie allo spostamento del mining e di altre attività negli stati che non vi aderissero.

Dal punto di vista dell'autorità emittente, coloro che non rispettassero tale divieto risulterebbero operare nel mercato nero. Sempre da questo punto di vista, uno stato che violasse tale proibizione verrebbe considerato uno stato canaglia. Una messa al bando è una semplice azione politica contro la quale Bitcoin non offre alcuna protezione.

Vi è un fallacia collegata che afferma che questa azione sarebbe praticamente impossibile da realizzare nel caso in cui Bitcoin goda di popolarità. Ciò si si basa sull'idea che Bitcoin sia reso sicuro dal voto, cosa che riduce il suo modello di sicurezza a quello della moneta di stato, eliminando di fatto la *value proposition* di Bitcoin.

Per definizione, le operazioni nel mercato legale vengono quindi eliminate da una messa al bando. La teoria quindi implica che Bitcoin è essenzialmente reso sicuro dalla protezione degli stati canaglia. Ciò si riduce ad un modello di sicurezza garantito attraverso il voto. Inoltre va considerato che gli stati più potenti hanno numerosi strumenti di tipo coercitivo per forzare l'azione degli altri stati, fino al punto di ingaggiare un conflitto aperto contro di essi. Questi strumenti sono comunemente usati in numerose guerre, come quelle condotte contro la droga, il riciclaggio di denaro ed il terrorismo. Una messa al bando di Bitcoin potrebbe utilizzare come giustificazione ciascuno di questi conflitti internazionali in corso.

Tuttavia, Bitcoin è specificamente progettato per operare senza il permesso di alcuno stato. Il suo funzionamento continuo come moneta del mercato nero potrebbero portare uno o più stati a provare a sopprimerlo attraverso la censura. Sebbene tale azione possa essere intrapresa da un singolo stato, è pratica comune che gli stati collaborino per preservare il loro potere di tassazione delle loro monete. Questo è lo scopo del Fondo Monetario Internazionale.

Questa azione può essere intrapresa più efficientemente da una singola entità geografica. In questo scenario gli stati canaglia non offrono alcuna difesa, non solo perché essi stanno rinunciando beneficio derivante dalla tassazione delle loro monete, ma perché stanno donando i rispettivi proventi per resistere alla censura. **Non si può assumere che gli stati canaglia possano sopraffare l'autorità censurante e inoltre, ogni dipendenza da essi riduce Bitcoin ad una moneta resa sicura dalla politica**. Per questa ragione la teoria è invalida.

Titolo originale: Jurisdictional Arbitrage Fallacy

Indice

Fallacia Lunare

Vi è una teoria secondo la quale l'accumulare bitcoin garantisca un profitto perpetuo (n.d.t. *to the moon!*). La teoria è basata sulle seguenti leggi economiche.

- Una moneta è meglio di due monete (Legge di Metcalfe).
- La moneta migliore scaccia le altre monete (Legge di Thiers).
- Con un'offerta fissa, il prezzo cresce con la domanda (Legge della Domanda e dell'Offerta).
- L'incremento potenziale della domanda è illimitato (lo scambio è un fenomeno a somma positiva).

L'accumulo è un fenomeno di natura puramente speculativa, con tutti i ritorni che costituiscono un profitto o una perdita. La moneta non viene data in prestito ad una controparte in cambio di un interesse e in questo modo è sempre disponibile per uno scambio di unità, un beneficio che va a compensare l'interesse a cui si è rinunciato.

Un corollario della teoria afferma che non è necessario alcun investimento nella produzione per ricavare un profitto da essa. L'impiego di capitale è necessario in ogni forma di produzione. I prestatori (investitori) guadagno interesse in cambio del tempo passato senza detenere il capitale nella loro disponibilità. La produzione è la fonte dello scambio commerciale e di conseguenza tutte le attività economiche derivano dall'investimento. Un accumulo è definito dall'assenza di consumo impiegato nella produzione. Se tutte le persone accumulassero il loro capitale non ci sarebbe nulla da scambiare e di conseguenza non ci sarebbe alcuna domanda per la moneta. Sembra che tale teoria sia irrazionale poiché supporta l'idea che Bitcoin sia in realtà la Magica Moneta di Internet.

La teoria non incorpora la Proprietà di Stabilità di Bitcoin ed è perciò invalida.

Titolo originale: Lunar Fallacy

Indice

Fallacia dell'Effetto Network

Esiste una teoria secondo la quale l'utilità creata da un'economia vari con il quadrato del numero dei commercianti appartenenti ad essa, sotto l'assunzione che ciascuno dei commercianti offra lo stesso valore di beni o servizi per mezzo di una sola moneta. La teoria rappresenta un'applicazione della Legge di Metcalfe.

Questo implica che una separazione in parti uguali dell'economia riduca l'utilità combinata della stessa della metà. Ad esempio, se 20 commercianti hanno un'utilità pari a 400 allora 2 reti costituite da 10 commercianti ciascuna hanno un'utilità di 200.

Tuttavia l'abilità di scambiare ciascuna unità di una moneta con un'altra porta l'utilità delle due economie verso un'economia ibrida. A causa del costo di conversione **la situazione ibrida ha un'utilità minore di quella che avrebbe un'economia basata su una singola moneta, ma questo non può essere confrontabile con la perdita intera di una delle due economie, a meno che il costo di conversione non sia illimitato**. La teoria è quindi invalida.

Titolo originale: Network Effect Fallacy

Indice

Fallacia del Dilemma del Prigioniero

Esiste una teoria secondo la quale, ogni stato, individualmente, se messo di fronte alla scelta di unirsi ad una messa al bando di Bitcoin affronti un dilemma del prigioniero. Una messa al bando significativa implica che uno o più stati (identificati come "prigioni") applicheranno delle sanzioni economiche (come minimo) ad altri stati (identificati come "prigionieri") che potrebbero potenzialmente adottare Bitcoin come valuta di riserva.

Assumiamo che i prigionieri che decidessero di adottare Bitcoin siano partner commerciali. In altre parole, l'uso di Bitcoin come moneta di riserva necessità di un partner con cui transare commercialmente.

L'utilità ordinale è implicata dal valore soggettivo. Non sono previste situazioni di parità, cosa che implica un dilemma in senso forte. Nel seguito sono prese in considerazione sia la configurazione di conoscenza simmetrica che quella asimmetrica.

Il risultato per l'adozione individuale di Bitcoin (**S**tupido):

- Sanzioni economiche.
- Nessun partner commerciale (che utilizza il Dollaro).
- Una valuta di riserva inutilizzabile (nessun partner commerciale).

Il risultato per una mutua adozione di Bitcoin (**R**icompensa):

- Sanzioni economiche.
- Sanzioni economiche al partner commerciale.
- Una valuta di riserva non tassata attraverso il signoraggio.

Il risultato per un'adozione individuale del Dollaro (**T**entazione):

- Nessuna sanzione economica.
- Sanzioni economiche al partner commerciale.
- Una valuta di riserva tassata attraverso il signoraggio.

Il risultato per una mutua adozione del Dollaro (**P**unizione):

- Nessuna sanzione economica.
- Nessuna sanzione economica al partner commerciale.
- Una valuta di riserva tassata attraverso il signoraggio.

Dilemma Simmetrico in forma Forte con Risultati in Relazione Ordinale

Brasile/Irlanda	Bitcoin	Dollaro
Bitcoin	R/R	S/T
Dollaro	T/S	P/P

Per essere considerato un dilemma del prigioniero deve valere la relazione `T > R > P > S` dove:

- `T > R` e `P > S` implicano che il Dollaro è la strategia dominante per ciascuno.
- `R > P` implica che la mutua adozione di Bitcoin è preferita alla mutua adozione del Dollaro.

Possiamo concludere che valga `P > S` in quanto una sanzione economica individuale implica che non vi sia nessun *settlement* internazionale e di conseguenza nessun beneficio dall'avere una riserva estera, e presumibilmente le sanzioni rappresentano una conseguenza non desiderabile.

Per determinare se valgano rispettivamente `R > P` e `T > R` risulta necessario impiegare un metodo oggettivo per confrontare il solo signoraggio con le sanzioni, in quanto le sanzioni rappresentano presumibilmente una conseguenza non desiderabile. Questa relazione d'ordine può essere ottenuta notando che l'oro non è soggetto né al signoraggio né alle sanzioni. **In altre parole l'oro fornisce i benefici descritti in precedenza per Bitcoin senza le sanzioni**. Tuttavia l'oro non è stato scelto come valuta di riserva (ed è stato abbandonato in favore del Dollaro), il che implica che l'utilizzo del Dollaro è preferito a quello dell'oro e di conseguenza anche all'utilizzo di Bitcoin. Per questa ragione nessuna delle strategie dominanti trova applicazione. Perciò non vi è alcun dilemma.

Dilemma Asimmetrico in forma Forte con Risultati in Relazione Ordinale

Brasile/Irlanda	Bitcoin	Dollaro
Bitcoin	Rr/Rc	Sr/Tc
Dollaro	Tr/Sc	Pr/Pc

Per essere considerato un dilemma del prigioniero deve valere la relazione `Ti > Ri > Pi > Si` dove:

- `Tr > Rr` e `Pr > Sr`
- `Tc > Rc` e `Pc > Sc`
- `Rr > Pr` e `Rc > Pc`

Se valgono tutte queste relazioni l'adozione individuale del Dollaro è preferita a Bitcoin e l'adozione mutua di Bitcoin è preferibile. Poiché queste relazioni sono le stesse valutate nello scenario simmetrico, non vi è alcun dilemma.

Altre assunzioni

La relazione tra oro e Bitcoin presume che i costi di *clearing*, di trasporto dell'oro e di conferma di Bitcoin siano trascurabili nel contesto del *settlement* internazionale. Il *clearing* richiede movimentazioni periodiche relative alla compensazione della bilancia dei pagamenti tra gli stati.

> ... ogni correzione degli sbilanciamenti economici verrebbe accelerata e normalmente non risulterebbe necessario aspettare fino al punto in cui risulterebbe necessario movimentare importanti quantità d'oro tra un paese e l'altro
>
> The Classical Gold Standard

Il Dollaro è stato preferito all'oro nonostante esso abbia peso simile, ingombro significativamente più grande, e che subisca l'applicazione del signoraggio. La relazione tra oro e Bitcoin presume che non vi sia alcuna distinzione tra i due in termini di volatilità e liquidità, sebbene l'oro superi oggettivamente Bitcoin in entrambi i campi. Poiché sia Bitcoin che l'oro sono monete stabili, non viene assunto alcun ritorno speculativo per entrambe. Si presume inoltre che altre proprietà monetarie relative all'oro, a Bitcoin e al Dollaro siano equivalenti o non rilevanti dal punto di vista di una valuta di riserva di stato.

Titolo originale: Prisoner's Dilemma Fallacy

Indice

Fallacia della Chiave Privata

Le chiavi private non rendono sicuro Bitcoin, esse garantiscono la sicurezza delle unità di Bitcoin. **Il controllo della chiave privata si applica alla sicurezza individuale, non alla sicurezza del sistema**. Chiunque controlli le chiavi è il proprietario, e Bitcoin garantisce la sicurezza di quel proprietario anche qualora le chiavi gli venissero rubate (n.d.t. quindi anche quella del ladro). La validazione decentralizzata protegge il consenso e la maggioranza dell'*hash power* protegge la conferma, ma la sicurezza della chiave privata è un problema del solo proprietario.

Titolo originale: Private Key Fallacy

Indice

Fallacia della Prova di Costo

In un mercato competitivo (libero), il mining di Bitcoin consuma sotto forma di costo ciò che viene creato come valore per il miner, sia sotto forma di emissione di nuove unità sia in termini di servizio di conferma. Ciò si verifica sia quando la ricompensa del blocco minato riflette completamente il ritorno del miner sia nelle altre situazioni.

La quantità di computazioni fornita nell'attività di mining si riflette probabilisticamente nella difficoltà del blocco. Ci si riferisce a questa operazione computazionale con il termine di lavoro. Una intestazione (*header*) di un blocco valido è una prova probabilistica che tale lavoro sia stato svolto. Ciò è alla base del termine "prova di lavoro" (*proof-of-work*).

La quantità di energia consumata nella produzione di un blocco non è dimostrabile, sia in maniera specifica sia probabilisticamente. L'efficienza energetica dei dispositivi di mining è variabile. L'intestazione di un blocco non riflette la "prova dell'energia consumata". Queste affermazioni rappresentano delle approssimazioni.

Il ritorno economico di un miner sulla produzione di un blocco non è riflesso completamente nel blocco stesso. Minare le proprie transazioni implica che la totalità delle *fee* non è necessariamente riflessa nel blocco, come accade per le *fee* a parte in generale. Un miner può introdurre transazioni aventi *fee* arbitrariamente alte o basse. La ricompensa del blocco non rappresenta una "prova di ricompensa". Queste affermazioni rappresentano delle assunzioni.

In un mercato libero, il ritorno sul mining è il valore della sua ricompensa - che quest'ultima si rifletta sul blocco o meno - e le *fee* guadagnate sono determinate dalla domanda di effettuare transazioni. Questa è una conseguenza della competizione. In questo caso è corretto considerare un'intestazione di un blocco come una "prova di costo", tuttavia l'ammontare di tale costo rimane sconosciuto. Tutto ciò che è possibile sapere è che il miner ha guadagnato un tasso di ritorno sul capitale.

Tuttavia, nel caso del monopolio di stato, il prezzo non è controllato dalla competizione. Un monopolio può far pagare qualsiasi prezzo il mercato sia disposto a sopportare. Il costo di applicazione del monopolio viene pagato dal contribuente. Il premio sul prezzo rappresenta un'altra tassa pagata dal consumatore. Il valore di questa tassa si trasferisce al monopolio.

Nel caso di un'azione di censura di Bitcoin sponsorizzata dallo stato, sia il costo di applicazione sia il premio sul prezzo (in termini di *fee*) rappresentano le tasse di uno scenario di monopolio. Il livello delle *fee* può superare il tasso di mercato e l'applicazione di tale aumento viene sussidiata dalle tasse. Il monopolio sul mining può dar luogo al signoraggio come avviene in qualsiasi altra moneta di monopolio. L'intestazione del blocco continua a fornire una prova di lavoro ma non più una prova di costo.

Allo stesso modo, l'esistenza di un'unità valida di moneta di monopolio fornisce una prova sufficiente di un costo reale di produzione, ma non fornisce alcuna prova che l'autorità emittente non abbia incassato un premio di monopolio su questo costo. Esiste a questo proposito una teoria secondo la quale il costo di produzione di Bitcoin "non sia falsificabile", mentre la rendita di signoraggio di una moneta di stato rappresenti un "costo di falsificazione". Come è stato dimostrato, **Bitcoin è soggetto anch'esso al signoraggio** rendendo quindi la teoria invalida.

Tutti i beni hanno costi di produzione reali. Il monopolio esiste per innalzare il prezzo al di sopra del costo. Benché Bitcoin sia resistente alla censura, l'efficacia di tale resistenza non è garantita.

Titolo originale: Proof of Cost Fallacy

Indice

Fallacia della Prova di Memorizzazione

E' stata formulata una proposta secondo la quale una prova di memorizzazione (*proo-of-memory* - PoM) possa sostituire una frazione del costo energetico della *proof-of-work* (PoW) con un costo hardware, anche facendo affidamento sui dispositivi di memorizzazione esistenti. Come mostrato nella Fallacia dello Spreco di Energia, un livello di sicurezza costante richiede una spesa ininterrotta e costante. Di conseguenza questo sistema richiederebbe un equivalente livello di consumo di hardware per compensare ciascuna riduzione del costo energetico. **In altre parole il consumo totale di energia non può essere ridotto, può essere solo trasferito alla fabbricazione, al funzionamento e allo smaltimento di hardware**.

Nel dicembre 2017 il costo energetico annualizzato stimato dell'energia consumata nel mining Bitcoin è stato di 1,628,000,000 $ basato sull'approssimazione di 32.56 TWh consumati ad un costo di 0.05 $/kWh. Contemporaneamente questo livello di costo è uguale al consumo di 32'560'000 TeraByte di memoria ad un costo medio di 50 $ per dispositivo. L'utilizzo dei dispositivi esistenti inutilizzati riduce il costo unitario degli stessi e quindi innalza per confronto il quantitativo richiesto.

Vale la pena analizzare il comportamento economico di un sistema teorico nel quale la PoM è determinata da un aggregato esistente di dispositivi di memorizzazione (a costo nullo) senza limite alla vita utile o costi operativi. Poiché in questo caso specifico il costo del mining è posto pari a zero, le ricompense si trasferirebbero senza alcuna spesa in proporzione alla memoria posseduta (assumendo nessuna pressione di raggruppamento). Ogni aumento delle *fee* medie va ad aumentare la ricompensa per la memoria. Il capitale investito è nullo e quindi il tasso di ritorno sarebbe perpetuamente infinito. Nonostante l'ipotesi di incentivo illimitato, l'assunzione di espansione nulla preclude ogni forma di competizione. Ma poiché la prova è esternalizzata, la competizione non può essere ristretta. In un sistema reale la fabbricazione di hardware si espande perpetuamente per un dato livello di *fee* , e questa espansione accelera all'aumentare del livello delle *fee*.

La *proof-of-memory* è uguale alla *proof-of-work* in termini del consumo di risorse e non vi è ragione di assumere alcuna riduzione della componente energetica in tale costo. L'hardware si comporta come una prova di immagazzinamento di energia (una batteria) che rappresenta l'energia che è stata spesa in maniera dimostrabile per la sua fabbricazione. Tutto ciò che è stato mostrato in questa fallacia è un argomento di facciata analogo a quello delle macchine elettriche con batteria "a zero emissioni".

Titolo originale: Proof of Memory Fallacy

Indice

Fallacia della Prova di Proprietà

Esiste una teoria secondo la quale la titolarità di una proprietà può essere protetta attraverso l'adozione di un registro immutabile dei titoli di proprietà, efficace sia contro la perdita del titolo sia contro il Rischio di Custodia.

Poiché il titolo di proprietà non è di per sé la proprietà da esso stesso rappresentata, il controllo della proprietà resta affidato al custode verso il quale ha valenza il titolo di proprietà. Un custode ha la possibilità di restituire o trattenere la proprietà e quindi egli si configura come una terza parte fidata. L'annullamento di un titolo di proprietà da parte del custode è sempre mitigato dalla firma del custode, sia in forma crittografica o di diversa natura, dove il compito di far valere il titolo viene lasciato al suo possessore.

La teoria afferma che un registro immutabile dei titoli fornisce protezione contro la perdita del titolo da parte del suo possessore, in quanto nessun altro individuo avrebbe un interesse in tale perdita. Tuttavia, per riscattare il titolo, il suo possessore deve fornire una prova di proprietà al custode. Questo richiede che il possessore non perda il segreto che fornisce la prova della sua proprietà. Come tale la protezione del titolo contro la perdita non è affatto mitigata, cambia solamente forma. La teoria è quindi invalida sulla base della prevenzione dalla perdita.

