

Bitcoin vs Bitcoin Cash: un agosto di fuoco, fra le gioie dei traders

scritto da Alberto De Luigi | 1 Settembre 2017

Indice:

- **Bitcoin**
- **Bitcoin Cash**
- **The Big Short: il trading a margine fatto con scienza**

Bitcoin

Spinti dall'enorme crescita del valore del Bitcoin nel primo trimestre 2017, negli ultimi mesi gli utenti hanno preso d'assalto servizi come Kraken o Coinbase: registrarsi e verificare gli account era divenuta un'odissea, i server degli exchange avevano cominciato a cigolare sotto il peso del traffico elevato. Mentre Coinbase dichiarava 1 milione di nuovi utenti in un solo mese, Kraken nello stesso periodo rispondeva alle richieste di supporto chiedendo agli utenti di avere pazienza e ammettendo esplicitamente di essere sottodimensionati in numero di personale. Tuttavia, in netto contrasto con questo nuovo flusso di investitori e neofiti appassionati, il prezzo sembrava essersi stabilizzato in una fascia attorno ai 2000€.

A frenare i desideri di acquisto degli utenti erano gli eventi previsti per il 1 agosto, in particolare le voci sul fork BIP148 detto UASF, che pretendeva di attivare SegWit forzando il consenso dei miners e quindi, eventualmente, provocando una divisione della rete, qualora ci fossero miners schierati con sufficiente potenza di calcolo da entrambe le parti. L'incertezza relativamente a ciò che sarebbe potuto accadere

spaventava i mercati e tratteneva l'euforia degli investitori.

L'accordo di New York del 23 maggio ha tuttavia permesso di attivare SegWit grazie all'implementazione di BIP91, ovvero la prima parte dell'upgrade previsto dall'accordo, mentre la seconda parte avverrà a Novembre. Come previsto, uno split dovuto a UASF non è avvenuto, poiché BIP91 è passato ai voti con la stragrande maggioranza già a luglio, forzando tutta la rete a segnalare BIP141 (compatibile con BIP148) prima di agosto (evitando così UASF) e ottenendo l'effettiva attivazione di SegWit il 24 agosto (vedasi l'articolo relativo).

Il desiderio di acquisto degli utenti, tenuto a freno dalle paure per BIP148, si è potuto quindi scatenare solo dopo il primo agosto e il prezzo del Bitcoin è quasi raddoppiato in un mese. Ad un esame attento della situazione tecnica ed economica, questi eventi erano assolutamente prevedibili e qualsiasi trader ben informato avrà certamente pensato di aprire almeno una posizione long su BTC durante il mese. Anche e soprattutto su questo blog avete letto le anticipazioni dell'andamento del prezzo e di quello che sarebbe accaduto. La vicenda dei forks e degli upgrade infatti è narrata nel dettaglio sin dall'articolo del 22 maggio che rivelava (in anteprima mondiale) i primi leaks e rumors relativi all'accordo di New York.

Chi ancora non ha fatto il grande passo, sappia che non è mai troppo tardi per entrare nel mercato. Il valore del Bitcoin nel lungo periodo continuerà a crescere. Grazie a SegWit, la capacità massima teorica di transazioni sostenibili dalla rete è quadruplicata. Ovviamente, i servizi e i wallet hanno bisogno di tempo per aggiornarsi e quindi gli effetti benefici dell'upgrade si vedranno solo nel corso del tempo. Infatti l'upgrade SegWit è un soft fork retrocompatibile, quindi non ha richiesto l'aggiornamento immediato di tutti i clients.

