MODULO 5:

# Yeld farming, DeFi, Cex, Dex, DAO, sidechains e rete Lightning

## DEFI

Cosa è la DeFi?

“DeFi”, o Decentralized Finance (Finanza Decentralizzata), è il nome che definisce una grande tendenza che si sta sviluppando intorno alla tecnologia blockchain negli ultimi anni che mira a sviluppare piccoli elementi della finanza tradizionale, ma con un ulteriore grado di trasparenza e decentralizzazione. Questi piccoli tasselli, proprio come i mattoncini Lego, sono combinabili tra loro con l’obiettivo di sviluppare un intero ecosistema di piccole soluzioni che, nel loro insieme, formino una grande soluzione per la finanza rendendo superflua la necessità di istituzioni finanziarie centralizzate e opache che non apportano più alcun valore.

Questa è l'idea che ha portato alla creazione del termine “DeFi”, e quella che ha portato la sua evoluzione fino al punto in cui si trova oggi. Infatti, al giorno d'oggi è impossibile ignorare l'enorme impatto che la DeFi ha sul mondo delle criptovalute.

DeFi, l'idea che sta cambiando il mondo finanziario

Immagina un mondo in cui chiunque possa creare prodotti finanziari trasparenti, equi ed efficienti, facendo passare in secondo piano banche, grandi istituzioni finanziarie, istituti di credito e compagnie assicurative, o addirittura, rendendoli del tutto superflui e facendoli scomparire. Immagina anche un mondo in cui chiunque

possa interagire liberamente con tali prodotti. Questa è la DeFi.

Potremmo dire che questo concetto trasforma le attuali strutture finanziarie centralizzate in strutture decentralizzate, senza intermediari di fiducia, basate su smart contract all'interno di una blockchain, in cui sia riportato in modo trasparente un registro scritto e inalterabile di ogni azione compiuta. L'impatto di una tendenza come questa è enorme. Siamo solo agli inizi e già la creatività della comunità mondiale sta dando forma a versioni alternative di quasi tutti i prodotti finanziari già esistenti.

Immagina di aver bisogno di un prestito per avviare un'attività. Invece di andare in banca, puoi rivolgerti a una piattaforma DeFi e richiedere un prestito. Tale prestito ha condizioni (tralasciando i tecnicismi) piuttosto chiare e trasparenti regolate da uno smart contract pubblico e immutabile. Inoltre, tutte le azioni effettuate sulla piattaforma rimangono visibili e registrate in modo immutabile anche sulla blockchain. Forse ancora non hai acquisito le competenze necessarie per verificare l'affidabilità di un servizio DeFi, ma grazie alla sua trasparenza, migliaia di occhi potranno analizzarlo e metterlo in discussione, segnalandone eventuali malfunzionamenti.

Grazie alla DeFi, non è necessario avere un conto corrente, né portare con sé decine di documenti, fare la fila per consegnarli e aspettare settimane per una

risposta. Invece, comodamente dal tuo divano, con il tuo smartphone puoi completare l'intera procedura e ricevere il denaro direttamente sul tuo conto.
Tuttavia, le DeFi possono essere molto di più: possono essere il veicolo per l'economia e la finanza di quel mondo sempre più presente che, grazie alla tecnologia blockchain, sta iniziando a decentralizzarsi. Sono lo strumento che apre le porte agli investimenti internazionali senza troppa burocrazia, costi e tempi lunghi, garantendo maggiori livelli di fiducia e trasparenza. Uno strumento che permetta alle persone non bancarizzate di accedere ai servizi senza le imposizioni delle banche, godendo delle stesse opportunità di crescita personale nel proprio percorso di sviluppo.

## Origini della DeFi

Se sei tra coloro che pensano che le DeFi abbiano avuto origine con la nascita del Bitcoin, hai ragione: il Bitcoin è senza dubbio la prima piattaforma DeFi al mondo.
Ma l'origine dell'idea è molto più antica. Nick Szabo indicava, forse senza saperlo, la nascita delle DeFi quando presentò la sua idea degli smart contract, nel 1995. Sono 13 anni prima della creazione del Bitcoin, e si tratta di un'idea senza dubbio in anticipo sui tempi.
Tuttavia, ciò che ha rappresentato un cambiamento radicale rispetto a questa idea è stato l'arrivo di Ethereum, nel 2014, e dei suoi smart contract che

consentivano agli sviluppatori di creare qualsiasi cosa potessero immaginare su una blockchain.
Ciò che era nato come un esperimento, si è ora trasformato in un movimento a sé stante, un ecosistema finanziario decentralizzato il cui TVL globale della DeFi nel 2026 oscilla tra gli 85 e i 180 miliardi di dollari a seconda del momento di mercato e della metodologia usata.
Alcuni progetti sono arrivati a creare ponti tra la finanza tradizionale e le criptovalute. Grazie a questo lavoro ora possiamo contare su mercati di liquidità, sistemi di prestito e exchange decentralizzati (DEX), e tutto questo è solo l'inizio.

Caratteristiche della DeFi

Ora che conosciamo il concetto, le sue origini e le differenze tra i vari modelli finanziari digitali, vediamo quali sono le caratteristiche delle piattaforme DeFi.
Sicure:
Funzionano sulla base della tecnologia blockchain e degli smart contract, presentano alti livelli di decentralizzazione e sono molto sicure grazie all'uso di potenti tecniche crittografiche che garantiscono che l'accesso e l'utilizzo della piattaforma possano essere effettuati solo da persone autorizzate. Le piattaforme DeFi hanno quindi la capacità di operare senza che una gerarchia burocratica si imponga sulle loro funzioni, senza fiducia in terzi. Ciò significa che non sono

necessari intermediari di fiducia, poiché tale funzione sarà svolta dalla blockchain, che terrà traccia di tutto in modo sicuro e immutabile.

Trasparenti:

Un'altra grande caratteristica delle DeFi è la loro trasparenza. Essendo basate su software libero, ogni riga di codice delle piattaforme è verificabile. Inoltre, anche i movimenti di risorse sono verificabili, poiché avvengono tutti sulla blockchain.

Senza confini:

L'accesso a una piattaforma DeFi non ha confini. Puoi trovarti in qualsiasi paese del mondo e accedere ai suoi servizi senza problemi.

Pro e contro della tecnologia

Naturalmente, come ogni tecnologia, presenta vantaggi e svantaggi, ed è per questo che ne esamineremo alcuni.

Pro:

- Consente l'accesso ai servizi finanziari a milioni di persone che non dispongono di un conto bancario. Si tratta senza dubbio di un'occasione d'oro per portare sviluppo e libertà finanziaria a coloro che, per vari motivi, non hanno potuto possono usufruire di questi servizi.
- Rende molto più semplice il finanziamento internazionale di aziende e progetti. Le piattaforme

DeFi possono adattarsi alle esigenze di un pubblico specifico per portare sviluppo e investimenti dove necessario, e tali investimenti possono provenire da qualsiasi parte del mondo in modo sicuro.