Conservare un riferimento solido al titolo può ridurre la dimensione, e quindi il costo, della sua inalterabile conservazione. Il titolo può essere costruito nella forma di un contratto in forma leggibile dalle persone o da una macchina, e referenziato attraverso un hash non invertibile. In ogni caso, è richiesta la validazione e l'esecuzione del contratto al fine di trasferire la proprietà dal custode. Di conseguenza un contratto referenziato sopperisce al rischio di perdita con dati addizionali, ovvero con il contratto stesso.

Come mostrato nel Principio della Condivisione del Rischio, alla base della sicurezza ci sono sempre le persone. Le persone possono agire collettivamente per proteggere l'immutabilità di una moneta e di conseguenza possono anche proteggere i dati di titolarità associati al controllo della moneta. Tuttavia, il

custode è una terza parte fidata. Titoli di tipo immutabile non mitigano in nessun modo attacchi diretti compiuti contro il custode, o dal custode stesso. Quando il custode è lo stato o un'entità assoggettata al suo controllo, il titolo non offre alcuna sicurezza contro la sostituzione dell'autorità dello stato a qualsiasi prova di titolarità. La teoria è quindi anche invalida sotto il profilo del fallimento del custode.

Bitcoin come moneta funziona senza custodia (è *non-custodial*). Le sue unità non rappresentano un asset custodito da una terza parte fidata. La moneta è scambiata direttamente tra cliente e commerciante. In questo senso *tutti i commercianti* sono i custodi del valore di Bitcoin. **La fallacia della blockchain (n.d.t. che si identifica con la fallacia della prova di proprietà ndt), nasce da una concezione errata del modello di sicurezza di Bitcoin, che attribuisce la sua protezione alla tecnologia e non alla sua distribuzione tra i commercianti**. Il termine "tecnologia blockchain" rafforza questo errore poiché implica che sia principalmente la struttura dati di Bitcoin a renderlo sicuro.

Titolo originale: Proof of Ownership Fallacy

Indice

Fallacia della *Proof of Stake*

La sicurezza della conferma richiede che una persona abbia l'autorità per ordinare le transazioni. Bitcoin assegna periodicamente questa autorità al miner che produce la più grande prova di lavoro (*proof-of-work*). Tutte le forme di lavoro si riducono necessariamente al consumo di energia. E' fondamentale che questo tipo di prova sia indipendente dalla storia della catena. Possiamo riferirci ad essa come ad una prova "esterna".

Ogni altra fonte di autorità deputata all'ordinamento è, di conseguenza, dipendente dalla storia della catena; a quest'ultima possiamo riferirci come ad una prova "interna". Esiste una teoria secondo la quale la *proof-of-stake* (PoS) costituisce un'alternativa comparabile alla *proof-of-work* in termini di sicurezza della conferma. E' vero che sia la PoS che la PoW delegano il controllo dell'ordinamento delle transazioni ad una persona che ha il controllo sul più grande quantitativo di una certa forma di capitale.

La distinzione tra le due prove è basata sull'impiego del capitale sottostante. La PoW esclude il capitale che non può essere convertito in lavoro, mentre la PoS esclude tutto il capitale che non può portare all'acquisizione di unità della moneta. Tale differenza ha una conseguenza essenziale per la sicurezza.

Ne il Principio degli Altri Mezzi viene mostrato come la resistenza alla censura dipenda dalle persone che pagano i miner per sopraffare il potere del censore. **Vincere la censura non è possibile in un sistema PoS, in quanto il censore ha acquisito una partecipazione (*stake*) maggioritaria e non può essere deposto**. Per questa ragione i sistemi PoS non sono resistenti alla censura e la teoria è quindi invalida.

Titolo originale: Proof of Stake Fallacy

Indice

Fallacia della *Proof of Work*

I commercianti acquistano servizi di mining che soddisfano le loro regole per una *fee* soddisfacente. Esiste una teoria secondo la quale i servizi di mining siano entità subordinate in questo scambio. Questa subordinazione è talvolta descritta come "asimmetria" o "regola degli utenti". Questa teoria porta le persone a credere che il mining possa essere fortemente raggruppato a condizione che i commercianti non siano centralizzati poiché, in questo caso, sarebbe l'economia a controllare il comportamento del mining, rendendo il sistema sicuro. La conseguenza di questa teoria invalida è quella di soprassedere completamente sull'insicurezza generata dal raggruppamento.

I miner controllano la selezione delle transazioni, mentre i commercianti controllano la proprietà offerta nello scambio. Se una parte dell'economia è insoddisfatta con la selezione operata dai miner, essa può offrire in vendita la sua proprietà utilizzando una moneta separata avente diversa regola di lavoro che rende obsoleti tutti i dispositivi di mining. Ciò viene tipicamente descritto come un *hard fork* della *proof-of-work*.

Secondo questa teoria i miner incorrerebbero in una perdita catastrofica dovuta all'impossibilità di recuperare l'investimento di capitale impiegato in hardware altamente specializzato. L'*hard fork* potrebbe includere un aggiustamento della difficoltà, che permetterebbe la prosecuzione dell'attività di conferma nonostante il calo significativo dell'*hash rate*. Grazie alla difficoltà più bassa e alla presunta mancanza di hardware specializzato, un numero maggiore di individui sarebbero in grado di unirsi all'attività di mining. Questo introdurrebbe nuovi miner nel settore e ridurrebbe l'aggregazione.

E' stato detto che l'abilità da parte dell'economia di imporre una perdita di capitale sui partner commerciali sia una asimmetria unica nel suo genere se confrontata con altri mercati. Ad esempio, una comunità di acquirenti di mele non può semplicemente "distruggere" i frutteti di tutti i suoi fornitori. La teoria **non riconosce che non vi è alcuna asimmetria in uno scambio commerciale**. Se tutti tutti gli acquirenti di mele decidono di non comprare più mele dai frutteti esistenti significa che essi hanno certamente questo potere.

Analogamente i frutteti hanno la possibilità di non vendere. Il prezzo rappresenta la continua risoluzione di questa tensione. Questa è la stessa esatta dinamica che ha luogo in ogni mercato.

La teoria, inoltre, **non riconosce la mancanza di identità**. Essa assume che la perdita di capitale causerà l'uscita dall'attività degli attuali miner "cattivi" e l'entrata di nuovi miner "buoni". Questa è una assunzione insostenibile. Non vi è alcuna ragione di credere che i miner attuali usciranno dall'attività o che i nuovi miner non prenderanno le stesse decisioni dei precedenti dato che sono impegnati nello stesso tipo di attività, tutto ciò assumendo che sia possibile anche solo dimostrare discernere tra l'uno e l'altro. Almeno nello scenario della vendita di mele un individuo sa da chi sta comprando le mele e può quindi discriminarlo, ciò non è possibile in Bitcoin.

La teoria, inoltre, **non tiene conto dell'economia del mining**. Vi è infatti un vantaggio di prossimità che permette di ottenere ritorni sul capitale più elevati ai i miner con maggiore *hash power*. I miner più grandi sono quindi più profittevoli dei piccoli miner. Quindi i primi saranno maggiormente capitalizzati rispetto ai loro competitori più piccoli. All'avvenuto cambiamento della regola di consenso i miner che rimarranno saranno quelli che potranno permettersi di sostituire i dispositivi e che saranno quelli di maggiore dimensione.

E' irrazionale assumere che tutti i miner cessino semplicemente l'attività. Ci aspetteremmo che tutti i coltivatori di mele vengano rimpiazzati da nuovi coltivatori? Nel mining non sono forse l'esperienza, la disponibilità di strutture, i contratti energetici, la disponibilità di macchinari generici i vantaggi più importanti sui nuovi entranti? I miner esistenti hanno un vantaggio intrinseco su coloro che dovrebbero presumibilmente rimpiazzarli. Questo significa che hanno maggiore accesso al capitale. Così, i miner più grandi non solo finirebbero per avere meno competizione, ma tutti i miner rimanenti avrebbero un vantaggio su qualsiasi nuovo miner.

La teoria, inoltre, **non riconosce che i commercianti necessitano del mining**. Il mining non verrebbe rimpiazzato attraverso la separazione poiché esso manterrebbe un completo controllo della selezione delle transazioni. Se ad esempio i miner "cattivi" fossero gli stati che stanno conducendo un attacco contro la moneta, sia lo stesso stato che i miner cooptati continuerebbero la loro azione distruttiva ad un costo energetico più basso. Poiché gli altri miner fallirebbero a causa di quella che è, a tutti gli effetti, una tassa del 100%, il costo energetico dell'attaccante continuerebbe a scendere. I servizi di mining che sono "buoni" per i commercianti non possono essere prodotti per mezzo di una separazione.

Infine, la teoria **non sa riconoscere le sue conseguenze reali**. Sulla base della precedente perdita di capitale sofferta da tutti i miner di una data moneta, tutti i miner della moneta sostitutiva si assicurerebbero contro la possibilità di un simile evento in futuro. Si potrebbero assicurare in autonomia, ma l'incremento di costo sarebbe inevitabile. Questo ridurrebbe *l'hash rate* a parità di *fee* finché

la possibilità di un tale evento non venisse ritenuta trascurabile. Così l'economia innalza le sue stesse *fee* e si ritrova con gli stessi miner e maggiore raggruppamento. Ciò rappresenta una riduzione della sicurezza su due livelli, senza alcun beneficio.

Titolo originale: Proof of Work Fallacy

Indice

Fallacia del Teorema di Regressione

Il Teorema di Regressione si basa sull'assunzione che le prime persone che attribuiscono valore di moneta a qualche bene devono necessariamente fare ciò basandosi sul ricordo del suo precedente valore d'uso, ove questo bene ottiene dapprima un'utilità nel baratto e infine valore monetario.

> Nessun bene può essere impiegato per funzionare come mezzo di scambio se, immediatamente prima del suo uso per questo scopo, esso non abbia un valore di scambio basato su altri usi.
>
> Mises: L'Azione Umana

Va notato che la teoria non prova semplicemente a spiegare l'origine del *concetto* di moneta, ma di qualsiasi cosa possa essere considerata moneta. In altre parole, se un bene non segue questa progressione non è moneta.

Il teorema contraddice la teoria del valore soggettivo sul quale esso stesso si basa. Il valore è soggettivo, il che implica che può essere basato su qualsiasi cosa, anche se oggettivamente tale base appare irrazionale.

Il teorema non pone termine alla sua stessa regressione non spiegando come una persona sia portata a dare valore a qualcosa per la sua utilità *originale*. Una persona deve *assumere* (non ricordare) che qualcosa sarà utile anche se nessuno ha mai tentato di usarla prima. Questa assunzione di utilità rappresenta la prima valutazione, che rimane soggettiva. La prima valutazione di una bene, come tutte quelle successive, può essere fatta per qualsiasi ragione, inclusa la sua utilità come moneta.

Poiché esiste un concetto preesistente di moneta, è stato suggerito che stabilire in anticipo lo *status* di moneta relativo al bene è di per sé sufficiente a soddisfare il teorema. In altre parole la moneta non deve seguire la progressione indicata dal teorema nella pratica effettiva. In questo caso, poiché vi è un concetto preesistente di moneta, *qualsiasi cosa* può essere moneta dal principio della sua esistenza. Questa interpretazione rende il teorema tautologico - qualsiasi cosa cui

le persone attribuiscono il valore di moneta può essere moneta. In altre parole, ciò si riduce al primo valore soggettivo.

Il teorema è in realtà basato sulle osservazioni empiriche dell'evoluzione monetaria. Tuttavia la teoria economica razionale sulla quale è basato il teorema, così come il teorema stesso, rifiutano esplicitamente l'empirismo.

> Tutte queste proposizioni implicate dal teorema di regressione sono enunciate apoditticamente per come implicato nell'apriorismo della prasseologia. Deve accadere necessariamente in questo modo. Nessuno potrà mai avere successo nella costruzione di un caso ipotetico nel quale le cose abbiano luogo in maniera differente.

Uno dei molti problemi che affliggono l'economia empirica e che le nuove osservazioni possono invalidare le conclusioni tratte in precedenza. Bitcoin ha fatto ciò con questo teorema. E' possibile osservare chiaramente che Satoshi intendeva creare una moneta il cui uso fosse quello monetario fin dal principio.

L'idea alla base del teorema rappresenta una ragionevole teoria empirica dell'evoluzione del concetto di moneta, ma tale idea è tuttavia invalida come teorema razionale per distinguere la moneta da ciò che non è moneta. La moneta si distingue da certi comportamenti espressi dalle persone. Concludere che qualcosa è moneta consiste nell'osservare questi comportamenti, un metodo strettamente empirico.

Titolo originale: Regression Fallacy

Indice

Fallacia della Propagazione

La rete *peer-to-peer* del protocollo Bitcoin diffonde i blocchi e le transazioni non confermate. Il protocollo stesso permette ai nodi di proteggersi dagli attacchi di tipo *denial of service*. Di conseguenza, questo tipo di comunicazione non richiede l'uso di identità. Questo tipo di protezione è il modo con il quale la rete non richiede l'impiego di un permesso per parteciparvi.

Tuttavia, questa protezione si realizza ad un costo in termini di latenza degli annunci e, a causa del vantaggio di prossimità, una più bassa latenza si traduce come un più elevato livello *hash power* apparente. Di conseguenza i miner competono per avere una più bassa latenza. Un modo per ridurre la latenza è tramite il raggruppamento, un altro è quello di utilizzare una rete di diffusione più efficiente. Presumibilmente, poiché il raggruppamento cede potere all'operatore, la seconda opzione è preferibile.

Un modo per migliorare la diffusione è quello di ottimizzare la rete *peer-to-peer*. L'altro è quello di unirsi ad un network distinto, chiamato propagatore (*relay*), che possiede una più bassa latenza dovuta alla rimozione delle protezioni degli attacchi *denial-of-service*, ad esempio:

> Il formato del messaggio cmpctblock è stato progettato per inserirsi efficacemente in un meccanismo di propagazione basato su UDP-FEC. La sola differenza è che lo mandiamo tramite UDP per mezzo del FEC... In questo modo, dei collegamenti extra non introducono maggiore latenza. Sfortunatamente, a causa della natura di codifica del FEC, non possiamo sapere se pacchetti individuali fanno parte di un blocco legittimo, o di un vero e proprio blocco, e di conseguenza è possibile attivare questa ottimizzazione tra nodi che sono eseguiti dallo stesso gruppo. bitcoinfibre.org.

Il propagatore accetta una comunicazione da un insieme di miner per mezzo del protocollo peer-to-peer, o di altri protocolli. Il propagatore consiste di un insieme di macchine soggette al controllo del relayer. Esso comunica gli annunci alla sua rete interna e infine ai miner che si sono uniti ad essa.

L'importante osservazione di sicurezza da analizzare è che la comunicazione per mezzo di un propagatore è soggetta al controllo del *relayer*. Poiché le protezioni

dal *denial-of-service* sono state rimosse il *controllo di tipo centrale* è necessario per il funzionamento di questa configurazione. Il relayer può infatti ritardare certi blocchi sulla base del miner, della regione, di uno specifica segnalazione, di un mancato pagamento etc. Un relayer **vende una riduzione di latenza** e fa quindi parte del business del mining a tutti gli effetti. Dal punto di vista della sicurezza non importa che il servizio sia offerto gratuitamente. I miner potrebbero offrire gratuitamente agli operatori dei dispositivi di mining (grinder) latenza e varianza ridotte.

I propagatori sono aggregazioni di miner e i miner sono a loro volta aggregazioni di grinder. Più grande è l'aggregazione di *hash power* maggiore è il profitto del centro di mining, così come lo è del propagatore. Si può considerare che i grinder siano liberi di lasciare i centri di mining e che i miner siano liberi di lasciare i propagatori, ed è possibile per un grinder operare il suo stesso centro di mining e il suo stesso propagatore. Ma le aggregazioni più estese sono più profittevoli, così lasciare i più grandi propagatori o centri di mining incrementa il costo relativo.

Una teoria sostiene che i propagatori riducano la pressione al raggruppamento. Si tratta di una fallacia in quanto **ogni riduzione al raggruppamento causata da un propagatore non scompare ma è *trasferita* al propagatore stesso come raggruppamento aggiuntivo**. Le statistiche del propagatore non sono mai mostrate affianco alle statistiche del mining, mascherando questo trasferimento di potere tra i due strumenti. Questo porta le persone a credere che il mining sia molto meno raggruppato di quanto non sia in realtà. La conseguenza di ciò è la mancata percezione dell'insicurezza causata dal reale livello di raggruppamento del mining.

Titolo originale: Relay Fallacy

Indice

Fallacia della *Replay Protection*

Esiste una teoria secondo la quale la *replay protection* applicata ad una catena separata aumenti l'utilità relativa della catena originale. La *replay protection* (n.d.t. protezione dalla ripetizione) è una regola progettata in relazione ad un'altra catena e avente un comportamento direzionale. La protezione rende le transazioni della catena protetta invalide sull'altra catena.

Anche senza protezione, è comunque possibile per un possessore effettuare una spesa in una maniera tale da impedirne la ripetizione in una direzione o in un altra, sebbene questo porti ad un costo in termini di *fee* e/o di complessità. Una separazione può ridurre ma non eliminare del tutto questo costo in una o entrambe le direzioni attraverso l'attivazione di regole che le azioni di spesa possono utilizzare *selettivamente*. Questo tipo di misura è chiamata *opt-in replay protection* e si differenzia dalla *replay protection* obbligatoria. La *opt-in replay protection* riduce ma non elimina il costo mentre la protezione obbligatoria può eliminarlo.

La ripetizione di una spesa in un'altra catena è un'azione che non porta a diluizione. L'output comune può essere speso su entrambe le catene con o senza ripetizione. **La sola distinzione fornita dalla protezione è che le spese possono essere *distinte* su ciascuna catena senza alcun costo aggiuntivo per colui che effettua la spesa**. L'offerta in ciascuna catena rimane inalterata dall'utilizzo della protezione.

Si tratta di una sorprendente quanto errata percezione quella di credere che una catena possa assorbire le transazioni dell'altra in un evento di separazione. Tutti gli output del segmento comune rimangono spendibili su entrambe le catene. La *replay protection* permette solo di ridurre il costo di spendere tali output sulla catena protetta.

E' possibile assumere che la mancanza di protezione renda meno probabile per un possessore spendere sulla catena non protetta, limitando di conseguenza l'offerta e aumentando il prezzo di scambio. Tuttavia questo presuppone che la domanda non sia influenzata da quello che si concretizza come un aumento dei

costi di scambio. Se il possessore non sta effettuando scambi in quanto vi è un incremento di costo nel farlo, allora l'utilità della moneta non aumenta ma bensì diminuisce.

Il costo di proteggersi autonomamente consiste in un demurrage *una tantum* che rimane finché la protezione è applicata alle unità non protette, in maniera intenzionale o altrimenti. Questo costo rappresenta uno sconto sull'utilità di una catena non protetta se confrontata con la stessa ipotetica catena dotata di protezione. Questo implica una *maggiore* utilità della catena protetta rispetto a quella non protetta - che si è formata a seguito della separazione - rispetto a quanto sarebbe avvenuto in condizioni differenti. Di conseguenza la teoria è invalida.

