BRIGHTSIDE CAPITAL

BABILONIA

"Whereas most technologies tend to automate workers on the periphery doing menial tasks, blockchains automate away the center.

Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly."

Vitalik Buterin, Ethereum Co-Founder

Nell'ultimo scritto dedicato al mondo crypto abbiamo provato a fare un po' di chiarezza sull'attività di Bitcoin Mining: dove avviene, come avviene e quali sono i temi più rilevanti che dividono l'opinione pubblica, sia in termini di consumo energetico che di effettiva utilità sociale della valuta digitale in senso lato.

Prima di approfondire altri aspetti più specifici dell'ecosistema digitale riteniamo però utile tentare di descrivere qualche concetto di base inerente alla blockchain. Lo scopo è di contribuire alla costruzione di un vocabolario specifico su questo tema, soffermandoci su ciò che pensiamo essere più importante per comprendere le differenze tra le varie applicazioni e progetti che si stanno sviluppando nello spazio.

Innanzitutto, cos'è una **blockchain**? Possiamo definire la blockchain come un database (anche definito *ledger*) pubblico e digitale all'interno del quale gli utenti si scambiano "blocchi" di dati. Lo scambio di informazioni avviene in maniera sicura grazie all'utilizzo di tecniche di crittografia ed il registro all'interno del quale sono archiviate è distribuito, ovvero ogni utente ne ha una copia, e quest'ultimo si aggiorna ogniqualvolta vengono inseriti nuovi dati. La blockchain infatti fa parte della macrocategoria delle *"Disitributed Ledger Technologies"*, ovvero tutti quei sistemi basati su un registro distribuito a cui gli utenti possono accedere e che possono modificare solo se raggiungono un **consenso** (tema che approfondiremo più avanti nell'articolo).

Tre sono le caratteristiche principali di una blockchain:

1) **Immutabilità**, ovvero la capacità di rimanere un elenco di transazioni permanente, inalterabile ed indelebile. La blockchain è infatti definita "*append only*", ovvero permette solo la possibilità di aggiungere dati e non di cancellarli.

2) **Decentralizzazione**, in quanto il controllo ed il potere decisionale sono assegnati ad un network distribuito di utenti, e non ad un'autorità centrale.

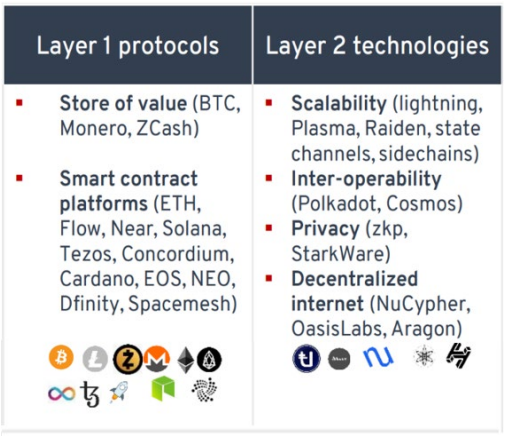
3) **Trasparenza**, che deriva dal fatto che le blockchain sono software *open-source* che consentono a tutti gli utenti, in maniera *permissionless*, di consultare l'intero storico di dati e transazioni.

Le tre caratteristiche sopra, unite all'uso della crittografia, rendono i sistemi basati sulla blockchain estremamente sicuri e totalmente verificabili.

Layer 1 vs. Layer 2

Un'altra distinzione su cui riteniamo utile soffermarci è la classificazione delle blockchain **sulla base della loro architettura**.

Possiamo infatti vedere la blockchain come un sistema composto da più livelli (o *Layer*): il Layer 0 costituisce la base dell'ecosistema ed è composto da connessioni, hardware e miners.