- Crea un nuovo punto di diversificazione economica e rappresenta un importante motore di sviluppo economico nel medio termine, grazie all'enorme potenziale economico di criptovalute come il Bitcoin.

Contro:

- Sebbene la blockchain abbia dimostrato di essere una tecnologia molto sicura, ci sono ancora molti aspetti da migliorare, in particolare per quanto riguarda il livello di sicurezza e la verifica di sicurezza degli smart contract. Un errore in uno smart contract comporta un errore nella piattaforma, come ha dimostrato The DAO.
- Protocolli di intervento di fronte alla volatilità delle criptovalute a volte insufficienti: molte piattaforme DeFi hanno creato meccanismi operativi che garantiscono la loro stabilità economica di fronte alla volatilità delle criptovalute. Tuttavia, a volte questi meccanismi non proteggono completamente l'ecosistema dalle forti fluttuazioni, situazione che porta a perdite milionarie. Un caso di questo tipo è quello di MakerDAO e DAI, le cui fluttuazioni e azioni di correzione hanno dimostrato che la decentralizzazione e i protocolli di azione mal

calibrati possono spesso rappresentare un punto debole per queste piattaforme, se non gestiti correttamente.

DeFi e FinTech: quali sono le differenze?

Ora, abbiamo tra le mani tre modelli finanziari che, in una certa misura, condividono lo stesso obiettivo comune: offrirci potenti strumenti finanziari per aiutarci a rafforzare le nostre finanze e i nostri portafogli. Tuttavia, il modo in cui raggiungono questo obiettivo è molto diverso per ciascuno di questi modelli.

Conosciamo già la finanza tradizionale: modello centralizzato, fortemente dipendente dalle banche, contorto, complesso e irraggiungibile per la stragrande maggioranza della popolazione mondiale. Parliamo di un modello che vediamo già andare verso il tramonto, non solo per la sua lentezza d'innovazione, ma anche perché gli stessi che lo sostengono hanno iniziato a capire che quegli strumenti non funzionano più nel mondo di oggi.

Dai tentativi di rinnovare e migliorare quel vecchio sistema nasce un secondo modello, rappresentato dalle FinTech (Financial Technologies – Tecnologie finanziarie). Si tratta di un tentativo di creare un sistema finanziario digitale in grado di raggiungere una fetta più ampia della popolazione, che sia veloce, efficiente, economico, globale e, soprattutto, più semplice da gestire. A partire dagli anni '90 e dall'inizio del nuovo millennio, le FinTech si sono affermate come l'apice della

tecnologia finanziaria e sembravano destinate a rappresentare il prossimo passo evolutivo della finanza globale. Tuttavia, tutto ciò è ormai un ricordo con l'avvento del Bitcoin, l'arrivo di Ethereum e dei primi sistemi DeFi. La possibilità di costruire una finanza decentralizzata, più sicura, più universale e senza confini ha decisamente cambiato le regole del gioco, non solo per il suo funzionamento, ma anche per le possibilità offerte dalla DeFi.

Ecco quindi una breve lista che ci aiuterà a distinguerle:

- Una FinTech è un'entità centralizzata, basata su software e caratterizzata da ambienti controllati e soggetti a censura. Al contrario, una DeFi opera implementando il proprio software su una blockchain decentralizzata.
- I contratti di una FinTech sono contratti che seguono il modello che tutti conosciamo. Mentre nella DeFi tali contratti sono stabiliti allo stesso modo per tutti, il cuore di una DeFi e dei suoi servizi sono gli smart contract sulla blockchain che possiamo vedere e verificare liberamente.
- Le decisioni relative all'approvazione di una FinTech e della TradiFi sono subordinate a una catena burocratica, lunga o breve che sia, che comporta una perdita di tempo per noi utenti, costretti ad attendere una risposta alle nostre richieste. In una DeFi, invece, la catena si riduce a un rapporto diretto tra te e chi ti concederà il credito; a volte, la catena non

esiste nemmeno, poiché l'approvazione avviene in modo automatico se soddisfi o superi i requisiti richiesti dalla piattaforma per accedere ai suoi servizi.

- Una FinTech si avvale delle banche e dell'intera struttura della finanza tradizionale per farti pervenire le risorse che richiedi. Ciò significa che, in ogni caso, devi essere titolare di un conto bancario ed essere registrato nel sistema per poter partecipare con determinate garanzie. Significa anche che quei fondi possono essere bloccati o limitati, se lo desiderano. Nella DeFi, questo non è un problema di cui preoccuparsi: non hai bisogno di un conto bancario, ma solo di un portafoglio di criptovalute dove ricevere i tuoi fondi, e per il resto hai piena libertà.

Alla luce di questa visione, risulta piuttosto chiaro che una FinTech è un'entità finanziaria digitalizzata. Alcuni progetti FinTech ben noti a livello mondiale sono Coinbase, Revolut o PayPal, solo per citarne alcuni.

Potenziali casi d'uso della DeFi

Ma a cosa servono oggi le DeFi? Quali sono i loro possibili utilizzi?

Ebbene, innanzitutto le DeFi fungono da ponte finanziario tra il patrimonio dei possessori di criptovalute e un mondo di servizi finanziari che possono essere offerti sfruttando tale patrimonio per generare ulteriore

ricchezza. Detto questo, tra i potenziali casi d'uso della DeFi possiamo citare:

- Sistemi di prestito decentralizzati: che, di fatto, è uno dei principali casi d'uso della DeFi al giorno d'oggi. Il sistema è semplice: se una persona desidera un prestito e vuole utilizzare le proprie criptovalute come garanzia, può farlo senza problemi. Il sistema funziona in modo molto simile alle FinTech o alla finanza tradizionale. Ma la DeFi offre solitamente condizioni di interesse migliori e, in genere, i prestiti vengono approvati quasi istantaneamente. Sono ormai un ricordo le ore trascorse in banca, l'invio di documenti digitali e l'attesa di giorni per una risposta: con la DeFi basta interagire con la DApp, effettuare il deposito di garanzia richiesto e avrai a disposizione il denaro che hai richiesto in prestito, il tutto in pochi minuti.
- Mercati decentralizzati: un altro caso d'uso della DeFi è rappresentato dai mercati decentralizzati. Creazioni come gli exchange decentralizzati (DEX), i pool di investimento, i derivati finanziari, i sistemi di staking, i mercati predittivi e altro ancora sono possibili grazie alla DeFi. Sistemi di pagamento: un altro uso che si fa della DeFi è quello dei sistemi di pagamenti. Le caratteristiche di queste piattaforme consentono loro di fungere da ponte affidabile per elaborare pagamenti provenienti da diverse

blockchain, avvalendosi di un'infrastruttura esterna, decentralizzata e autonoma.

Servizi bancari e assicurativi: un altro utilizzo della DeFi è quello di offrire servizi di tipo "bancario" senza essere esattamente una banca. Ad esempio, esistono protocolli DeFi che consentono ai propri utenti di effettuare un determinato investimento e di recuperarlo dopo un certo periodo con un margine di profitto (grazie agli interessi che esso ha generato).

