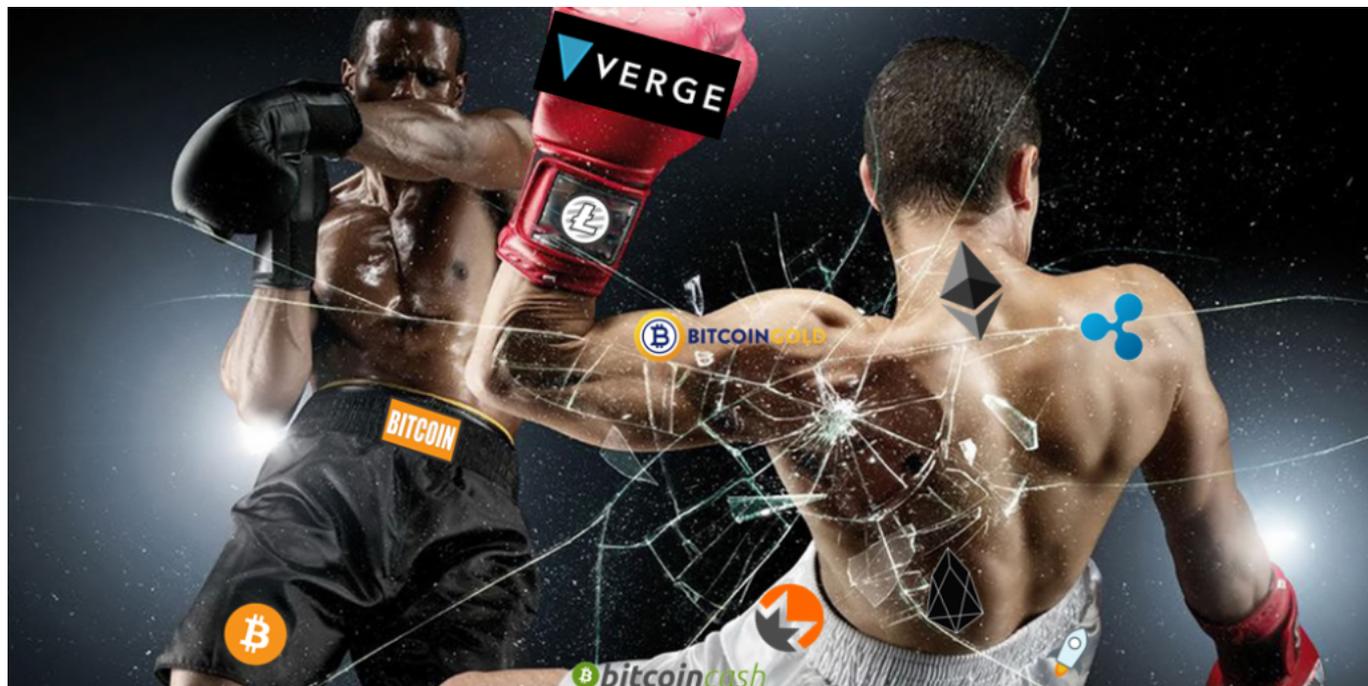


# Ecco perché Bitcoin è superiore alle altre crypto

scritto da Alberto De Luigi | 26 Maggio 2018



Vi sono centinaia se non migliaia di cryptovalute, ognuna osannata dai fan o dai rispettivi sviluppatori come più veloce di Bitcoin, più sicura a possibili attacchi e che garantisce maggiore decentralizzazione. Gli esperti non hanno mai dato credito a queste sciocchezze, ma gli utenti e speculatori comuni sono fastidiosamente inclini a bersi qualunque diceria. Per fortuna, c'è un buon hacker per ogni cattiva bugia: l'attacco che ha subito la blockchain di Verge ad aprile e poi ancora a maggio, qualche giorno fa, è davvero emblematico, perciò lo analizzeremo a fondo in questo articolo.

Verge è una cryptovaluta di cui si può sentir parlare allo sfinimento su forum e chat, come di un protocollo rivoluzionario e con grande potenziale. Quali sono le sue peculiarità? Nessuna, a parte l'aver sviluppatori ciarlatani e un codice che di innovativo introduce soltanto delle vulnerabilità ad attacchi inediti.

La pretesa di Verge è quella di risolvere 3 “problemi” di Bitcoin:

- 1. la lentezza e il costo delle transazioni di Bitcoin,**
- 2. la mancanza di privacy,**
- 3. i rischi legati a una centralizzazione del mining.**

È una novità? Ovviamente no, praticamente qualsiasi altcoin viene sponsorizzata con gli stessi pretesti. E praticamente tutte le altcoin falliscono miseramente nel tentativo di proporre qualcosa di migliore rispetto a Bitcoin. Vediamo brevemente questi tre punti.

