Non enumerato

Una varietà infinita di argomenti

Sabato 27 dicembre 2008

Un po' d'oro

Molto tempo fa mi venne in mente l'idea di un po' d'oro. Il problema, in poche parole, è che i nostri soldi attualmente dipendono dalla fiducia in una terza parte per il loro valore. Come hanno dimostrato molti episodi inflazionistici e iperinflazionistici nel corso del 20° secolo, questo non è uno stato di cose ideale. Allo stesso modo, l'emissione di banconote private , sebbene presentasse vari vantaggi e svantaggi, dipendeva allo stesso modo da una terza parte di fiducia.

Metalli preziosi e oggetti da collezionehanno una scarsità imperdibile a causa del costo della loro creazione. Questo una volta forniva denaro il cui valore era in gran parte indipendente da qualsiasi terza parte fidata. Tuttavia, i metalli preziosi hanno problemi. È troppo costoso testare ripetutamente i metalli per le transazioni comuni. Così una terza parte fidata (solitamente associata a un esattore delle tasse che accettava le monete come pagamento) veniva invocata per imprimere un importo standard del metallo in una moneta. Il trasporto di grandi valori di metallo può essere un affare piuttosto insicuro, come hanno scoperto gli inglesi durante il trasporto dell'oro attraverso un Atlantico infestato da sottomarini in Canada durante la prima guerra mondiale per supportare il loro gold standard. Quel che è peggio, non puoi pagare online con il metallo.

Pertanto, sarebbe molto bello se esistesse un protocollo in base al quale i bit irredibilmente costosi potrebbero essere creati online con una dipendenza minima da terze parti fidate, e quindi archiviati, trasferiti e analizzati in modo sicuro con una fiducia minima simile. Un po' d'oro.

La mia proposta per bit gold si basa sul calcolo di una stringa di bit da una stringa di bit di sfida, utilizzando funzioni chiamate in vari modi "funzione puzzle client", "funzione proof of work" o "funzione benchmark sicura". . La stringa di bit risultante è la prova del lavoro. Laddove una funzione unidirezionale è proibitivamente difficile da calcolare all'indietro, una funzione di benchmark sicura ha idealmente un costo specifico, misurato in cicli di calcolo, per calcolare all'indietro.

(1) Viene creata una stringa pubblica di bit, la "stringa di sfida" (vedere il passaggio 5).

(2) Alice sul suo computer genera la stringa di prova di lavoro dai bit di sfida utilizzando una funzione di benchmark.

(3) La prova del lavoro è contrassegnata da un timestamp sicuro. Questo dovrebbe funzionare in modo distribuito, con diversi servizi di timestamp in modo che nessun servizio di timestamp particolare debba essere sostanzialmente basato.

(4) Alice aggiunge la stringa di verifica e la stringa di prova di lavoro con timestamp a un registro del titolo di proprietà distribuito per bit gold. Anche in questo caso, per il corretto funzionamento del registro non si fa affidamento su un singolo server.

(5) L'ultima stringa di bit d'oro creata fornisce i bit di sfida per la stringa successiva.

(6) Per verificare che Alice sia la proprietaria di una particolare stringa di bit gold, Bob controlla la catena di titoli non falsificabile nel registro dei titoli di bit gold.

(7) Per valutare il valore di una stringa di bit d'oro, Bob controlla e verifica i bit di sfida, la stringa di prova di lavoro e il timestamp.

Nota che il controllo di Alice sul suo bit d'oro non dipende dal suo unico possesso dei bit, ma piuttosto dalla sua posizione di vantaggio nella catena di titoli non falsificabili (catena di firme digitali) nel registro dei titoli.

Tutto questo può essere automatizzato tramite software. I principali limiti alla sicurezza dello schema sono quanto bene la fiducia possa essere distribuita nei passaggi (3) e (4) e il problema dell'architettura della macchina che sarà discusso di seguito.

Hal Finney ha implementato una variante di bit gold chiamata RPOW(Prove di lavoro riutilizzabili). Ciò si basa sulla pubblicazione del codice del computer per la "zecca", che viene eseguito su un computer remoto a prova di manomissione. L'acquirente di bit gold può quindi utilizzare l'attestazione remota, che Finney chiama la tecnica del server trasparente , per verificare che un determinato numero di cicli sia stato effettivamente eseguito.