Ma non solo: esistono anche sistemi che consentono l'emissione di stablecoin, nonché sistemi di identificazione digitale e di assicurazioni finanziarie. A questo punto, è chiaro che il potenziale della DeFi nell'offrire servizi e soluzioni è infinito, tanto quanto la creatività delle persone che sviluppano tali sistemi.

**Cos'è lo yield farming?**

Lo yield farming, chiamato anche liquidity mining (mining di liquidità), è un modo per generare ricompense con i valori del proprio portafoglio di criptovalute.

In poche parole, significa bloccare le criptovalute in deposito e ottenere ricompense. In un certo senso, lo yield farming può essere paragonato allo staking.

Tuttavia, dietro le quinte si nasconde una grande complessità. In molti casi, funziona grazie a degli utenti chiamati fornitori di liquidità (liquidity providers o LP) ovvero coloro che aggiungono fondi ai pool di liquidità (liquidity pools).

Che cos'è un pool di liquidità?

Fondamentalmente, si tratta di uno smart contract che contiene fondi. In cambio della fornitura di liquidità alla riserva, gli LP ricevono una ricompensa. Tale ricompensa può provenire dalle commissioni (fee) generate dalla piattaforma DeFi sottostante o da qualche altra fonte. Alcuni pool di liquidità distribuiscono i propri premi in più token. Questi token di ricompensa possono poi essere depositati in altri pool di liquidità per ottenere ricompense anche lì, e così via. Ma l'idea di base è che il fornitore di liquidità depositi fondi in un pool di liquidità e, in cambio, ottenga ricompense.

Lo yield farming viene solitamente effettuato utilizzando token ERC- 20 di Ethereum, e anche i premi sono solitamente un tipo di token ERC- 20, visto che attualmente la maggior parte di questa attività si svolge nell'ecosistema Ethereum. Tuttavia, i ponti cross-chain (cross-chain bridges) consentono alle applicazioni DeFi di diventare indipendenti dalla blockchain.
Di norma, gli yield farmer spostano spesso i propri fondi tra diversi protocolli alla ricerca di rendimenti elevati. Di conseguenza, le piattaforme DeFi possono fornire anche altri incentivi economici per attirare più capitale. Proprio come accade con gli exchange centralizzati, la liquidità tende ad attrarre ulteriore liquidità.

Come funziona lo yield farming?
Lo yield farming nasce principalmente nell'ambito degli Automated Market Maker (AMM), ma nel tempo si è esteso anche ad altri protocolli DeFi come lending platform, derivati decentralizzati e sistemi di staking. Questo modello coinvolge solitamente i fornitori di liquidità (LP) e i pool di liquidità. Vediamo come funziona.
I fornitori di liquidità depositano fondi in un liquidity pool (riserva di liquidità). Tale riserva alimenta un marketplace in cui gli utenti possono concedere e contrarre prestiti, o scambiare token. L'utilizzo di tali piattaforme comporta delle commissioni (fee), che vengono pagate agli LP in base alla loro quota nella riserva di liquidità. Questo è il

principio su cui si basa il funzionamento di un AMM. Tuttavia, le implementazioni possono variare enormemente ed, essendo una tecnologia nuova, non c'è dubbio che in futuro assisteremo a nuovi approcci che miglioreranno le implementazioni attuali.

Oltre alle commissioni (fees), un altro incentivo per aggiungere fondi a una riserva di liquidità potrebbe essere la distribuzione di un nuovo token. Ad esempio, potrebbe non esserci modo di acquistare un token sul mercato libero, se non in quantità molto ridotte, ma di poterlo accumulare mediante l'apporto di liquidità a una riserva specifica. Le regole di distribuzione dipenderanno dall'implementazione specifica del protocollo.

I fondi depositati sono solitamente stablecoin (monete stabili) ancorate al dollaro statunitense, sebbene questo non sia un requisito generale. Alcune delle stablecoin più comuni utilizzate nella DeFi sono: USDT (Tether), USDC (Circle), DAI / USDS (Maker/Sky), USDe (Ethena). In crescita (ma ancora minoritarie) FDUSD, PYUSD, USD1.

Alcuni protocolli coniano token che rappresentano le valute che hai depositato nel sistema. Ad esempio, se depositi DAI su Compound, riceverai cDAI (Compound DAI). Se depositi ETH su Compound, riceverai cETH. Come puoi immaginare, qui possono esserci molti livelli di complessità. Potresti depositare il tuo cDAI su un altro protocollo, che conia un terzo token che rappresenta il

tuo cDAI – il quale, a sua volta, rappresenta il tuo DAI. E così via. Queste catene possono essere molto complesse e difficili da seguire.

Da dove arrivano i rendimenti dello yield farming?

I rendimenti dello yield farming possono derivare da diverse fonti contemporaneamente:

- commissioni di trading pagate dagli utenti che utilizzano il liquidity pool;
- interessi generati da attività di lending e borrowing;
- incentivi distribuiti dal protocollo sotto forma di token governance;
- strategie di leverage e reinvestimento automatico adottate da alcuni protocolli.

Per questo motivo gli APY (Annual Percentage Yield) possono variare notevolmente nel tempo: rendimenti molto elevati sono spesso associati a rischi maggiori o a incentivi temporanei destinati ad attrarre liquidità.

Impermanent loss

Uno dei principali rischi per i liquidity provider è l'"impermanent loss" (perdita temporanea). Questo fenomeno si verifica quando il prezzo dei token depositati in un liquidity pool cambia significativamente rispetto al momento del deposito.

In alcuni casi, il valore finale dei token detenuti nel pool può risultare inferiore rispetto a quello che si sarebbe ottenuto semplicemente mantenendo gli asset nel wallet (“holding”). Le commissioni generate dal pool possono compensare questa perdita, ma non sempre accade.

Smart contract risk

Lo yield farming dipende da smart contract, cioè programmi automatici eseguiti sulla blockchain. Se uno smart contract contiene bug, vulnerabilità o viene compromesso da un attacco hacker, i fondi depositati potrebbero essere persi parzialmente o totalmente.

Per questo motivo molti utenti preferiscono protocolli consolidati e sottoposti ad audit di sicurezza indipendenti.

Liquidità e sostenibilità dei rendimenti

Non tutti i rendimenti DeFi sono sostenibili nel lungo periodo.
Alcuni protocolli offrono APY molto elevati grazie all’emissione continua di nuovi token. Se la domanda per tali token diminuisce, il loro valore può crollare rapidamente, riducendo o annullando i guadagni ottenuti.

Per questa ragione è importante distinguere tra:

- rendimento generato da attività economiche reali (fee, interessi, utilizzo del protocollo)
- rendimento derivante principalmente da emissione inflazionistica di nuovi token.