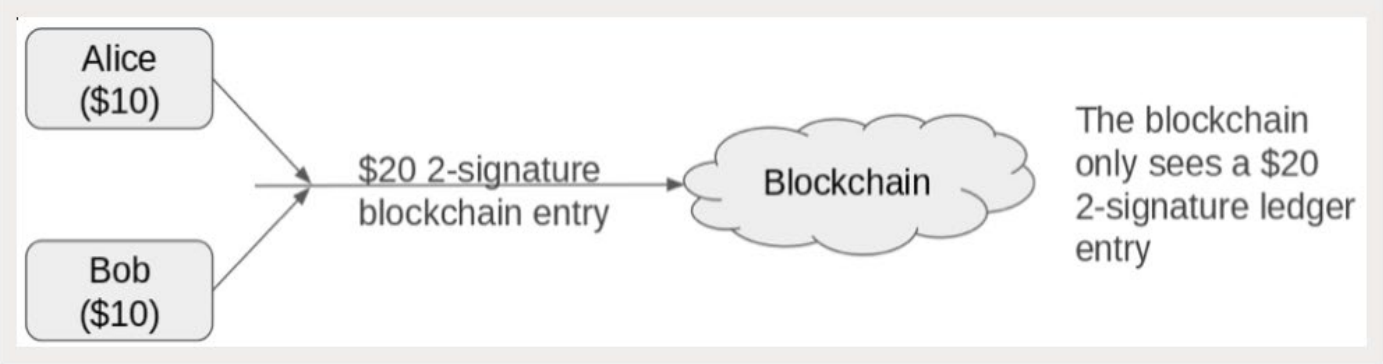
Con il termine **Layer 1** (anche detto *base layer*) ci si riferisce invece alla blockchain vera e propria, quel livello che garantisce sicurezza ed immutabilità delle transazioni ma che ha come limitazione principale la scalabilità (velocità e numero degli output). Infatti, gli sviluppatori di blockchain devono effettuare delle scelte (*trade-offs*) durante la fase di design della "catena", decidendo se prediligere decentralizzazione, sicurezza o scalabilità: il cosidetto Blockchain Trilemma, che impedisce di raggiungere e massimizzare tutti e tre gli obiettivi all'interno della stessa rete. Il Bitcoin è il perfetto esempio di Layer 1: è molto sicuro, ha un elevato livello di decentralizzazione ma non riesce a produrre più di sette transazioni al secondo. Questo è principalmente dovuto al fatto che il Layer 1 rappresenta anche il **Settlement Layer**, ovvero la rete all'interno della quale tutte le transazioni vengono regolate.

Col termine **Layer 2** ci si riferisce invece ad un protocollo secondario **costruito su un sistema blockchain già esistente**: le soluzioni di tipo Layer 2 permettono di beneficiare della sicurezza della *main chain* interagendo con essa, e allo stesso tempo scalano il numero di output e validano le transazioni più piccole in maniera più rapida *"off-chain"*, lontano dalla blockchain principale, con conseguente riduzione del traffico di dati sulla rete primaria.

Vi sono diversi sistemi di Layer 2: quelli che massimizzano la scalabilità (Plasma per Ethereum, Lightning Network per Bitcoin) e quelli che si focalizzano invece sull'inter-operabilità tra le diverse blockchain (Polkadot, Cosmos).

Ad esempio, **il Lightning Network rappresenta la soluzione Layer 2 per scalare Bitcoin**: richiede l'apertura di un canale di pagamento tra due utenti all'interno del quale questi ultimi depositano una determinata somma di Bitcoin (questa transazione avviene sulla *main* blockchain ed i partecipanti alla rete validano l'importo iniziale tramite meccanismi di consenso, esemplificato nella figura sotto) e, da quel momento, tutte le piccole transazioni tra le due parti (di fatto una redistribuzione dell'importo depositato) avvengono senza dover passare nuovamente sulla *main chain*, permettendone la scalabilità e riducendo di molto i

costi. Solo quando il canale tra i due utenti viene chiuso, i fondi vengono effettivamente distribuiti e la transazione validata ancora dalla blockchain principale.



Ciò che rende LN una tecnologia realmente scalabile è che non è sempre necessario che due utenti aprano un canale dedicato per transare: utilizzando i canali con le persone con le quali si è già connessi, LN troverà automaticamente il "percorso più breve", di fatto sfruttando il *network effect* della tecnologia.