Un importantissimo risultato dell'upgrade è la possibilità di

testare sul campo i primi clients e le prime apps che permettono pagamenti tramite la rete Lightning Network. Attualmente i principali sviluppatori di software che utilizzano LN stanno studiando uno standard comune affinché i clients possano interagire al meglio fra loro. Una volta che questa tecnologia sarà affinata e diffusa, due saranno gli effetti tecnologici principali:

- Pagamenti istantanei, anonimi, a fee basse o bassissime
- Scalabilità del Bitcoin aumentata esponenzialmente. Finalmente sarà possibile un'adozione di massa del Bitcoin, senza che le fee e i tempi di transazione aumentino parallelamente all'aumento di adozione

Un'ulteriore novità è l'annuncio da parte dell'azienda Blockstream di una connessione satellitare per Bitcoin. Il satellite non rende più necessario avere una connessione a internet e permette così di utilizzare Bitcoin ovunque. Questo fatto è importante soprattutto per quei paesi del terzo mondo dove la percentuale di persone unbanked è altissima e dove le monete di Stato sono inaffidabili e iperinflazionate. Il Bitcoin potrebbe costituire davvero la svolta per queste economie e aiuterebbe alcune popolazioni a emanciparsi dall'ingordigia dei burocrati e politici, oltre che facilitare alcune zone del mondo ad avere accesso a mercati internazionali.

Bitcoin Cash

Mentre il pericolo di UASF sfumava, si è verificato un evento estremamente interessante per tutti gli holder di Bitcoin. Un gruppo di utenti contrari all'upgrade SegWit ha dato vita ad una nuova moneta: Bitcoin Cash, la cui data di lancio coincide proprio col primo agosto. Il motivo di aver scelto proprio quella data, in anticipo rispetto all'upgrade a SegWit avvenuto effettivamente il 24 agosto, è che, qualora SegWit2x

non fosse passato ai voti dei miners e di conseguenza i sostenitori di BIP148 avessero tentato un UASF (User Activated Soft Fork) per approvare SegWit già il 1 agosto, Bitcoin Cash avrebbe comunque forkato dal network.

Alla conferenza "The future of Bitcoin" lo sviluppatore Amaury Séchet presentò l'idea di Bitcoin Cash, che è stata promossa in primis da Bitmain, azienda produttrice di mining hardware nonché proprietaria di alcune mining pool (Antpool, BTC.com e ConnectBTC) e con partecipazioni in varie altre aziende. La somma delle tre pool possedute da Bitmain ammonta a circa un terzo dell'hashpower dell'intero network Bitcoin. Si può dire che Jihan Wu, alla guida di Bitmain, sia l'uomo più influente sulle decisioni politiche negli upgrade di Bitcoin. Il motivo del supporto di Jihan a Cash era facilmente intuibile:

SegWit2x è una soluzione di compromesso fra l'aumento del blocksize (scalabilità onchain) e SegWit (scalabilità offchain). Prima dell'accordo su SegWit2x (BIP91 è passato con oltre il 90% dei voti), SegWit (BIP141) raggiungeva un massimo del 36% mentre il 50% di hashrate supportava soluzioni come Bitcoin Unlimited che prevedevano l'aumento del blocco. Qualora SegWit2x fosse fallito e UASF avesse avuto successo, sarebbe stato chiaro che la via onchain avrebbe avuto molte più difficoltà ad affermarsi in futuro. Jihan Wu, firmando il New York Agreement e sostenendo SegWit (tramite BIP91), rinunciava a un'ottimizzazione dei suoi Antminer detta Asicboost (incompatibile con SegWit), ma come molti altri miners non era certo disposto a perdere anche ogni prospettiva di scalare onchain a breve o medio termine. Per questa ragione, in via preventiva, Bitmain ha pubblicato un post a supporto del client Bitcoin ABC (Adjustable Blocksize Cap), ovvero il client di riferimento per il fork Bitcoin Cash.