## **1. La lentezza e il costo delle transazioni**



Questo è il solito tema della scalabilità. Più transazioni nella rete intasano la blockchain allungando i tempi di transazione e dando vita a un mercato delle fee, come spiegato qui. Attualmente nessuna altcoin ha sviluppato alcun sistema funzionante per migliorare la scalabilità della blockchain. Al contrario, molte altcoin sono meno scalabili di Bitcoin. Come mai allora vi sono crypto che risultano più veloci e meno costose da transare? Ci sono tre risposte:

- 1. sono poco usate, ma se fossero utilizzate quanto Bitcoin, avrebbero gli stessi problemi**
- 2. hanno aumentato la dimensione dei blocchi (come ad esempio Bitcoin Cash)**

### **3. hanno ridotto lo scarto temporale medio fra la creazione di un blocco e il successivo (come Ethereum o Litecoin).**

Le motivazioni 2 e 3 non derivano affatto da innovazioni tecnologiche: dall'oggi al domani anche Bitcoin può aumentare la capacità onchain modificando blocksize o scarto temporale medio fra i blocchi. Per farlo è sufficiente effettuare un upgrade della rete (tecnicamente si chiama consensus fork) come ne sono stati già fatti altri 18 nella storia di Bitcoin. Se non si è già fatto è solo perché la maggioranza dei miners e nodi economici rilevanti ha deciso che non è quello il modo giusto di scalare. La vera innovazione in merito alla scalabilità è il protocollo Lightning Network sviluppato su Bitcoin, utilizzabile grazie all'upgrade a SegWit avvenuto il 24 agosto 2017. Una transazione su LN è istantanea, a fee bassissime e ha peso zero sulla blockchain, poiché è salvata esclusivamente in locale sul wallet di mittente e destinatario.

Per quanto riguarda Verge, al fine di aumentare la velocità delle transazioni e assicurarsi di mantenere fee basse, gli sviluppatori non hanno fatto assolutamente niente di innovativo, semplicemente hanno scelto di impostare una frequenza di creazione dei blocchi di 30 secondi con un coefficiente di difficoltà di mining che si aggiusta ogni 2 ore. Spiegherò a breve con quali conseguenze.

Il secondo punto sollevato dai detrattori di Bitcoin è la mancanza di privacy.

## **2. La mancanza di privacy**



Le transazioni Bitcoin sono pseudonime, ma pubbliche e quindi completamente tracciabili. Basta conoscere nome e cognome dell'ultimo destinatario che ha ricevuto i bitcoin per provare a risalire la catena e scoprire chi c'è dietro a ogni indirizzo da cui quei bitcoin provengono.

Questo tema è vivo sin dall'ottobre 2013 quando Adam Back ha discusso su Bitcointalk la "homomorphic encryption" per permettere di encrittare le quantità di bitcoin inviate in una transazione, che possono così essere conosciute solo dal mittente e destinatario. Successivamente, il Core developer Gregory Maxwell e l'azienda Blockstream hanno iniziato a lavorarci attribuendo all'idea il nome di "Confidential Transactions".

Gli sviluppatori di Bitcoin Core non hanno però ancora proposto un upgrade per implementare le Confidential Transactions, poiché i costi di attuazione sono troppo elevati: una CT pesa molto di più rispetto a una transazione tradizionale. Nonostante l'enorme costo, qualcuno ha voluto mettere in pratica la cosa, così è nato, per esempio, Monero. Oltre a nascondere le quantità inviate (RingCT transactions), in Monero le Ring Signatures fanno sì che gli input di una transazione vengano mischiati con quelli di altri utenti, rendendo difficile collegare mittente con destinatario, mentre i cosiddetti Stealth Address rendono impossibile riconoscere l'indirizzo di destinazione per chi non è il mittente o il destinatario della transazione.