**Come funziona un CEX (exchange centralizzato):**
Su un exchange centralizzato abituale, devi depositare il tuo denaro sia esso fiat (tramite bonifico bancario o carta di credito) o in criptovalute. Quando lo fai, ne cedi il controllo. Non dal punto di vista dell'usabilità (dato che puoi fare trading con esse o prelevarle) ma dal punto di vista tecnico: infatti, non puoi spenderle sulla blockchain. Non essendo tu in possesso delle chiavi private dei fondi, quando effettui un prelievo chiedi effettivamente all'exchange di firmare una transazione a tuo nome. Quando fai trading, le transazioni non avvengono on-chain: l'exchange assegna invece i saldi agli utenti nel proprio database. Il "workflow" generale (flusso di lavoro) è incredibilmente snello, il trading non è ostacolato dalla bassa velocità delle blockchain e tutto avviene all'interno del sistema di un unico operatore. È più facile acquistare e vendere criptovalute, e hai a disposizione un maggior numero di strumenti.
Tutto ciò, però, si ottiene a scapito dell'indipendenza e dovrai affidare i tuoi soldi, esponendoti così a determinati rischi di controparte. Cosa succede se il team sparisce con i BTC che hai guadagnato con tanta fatica? Cosa succede se un hacker mette fuori uso il sistema e prosciuga i fondi? Per molti utenti, questo rappresenta un livello di rischio accettabile. Si limiteranno semplicemente a utilizzare exchange affidabili, con una solida storia, un'assicurazione e misure di sicurezza che riducano le violazioni dei dati.

**Cos'è un exchange decentralizzato (DEX)?**

In teoria, qualsiasi scambio peer-to-peer può costituire un'operazione decentralizzata. Tuttavia, in questo articolo ci interessano principalmente le piattaforme che emulano le funzioni degli exchange centralizzati. La differenza fondamentale sta nel fatto che il "backend" risiede su una blockchain. Nessuno detiene la custodia dei tuoi fondi (solo tu e il tuo wallet) e non dovrai fidarti dell'exchange nella stessa misura in cui lo fai con quelli centralizzati.

Come funziona un exchange decentralizzato:

I DEX sono simili alle loro controparti centralizzate sotto certi aspetti, ma significativamente diversi sotto altri. Va sottolineato, innanzitutto, che gli utenti hanno a disposizione diversi tipi di exchange decentralizzati. Il denominatore comune a tutti è che gli ordini vengono eseguiti on-chain (tramite smart contract) e che gli utenti non cedono in alcun momento la custodia dei propri fondi.

Sebbene siano stati realizzati progetti relativi a DEX di tipo "cross- chain", quelli più diffusi ruotano attorno ad asset di una singola blockchain (come ad esempio Ethereum o Binance Chain).

Ordinary on chain

In alcune piattaforme di scambio decentralizzate, tutte le operazioni avvengono on-chain (parleremo tra poco degli approcci ibridi). Ogni ordine (così come ogni

modifica o annullamento) viene registrato sulla blockchain.

Questo è probabilmente l'approccio più trasparente, dato che non è necessario affidarsi a una terza parte per la trasmissione degli ordini e non c'è modo di occultarli. Purtroppo, è anche il meno pratico. Chiedendo a ogni nodo della rete di registrare l'ordine in modo permanente, dovrai pagare una commissione e aspettare che un miner aggiunga il tuo messaggio alla blockchain, il che può rendere l'esperienza piuttosto macchinosa.

Alcuni indicano il front running come un difetto di questo modello. Il front running si verifica nei mercati quando un "insider" (un soggetto in possesso di informazioni privilegiate) viene a conoscenza dell'esistenza di una transazione in sospeso e utilizza tali informazioni per effettuare un'operazione prima che la transazione venga elaborata. Il "front runner", quindi, trae vantaggio da informazioni non note al pubblico. Di norma, si tratta di un comportamento illegale. Ovviamente, se tutto viene registrato in un registro globale, non c'è modo di agire in anticipo nel senso tradizionale del termine. Detto questo, è possibile mettere in atto un tipo diverso di attacco: uno in cui un miner vede l'ordine prima che venga confermato e si assicura che il proprio ordine venga aggiunto per primo alla blockchain. Esempi di modelli di registri degli ordini on-chain includono i DEX Stellar e Bitshares.

## Registri degli ordini off-chain

I registri degli ordini DEX off-chain sono ancora decentralizzati sotto certi aspetti, ma è vero che sono più centralizzati rispetto al punto precedente. Invece di pubblicare tutti gli ordini sulla blockchain, questi vengono ospitati altrove. Dove? Dipende. A carico del libro degli ordini potrebbe esserci un'entità centralizzata. La blockchain di Ethereum ne è un ottimo esempio. Anziché funzionare come un singolo DEX, fornisce un framework che consente a soggetti noti come «relay» di gestire i registri degli ordini off-chain. Sfruttando gli smart contract 0x e alcuni altri strumenti, i relay possono attingere a un pool di liquidità combinato e trasmettere gli ordini tra gli utenti. L'operazione viene eseguita on-chain solo una volta che le parti hanno trovato un accordo. Questi approcci sono superiori dal punto di vista dell'usabilità rispetto a rispetto a quelli basati su registri degli ordini on-chain e non presentano le stesse limitazioni in termini di velocità, poiché non fanno un uso così intensivo della blockchain. Tuttavia, le transazioni devono essere risolte sulla blockchain, quindi il modello del registro degli ordini off-chain rimane inferiore in termini di velocità alle borse centralizzate.

## AUTOMATED MARKET MAKERS (AMM)

Stufo di leggere il termine "order book"? Ottimo, perché il modello Automated Market Maker (AMM) elimina completamente il concetto. Non richiede maker o taker,

solo utenti, teoria dei giochi e un po' di magia nera ben formulata.
I dettagli degli AMM dipendono dall'implementazione; in generale, combinano una serie di contratti intelligenti e offrono incentivi intelligenti per garantire la partecipazione degli utenti.
I DEX basati su AMM attualmente disponibili tendono ad essere relativamente facili da usare e si integrano con i portafogli come MetaMask o Trust Wallet. Tuttavia, come per altre forme di DEX, è necessario effettuare una transazione on-chain per regolare le operazioni. I progetti che operano in questo ambito includono la rete Uniswap.
VANTAGGI DEI DEX

- Senza KYC
  Il rispetto delle norme KYC/AML (Know Your Customer e Anti-Money Laundering) è la prassi standard per molte piattaforme di scambio. Per motivi normativi, gli utenti devono spesso presentare un documento di identità, un selfie e un documento che attesti il proprio indirizzo. Per alcuni si tratta di un problema di privacy, per altri di accessibilità. Cosa succede se non hai documenti validi, di un formato differente o scaduti? Cosa succede se le informazioni vengono divulgate in qualche modo? Dato che i DEX non richiedono autorizzazioni, nessuno verifica la tua identità. Tutto ciò che ti serve è un portafoglio di criptovalute.

Tuttavia, esistono alcuni requisiti legali quando i DEX sono gestiti in parte da un'autorità centrale. In alcuni casi, se il registro degli ordini è centralizzato, l'host deve continuare ad adempiere ai propri obblighi. Nessun rischio di controparte. Il principale vantaggio degli exchange di criptovalute decentralizzati è che non trattengono i fondi dei clienti. Pertanto, anche incidenti catastrofici come l'hacking di Mt.Gox o il fallimento di FTX non metteranno a rischio i fondi degli utenti, né esporranno informazioni personali riservate.