Nel post si specifica che ABC sarebbe stata una soluzione di ripiego qualora SegWit2x fallisse. In seguito, con la vittoria schiacciante di BIP91, Bitcoin ABC è stato messo da parte da Bitmain, ma alcuni utenti particolarmente influenti nella

community internazionale hanno voluto comunque portare avanti l'idea del fork di Bitcoin Cash, nonostante non ci fosse un significativo hashpower a favore. In particolare l'italiano Franco Cimatti (HostFat), già sostenitore di soluzioni di scalabilità onchain come Bitcoin Unlimited, è l'autore di alcune delle principali pubblicazioni relative a Bitcoin Cash nei canali più utilizzati dalla community per le comunicazioni pubbliche: BitcoinTalk e Reddit. Ad es: <https://bitcointalk.org/index.php?topic=2040221.0>

Avendo Bitcoin Cash ottenuto così una certa rilevanza mediatica, qualche miner si è spinto a sperimentare il fork, nonostante il rischio di incorrere in alcune perdite per via della spesa energetica. Così la mining pool cinese ViaBTC ha deciso, insieme ad un altro miner ad oggi ancora rimasto anonimo, di impiegare una parte di hashpower a favore di Bitcoin Cash. È curioso notare che entrambi i miners hanno conservato i BCH minati senza venderli, forse per non aumentare ulteriormente l'offerta e quindi mantenere alto il prezzo nei primi giorni di vita della nuova moneta.

Come era già stato anticipato su questo Blog, il lancio di BCH non sarebbe stato deleterio per Bitcoin, pur trattandosi tecnicamente di un fork della blockchain Bitcoin. Bitcoin Cash infatti è in tutto e per tutto una nuova moneta, come Litecoin o qualsiasi altcoin, con l'unica differenza che ogni possessore di Bitcoin ha ottenuto un equivalente ammontare di Bitcoin Cash (seguendo alcuni accorgimenti tecnici). Mentre BIP148 avrebbe potuto portare a una guerra fra miners (e altri stakeholders di Bitcoin), in cui il vincitore avrebbe determinato quale delle due catene sarebbe stato l'unico vero Bitcoin, nel caso della creazione di Bitcoin Cash invece le due blockchain sono chiaramente distinte, andando a formare due network e monete differenti senza creare conflitti interni.

Un **articolo** di questo blog spiegava come ottenere e vendere Bitcoin Cash, prevedendo che probabilmente la nuova moneta

avrebbe avuto effettivamente un certo valore, per quanto basso potesse essere. Personalmente mi aspettavo che il crollo del valore di Bitcoin Cash sarebbe avvenuto immediatamente, non appena i primi holders di Bitcoin avrebbero venduto in massa i propri BCH. Tuttavia, le mie previsioni sono state disattese per via del verificarsi di circostanze tecnologiche molto particolari.

La potenza di calcolo spostata dalla catena BTC a quella BCH è stata di circa il 3%, appena sufficiente per creare i primi blocchi solo ore dopo il fork. Questo significa che per spostare i BCH da un indirizzo a un altro era necessario attendere ore o addirittura giorni. Gli exchange che sono soliti accreditare all'utente i BTC solo dopo almeno 3 conferme, per i BCH invece ne attendevano 20. Infatti la catena di Cash, avendo una ridotta potenza di calcolo, è molto meno sicura in caso di attacco. I pagamenti in BCH vengono quindi accettati solo dopo la creazione di molti blocchi, quindi solo dopo molto tempo l'effettiva immissione della transazione da parte dell'utente. Per questa ragione, specialmente nei primi giorni di vita di BCH, le transazioni verso gli exchange (per lo più di chi spediva BCH per venderli) erano lentissime. Inoltre solo alcuni exchange (come ViaBTC) accettavano depositi in BCH sin da subito. Questa combinazione di fattori è risultata in un'insolita situazione: la mancanza di offerta di BCH sugli exchange. Al contrario, la domanda era sin dai primi momenti del fork piuttosto sostenuta, probabilmente per via di immissione di moneta fiat. Tale situazione era assolutamente palese soprattutto guardando alla differenza di prezzo di BCH fra gli exchange che accettavano depositi e quelli dove l'offerta di BCH non era ancora arrivata.

