BITCOIN CONTRO SISTEMI DI PAGAMENTO TRADIZIONALI: UNO È PIÙ EFFICIENTE DELL'ALTRO?

Florian Ginez, CFA, Senior Quantitative Associate
August 2019

Quando Bitcoin fu inizialmente presentato al mondo, su internet, dal suo anonimo inventore noto sotto lo pseudonimo di Satoshi Nakamoto, nel 2008, aveva a sostenerlo solo una manciata di entusiasti. Le cose sono decisamente cambiate negli ultimi anni e la cripto-valuta si è diffusa in maniera tale da diventare uno degli sviluppi tecnologici di maggiore interesse a livello mondiale.

Con l'introduzione del concetto di "blockchain" per i pagamenti, Bitcoin prometteva di portare un più alto livello di fiducia e sicurezza nella realtà delle transazioni finanziarie. Anche se dall'arrivo di Bitcoin sono stati lanciati altri sistemi di blockchain, quest'ultimo è ancora considerato da molti il sistema più sviluppato e affidabile; percezione in parte dovuta al fatto che l'infrastruttura costruita attorno a Bitcoin supera ancora quella delle alternative.

Oggi, Bitcoin gestisce un numero significativo e un elevato volume di transazioni in dollari, aspetto che ha attirato l'attenzione del mondo sul suo potenziale come sistema di pagamento. Ma come si raffronta rispetto ai sistemi di pagamento tradizionali? E' più efficiente?

In questo articolo illustreremo le principali differenze tra Bitcoin e i sistemi di pagamento tradizionali ed esamineremo i punti di forza e le debolezze di ciascuno.

Che cos'è Bitcoin?

Pensato come sistema di pagamento, Bitcoin permette il trasferimento di valore allo stesso modo dei bonifici bancari o dei pagamenti a mezzo carta. Tuttavia, l'uso del termine "Bitcoin" a volte può creare confusione, poiché non si riferisce sempre alla stessa cosa. Infatti, lo stesso termine indica una moneta, un protocollo e una rete. A un livello molto alto, queste sub-componenti sono simili a quelle che costituiscono i sistemi di pagamento elettronico tradizionali. Esistono tuttavia differenze sostanziali nel modo in cui i due sistemi operano. Prima di mettere a confronto il sistema Bitcoin con i sistemi di pagamento tradizionali, analizziamo più in dettaglio le sub-componenti di Bitcoin.

UNA MONETA

Una moneta è una forma di denaro generalmente accettata e usata quale mezzo di scambio, una riserva di valore o un'unità di conto. Le monete tradizionali come il dollaro USA, l'euro o la sterlina britannica – spesso chiamate monete fiat o monete a corso legale- sono garantite dai governi e traggono il loro valore da tale supporto. Oggi, le monete non sono garantite direttamente dall'oro o da altre materie prime o attivi.

Analogamente ai sistemi tradizionali, anche Bitcoin è usato come mezzo di scambio, una riserva di valore o un'unità di conto. E come le monete fiat, la cripto-valuta non è garantita da commodity o altri attivi. Tuttavia, una differenza sostanziale tra il bitcoin e le monete fiat tradizionali è che, mentre queste ultime hanno corso legale e sono garantite da un governo e controllate da una banca centrale, il bitcoin è una valuta globale "distribuita", non controllata da nessun ente centralizzato, e le sue scorte aumentano automaticamente ad un tasso prestabilito.

Immagine 1: transazione fiat contro transazione bitcoin

mBTC = millibitcoin.

UN PROTOCOLLO

Un protocollo può essere descritto come un insieme di regole che disciplinano alcune azioni o comunicazioni in determinate condizioni.

Il termine Bitcoin si riferisce anche al protocollo sottostante alle transazioni o all'insieme di regole e meccanismi che consentono al sistema di operare in sicurezza, pur funzionando secondo una logica distribuita e non centralizzata.