- Token non quotati

  I token che non sono quotati su exchange centralizzati possono comunque essere scambiati liberamente sui DEX, purché vi siano domanda e offerta.

SVANTAGGI DEI DEX

- Usabilità

  A dire il vero, i DEX non sono così facili da usare come gli exchange tradizionali. Le piattaforme centralizzate offrono operazioni in tempo reale che non subiscono ritardi. Per i neofiti che non hanno familiarità con i portafogli di criptovalute non custoditi, i CEX offrono un'esperienza più intuitiva. Se dimentichi la password, puoi semplicemente reimpostarla. Nei DEX, se perdi la tua frase seed, i

tuoi fondi andranno irrimediabilmente persi nel cyberspazio.

- Volumi di trading e liquidità
  Il volume scambiato sui CEX supera ancora quello dei DEX.
  Forse l'aspetto più importante è che i CEX tendono anche ad avere una maggiore liquidità, ovvero la facilità con cui è possibile acquistare o vendere attività a un prezzo ragionevole. In un mercato altamente liquido, lo scarto tra domanda e offerta è minimo, il che implica un'elevata concorrenza tra acquirenti e venditori. In un mercato illiquido, sarà più difficile trovare qualcuno disposto a negoziare l'attività a un prezzo ragionevole. I DEX rimangono ancora relativamente di nicchia, quindi può non esserci sempre domanda o offerta per le criptovalute che desideri scambiare. Inoltre, potresti non riuscire a trovare le coppie di trading che desideri utilizzare, o è possibile che gli asset non vengano scambiati a un prezzo equo.
- Commissioni
  Sui DEX, le commissioni possono essere più alte, soprattutto quando la rete è congestionata o se si utilizza un order book on-chain.
  In conclusione
  Nel corso degli anni sono emersi molti exchange decentralizzati, ognuno dei quali si basa sui tentativi

precedenti di ottimizzare l'esperienza dell'utente e creare piattaforme di trading più efficienti. In definitiva, l'idea sembra essere perfettamente in linea con lo spirito dell'autosovranità: proprio come nel caso delle criptovalute, gli utenti non devono affidarsi a terzi. Con il boom della DeFi, gli exchange decentralizzati basati su Ethereum o su Solana hanno registrato un enorme aumento di utilizzo. Se questo slancio continuerà, è probabile che assisteremo a una maggiore innovazione tecnologica in tutto il settore.

## Che cos'è una DAO?

L'acronimo DAO deriva dall'inglese Decentralized Autonomous Organization, ovvero Organizzazione Autonoma Decentralizzata. Si tratta di un tipo di organizzazione controllata interamente da algoritmi informatici.

Questi algoritmi sono noti come smart contract e stabiliscono le regole della cooperazione tra le parti coinvolte nella DAO.

Le DAO (Decentralized Autonomous Organizations) operano tramite smart contract su blockchain e presentano una struttura decentralizzata che rende complessa la loro qualificazione giuridica secondo i modelli tradizionali. In molti ordinamenti manca ancora una normativa specifica e uniforme dedicata alle DAO; tuttavia, esse possono comunque essere soggette a leggi esistenti in materia societaria, finanziaria, fiscale, antiriciclaggio e di responsabilità civile o penale, a seconda delle modalità operative e del grado di decentralizzazione effettivo.

Gli smart contract che le rigono possono essere tanto semplici o molto complessi, secondo come sono stati programmati. Una volta pubblicati sulla blockchain, questi rimarranno trasparenti e immutabili. Ciò consente a chiunque di verificarne il funzionamento e le regole al loro interno, con la certezza che non potranno essere modificati in futuro. Trattandosi di frammenti di codice informatico, ovvero di linguaggio puramente digitale,

aprono la strada a un nuovo livello di cooperazione, consentendo la gestione del processo decisionale tra esseri umani, macchine e altri smart contract (che a loro volta possono essere gestiti da altri esseri umani, macchine e smart contract). È per questo che le DAO rappresentano una potente innovazione tecnologica. Una tecnologia che mira a ridefinire le modalità di collaborazione tra le diverse parti. Ciò è possibile grazie alla creazione di organizzazioni autonome, autogestite, trasparenti e più efficienti.

Come funziona una DAO?

Le DAO si basano su una serie di meccanismi che ne garantiscono il funzionamento in ogni momento.

Il primo di questi meccanismi è legato alla capacità di programmare azioni e farle eseguire secondo determinati parametri. In questo modo, la DAO acquisisce la capacità di eseguire azioni in modo autonomo; questa programmazione corrisponde all'insieme delle regole che disciplinano la DAO e il modo più comune per programmare tali azioni è tramite gli smart contract.

Il secondo meccanismo è un protocollo di consenso. Il suo scopo è garantire che le decisioni prese all'interno della DAO siano adottate per consenso tra le sue parti. Nessun fattore esterno alla rete, né chi non vi partecipa direttamente, può alterare o influenzare tali decisioni.

Inoltre, le DAO dispongono di un terzo meccanismo che dipende dell'emissione di un token o di un mezzo di scambio. Lo scopo di questo meccanismo è garantire un mezzo che sostenga economicamente la DAO. Oltre a consentire agli utenti di acquisire potere di voto, funge anche da meccanismo di scambio e di ricompensa economica.

Infine, dispongono di un quarto meccanismo il cui scopo è quello di registrare tutto ciò che accade nella DAO. Questo compito spetta alla blockchain, dove tutte le informazioni vengono archiviate per essere accessibili pubblicamente e garantirne la sicurezza. L'unione di questi quattro elementi è ciò che consente il funzionamento di una DAO in ogni momento.

Esempio di base di una DAO

Esistono molti scenari che illustrano come potrebbe essere utilizzata una DAO. Simuleremo uno scenario semplice: un'associazione di vicini.

In un'associazione di vicini tradizionale, ogni famiglia versa una quota annuale, che viene utilizzata per far fronte alle spese relative a guasti e lavori di miglioramento nel complesso residenziale. Ebbene, utilizzando uno smart contract tutti i residenti potrebbero depositare i fondi (sotto forma di ether o anche di qualche stablecoin basato su valuta fiat), che non sarebbero nelle mani di una sola persona, né di due, ma sarebbero nelle mani di tutti e di nessuno allo stesso tempo. Lo smart contract li terrebbe bloccati in attesa di

una decisione democratica, rendendoli visibili in modo trasparente, ma senza che nessuno possa usarli a proprio piacimento in modo sleale. Per ogni nuova spesa (ad esempio una riparazione o un intervento di miglioramento) verrebbe generata una richiesta, a cui verrebbero successivamente associati i diversi preventivi inviati dai fornitori. Successivamente, i residenti potrebbero decidere in modo democratico, entro un determinato termine, quale preventivo preferiscono, sbloccando i fondi solo per il preventivo che ha ottenuto il maggior numero di voti, secondo regole note a tutti.
Immagina un'auto a guida autonoma, acquistata da 10 persone sparpagliate per il mondo, che funge da taxi, sbloccandosi a fronte di un pagamento e distribuendo i profitti a ciascun socio, in modo diretto e senza banche.
O, andando oltre, riesci a immaginare un paese gestito da una DAO? I politici candidati presenterebero ogni 4 anni uno smart contract, affinché in seguito la società decida quale di questi  vuole che la governi. Come puoi vedere, i casi d'uso possono essere molti, e i limiti sono ancora da scoprire. Come per ogni innovazione, solo lacreatività dirà dove sarà in grado di portarci questo nuovo strumentoofferto dalla tecnologia blockchain.

