LA TECNOLOGIA BLOCKCHAIN E I BITCOIN

Alessio Salvetti

Bcademy

17.12.2018 - ore 15.00

Il Fondo Sociale Europeo in Friuli Venezia Giulia
Programma Operativo Regionale 2014-2020

Unione europea
Fondo sociale europeo

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

UN INVESTIMENTO PER IL TUO FUTURO

in rete fvg
seminari per l'innovazione in rete

ALESSIO SALVETTI

Co-founder di Bcademy e board member (VP), Alessio è partner e board member di Impact Hub Trentino, uno dei 102 nodi del network mondiale. Dopo un'esperienza come docente di filosofia, abbandona l'insegnamento per coordinare un team di ricerca sui temi della connessione tra neuroscienze ed economia, prima di dedicarsi alla vera e propria creazione d'impresa. Business developer e consulente per numerose startup, bitcoiner per passione ed esperto di modeling e lean startup, è co-founder di Inbitcoin e responsabile per l'erogazione dei prodotti di Bcademy.

Bcademy

Il Fondo Sociale Europeo in Friuli Venezia Giulia
Programma Operativo Regionale 2014-2020

Unione europea
Fondo sociale europeo

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

UN INVESTIMENTO PER IL TUO FUTURO

in rete fvg
seminari per l'innovazione in rete

WHAT IS BLOCKCHAIN?

Centre for International
Governance Innovation

What is Blockchain?

Bcademy

Il Fondo Sociale Europeo
in Friuli Venezia Giulia
Programma Operativo Regionale 2014-2020

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

UN INVESTIMENTO PER IL TUO FUTURO

in rete fvg
seminari per l'innovazione in rete

WHAT IS BLOCKCHAIN?

By The Centre for International Governance Innovation

Questo video realizzato dal Centre for International Governance Innovation (una think tank indipendente focalizzata sulla ricerca inerente la governance intesa nella sua globalità), è stato mostrato perché è uno specchio molto fedele della prospettiva istituzionale relativa alla tecnologia blockchain. Lo utilizzeremo come binario per approfondire questa tecnologia e la sua relazione con Bitcoin. Partendo da quest'ultimo punto, che è anche il punto iniziale del video…

Molte persone pensano alla blockchain come alla tecnologia che alimenta Bitcoin. Se questo era certamente il suo scopo originale, la blockchain permette molte altre possibilità.

BITCOIN

A Peer-to-Peer Electronic Cash System

Il 31 ottobre 2008 apparve sulla Cryptography Mailing List il seguente messaggio:
“I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.
The paper is available at: http://www.bitcoin.org/bitcoin.pdf
The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.”

Bcademy
Il Fondo Sociale Europeo in Friuli Venezia Giulia
Programma Operativo Regionale 2014-2020
REGIONE AUTONOMA FRIULI VENEZIA GIULIA
UN INVESTIMENTO PER IL TUO FUTURO
in rete fvg
seminari per l'innovazione in rete

BITCOIN

A Peer-to-Peer Electronic Cash System

L'identità del proponente, considerato il padre del Bitcoin, non è mai stata rivelata, e sono in molti a sostenere che si tratti di un multiple name, ovvero di un nome che rappresenta un collettivo.
Satoshi Nakamoto, nel breve testo di accompagnamento al link di download del paper, elenca le proprietà principali del suo sistema di pagamento interamente tra pari, senza terze parti fiduciarie:

- prevenzione della doppia-spesa grazie ad una rete tra pari;
- assenza di fiducia nella zecca o in terze parti;
- i partecipanti possono rimanere anonimi;
- le nuove monete sono create tramite una prova di lavoro in stile Hashcash;
- la prova di lavoro per la generazione di nuove monete rinforza la rete per prevenire la doppia-spesa.