Il protocollo Bitcoin usa la tecnologia Distributed Ledger (o DLT) – un data base distribuito, basato sul consenso- oltre a una crittografia (che protegge le informazioni) per verificare e registrare le transazioni, risolvendo al contempo il problema della "doppia spesa", ossia il rischio che il denaro digitale venga copiato e speso più volte. Il protocollo Bitcoin è il primo sistema a gestire la questione senza la necessità di un'autorità centrale.

Immagine 2: transazione bancaria contro transazione Bitcoin

Il sistema bancario tradizionale dipende, inoltre, da standard di comunicazione e da svariate regole e meccanismi per l'autorizzazione, il controllo e il regolamento dei trasferimenti. La differenza sostanziale risiede, ancora una volta, nel fatto che il sistema tradizionale è affidato a controparti centralizzate mentre il protocollo Bitcoin rende superflua la presenza di questi intermediari.

UNA RETE

Il sistema di pagamento tradizionale dipende dalla rete bancaria per processare le transazioni. Gli istituti bancari di tutto il mondo sono direttamente o indirettamente connessi l'uno con l'altro e, quando un pagamento viene avviato dalla banca di un pagatore, passa in sequenza attraverso vari processi di controllo di una rete di intermediari.

Per contro, la rete Bitcoin è paritaria (P2P), un eco-sistema di computer interconnessi che verifica e approva le transazioni, mantenendo contemporaneamente un registro di tutte le transazioni avvenute: la blockchain. Questo registro è pubblico e chiunque può installare un software Bitcoin e verificare tutto lo storico di ogni transazione Bitcoin processata. Questi computer sono chiamati "nodi".

Immagine 3: rete bancaria contro transazione Bitcoin

Il sistema Bitcoin in cosa differisce dai sistemi di pagamento tradizionali?

Tutti i sistemi di transazione si basano su un principio cardine: la fiducia. Quando si decide di vendere un prodotto in cambio di denaro è essenziale avere la certezza che si verrà effettivamente pagati. L'acquirente possiede la somma necessaria all'acquisto? Ha la possibilità di bloccare il pagamento una volta che quest'ultimo è stato avviato? Osserviamo la differenza tra le transazioni con carta e contanti rispetto alle transazioni Bitcoin.

TRANSAZIONI IN CONTANTI

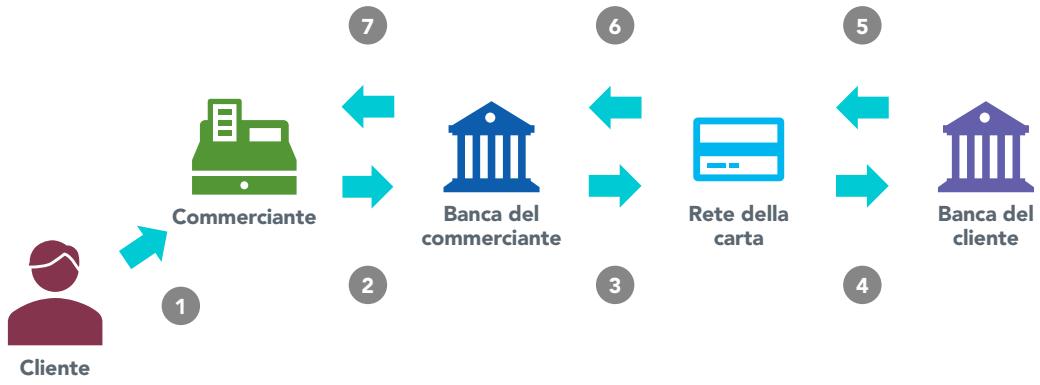
Una transazione in contanti gestisce la questione della fiducia in maniera piuttosto efficace. Se un cliente vi dà una banconota avrete direttamente tra le mani il denaro derivante dall'operazione. **Non c'è intermediario.** Tuttavia, anche questa procedura presenta dei difetti. Ad esempio, l'acquirente potrebbe darvi una banconota falsa.