Il problema principale con tutti questi schemi è che gli schemi di verifica del lavoro dipendono dall'architettura del computer, non solo da una matematica astratta basata su un "ciclo di calcolo" astratto. (Ne ho scritto oscuramente diversi anni fa.) Pertanto, potrebbe essere possibile essere un produttore a bassissimo costo (di diversi ordini di grandezza) e sommergere il mercato con bit d'oro. Tuttavia, poiché il bit d'oro è dotato di timestamp, è possibile provare automaticamente il tempo creato e la difficoltà matematica del lavoro. Da ciò, di solito si può dedurre quale fosse il costo di produzione durante quel periodo di tempo.

A differenza degli atomi d'oro fungibili, ma come per gli oggetti da collezione, una grande scorta in un determinato periodo di tempo farà diminuire il valore di quegli oggetti particolari. In questo senso "bit gold" si comporta più come un oggetto da collezione che come l'oro. Tuttavia, l'incontro tra questo mercato ex post e l'asta che determina il valore iniziale potrebbe creare un profitto molto consistente per il "minatore d'oro di bit" che inventa e implementa un'architettura di computer ottimizzata.

Pertanto, il bit d'oro non sarà fungibile in base a una semplice funzione, ad esempio, della lunghezza della corda. Invece, per creare unità fungibili, i rivenditori dovranno combinare pezzi di bit d'oro di valore diverso in unità più grandi di valore approssimativamente uguale. Questo è analogo a ciò che fanno oggi molti commercianti di materie prime per rendere possibili i mercati delle materie prime. La fiducia è ancora distribuita perché i valori stimati di tali pacchetti possono essere verificati indipendentemente da molte altre parti in modo ampiamente o completamente automatizzato.

Pagine

- Casa

Su di me

Nick Szabo

"Un importante pensatore di storia diritto ed economia e le lezioni ch hanno per la sicurezza". -- Adam Shostak, Caos emergente

"Szabo esce con questi saggi che m lasciano a bocca aperta." -- Brian Dunbar

"Leggere materiale eclettico, stimolante e infinitamente affascinante." -- Sean McGrath, Propylon

"Come la maggior parte dei blog ch meritano la mia attenzione, quest blog viene aggiornato solo di rado. Questo perché gli autori dei blog c meritano la mia attenzione pubblicano solo quando hanno qualcosa da dire che è vero, rilevante e non già conosciuto dal loro pubblico. La maggior parte de umani la razza non ha la capacità sapere quando un'idea ha queste t proprietà. L'abilità è particolarmente rara nei campi de politica e dell'economia, motivo pe cui questo blog è una cosa così rar e preziosa". -- Richard Hollerith

Visualizza il mio profilo completo

archivio del blog

- 2018 (1)
- 2017 (3)
- 2016 (4)
- 2015 (3)
- 2014 (3)
- 2013 (3)
- 2012 (8)
- 2011 (12)
- 2010 (9)
- 2009 (29)
- 2008 (55)
  - Dicembre (2)
    - Mercati dell'oro
    - Un po' d'oro
  - ottobre (2)
  - Settembre (4)
  - Agosto (9)
  - Luglio (4)
  - giugno (6)
  - maggio (6)
  - aprile (4)
  - marzo (10)
  - Febbraio (5)
  - gennaio (3)
- 2007 (47)
- 2006 (130)

► 2005 (44)

In sintesi, tutto il denaro che l'umanità ha mai usato è stato insicuro in un modo o nell'altro. Questa insicurezza si è manifestata in un'ampia varietà di modi, dalla contraffazione al furto, ma il più pernicioso dei quali è stato probabilmente l'inflazione. Bit gold può fornirci una sicurezza senza precedenti da questi pericoli. Il potenziale eccesso di offerta inizialmente nascosto dovuto a innovazioni nascoste nell'architettura della macchina è un potenziale difetto del bit gold, o almeno un'imperfezione che le aste iniziali e gli scambi ex post di bit gold dovranno affrontare.