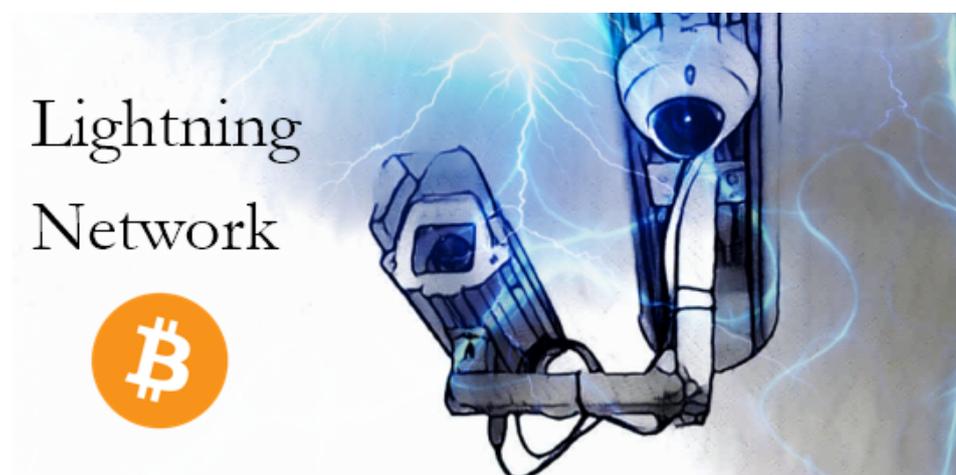
Non è però tutto oro quello che luccica. Una transazione Monero occupa 12 mila bytes, contro i 200 bytes di Bitcoin, quindi sessanta volte tanto. Se Monero vedesse lo stesso numero di transazioni di Bitcoin, la blockchain (che in Bitcoin cresce di circa 60 Gb all'anno) vedrebbe un incremento di 3.600 Gb annui, un numero chiaramente insostenibile. E non è tutto: una ricerca importante dell'aprile 2017 ha individuato tre possibili minacce alla privacy di Monero, evidenziando che almeno in certi casi è possibile risalire all'identità di chi ha effettuato la transazione. Per scongiurare tali casistiche è stato effettuato un fork il 10 gennaio 2017, implementando le RingCT (Ring Confidential Transactions). Il vero problema è che le RingCT arrivano a pesare anche 60.000bytes (60kb). Questo significa che un pagamento anonimo in monero occupa dalle 60 alle 300 volte tanto lo spazio occupato da un pagamento in bitcoin.

Gregory Maxwell di Bitcoin Core ha continuato lo sviluppo delle Confidential Transactions, riuscendo a ridurre le dimensioni di tali transazioni a un peso soltanto 3 volte maggiore rispetto a quelle tradizionali, seppure l'obiettivo delle CT sia "solo" quello di nascondere le quantità inviate e non anche gli indirizzi, come per Monero.



Nonostante il rapporto di dimensione sia di 3 a 1 (e non di 300 a 1!) per Bitcoin è ancora considerato eccessivo (e a

ragion veduta!), per cui non è ancora stato presentato un BIP relativo alle CT su Bitcoin. Bisogna dire in realtà che l'implementazione delle CT non è nemmeno così prioritaria, vista la presenza di altre migliorie in piano che, oltre a conferire una relativamente maggiore privacy, efficientano anche lo spazio sulla blockchain, come le Schnorr signatures.