Immagine 4: una transazione in contanti

TRANSAZIONI CON CARTA

Quando il pagamento avviene con carta, il pagamento medesimo deve essere processato da un circuito come VISA o Mastercard, oltre che da una rete di banche per l'autorizzazione, il controllo e il regolamento. La fiducia nasce dall'affidarsi a note istituzioni finanziarie che eseguono una serie di controlli mentre la transazione è in atto. Le immagini dalla 5 alla 7, illustrate di seguito, mostrano il processo per i pagamenti tramite carta.

Immagine 5: iter autorizzativo del pagamento con carta

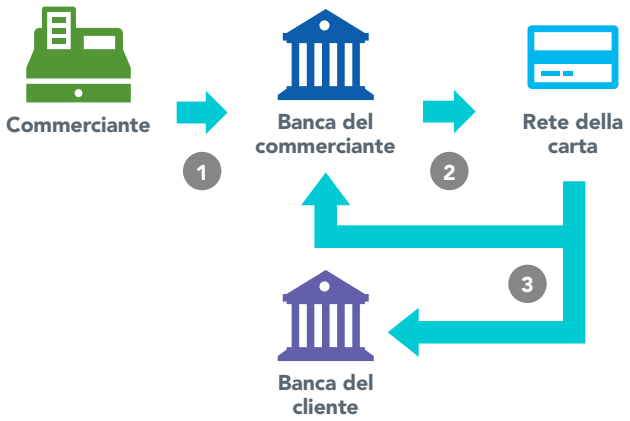


La fase autorizzativa serve per verificare l'identità del cliente e il suo reale possesso dei fondi che sta cercando di usare, oltre che la disponibilità dei fondi medesimi.

Quando inserite la vostra carta in un terminale e digitate il codice pin (1) nel corso di una transazione, i dettagli del pagamento e le informazioni sulla carta vengono inviate alla banca del commerciante (2), che in seguito sottopone tali dettagli al circuito su cui poggia la carta stessa (3). A sua volta, il circuito richiederà autorizzazione alla vostra banca (4) e, se i dettagli sono corretti e disponete dei fondi, la vostra banca invierà un'autorizzazione al commerciante tramite gli stessi intermediari, uno dopo l'altro (5, 6, 7).

L'intero processo avviene nel giro di pochi secondi, passati i quali potrete uscire dal negozio con le merci acquistate. Ma il processo continua dietro le quinte. Anche se l'autorizzazione è stata data, i fondi sono ancora sul vostro conto.

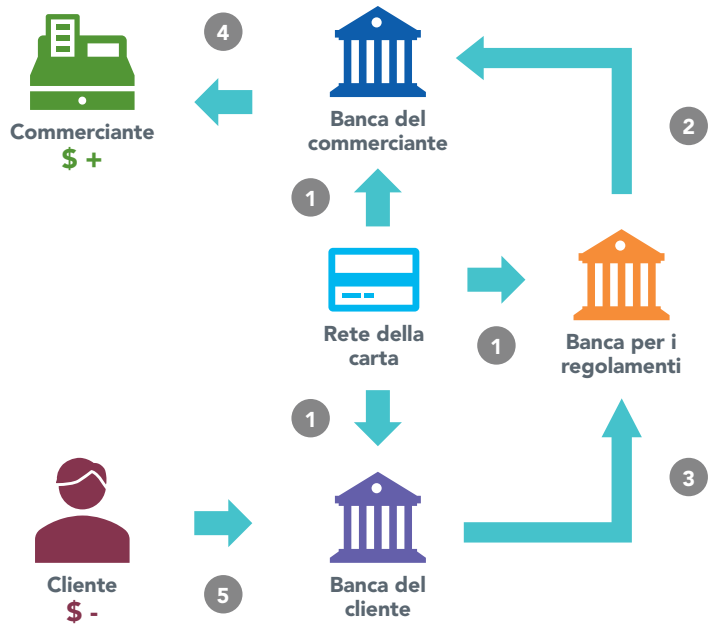
Immagine 6: processo di controllo del pagamento con carta



Il processo di controllo comporta lo scambio di informazioni correlate alla transazione usato per la verifica del denaro che dovrà essere addebitato alla banca del cliente e accreditato sulla banca del venditore.