Titolo originale: Replay Protection Fallacy

Indice

Fallacia della Valuta di Riserva

Esiste una teoria secondo la quale, prima o poi, gli stati adotteranno Bitcoin come valuta di riserva e che gli individui transeranno per mezzo di una moneta di monopolio "coperta" da Bitcoin. La teoria sostiene che il volume delle transazioni per far sì che Bitcoin venga usato come valuta per il consumatore sia insufficiente, ma le sue proprietà atte ad impedire l'inflazione monetaria rendono Bitcoin un asset di riserva ideale. Le banche centrali è i funzionari da loro autorizzati emetterebbero delle cambiali detenendo i relativi Bitcoin a riserva. Poiché Bitcoin non può essere inflazionato, prosegue la teoria, la moltitudine di problemi causata dal controllo dello stato sulla moneta verrebbe risolta, dando inizio ad una nuova era di prosperità. Le *fee* di transazione sarebbero basse mentre il volume delle stesse transazioni sarebbe illimitato.

Analizziamo come si svilupperebbe questo scenario. Bitcoin diventa una valuta regolarmente e ampiamente utilizzata ma affetta da diversi problemi quali bassi volumi di transazione, *fee* elevate e lunghi tempi di conferma. Al fine di ottenere una riserva di bitcoin (BTC) lo stato emette Certificati negoziabili di Bitcoin (CB) in cambio di bitcoin. Questo potrebbe essere realizzato sequestrando i conti centralizzati (forzandone la conversione) o attraverso scambi a mercato, ovvero le stesse due modalità che sono state adottate per costituire le riserve auree. Viene istituito un meccanismo di controllo per mezzo del quale le persone possono verificare che i CB emessi non superino le riserve di BTC. Vengono create leggi di corso legale, che obbligano le persone ad accettare i CB per fare *settlement* dei debiti, a meno che non venga esplicitamente stabilita una modalità differente. Le persone acquistano i CB con BTC così da poter pagare le tasse e pagare i beni del mercato legale ai rivenditori. Alla fine la maggior parte dei BTC è detenuta come riserva di stato.

Questo scenario dovrebbe suonare familiare, in quanto è lo stesso modo con il quale gli stati sono finiti in possesso dell'oro e le persone sono rimaste in possesso della carta delle banconote. La teoria è invalida su molteplici piani.

Il rapporto tra CB emessi e BTC a riserva non può mai essere efficacemente verificato. Anche se le regole di consenso di Bitcoin rimanessero in qualche modo in vigore, non vi è modo di sapere quanti CB siano stati emessi, e non vi è modo di intervenire se venisse sospettata una svalutazione. E' necessario fidarsi della banca centrale per tenere conto dell'emissione di CB e sostanzialmente questo significa che ognuno deve fidarsi del fatto che lo stato non ponga in essere politiche di *easing*. La storia ha dimostrato che questo genere di correttezza da parte dello stato è improbabile e cionondimeno non vi è alcun miglioramento rispetto alle attuali monete di stato.

Allora, come è possibile che una persona non possa mai efficacemente verificare (validare) i CB, mentre ciò è possibile con i BTC che i certificati hanno sostituito? Perché ciò renderebbe i CB indistinguibili dai BTC tenuti a riserva. In altre parole la *ragione* per cui vi è una differenza tra valuta a corso legale e valuta di riserva è quella di permettere l'inflazione della valuta (una forma di tasssazione) mantenendo a riserva (n.d.t. accumulando) una moneta migliore.

Inoltre, affinché Bitcoin sopravviva, deve esistere un reale economia decentralizzata basata su di esso. In assenza di individui che validano i BTC ricevuti in uno scambio, non vi è nessuno che possa rifiutare BTC invalidi, cosa che avviene quando essi vengono ridefiniti dallo stato. In questo caso la censura e l'inflazione possono essere introdotti facilmente, invalidando la teoria. Solo le transazioni Bitcoin del mercato nero ed il mining possono resistere a questo tipo di transizione. Questo porta sullo stato una ridotta pressione economica a mantenere la consistenza con le regole di consenso di Bitcoin.

Il *layering* conserva i principi criptodinamici della decentralizzazione, mentre la "copertura" rappresenta il fenomeno che dimostra il loro completo abbandono. Bitcoin non può essere sostenuto in uno scenario dove esso funge da moneta di copertura per i certificati di una banca centrale. Le persone devono effettuare degli scambi con esso per garantirne la sicurezza. E' certamente possibile che Bitcoin sia detenuto come patrimonio di stato, ma questo non offre alle persone alcuna scalabilità delle transazioni o vantaggi di altro tipo.

Titolo originale: Reserve Currency Fallacy

Indice

Fallacia del Rendimento *Risk Free*

Il concetto ipotetico di tasso di rendimento *risk free* rappresenta il tasso di interesse economico ottenibile con un rendimento garantito sul principale del prestito. Esiste una teoria secondo la quale Bitcoin ammetta nella pratica l'esistenza di tale rendimento attraverso l'imposizione della restituzione del principale. Un corollario di questa teoria afferma che questa proprietà consente anche di limitare l'espansione del credito in generale.

La teoria richiede l'esistenza dimostrabile di una garanzia (*covenant*) a scadenza temporale fissa sulle unità della moneta date in prestito dal creditore. La garanzia assicura che il creditore non possa spendere le unità fino a quando il prestito non arrivi a maturità e che le unità tornino in possesso del creditore solo in quel momento. Il creditore scambia con il debitore queste unità bloccate in cambio di un interesse. Il costo opportunità del prestatore imposto dalle unità bloccate dalla garanzia è compensato dall'interesse.

Tuttavia, le unità bloccate non forniscono alcuna utilità a colui che le ha prese in prestito. Il pieno controllo delle unità ritorna in maniera dimostrabile al prestatore, lasciando ogni persona che le ha accettate con nulla in mano al momento del termine del prestito. **Questo valore nullo è necessariamente attribuito in ogni scambio precedente al termine del prestito e di conseguenza al prestito stesso, rendendo invalida la teoria**.

Esiste una teoria collegata secondo la quale le unità date in prestito possono essere invece usate da colui che le prende in prestito per tracciare un asset di valore perpetuo. Poiché il tracciamento termina con la scadenza del prestito, la teoria è invalida per la stessa ragione.

In aggiunta, vi è una teoria collegata secondo la quale il costo opportunità del prestatore può essere usato per rappresentare una spesa dimostrabile, come avviene con la *proof-of-work*. Questo può essere usato in maniera simile ad hashcash, ovvero come un modo per mitigare il *denial of service*. Ciò è vero, ma questo rappresenta una spesa e, come tale, essa può avverarsi solo spendendo unità (anche attraverso la loro distruzione). Così come nella *proof-of-work*,

questo rappresenta uno scambio tra un costo dimostrabile di capitale e unità. Per questa ragione esso non costituisce un prestito (i.e. non dà luogo ad interesse), invalidando la teoria.

In aggiunta, esiste una teoria collegata secondo la quale le unità prese a prestito possono essere usate per tracciare un asset a scadenza definita che termina alla scadenza del prestito (e.g. un biglietto del teatro). Ciò risulta possibile, tuttavia il costo di tracciamento, per qualsiasi durata, è limitato in BTC dalla regola di consenso del limite di trasferimento (*dust limit*) fissata ad una unità. Così il costo opportunità è limitato ad un'unità in aggiunta alle *fee* di transazione necessaria per stabilire il prestito. L'utilità per il debitore è rappresentata dalla riduzione del costo di tracciamento per il tempo del prestito. Con un tasso di interesse del 10% e una scadenza approssimativamente superiore a 7.2 anni diventa meno costoso spendere una unità rispetto a prenderla in prestito. Spendendo immediatamente un'unità l'asset verrebbe tracciato indefinitamente.

Sebbene lo scenario economico finale di quanto appena proposto sia economicamente razionale, esso non può essere descritto accuratamente come un prestito, poiché le unità non possono essere né scambiate né distrutte dalla persona identificata come il destinatario del prestito. Sarebbe più appropriato riferirsi a questo costrutto come ad un "affitto" delle unità, per la sola ragione di distinguerlo da un vero prestito.

Ciò nonostante, un rendimento può essere teoricamente ricavato sull'affitto di una unità, fino al limite economico imposto dal tasso di interesse (e.g. circa 7.2 anni al 10%). Tuttavia le *fee* richieste dall'operazione, per essere economicamente razionale, dovrebbero essere di 0 unità, in quanto è richiesta una transazione che dia avvio al prestito, cosa che non avviene quando vengono usate le proprie unità per fini di tracciamento. Così nel caso la domanda di transazione ecceda l'offerta fissa di conferma, questo scenario non è economicamente razionale. Questa relazione è valida per ogni valore del livello minimo (*dust limit*) maggiore di 0 ma che rappresenti anche una *fee* insufficiente per finanziare la conferma.

Titolo originale: Risk Free Return Fallacy

Indice

Fallacia della Scarsità

Come concetto *assoluto*, la scarsità economica di una risorsa implica solo che essa non sia disponibile con offerta illimitata. Ciò nonostante, se nessuna persona richiede tale risorsa, la risorsa non ha valore. Una risorsa scarsa quando viene richiesta diventa una proprietà. Tuttavia, secondo questa costruzione, non viene considerato alcun grado di difficoltà nel produrre la risorsa.

Ci si può riferire alla scarsità come alla *relativa* disponibilità di una certa proprietà. Per una certa offerta, un aumento di domanda implica una diminuzione di disponibilità (aumentando la scarsità). Tuttavia, un incremento di domanda tende ad incrementare l'offerta, e quindi la disponibilità. In maniera simile, per una certa domanda, un incremento di offerta implica un aumento di disponibilità (diminuendo la scarsità). Tuttavia un aumento di offerta tende a diminuire la domanda, e quindi ciò porta (n.d.t. l'offerta, in risposta) a diminuire la disponibilità. Queste retroazioni negative stabilizzano la disponibilità e in maniera corrispondente il prezzo.

Una sola moneta possiede un'offerta fissa. Esiste una teoria secondo la quale l'offerta fissa di Bitcoin sia la fonte del suo valore. Così come per Bitcoin, vi è un'offerta fissa della Gioconda, ne esiste una sola. La teoria implica che l'unicità del famoso dipinto sia la fonte del suo valore. Tuttavia vi è una innumerevole quantità di opere uniche per le quali non vi è alcuna domanda e quindi nessun valore. **Bitcoin non può aumentare di valore solo per la sua scarsità assoluta**. Al contrario, esso diventa necessariamente più scarso all'aumentare del suo valore.

Un aspetto della teoria è che l'offerta fissa di Bitcoin è la fonte della sua utilità in quanto garantisce che la sua disponibilità non venga aumentata. Tuttavia ciò richiede che la sua domanda non diminuisca.

Bitcoin è unico nel dominio delle proprietà in quanto il costo per trasferirlo aumenta intrinsecamente con l'aumento di domanda nell'effettuare questa operazione. A differenza della Gioconda, esso è soggetto ad una effettiva capacità di essere sostituito (n.d.t. da altre monete e asset digitali e non). Queste forze creano necessariamente la retroazione negativa della domanda che si osserva nei beni senza offerta fissa. Poiché la mancata diminuzione della domanda non può essere data per certa, la teoria è invalida. Come spesso accade nelle fallacie

economiche, l'errore deriva, in parte, dal considerare solo un lato della relazione di domanda-offerta.

Un'altra causa dell'errore va ricercata nell'errata interpretazione del comportamento delle monete merce. A causa della sua bassa diffusione sulla superficie della terra, l'oro ha conservato la sua portabilità nel corso della storia rispetto a materiali più diffusi come il ferro e il sale. Tuttavia la portabilità della moneta elettronica è indipendente dal numero di unità esistenti. Mettendo da parte la questione della sufficiente divisibilità, il numero totale di unità di Bitcoin è completamente arbitrario e quindi indipendente dalla sua utilità.

Un'altra causa dell'errore sta nell'errata interpretazione del comportamento delle monete di stato. Per mezzo delle leggi sulla non contraffazione lo stato controlla l'offerta della sua moneta limitando la competizione. Può quindi riscuotere una tassa di inflazione espandendo l'offerta senza consumare capitale, incrementando quindi il rapporto tra moneta e capitale. Senza limitazione della competizione l'offerta si espanderebbe attraverso le forze di mercato, in risposta alla domanda, eliminando la tassa. In altre parole la moneta si comporterebbe come una commodity diffusa con scarsa portabilità (almeno fino a quando non viene ridenominata dallo stato). La scarsa portabilità è spesso una conseguenza reale dell'iperinflazione.

La bassa diffusione (o numero di unità) non rappresenta una proprietà monetaria importante eccetto che per quanto riguarda la portabilità. La scarsità è una funzione sia dell'offerta che della domanda e di conseguenza non può essere una caratteristica intrinseca di una moneta, anche nel caso essa sia dotata di offerta fissa. Sia la moneta merce che Bitcoin eliminano la tassa di inflazione, tuttavia la moneta merce è soggetta alla retroazione negativa data dall'inflazione (n.d.t. aumento dell'offerta dovuto a creazione/estrazione e.g. dell'oro) e Bitcoin è soggetto alla retroazione negativa data dall'incremento delle *fee*.

Titolo originale: Scarcity Fallacy

Indice

Fallacia del *Selfish Mining*

Il termine "*selfish mining*" si riferisce a un'ottimizzazione del mining. Tuttavia un articolo accademico inquadra questa ottimizzazione nel seguente modo:

> La convinzione comune afferma che il protocollo del mining è compatibile con gli incentivi economici ed è protetto dalla collusione di gruppi di minoranza, ovvero, esso incentiva i miner a seguire il protocollo come prescritto. Mostriamo qui che il protocollo di mining di Bitcoin non è compatibile con gli incentivi economici.

Questa affermazione presuppone che esista un "protocollo di mining di Bitcoin stabilito" che impedisca il trattenimento, cosa che rappresenta una argomentazione fallace. Necessariamente, le regole di consenso di Bitcoin non si esprimono su quale sia il tempo di attesa degli annunci.

> Presentiamo qui un attacco con il quale i miner collusi ottengono un ricavo più grande rispetto a quella che sarebbe la loro giusta quota parte.

Questa affermazione assume che esista il concetto di "giusta quota parte" che è estraneo a Bitcoin e rappresenta un'altra argomentazione fallace. Un miner è ricompensato sulla base dei blocchi da lui trovati che raggiungono la maturità, non sulla proporzione dell'*hash rate* corrente.

Questi argomenti fallaci vengono esplicitamente attribuiti alla "convinzione comune". In altre parole, l'articolo li utilizza per mostrare che la convinzione comune è scorretta. Tuttavia, l'articolo sbaglia a dichiarare in maniera incondizionata che questa *ingiusta violazione del protocollo* costituisca un attacco.

> Questo attacco può avere conseguenze significative per Bitcoin: i miner razionali preferiranno unirsi ai *selfish miner* ed il gruppo colluso aumenterà di dimensione finché non diventerà la maggioranza. A questo punto il sistema Bitcoin cessa di essere una valuta decentralizzata.

Questa è l'origine della fallacia. Non si tratta dell'attacco alla convinzione comune ad essere scorretto, ma l'errore sta nel dare per assunta la convinzione comune. Il *selfish mining* implica che Bitcoin manifesta una pressione al raggruppamento

basata sulla latenza, benché questo sia un difetto ben conosciuto. Tutte le pressione al raggruppamento tendono a ridurre il numero di miner, esponendo Bitcoin agli attacchi.

Le ottimizzazioni non sono attacchi. Il raggruppamento aumenta l'*opportunità* degli attacchi, ma la sola opportunità non dovrebbe essere confusa con l'azione vera e propria. Il termine "attacco" implica il furto. Ad esempio il whitepaper di Bitcoin usa questo termine solo per descrivere i tentativi di doppia spesa.

Titolo originale: Selfish Mining Fallacy

Indice

Fallacia delle *Fee* a Parte

Esiste una teoria secondo la quale le *fee off-chain* rappresentino un incentivo individuale che va contro la sicurezza del sistema (rappresenterebbero un incentivo economico incompatibile). La teoria afferma che un commerciante che paga un miner "a parte" al fine di confermare le sue transazioni impedisce alle transazioni di altri commercianti di essere confermate, oppure che questa azione alza il costo di queste conferme dando vantaggio a coloro che accettano tali *fee*.

Un effetto di questi accordi è che un livello *storico* medio delle *fee* non può essere determinato attraverso l'analisi della catena (*chain analysis*). Il livello apparente sarebbe più basso del livello del mercato. Questo può naturalmente portare coloro che effettuano le spese a sottostimare un livello di *fee* sufficiente. Tuttavia non vi è alcuna proprietà di Bitcoin che richiede che le *fee* future eguaglino un qualche livello medio delle *fee* del passato. La stima necessariamente si compensa, come per esempio ignorando le transazioni "gratuite" in blocchi pieni o usando la deviazione standard per identificare i valori estremi. Ma la stima della *fee* è solo una stima. I livelli attuali delle *fee* rispondono alla competizione.

Un altro effetto di questo fenomeno è che livelli relativamente eterogenei delle *fee* possono evidenziare che certe transazioni sono associate con questi accordi. Questo può contribuire a tracciare la transazione del commerciante e/o la transazione coinbase del miner. Ma poiché un tale tipo di accordo è una scelta fatta dal creatore di queste transazioni, non vi è alcuna perdita di privacy.

Non vi è alcun effetto sui livelli del mercato delle *fee* o nella possibilità per altri di ottenere delle conferme. Se l'accordo si discosta dai livelli di mercato allora o il commerciante o il miner stanno accettando una perdita non necessaria. Questo comportamento non è differente da quello di un miner che conferma transazioni con *fee on-chain* al di sotto del livello di mercato o da quello di un commerciante che sovrastima le fee *on-chain*, rispettivamente. In ogni caso, non ci sarebbe alcun pericolo per la sicurezza del sistema anche se tutte le *fee* venissero pagate *off-chain*.

Bitcoin fornisce un meccanismo per le *fee on-chain* che fa in modo che una transazione possa ricompensare *ogni* potenziale miner senza l'uso dell'identità. E' una comodità che preserva la privacy. **Se i miner e i commercianti preferiscono indebolire la loro stessa privacy attraverso operazioni**

aggiuntive, non vi è motivo di considerare ciò non desiderabile. La teoria è quindi invalida.

Inoltre, a meno che l'*hash power* di un miner sia il 100%, il commerciante deve accettare un ritardo nella conferma che è inversamente proporzionale all'*hash power* di quel miner. La *fee* a parte è offerta al tasso di mercato poiché altrimenti il miner incorrerebbe in un costo opportunità.