BITCOIN

A Peer-to-Peer Electronic Cash System

I medesimi concetti sono ribaditi nella parte del paper ancora precedente all'introduzione:

- **il problema del trasferimento di denaro elettronico è l'intermediazione** (con particolare riferimento alle istituzioni finanziarie);
- **la soluzione è una rete tra pari, capace di risolvere il problema della doppia spesa, che stampa un marcatore temporale sulle transazioni facendo hashing sulle stesse e incatenandole in una catena di proof-of-work basata sugli hash**, formando una registrazione che non può essere modificata senza rifare la proof-of-work.

BITCOIN

A Peer-to-Peer Electronic Cash System

Tali aspetti ci permettono di comprendere che cos'è **Bitcoin: un protocollo che genera una rete tra pari che permette ad ogni nodo che la compone di transare liberamente e pseudonimamente valore ad altri nodi della rete**. Tale valore, o più correttamente, rappresentazione digitale di valore, viene generato dal protocollo in modo da garantire scarsità, sicurezza nell'ordine delle transazioni, sicurezza del sistema stesso.

Nel white paper non compare il termine blockchain, ma semplicemente la perifrasi "chain of blocks". La blockchain è una delle tecnologie, insieme alle *firme digitali* e alla *prova di lavoro*, che permette la creazione e il funzionamento di quello che è **il primo asset digitale, trasferibile, non duplicabile, decentralizzato.**

WHAT IS BLOCKCHAIN? |2

By The Centre for International Governance Innovation

Nonostante il suono della parola, non c'è solo una blockchain. Blockchain è un'abbreviazione per un'intera suite di tecnologie di registro distribuito (DLT) che possono essere programmate per registrare e tracciare qualsiasi cosa di valore: dalla transazione finanziaria alla documentazione medica o persino ai titoli di terra. Potresti pensare: abbiamo già processi in atto per tracciare dati. Cosa c'è di speciale nella blockchain?

Analizziamo il motivo per cui la tecnologia blockchain sta rivoluzionando il modo in cui sono interconnessi l'uno con l'altro.

WHAT IS BLOCKCHAIN? |2

Broad and narrow definition

Se è vero che non c'è una sola blockchain, è altrettanto vero che quando si parla delLa blockchain si fa riferimento alla blockchain per antonomasia, quella di Bitcoin. Perché è possibile avere molte blockchain? Perché in primo luogo il protocollo Bitcoin è open source, e questo ha reso possibile la creazione di innumerevoli cloni.

WHAT IS BLOCKCHAIN? |2

Broad and narrow definition

Il fenomeno a cui si assiste, al di là di attenersi ad una definizione stretta di blockchain *(La blockchain)* piuttosto che ad una più ampia *(una differenza specifica all'interno del genere delle DLT)* è generalmente quello di una "deterritorializzazione" della blockchain: da una tecnologia idonea a risolvere un particolare problema di trasmissione di valore digitale in un ambiente decentralizzato, ad una tecnologia candidata a risolvere problemi generali di affidabilità di dati.

WHAT IS BLOCKCHAIN? |2

Perché la blockchain sta rivoluzionando… Motivo num. 1

Il modo in cui tiene traccia e memorizza i dati.
La blockchain immagazzina informazioni in lotti, chiamati blocchi che sono collegati in modo cronologico per formare una linea continua: metaforicamente una catena di blocchi.
Se si apportano modifiche alle informazioni registrate in un particolare blocco, non lo riscrive. Le modifiche sono memorizzate in un nuovo blocco che mostra che x è cambiato in y in un dato "dato" e in un dato "momento".
Suona familiare? Questo perché blockchain si basa sul metodo secolare del libro mastro finanziario generale. È un modo non descrittivo per tracciare i cambiamenti dei dati nel tempo.

WHAT IS BLOCKCHAIN? |2

Perché la blockchain sta rivoluzionando… Motivo num. 1

A differenza del vecchio metodo di libro mastro - originariamente un libro, quindi un file di database memorizzato su un singolo sistema - blockchain voleva essere decentralizzato e distribuito su un grande reticolo di computer. Questo decentramento delle informazioni riduce la capacità di manipolazione dei dati e porta al secondo fattore che rende unica la blockchain.