Alla fine di ogni giorno, tutte le transazioni approvate nel corso della giornata vengono inviate dal commerciante alla banca del commerciante (1), che poi trasmette i dettagli al circuito su cui poggia la carta (2). Il circuito convalida le informazioni, invia le informazioni sull'acquisto alle banche dei clienti e, infine, manda le informazioni necessarie per le riconciliazioni sia alla banca del commerciante che alle banche dei clienti (3).

Immagine 7: processo di regolamento dei pagamenti con carta



Infine, il pagamento può essere regolato, come illustra l'Immagine 7. Il regolamento si verifica ogni giorno su base netta aggregata e coinvolge il reale trasferimento dei fondi. Il circuito su cui poggia la carta computa la posizione del regolamento netto che la banca del cliente deve pagare alla banca del commerciante e invia l'informazione a entrambe le banche, oltre che ad un nuovo attore, la banca per i regolamenti (1). La banca per i regolamenti paga la banca del commerciante (2) e quest'ultima paga la banca per i regolamenti (3). Infine, il commerciante avrà l'accredito (4) e il cliente l'addebito (5).

Tutto il processo (dall'autorizzazione al regolamento) in genere richiede tra le 24 e le 48 ore. Come mostrano i diagrammi di cui sopra, è un processo piuttosto farraginoso che coinvolge diverse controparti, le quali devono creare e trasmettere informazioni in sequenza.

Si tratta, tuttavia, di un sistema ben consolidato e sufficientemente affidabile da essersi guadagnato un alto livello di fiducia da parte degli utenti. E' infatti così ampiamente diffuso e accettato che Paesi come la Svezia puntano a diventare "cashless societies", cioè letteralmente "società senza denaro contante".

In questo modello, il circuito su cui poggia la carta svolge un ruolo essenziale. Poiché nel processo sono coinvolte numerose figure, tutte con i propri sistemi informatici, la comunicazione può diventare piuttosto difficile. Il circuito "è responsabile della raccolta di tutte le transazioni e del funzionamento di un gateway. Scambia informazioni tra la [banca dei clienti] e le [banche dei commercianti], stabilisce regole e processi per la partecipazione al circuito, crea standard di formattazione per le informazioni che circolano nel circuito e facilita il regolamento monetario tra le sue banche clienti"[1].

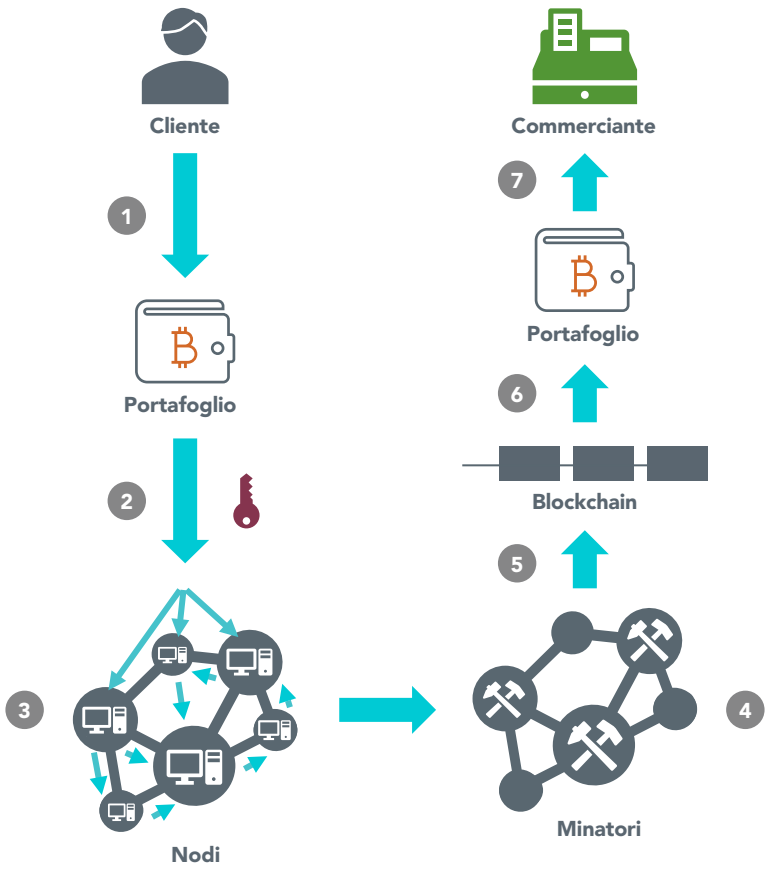
In altri termini, fornisce l'infrastruttura e gli standard per lo scambio di informazioni tra i soggetti coinvolti.