Vi è una teoria collegata secondo la quale accordi sulle *fee* a parte costituiscono una pressione al raggruppamento. Se le *fee* pagate sono coerenti con il mercato non può esserci effetto di raggruppamento. Le *fee* al di sopra del mercato sono un sussidio di stato, in quanto dobbiamo trattare il sussidio come un fenomeno non economicamente razionale. Le *fee* al di sotto del mercato sono una tassa, in quanto dobbiamo trattarle come una perdita non volontaria. Queste sono distorsioni come lo è qualsiasi tipo di sussidio/tassa di stato e non sono quindi unicamente presenti nelle *fee* a parte. L'esistenza delle *fee* a parte non rappresenta una nuova pressione al raggruppamento in aggiunta a quelle già esistenti nelle *fee on-chain* e la teoria è quindi invalida.

Titolo originale: Side Fee Fallacy

Indice

Fallacia dell'Espansione Separata del Credito

Esiste una teoria secondo la quale l'incremento delle unità monetarie derivante da un evento di separazione o dalla creazione di una nuova moneta, crei del credito. Questo è un errore che presumibilmente trae origine dall'assunzione che l'espansione del credito guidata dall'espansione monetaria dello stato sia una forza di mercato. Questa assunzione non tiene conto del fatto che una moneta di mercato non può dare luogo a signoraggio.

Il signoraggio è una tassa. Le unità monetarie create non rappresentano nuovo capitale ma, al contrario, rappresentano una diluizione delle unità esistenti da parte dello stato che trasferisce la proprietà del capitale che esse rappresentano al sovrano. Quando questo capitale è messo in opera al fine di sussidiare l'attività di prestito da parte del cartello bancario di stato, poiché sotto forma di moneta a sconto e di assicurazione, il costo del capitale per i clienti della banca viene ridotto.

L'espansione del credito sotto questa accezione non è semplicemente il risultato della riserva frazionaria come forza di mercato. E' la conseguenza dell'azione dello stato che favorisce i debitori alle spese dei risparmiatori. In un libero mercato bancario, le banche sono semplicemente dei fondi di investimento. Gli investitori ottengono in media un ritorno a mercato sul capitale investito e sono soggetti al relativo grado di rischio. In un sistema bancario di stato il rischio, e quindi il capitale, sono riorganizzati in funzione di obiettivi politici.

L'espansione del credito del mercato libero manifesta un aumento di capitale dato in prestito che si contrappone al suo accumulo. Un aumento della quantità di credito è conseguenza di una ridotta preferenza temporale e ciò porta a ridurre il costo del capitale. E' impossibile mostrare che un evento di separazione o la creazione di una nuova moneta (o in generale qualsiasi altra cosa) riduca la preferenza temporale. Per questa ragione è un errore assumere che queste forme di creazione di moneta incrementino la disponibilità di capitale o riducano il suo costo.

Titolo originale: Split Credit Expansion Fallacy

Indice

Fallacia del Rapporto Stock Flusso

Storicamente, il rapporto stock-flusso descrive la relazione tra capitale ed entrate, permettendo la stima di un determinato capitale futuro a partire da un livello atteso di entrate. In un momento successivo questo concetto basilare è stato applicato all'offerta di moneta in generale.

Il rapporto stock-flusso rappresenta una misura di tempo. Con un rapporto più levato, lo stock crescerà più lentamente. Esiste una teoria secondo la quale una moneta con rapporto stock-flusso intrinsecamente più elevato sarà proporzionalmente soggetta ad un minor effetto di inflazione monetaria rispetto ad una moneta avente un rapporto più basso. La teoria afferma che un rapporto più alto implica una moneta "più forte" ovvero definita come più resistente agli effetti dell'inflazione monetaria.

La teoria non considera correttamente la fonte della grandezza dei flussi. Essa assume necessariamente che il tasso di produzione rappresenti semplicemente la proprietà di una sostanza. Ma la produzione di qualsiasi cosa ha luogo quando il suo prezzo anticipato rende la produzione profittevole. Un profitto potenzialmente più elevato si traduce in maggiore competizione, accelerando l'incremento dell'offerta. Un maggior numero di persone che scava alla ricerca dell'oro aumenta il suo flusso.

In altre parole, il flusso è una funzione della domanda. Una perdita che viene anticipata non da luogo ad alcuna produzione di sorta. La mancanza di qualsiasi flusso non è intrinseca della sostanza ma è una conseguenza della mancanza di domanda. Poiché sia l'offerta che la domanda determinano il flusso, la teoria non è valida. Questo errore, compreso da lungo tempo, non rappresenta una proprietà del basilare concetto del rapporto stock-flusso, ma una sua errata applicazione.

La presenza delle leggi anti-contraffazione fa in modo che la competizione alla produzione di moneta di stato venga limitata, permettendo il controllo dell'offerta da parte dello stato indipendentemente dalle forze di mercato. Come per altre monete, domanda e offerta sono generalmente imprevedibili. Uno stato può

"agganciare" la sua emissione di titoli di riserva ad un'altra moneta come ad esempio all'oro. Questa relazione può rimanere valida anche per diverse decadi. In questo caso il rapporto stock-flusso indicherebbe in maniera non corretta una "robustezza" confrontabile con quella dell'oro.

Poiché il rapporto stock-flusso di una moneta rappresenta il tasso di inflazione invertito della stessa, la sua relazione con l'inflazione monetaria è tautologica. La relazione infatti non implica nulla sull'inflazione monetaria futura. Essa può essere usata per analizzare relazioni storiche e calcolare futuri stock basati su un *assunto* flusso futuro, ma non può essere usata per *predire* inflazione monetaria futura. Ogni dichiarazione relativa al fatto che un tipo di speculazione sarà più profittevole di un altro basato sull'andamento storico del rapporto stock flusso rappresenta un errore.

Titolo originale: Stock to Flow Fallacy

Indice

Fallacia della Creazione dal Nulla

Esiste una teoria secondo la quale un sistema bancario a riserva frazionaria dia intrinsecamente la capacità alle banche di creare moneta senza alcun costo reale. La teoria non dipende dal privilegio di stato del signoraggio. Essa è considerata altresì una conseguenza delle pratiche contabili del *free banking*. Talvolta ci si riferisce ad essa come alla creazione di moneta *ex nihilo* o "dal nulla".

> Lord Adair Turner, già a capo della autorità di vigilanza finanziaria del Regno Unito, ebbe a dire: "Le banche, contrariamente a quanto affermano fin troppi libri di testo, non prendono i depositi monetari dai depositanti e li danno in prestito ai soggetti richiedenti: esse creano il credito e la moneta *ex nihilo* - accendendo il prestito e contemporaneamente accreditando moneta sul conto del debitore."

I seguaci della teoria descrivono due visioni sulla creazione della moneta in competizione tra loro. Come implicato dalle parole di Lord Turner, la visione tradizionale è ritenuta quella più semplice rispetto alla rappresentazione più pratica. La teoria afferma che il sistema bancario crei intrinsecamente non solo il credito, ma anche la moneta.

Visione Semplice

La moneta è creata dai miner ad un costo reale, viene venduta alle persone, e infine data in prestito ad altre persone. La teoria ritiene che il prestatore sta dando in prestito solo il denaro in suo possesso. Come tale il prestatore sta operando a riserva intera e non può mettere in pratica operazioni a riserva frazionaria che sono considerate fraudolente. Un prestatore onesto può solo emettere dei titoli (moneta rappresentativa) contro moneta in suo possesso, impedendo l'espansione del credito e quindi una perdurante inflazione dei prezzi.

Visione Pratica

I sostituti monetari vengono creati dalle banche, senza sostenere alcun costo reale e come conseguenza della riserva frazionaria. L'offerta di questi sostituti si

espande ad ogni prestito e si contrae quando il prestito si estingue. Poiché non viene posto alcun vincolo all'espansione del credito, il debito complessivo cresce senza limiti creando una perdurante inflazione dei prezzi.

In un libero mercato le persone possono svolgere le stesse operazioni delle banche, senza necessariamente chiamarsi banche. Di conseguenza, la distinzione tra queste due possibilità deve basarsi sul modo con cui viene celata una supposta frode. La teoria sostiene che questo occultamento è raggiunto usando un trucco contabile che non viene compreso dalle persone su larga scala. Proponiamoci allora di analizzare in profondità tale aspetto. Ogni tipo di moneta risulterà sufficiente per condurre questa ricerca sui sostituti monetari creati al di sopra di essa, e che includono Oro, Bitcoin o moneta di monopolio.

Nella visione semplice, il potenziale prestatore ha risparmiato sia la liquidità necessaria per il suo consumo personale (accumulo) sia l'ammontare destinato a ricavare un interesse (investimento). In questo scenario tutta l'attività di prestito deriva dai risparmi, come ad esempio l'oro accumulato (n.d.t. ad esempio) dopo averlo trovato passando la bateia. I risparmi sono costituiti dalla somma del denaro accumulato (moneta) ed del quantitativo di crediti in eccesso sui debiti: `risparmi = moneta + (credito - debito)` . La moneta è l'oro ed i crediti sono sostituti monetari:

	risparmi	moneta	credito	debito
Persona	100 oz	100 oz		

Secondo questa visione del prestito personale, la Persona cede 81 once d'oro (oz) al Debitore. Il Debitore accetta l'obbligo di ripagare la Persona assieme ad un interesse alla scadenza del prestito. Per semplificare la contabilità assumeremo che vi sia interesse nullo e non si tenga conto del rischio di controparte (i.e. scontandolo):

	risparmi	moneta	credito	debito
Persona	100 oz	19 oz	81 oz	
Debitore		81 oz		81 oz

La Persona, in realtà, ha dato in prestito alla sua stessa Impresa (e.g. un'attività di prestito) una frazione dei suo risparmi, di cui è tenuto conto di seguito. Assumiamo che la Persona tenga da parte (accumuli) il 10% dei suo risparmi per far fronte alla liquidità necessaria ai consumi di breve termine e che l'Impresa accumuli il 10% per lo stesso motivo:

	risparmi	moneta	credito	debito
Persona	100 oz	10 oz	90 oz	

	risparmi	moneta	credito	debito
Impresa		9 oz	81 oz	90 oz
Debitore		81 oz		81 oz

L'Impresa della persona sta operando con una riserva del 10% in quanto il 90% dei suoi risparmi è diventato capitale di rischio. Applicare questo schema alla visione semplice del sistema bancario richiede solamente di sostituire il termine "Prestatore" (n.d.t. la Persona) con il termine "Depositante" e "Impresa" con "Banca". Non vi è necessità di assumere che questi siano due individui distinti:

	risparmi	moneta	credito	debito
Depositante	100 oz	10 oz	90 oz	
Banca		9 oz	81 oz	90 oz
Debitore		81 oz		81 oz

Rappresentando correttamente la Persona come un soggetto avente capitale di rischio (i.e. il depositante) possiamo vedere che tutta l'attività di prestito è a riserva frazionaria. In questo scenario dove la riserva è al 10% ci sono due prestiti che danno luogo a sostituti monetari (credito) pari al 171% della moneta sottostante. Data l'assunzione di una preferenza temporale uniforme il Debitore darà in prestito il 10% dei suoi risparmi, come tutti i debitori successivi. Assumendo un prestito minimo pari ad 1 oncia, dopo 43 prestiti l'espansione del credito termina con 8.903 volte il valore della moneta sottostante.

Sia `r`il livello uniforme delle riserve individuali e `m` la quantità di moneta, l'ammontare totale del credito `c` per ogni dato numero di prestiti `n` è dato dalla seguente somma parziale (n.d.t. si tratta di una serie geometrica):

```
c = Somma(n=1..n)[m * (1 - r)^n] =
(m * (r - 1)*((1 - r)^n - 1))/r =
(100 oz * (10% - 1) ((1 - 10%)^43 - 1))/10% = 890.3 oz
```

Il rapporto di riserva `rr` è dato dal rapporto tra moneta e credito:

```
rr = m/c = 100 oz / 890.3 oz = ~11.23%
```

Il moltiplicatore monetario è dato dall'inverso del rapporto di riserva:

```
1/rr = 1/(100oz/890.3oz) = 8.903
```

(n.d.t. si noti, tra l'altro, che l'espansione non è limitata dalla divisibilità finita delle unità, che in caso di seria geometrica infinita da luogo ad un ammontare di credito paria `am * (1-r)/r`, che con una riserva `r` del 10% porta ad un moltiplicatore monetario di 9)

Prestito	Accumulo	Prestito	Credito
1	10.00	90.00	90.00
2	19.00	81.00	171.00
3	27.10	72.90	243.90
4	34.39	65.61	309.51
5	40.95	59.05	368.56
6	46.86	53.14	421.70
7	52.17	47.83	469.53
8	56.95	43.05	512.58
9	61.26	38.74	551.32
10	65.13	34.87	586.19
11	68.62	31.38	617.57
12	71.76	28.24	645.81
13	74.58	25.42	671.23
14	77.12	22.88	694.11
15	79.41	20.59	714.70
16	81.47	18.53	733.23
17	83.32	16.68	749.91
18	84.99	15.01	764.91
19	86.49	13.51	778.42
20	87.84	12.16	790.58
21	89.06	10.94	801.52
22	90.15	9.85	811.37
23	91.14	8.86	820.23
24	92.02	7.98	828.21
25	92.82	7.18	835.39
26	93.54	6.46	841.85
27	94.19	5.81	847.67
28	94.77	5.23	852.90
29	95.29	4.71	857.61
30	95.76	4.24	861.85
31	96.18	3.82	865.66
32	96.57	3.43	869.10
33	96.91	3.09	872.19
34	97.22	2.78	874.97
35	97.50	2.50	877.47
36	97.75	2.25	879.72
37	97.97	2.03	881.75
38	98.18	1.82	883.58
39	98.36	1.64	885.22
40	98.52	1.48	886.70
41	98.67	1.33	888.03
42	98.80	1.20	889.22
43	98.92	1.08	890.30

Si noti che, in condizione di espansione completa, affinché una persona spenda il proprio denaro accumulato mantenendo la propria preferenza temporale, un prestito deve essere estinto in modo da compensare la spesa. Il processo di estinzione [finalizzazione] del prestito muove il denaro dal primo debitore al suo creditore, e da luogo alla cancellazione della nota di debito. La persona che riceverà le monete derivanti dalla spesa le darà necessariamente in prestito per soddisfare la sua preferenza temporale e così via.

Non è possibile alcuna ulteriore espansione senza l'incremento della quantità di moneta o di una riduzione complessiva della preferenza temporale. Un incremento della moneta incrementa il quantitativo assoluto di credito disponibile e una riduzione della preferenza temporale incrementa la proporzione di credito rispetto alla moneta. Poiché moneta e credito evolvono assieme, non vi è mai un incremento reale dei sostituti monetari se non derivante da questi cambiamenti.

Nella tipica pratica della contabilità bancaria la Banca non cede il denaro. Al suo posto essa crea delle voci contabili in un processo noto con il nome di "creazione del credito". Il processo crea delle voci di libro contabile che si compensano tra i ricavi e i prestiti del Depositante ("credito" e "debito") e delle voci che si compensano con lo stato patrimoniale della banca stessa ("attività" (*assets*) e "passività" (*liabilities*)). All'emissione del prestito, i conti appaiono come indicato di seguito:

	risparmi	moneta	credito	debito	attività (*assets*)	passività (*liabilities*)
Depositante	100 oz	10 oz	90 oz		100 oz	
Banca		90 oz	81 oz	171 oz	171 oz	171 oz
Debitore			81 oz	81 oz	81 oz	81 oz

A questo punto le spiegazioni che è in grado di fornire la teoria tendono ad esaurirsi. Le partite di compensazione sia della Banca che del Debitore si controbilanciano, ma il Debitore ha a disposizione 81 once d'oro da spendere e la Banca non ha avuto necessità di cedere alcuna oncia d'oro al Debitore. Ci sono sempre 100 once in moneta, ma il Debitore ha 81 once di sostituto monetario e la Banca ha 81 once d'oro in più di attività. La teoria afferma che quindi la Banca ha creato non solo credito, ma anche *moneta*. Si noti che tutto il quadro contabile è ancora bilanciato e tutti i conti possono essere finalizzati, e ciò sembrerebbe dare ragione alla teoria per come esposta da Lord Turner:

> "... esse creano il credito e la moneta *ex nihilo* - accendendo il prestito e contemporaneamente accreditando moneta sul conto del debitore."

Questo tuttavia dimostra che nessuna spesa reale è stata ancora effettuata a partire dal credito del prestito o dall'asset della banca. Spingiamoci ancora leggermente oltre nel ragionamento assumendo che il Debitore proceda al *clearing* del suo conto e di conseguenza finalizzi le corrispondenti attività e passività della Banca.

	risparmi	moneta	credito	debito	attività (*asset*)	passività (*liability*)
Depositante	100 oz	10 oz	90 oz		100 oz	
Banca		90 oz	81 oz	90 oz	90 oz	90 oz
Debitore		81 oz		81 oz	81 oz	81 oz

Si noti che questo è un esito identico a quello della visione semplice. **Non vi è quindi distinzione tra queste due visioni apparentemente in competizione sulla creazione di moneta**, e ciò rende invalida la teoria. Questo fatto porta a risolve la secolare questione, cominciata apparentemente tra Platone e Aristotele che si domandavano se la moneta fosse basata sull'attività estrattiva o sul credito. Le teorie sono identiche, in quanto la moneta ed il credito sono duali.

> Secondo Joseph Schumpeter, il primo seguace conosciuto della teoria del credito fu Platone. Schumpeter descrive il metallismo come l'altra teoria "delle due fondamentali teorie della moneta", aggiungendo che il primo seguace della teoria del metallismo fu Aristotele.

I seguaci delle due teorie stanno parlando semplicemente della stessa cosa. Bitcoin, in qualità di moneta fiat (i.e. una moneta che non ha valore d'uso) che opera in assenza del supporto dello stato, ha finalmente reso evidente sia gli errori logici del metallismo, che provò a mostrare la necessità di una moneta con valore d'uso, che quelli del cartalismo che provò a mostrare la necessità del supporto dello stato alla moneta fiat.

Si deve ricordare che ogni prestito ha una riserva del 10%, così la banca può dare in prestito fino a 8.903 volte l'ammontare di moneta a riserva, ovvero 890.30 once di sostituti monetari contro le 100 once di moneta a riserva. Se la Banca avesse una riserva del 0% per ogni prestito, l'espansione del credito sarebbe infinita. Tuttavia questo implica una preferenza temporale pari a zero, equivalente all'idea che il tempo non abbia valore, cosa che implica che tutto il denaro venga imprestato indefinitamente. Nel caso della Banca, lo 0% in riserva implica che non vi sia alcuna liquidità per soddisfare alcun prelievo (i.e. la bancarotta immediata). Tuttavia, assumendo una preferenza temporale nulla, non potrebbe mai esservi alcun prelievo e ciò rende lo scenario non rilevante ai fini pratici. L'espansione del credito è necessariamente finita.