Inserito da Nick Szabo alle 16:16

33 commenti:

Anonimo ha detto...

Nick,
questo non è proprio un commento su questo post, ma poiché non ho trovato un modo per inviarti un'e-mail, ho pensato di utilizzare questo modo per farti sapere che ho fatto riferimento a uno dei tuoi articoli in un post recente sul mio blog fiscale, Don't Mess With Taxes. È nella voce relativa alle tasse sulla proprietà .
Il migliore,
Kay Bell

14:16

Nick Szabo ha detto...

Grazie! Questo è un buon articolo che hai sulle tasse sulla proprietà, ed è affascinante vedere che le case strette sono arrivate in Virginia. . Ecco il mio articolo citato sulla misurazione del valore e le tasse .

14:44

Anonimo ha detto...

Ho appena aggiunto il link dell'articolo nel mio post. Grazie!

15:13

Patrizio ha detto...

Ciao Nick,
Il "Bit Gold" di maggiore interesse è la serie di bit che si sommano a nuove preziose informazioni. Lo sforzo implicato nel calcolo di un valore hash è significativo, ma lo sforzo veramente importante è quello implicato nella creazione di qualcosa come un contributo sostanziale al kernel Linux, o un documento scientifico che descrive la ricerca originale. Il flusso di bit precedentemente sconosciuto che descrive una proteina che cura il cancro è VERAMENTE un po' d'oro, no?

Il lavoro che sto facendo su http://infoeng.sourceforge.net è progettato per creare strumenti finanziari digitali che rappresentino tali flussi di bit (ovvero software e altre informazioni utili).

Ci scusiamo per il blurb di marketing, e per un blurb incompleto, ma ho pensato che sarebbe stato appropriato. :)

Patrizio

20:53

l'antirobot ha detto...

Sarebbe questa la valuta di un'economia dell'informazione? Immagino che un sito di contenuti prodotto da un utente assegna bitgold agli utenti che hanno creato contenuti popolari, o forse contenuti promossi all'inizio che sono diventati popolari. Il sito web guadagna, compra oro e lo mette in una tesoreria. Quindi gli utenti possono scambiare il loro bitgold con oro reale. Il sito può manipolare/mantenere il tasso di cambio emettendo più bitgold. Immagino che questo sia il modo in cui funzionerà il governo tra qualche anno, quando Internet sarà il governo.

20:18

Daniel A. Nagy ha detto...

Ho due problemi con bitgold:

0.) Cosa lo rende desiderabile? Perché dovrei voler possedere le prove di uno spreco di lavoro computazionale? L'oro è desiderato per vari motivi evolutivi a livello di istinti, almeno con alcune persone. Ma pezzi senza senso? Non riesco a vedere come Bitgold riesca a diventare denaro.

1.) Quanto è esatta la legge di Moore? Qual è il tasso di cambio tra un gigaciclo oggi e un gigaciclo l'anno prossimo?

16:20

Anonimo ha detto...

Sono in qualche modo d'accordo con il punto #0 di "Daniel A. Nagy".

Continui a dire che questo "accadrà". Ciò deve richiedere un po' di generalizzazione eccessiva di un principio (gli standard monetari si basano su cose scarse) quando non hai spiegato perché o come è persino
probabile che venga adottato uno standard monetario "bit gold" *tra tutte le possibili alternative* .

Ipoteticamente, si potrebbe sperare che *qualcuno* possa essere motivato ad adottare o promuovere lo standard se un sistema "bit gold" può essere costruito in modo tale che la produzione di "bit gold" svolga un lavoro di valore effettivo per una parte che sarebbe quindi motivata per supportare lo standard. (Non che tu abbia mai accennato a questo punto.)
Esempi di lavoro utile (se possibile inadeguato) potrebbero includere qualsiasi delle attività che sono attualmente svolte dal calcolo distribuito volontario, come il SETI e l'analisi biochimica.

Tuttavia, dubito che governi e banche centrali potenti sarebbero ansiosi di promuovere o addirittura consentire il passaggio a uno standard "bit gold" quando ciò demolirebbe gran parte della loro attuale capacità di influenzare l'economia attraverso la politica

monetaria.