Questo utilizzo della blockchain, che potremo definire notarile o BAAN (blockchain as a notary) ci riporta già alla definizione ampia di blockchain, dove la blockchain non attesta un passaggio di valore quanto piuttosto la prova del possesso di un documento in un dato momento.

WHAT IS BLOCKCHAIN? |2

Perché la blockchain sta rivoluzionando… Motivo num. 2

Prima che un blocco possa essere aggiunto alla catena, alcune cose devono accadere.

Innanzitutto, un puzzle crittografico deve essere risolto, creando così il blocco. Il computer che risolve il puzzle condivide la soluzione con tutti gli altri computer sulla rete, questo è chiamato proof-of-work. La rete verificherà quindi questa prova di lavoro e, se corretta, il blocco verrà aggiunto alla catena. La combinazione di questi complessi puzzle matematici e la verifica da parte di molti computer assicura che sia possibile fidarsi di ogni singolo blocco della catena.

Poiché la rete crea fiducia per noi, ora abbiamo l'opportunità di interagire direttamente con i nostri dati in tempo reale.

WHAT IS BLOCKCHAIN? |2

Perché la blockchain sta rivoluzionando… Motivo num. 2

La tecnologia blockchain tiene conto dei problemi di sicurezza e fiducia in diversi modi. Innanzitutto, i nuovi blocchi vengono sempre archiviati in modo lineare e cronologico. Cioè, vengono sempre aggiunti alla "fine" della blockchain. Se si sà un'occhiata alla blockchain di Bitcoin, si vedrà che ogni blocco ha una posizione sulla catena, chiamata "altezza".

Dopo che un blocco è stato aggiunto alla fine della blockchain, è molto difficile tornare indietro e modificare il contenuto del blocco. Questo perché ogni blocco contiene il proprio hash, insieme all'hash del blocco prima di esso.

WHAT IS BLOCKCHAIN? |2

Perché la blockchain sta rivoluzionando… Motivo num. 2

I codici hash vengono creati da una funzione matematica che trasforma le informazioni digitali in una stringa di numeri e lettere. Se tale informazione viene modificata in qualsiasi modo, anche il codice hash cambia.

Per cambiare un singolo blocco, quindi, un hacker dovrebbe cambiare ogni singolo blocco dopo di esso sulla blockchain. Ricalcolare tutti quegli hash richiederebbe una quantità enorme e improbabile di potenza di calcolo. In altre parole, una volta aggiunto un blocco alla blockchain diventa molto difficile da modificare e impossibile da eliminare.

WHAT IS BLOCKCHAIN? |2

Perché la blockchain sta rivoluzionando… Motivo num. 2

Per affrontare il problema della fiducia, le reti blockchain hanno implementato test per i computer che vogliono unirsi e aggiungere blocchi alla catena. I test, chiamati "modelli di consenso", richiedono agli utenti di "provare" se stessi prima di poter partecipare a una rete blockchain. Uno degli esempi più comuni utilizzati da Bitcoin è chiamato "prova di lavoro".

