AEQUITUM

Blockchain

«Wouldst thou'» – so the helmsman answered – «Learn the secret of the sea?
Only those who brave its dangers Comprehend its mystery!»

HENRY WADSWORTH LONGFELLOW

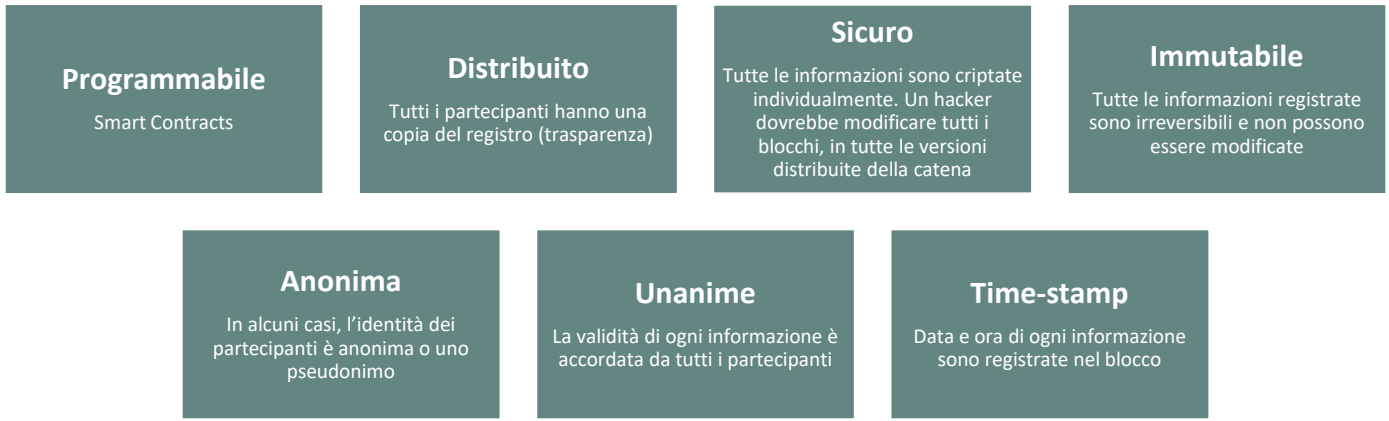
Indice

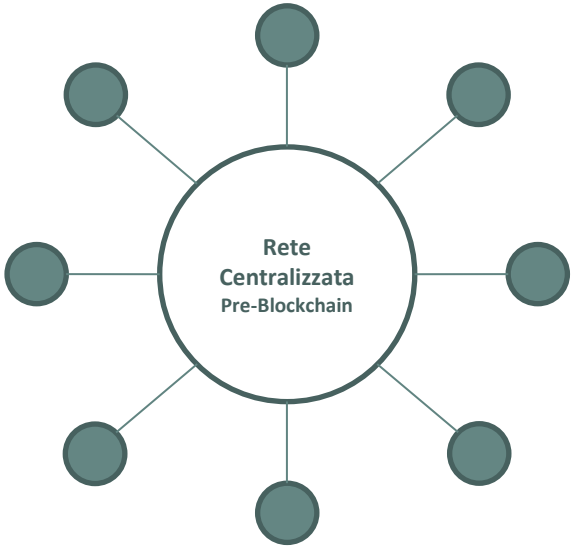
Che cosa è?

Blockchain è una tecnologia capace di registrare informazioni in modo sicuro e permanente tramite la condivisione di un database. Questa condivisione **permette di rimuovere la necessità di intermediari** che solitamente coprono il ruolo di terze parti di fiducia per verificare, registrare e coordinare i dati. Tutte queste informazioni sono registrate digitalmente all'interno di questa «catena di blocchi»

- Per monitorare ed approvare le informazioni, il registro viene distribuito a vari partecipanti che provvedono a controllarlo ed approvarlo (**decentralizzazione**). Questo è il principio della «Distributed Ledger Technology» (DLT). Ogni nuova informazione all'interno della catena viene redistribuita a tutti i partecipanti per essere approvata e registrata con una firma crittografica immutabile (hash). Perciò, se un blocco venisse hackerato/modificato sarebbe immediatamente evidente

- Proprietà DLT:





Scalabile

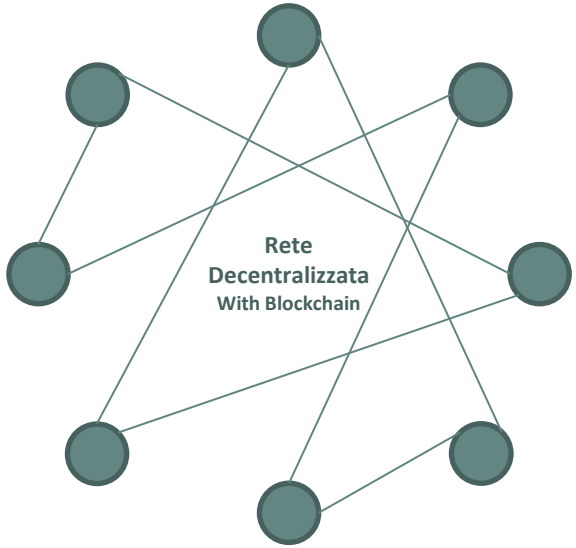
Cloud → Calcoli ed archiviazione potenzialmente illimitate

Efficiente

Tecnologia approvata e matura → consumo energia limitato

Governance dei dati

Autorità centrale controlla i tipi di dati da archiviare e valutare



Aperta e condivisa

Tutti hanno accesso ai dati (controllo centrale assente)

Sicura

Dati criptabili

No intermediario

Modifiche nella blockchain sono gestiti dai partecipanti

Evoluzione della Blockchain & Smart Contracts

Anni '90

Prime applicazioni di DLT pensate per aumentare la sicurezza dei dati digitali delle banche

31 Ottobre 2008

Paper di Satoshi Nakamoto sul concetto di Ledger (registro) distribuito in una rete aperta, fondata su meccanismi di consenso diffuso tra tutti i partecipanti

2011 (Blockchain 1.0)

Blockchain come base tecnologica delle criptovalute (Bitcoin) e nei servizi di pagamento collegati

2014 (Blockchain 2.0)

- Lancio della piattaforma di Ethereum
- Da Blockchain come strumento monetario a strumento ordinario di ***Smart Contracts***, autonomamente eseguibili ed auto ottemperanti

Smart Contracts

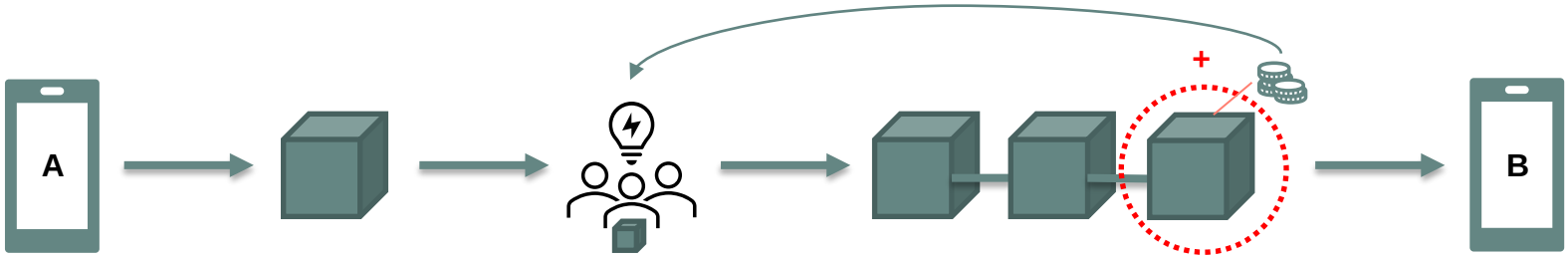
Programmi archiviati su una blockchain che vengono **eseguiti automaticamente se alcune condizioni predeterminate vengono soddisfatte**. Sono anche utilizzati per **l'automatizzazione di un flusso di lavoro**, attivando l'azione successiva quando le condizioni sono soddisfatte

Hanno reso possibile la programmazione a 360 grado della Blockchain

Blockchain 3.0

Compatibilità della Blockchain con altre tecnologie simbolo della Rivoluzione Industriale 4.0 → **IoT**, **AI**, ecc…

Tecnologia Blockchain



Pagamento da A a B

Dettagli transazione archiviati in un blocco

Mining/Forging
Partecipanti controllano e approvano i dati del blocco, lo aggiungono alla catena e ricevono una ricompensa (mining/forging reward)