[1] Herbst-Murphy, Susan (2013). "Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts".

TRANSAZIONI BITCOIN

Quando invia bitcoin tramite la rete Bitcoin, il processo segue invece un percorso molto diverso.

Immagine 8: processo di transazione in bitcoin



Anzitutto, come mittente, inserirete l'indirizzo Bitcoin del destinatario (analogo a un numero di conto bancario in un bonifico) e il numero di bitcoin da spedire usando la vostra interfaccia di portafoglio digitale (1). Potete pensare a questa fase come equivalente al terminale di pagamento del commerciante che prepara le informazioni per il pagamento in una transazione con carta. Per i pagamenti con bitcoin in negozio, i commercianti spesso scannerizzano la merce e poi creano un codice QR che potete scannerizzare con il vostro portafoglio digitale sul vostro telefono, inserendo automaticamente la somma da pagare e l'indirizzo del commerciante.

Il portafoglio invia poi queste informazioni al circuito, usando la vostra "credenziale personale" per la firma digitale della transazione (2). La firma digitale è in un certo senso simile a quando un cliente inserisce il codice pin o firma la ricevuta nel corso di una transazione con carta. Il suo scopo è infatti quello di provare la titolarità dei fondi da parte del mittente.

Alcuni nodi riceveranno la transazione, prima di trasferire i dettagli ad altri nodi e, in pochi secondi, la vostra transazione si diffonderà in tutto il circuito (3). Tutti i nodi possono verificare in maniera indipendente la transazione e controllare che disponiate effettivamente dei bitcoin che intendete spedire e che non li abbiate già spediti in precedenza. Le fasi 1, 2 e 3 corrispondono alla fase autorizzativa dei pagamenti con carta.

I "minatori" raggrupperanno quindi le transazioni in un'unità o batch e cercheranno di risolvere un problema intensivo dal punto di vista computazionale. Il primo a risolvere il problema notificherà alla rete il completamento del pagamento (4). Tutti gli altri nodi potranno facilmente verificare se il minatore sta dicendo la verità, nel qual caso il nuovo batch - un blocco- verrà aggiunto alla blockchain (5). Il passaggio 5 è simile alla fase di regolamento nell'esempio di transazione con carta poiché è in questa fase che il denaro cambia effettivamente proprietà.

Lo scopo della fase 4 è quello di garantire che la blockchain non possa essere modificata. Modificarla richiederebbe una forte potenza di calcolo e, pertanto, operativamente sarebbe molto difficile. Poiché, dopo il blocco contenente la vostra transazione ne vengono aggiunti altri, modificare tale blocco diventa esponenzialmente più difficile.

Una volta che il blocco contenente la transazione viene aggiunto alla blockchain e registrato nel registro distribuito, il portafoglio del commerciante vedrà il pagamento come confermato (6) e il commerciante sarà il nuovo proprietario di quei bitcoin (7).