Ad ogni modo, se leggi fino a qui, per favore capisci che hai scritto molto che ammiro, e questo caso è un'eccezione relativamente rara.

--Persona che digita il gatto

20:50

Anonimo ha detto...

Penso che un database contenente il DNA di ogni individuo generi una chiave privata/pubblica.

Quando nasce un essere umano, il DNA di quell'uomo va nella "Banca" e a quell'essere umano viene assegnato 1 "dollaro speciale" da utilizzare durante la sua vita, in cambio di beni o servizi.

Quindi, ad esempio, acquistare una pagnotta sarebbe 0,00000648 "specialdollaro" poiché 365 * 80 / 2 = 14600 (1 pagnotta ogni 2 giorni).

Per fare il cambio, firma l'importo con la tua banca e genera una nota di tale importo con la tua chiave pubblica.

Per prevenire l'inflazione, la "Banca" può detrarre una percentuale da ciascun conto bancario ogni volta che un individuo muore.

Sembra pazzesco, ma con la tecnologia odierna qualcosa del genere è possibile, ma noioso.

5:07

Jack Lloyd ha detto...

"A differenza degli atomi d'oro fungibili, ma come per gli oggetti da collezione, una grande scorta in un determinato periodo di tempo farà diminuire il valore di quegli oggetti particolari".

Non sono convinto che questa distinzione sia effettivamente corretta. È solo il caso che, negli ultimi secoli, la quantità di oro appena disponibile in qualsiasi anno come percentuale dello stock totale è stata relativamente piccola, quindi non osserviamo questo effetto. Tuttavia in Spagna nel 1500 la quantità di oro importata dal nuovo mondo era sufficiente a causare una notevole inflazione.

Come esercizio intellettuale, considera cosa accadrebbe al prezzo dell'oro se ogni giorno ogni persona nel mondo si svegliasse con un nuovo luccicante kruggerand sotto il cuscino.

18:15

Sconosciuto ha detto...

So che questo è un vecchio post, ma se sei ancora interessato ai sistemi di proof-of-work e alla loro applicabilità come valuta digitale, potresti voler controllare http://www.bitcoin.org È un P2P decentralizzato, criptovaluta basata su un algoritmo proof of work.

00:09

Sinonimo ha detto...

Il denaro, in termini generali, è un fattore limitante per il progresso della civiltà umana.

Con la tua idea, chiunque abbia un computer ha la capacità di creare ricchezza! Ha più o meno lo stesso modello di business della terra, chiunque abbia la terra può vivere da essa in vari modi.

La tua idea mette il potere della ricchezza nelle mani della gente comune. Spero che prenda piede!

7:14

Tommy J ha detto...

Sono d'accordo, questo suona come un concetto rivoluzionario e spero che esca. . . . .almeno in forma di prova.

6:02

Anonimo ha detto...

Ciao Nick,

ottimo articolo! Sono un produttore di HuffPost Live, la rete di notizie in streaming online dell'Huffington Post. Sto lavorando a una web-chat, prevista per oggi, martedì. 2/12 alle 17:00 ET su Bitcoin. La valuta virtuale regnerà in futuro? Amazon ora ha "monete" e Bitcoin si sta preparando per un futuro dipendente dalla valuta virtuale. La crittografia può essere utilizzata per evitare le insidie dell'autorità centrale?

Mi piacerebbe sentire i tuoi pensieri su questo argomento. Per favore fatemi sapere se siete interessati e disponibili ad unirvi a noi tramite webcam e vi invierò ulteriori dettagli.

Migliore,
Shelley Thomas
shelley.thomas@huffingtonpost.com
live.huffingtonpost.com

7:04

Anonimo ha detto...

Congratulazioni per aver inventato BitCoin

22:04

Anonimo ha detto...

omagunloye@gmail.com

Mi piace questa idea, ma quello con cui non sono d'accordo è la centralizzazione. Bitcoin è già su quello, quindi perché non lo implementi con ... beh, inviami un'e-mail per scoprire i miei pensieri (se ti interessa).