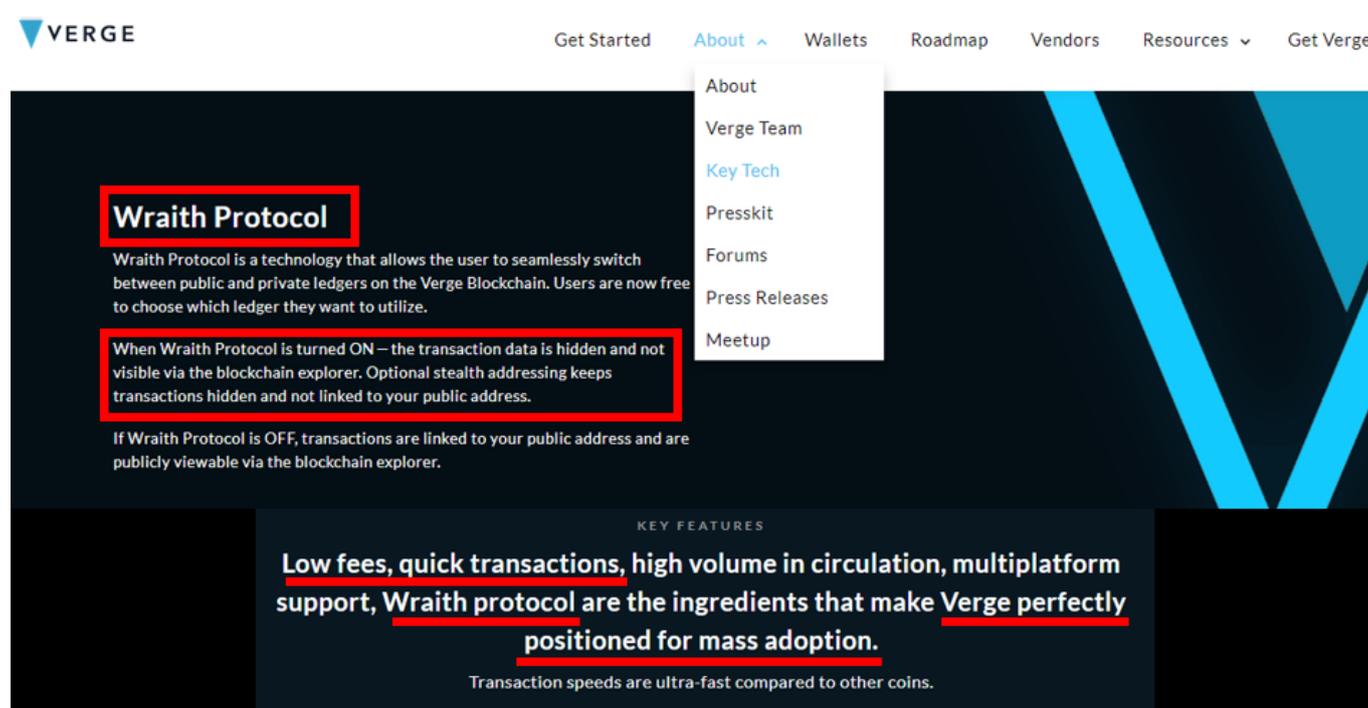


Soprattutto però, c'è Lightning Network che è una rivoluzione da tutti i punti di vista: le transazioni LN sono scritte in locale sul wallet, non su blockchain, dove soltanto l'apertura e chiusura dei canali è tracciata. È difficile risalire ai movimenti di bitcoin con LN persino se si controlla un nodo intermediario fra destinatario e mittente. Infatti i bitcoin possono essere spostati per un'unica transazione attraverso più canali uno di seguito all'altro (routing) e persino per vie parallele (Alice paga a Bob 1 bitcoin, usando come intermediario Charlie per spostare 0,5btc e Dave per spostare gli altri 0,5btc). Perciò risulta estremamente difficile ricostruire i trasferimenti anche potendo monitorare attentamente alcuni canali che si controllano. In questo modo si ottiene una privacy incredibilmente maggiore a costo zero in termini di fees e di peso della blockchain.

Tornando a Verge, qual è l'innovazione che porta? Nessuna. Ha solo rispolverato due concetti già conosciuti e studiati allo sfinimento negli anni dagli sviluppatori Bitcoin. Uno è il "Wraith protocol" ovvero gli stealth payments, di cui possiamo

vedere un BIP scritto da Peter Todd per Bitcoin già nel 2015. Tale BIP era stato abbandonato perché i benefici sono pochi (solo il ricevente ha maggiore privacy, non il mittente) e i costi esagerati: allunga estremamente i tempi che un wallet impiega nel riconoscere il proprio balance (da alcuni test un light wallet impiegava fino a 2 ore per visualizzare soltanto quanto ricevuto nelle ultime 24 ore).

Guardacaso, Wraith pur essendo sfacciatamente sbandierato in primo piano sul sito di Verge, non è nemmeno stato ancora implementato.



The screenshot shows the Verge website's navigation menu and a section titled "Wraith Protocol". The navigation menu includes "Get Started", "About", "Wallets", "Roadmap", "Vendors", "Resources", and "Get Verge". The "About" menu is open, listing "About", "Verge Team", "Key Tech", "Presskit", "Forums", "Press Releases", and "Meetup". The "Wraith Protocol" section contains the following text:

**Wraith Protocol**

Wraith Protocol is a technology that allows the user to seamlessly switch between public and private ledgers on the Verge Blockchain. Users are now free to choose which ledger they want to utilize.

When Wraith Protocol is turned ON – the transaction data is hidden and not visible via the blockchain explorer. Optional stealth addressing keeps transactions hidden and not linked to your public address.

If Wraith Protocol is OFF, transactions are linked to your public address and are publicly viewable via the blockchain explorer.

**KEY FEATURES**

**Low fees, quick transactions, high volume in circulation, multiplatform support, Wraith protocol are the ingredients that make Verge perfectly positioned for mass adoption.**

Transaction speeds are ultra-fast compared to other coins.

La seconda caratteristica pro-privacy che Verge “vanta” è il fatto di girare su rete Tor. Standing ovation? Macché. Per anni si è parlato di far girare Bitcoin su Tor, Verge non ha inventato niente. Perché quindi non si fa già su Bitcoin? Anzitutto perché non è molto utile: la storia insegna che tutti gli arresti effettuati a discapito di chi usava bitcoin (vedi) sono stati fatti tracciando le transazioni tramite blockchain, non c'è un singolo caso di persona scoperta perché aveva rivelato il proprio IP nell'effettuare una transazione. In secondo luogo, far girare Bitcoin su Tor oltre che poco utile non è nemmeno del tutto sicuro. Infatti con Tor il

Network Bitcoin si sottoporrebbe a nuovi vettori di attacco che sfruttano il sistema di anti-DoS implementato in Bitcoin su base reputazionale: se dei nodi malevoli inondassero il network di transazioni volutamente "irregolari" (ad esempio una coinbase transaction di 60 bytes in size), i nodi onesti verrebbero bloccati dall'anti-spam e rimarrebbero solo nodi malevoli (vedi il relativo paper di ricerca per approfondimenti).

In poche parole, in merito a privacy e soprattutto scalabilità la vera innovazione è su Bitcoin, le altcoin implementano gli scarti di lavorazione di Bitcoin, vendendoli ai creduloni come incredibili rivoluzioni ingegneristiche. Ma c'è un'ultima critica comunemente mossa a Bitcoin: la centralizzazione del mining.