Che sia stata un'immissione di moneta fiat a tirare su il prezzo di BCH e non la compravendita mediante altre cyptomonete si può assumere dai grafici del prezzo delle varie crypto. Ben pochi hanno venduto Bitcoin per ricevere Bitcoin

Cash, tant'è che il prezzo del BTC non ha risentito affatto negativamente del fork e nemmeno altre altcoin come Ethereum hanno visto cali sostanziali. L'acquisto di BCH mediante euro o dollari è probabilmente dovuto alla recente moda o "febbre" per le cryptomonete. È ricorrente il fatto che ad ogni lancio di una nuova ICO o una nuova altcoin, gli utenti acquistino nella speranza che si ripeta il fenomeno Bitcoin: "pochi euro oggi potranno essere milioni in futuro". In realtà, la stragrande maggioranza di queste altcoin sono destinate a finire nel nulla.

Personalmente, per quanto riguarda la tecnologia di Bitcoin Cash, lo ritengo un downgrade più che un upgrade, rispetto al Bitcoin di SegWit, perciò non gli avrei dato un centesimo, anzi ho venduto immediatamente i miei BCH, nel timore del crollo immediato appena la massa dell'offerta avrebbe raggiunto gli exchange. Non avevo però tenuto conto di due cose:

- L'asincronia fra la domanda, immediatamente presente al lancio di BCH, e l'offerta che invece tardava a raggiungere gli exchange.
- Il fatto che gli investitori spesso non sono informati a fondo sulle questioni tecnologiche. Sui media si poteva leggere semplicemente di un upgrade di Bitcoin, perciò molti investitori avranno pensato che BCH potesse essere una versione potenziata di BTC, ma il vero upgrade di Bitcoin era SegWit, mentre BCH è un fork conservativo per evitarlo.

Questi fattori hanno portato ad una bolla speculativa, dove il prezzo del BCH era chiaramente distorto verso l'alto per via dell'assenza di un'offerta in grado di soddisfare la domanda. Alcuni bravi trader sicuramente avranno saputo cavalcare la bolla riuscendo a uscirne prima del crollo. BCH ha così raggiunto i 750\$ in poche ore dal lancio su numerosi exchange. Chi come il sottoscritto aveva venduto per molto meno è rimasto a bocca aperta osservando l'opportunità bruciata. Ma

non tutto era perduto...

The Big Short: il trading a margine fatto con scienza

Confidando nelle leggi economiche e nel fatto che gli holder più ricchi ed esperti di BTC avrebbero venduto in massa i propri BCH una volta raggiunti gli exchange, molti trader hanno aperto una posizione di margin trading in short, scommettendo su un ribasso del BCH. Una conferma che lo short avrebbe funzionato era il divario del prezzo di circa il 30% fra gli exchange dove i depositi in BCH erano già ammessi (come Bitfinex, con prezzo del BCH inferiore) e quelli dove c'era ancora solo la possibilità di acquistare, ma non depositare e quindi vendere BCH (come Kraken, con prezzo decisamente maggiore).

Aprire una posizione in short è considerata una scommessa rischiosa, ma il mercato delle crypto è molto diverso dalla borsa. Nel caso in esame è stato possibile effettuare un'operazione di short con una buona dose di sicurezza, conoscendo bene i fondamentali tecnologici delle crypto e le leggi economiche che governano il mercato. I guadagni che si possono ottenere col trading a margine sono notevoli: con uno short fatto al momento giusto, si può raddoppiare il capitale in brevissimo tempo, con un guadagno netto del 100%. Ad esempio all'apertura dei depositi fra il 4 e il 6 agosto, chiunque avesse shortato BCH contro BTC ponendo a collaterale 10BTC, avrebbe avuto un guadagno netto di 10BTC senza problemi, ritrovandosene 20 sul conto (ma con un po' di fortuna, entrando proprio al top e uscendo al bottom, i margini di guadagno sarebbero stati decisamente maggiori). A breve sul blog verrà aperta la sezione "Trading", che fornirà tutte le informazioni necessarie ai neofiti per capire i termini e le regole del margin trading e spiegherà come effettuarlo sui principali exchange, aprendo o chiudendo posizioni long o short. Gli utenti iscritti alla **newsletter** verranno informati.