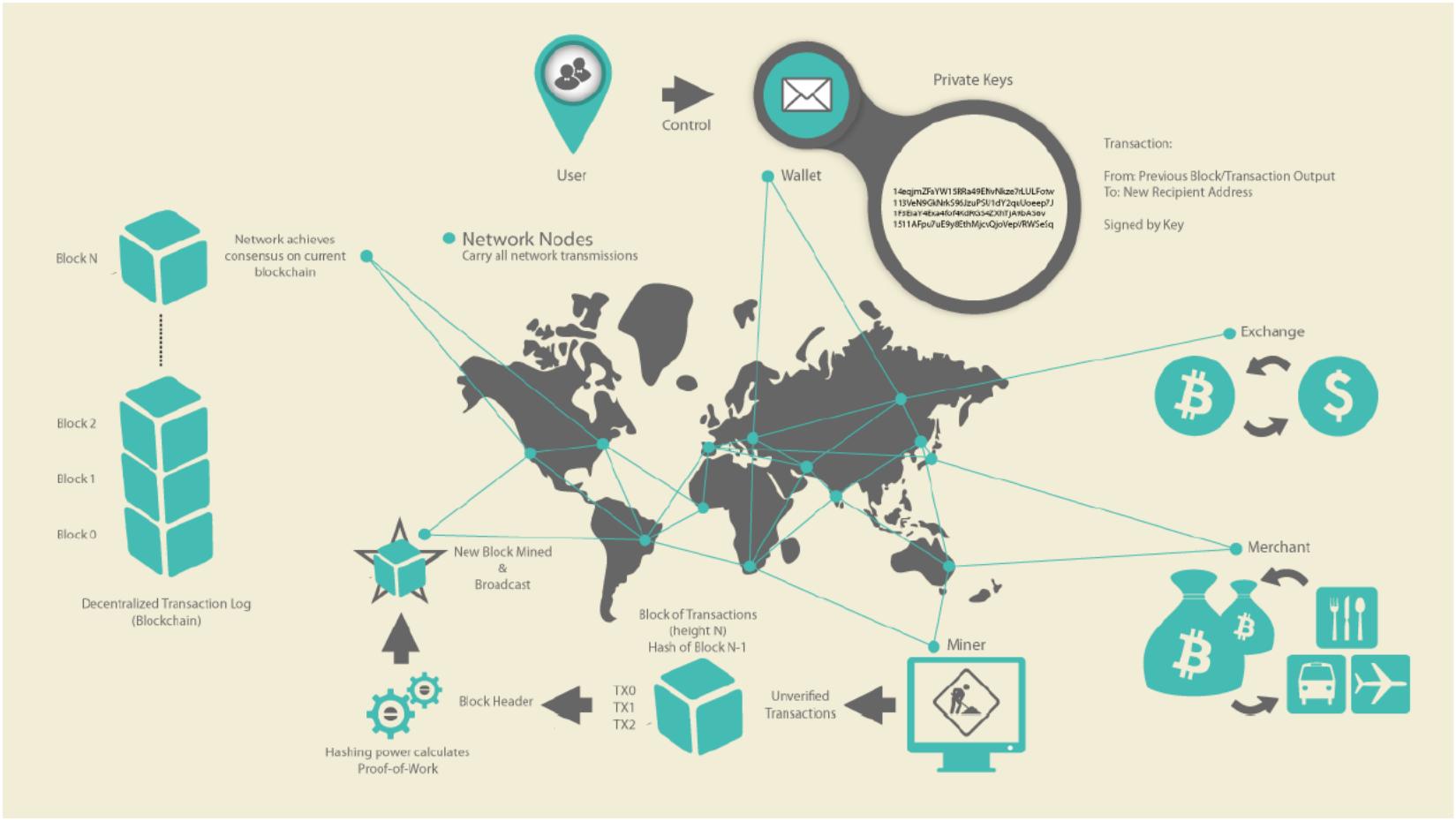
Nella prova del sistema di lavoro, i computer devono "dimostrare" di aver fatto "lavoro" risolvendo un complesso problema matematico computazionale. Se un computer risolve uno di questi problemi, diventa idoneo ad aggiungere un blocco alla blockchain. Ma il processo di aggiungere blocchi alla blockchain, ciò che il mondo della criptovaluta chiama "mining", non è facile.

WHAT IS BLOCKCHAIN? |2

Perché la blockchain sta rivoluzionando… Motivo num. 2

Per risolvere complessi problemi di matematica a quelle quote, i computer devono eseguire programmi che costano loro quantità significative di energia (leggi: denaro).

La prova del lavoro non rende gli attacchi degli hacker impossibili, ma li rende in qualche modo inutili. Se un hacker volesse coordinare un attacco alla blockchain, avrebbe bisogno di risolvere complessi problemi matematici computazionali a 1 su 7 trilioni di probabilità, proprio come tutti gli altri. Il costo di organizzare un simile attacco sarebbe quasi certamente superiore ai benefici.