Torniamo ora ad analizzare lo scenario nel quale la Banca crea del credito con una riserva negativa (i.e dal nulla), considerando questa volta una spesa. Ad esempio, su un deposito di 0 once la Banca ha intenzione di accendere un prestito di 1000 once. Al posto di basarsi sulla moneta a riserva per riuscire alla fine a finalizzare il prestito, la Banca "crea moneta" sul suo stato patrimoniale. La banca quindi procede a creare i conti di credito e debito intestati al debitore che rappresentano rispettivamente la moneta presa a prestito e l'obbligo di ripagare il prestito:

	risparmi	moneta	credito	debito	attività (*asset*)	passività (*liability*)
Banca			1000 oz	1000 oz	1000 oz	1000 oz
Debitore			1000 oz	1000 oz	1000 oz	1000 oz

Quando il debitore scambia 1 oncia d'oro (dal suo conto di credito) in cambio di una macchina, il suo conto viene diminuito di 1 oncia e quello del commerciante è incrementato di 1 oncia. Si noti che il Debitore ora deve alla banca 1 oncia che è stata anticipata per mezzo del prestito.

	risparmi	moneta	credito	debito	attività (*asset*)	passività (*liability*)
Banca			1000 oz	1000 oz	1000 oz	1000 oz
Debitore	-1 oz		999 oz	1000 oz	999 oz	1000 oz
Commerciante	1 oz		1 oz		1 oz	

Tutto sembra procedere bene finché il commerciante non prova a ritirare dal suo conto. A questo punto la Banca è in default e il Commerciante non può essere pagato. Se il conto del commerciante è con un'altra banca, il pagamento fallisce quando le due banche procedono a fare il *settlment* dei conti. Con una ipotetica riserva negativa, i conti si bilanciano nel seguente modo, implicando che la Banca è in fallimento (moneta negativa):

	risparmi	moneta	credito	debito	attività [asset]	passività [liability]
Banca	-1 oz	-1oz	1000 oz	999 oz	999 oz	999 oz
Debitore			999 oz	1000 oz	999 oz	1000 oz
Commerciante	1 oz	1 oz			1 oz	

La moneta deve essere realmente spostata dal controllo della Banca al Commerciante o alla Banca del Commerciante, cosa che non è possibile. Un esempio più semplice di ciò che accadrebbe è l'impossibilità da parte del Debitore di prelevare dal suo conto. Le Banche possono creare tutta la quantità di sostituti monetari che desiderano, ma le riserve negative rappresentano solamente una mancata promessa. In questo esempio la banca ha creato 1000 once di promesse che non può mantenere.

La mancata comprensione di questi principi deriva probabilmente dalla mancata comprensione del funzionamento del processo di *settlement*. E questo deriva probabilmente dal non riconoscere la intrinseca *dualità della moneta e del credito*, in quanto il primo deve necessariamente esistere per finalizzare i titoli di credito implicati dal secondo. E ciò deriva probabilmente dall'abitudine di riferirsi alla moneta (e.g l'oro) negli stessi termini con cui ci si riferisce ai sostituti monetari (e.g. crediti dell'oro).

Le voci contabili di attività e passività e relativa compensazione serve solamente per tenere conto dei prestiti emessi ed in sospeso, cosa che sta alla base dello stato patrimoniale della Banca. In maniera simile, la Banca non ha creato la voci di credito e debito, e loro relativa compensazione, per occultare la creazione fraudolenta di moneta. La Banca ha creato queste voci per due ragioni:

- Precludere la possibilità del trasferimento fisico solo per ri-depositare il denaro nella Banca
- Incoraggiare il ri-deposito nella Banca a discapito dei concorrenti (o dell'accumulo da parte del Debitore).

Quando la Banca non ha riserve sufficienti per soddisfare i prelievi, dovuti a prestiti in default o ad una corsa agli sportelli, ha solo due opzioni: andare in fallimento oppure chiedere un prestito. Per impedire il verificarsi della prima opzione è stato creato il sistema bancario centrale atto a fornire la seconda opzione. Questo è il significato del termine "prestatore di ultima istanza". Il Principio della Banca di Stato fornisce una dettagliata spiegazione relativa alla reale fonte dell'inflazione monetaria.

In breve, è stato mostrato che:

- Le banche non hanno il potere di creare moneta.
- La riserva frazionaria è intrinseca all'attività di prestito.
- La quantità in riserva è una espressione della preferenza temporale.
- Una riserva pari a zero preclude ogni possibilità di effettuare il *settlement* dei conti.
- Non esiste alcuna distinzione tra la visione semplice e la visione pratica come teorie della creazione di moneta.

Titolo originale: Thin Air Fallacy

Indice

Fallacia della Preferenza Temporale

Esiste una teoria secondo la quale avere una più bassa preferenza temporale sia migliore di averne una più alta, in quanto ciò porta ad una maggiore produzione e quindi a maggior ricchezza. Questo fatto rappresenta semplicemente uno scambio della causa con l'effetto.

La preferenza temporale è un assioma economico che afferma che le persone preferiscono un "bene nel presente" rispetto allo stesso "bene nel futuro". A differenza del valore soggettivo, questa idea non può essere provata. Il tempo è una entità unica se si assume che esso abbia valore intrinseco. Questa assunzione è supportata osservando che le persone possiedono un tempo limitato e che esso è un fattore necessario ad ogni produzione.

Il valore deriva dalla percezione umana di utilità. Una persona che scambia una macchina per un cavallo sta oggettivamente valutando maggiormente l'utilità di possedere un cavallo rispetto a quella di possedere una macchina. Questo non implica nulla sul perché un bene abbia maggiormente valore di un altro per una persona, anche a seguito dello scambio. Il maggior valore attribuito ad un bene rispetto ad un altro rappresenta una preferenza. Non si può dimostrare che una persona possa esprimere una preferenza per ogni bene, anche per la sua stessa vita. La ragione di una preferenza non può essere provata nell'ambito della teoria dell'economica razionale con una sola eccezione - l'effetto della ricchezza sulla preferenza temporale.

L'utilità marginale decrescente implica che ogni unità addizionale di un bene accumulato da una persona ha, per essa, una più bassa utilità rispetto all'unità precedente. Questo implica che, per un dato tasso di interesse, una maggiore ricchezza implica una maggiore disponibilità a dare in prestito. Questa è l'espressione della preferenza temporale decrescente, che si riflette conseguentemente nella diminuzione del tasso di interesse dovuta alla maggiore offerta di capitale che compete per essere impiegata nei prestiti.

Il tasso di interesse economico è semplicemente il riflesso della preferenza temporale. Benché potenzialmente qualsiasi fattore possa influenzare la preferenza

temporale di una persona, solamente una variazione nella sua ricchezza implica un cambiamento necessario. Un più elevato tasso di interesse implica una maggiore disponibilità ad imprestare di una persona avente una data preferenza temporale. Tuttavia sarebbe un errore assumere che un più elevato tasso di interesse porti ad aumentare la preferenza temporale. In maniera simile è un errore assumere che una persona diventi più ricca abbassando la sua preferenza temporale. Queste considerazioni rappresentano entrambi una inversione di causa ed effetto. Per questa ragione la teoria è invalida.

Una preferenza temporale infinita implica l'assenza di ogni forma di prestito e quindi l'assenza di ogni forma di produzione. Una preferenza temporale nulla implica l'assenza di ogni forma di consumo di ciò che è stato prodotto. Poiché la produzione esiste solamente per soddisfare il consumo futuro, una preferenza temporale nulla implica allo stesso modo l'assenza di produzione, in quanto non può essere attribuito alcun valore al consumo dei prodotti. Quindi la più bassa preferenza temporale non è intrinsecamente più produttiva. Per questa ragione la teoria è invalida. **La preferenza temporale rappresenta l'equilibrio tra produzione e consumo**.

La ricchezza di una persona aumenta solamente nella misura in cui essa è in grado di soddisfare maggiormente le sue preferenze e che includono anche quelle relative al consumo presente e a quello differito. Gli stati impiegato lo stimolo fiscale e monetario nel tentativo di incrementare rispettivamente il consumo o la produzione. Tuttavia ciò avviene al costo della tassazione. Il risultato è lo spostamento sulle decisioni di allocazione del capitale dal mercato allo stato, cosa che porta allo spreco del capitale in prodotti non consumati (che vengono avanzati) o non disponibili (che scarseggiano). Questo implica che le persone sono meno in grado di *soddisfare* le loro preferenze. Tuttavia questo fatto non implica alcun cambiamento delle preferenze che essi possiedono, eccetto per il fatto che la tassazione diminuisce la loro ricchezza e che il sussidio la incrementa.

L'economia non formula giudizi di valore, essa deduce le loro necessarie conseguenze. La teoria che viene qui analizzata presuppone una moralità che può essere assunta ma che deve essere oggettiva. L'aggressione distingue il libero mercato dall'intervento sul mercato, ad esempio ad opera dello stato. Tuttavia, anche accettando il principio di non-aggressione come linea di demarcazione sul piano morale, non può esserci alcuna distinzione etica tra una più elevata ed una più bassa preferenza temporale. Non vi è rapporto tra consumo e produzione che possa implicare l'aggressione, essa rimane soggettiva benché venga influenzata dalla ricchezza posseduta. Per questa ragione la teoria è invalida.

Può essere chiarificante considerare la soggettività dei valori in termini di preferenza sessuale.

- `{ X, Y }`
- `{ X->X, Y->Y }`
- `{ X->X|Y, Y->X|Y }`
- `{ X->Y, Y->X }`

Si può considerare che questa lista sia ordinata in termini di produzione crescente (i.e. produzione di più esseri umani). Numerosi stati provano a ridurre la preferenza sessuale al gruppo `{ X->Y, Y->X }`. Sia l'aperta criminalizzazione delle preferenze sia l'incentivo economico esplicito sono utilizzati per questo fine. Questo ha un impatto distinguibile sull'*espressione* della preferenza sessuale, ma non si può dire che essa abbia un impatto sulla preferenza in sé.

In maniera simile dovrebbe essere chiaro che un incremento della produzione non è sempre obiettivamente una cosa buona. Le persone che fanno ciò che preferiscono rappresenta il bene morale, assumendo sempre il rispetto del principio morale di non-aggressione. Anche assumendo che tutte le persone preferiscano la continuazione della specie, questo non implica alcun effetto sulla preferenza sessuale individuale.

Una teoria affine afferma che le persone possono dimostrare minore preferenza temporale accumulando più bitcoin. Un più elevato livello di accumulo a discapito dell'attività di prestito implica una *più elevata* preferenza temporale. Un più elevato livello di accumulo a discapito del consumo sembrerebbe, al contrario, implicare una più bassa preferenza temporale, in quanto il consumo appare differito. Tuttavia un accumulo rappresenta solamente la liquidità necessaria per il consumo.

Come nei giochi di fortuna, ogni tipo di speculazione rappresenta il consumo del costo necessario per "partecipare al gioco", sostenuto dalla liquidità richiesta. Questo costo è, come minimo, il costo opportunità di non investire quell'importo (i.e. in cambio dell'interesse). Benché il gioco, come ogni forma di consumo, richieda tempo, la preferenza che viene espressa dall'azione è quella di partecipare al "gioco", non di catturare il valore del tempo. Per questa ragione la teoria è invalida allo stesso modo.

Vi è inoltre una teoria affine secondo la quale la preferenza temporale è espressa da un consumo differito - che ha luogo quando una persona accumula dei risparmi al posto di utilizzarli. Come mostrato ne il Consumo Speculativo questa assunzione rappresenta in modo errato il fatto che tutti i risparmi vengano necessariamente investiti. Il risparmio è un termine generalizzato che include sia l'accumulo che l'investimento di una persona. Il risparmio è la *fonte* di ogni investimento, ma solo il reale investimento è espressione della preferenza temporale. Un accumulo può sicuramente cambiare il suo valore di mercato. Ma considerare un maggiore accumulo un'espressione di una minore preferenza temporale rappresenta una assai diffusa ed errata interpretazione del significato economico del termine. Questa interpretazione porta a ribaltarne il significato e conduce alla conclusione secondo la quale un accumulo totale di tutta la ricchezza porterebbe ad una preferenza temporale nulla. Al contrario con un accumulo totale il tasso di interesse sarebbe infinito ed un tasso di interesse infinito riflette una preferenza temporale infinita. Questa evidente contraddizione mette in luce il fatto che il significato del termine preferenza temporale è stato invertito, rendendo quindi invalida la teoria.

Titolo originale: Time Preference Fallacy

Indice

Fallacia della Moneta non Prestabile

L'equazione di Fisher viene usata per calcolare il tasso di crescita in una moneta soggetta ad inflazione, in quanto si deve tenere conto dell'effetto di svalutazione sulla moneta stessa nel futuro. Questo fenomeno porta ad aggiustare il tasso di interesse nominale al fine di ottenere il tasso di interesse reale. La dimostrazione è semplificata usando i rapporti al posto dei tassi. Come mostrato ne il Principio della Svalutazione, il tasso di svalutazione di una moneta merce è pari allo 0%, ovvero è pari ad un rapporto di crescita del 100%.

La moneta di monopolio è soggetta a svalutazione a causa del signoraggio.

```
rapporto-di-crescita-moneta-monopolio = rapporto-di-crescita-moneta-merce / rapporto-di-sign
~97% = 100% / 103%
```

Una moneta ad offerta fissa può apprezzarsi a causa della deflazione dei prezzi.

```
rapporto-di-crescita-moneta-monopolio = rapporto-di-crescita-moneta-merce
/ rapporto-di-signoraggio. rapporto-di-crescita-moneta-offerta-fissa
= rapporto-di-crescita-moneta-merce / rapporto-di-inflazione.
~103% = 100% / 97%
```

Si presume che una moneta ad offerta fissa vari il suo potere d'acquisto in proporzione ai prodotti che essa rappresenta. In altre parole, con un quantitativo doppio di prodotti, ogni unità della moneta sarà in grado di scambiare il doppio del quantitativo dei prodotti rispetto a prima.

```
potere-di-acquisto-anno-corrente = potere-di-acquisto-anno-precedente * rapporto-di-crescita
103 = 100 * 103%
```

La presunzione relativa alla deflazione dei prezzi di una moneta ad offerta fissata si basa anche sull'assunzione di una crescita economica positiva. Nel caso di una contrazione economica la moneta esibisce un inflazione dei prezzi. Il caso relativo alla crescita economica (aumento di ricchezza) implica che l'interesse superi la svalutazione. Sia l'interesse che la svalutazione devono essere sempre positivi per come implicato dalla preferenza temporale.

```
rapporto-di-interesse > rapporto-di-svalutazione > 100%
rapporto-di-interesse / rapporto-di-crescita = rapporto-di-svalutazione
rapporto-di-interesse / rapporto-di-crescita  > 100%
rapporto-di-interesse > rapporto-di-crescita
```

La contrazione economica (diminuzione di ricchezza) implica un incremento del tasso di interesse, come implicato dalla teoria dell'utilità marginale, finché non viene ristabilita una crescita positiva. Come tale la contrazione è una condizione che porta ad una correzione automatica.

```
rapporto-di-svalutazione > rapporto-di-interesse > 100%
rapporto-di-interesse / rapporto-di-crescita = rapporto-di-svalutazione
rapporto-di-interesse / rapporto-di-crescita  > 100%
rapporto-di-interesse > rapporto-di-crescita
```

Si noti che in entrambi i casi di crescita e di contrazione, l'interesse deve eccedere la crescita, in quanto l'attività di prestito è l'unica fonte della crescita. Poiché la crescita è l'unico fondamento della deflazione in una moneta deflazionaria, l'accumulo di moneta rappresenta una svalutazione monetaria (un consumo).

Esiste una teoria secondo la quale è economicamente irrazionale dare in prestito una moneta deflazionaria. **Come è stato mostrato, è razionale imprestare qualsiasi tipo di moneta, inclusa una moneta che è deflazionaria, circostanza che invalida la teoria**. Ogni comportamento differente implica l'esercizio di una scelta puramente speculativa che non è supportata dal fatto che la moneta sia ad offerta fissa.

Titolo originale: Unlendable Money Fallacy

Indice

Obiettivi di una *Fedcoin*

Per come implicato dalla *Value Proposition*, ci sono due aspetti che fanno di Bitcoin un obiettivo del controllo dello stato, ed entrambi rappresentato una minaccia al gettito fiscale.

Nel combattere Bitcoin lo stato potrebbe tentare di introdurre una moneta apparentemente simile, a cui potremmo riferirci con il nome di Fedcoin. Essa potrebbe essere introdotta attraverso una separazione o come moneta alternativa. L'obiettivo della sua implementazione sarebbe quello di mantenere apparentemente le caratteristiche di Bitcoin eliminando al contempo la sua *value proposition*. Questo porterebbe a proteggere le entrate fiscali pubblicizzando nel frattempo la Fedcoin come un'alternativa "più sicura" di Bitcoin. La creazione di una Fedcoin non è di per sé rilevante per Bitcoin, è solamente l'imposizione del suo uso a richiedere una forma di resistenza.

I due aspetti che differenziano la Fedcoin rispetto a Bitcoin consentono allo stato di creare arbitrariamente nuove unità (signoraggio) e di impedire il trasferimento (censura). L'obiettivo del signoraggio può essere raggiunto attraverso un *hard fork* che introduce una nuova regola di consenso. Questa regola permetterebbe l'introduzione di nuove unità nel caso lo stato avesse firmato una transazione di tipo inflazionario. L'obiettivo di censura potrebbe essere raggiunto attraverso un *soft fork* che impedisce la conferma di transazioni alle quali manca la firma dello stato.

Impedire allo stato di obbligare l'implementazione di questi *fork* è lo scopo principale della sicurezza di sistema di Bitcoin. L'economia garantisce la protezione dall'hard fork e i miner garantiscono la protezione dal soft fork. I rischi che vengono affrontati da queste persone garantiscono il valore della moneta in contrapposizione alle alternative controllate dallo stato.

Titolo originale: Fedcoin Objectives

Indice

L'errore di Hearn

Esiste una teoria secondo la quale lo stato non possa proibire le cose popolari.

Questo implica che un alto volume di transazioni permetta una difesa efficace contro gli attacchi e la coercizione. Ciò, a propria volta, implica che Bitcoin può essere difeso accettando la forza centralizzante di un elevato volume di transazioni.

Questa teoria è invalida in quanto è basata su osservazioni empiriche che tuttavia derivano da un un errore fattuale. **E' evidente che lo stato *preferisca* in realtà proibire le cose popolari**. Qui di seguito vi è un breve elenco di cose popolari che vengono comunemente proibite:

- Droga
- Gioco d'azzardo
- Prostituzione
- Religione
- Libertà di Espressione
- Libertà di Assemblea
- Commercio
- Immigrazione
- Armi
- Lavoro
- Libri
- Moneta

Questo errore può derivare dal non accettare l'Assioma di Resistenza pur continuando a lavorare nell'ambito di Bitcoin. Questo probabilmente può dar luogo a dissonanza cognitiva. La successiva ricerca di sollievo può portare a questo punto. Tuttavia, alla fine, l'errore diventa innegabile, cosa che può portare ad una furiosa uscita di scena.