Pagamento inviato da A a B

Il processo rappresentato sopra può essere applicato a tutti i tipi di asset digitali (es. Smart Contracts e applicazioni software)

Alcuni benefici della Blockchain

Agilità operativa

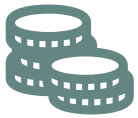
- Ottimizzazione dei flussi di lavoro
- No intermediazione
- Accelerazione delle prestazioni in tutta la catena del valore

Assorbimento dei costi e mitigazione del rischio

- Dati più sicuri e trasparenti (possibilità di criptare tutti i dati)
- Riduzione controversie
- Processi più semplici ed automatizzati

Nuove opportunità di monetizzazione

- Possibilità di accesso a nuovi mercati con la «tokenizzazione» degli asset (clicca qui per vedere un esempio)



Fonte: IBM, https://www.ibm.com/blockchain

Alcuni rischi della Blockchain

Effetto rete

Le tecnologie legate alla blockchain beneficiano di un effetto rete, il che vuol dire che l'aggiunta di ogni persona alla rete aumenta il valore della presenza nella rete per tutti gli altri. Di conseguenza, una rete meno partecipata, rischia di comprometterne l'efficacia ed efficienza

Incertezza normativa

Nuove disposizioni che limitino le attività realizzabili con la blockchain potrebbero far diminuire e/o eliminare la sua attrattiva rispetto ai metodi tradizionali di esecuzione delle transazioni finanziarie

Fabbisogno energetico & spazi di archiviazione

Dal momento che le blockchain sono libri mastri distribuiti e che tutti i dati archiviati nella blockchain sono disponibili presso ciascun nodo, il fabbisogno in termini di spazio di archiviazione di tale sistema cresce in modo esponenziale mano a mano che si aggiungono nodi/utenti al sistema complessivo

Fonte: Morgan Stanley, https://www.morganstanley.com/im/publication/insights/investment-insights/ii_theedgeblockchain_it.pdf

Criptovalute

La tecnologia della Blockchain ha creato le premesse per investire in asset digitali, al di fuori del sistema bancario tradizionale, con la possibilità di averlo a portata di mano 24/7.

Cosa sono le criptovalute?

- Sono monete digitali **decentralizzate** e come tali **non sono controllate da governi o istituti finanziari**
- Possono essere acquistate con qualsiasi valuta tradizionale
- Attualmente sono disponibili **8'626** criptovalute diverse, con una capitalizzazione di mercato equivalente a **$2.64 triliardi**
- In teoria, il loro prezzo **non è legato all'andamento economico generale** e sono **decorrelate dai tassi d'interesse. Per queste ragioni la loro valutazione rimane un esercizio piuttosto complicato**
- Sono considerate come asset finanziario **decorrelato dalle restante classi d'investimento** (anche se a lato pratico finora si è notata una correlazione importante con l'indice NASDAQ o, forse meglio dire, correlate con il Risk On Trade)
- Possono essere trattate in determinati **Exchange Decentralizzati (DEX)** 24/7 e vengono depositate nel «**wallet**» personale
- Il trasferimento delle criptovalute ad un altro wallet avviene **senza la partecipazione di alcun intermediario**. Per raggiungere il wallet destinatario, la transazione viene verificata e validata dai partecipanti della blockchain (**mining**)

Metodi di validazione

Proof-of-Work (PoW)

- Inizialmente introdotta nel 1993 e utilizzata ufficialmente con l'avvento del Bitcoin nel 2009
- Metodo di validazione: Mining/Miners
- Con l'attrezzatura adeguata, tutti possono minare
- Quando le transazioni entrano nel sistema per essere verificate, tutti i miners (nodi) interessati cercano di risolvere il «puzzle» mediante algoritmi. Il primo che risolve, viene ricompensato dal protocollo con un ammontare di monete predefinite (miner reward). Queste ricompense hanno portato la costruzione di mining farm con dimensioni sempre più grandi, aumentando a dismisura il consumo energetico (54 TWG/anno = consumo 5 Mio cittadini USA, consumo annuale Nuova Zelanda/Ungheria)
- Maggiore è l'Hash Rate, maggiore è la probabilità di successo
- Possibilità di aumentare la probabilità di successo mediante «mining pools», combinando l'hashing power e distribuendo la ricompensa tra tutti i partecipanti (centralizzazione della blockchain). Dal momento che un pool possiede il 51% della market cap della moneta in questione ci potrebbe essere il rischio che questi approvino transazioni fraudolente (51% Attack)