Il tempo necessario per compiere l'intero processo varia a seconda di diversi fattori. Tuttavia, per estrarre un blocco servono in media 10 minuti. Quindi, anche nel caso vogliate aspettare altri cinque blocchi (lo standard sono sei conferme) per considerare effettivamente la transazione come avvenuta, ragionevolmente ci vorrà un'ora di tempo.

Quali sono i vantaggi di Bitcoin rispetto ai sistemi di pagamento tradizionali?

Anche se alcuni dei potenziali benefici del sistema Bitcoin, quali ad esempio l'anonimato, la trasparenza e l'indipendenza dai governi e dalle banche centrali sembrano essere più che altro una questione ideologica, Bitcoin di certo offre dei vantaggi concreti in termini di fiducia ed efficienza operativa.

MENO INTERMEDIARI

Quando i bitcoin vengono trasferiti ad un altro soggetto sono essenzialmente necessari altri due intermediari affinché il trasferimento delle monete sia effettivo: il vostro portafoglio e il circuito Bitcoin. I nodi e i minatori rappresentano solo delle sotto-componenti della rete e aggiungerne o rimuoverne alcuni non intacca il suo funzionamento. Al contrario, il sistema di pagamento con carta richiede un minimo di quattro intermediari, spesso in realtà anche qualcuno di più.

IPIÙ EFFICIENTE

Trattandosi di un sistema distributivo, il protocollo Bitcoin permette ad ogni componente di accedere e verificare tutte le transazioni passate e quelle in sospeso, in ogni momento e contemporaneamente, caratteristica che consente di ottimizzare i tempi. Durante il procedimento non possono verificarsi errori; è sufficiente che l'indirizzo venga inserito correttamente all'inizio della transazione e i fondi arriveranno a destinazione.

Non solo il sistema di pagamento tradizionale necessita di un numero maggiore di intermediari ma esso moltiplica anche gli scambi di comunicazioni avanti e indietro, processo che deve avvenire in sequenza. Ciò richiede del tempo e, per strada, possono verificarsi degli errori.

FIDUCIA DISTRIBUITA E SINGOLI PUNTI DEBOLI

Tuttavia, il vantaggio principale di Bitcoin risiede in realtà nel modo in cui il sistema gestisce la fiducia nelle transazioni ed elimina i singoli punti deboli.

Con il sistema tradizionale è necessario confidare nel fatto che le regole e i meccanismi non comportino errori e che **ogni singola controparte** coinvolta operi in maniera corretta. Se una controparte lungo la catena risulta compromessa per una ragione o per l'altra, allora l'intera catena è compromessa.

Con Bitcoin, l'insieme di regole e meccanismi che puntellano il sistema rende la frode, la manipolazione e gli errori impossibili. Poiché il software Bitcoin è una fonte aperta, chiunque nel mondo può accedervi e verificarlo. Nella serie storica decennale di Bitcoin non è mai stata rinvenuta nessuna falla in termini di sicurezza. Nessuno ha mai trovato il modo di modificare una transazione firmata o di alterare la blockchain.

Inoltre, il bello di un sistema distribuito è che non è necessario fidarsi di ogni singolo componente poiché non c'è un singolo punto debole. La compromissione di uno o più nodi non compromette l'intero circuito. Per modificare in maniera fraudolenta le transazioni in sospeso o la blockchain delle transazioni passate sarebbe necessario assumere il controllo della maggioranza del potere computazionale delle rete.

Infine, il rischio risiede nel vostro portafoglio digitale, in quanto quest'ultimo custodisce le vostre credenziali personali. Chiunque entri in possesso delle vostre credenziali private può spendere i fondi presenti nel portafoglio. E' questa la ragione per la quale, al fine di prevenire il fenomeno dell'hackeraggio, vengono adottati portafogli offline, comunemente definiti "celle frigorifere". Ma, nel momento in cui la transazione è stata firmata, è sicura. Non ci sono singoli punti deboli e non è necessario che vi fidiate di ogni singolo componente.