## Origini delle DAO

Un errore comune è pensare che le DAO siano nate con Ethereum. Sebbene sia vero che Ethereum abbia fatto conoscere questo concetto a gran parte del pubblico del

settore blockchain, la nascita delle DAO risale a molto tempo prima.
Questo concetto innovativo fu inizialmente proposto da Werner Dilger, un rinomato professore tedesco di informatica. Fu proprio Dilger a sviluppare nel 1997 il suo lavoro intitolato «Organizzazione autonoma decentralizzata della casa intelligente secondo il principio del sistema immunitario». In esso, Dilger definiva le basi delle DAO come sistema autosufficiente e autonomo, un lavoro senza dubbio in anticipo sui tempi.
Tuttavia, in quel momento, la sua idea risultava impraticabile. La sfida tecnica di creare una DAO non poté essere superata fino all'arrivo della blockchain. Fu allora che il concetto di DAO tornò alla ribalta. Il 7 settembre 2013, Daniel Larimer, fondatore di BitShares e Steem, ne ha parlato sul sito "Let's Talk Bitcoin!". All'epoca, Daniel ne parlava come di "Società Autonome Decentralizzate" (DAC), un altro dei modi comuni per chiamare le DAO. Fu solo nel 2015 che Vitalik Buterin rilanciò il concetto grazie al lancio di Ethereum, che consentiva di creare codici trasparenti e immutabili avanzati (turing-completi), il che facilitava notevolmente la creazione di DAO e l'interazione con esse.

Le DAO, alcuni esempi reali
A questo punto, ti starai sicuramente chiedendo: esistono davvero delle DAO nella realtà? La risposta è

sì. Certamente una DAO non è un'organizzazione qualsiasi e la complessità necessaria per realizzarle è enorme. Tuttavia, ciò non ha impedito che diventassero una realtà. Tra i primi esempi storici di DAO vi sono “The DAO”, “Dash DAO Governance” e “DigixDAO”. Questi progetti hanno contribuito allo sviluppo del modello pur con esiti differenti nel tempo.

La DAO più famosa: The DAO

Senza dubbio una delle DAO più note è stata “The DAO”. Il progetto, creato nel 2016 da Simon Jentzsch e Christoph Jentzsch, fu lanciato con l’obiettivo di costruire una delle più grandi organizzazioni autonome decentralizzate mai realizzate, sfruttando le potenzialità di Ethereum.

“The DAO” è ricordata non solo per l’enorme quantità di capitale raccolto, ma anche per le conseguenze che seguirono al suo fallimento. Il progetto riuscì infatti a raccogliere circa 150 milioni di dollari in Ether, diventando una delle più grandi campagne di crowdfunding dell’epoca.

Tuttavia, poco dopo il lancio venne scoperta una grave vulnerabilità nello smart contract di “The DAO” e un hacker riuscì a sfruttare tale vulnerabilità sottraendo circa 3,6 milioni di ETH, (equivalenti a circa 50 milioni di dollari del tempo).

L’evento ebbe un impatto enorme sull’intero ecosistema Ethereum e portò la comunità a eseguire un hard fork

della blockchain. Da questa divisione nacquero due reti separate:

- Ethereum, che annullò gli effetti dell'attacco;
- Ethereum Classic, che mantenne la blockchain originale immutata.

Il caso "The DAO" dimostrò sia il potenziale delle DAO sia i rischi legati alla sicurezza degli smart contract. In particolare, evidenziò come errori nel codice possano avere conseguenze economiche enormi in sistemi progettati per essere decentralizzati e immutabili.

## Che cos'è una sidechain?

Una sidechain è una blockchain alternativa collegata ad una già esistente, ed è utilizzata per migliorarne le prestazioni e interagire con essa.

Pur presentando una programmazione e caratteristiche completamente diverse, la sidechain e con la blockchain a cui si collega. In questo modo, entrambe le blockchain possono comunicare e integrare le rispettive funzionalità.

Un esempio potrebbe essere il seguente: immaginiamo che uno sviluppatore voglia creare una DApp e implementarla su Bitcoin. Al momento, farlo direttamente su Bitcoin è estremamente complesso. Tuttavia, è possibile sviluppare una sidechain che aggiunga tale funzionalità a Bitcoin in modo più semplice. Questa sidechain avrebbe la capacità di implementare le DApp e interagire in modo bidirezionale con la catena di Bitcoin. Il risultato è che sarebbe possibile sviluppare DApp che sfruttino il potenziale di Bitcoin (il suo mining e altre proprietà) grazie all'uso di questa sidechain.

Come funzionano?

Il funzionamento di una sidechain non è semplice. Dal punto di vista tecnico, si tratta di una sfida complessa che ha richiesto anni di sviluppo e sperimentazione. In linea generale, una sidechain funziona tramite un meccanismo di trasferimento bidirezionale degli asset (“two-way peg”).

Il processo avviene generalmente nel seguente modo:

1. l'utente invia criptovalute a un indirizzo o smart contract sulla blockchain principale;
2. tali fondi vengono bloccati sulla mainchain;
3. la sidechain verifica il blocco dei fondi tramite specifici meccanismi di validazione;
4. una quantità equivalente di token viene emessa sulla sidechain;
5. questi token rappresentano gli asset originali bloccati sulla blockchain principale e possono essere utilizzati all'interno della sidechain.

A questo punto gli utenti possono trasferire, scambiare o utilizzare tali asset sfruttando le funzionalità offerte dalla sidechain.

Le sidechain possono infatti offrire caratteristiche differenti rispetto alla blockchain principale, come:

- maggiore velocità di elaborazione delle transazioni;
- commissioni più basse;
- supporto a smart contract avanzati;
- linguaggi di scripting più complessi o Turing-completi;
- maggiore scalabilità.

Quando l'utente desidera tornare alla blockchain principale, il processo avviene in senso inverso: i token

presenti sulla sidechain vengono distrutti o bloccati e gli asset originali vengono sbloccati sulla mainchain.

Le possibilità offerte dalle sidechain sono molto ampie e consentono di sperimentare nuove funzionalità senza modificare direttamente la blockchain principale.