Proof-of-Stake (PoS)

- Inizialmente introdotta nel 2011 e utilizzata maggiormente con l'avvento di Ethereum
- Attualmente tecnologia maggiormente utilizzata nel mondo delle criptovalute
- Metodo di validazione: Minting or Forging/Validators
- Idea di ridurre il consumo energetico, non dando a tutte le persone la possibilità di validare: solamente 1 nodo viene selezionato dal protocollo in base ad alcuni criteri
- I nodi (partecipanti) devono depositare/bloccare un certo numero di monete nel network o «staking», come deposito cauzionale. Maggiore è la stake depositata, maggiore è la possibilità di essere scelto nel processo di forging. Quando il nodo viene selezionato, deve verificare che tutte le transazioni del blocco siano corrette, per poi aggiungerlo alla blockchain e ricevere la ricompensa.
- Se i validator approvano transazioni fraudolente, perderanno tutto o parte del valore in stake
- I costi di settaggio di un nodo sono molto più bassi
- Rischio 1: 51% Attack (anche se meno probabile che PoW)
- Rischio 2: No validatori backup nel caso di non riuscita del nodo selezionato

Hash Rate: è la misura della potenza di calcolo al secondo utilizzata durante il mining. Più semplicemente, è la velocità del mining (https://bitflyer.com/en-eu/s/glossary/hashrate)

Bitcoin vs Ethereum

Bitcoin (BTC)

- Nata nel 2009 come prima criptovaluta
- Utilizzato come «store of value» ed hedge contro inflazione, con obiettivo iniziale di dare la possibilità ai detentori di pagare beni in via digitale
- Criptovaluta con maggior capitalizzazione di mercato: 1 triliardo circa (Novrembre 21)
- **Offerta limitata**: offerta totale limitata a 21Mio di monete. Attualmente in circolazioni ce ne sono circa 18Mio (~ 90%)
- **Proof-of-Work (PoW)**: vedi pagina precedente
- **Vantaggi PoW:**
  - I Mining Pool aumentano possibilità di essere selezionato
- **Svantaggi PoW**:
  - Richiede un'alta intensità energetica: poco scalabile
  - Centralizzazione Blockchain (mining pool)
  - 51% Attack
  - Costi setup nodo molto elevati

Ethereum (ETH)

- Nata nel 2015 è la seconda criptovaluta
- A differenza del Bitcoin (store of value), Ethereum è una piattaforma infrastrutturale per l'esecuzione di applicazioni decentralizzate (dApps)
- Protocollo ultilizzato:
  - ETH 1.0: PoW
  - ETH 2.0: Proof-of-Stake (PoS)
- **Offerta illimitata**
- **Proof-of-Stake (PoS)**: vedi pagina precedente
- **Vantaggi PoS:**
  - Accessibile a più persone per i costi minori di setup (decentralizzazione blockchain)
  - Consumo minore energia: più scalabile
  - Validazione più rapida (PoW 30 trans/sec vs PoS 100'000 trans/sec.)
  - Stake a collaterale
- **Svantaggi PoS**:
  - 51% Attack (anche se meno probabile che nel PoW)
  - No validatori a backup

I limiti delle Criptovalute

Regolamentazioni

Alcuni paesi potrebbero vietare l'utilizzo di criptovalute o dichiarare che transazioni violino le norme di antiriciclaggio. I regolatori dovranno anche considerare i potenziali rischi della decentralizzazione al sistema finanziario.

Transazioni illecite

Tuttavia nel 2020 le transazioni criminali legate a criptovalute risultano essere scese allo 0.34% rispetto al 2.1% del 2019 *(Chainalysis)*

Offerta illimitata

Alcune criptovalute hanno un'**offerta limitata** (Bitcoin), altre hanno un'**offerta illimitata**, che potrebbe limitare i loro rendimenti potenziali nel tempo. I dipendenti sono spesso pagati con token aggiungendo un'offerta che è strutturalmente venduta (come le stock option per le società listate)

Ambiente

L'estrazione di asset digitali è difficile da conciliare positivamente con metriche ESG

Viene utilizzata molta energia (anche se principalmente rinnovabile) e non è ancora una tecnologia distribuita in scala nell'economia reale

Fonte: UBP – Decoding Blockchain

Decentralized Finance (#DeFi)

Il termine DeFi descrive un sistema finanziario **privo di intermediari** centralizzati, in altre parole un sistema **autonomo**.