Titolo originale: Hearn Error

Indice

Tautologia dell'Oggetto da Collezione

Nel tentativo di applicare il Teorema di Regressione a Bitcoin si potrebbe postulare che Bitcoin abbia cominciato con l'essere un "oggetto da collezione", destando interesse tra i teorici dei sistemi monetari. L'oggetto da collezione avrebbe ottenuto un valore d'uso originale dovuto alle loro preferenze personali. E' stato quindi barattato in forza del suo valore d'uso, diventando quindi un mezzo di scambio basato sul ricordo del suo valore emerso dal baratto.

Ciò appare coerente con il teorema che afferma che ogni moneta *debba* trarre origine da una commodity che ottiene dapprima valore dal baratto e successivamente valore di scambio monetario. Tuttavia, se il valore di una commodity può derivare dal potenziale valore come moneta allora il teorema è una tautologia che implica niente di più che la moneta è moneta.

> Ora, il teorema di regressione si prefigge di interpretare la prima apparizione di una domanda di moneta per un bene che prima è stato esclusivamente domandato per necessità industriali, in quanto influenzato dal valore di scambio a lui attribuito in quel momento sulla base del solo servizio non monetario.
>
> Mises: L'Azione Umana

Il postulato si avvantaggia della comune ambiguità che esiste sulla parola "commodity", a dispetto dell'esplicito riferimento al valore d'uso "industriale" presente nel teorema stesso. **Se qualsiasi cosa può essere definita una commodity allora il Teorema di Regressione implicherebbe, al contrario della sua formulazione, che ogni cosa può essere moneta**.

> In economia una commodity è un bene economico o un servizio che possiede piena o sostanziale fungibilità: che significa che il mercato tratta ogni entità del bene come equivalente o quasi equivalente indipendentemente da chi lo abbia prodotto. [...]
>
> La maggior parte delle commodity sono materiali grezzi, risorse base, prodotti agricoli, prodotti da estrazione come il minerale ferroso, lo

> zucchero, o i cereali come il riso e l'orzo. Le commodity possono anche essere prodotti di massa non specializzati come materiali chimici e memorie per computer.
>
> Wikipedia: Commodity

Il Teorema di Regressione usa la parola "commodity" per distinguere la moneta da qualcosa senza valore d'uso originale. Se con questo si intende che *ogni cosa* può essere una commodity, ciò rappresenta una tautologia, o altrimenti tale postulato è una errata rappresentazione del teorema.

Titolo originale: Collectible Tautology

Indice

Stime di Prezzo

La capitalizzazione potenziale e di conseguenza il prezzo unitario di Bitcoin possono essere stimati in numerosi modi. Un approccio comune è quello di immaginare che Bitcoin sostituisca tutta la moneta di stato o anche il prodotto lordo mondiale. Altri approcci che fanno uso di modelli del prezzo passato per prevedere il prezzo futuro sono economicamente irrazionali e non vengono qui ulteriormente esplorati. L'ipotesi di trattare Bitcoin come la moneta di riserva globale viene scartata per le ragioni discusse ne la Fallacia della Moneta di Riserva. Gli effetti dell'accumulo speculativo sui prezzi non vengono considerati poiché la teoria catallattica dimostra che la speculazione non determina i prezzi.

Dato che Bitcoin è moneta e non credito, l'approccio "della moneta" rappresenta l'assunzione di partenza più razionale. Tuttavia senza una chiara comprensione della fondamentale distinzione tra moneta e credito questo approccio è spesso viziato nella pratica. Come mostrato ne la Fallacia dell'Espansione del Credito, Bitcoin non può limitare l'espansione del credito. Se esso potesse (ipoteticamente) eliminare l'espansione del credito non vi sarebbe alcuna produzione di sorta ed esso non varrebbe nulla. La più ragionevole ipotesi iniziale che include l'espansione del credito è quella per cui Bitcoin viene riservato allo stesso livello delle altre monete. Il tasso di espansione del credito è guidato dalla sola preferenza temporale degli individui, così questa rappresenta un'assunzione coerente con la prassi storica.

Prendiamo in considerazione 5 possibili scelte di "moneta" che Bitcoin può sostituire:

- Moneta tangibile.
- Base monetaria (M0).
- Credito bancario (M3 - M0).
- Tutto il credito (bancario, debito, capitale societario).
- Prodotto lordo totale.

Usare solamente la moneta tangibile (la "liquidità in contante") è un approccio irrazionale. La moneta considerata come equivalente monetario della moneta tangibile deve essere inclusa allo stesso modo, in quanto fa parte della stessa offerta. Le banche centrali, quando richiesto, stampano e coniano moneta tangibile sulla base di "obblighi" da rispettare, e tutto il credito viene espanso

su questa base monetaria. Questo concetto viene affrontato ne il Principio del Sistema Bancario di Stato. Utilizzare il credito è allo stesso modo un approccio irrazionale, in quanto Bitcoin non è una forma di credito. Essendo moneta esso viene utilizzato per fare *settlement* delle obbligazioni creditizie. Questo concetto è affrontato ne la Fallacia del Loop del Debito. Quindi, l'utilizzo di una combinazione di moneta e credito (ad esempio M1, M2 o M3, poiché esse includono M0) è irrazionale per lo stesso tipo di ragionamento. L'impiego del prodotto lordo globale è ingiustificabile in maniera simile, poiché esso non è né una forma di moneta né una forma di credito.

Tuttavia, ai soli fini del confronto, procediamo a stimare ciascuna delle cinque ipotesi riportate sopra. I valori di base impiegati nella seguente tabella sono in Dollari Statunitensi e presi dal capitolo della Fallacia dell'Espansione del Credito. A loro volta, questi valori sono stati incrementati sulla base di una stima della dimensione relativa dell'economia mondiale rapportata alla capitalizzazione del mercato azionario. Il mercato statunitense è approssimativamente pari al 40% del mercato mondiale. Di conseguenza questi valori sono incrementati rispetto agli Stati Uniti di un fattore 1/40%. Questo approccio favorisce la semplicità sull'accuratezza in quanto l'obiettivo della discussione è quello di dimostrare un metodo razionale di stima. Il quantitativo di Bitcoin stimato è pari a 18'952'500 di cui il 95% è stato minato (~ 10 anni nel futuro) e il 5% è stato perso (e.g. le chiavi private perdute di Satoshi).

Le valutazioni sono basate sul 2019 sebbene l'inflazione di Bitcoin sia quella del 2029. Ciò implica che, basandosi sull'assunzione di crescita economica e di inflazione monetaria del Dollaro Statunitense, i valori dovrebbero essere più elevati. L'ultima ipotesi può essere eliminata considerando una proiezione costante del valore del dollaro del 2019. Assumendo un tasso reale annuo di crescita economica del 2% composto su 10 anni, i valori al 2029 vengono incrementati del ~22%.

Sostituto	Dimensione (2019)	USD/BTC (2029)
Moneta tangibile	4'347'460'000'000 $	279'852 $
Base monetaria	8'187'102'500'000 $	527'016 $
Credito bancario	36'018'735'000'000 $	2'318'578 $
Tutto il credito	236'812'492'891'206 $	15'243'965 $
Prodotto lordo	80'270'000'000'000 $	5'167'097 $

La stima di prezzo per la sostituzione della base monetaria globale è pari a 527'016 $ per bitcoin. La determinazione del valore attuale netto richiede una stima del costo del capitale. Usando un valore conservativo del tasso di interesse pari al 7.2% è implicato un costo opportunità della speculazione del 100% (n.d.t. raddoppio) in circa 10 anni di tempo, che equivarrebbe ad un valore presente di circa 263'508 $ per bitcoin.

Consideriamo ora la prima assunzione, relativa alla sostituzione di tutta la moneta. Bitcoin non offre protezione contro il divieto del suo uso negli scambi da parte dello stato. Assumendo che lo stato mantenga i suoi poteri di signoraggio e censura possiamo procedere moltiplicando il valore della prima assunzione per la frazione del mercato nero globale, che è stimata essere dell'ordine del ~28% del mercato globale. La stima riguardante la base monetaria include *tutte* le attività del mercato denominate nella moneta (la stima del credito non le include tutte). Con una sostituzione del 100% di tutti gli scambi del mercato nero il prezzo è pari a 73'782 $ per bitcoin.

Tuttavia anche ipotizzando che tutte le monete di stato vengano esclusivamente usate nel mercato legale, non è possibile assumere che l'attività del mercato nero sia denominata al 100% in Bitcoin. Non vi è una base chiara per stimare questa proporzione, ma il prezzo di mercato del 2019 pari a circa ~10'000 $ implica una proiezione di adozione nel mercato nero al 2029 pari al ~7.4%

Questa stima non considera la Proprietà di Stabilità di Bitcoin. E' inoltre possibile che per gli scambi in Bitcoin venga imposto l'utilizzo di sostituti monetari prima che l'adozione futura attualmente prevista possa essere raggiunta.

Titolo originale: Price Estimation

Indice

Relazione del Risparmio

La preferenza temporale è l'assunzione di natura catallattica per la quale gli individui hanno preferenza dei beni presenti rispetto ai beni futuri. E' ormai un fatto ben assodato che la preferenza temporale si rifletta nel tasso di interesse. Viene qui dimostrato che il rapporto di capitale ha lo stesso significato e valore.

> Il livello del puro tasso di interesse è determinato dal mercato in relazione allo scambio di beni presenti rispetto ai beni futuri, un mercato che, come vedremo, permea notevolmente differenti parti del sistema economico. [...] Se, quindi, nel mercato temporale, 100 once d'oro vengono scambiate nella prospettiva di ottenere 105 once d'oro di qui ad un anno, allora il tasso di interesse è approssimativamente del 5% all'anno. Questo è il tasso di sconto temporale della moneta futura rispetto a quella presente. [...] Il puro tasso di interesse sarà quindi il corrente tasso di sconto del tempo, il rapporto di prezzo tra i beni presenti rispetto ai beni futuri.
>
> Rothbard: Man, Economy and State.

Un accumulo (una forma di consumo) rappresenta l'opportunità di investire così come un investimento è l'opportunità di consumare. Uno è scambiato per l'altro finché non vi è alcun ulteriore un incremento di utilità nel fare ciò.

Intraprendendo un investimento, un individuo valuta maggiormente il quantitativo di interesse futuro rispetto al quantitativo non investito. Non investendo, un individuo valuta maggiormente l'ammontare presente non investito rispetto all'interesse futuro: se così non fosse, avrebbe luogo rispettivamente un più basso ed un più elevato livello di investimento. L'avvenuto scambio rende la preferenza temporale una manifestazione oggettiva. Il tasso di interesse viene usato per mettere in relazione l'accumulo presente rispetto all'interesse futuro.

```
valore-accumulato = valore-investito * tasso-interesse
```

Come mostrato nel Principio della Svalutazione, non avviene alcun consumo reale durante lo scambio di un prodotto tra produttore e consumatore. Ciò risulta evidente in quanto il prodotto può essere rivenduto al prezzo corrente recuperando il valore monetario della porzione non consumata. In modo analogo, ogni porzione non consumata del bene può essere consumata nel futuro compensando il prezzo

corrente di acquistare una quantità maggiore dello stesso prodotto. Accumulare è un atto di consumo dove la frazione svalutata è stata consumata.

I beni che rimangono non consumati rappresentano dei beni futuri in relazione all'accumulo originale dei beni stessi. Un tasso di svalutazione viene impiegato per ottenere la riduzione del valore futuro dell'accumulo.

```
valore-non-consumato = valore-accumulato * tasso-di-svalutazione
```

Riarrangiando e sostituendo l'espressione del valore non consumato al valore accumulato, si ottiene la relazione tra beni accumulati che si stanno svalutando e beni investiti che non si stanno deprezzando. I beni futuri non esistono finché non diventano beni presenti e di conseguenza non si deprezzano.

```
tasso-di-interesse = (valore-accumulato * tasso-di-svalutazione) / valore-investito
```

Il rapporto di capitale è il rapporto tra il capitale accumulato (riservato) ed il capitale investito. Il *tasso* di interesse è il *rapporto* di capitale. Entrambi rappresentano lo stesso riflesso della preferenza temporale. **Il tasso di interesse è il rapporto tra il capitale consumato ed il capitale investito**.

Titolo originale: Savings Relation

Indice

Commento

A seguito di lungo e proficuo confronto con l'autore, è stato possibile accertare che il ragionamento sviluppato in questa versione della relazione del risparmio non ha validità generale nell'ambito dell'economia razionale. Per questa ragione, esso è stato modificato nella seconda edizione di Cryptoeconomics e verrà aggiornato anche nel repository originale e nella traduzione. Credo possa essere di utilità riportare la versione originale accompagnata da un commento, sia per ragioni di completezza, sia per dare contesto alle motivazioni della modifica.

Ogni preferenza umana, inclusa la preferenza temporale, si manifesta attraverso scale di valori individuali, e che mostrano, in questo specifico caso, le disponibilità degli individui a scambiare beni presenti per beni futuri.

Va notato innanzitutto che lo scambio dal punto di vista del creditore avviene tra la somma data in prestito (il principale) e la promessa di ricevere nel futuro tale somma in aggiunta all'interesse. Il debitore avrà la posizione esattamente speculare. Va anche notato che il "mercato temporale" si applica per semplicità alla moneta, ma teoricamente il ragionamento potrebbe applicarsi ad ogni bene capitale, al lavoro e alla produzione in generale. Nella discussione più estesa con Eric Voskuil è sorto il problema di come quantificare, ai fini della relazione del risparmio, il capitale dell'individuo: se in forma aggregata - sommando tutto

il capitale che un individuo possiede (incluso quindi tutto il tempo, i beni ed il denaro) - oppure separatamente per tipologia di bene capitale o servizio e che possiedono in generale differenti mercati (benché interconnessi tra loro) e differente grado di utilità (serviceable utility). La questione è rimasta tutt'ora aperta.

Ritornando alla discussione principale, le disponibilità individuali, a loro volta, si manifestano nella dinamica di domanda e offerta, dove un tasso di interesse - rispettivamente minimo e massimo - viene implicitamente implicato per ogni unità addizionale ceduta (dal creditore) e aggiunta (dal debitore) in uno scambio. In forza dell'utilità marginale decrescente, ogni unità aggiuntiva ceduta da un creditore richiederà un tasso di interesse più elevato mentre ogni unità aggiuntiva acquisita dal debitore richiederà un tasso di interesse inferiore dell'unità precedente. Le asimmetrie tra le preferenze portano - in un mercato libero ed efficiente - a stabilire un unico tasso di interesse che porta i creditori a cedere parte del loro capitale (investimento) e a trattenere parte di esso (accumulo) in funzione della scala di valori espressa e quindi a determinare un *rapporto di capitale* individuale.

Di conseguenza, il tasso di interesse è determinato dalle scale valori dei partecipanti al mercato e ciò, a sua volta, determina la suddivisione individuale tra capitale investito e capitale accumulato di ciascuno di essi. Si noti ad esempio, che per un dato un tasso di interesse di mercato, alcuni individui potrebbero non cedere nessuna unità del loro capitale, mentre altri potrebbero cederlo quasi interamente. Il rapporto di capitale rappresenta nello stesso tempo la causa individuale e la risposta del tasso di interesse a mercato, ed entrambi sono manifestazione della preferenza temporale, marginale ed individuale rispettivamente.

Ceteris paribus, per un dato tasso di interesse del mercato, un individuo con più elevata preferenza temporale esprimerà un più elevato rapporto di capitale (accumulerà di più rispetto ad investire) mentre un individuo con più bassa preferenza temporale esprimerà un rapporto di capitale relativamente più basso. Un aumento del tasso di interesse (causato da una variazione della preferenza temporale di uno o più partecipanti del mercato) porterà dunque a diminuire il rapporto di capitale di un singolo individuo (tenderà ad investire maggiormente per soddisfare la sua preferenza, ipotizzando sia rimasta la stessa delle precedenti interazioni di mercato) opponendosi al contempo a tale aumento. Allo stesso modo, una diminuzione del tasso di interesse porterà alcuni partecipanti di mercato ad accumulare una frazione maggiore di capitale (poiché il loro impiego non soddisferebbe le loro preferenze di investimento, anche qui ipotizzando sia rimasta la stessa dei precedenti interazioni) quindi opponendosi a tale diminuzione.

Sempre *ceteris paribus* una maggiore ricchezza degli individui nella loro globalità (soggettivamente percepita) porterà ad una maggiore disponibilità di capitale e che tenderà ad abbassare il tasso di interesse a mercato poiché si assisterà necessariamente ad una maggiore competizione per soddisfare la domanda di prestiti.

La relazione del risparmio descritta nel presente capitolo: `tasso-interesse = valore-accumulato / valore-investito` va implicitamente ad imporre una relazione di domanda di capitale costruita sull'offerta totale di capitale disponibile nel mercato. Secondo tale relazione, se tutto il capitale venisse dato in prestito il tasso di interesse sarebbe nullo, mentre se tutto il capitale fosse accumulato il tasso di interesse sarebbe infinito. Benché questi estremi mettano in evidenza dei comportamenti limite del tasso di interesse (legati anche alla necessità di tenere conto di tutte le forme di capitale nella loro globalità e non solo del mercato monetario, come riferito nella questione ancora aperta accennata sopra), nella realtà, gli individui possono domandare ed offrire capitale nelle quantità, al tasso e nel mercato che essi preferiscono in funzione delle più differenti ragioni e ciò porta anche a notevoli differenze tra il tasso di mercato e i rapporti di capitale individuale.

E' interessante illustrare un'applicazione della relazione che fa tuttavia uso di ipotesi aggiuntive e che quindi pone la relazione al di fuori dei principi economici razionali di più generale applicazione.

Adottando la definizione di risparmi individuali come la somma del capitale accumulato (Hoard) e dell'investimento (Investment) `S = H + I`, ed ipotizzando:

- un'uniformità della preferenza temporale degli individui con un rapporto di capitale di ogni individuo pari al tasso di interesse corrente `r = H/I`
- una completa ed uniforme svalutazione del capitale accumulato da ciascun individuo

La relazione del risparmio, nella sua forma originale qui presentata, garantisce che al termine del periodo di prestito *la frazione di capitale globale svalutata sia esattamente rimpiazzata dall'interesse ottenuto dall'investimento.* Ad esempio, con un livello uniforme del 10% di accumulo individuale sul totale dei risparmi (rapporto di capitale = 1/9) che si andrà totalmente a svalutare, la relazione sarà verificata a fronte di un interesse di mercato di 1/9 (~ 11,1%) sulla parte investita (90%). In altre parole, la quantità di capitale investito secondo la relazione garantisce il mantenimento della quantità di capitale precedente posseduta. Questa circostanza porta alla realizzazione di un livello di crescita nullo e stabilisce quindi, in assenza di ulteriori variazioni, un'ipotetica condizione di Economia Uniformemente Rotante (Evenly Rotating Economy - ERE. A questo proposito si faccia riferimento anche alla più estesa trattazione dell'argomento magistralmente condotta da Von Mises ne L'Azione Umana).