Proof of Work vs. Proof of Stake

Le cryptovalute vengono anche categorizzate per rapporto al sistema che usano per validare le transazioni che avvengono sulla loro blockchain. In generale si sono affermate due categorie:

1) **Proof of Work (PoW):** è l'algoritmo di consenso originale in una rete blockchain. Questo algoritmo viene utilizzato per confermare le transazioni e produrre nuovi blocchi nella catena. Con PoW, i cosidetti "minatori" competono l'uno contro l'altro per risolvere un rompicapo matematico utilizzando potenti risorse informatiche al fine di validare e completare le transazioni sulla rete. I "minatori" vengono premiati per il loro sforzo ricevendo direttamente la cryptovaluta per la quale stanno validando le transazioni. Le principali cryptovalute che usano PoW sono Bitcoin ed Ethereum.

2) **Proof of Stake (PoS):** a differenza dei blocchi della PoW, nella PoS essi non vengono estratti, ma coniati. I detentori delle cryptovalute che lo desiderano, si mettono direttamente a disposizione per validare le transazioni. In questo caso chi le valida è selezionato su base pseudocasuale per coniare i blocchi e aggiungerli alla blockchain. Il processo di selezione pseudocasuale entra in funzione dopo che il sistema ha analizzato diversi fattori al fine di garantire che siano selezionati gli individui che partecipano al sistema con una quota

maggiore. Vi sono però variabili che assicurano che anche altri, con una stake inferiore, possano comunque coniare un blocco.

La validazione dei blocchi nella PoS permette di ottenere degli Annual Percentage Yield (APY) anche superiori al 5%. La partecipazione dei detentori dei coins al network viene così incentivata in modo diretto.

Smart Contracts

I "contratti intelligenti", o Smart Contract, sono dei contratti localizzati sulla blockchain che vengono eseguiti automaticamente al verificarsi di determinate condizioni.

All'interno dello Smart Contract vengono specificati in maniera dettagliata i termini della negoziazione, o contratto, tra le due parti, **di fatto eliminando la necessità di una *trusted third-party* che verifichi che le condizioni vengano rispettate. Questo permette di rimuovere la possibilità di errori (l'unico intervento umano è nella scrittura del codice), manipolazioni o ritardi ma soprattutto consente di risparmiare notevolmente**, in quanto tutti i *middle men* coinvolti nel processo (generalmente remunerati con una commissione) andrebbero a scomparire.

Questi "accordi virtuali" sono in grado di facilitare il trasferimento di, potenzialmente, qualsiasi asset e le loro applicazioni possono essere estese a tutti i settori, con la possibilità di cambiare radicalmente interi modelli di business: real estate, settori bancario ed assicurativo, *trade* e *supply chain finance* per citarne solo alcuni.

Gli Smart Contract condividono tutti i vantaggi legati all'utilizzo della tecnologia blockchain (trasparenza, efficenza, rapidità e immutabilità) e sono altamente personalizzabili, quindi possono essere utilizzati per creare diverse tipologie di applicazioni decentralizzate (DApps), che formano il core della finanza decentralizzata (DeFi).

Decentralized Finance

Il termine **"Finanza decentralizzata" (DeFi)** coinvolge tutti i servizi finanziari svolti su di una blockchain. L'aspetto più caratterizzante della DeFi si basa sul fatto che tali servizi vengono svolti senza l'ausilio di un'autorità centrale o di un garante. La DeFi permette pertanto l'accesso a tutti i servizi tradizionali del sistema finanziario, sostituendo gli intermediari con