### 3. I rischi legati alla centralizzazione del mining



Si parla allo sfinimento di quanto il mining di bitcoin sia centralizzato e quindi alcune entità (o mining pool) avrebbero il potere di governare lo sviluppo del protocollo, di censurare transazioni o fare double spending: insomma,

sfruttare in qualche modo un 50+1 attack. Molte altcoin quindi hanno cavalcato queste voci per lanciarsi sul mercato spacciandosi per protocolli innovativi a prova di centralizzazione. Con risultati comici.

Anzitutto, bisogna premettere che nessun miner e nemmeno nessuna pool (cioè un aggregato di molti miners) ha il 51% di hashrate del network Bitcoin, seppur sia vero che alcune aziende hanno un'influenza molto grande. In particolare, Bitmain produce ASICS miner per mezzo mondo e se sommiamo l'hashrate delle pool che Bitmain controlla (AntPool, BTC.com) o in cui ha partecipazioni (ViaBTC) questo sfiora quasi il 50%. Ciò non significa però controllare il 50% della potenza di calcolo mondiale: ciascuna pool è fatta da centinaia o migliaia di utenti ed è assolutamente improbabile che questi sostengano un attacco alla rete Bitcoin guidato dall'azienda che amministra la pool. Soprattutto però, se la teoria dei giochi pensata da Satoshi Nakamoto funziona, anche se un singolo miner superasse il 50% di hashrate, quest'ultimo non avrebbe alcuna convenienza ad attaccare la rete Bitcoin, che è la fonte del suo guadagno, dopo aver investito un capitale in hardware specializzato che non può far altro che minare Bitcoin. Il risultato di un attacco (costosissimo da attuare) sarebbe quello di danneggiare la reputazione della moneta, far crollare il prezzo, quindi gli stessi guadagni e la reputazione del miner che ha effettuato l'attacco.

Ma è inutile parlare di teoria quando abbiamo di fronte la pratica: lo stesso Jihan Wu, fondatore e CEO di Bitmain, era fra i primi promotori del fork con blocksize increase SegWit2x (è anche ben nota la passione di Jihan per Bitcoin Cash) eppure, nonostante il peso delle sue aziende e l'hashrate che queste controllano, sappiamo bene come la "battaglia" per il blocksize increase sia andata a finire nel novembre 2017. Chi non se lo ricorda può ripassare l'articolo di novembre, che aiuta a comprendere quali siano le dinamiche politiche di un upgrade del protocollo Bitcoin:



Insomma, il miner più potente della rete, per giunta in accordo con quasi tutti i principali altri miner e parecchie aziende, non è riuscito nemmeno a far passare un upgrade del tutto legittimo come un raddoppio del blocksize, figuriamoci eseguire un attacco vero e proprio. Sembra però che gli sviluppatori di altcoin siano ossessionati con questa storia della centralizzazione e facciano di tutto per risolvere “il problema” anche dove il problema non c'è. Le soluzioni trovate sono ben più catastrofiche del problema.

Prima si sono inventati che l'algoritmo SHA256 non è adatto per il mining, poiché solo delle macchine specializzate minano in modo efficiente SHA256 (gli ASICS). Questo comporterebbe che il mining non è accessibile a chiunque voglia cimentarsi con hardware generico, come le schede video per PC. Paradossalmente, questo è il punto di forza dello SHA256 e non la sua debolezza. Infatti se l'hardware è generico si può affittare (o comprare per poi rivendere) con l'unico scopo di effettuare un attacco alla rete. Se invece è hardware specializzato, l'unico modo in cui è possibile fare un attacco è spendere miliardi in costose stufette elettriche inutili a fare qualsiasi cosa se non minare Bitcoin. Quando la rete reagisce all'attacco 50+1 con un hard fork per cambiare l'algoritmo di Proof of Work, le costosissime stufette andranno buttate perché ormai inutili. In poche parole, l'attacco sarebbe economicamente proibitivo e avrebbe risultati incerti (dopo il cambio POW Bitcoin potrebbe benissimo sopravvivere e prosperare). Nonostante la teoria, sono nate cryptovalute senza senso come Bitcoin Gold, minabile con GPU. Ironia della sorte, Bitcoin Gold ha recentemente subito un attacco 50+1 in cui l'attaccante depositava e

ritirava sugli exchange coin “contraffatti” con double spending, vendendo i BTG e prelevando dall’exchange cryptovalute più sicure. L’attacco è valso ben 18 milioni di dollari.



Da notare che anche a Bitcoin Cash potrebbe spettare la stessa sorte di Bitcoin Gold, nonostante sia uno SHA256: questo perché seppur SHA256 richieda macchine specializzate per il mining, c’è un ammontare di hashpower SHA256 incredibilmente maggiore su Bitcoin rispetto alla potenza di calcolo di BCH, perciò basterebbe che un grosso miner BTC spostasse momentaneamente l’hashrate su BCH con intenzioni malevole per uccidere quella blockchain (o fare double spending) decretando la fine della cryptovaluta. Dopodiché, l’attaccante sposterà l’hashrate nuovamente su BTC, senza così incorrere in quel costo economico che nella teoria dovrebbe disincentivare l’attacco o renderlo proibitivo.