Al contrario, un tasso di interesse realizzato indefinitamente sempre maggiore del tasso di svalutazione implicherebbe una condizione di crescita perpetua. A parità di altre condizioni, l'utilità marginale decrescente del nuovo capitale accumulato dalla crescita porterebbe ad una diminuzione del tasso di interesse: quindi *la crescita globale si arresterebbe solamente qualora il livello di capitale raggiunto subisse complessivamente e uniformemente una svalutazione pari al tasso di interesse stesso.*

Tuttavia, come già ricordato in precedenza, questa costruzione teorica può differire, anche significativamente, dalle condizioni che occorrono nella realtà e basate sulla valutazione soggettiva degli individui rispetto ai tassi di interesse, alla svalutazione, agli errori imprenditoriali, alla disponibilità di risorse, spazi, processi tecnologici e innumerevoli altri fattori ed eventi che avranno luogo nel futuro. Da un punto di vista storico è possibile osservare che la quantità di ricchezza è sempre generalmente aumentata dalla preistoria ai giorni nostri. Grazie alla incessante e onnipresente attività imprenditoriale e ad un mercato dei capitali sempre più aperto e ampiamente disponibile, i consumatori hanno potuto godere di una cornucopia di beni e servizi in misura via via crescente nel corso della storia. Sono personalmente incoraggiato a credere (mia valutazione soggettiva "speculativa" ancorché fortunatamente condivisa da molti altri) che tale stato di cose non potrà che proseguire nel futuro, grazie alle nuove frontiere della ricerca, della tecnologia e dell'industria (e.g. lo spazio) e della moneta (sic!), ma non vi è alcuna certezza di ciò. Qualunque cosa accada nel futuro, tuttavia, a differenza delle ipotesi e dei modelli, i principi economici razionali non smetteranno mai di trovare generale applicazione all'esistenza degli individui.

Consumo Speculativo

La catallattica definisce due categorie d'uso del capitale, consumo e produzione. I prodotti vengono prodotti e consumati. La produzione, ovvero la creazione di prodotti, richiede tempo e di conseguenza capitale risparmiato (sotto forma di investimento). Il consumo richiede anch'esso del tempo e di conseguenza necessita anch'esso di capitale risparmiato (come accumulo).

L'energia umana può essere spesa nel tempo libero o nel lavoro, dove la svalutazione dell'energia umana immagazzinata rappresenta un fattore (un costo) di produzione. In ogni caso la conversione di questa energia potenziale in lavoro rappresenta un consumo di capitale immagazzinato. Il lavoro può produrre del cibo e una persona può mangiarlo immediatamente. Si tratta di una forma di economia di assoluta sussistenza, dove l'unico risparmio è rappresentato da energia potenziale immagazzinata nel corpo di un individuo. Il prodotto di lavoro, tempo e fattori naturali viene continuamente consumato o nella produzione (e.g. raccogliendo mirtilli) o nel tempo libero (e.g. dormendo). Ci si riferisce a questo paradigma come ad una vita "dalla mano alla bocca". La proprietà risparmiata in questo processo è il corpo della persona. Un bambino comincia a vivere grazie all'"energia potenziale" donata dalla sua madre.

Il risparmio è quindi la sola fonte sia della produzione che del tempo libero. Sorge quindi spontanea la domanda, come viene impiegato il risparmio? Anche nel caso del cibo che è stato digerito, la domanda rimane. Il capitale impiegato nella produzione viene scambiato per la titolarità di ciò che alla fine viene prodotto. Questa titolarità di un bene futuro è chiamata un "risparmio-investimento" (o semplicemente "investimento"). Il capitale non impiegato nella produzione è chiamato "risparmio-accumulo" (o semplicemente "accumulo"). I risparmi sono la somma del capitale accumulato ed investito di un individuo. Il processo che porta ad impiegare il capitale accumulato nell'investimento o nel tempo libero è chiamato "disaccumulo"

> Dopo aver venduto i suoi servizi, egli acquisisce il proprio denaro guadagnato dalla produzione e quindi lo aggiunge alla propria riserva di denaro. Egli quindi alloca questo guadagno tra consumo e risparmio-investimento, assumendo che non avvenga accumulo e disaccumulo.

Rothbard: Man Economy and State

La Catallattica concerne l'*azione* umana e rifiuta esplicitamente l'analisi dei *pensieri* umani. I pensieri sono soggettivi ma espressi oggettivamente solo in un'azione di scambio. Questo principio è incorporato nella teoria del valore soggettivo. Come fattore necessario sia alla produzione che al tempo libero si *assume* che il tempo abbia valore oggettivo. Non vi è alcuna espressione del fatto che i risparmi di un individuo debbano essere usati nella produzione o nel tempo libero finché essi non vengono disaccumulati. Una persona potrebbe preferire di impiegare i risparmi nella produzione ma mentre sta dormendo essa li consuma sotto forma di tempo libero. In maniera analoga un individuo potrebbe preferire il consumo di mele ma scambiare effettivamente una mela per un'arancia. L'unica espressione oggettiva di una preferenza è rappresentata dallo scambio e ciò include anche il consumo dei risparmi nella produzione o nel tempo libero. Quando non viene impiegato nella produzione il capitale accumulato è chiamato "improduttivo" allo stesso modo di una persona che non è impegnata nella produzione.

L'accumulo è una conseguenza necessaria dell'incertezza. All'aumentare dell'incertezza le persone tendono ad incrementare il loro livello di accumulo a discapito del tempo libero o della produzione. Questo permette al capitale da essi accumulato di essere impiegato in entrambe le attività nel futuro. Tuttavia il capitale improduttivo subisce un costo del tempo. Il tempo possiede oggettivamente del valore. L'opportunità di usare il capitale nella produzione è stata scambiato contro una aumentata certezza. Questo è il costo opportunità della certezza, una spesa. Sia gli usi produttivi che quelli improduttivi del capitale danno luogo allo scambio di opportunità per certezza. Ci si riferisce all'accumulo come alla "liquidità", ed essa risulta necessaria solamente per il fatto che esiste l'incertezza.

Come mostrato ne la Relazione del Risparmio, il rapporto tra risparmi accumulati e quelli investiti è un'espressione della preferenza temporale dell'individuo. Come per tutte le valutazioni quella della certezza rispetto al costo opportunità è soggettiva. Benché il tempo abbia valore oggettivo (i.e. avere più tempo vale di più di averne meno) tale valore rimane relativo e soggettivo. Tuttavia, come per tutte le valutazioni, la conseguenza di ciò è la comparsa di un prezzo oggettivo per il capitale nel tempo espresso sotto forma di scambio e chiamato tasso di interesse. L'interesse rappresenta sia il ritorno sul capitale che il costo del capitale. Il costo opportunità è la perdita di un guadagno produttivo, misurato dal tasso di interesse, che deriva dall'accumulo di capitale.

Un accumulo rappresenta la valutazione soggettiva che esso valga di più rispetto al suo costo opportunità nel corso di quel periodo di tempo. Questo fatto è chiamato "speculazione". Essa è l'espressione della preferenza di possedere un bene rispetto a quella di separarsi da esso ove il costo è misurato dal mancato interesse. L'opportunità di investire l'accumulo nel tempo in cui esso è stato trattenuto è persa per sempre. In altre parole l'atto di non investire capitale rappresenta il consumo del capitale. Con tutto il capitale tenuto in accumulo

non ha luogo la produzione di nuovo capitale e alla fine il capitale verrebbe consumato per intero.

Il modo in cui questa speculazione sia "giustificata" non è rilevante ai fini della distinzione, in quanto il valore è soggettivo. Tuttavia, un certo livello di accumulo risulta necessario poiché vi è sempre incertezza (i.e. del futuro). Una preferenza per il capitale nel presente, che si contrappone a quella nel futuro, è sempre espressa attraverso un accumulo. Una persona può certamente accumulare ad un livello che sia superiore rispetto alla liquidità richiesta per compensare l'incertezza. Ad esempio, una persona potrebbe accumulare per il valore dato dal divertimento dei giochi di fortuna. In questo caso il costo opportunità è dato dalla spesa per il divertimento. Una persona potrebbe anche accumulare per attendere il giusto momento per una vendita (*market timing*). In questo caso il costo opportunità viene chiamato "assorbimento del contante" (*cash drag*). Non importa che una persona abbia anticipato un guadagno o che lo realizzi, l'accumulo rappresenta necessariamente una spesa - perché il tempo ha valore.

Tuttavia la preferenza temporale viene talvolta erroneamente interpretata come una relazione tra consumo e risparmio. Questo fatto viene spesso vagamente descritto come un "consumo differito" o una "gratificazione posticipata". Tuttavia, come è stato mostrato, l'accumulo è una forma di consumo. Il consumo non è stato differito; la gratificazione non è stata posticipata. Compensare l'incertezza rappresenta una gratificazione (la serenità), il divertimento è una gratificazione (una attività di svago), il guadagno potenziale basato su una vendita effettuata nel giusto momento è una gratificazione (anticipazione di un prezzo migliore). Tutte queste situazioni consumano capitale. La distinzione introdotta dal concetto della preferenza temporale sta nello scambio di capitale nel tempo in cambio di interesse. Una speculazione non da luogo ad uno scambio simile.

Tutte le proprietà di una persona (i risparmi) vengono accumulati o investiti. L'accumulo erode il valore della proprietà nel tempo. Le macchine si usurano, il cibo viene convertito in energia, i mobili si deteriorano, il capitale perde valore. Il denaro non è differente, esso declina in valore a causa sia del costo di mantenimento (*cost of carry*) che del costo opportunità. Il valore attuale della moneta viene sempre scontato rispetto al suo valore futuro. Ciò viene descritto come il "valore temporale del denaro". Poiché si effettuerà una spesa di valore futuro, l'accumulo di denaro si sta in realtà svalutando di una quantità pari alla quantità di sconto applicata a tutto il periodo dell'accumulo.

Come mostrato ne il Principio della Svalutazione, acquistare dei beni non rappresenta un consumo. Non vi è mai alcun consumo reale ad eccezione di quello che avviene quando la proprietà si svaluta. Per questa ragione, non c'è distinzione tra il posticipare il consumo di beni o acquistarli subito. Si tratta solamente di uno scambio di un tipo di proprietà con un altro, entrambi soggetti a svalutazione. La preferenza temporale non rappresenta una distinzione tra consumo e risparmi, è una distinzione tra accumulo ed investimento.

L'imprenditorialità comporta necessariamente speculazione ed investimento. L'impiego di capitale è richiesto per la produzione e l'imprenditore sta speculando sul prezzo di ciò che verrà prodotto. Questa speculazione su un bene futuro rappresenta infatti l'inevitabile effetto collaterale di produrre dei prodotti senza prezzo già stabilito. L'imprenditorialità e quindi una "produzione speculativa" mentre la svalutazione di un bene presente è un "consumo speculativo". Poiché ogni stima di prezzo futura è soggetta ad errore, ogni investimento è, in qualche misura, di tipo imprenditoriale. L'investimento rappresenta la produzione speculativa e l'accumulo rappresenta il consumo speculativo. Ciò risulta evidente dal fatto che se tutto il capitale venisse accumulato non ci sarebbe produzione.

La discussione affrontata sopra pone una distinzione tra l'uso produttivo e consuntivo del capitale dal punto di vista di un singolo individuo. Ai fini di una trattazione più semplice abbiamo discusso solamente il consumo relativo al tempo libero (i.e. dell'accumulo del consumatore) evitando di analizzare il consumo produttivo (i.e. l'accumulo del produttore). Mentre un singolo individuo può essere sia consumatore che produttore, un produttore deve anche consumare nella produzione. Poiché il termine diventa sovraccarico di significato, è più semplice pensare all'investimento di una persona come all'investimento nell'attività di produzione di un'altra persona.

Lo *scopo* di una persona è il tempo libero mentre quello di una attività imprenditoriale è la produzione. Entrambi gli scopi sono consuntivi per natura, tuttavia, il consumo espresso nel contesto di una attività imprenditoriale è riservato alla produzione, non al tempo libero. Come avviene per ogni persona, un'attività imprenditoriale deve determinare il suo rapporto tra accumulo ed investimento basato sulla preferenza temporale. L'investimento di una attività imprenditoriale non può essere nella sua stessa produzione, così come quello di una persona non può essere nel suo stesso tempo libero in quanto entrambi sarebbero circolari. Un'attività imprenditoriale acquisisce asset e li svaluta nel tempo. Benché ci si riferisca informalmente a questi ultimi come a degli investimenti, un'attività imprenditoriale non paga a sé stessa un interesse. Questi asset rappresentano capitale accumulato nel processo di consumo con il fine della produzione. Il capitale rimanente è investito in altre attività, come ad esempio fondi di investimento o conti correnti bancari con interesse. Poiché ogni persona accumula una frazione del suo capitale ed investe il rimanente, il credito si espande sulla moneta in funzione della preferenza temporale.

L'idea che una persona sia contemporaneamente un consumatore ed un produttore solleva un quesito sulla classificazione del lavoro. Benché tutte le persone debbano necessariamente consumare, molte sono anche produttori. Una persona impiegata in un lavoro stipendiato è un produttore. Un impiegato investe capitale nella sua persona (e.g. istruzione, reputazione, cibo) ed investe del tempo senza disporre del suo capitale umano quando la sua persona non gode del tempo libero. Gli stipendi e i benefici associati rappresentano il ritorno sull'investimento. A causa della competizione nell'ambito lavorativo, questi ritorni vanno alla ricerca

dell'opportuno livello di interesse in base al loro "valore" a mercato durante la vita lavorativa.

La speculazione è una conseguenza necessaria dell'errore che, a sua volta, è intrinseco sia al consumo che all'investimento. Accumulare è un'azione consuntiva mentre l'investire è un'azione produttiva. Il concetto economico della preferenza temporale è specificamente la distinzione tra l'accumulo e l'investimento. Ciò risulta evidente nella relazione tra preferenza temporale ed interesse economico. **Una più alta proporzione di accumulo rispetto all'investimento riflette una più elevata preferenza temporale ed implica una minore produzione**.

Titolo originale: Speculative Consumption

Indice

L'Inappropriata Denominazione dello *Spam*

Il termine *spam*, nella sua accezione informatica, si riferiva originariamente al *cross-posting* su rete *Usenet* e più tardi è diventato sinonimo dell'invio di email indesiderate. Benché non esista una chiara distinzione tra email desiderate ed indesiderate, i messaggi portano con sé un'identità, non sono fungibili e non comportano alcun tipo di pagamento per essere processati dal destinatario. In confronto, le transazioni Bitcoin sono necessariamente anonime, fungibili e includono un pagamento per essere processate.

Benché il processo di identificazione dello *spam* sia un processo soggettivo, esso è un'attività necessaria in quanto non è previsto alcun pagamento per il processamento del messaggio. Questo processo è facilitato dall'identità e della mancanza di fungibilità. Al contrario, in forza degli obiettivi di anonimità e fungibilità non è possibile verificare la legittimità di una transazione e, grazie al pagamento, non vi è alcuna necessità di effettuare tale verifica. In altre parole, tutte le transazioni valide sono egualmente legittime e questo non rende i nodi soggetti al *denial of service*. Un nome appropriato per una transazione con *fee* basse è "transazione con *fee* basse".

L'invio di un elevato volume di transazioni ridondanti è un tipico problema di *denial of service*, che è indipendente dalle *fee* di transazione e che può essere affrontato da qualunque persona, non solo da colui che effettua la spesa. Transazioni non ridondanti, che incorporano delle spese in conflitto tra loro, non rappresentano un rischio di *denial of service* in quanto esse vengono o rigettate come invalide o accettate grazie ad un sufficiente incremento delle *fee*.

Titolo originale: Spam Misnomer

Indice

Il Paradosso dell'Efficienza

Il mining di Bitcoin, nel suo complesso, non può essere reso più efficiente in termini di costo reale. Poiché tutti i costi si misurano in termini di energia, questa frase può essere riformulata come: Bitcoin non può essere reso più efficiente energeticamente. Paradossalmente, indipendentemente da qualsiasi miglioramento tecnologico venga introdotto, il costo della conferma delle transazioni rimane la somma delle ricompense per la conferma.

In ultima istanza, questa apparente contraddizione deriva dal fatto che la ricompensa determina il costo. Un incremento di *hash rate* allo stesso costo porta ad un incremento della difficoltà al fine di mantenere lo stesso periodo di tempo tra i blocchi, incrementando conseguentemente il costo. Il mining di Bitcoin deve sempre consumare sotto forma di costo l'ammontare della sua ricompensa corrente.

Titolo originale: Efficiency Paradox

Indice

Il Dilemma dello Speculatore in caso di Separazione

In seguito ad una separazione, un possessore della moneta originale si trova davanti alla scelta di tenere o vendere le unità della catena originale o di quella che si è separata.

Come discusso ne la Fallacia del Dumping non vi è modo di influenzare l'esistenza di una catena o dell'altra scambiando o accumulando le unità di una delle due. Di conseguenza, andremo a valutare questa scelta come una questione legata strettamente al modo con cui massimizzare il valore della proprietà esistente a seguito di una separazione.

Data una certa posizione prima della separazione, un proprietario è affetto dall'aumento di costo di conversione delle unità e dalla *replay protection* quando applicabile. Questi rappresentano degli inevitabili costi di scambio nel futuro che riducono il valore attuale netto delle unità. Tuttavia questi fattori non rispondono al quesito.

Le considerazioni rimanenti sono basate sull'*assunzione* che le monete in forma combinata aumenteranno di prezzo nell'intervallo di tempo considerato.

Sotto le ipotesi formulate per il Principio di Consolidamento due monete simili saranno destinate a consolidarsi riducendo a zero il valore di una delle due nel tempo. Se una persona è in grado di sapere quale delle due subirà questa sorte, è un'azione razionale vendere questa moneta in favore dell'altra. Tuttavia, poiché è altrettanto plausibile *non* sapere quale moneta sopravviverà, vi è la possibilità che, vendendo la moneta che avrà successo per quella destinata al fallimento, si sacrifichi *per intero* il valore delle unità originarie. Senza conoscenza del futuro, vendere tutto o una parte di una moneta per l'altra porta ad incrementare il profitto potenziale proporzionalmente ad un livello di rischio più elevato. Per questa ragione è razionale allo stesso modo accumulare entrambe le monete, cosa che preserva le assunzioni ritenute valide prima della separazione.

In conclusione dovrebbe essere sottolineato che entrambe le catene potrebbero fallire qualora il valore si spostasse su una catena indipendente, su una commodity o su una moneta di stato. Questo capitolo si propone solamente di fornire un quadro di decisione razionale basato su assunzioni che tuttavia potrebbero non verificarsi.

Titolo originale: Split Speculator Dilemma

Indice

Etichette di Bitcoin

Fin dal suo inizio, Bitcoin si è sottratto ad una chiara definizione. Questa è una conseguenza dell'uso massiccio che viene fatto di questo termine. Il termine venne coniato da Satoshi in Bitcoin: Un Sistema di Moneta Elettronica Peer-to-Peer come etichetta indicante i suoi concetti essenziali. Più tardi il termine venne anche impiegato per definire: il prototipo della sua implementazione, una catena (una storia) delle transazioni confermate, un insieme di regole di consenso che pongono dei vincoli alla catena (alla moneta), un'aggregato di unità della moneta, una comunità di persone legate in maniera indistinta.