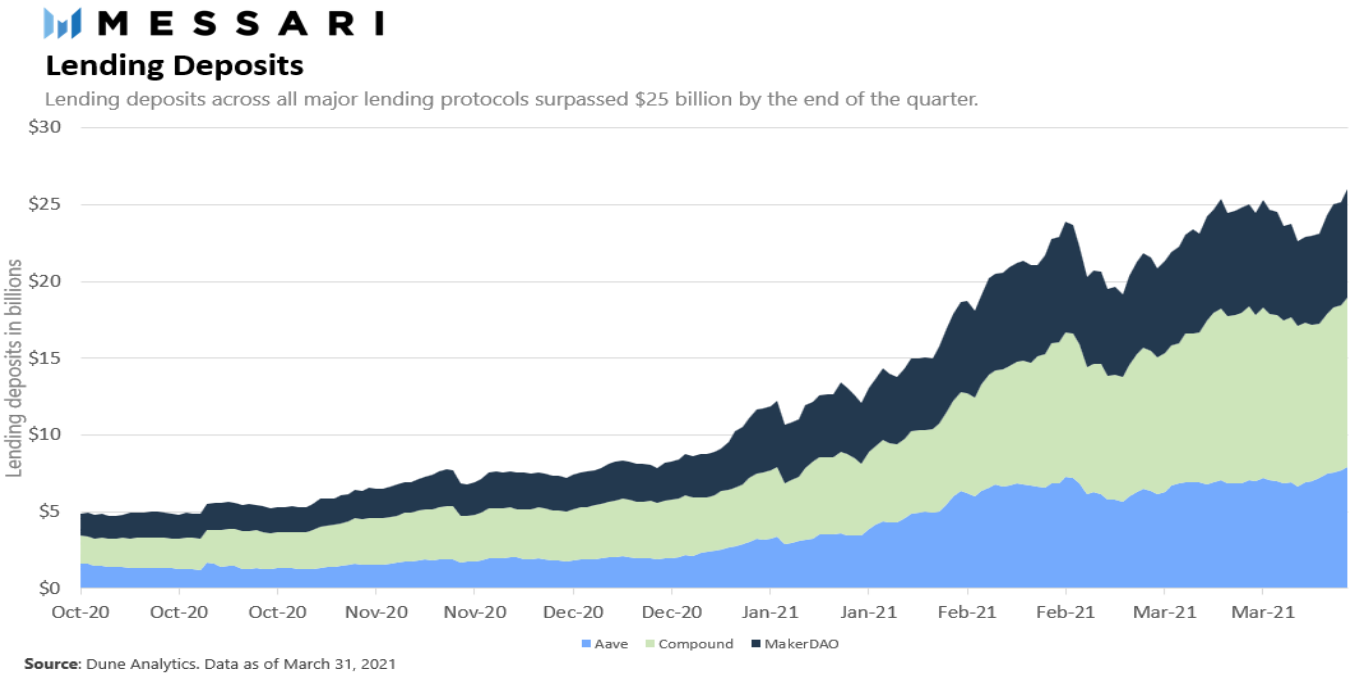
uno *smart contract*. In essenza potremmo descriverla come la fusione tra i servizi bancari tradizionali e la tecnologia blockchain.

Per permettere alla DeFi di funzionare è necessario costruire un'infrastruttura decentralizzata su cui operare. È qui che entra in gioco Ethereum. La blockchain Ethereum è la principale piattaforma dove vengono create le applicazioni decentralizzate (DApps). Ad oggi, secondo i dati di Defi Pulse (https://defipulse.com) circa 90 miliardi di USD sono impiegati tramite DApps nella Finanza decentralizzata).

A questo punto vale la pena entrare nel dettaglio delle più importanti applicazioni che offre la DeFi:

1) **Decentralized exchanges (DEXs):** sono exchanges che operano senza un intermediario. Con i DEX, gli utenti possono connettersi direttamente tra loro per comprare e vendere criptovalute, in un ambiente dove le transazioni avvengono "*trustless*", senza quindi nessun garante nel mezzo. I beni scambiati con i DEX non sono mai tenuti in un escrow account o in un wallet posseduto da terze parti, come viene fatto con gli exchange centralizzati. Il concetto di DEX è proprio delle cryptovalute: nella finanza tradizionale, anche gli scambi eseguiti over-the-counter non sono *"trustless"*. Un altro aspetto rilevante da enfatizzare risiede nel fatto che anche la custodia degli asset digitali che vengono comperati e venduti tramite DEX, avviene senza dover ricorrere ad una entità che faccia da "custody". Uniswap e Sushiswap sono buoni esempi di DEX.