Oltre ai fan dell’hardware generico per il mining, ci sono anche quelli che osannano la Proof of Stake, alternativa alla Proof of Work di Bitcoin. Il tema merita un discorso a parte perché è complesso e non lo tratterò esaurientemente qui, ma per chiunque abbia studiato è evidente che un sistema esclusivamente POS sia infinitamente più centralizzato del POW. Vitalik Buterin stesso lo afferma:

*All “pure” proof-of-stake systems are ultimately permanent nobilities where the members of the genesis block allocation always have the ultimate say. No matter what happens ten million blocks down the road, the genesis block members can always come together and launch an alternate fork with an alternate transaction history and have that fork take over”.*

Per riassumere il concetto: chi ha più coin continua ad

accumularne sempre di più mediante mining tramite POS, quindi diventa sempre più potente e, più passa il tempo, più può influenzare a suo piacimento lo sviluppo del protocollo o tentare un attacco alla rete.



Nonostante questi concetti basilari siano ben noti persino agli stessi sostenitori di sistemi misti POW+POS, fioccano su forum e chat post di utenti ignoranti che celebrano i sistemi POS a discapito del “centralizzato” SHA256 di Bitcoin. Non ci si può pronunciare sul tema senza aver letto quantomeno lo storico paper di Bitfury su POS vs POW.

Infine, c'è il già citato caso Verge, che raggiunge livelli di comicità imbarazzanti. E la bella notizia è che Verge non è un'eccezione, ma segue il 99% delle cryptovalute in circolazione, che sono null'altro che vaporware, scam, o esperimenti tecnologici e sociali di scarso successo.

## **L'attacco hacker a Verge**

L'attacco hacker su Verge non ha sfruttato un bug di quest'ultimo, ma proprio alcune delle caratteristiche per cui Verge declamava di essere superiore a Bitcoin.

Verge per “decentralizzare” il mining sfrutta 5 diversi tipi

di algoritmo: Scrypt, x17, groestl, blake2s e lyra2rev2. Ognuno dei 5 algoritmi ha il proprio aggiustamento della difficoltà, perciò se ci sono pochi blocchi creati mediante uno solo di quegli algoritmi, la difficoltà diminuisce solo per quest'ultimo. Gli aggiustamenti avvengono circa ogni 2 ore.

Gli sviluppatori di Verge hanno fatto 3 errori che sono costati cari:

- **5 algoritmi diversi di mining (su Bitcoin c'è 1 solo algoritmo SHA256)**
- **Blocchi prodotti con elevata frequenza, ovvero ogni 30 secondi (su Bitcoin sono ogni 10 minuti)**
- **La difficoltà di mining si aggiusta ogni 2 ore (su Bitcoin ogni 2 settimane)**

Vediamo questi punti separatamente, comprendendo il motivo per cui sono un terribile errore, specialmente se combinati insieme.



**1** – Dividere l'hashpower su 5 algoritmi diversi significa che per prevalere su un singolo algoritmo è sufficiente l'11% di hashpower totale della rete. Questo perché fatto 100 l'hashpower totale, ipotizzando che tutti e 5 gli algoritmi abbiano lo stesso peso, l'hashpower relativo a ogni algoritmo è soltanto 20. Quindi con una potenza di calcolo di 10+1 (su 100) un singolo miner può ottenere una dominanza del 51% su quell'algoritmo. A breve capiremo le conseguenze.

**2** – Il fatto che i blocchi siano creati ogni 30 secondi

significa che, per creare un singolo blocco, l'hashpower richiesto è un ventesimo rispetto a quello necessario rispetto a una blockchain con blocchi ogni 10 minuti. E questo blocco potrebbe essere "malevolo" e fare double spending dei blocchi precedenti. Perciò fatto 100 l'hashpower totale prodotto per Bitcoin nell'arco di 10 minuti, la potenza di calcolo sviluppata in 30 secondi è soltanto di 5. È quindi sufficiente avere temporaneamente una maggioranza di 3 punti su 5 per provare un attacco 50+1 nel breve periodo, magari noleggiando o comprando hashpower da terzi.

L'investimento economico dei miners che mettono in sicurezza la rete di Verge è incredibilmente inferiore a quello di Bitcoin (cosa che del resto vale per tutte le altcoin), ciononostante, ottenere il 50% di hashpower totale del network sarebbe estremamente costoso. Tuttavia, ottenere solo l'11% di hashpower per prevalere su uno dei 5 algoritmi non è così proibitivo, specialmente se soltanto per un periodo di tempo molto breve. Dato che la creazione di blocchi su Verge è estremamente frequente, un attacco di breve periodo non risulta più così impossibile.