Bcademy

Il Fondo Sociale Europeo in Friuli Venezia Giulia
Programma Operativo Regionale 2014-2020

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

UN INVESTIMENTO PER IL TUO FUTURO

in rete fvg
seminari per l'innovazione in rete

WHAT IS BLOCKCHAIN? |2

Perché la blockchain sta rivoluzionando… Motivo num. 3

Niente più intermediari.

Attualmente, quando facciamo affari con l'altro, non mostriamo all'altra persona i nostri documenti finanziari o aziendali. Invece, ci affidiamo a intermediari di fiducia, come una banca o un avvocato, per visualizzare i nostri dati e mantenere tali informazioni riservate. Questi intermediari creano fiducia tra le parti e sono in grado di verificare, ad esempio, che "Sì, Anna è il legittimo proprietario di questa terra". Questo approccio limita l'esposizione e il rischio, ma aggiunge anche un altro passo allo scambio…

WHAT IS BLOCKCHAIN? |2

Perché la blockchain sta rivoluzionando… Motivo num. 3

Come ora sappiamo, tutti i blocchi aggiunti alla catena sono stati verificati come veri e non possono essere manomessi, quindi Anna può semplicemente mostrare a Steve le sue informazioni sul titolo di proprietà sulla blockchain.

Questo tipo di interazione peer-to-peer affidabile con i nostri dati può rivoluzionare il modo in cui accediamo, verifichiamo e trasferiamo gli uni con gli altri. E poiché blockchain è un tipo di tecnologia, e non una singola rete, può essere implementata in molti modi diversi. Alcune blockchain possono essere completamente pubbliche e aperte a tutti per la visualizzazione e l'accesso. Altre possono essere chiuse a un gruppo selezionato di utenti autorizzati, ad esempio la vostra azienda, un gruppo di banche o agenzie governative.

WHAT IS BLOCKCHAIN? |3

Perché la blockchain sta rivoluzionando… Motivo num. 3

Deve essere chiaro che parlare di blockchain privata significa attingere al significato più lasco di blockchain. Potremo dire che, al di là di perdere gli attributi di *permissionless* e di *riservatezza e libertà finanziaria* per cui è stata creata... (1) Non può esserci una blockchain trustless senza avere la capacità di disporre di hashing power per disincetivare economicamente un potenziale attaccante. (2) Senza una criptovaluta nativa come incentivo per la remunerazione dei minatori, non c'è nessuna garanzia nella scarsità del mezzo di scambio che è alla base dell'intero sistema. Da questo punto di vista è possibile ma non sensato parlare di blockchain privata, poiché separando blockchain da criptovaluta non sempra possibile garantire la sicurezza nella validazione e storaggio dei dati senza riporre la fiducia in un terzo.

WHAT IS BLOCKCHAIN? |3

Perché la blockchain sta rivoluzionando… Motivo num. 3

Se una blockchain privata ha senso, lo è come strumento di marketing (BAAE, ovvero, Blockchain as an Excuse). In una blockchain privata non sembra essere possibile garantire che il gatekeeper, o alcuni elementi stessi del consorzio che la gestisce non abbiano la capacità di alterare i dati. Questo in Bitcoin è evitato dalla ampiezza della rete, ergo dall'hashing power. Ci possono essere dunque altre applicazioni significative della blockchain al di là di essere La blockchain di Bitcoin, o al limite la tecnologia che permette lo scambio di valore senza terze parti implicate all'interno di altre crittovalute?

WHAT IS BLOCKCHAIN? |3

Perché la blockchain sta rivoluzionando… Motivo num. 3

Poniamo il caso di un gruppo di aziende che vogliono condividere tra loro un insieme definito di informazioni sulle loro operazioni, è possibile creare una blockchain permissioned del consorziale, senza mining e crittovaluta, per garantire che nessun attore del consorzio possa manipolare i dati una volta condivisi?

Sì, è possibile utilizzare questa tecnologia, inserendo un tempo di validazione del blocco arbitrario dove ciascun blocco deve essere firmato con la chiave privata di ciascun partecipante. Così, ogni partecipante ha una copia dell'intera blockchain e nessun altro (nemmeno a maggioranza!) può modificarla. La domanda successiva è: può un attore esterno essere certo che questa blockchain è a prova di manomissione?