2) **Piattaforme di lending**: uno dei vantaggi principali della DeFi è quello di democratizzare l'accesso al mondo della finanza. In particolare, permette di accendere un prestito senza necessitare di una banca e di un conto corrente. Questo è un aspetto molto rilevante soprattutto per chi vive in parti del mondo dove la penetrazione dei servizi finanziari è molto bassa (ci riferiamo in particolare all'Africa o all'India). Le piattaforme di lending, utilizzando appositi smart contracts, permettono l'incontro tra lenders e borrowers, senza che nessuno debba identificarsi. Tutti hanno accesso alla piattaforma e possono potenzialmente prendere a prestito denaro digitale o fornire liquidità per guadagnare interessi. Similmente al sistema finanziario tradizionale, è necessario offrire criptovalute in garanzia, prima di poter accedere ai prestiti: per certi versi molto simile a quello che viene definito un prestito Lombard in finanza tradizionale. Alcune delle migliori piattaforme di prestito DeFi includono Maker, Compound, e Aave.



Stablecoins

Uno **stablecoin** è una cryptovaluta progettata per mantenere un valore di mercato stabile tramite meccansimi di *peg*, legando il proprio valore ad un altro asset (moneta *fiat*, commodities o altre cryptovalute).

Il maggiore *use case* di questa tipologia di asset è quello legato al ***trading***, in quanto gli stablecoin permettono agli investitori di *swappare* la propria allocazione dalle cryptovalute più volatili a questa forma di moneta digitale, senza necessariamente effettuare una conversione in moneta *fiat* ed evitando così costi più alti. Gli stablecoin sono anche utilizzati per facilitare i **pagamenti cross-border** (come nel caso delle *remittances* verso paesi in via di sviluppo), grazie al settlement istantaneo delle transazioni e alle basse commissioni. Infine, gli stablecoin hanno anche un ruolo molto importante per tutte le attività di ***lending***, permettendo agli investitori in asset digitali di conseguire interessi a doppia cifra dando a prestito la moneta ad altri operatori di mercato (ovviamente non senza rischi, legati principalmente all'effettiva stabilità del *peg*).

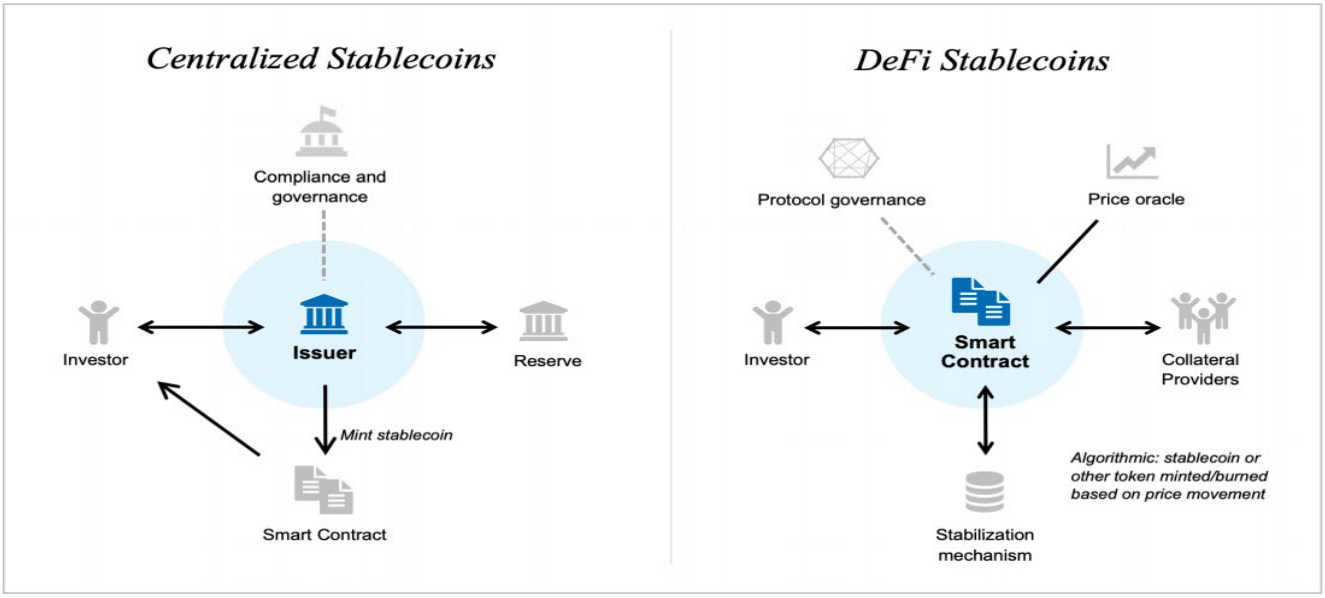
Di seguito mostriamo i cinque maggiori stablecoin per capitalizzazione di mercato, da Ethereum.org al 03/10/21:

VALUTA	CAPITALIZZAZIONE DI MERCATO	TIPO DI GARANZIA	↗
Tether	$69,107,162,929	Valuta a corso legale	↗
USD Coin	$32,173,951,885	Valuta a corso legale	↗
Binance USD	$13,110,670,901	Valuta a corso legale	↗
Dai	$6,222,615,429	Criptovaluta	↗
TrueUSD	$1,342,214,417	Valuta a corso legale	↗

Gli stablecoin sono diventati una parte centrale dell'ecosistema di asset digitali, e quelli maggiormente utilizzati sono quelli ***Fiat-collateralized***, ovvero quegli stablecoins che dichiarano che il proprio valore è *backed* da moneta *fiat (*EUR, USD, GBP etc.) con un ratio 1:1. Tra i maggiori si includono *Tether* (USDT, il più utilizzato) e *USDC* (gestito da un consorzio di società crypto e dall'exchange Coinbase). Le critiche che più spesso vengono fatte a questo tipo di stablecoin sono la scarsa trasparenza circa le effettive riserve di *fiat* money (nel caso di Tether) o il fatto che vengano gestiti da entità centralizzate e quindi non in linea coi principi di decentralizzazione delle blockchain.

Un'altra tipologia che sta acquisendo sempre più rilievo è quella degli stablecoin ***crypto-collateralized***, ovvero quelle monete digitali che legano il proprio valore a quello di un altro asset digitale tramite uno smart contract. Questi asset sono molto più decentralizzati rispetto alla tipologia precedente, in quanto il loro valore non è legato ad alcun attivo "centralizzato"

e sono interamente eseguiti sulla blockchain. Per mitigare i rischi associati alla volatilità di prezzo, nella maggior parte dei casi questi stablecoin sono *over-collateralized* (ad es. per ricevere il corrispettivo di 500 USD di stablecoin è necessario depositare l'equivalente di 1,000 USD di Ethereum). In questa categoria lo stablecoin che raggiunge maggiori volumi è *Dai*, uno stablecoin algoritmico emesso da Maker DAO (una piattaforma di finanza decentralizzata sulla blockchain Ethereum).



Di recente la Security and Exchange Commission americana (SEC) e la Federal Reserve hanno manifestato la necessità di introdurre normative piu' chiare per regolamentare tutto il settore degli asset digitali, soffermandosi in particolare sulla categoria degli Stablecoins e della Finanza Decentralizzata. E' infatti atteso per i prossimi mesi un paper della FED sui costi e benefici dell'adozione di un dollaro digitale (CBDC), che potrebbe anche gettare luce su come il regolatore intende affrontare il tema degli Stablecoins.

Interoperability

La nascita di nuove blockchains alternative al Bitcoin ha progressivamente creato decine di ecosistemi diversi ed indipendenti. Come abbiamo visto precdentemente, ogni blockchain ha le sue caratteristiche, i suoi punti forti e punti deboli. Alcune sono state disegnate per garantire la massima sicurezza delle transazioni, altre con l'intento di processare il più alto numero

possibile di transazioni, altre ancora con lo scopo di fungere da spina dorsale per le DApp. Gli sviluppatori informatici sono alla costante ricerca di soluzioni che possano garantire un corretto equilibrio tra sicurezza, decentralizzazione e scalabilità. E' evidente che ad oggi non esiste ancora una blockchain perfetta, da qui nasce l'esigenza di poter unire i benefici di più blockchains: ci riferiamo alla Cross Chain Technology. **Consentendo l'interoperabilità tra svariate blockchain indipendenti si possono massimizzare i loro vantaggi e contemporaneamente trasferire informazioni, assets, fees, etc da una all'altra.** Un progetto molto avanzato nel campo dell'interoperabilità è Cosmos.

Lugano, 03/10/2021