Ma agosto non aveva ancora finito di offrire occasioni, un'altra operazione profittevole che si poteva eseguire con buona sicurezza era l'arbitraggio. Dopo lo scoppio della bolla, era rimasto un notevole divario fra alcuni grossi exchange come Kraken e Bitfinex. Il pomeriggio del 7 agosto mi trovavo in spiaggia quando il mio compagno di merende Gianluigi Crimi mi notifica che 23 minuti prima l'account ufficiale di Kraken aveva tweettato che i depositi di BCH erano finalmente aperti. Il prezzo era il 25% superiore rispetto a Bitfinex. Alla notizia, corro a casa per acquistare BCH su Bitfinex e rivenderli su Kraken. Il blocco 478438, insolitamente grande rispetto ai precedenti (36.000 BCH e 1,6mb) veniva quindi validato, contenente anche una grossa transazione diretta da Bitfinex a Kraken. Venti blocchi più tardi, al blocco 478458, la transazione veniva confermata dall'exchange e la somma poteva essere rivenduta. Dal momento della validazione del blocco, sono passati pochi istanti e il divario fra i due exchange si è "magicamente" azzerato. Sui mercati tradizionali come il FOREX, fare arbitraggio "a mano" è praticamente impossibile, poiché ci sono BOT programmati molto più veloci degli uomini. Ma il mercato delle crypto è molto diverso. L'esempio riportato presenta solo uno degli entusiasmanti vantaggi del mercato crypto per gli appassionati di trading, non certo gli unici. Anzitutto, è possibile entrare nel mercato senza alcun costo e investire qualsiasi tipo di somma, anche solo pochi euro. Inoltre è possibile farlo in modo anonimo, registrandosi semplicemente sugli exchange con mail e password (a patto di possedere in partenza dei Bitcoin da tradare e che non si esca o entri dagli exchange in moneta fiat).

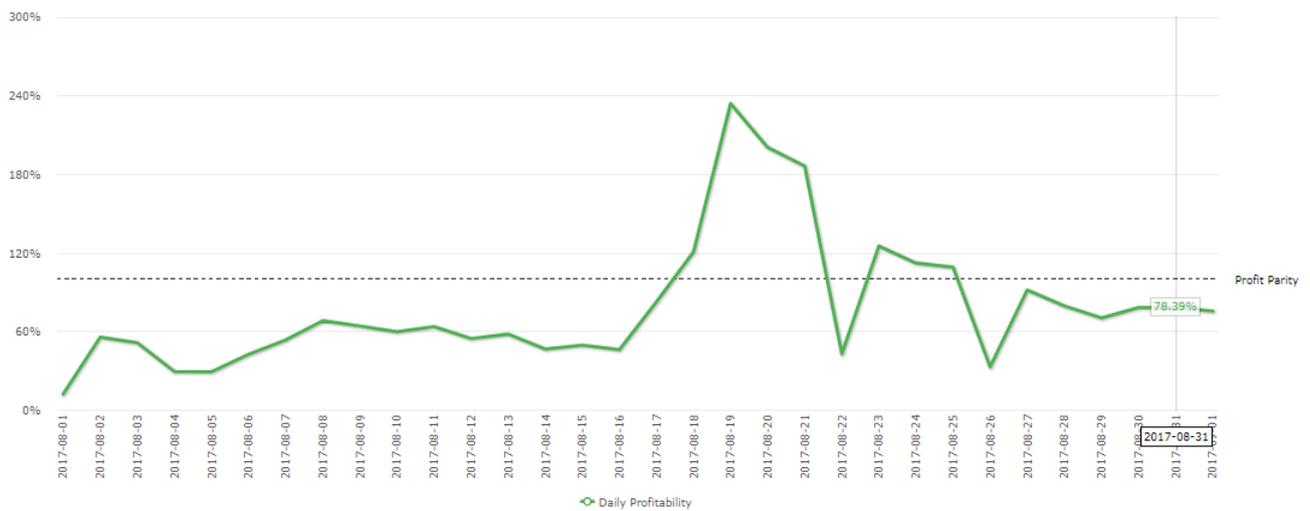
Successivamente, i movimenti del prezzo di Bitcoin Cash hanno seguito dei pattern interpretabili mediante la profittabilità del mining sulla blockchain. BCH ovviamente presenta alcune regole modificate rispetto al protocollo BTC e fra queste anche un aggiustamento rapido della difficoltà, per affrancarsi dalla difficoltà di mining troppo elevata di