8:47

Anonimo ha detto...

Grazie per aver gettato le basi per bitcoin Nick, abbiamo un grande debito con te.

20:40

hai gli antipasti...

Ecco il resoconto di un grande momento della storia umana.

11:40

Sebastian Schepis ha detto...

Un giorno, le persone considereranno questo post come l'effettivo momento della genesi di Bitcoin. Questo è un pezzo di storia digitale, degno di conservazione. Grazie Nick.

8:23

Sandro ha detto...

È un piacere lasciare il mio segno minuscolo in questa pagina fondamentale per la storia dell'umanità.

17:58

jessilidia ha detto...

It's very *odd* that such smart people miss the basic problem left unsolved. No matter what the token, its value is what you can exchange it for.

The real threat to the stability of currencies has been the self-contradictory *practice* (whatever coinage is used) of compounding returns on investment, as if believing that every coin earned in the past can be owed limitlessly growing new returns in the future.

Yes, I know the idea of investors having the responsibility to **spend their winnings**, as the one way to keep debts in the system from becoming an existential threat to the system, and destabilizing the pool, is just silly and abhorrent to money makers as anything could be. It's also VERY REAL OBLIGATION TO PRESERVE THE SYSTEM, in environmental terms.

No matter what pile of credit you accumulate, it's ONLY real value is what you can EXCHANGE IT FOR. So accumulating credits for SERVICES NOT CONSUMED, withdrawing the credit to your own account exponentially, and so removing it from the system for exchanges as a rule, as we're all told to do to "make money", doesn't work.

It does in fact directly cause what you can exchange it for to inflate in false value to a point of collapse, *very naturally*.

4:51 AM

Anonymous said...

Here lies something beautiful. Polymatheus

8:53 AM

PeterIII said...

Well said Sandro.

Thank you Nick.

12:47 PM

Tom Eck said...

Mssr. Szabo, the entire cryptocurrency 'establishment' owes you an immense debt of gratitude. I do agree with some of the comments (and had arrived at the same opinion independently) that we'd be better off with a POW function that does something more important than just solving a meaningless puzzle. I'm thinking of a domain-specific function such as predicting protein folding (critical in medicine and bio-tech) or for general purpose (e.g. spending cycles on a highly distributed problem, which has its own value). Of course, the two major constraints of POW must be maintained: 1/ confirmation of the solution must be trivial, and 2/ the computational cost for producing the solution must be controllable. Or maybe not - perhaps you get more in return for having provided more value in your POW.

4:23 PM

Unknown said...

Thank you soo much Nick, your thinking has changed my life in nearly every aspect. Much love and respect.

6:10 PM

Anonymous said...

great idea that will revolutionize the way we do business. its now 2015... only a couple of more years and I believe it will be a mainstream thing. Congratulations on your good work.

Deno

7:05 AM

Anonymous said...

One small post for Nick, a giant leap for humanity.
Simply Nobel prise worthy.
MG

7:09 PM

Unknown said...

You changed many a nerds life

3:45 AM

Matthew said...

And thus the world is changed, forever, for the better.

Thanks Nick

7:56 PM

zac said...

Interesting to think of the (cost of work)/coin as the fundamental price-driving force. Makes me wonder what will happen to the price of other coins when the rewards halve, or the even more unknown territory, proof-of-steak

4:26 PM

Nosliv said...

Inspiring...

Freedom is never given; it is won.

8:26 AM

Anonymous said...

Nick I hope this concept becomes every mans reality :)

9:48 PM

Alex Millar (@bitcoin3000) said...

Nick, amazing work. Thank you. That you foresaw the issue of ASIC's is demonstrates your great knowledge: "The main problem with all these schemes is that proof of work schemes depend on computer architecture, not just an abstract mathematics based on an abstract "compute cycle." "

2:17 PM

Charles said...

RISPETTO SIGNORE! Grazie per tutto quello che hai fatto NS.

18:49

Posta un commento

Post più recente Casa Post più vecchio

Iscriviti a: Pubblica commenti (Atom)

Tema semplice. Realizzato da Blogger .