Le applicazioni della DeFi sono varie, di seguito alcune delle più rilevanti:

Criptovalute & Stablecoins

Lending & Borrowing
senza intermediari
(clicca qui per info su Oracolo e Flash Lending)

Derivati (Asset sintetici)
Contratti il cui valore deriva da performance di un asset sottostante

Aggregatori DeFi
Mercati più efficienti

Exchange decentralizzati
Possibilità di trattare asset digitali senza intermediari centralizzati 24/7

Assicurazioni
Coperture assicurative contro certi rischi (rischi smart contract e asset digitale sottostante) senza intermediari

Fonte: PWC, DeFi: Defining the future of finance (https://www.pwc.ch/en/insights/digital/defi-defining-the-future-of-finance.html)

CeFi vs DeFi

Clienti

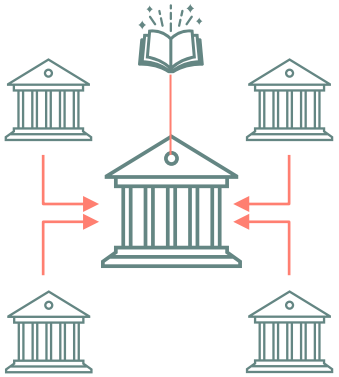
- Login
- Registrazione/Creazione Account
- Trasferimento Fondi all'exchange

Permessi della Piattaforma

- Caricamento ID/KYC/AML applications
- Depositare/Prelevare/Limiti di scambio
- Blocco del prelievo

Exchange Wallet

- Fondi dei clienti detenuti dell'exchange
- Rischio di perdita da furto
- «Not your keys, not your wallet»



- Connettere Wallet
- Garantire permesso allo Smart Contract
- Nessun Account/Login/Registrazione

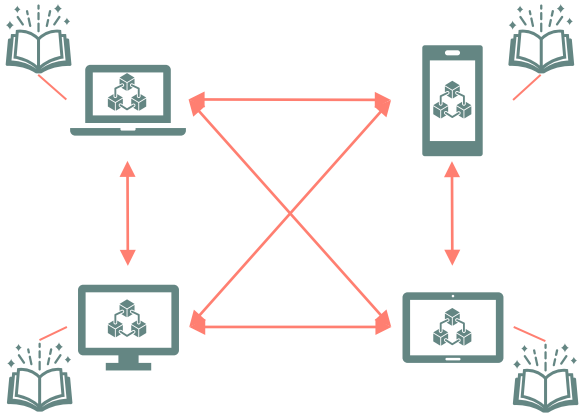
Wallet Privato

- Transazione con Smart Contract
- Compravendite depositate direttamente nel wallet
- No limiti/no blocchi/no applications