Esempi di progetti basati su sidechain:

Liquid Network

È un progetto sviluppato da Blockstream, una delle aziende più note dell'ecosistema Bitcoin. Liquid Network è una sidechain progettata per interoperare con Bitcoin e consentire trasferimenti più rapidi ed efficienti di asset digitali, soprattutto tra exchange, aziende e operatori professionali. La rete utilizza un asset chiamato L-BTC (Liquid Bitcoin), ancorato 1:1 a Bitcoin. Gli utenti possono bloccare BTC sulla rete principale e ricevere la corrispondente quantità di L-BTC sulla sidechain.

Rispetto alla rete Bitcoin principale Liquid offre tempi di conferma più rapidi, maggiore riservatezza delle transazioni, emissione di asset tokenizzati e funzionalità avanzate.

Rootstock

Rootstock, inizialmente conosciuta come RSK, è una sidechain progettata per introdurre smart contract compatibili con Ethereum nell'ecosistema Bitcoin.

L’obiettivo principale del progetto è ampliare le funzionalità di Bitcoin permettendo lo sviluppo di:

- smart contract avanzati
- applicazioni decentralizzate (DApp)
- servizi DeFi compatibili con Bitcoin

Rootstock utilizza il merged mining con Bitcoin, consentendo ai miner di contribuire contemporaneamente alla sicurezza di entrambe le reti.

Lisk

Lisk è una piattaforma blockchain orientata allo sviluppo di applicazioni decentralizzate tramite JavaScript. Storicamente il progetto è stato associato al concetto di sidechain, poiché consentiva agli sviluppatori di creare blockchain personalizzate collegate all’ecosistema principale di Lisk.

La piattaforma utilizza un meccanismo di consenso Delegated Proof of Stake (DPoS), progettato per offrire maggiore scalabilità, velocità di elaborazione delle transazioni e flessibilità nello sviluppo delle applicazioni.

Oggi il concetto di sidechain si è evoluto e molti progetti moderni utilizzano architetture differenti come layer 2, rollup o app-chain modulari. Per questo motivo Lisk viene considerata più una piattaforma blockchain applicativa che un classico esempio moderno di sidechain.

Le sidechain sono sicure?

La sicurezza delle sidechain dipende molto da come sono implementate. Alcune di esse utilizzano lo stesso protocollo di consenso e le stesse misure di sicurezza della blockchain della quale ampliano la funzionalità. In altri casi, implementano un protocollo di consenso e misure di sicurezza proprie. In ogni caso, la sicurezza delle sidechain è garantita da questi elementi.

Perché le sidechain sono importanti?

Le sidechain rivestono una grande importanza poiché consentono di ottimizzare in modo unico il funzionamento delle blockchain. Grazie alle sidechain sarebbe possibile inviare BTC a un' altra sidechain, la quale converte tali BTC in un determinato token che successivamente passa alla blockchain di Ethereum. Inoltre, le sidechain possono aumentare la sicurezza (evitando i problemi che si sono verificati in altri progetti di altcoin), aggiungere nuove funzionalità uniche a una blockchain senza la necessità di alterarne il protocollo, risolvere la mancanza di liquidità in bitcoin, ridurne la volatilità e la frammentazione del mercato ed evitare le frodi.

In poche parole, si tratta di uno strumento perfetto per sviluppare nuove tecnologie che possano essere adattate a quelle già esistenti. Il tutto senza dover apportare grandi cambiamenti e con la possibilità di continuare ad ampliarne il potenziale.

Allo stesso tempo, dato che le sidechain rimangono blockchain indipendenti, è possibile sperimentarvi ogni tipo di funzionalità senza alcun rischio. Ciò include nuovi modelli di transazione, modelli di fiducia o economici, l'emissione di asset semantici o nuove funzionalità crittografiche.

## Cos'è la Lightning Network?

Lightning Network è un protocollo di secondo livello sviluppato per migliorare la scalabilità di Bitcoin. L'idea alla base di questa tecnologia è semplice: permettere agli utenti di effettuare pagamenti quasi istantanei e con commissioni molto basse senza dover registrare ogni singola transazione direttamente sulla blockchain principale.

Il progetto nasce dal lavoro di Joseph Poon e Thaddeus Dryja ed è oggi sviluppato da aziende e gruppi di ricerca come Blockstream, Lightning Labs e ACINQ.

Per comprendere perché la Lightning Network sia stata considerata così importante, bisogna partire da un limite storico di Bitcoin: la scalabilità. La rete Bitcoin è estremamente sicura e decentralizzata, ma queste caratteristiche hanno un costo in termini di prestazioni. La blockchain può elaborare soltanto un numero limitato di transazioni al secondo, mediamente circa 7, un valore molto basso rispetto ai circuiti di pagamento tradizionali. Quando l'utilizzo della rete aumenta, il mempool — cioè l'area in cui vengono temporaneamente conservate le transazioni in attesa di conferma — tende a congestionarsi.

In queste situazioni gli utenti iniziano a competere tra loro offrendo commissioni più alte per ottenere priorità dai

miner e, di conseguenza, le fee aumentano e i tempi di conferma possono diventare più lunghi. Questo problema rende poco pratici i micropagamenti. In alcuni momenti di forte congestione, inviare pochi euro in bitcoin potrebbe comportare commissioni pari o addirittura superiori all'importo trasferito.

È proprio per risolvere questo limite che è nata la Lightning Network, che funziona creando canali di pagamento tra utenti. Due persone possono aprire un canale effettuando una transazione sulla blockchain Bitcoin e scambiarsi fondi un numero praticamente illimitato di volte senza dover registrare ogni movimento sulla blockchain principale. Le transazioni avvengono infatti "off-chain", cioè al di fuori della rete Bitcoin principale. Solo quando il canale viene chiuso il saldo finale viene registrato sulla blockchain. In questo modo la rete Bitcoin deve gestire molte meno transazioni, mentre gli utenti ottengono pagamenti quasi istantanei e commissioni estremamente ridotte. Un aspetto molto interessante è che gli utenti non devono necessariamente aprire un canale diretto con ogni persona, perché Lightning Network crea una rete interconnessa di nodi in grado di instradare i pagamenti tra diversi partecipanti, rendendo possibile inviare fondi anche a utenti con cui non esiste un collegamento diretto. La Lightning Network rappresenta quindi una delle principali soluzioni di scaling per Bitcoin. Pur non sostituendo la blockchain

principale, ne amplia le capacità, rendendo possibile un utilizzo più efficiente della criptovaluta soprattutto nei pagamenti rapidi e nei micropagamenti quotidiani.

Nonostante il suo enorme potenziale, la tecnologia presenta ancora alcune sfide, tra cui la gestione della liquidità nei canali, la complessità tecnica dell'infrastruttura e un'esperienza utente non sempre semplice per chi è alle prime armi. Tuttavia, negli ultimi anni l'ecosistema Lightning è cresciuto notevolmente ed è oggi considerato uno degli sviluppi più importanti dell'universo Bitcoin.