WHAT IS BLOCKCHAIN? |3

Perché la blockchain sta rivoluzionando… Motivo num. 3

No, i partecipanti del consorzio potrebbero accordarsi per alterare i dati storati ad esempio...

Ma allora, è davvero impossibile garantire affidabilità e sicurezza?

Un uso che potremmo chiamare “parassitario” della blockchain di Bitcoin potrebbe risolvere questo problema immaginate semplicemente di prendere l’hash di ogni blocco della blockchain privata, e di inserirlo attraverso una transazione nella blockchain di Bitcoin.

WHAT IS BLOCKCHAIN? |3

Perché la blockchain sta rivoluzionando… Motivo num. 3

Ma, al di là che questo è reso possibile solo tornando alla blockchain di Bitcoin…

Questo risolverebbe tutti i problemi a livello di immutabilità del dato, ma lascerebbe aperto un altro problema: la verità e l'immutabilità non sono la stessa cosa…

Scrivere sulla blockchain che sono il Principe delle tenebre, non significa che questo sia vero… (ma lo rende immutabile)

Capite qual è il problema? "Deterritorializzare" la blockchain dal suo "territorio" (Bitcoin e cloni) tende a porre problemi di altro tipo…

WHAT IS BLOCKCHAIN? |3

Perché la blockchain sta rivoluzionando… Motivo num. 3

E ci sono anche blockchain ibride pubblico-privato. In alcune, gli accessi privati possono vedere tutti i dati, mentre il pubblico può vedere solo delle selezioni. In altri, tutti possono vedere tutti i dati, ma solo alcune persone hanno accesso per aggiungere nuovi dati. Un governo, per esempio, potrebbe utilizzare un sistema ibrido per registrare i confini della proprietà di Anne, e il fatto che lei lo possiede, pur mantenendo private le sue informazioni personali. Oppure potrebbe consentire a tutti di visualizzare i record di proprietà, ma si riserva il diritto esclusivo di aggiornarli.

WHAT IS BLOCKCHAIN? |3

Perché la blockchain sta rivoluzionando… Motivo num. 3

È la combinazione di tutti questi fattori - decentralizzare i dati, creare fiducia nei dati e permetterci di interagire direttamente l'uno con l'altro e i dati - che dà alla tecnologia blockchain il potenziale per sostenere molti dei modi in cui interagiamo l'uno con l'altro. Ma, proprio come l'ascesa di internet, questa tecnologia porterà con sé tutti i tipi di complesse questioni politiche riguardanti la governance, il diritto internazionale, la sicurezza e l'economia. […]