I primi due errori degli sviluppatori di Verge sembrano un'accoppiata allarmante, ma soltanto comprendendo il terzo errore si scopre che l'insieme è una combo micidiale.



**3** – In ogni blockchain i blocchi riportano una data e ora. Non esiste un sistema informatico globale di validazione del tempo che sia decentralizzato, perciò i blocchi vengono accettati dagli altri clients e miners anche se riportano una data con uno scarto temporale abbastanza ampio: per Bitcoin un blocco

non deve riportare un orario uguale o precedente all'orario mediano degli ultimi 11 blocchi. Anche su Verge c'è questo ampio scarto, per cui possono essere accettati blocchi con un timestamp risalente anche a due ore nel passato. A differenza di Bitcoin però, la difficoltà di mining per Verge si aggiusta ogni 2 ore, anziché 2 settimane. Quindi se nelle ultime 2 ore la blockchain di Verge non presenta un sufficiente numero di blocchi "recenti" per garantire una media di un blocco ogni 30 secondi (in base al timestamp del blocco, non all'orario "reale" in cui il blocco è minato!), si presuppone che l'hashpower non sia sufficiente e la difficoltà debba quindi calare. La difficoltà però cala solo sull'algoritmo di mining che non ha prodotto blocchi "recenti". L'hacker ha sfruttato proprio questa caratteristica per attaccare la rete in questo modo:

- **Ha acquistato o noleggiato almeno l'11% di potenza di calcolo del network Verge, ma esclusivamente in uno dei 5 algoritmi, Scrypt (lo stesso usato su Litecoin) così da assicurarsi il 50+1 su quell'algoritmo. [Potremmo anche ipotizzare che l'attaccante abbia noleggiato dai miners di Litecoin della potenza di calcolo]**
- **Ha prodotto blocchi con timestamp antecedente al momento reale di creazione (1 ora circa), ma sufficientemente recenti da essere comunque accettati dalle regole del protocollo e quindi validati dal resto della rete**
- **Le regole di aggiustamento di difficoltà di Verge, in conseguenza dei pochi blocchi creati nell'ultimo periodo (proprio poiché il timestamp di tutti quelli creati dall'hacker è un'ora nel passato) ha effettuato un aggiornamento della difficoltà riducendo drasticamente la potenza di calcolo necessaria a minare Verge**
- **Poiché la difficoltà di mining è calcolata indipendentemente sui 5 algoritmi, è stata ridotta soltanto su Scrypt, ovvero l'algoritmo che non produceva più blocchi recenti, e non sugli altri algoritmi.**
- **L'hacker quindi, avendo la maggioranza di hashpower su**

Script, ha potuto inondare la rete di moltissimi blocchi creati con estrema facilità, peraltro tutti con timestamp nel passato così da assicurarsi che la difficoltà scendesse ulteriormente (è scesa addirittura del 99,999999%)

- In questo modo l'attaccante ha dominato completamente la rete di Verge, creando milioni di Verge coin per se e potendo anche fare tutti i double spending desiderati ai danni degli exchange, su cui vendere Verge per convertirli in crypto più affidabili.



Da notare che l'abbassamento della difficoltà mediante alteramento dei timestamp del blocco è chiamato time spoofing e, tanto per cambiare, è un tema dibattuto nella community Bitcoin già nel 2011 (si veda questo post di Alex Boverman seguito da un thread su BitcoinTalk). Su Bitcoin l'aggiustamento della difficoltà ogni 2016 blocchi (due settimane circa) rende impossibile un risultato analogo a quello avvenuto su Verge, poiché le variazioni di timestamp nell'arco di poche ore sono insignificanti. Dietro le scelte fatte su Bitcoin c'è una ragione, ma i developers di Verge evidentemente hanno studiato poco, prestando troppa attenzione al marketing e per niente alla tecnologia. Dovrebbero leggere con più attenzione quanto ci ha lasciato in eredità Satoshi Nakamoto.

Il miner hacker ha dominato il network di Verge in tre diverse occasioni per intervalli di alcune ore fra il 4 e il 6 aprile, impedendo a qualsiasi utente di transare con Verge. In quell'intervallo di tempo, ha creato Verge a un tasso di 1560 coin al secondo (circa 80 dollari al secondo) minando per un valore di 1,8 milioni di dollari. Qual è stata la risposta dei dev di Verge? Un hard fork, che costringe tutti gli utenti ed exchange a fare un upgrade del client wallet. Nonostante questa misura, il 22 maggio, l'hacker ha eseguito lo stesso attacco, questa volta controllando la maggioranza di hashpower su due algoritmi anziché uno solo, mettendo ancora più in ridicolo gli sviluppatori di Verge. Questo secondo attacco è valso 1,7 milioni di dollari.