In Bitcoin e Litecoin la proprietà di non malleabilità delle transazioni sono state introdotte grazie all'arrivo di SegWit (Segregated Witness).
Con questo soft fork, Bitcoin ha risolto il problema e ha posto le prime pietre miliari per una nuova modalità di espansione delle proprie capacità. È così che è iniziato lo sviluppo di Lightning Network e dei suoi cosiddetti canali di pagamento. Questi canali di pagamento sono la pietra angolare del funzionamento di Lightning Network e la chiave per consentire una scalabilità senza precedenti in Bitcoin.
Cosa sono i canali di pagamento?
I canali di pagamento (o payment channels) sono alla base della Lightning Network. Un canale di pagamento è in realtà una transazione multifirma sulla blockchain,

nella quale almeno una delle parti invia fondi. In tale canale, ogni persona possiede una chiave privata e ogni transazione futura potrà essere effettuata solo se le chiavi di entrambe le parti appongono la propria firma. Ciò costituisce un mezzo di consenso che la transazione è stata approvata per l'esecuzione da entrambe le parti. I canali di pagamento possono rimanere aperti per un determinato periodo di tempo. Di solito si tratta di circa 10 minuti (o del tempo necessario per minare il blocco successivo nella blockchain).

Spiegazione passo dopo passo del funzionamento della Lightning Network:

Innanzitutto, all'interno di Lightning avremo due partecipanti che creeranno una transazione iniziale sulla blockchain del valore di 20 $. Di questi 20 $, 10 $ saranno di Carmen e 10 $ di Aitor. Questa ripartizione potrebbe variare all'interno del canale, per cui Carmen potrebbe avere 15 $ e Aitor 5$ al termine di tutti gli scambi. Ciò che fa Lightning è sfruttare la tecnologia alla base dei canali di pagamento e creare una rete che li integri, utilizzando gli smart contract per garantire che la rete possa funzionare in modo decentralizzato. In tal senso, avremmo la seguente suddivisione del processo:

1. Carmen apre un canale di pagamento con Aitor, il quale a sua volta ha un canale con Laura, che a sua volta ha un canale aperto con David.
2. Al momento abbiamo quattro parti coinvolte in diversi canali di pagamento.

3. Carmen vuole scambiare asset con David, quindi potrà inviare fondi tramite Aitor e Laura affinché arrivino infine a David, il destinatario.
4. Data la natura della Lightning Network, Carmen non ha necessità di fidarsi di Aitor e Laura all'interno del processo, poiché si utilizza la crittografia per garantire che i fondi che David riceverà siano esattamente gli stessi che ha inviato. In caso contrario, i fondi verranno automaticamente restituiti a Carmen.

A questo punto ci rimangono una serie di domande molto importanti:

Come è possibile fidarsi del passaggio 3?

In realtà, Aitor e Laura fungono da nodi all'interno della rete che possiamo paragonare ai miner della rete Bitcoin. Questo perché elaborano in modo decentralizzato tutte le transazioni senza avere il controllo dei fondi che aiutano a trasferire. Per questo motivo, in nessun momento Aitor e Laura potrebbero sottrarre i fondi di Carmen, poiché riceveranno i fondi da inviare solo se è già stata effettuata la transazione di uscita verso il destinatario finale, che in questo caso è David.

Cosa succede con la disponibilità?

Se Aitor si disconnette, i fondi del canale non rimangono intrappolati in esso a tempo indeterminato. Infatti, all’interno del meccanismo degli smart contract della Lightning Network, gli utenti possono chiudere

unilateralmente i canali. In questo modo, se Aitor scomparisse, Carmen potrebbe recuperare i propri soldi grazie all'attributo temporale aggiunto nel contratto. Quando un canale viene chiuso e viene completata la transazione, i saldi finali di ciascuna parte saranno registrati sulla blockchain entro 10 minuti (o nel tempo necessario per la creazione del prossimo blocco della rete).

Come si combatte la frode?

Immaginiamo che Carmen invii fondi dal suo conto a quello di David all'indirizzo multifirma Lightning Network, ma che non rispetti le regole (per esempio, cerca di inviare una transazione obsoleta sulla blockchain per chiudere il canale nello stato in cui si trovava prima di inviare la transazione a David).

Il software stesso, alla ricerca di questo tipo di azioni, farà sì che Carmen perda tutti i fondi inviati a David. Ciò costituisce una sanzione per tale azione, pertanto chiunque tenti di trasmettere una transazione obsoleta e non valida verrà penalizzato. Grazie a questa rete di canali peer-to-peer è possibile individuare uno schema all'interno della rete, attraverso il quale trasmettere transazioni fuori dalla blockchain senza limiti. Il tutto senza perdere la certezza che, successivamente e dopo la chiusura del canale, queste transazioni saranno registrate nella blockchain di Bitcoin.

## Vantaggi e svantaggi di Lightning Network

### Vantaggi

- Lightning offre una delle più potenti opzioni per migliorare la scalabilità di Bitcoin. Lightning può infatti portare Bitcoin a livelli vicini al milione di transazioni al secondo, molto più di quelle gestite da sistemi di pagamento come VISA e MasterCard.
- Offre elevati livelli di sicurezza e anonimato. Questo è dovutoal fatto che le transazioni avvengono off-chain, rendendo i pagamenti praticamente impossibili da tracciare.
- Lightning è compatibile con altri progetti di criptovalute oltre a Bitcoin. Ad esempio, è possibile utilizzare Lightning con Litecoin.
- È in grado di ridurre enormemente il volume di transazioni all'interno della rete Bitcoin. Ciò renderebbe la rete molto più efficiente.
- Le transazioni che utilizzano Lightning Network vengono effettuate in modo quasi istantaneo.
- Consente di effettuare micropagamenti e ne permette persino l'automazione.
- Consente di effettuare scambi atomici cross- chain. Ciò consente a due blockchain che utilizzano la stessa funzione hash, di scambiarsi token senza bisogno di un intermediario come un exchange.

Svantaggi

- Uno dei principali svantaggi di Lightning è che i pagamenti possono essere effettuati solo a utenti connessi a un canale di pagamento. Ciò significa che l'utente deve essere attivo e connesso al canale. A differenza di ciò, le transazioni con le criptovalute tradizionali non presentano questa limitazione.
- La Lightning Network non è una tecnologia sperimentale in senso stretto, ma un protocollo in continua evoluzione. È già utilizzata in contesti reali, anche se molti sviluppatori e provider consigliano ancora cautela nell'utilizzo per transazioni di valore molto elevato, soprattutto a causa della complessità operativa e della gestione dei canali.
- Uno dei principali limiti del sistema riguarda la liquidità. Ogni canale di pagamento ha infatti una capacità massima pari ai fondi che vengono bloccati sulla blockchain principale al momento della sua apertura. Questo significa che i pagamenti all'interno del canale non possono superare tale limite. Inoltre, la distribuzione della liquidità nei canali può creare inefficienze: un utente potrebbe avere fondi "bloccati" da un lato del canale e non poterli utilizzare liberamente per inviare o ricevere pagamenti in tutte le direzioni. Questo porta spesso gli utenti più avanzati a gestire attentamente la distribuzione del capitale tra canali Lightning e fondi on-chain, per mantenere una buona operatività.