Quale migliore sistema di fiducia di uno in cui non è necessario fidarsi di nessuno?

INFORMAZIONI IMPORTANTI

Comunicazioni emesse all'interno dello Spazio economico europeo ("SEE"): Il presente documento è stato emesso e approvato da WisdomTree Ireland Limited, società autorizzata e regolamentata dalla Central Bank of Ireland.

Comunicazioni emesse in giurisdizioni non appartenenti al SEE: Il presente documento è stato emesso e approvato da WisdomTree UK Limited, società autorizzata e regolamentata dalla Financial Conduct Authority del Regno Unito.

Per fare riferimento a WisdomTree Ireland Limited e a WisdomTree UK Limited si utilizza per entrambe la denominazione "WisdomTree" (come applicabile). La nostra politica sui conflitti d'interesse e il nostro inventario sono disponibili su richiesta.

Solo per clienti professionali. Le informazioni contenute nel presente documento sono fornite a titolo meramente informativo e non costituiscono né un'offerta di vendita né una sollecitazione di un'offerta di acquisto di titoli o azioni. Il presente documento non deve essere utilizzato come base per una qualsiasi decisione d'investimento. Gli investimenti possono aumentare o diminuire di valore e si può perdere una parte o la totalità dell'importo investito. Le performance passate non sono necessariamente indicative di performance future. Qualsiasi decisione d'investimento deve essere basata sulle informazioni contenute nel Prospetto informativo di riferimento e deve essere presa dopo aver richiesto il parere di un consulente d'investimento, fiscale e legale indipendente.

Il presente documento non è, e in nessun caso deve essere interpretato come, una pubblicità o qualsiasi altro strumento di promozione di un'offerta pubblica di azioni o titoli negli Stati Uniti o in qualsiasi provincia o territorio degli Stati Uniti. Né il presente documento né alcuna copia dello stesso devono essere acquisiti, trasmessi o distribuiti (direttamente o indirettamente) negli Stati Uniti.

Il presente documento può contenere commenti indipendenti sul mercato redatti da WisdomTree sulla base delle informazioni disponibili al pubblico. Benché WisdomTree si adoperi per garantire l'esattezza del contenuto del presente documento, WisdomTree non garantisce né assicura la sua esattezza o correttezza. Qualsiasi terzo fornitore di dati di cui ci si avvalga per reperire le informazioni contenute nel presente documento non rilascia alcuna garanzia o dichiarazione di sorta in relazione ai suddetti dati. Laddove WisdomTree abbia espresso dei pareri relativamente al prodotto o all'attività di mercato, si ricorda che tali pareri possono cambiare. Né WisdomTree, né alcuna consociata, né alcuno dei rispettivi funzionari, amministratori, partner o dipendenti, accetta alcuna responsabilità per qualsiasi perdita, diretta o indiretta, derivante dall'utilizzo del presente documento o del suo contenuto.

Il presente documento può contenere dichiarazioni previsionali, comprese dichiarazioni riguardanti le attuali aspettative o convinzioni in relazione alla performance di determinate classi di attività e/o settori. Le dichiarazioni previsionali sono soggette a determinati rischi, incertezze e ipotesi. Non vi è alcuna garanzia che tali dichiarazioni siano esatte, e i risultati effettivi possano discostarsi significativamente da quelli previsti in dette dichiarazioni. WisdomTree raccomanda vivamente di non fare indebito affidamento sulle summenzionate dichiarazioni previsionali.

I rendimenti storici ricompresi nel presente documento potrebbero essere basati sul back test, ossia la procedura di valutazione di una strategia d'investimento, che viene applicata ai dati storici per simulare quali sarebbero stati i rendimenti di tale strategia. Tuttavia, i rendimenti basati sul back test sono puramente ipotetici e vengono forniti nel presente documento a soli fini informativi. I dati basati sul back test non rappresentano rendimenti effettivi e non devono intendersi come un'indicazione di rendimenti effettivi o futuri.