Bitcoin. Infatti i supporters di Cash immaginavano che l'hashrate a favore sarebbe stato una frazione irrisoria di Bitcoin, quindi per avere una blockchain funzionante doveva essere necessariamente prevista una misura di aggiustamento di emergenza della difficoltà di creazione dei blocchi, ripristinando così la normale velocità di validazione delle transazioni e creazione di nuovi BCH (un blocco dovrebbe essere creato mediamente ogni 10 minuti, come su BTC). I miners si sono però messi a "giocare" su questa nuova regola dell'aggiustamento della difficoltà: nel momento in cui la difficoltà si abbassa, i miners creano numerosissimi blocchi in pochissimo tempo (rispetto all'hashpower ed elettricità impiegati), quindi ottenendo maggiore profitto, per poi attendere periodi senza effettuare mining (ovvero tornando ad impiegare hashpower sulla catena Bitcoin anziché Bitcoin Cash) per far scendere nuovamente la difficoltà. Quando infatti passano 12 ore senza che siano minati 6 blocchi, la difficoltà scende, la profittabilità di mining diviene superiore rispetto alla blockchain Bitcoin e il miner torna su Cash, con un singolare ping pong. Al 2016esimo blocco creato, scatta nuovamente il retarget della difficoltà rallentando la catena. Su <https://cash.coin.dance> si può vedere la profittabilità del mining sulla catena BCH rispetto alla catena BTC. Si può notare dai due grafici riportati sotto come il prezzo del coin sia perfettamente proporzionale alla profittabilità di mining sulla catena. La relazione di causalità è probabilmente in entrambi i sensi: se il prezzo sale, sale la profittabilità, ma se la difficoltà è elevata e i miners tornano su BTC senza più minare blocchi, la catena BCH rimane in stato di congelamento totale fino al cambio di difficoltà successivo, perciò il prezzo scende. Ceteris paribus, si può quindi ipotizzare una discesa del prezzo nel momento in cui scatta l'aumento di difficoltà.

[Switch to Log Chart](#)

Daily Bitcoin Cash Profitability Against Original Chain
coin.dance

🔍 🔄 📄 📱



Bitcoin Cash Charts



Zoom 1d 7d **1m** 3m 1y YTD ALL

From Aug 1, 2017 To Sep 1, 2017



Un andamento così schizofrenico, dove ci sono periodi in cui non è possibile vedersi validata una transazione e dove la potenza di calcolo che “mette in sicurezza” la catena se ne va e viene come il bel tempo, non è compatibile con la vita di una moneta realmente utilizzabile al di fuori della mera speculazione. Insomma Bitcoin Cash è nato zoppo. Finché dura però, è la gallina dalle uova d’oro per i traders.

Iscrivi alla newsletter qui

Grazie a Gianluigi Crimi e Emanuele Laface per gli insights.