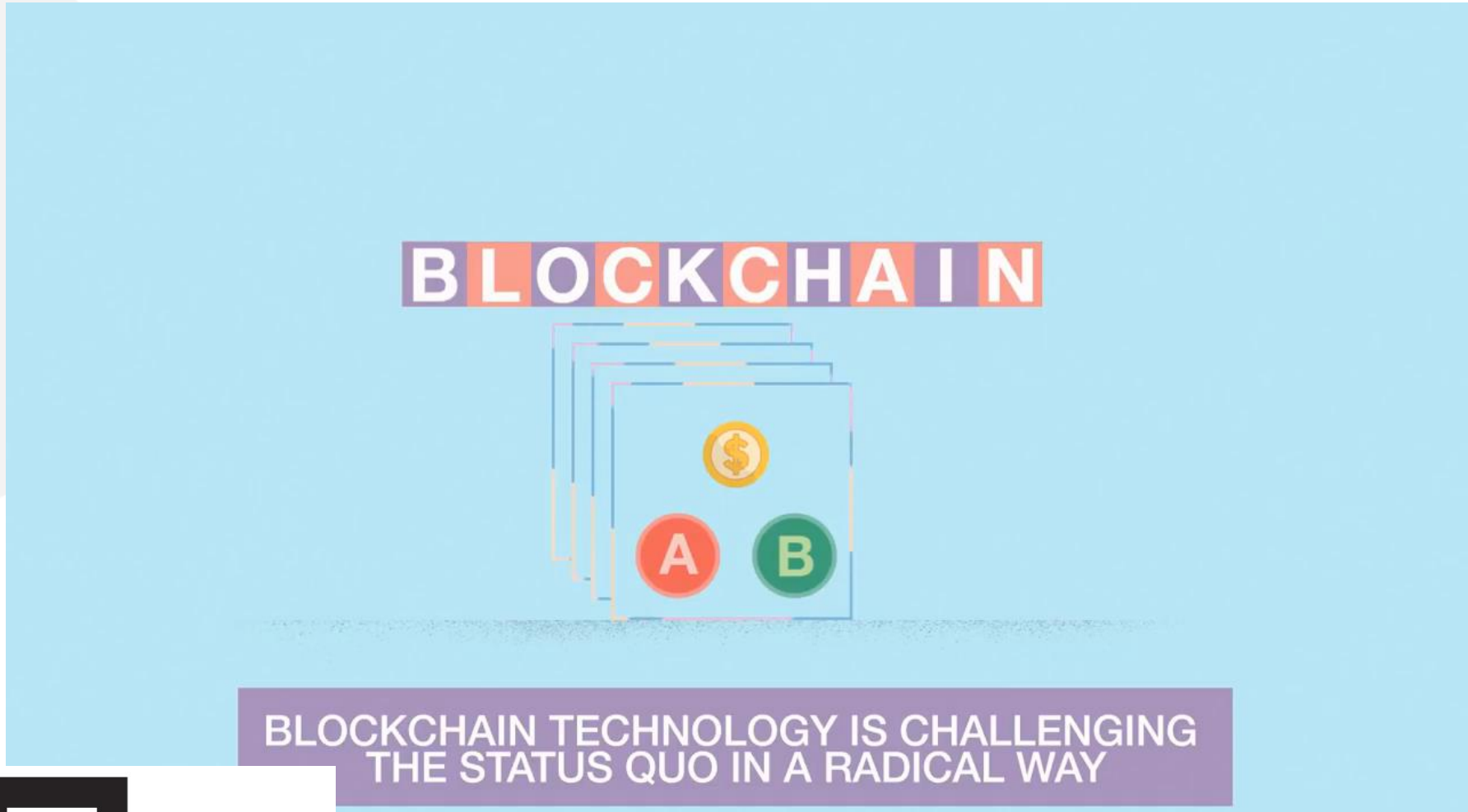
IN CONCLUSIONE…

Perché la blockchain sta rivoluzionando… Motivo num. 3

L'intento di questo webinar era duplice...

- Dare un'idea generale di come sia nata storicamente la blockchain, di come funzioni nelle sue linee generali e di quali siano le sue proprietà.
- Sviluppare un minimo di pensiero critico sul bombardamento di "blockchain come panacea di tutti i malanni".
- E, a proposito di debunking…

DEBUNKING?


BLOCKCHAIN
A
B
BLOCKCHAIN TECHNOLOGY IS CHALLENGING
THE STATUS QUO IN A RADICAL WAY

CONTATTI

B CADEMY Srl.
Via Villanova di Sotto
33170 Pordenone
info@bcademy.it

Bcademy **bcademy.it**

Alessio Salvetti
Co-founder & VP
Chief Product Officer

alessio.salvetti@bcademy.it

+39 340 1554099

Il Fondo Sociale Europeo in Friuli Venezia Giulia
Programma Operativo Regionale 2014-2020

Unione europea
Fondo sociale europeo

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

UN INVESTIMENTO PER IL TUO FUTURO

in rete fvg
seminari per l'innovazione in rete

GRAZIE!

Il Fondo Sociale Europeo in Friuli Venezia Giulia
Programma Operativo Regionale 2014-2020
Unione europea Fondo sociale europeo
REGIONE AUTONOMA FRIULI VENEZIA GIULIA
UN INVESTIMENTO PER IL TUO FUTURO
in rete fvg
seminari per l'innovazione in rete