Nonostante esista un solo insieme di concetti, ciascuno degli altri contesti contiene al suo interno un numero pressoché illimitato di possibili variazioni che sono coerenti con essi. Vi sono numerose implementazioni (del prototipo e di tipo differente), le regole di consenso sono state modificate (nel prototipo o in altre implementazioni), la storia varia in maniera dinamica ed arbitraria (anche il blocco genesi implementato nel prototipo sarebbe potuto essere differente senza alcuna conseguenza) e ciascuna moneta manifesta un insieme indipendente di unità ed è supportata dal proprio gruppo di sostenitori.

Per queste ragioni Bitcoin viene usato qui come una etichetta dei Principi della Criptodinamica. Alle implementazione ci si riferisce attraverso il nome del loro marchio come "Bitcoin Core" o "Libbitcoin"; alle catene ci si riferisce attraverso il simbolo di trading usato comunemente, come ad esempio "BTC" e "LTC"; alle regole di consenso di una data catena ci si riferisce utilizzando lo stesso contesto del simbolo di trading come ad esempio "le regole di consenso di LTC"; ad un aggregato di unità della moneta ci si riferisce utilizzando il simbolo di trading in lettere minuscole, come ad esempio in "btc" o "ltc" (cosa che rappresenta un miglioramento rispetto all'ambigua convenzione di usare "bitcoin" per riferirsi ad unità di "BTC"); alle comunità ci si riferisce sia come "*community* Bitcoin" (in generale) o "*community* BTC" (nello specifico).

Nonostante i massimalisti possano rigettare l'uso del termine "Bitcoin" come etichetta concettuale, associandolo invece ad una storia, **il termine venne coniato in relazione ad un insieme di principi e continua ad applicarsi ad esso**. Inoltre, esistono molteplici istanze di catene indipendenti che sono coerenti con con questi principi rendendo l'etichetta basata sulla storia una scelta

ambigua. A causa di questa ambiguità le persone hanno naturalmente adottato la convenzione di riferirsi alle storie in maniera univoca attraverso i simboli di trading.

Titolo originale: Etichette di Bitcoin

Indice

La Pretesa del Marchio

Bitcoin è un insieme di concetti fondamentali, non una catena. Nessuna persona può controllare i concetti. Le persone li useranno per descrivere una o più catene e le separazioni a mano a mano che esse evolvono. Ciò avviene con tutte le monete inclusi l'oro ed il petrolio che vengono scambiati con differenti gradi di purezza e qualità.

Ciò è coerente con la dichiarazione di Bitcoin che lega assieme un insieme di concetti, non un insieme di regole, protocolli o implementazioni. Le persone che hanno investito del capitale hanno un intrinseco desiderio di associare ad esso un marchio, ma non esiste alcuna pretesa "legittima" per giustificare questa associazione.

Titolo originale: Brand Arrogation

Indice

Definizione di Riserva

Una riserva è il capitale posseduto da una persona. Si tratta di capitale presente, al contrario del capitale investito. Il capitale presente si svaluta e per questa ragione rappresenta un costo continuo per il suo possessore. Il rapporto tra capitale riservato ed investito è un riflesso della preferenza temporale del possessore.

Il capitale messo a riserva con lo scopo di finalizzare i debiti è il mezzo con cui si effettua il *settlement*. Ad esempio, quando l'oro è il mezzo di *settlement*, l'oro rappresenta il capitale a riserva. Una promessa sull'oro, come può essere un certificato sull'oro, è un prestito e di conseguenza non rappresenta una riserva per quel tipo di debito. Se il debito può essere finalizzato con certificati aurei, allora il possesso dei certificati costituisce una riserva.

Benché la detenzione di un certificato come riserva rispetto al debito rappresentato dal certificato sembri contraddire la definizione di riserva come capitale presente, essa in realtà non è contraddittoria. In qualità di mezzo di *settlement* il certificato stesso non è altro che un documento cartaceo per la persona che lo tiene in riserva. I termini specificati su di esso hanno valenza sull'emittente del certificato. Nessun costo o guadagno viene subito in un'operazione di *settlement* da parte della persona che tiene a riserva il certificato. Per lui, il costo di *settlement* è solo la conseguenza di trasferire il documento al suo creditore.

La riserva viene spesso confusa con la gestione delle maturità (*maturity matching*). La gestione di differenti maturità e tassi di interesse rappresenta una strategia di gestione del rischio finanziario. Benché la riserva di capitale sia essa stessa una strategia di gestione del rischio, la distinzione per una riserva è che il capitale riservato è "presente" ovvero ha una maturità pari a zero.

Ogni debito implica una mezzo di *settlement*. Come tale, anche nel caso vengano impiegati strumenti di debito come mezzo di *settlement* intermedio, il mezzo stesso possiede, in ultima istanza, un capitale presente riservato. Altrimenti il ragionamento implicherebbe una regressione infinita del debito.

Titolo originale: Reserve Definition

Indice

Definizione di Massimalismo

Il Massimalismo rappresenta uno sforzo nelle pubbliche relazioni teso a scoraggiare la formazione di sostituti per una determinata moneta. Nella misura in cui questo sforzo abbia successo, esso può avvantaggiare gli attuali possessori restringendo l'offerta e di conseguenza elevando il prezzo. Tuttavia, quando le persone non riescono a trovare dei sostituti vicini alla moneta, la loro attività di muove verso quelli più lontani. Nel caso dei pagamenti elettronici questi sono rappresentati in generale dalla moneta di stato.

Il Massimalismo si distingue dalla consapevolezza delle *shitcoin* poiché è caratterizzato dalla promozione di un Bitcoin su tutti gli altri. I proponenti esprimono spesso la contraddittoria teoria secondo la quale nessuna altra moneta possa competere con la loro moneta preferita. Se questo fosse il caso, non ci sarebbe ragione di sostenere una singola moneta.

Titolo originale: Maximalism Definition

Indice

Definizione di *Shitcoin*

Una *shitcoin* è un qualsiasi sistema che non è criptodinamicamente sicuro ma che afferma di incorporare la *value proposition* di Bitcoin.

Si presuppone che le *shitcoin* siano delle truffe, sebbene sia sempre possibile che i proponenti abbiano buone intenzioni ma ignorino i principi della criptodinamica. Ad esempio, le tecnologie *proof-of-stake* sono *shitcoin*.

Nonostante possano esserci implementazioni di Bitcoin più sicure di altre, queste sono questioni di valutazioni reciproche. Non può essere dimostrato che Bitcoin sia un sistema sicuro in senso assoluto. Come tale, il termine non è ragionevolmente applicato a nessun sistema Bitcoin. Ad esempio, le tecnologie basate su *proof-of-memory* potrebbero non essere delle *shitcoin* (sebbene non riescano a raggiungere i loro obiettivi fondamentali).

Titolo originale: Shitcoin Definition

Indice

Glossario

Fondamenti

Persona

Decisore.

Macchina

Esecutore di istruzioni.

L'accordo

Bitcoin

L'insieme di principi che proteggono una Moneta dallo Stato.

> I termini ed i principi sono stati definiti da Satoshi in "Bitcoin: A Peer-to-Peer Electronic Cash System".

Consenso

Un accordo tra Persone.

> Indica anche l'insieme di persone che partecipano ad un accordo.

Moneta

Un Consenso che riguarda un mezzo di Scambio mutuamente accettato.

> BTC è una Moneta

Regole di Consenso

L'insieme dei vincoli che definisce una Moneta.

Regola

Un sottoinsieme delle Regole di Consenso.

Validità

Conformità alle Regole di Consenso.

Validazione

Il Processo volto a determinare la Validità.

Applicazione delle Regole (Enforcement)

L'atto di rigettare dati Invalidi.

Oggetti

Unità

Minima frazione di proprietà che può essere trasferita e rappresentata da una Moneta.

> Il Satoshi è l'unità di Bitcoin.

Trasferimento

Cambio di titolarità che coinvolge un certo numero di Unità.

Transazione

Registrazione Validata di un Trasferimento.

Blocco

Insieme Valido di Transazioni dotate di *Timestamp* e Prova.

Catena

Ramo avente la maggior Prova cumulata.

Transazioni

Script

Insieme di Operazioni che autorizzano un Trasferimento.

Operazione

Dichiarazione atomica (univoca) di intenti.

Contratto

Script che esprime delle condizioni di Trasferimento.

> *Public Key Script* è una formulazione anacronistica per questo termine.

Endorsement

Uno Script che soddisfa un Contratto.

> Signature Script (ScriptSig) è una formulazione anacronistica per questo termine.

Point

Riferimento ad un Output o ad un Input.

Output

Un Trasferimento esplicito collegato ad un Contratto.

Input

Un *Output Point* collegato ad un *Endorsment*.

Output precedente

L'Output al quale si riferisce un Input.

Locktime

Un'espressione relativa alla più recente Validità di una Transazione.

Dust

Un numero insufficiente di Unità necessarie per effettuare un Trasferimento attraverso un Output.

> Le regole di consenso di BTC proibiscono il trasferimento di meno di una unità

Blocchi

Marcatura Temporale (Timestamp)

Una dichiarazione relativa al tempo di produzione di un Blocco.

Tempo Mediano Trascorso

Una media dei *Timestamp* dei precedenti Blocchi.

Prova

Una dimostrazione probabilistica della quantità di Lavoro svolta.

Ramo (Branch)

Una sequenza Valida di Blocchi.

Ramo Debole (Weak Branch)

Un Ramo avente meno Prova cumulata rispetto ad un altro.

> Ramo orfano è un nome fuorviante di questo termine.

Ramo Forte (Strong Branch)

Un Ramo avente maggiore Prova cumulata rispetto ad un altro.

Sequenza

Conferma

Inclusione di una Transazione in un Blocco.

Non Confermata

Una Transazione che non è inclusa in alcun Blocco.

Transaction Pool

L'insieme delle Transazioni Non Confermate.

> Memory Pool (Mempool) è un nome fuorviante per questo termine.

Block Pool

L'insieme dei Blocchi Deboli.

> Pool dei Blocchi Orfani è un nome fuorviante di questo termine.

Blocco Genesi

Il primo Blocco di tutti i Rami di una Moneta.

Profondità (Depth)

Il numero di Blocchi più uno dopo una Conferma.

Altezza (Height)

Il numero di blocchi precedenti contenuti in un Ramo.

Segmento

Un sottoinsieme contiguo (di blocchi) in un Ramo.

Organizzazione

Un Annuncio relativo all'aggiunta di un Blocco alla Catena.

Periodo

Tempo medio trascorso tra due Organizzazioni.

Layering

Scambio effettuato utilizzando una sequenza di Transazioni Non Confermate che possono essere Finalizzate da ambo le Controparti.

Finalizzazione (Settlement)

Conferma di Transazioni Layerizzate.

Denaro

Spesa

La prima pubblicazione di una Transazione.

Doppia Spesa

Endorsment dello stesso Output in due Spese distinte.

Sussidio (Subsidy)

Emissione di nuove Unità ad un Miner.

Inflazione

L'aumento di Offerta dovuta al Sussidio.

> Il termine si riferisce all'inflazione monetaria che non va confusa con l'inflazione dei prezzi.

Commissione di Transazione (Fee)

Un Trasferimento implicito ad un Miner.

Ricompensa (Reward)

La somma del Sussidio e delle Commissioni per un Blocco.

Coinbase

Una Transazione che trasferisce la Ricompensa (di un Blocco).

Maturità

La Profondità alla quale un Output della Coinbase diventa Trasferibile.

Dimezzamento (Halving)

Riduzione (pari alla metà) della quantità di Sussidio.

Difficoltà

Il livello di Prova richiesto per la Validità.

Aggiustamento

Cambiamento nella Difficoltà.

Limite (Cap)

Il limite posto all'Offerta nel tempo.

Prezzo

Media variabile di valori di Scambio.

Capitalizzazione

Prodotto del Prezzo per l'Offerta

Economia

Scambio

Passaggio volontario di proprietà tra due Persone.

Utilità

Il grado di beneficio che ha una certa proprietà per una Persona.

Valore

La preferenza accordata da una Persona su una proprietà rispetto ad un altra.

Offerta

L'insieme di tutte le Unità emesse.

Scambio di Unità

Lo Scambio di Unità per altra proprietà.

Inflazione di prezzo

Aumento nel prezzo medio di Scambio nel tempo.

Accumulare

Possedere per un uso futuro.

> Non si tratta né di speculazione né di investimento.

Speculare

Possedere nell'aspettativa di un aumento di Prezzo.

> In maniera equivalente anche dare in prestito nell'aspettativa di una diminuzione del prezzo.

Dare in Prestito - Investire

Scambiare tempo privandosi di Unità per acquisire (nel futuro) una proprietà di maggiore Utilità.

Prendere a Prestito

Scambiare tempo per Unità che garantiscono al Prestatore maggiore Utilità (nel futuro).

Interesse

Il tasso relativo all'aumento di Utilità nel Dare in prestito.

Profitto

Il ritorno (economico) derivante dalla Speculazione.

> Ciò esclude l'interesse.

Perdita

Fallimento nel percepire l'Interesse in un Investimento.

> Si tratta di profitto negativo.

Volatilità

Variazioni del Prezzo che avvengono nel tempo.

Mercato

Lo Scambio di certe proprietà.

Network

Comunicazione

Trasmissione di dati tra due Macchine.

Protocollo

Un insieme di convenzioni adottate nella Comunicazione.

Peer-to-Peer

Un Protocollo simmetrico.

Client-Server

Un Protocollo asimmetrico.

Latenza

Il ritardo intrinseco nella Comunicazione.

Partizione

Una impossibilità di certi Nodi di Comunicare.

Denial of Service

Utilizzare la Comunicazione per sfruttare difetti nel Protocollo o nell'Implementazione che portano a degradare le prestazioni.

DoS è un acronimo di questo termine.

Componenti

Centro di Mining (Mine)

Uno Strumento che compie Lavoro.

Dispositivo di Mining (Grind)

Uno Strumento che compie operazioni di Hashing.

Propagatore (Relay)

Uno Strumento che propaga nuovi Blocchi.

Nodo

Uno Strumento che esegue l'operazione di Validazione.

Wallet

Uno Strumento che crea Transazioni.

Strumento (Tool)

Un insieme di istruzioni Macchina.

Implementazione

Uno specifico insieme di Strumenti.

Attori

Miner

Una Persona che opera un Centro di Mining.

Operatore di Dispositivo di Mining (Grinder)

Una Persona che opera un Dispositivo di Mining.

Relayer

Una Persona che opera un Propagatore (Relay).

Commerciante

Una Persona che accetta Unità in uno Scambio.

> Utente è un sinonimo comune di questo termine.

Proprietario

Una Persona che ha il controllo di certe Untità.

> Detentore è un sinonimo comune di questo termine.

Sviluppatore (Developer)

Una Persona che crea una Implementazione.

Ricorrente (Claimant)

Una Persona che detiene un titolo di una proprietà sotto il controllo di un Custode.

Custode (Custodian)

Una Persona che controlla la proprietà di un'altra.

Mining

Lavoro

Il processo di produzione di un Blocco.

Candidato

Un Blocco potenziale con una Prova non definita.

Hash

Una singola computazione svolta per Provare la Validità di un blocco Candidato.

Hash Rate

La quantità di Hash calcolati nell'unità di tempo.

Hash Power Apparente

Un frazione di Blocchi in un Segmento di Catena.

> Le stime pubbliche dell'hash power di un miner sono basate su questa definizione.

Maggioranza dell'Hash Power

Un sottoinsieme di Miner dotato di sufficiente Hash Power tale da compiere un Attacco sostenuto nel tempo.

> 51% è una comune approssimazione di sufficiente hash power.

Ottimizzazione

Uno Strumento che riduce il costo del Mining.

Annuncio

La prima comunicazione di un Blocco ad un'altra Persona.

Trattenimento (Withholding)

Il ritardo intenzionale di un Annucio.

Onesto

Un Miner che costruisce sui Blocchi di altri.

Selfish Miner

Un Miner che non si dimostra sempre Onesto.

Varianza

La frequenza variabile con cui si ottiene la Ricompensa.

Disaccoppiamento (Decouple)

Un Centro di Mining che condivide la Ricompensa con un altro al fine di ridurre la Varianza.

Deviazioni

Fork

Una divergenza nelle Regole di Consenso.

Hard Fork

Un Fork che implica una Separazione.

Soft Fork

Un Fork che implica una Separazione a meno che il cambiamento nelle regole non sia Applicato dalla Maggioranza dell'Hash Power.

> Si riduce l'insieme dei blocchi potenzialmente validi.

Separazione (Split)

Una biforcazione di una Moneta.

Riorganizzazione

Un Annuncio che promuove un Ramo Debole sulla Catena.

> Reorg è una abbreviazione di questo termine.

Stallo

L'assenza di incremento di Altezza nel tempo.

Attivazione

Iniziare ad Applicare una nuova Regola.

Segnalazione (Signal)

Una indicazione di un Miner veicolata dai dati di un Blocco relativa all'intenzione di Applicare una nuova Regola.

Privacy

Identità

I modi di associare una Comunicazione ad una Persona.

Tracciamento (Taint)

Determinazione della Proprietà.

Sicurezza

Potere

Il livello relativo di controllo di una Persona su una Catena o una Moneta.

Economia

L'insieme di tutti i Commercianti.

Potere Economico

Una frazione di tutte le proprietà offerte in Scambio.

Hash Power

Una frazione dell'Hash Rate di tutti i Centri di Mining.

Attacco

Utilizzo di Hash Power al fine di realizzare una Doppia Spesa.

> Impedire una conferma è un modo per consentire una doppia spesa.

Cooptazione (Co-option)

Ricorso all'aggressione al fine di controllare dell'Hash Power.

Coercizione

Ricorso all'aggressione al fine di indurre una Attivazione.

Distorsione

Aggressione al Mercato che altera il costo del Mining.

Variazione

Differenze nel costo della risorsa per il Mining.

Censura

Conferma soggettiva.

Stato

Insieme di Persone che utilizzano l'aggressione al posto dello Scambio.

> Opera tipicamente in un regime di impunità all'interno di limiti geografici.

Politico

Che concerne le azioni degli Stati.

Debolezza

Aggregazione

La Tendenza alla ridotta partecipazione nel Mining o nella Validazione.

> Implica il raggruppamento o la centralizzazione.

Raggruppamento (Pooling)

La tendenza verso l'esistenza di pochi Miner, che include il consolidamento dei Relay.

> Collusione è un comune sinonimo per questo termine.

Centralizzazione

La tendenza verso l'esistenza di pochi Commercianti.

> I Commercianti controllano direttamente la validazione.

Delegazione

La tendenza verso l'esistenza di pochi Proprietari.

> I Proprietari controllano direttamente la spesa.

Partizionamento

La tendenza verso Partizioni persistenti.

> L'identità implica l'esclusione.

Correlazione

L'abilità di Tracciare usando metodi statistici di analisi della catena (*chain analysis*).

Titolo originale: Glossary

Indice