Ma quelli di Verge, campioni di marketing (e non sono un'eccezione fra i promotori delle varie altcoin) in risposta agli attacchi hanno tirato fuori l'asso nella manica, la campagna mediatica:

- **“La Verge Debit Card!”** (UQUID.com)
- **“Pornhub accetta Verge!”** (Wired, 17 aprile) – **il prezzo di Verge si impenna**
- **Articoli su Verge che punta alle grandi partnership, ad es. con Spotify dopo l'accordo siglato con MindGeek...** (ethereumworldnews.com)



Come reagiva nel frattempo il mercato? Ecco qui che si palesa l'ignoranza degli speculatori. Dopo il primo hack del 4-6 aprile, il prezzo sale e addirittura ha uno spike il 17 aprile, in corrispondenza dell'articolo su Wired relativo alla collaborazione con pornhub (se anche fosse vero, chi è che

compra contenuti su pornhub?).



Ma trader e speculatori non sono gli unici a magnificare la loro distopica ignoranza. Le istituzioni statali sono imbattibili. il Ministero dell'industria cinese il 16 maggio ha pubblicato una meravigliosa tabellina dove Verge è presentato con un punteggio in tecnologia di ben SESSANTASEI PUNTO UNO (contro 39,4 di Bitcoin). A noi bitcoiners è andata male questa volta, ma sono certo che recupereremo coi tuffi olimpionici dalle piattaforme 7,5 e 10 metri. I giudici sono gli stessi.



cnLedger [Not giving away ETH]

@cnLedger

Segui

## 4/ Detailed scores of the first crypto ratings by CCID Research, China's Ministry of Industry & Information Technology

Traduci il Tweet

Public Blockchain Ratings by CCID, China's Ministry of Industry & Information Technology

Project	Sub-Index			Total Index	Ranking
	Technology	Application	Innovation		
Ethereum	80.3	23.7	25.4	129.4	1
Steem	82.6	9.4	23.9	115.9	2
Lisk	64.4	20.9	19.5	104.8	3
NEO	69.2	26.6	7.3	103	4
Komodo	60.3	12.8	28.5	101.5	5
Stellar	70.8	18.1	11.8	100.7	6
Cardano	60.3	13.7	24.3	98.2	7
IOTA	65.9	14.9	17.4	98.2	7
Monero	65.7	11.1	15.8	92.6	9
Stratis	60.2	19.3	12.2	91.7	10
Qtum	58.3	22.8	10	91	11
BitShares	71.6	12.3	7	90.8	12
Bitcoin	39.4	13.1	35.6	88.1	13
Verge	66.1	10.9	11.1	88.1	13
Waves	58.2	12.3	16	86.5	15

16-28: ETC, XRP, DASH, SC, BCN, LTC, ARK, ZEC, NANO, BCH, DCR, HSR, XEM  
@cnLedger (twitter.com/cnLedger)

20:07 - 16 mag 2018

In conclusione, le altcoin non hanno senso di esistere? In realtà un'utilità ce l'hanno: le innovazioni sviluppate per Bitcoin vengono messe alla prova a lungo nell'ambiente di testnet, tuttavia un errore lì non comporta la perdita di denaro per nessuno. Il vero test è l'ambiente "di produzione", dove gli hacker sono in agguato. Poiché non tutte le conseguenze di un upgrade sono sempre prevedibili, specialmente quando una modifica del codice può innescare determinate dinamiche di tipo sociale, l'unico vero test è la realtà. Allora come possiamo essere certi che un upgrade sia sicuro solo se abbiamo fatto delle verifiche tecniche in testnet? Ecco dove sta l'utilità delle altcoin: queste rappresentano un ambiente sperimentale, come la testnet Bitcoin, ma dove ci sono in gioco soldi veri e dinamiche

sociali. Ricordiamo che SegWit, inventato per Bitcoin da sviluppatori Bitcoin, è stato introdotto prima su Litecoin e, solo una volta che ne è stata dimostrata a chiunque la solidità, è stato finalmente approvato dai miners anche su Bitcoin. Dagli errori delle altcoin impariamo a capire dove non dobbiamo spingerci, da eventuali successi delle altcoin potremo copiare il codice da importare su Bitcoin.

In fondo, la stragrande maggioranza delle altcoin e i loro sviluppatori servono esclusivamente un unico fine: Bitcoin (anche se in modo inconsapevole). Un giorno forse anche i traders più ignoranti se ne accorgeranno, e per quel giorno sarà meglio che avremo già venduto da un pezzo tutte le cryptoschifezze che abbiamo in portafoglio.

Tieniti aggiornato sulle news quotidiane più importanti seguendo [la pagina facebook: https://www.facebook.com/albertodeluigi.news](https://www.facebook.com/albertodeluigi.news)

Iscriviti alla newsletter del blog, riceverai una mail ad ogni nuovo articolo pubblicato