Smart Contract

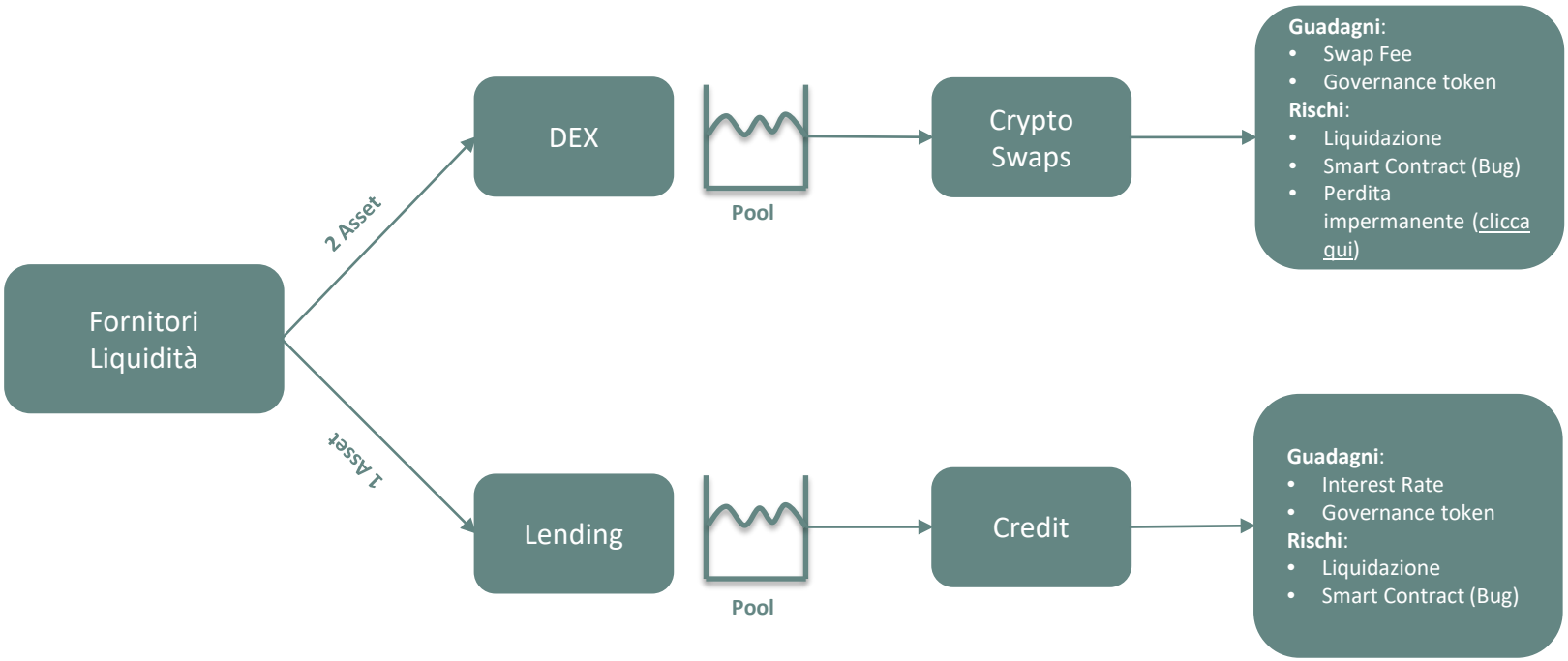
- Fondi bloccati nello Smart Contract mentre sono in uso
- Possono essere sbloccati in ogni momento

Token Pool Decentralizzato



DeFi: Yield Farming

Il termine «Yield Farming» si intende la possibilità di ottenere rendimenti sul mondo delle criptovalute. Essa comporta lo «staking» (blocco) della moneta per un periodo di tempo flessibile o fisso in cambio di interessi e/o altre criptovalute.



Pool

Pool di liquidità: è uno smart contract che contiene fondi. La liquidità fornita alla pool viene ricompensata con commissioni e/o altre criptovalute.
Il Valore Totale Bloccato (VTB) rappresenta la liquidità aggregata nella pool. Viene perciò considerato come parametro efficace per quantificare la «salute» della DeFi e permette di mettere a confronto i vari protocolli DeFi.

Fonte: SEBA Bank; Binance Academy

Decentralized Autonomous Organizations (DAOs)

Con l'acronimo **DAO** si definisce una **Organizzazione Autonoma Decentralizzata**. Essa è un programma informatico che tramite tecnologia blockchain definisce tutte le regole alla base di un'organizzazione, con l'obiettivo di avere una **governance completamente decentralizzata** ed una serie di Smart Contract che contribuiscono all'automazione ed alla trasparenza di queste regole predefinite.

A parte il momento della creazione del codice alla base degli Smart Contracts, la salvaguardia e l'implementazione di queste regole avviene autonomamente, senza l'intervento di alcun intermediario che agisca da garante.

Tutte le decisioni e azioni vengono intraprese in piena trasparenza e con un **sistema di votazione** autonomo (no autorità centrale) da parte di tutta la community. Al momento dell'approvazione della proposta, l'intera somma raccolta ha come unico obiettivo quello di finanziare il suo sviluppo. Perciò, è nell'interesse della community votare per una proposta che possa portare valore alla piattaforma (DAO), con la possibilità di diventare sempre più richiesta ed utilizzata e perciò aumentando il valore del suo token di riferimento (detenuti della community).

Il diritto di votazione di un utente è rappresentato dal possesso del «**token governance**», che possono essere intese come le azioni con diritto di voto di una società tradizionale. L'unica differenza è che non importa quanti token un individuo detiene, il possesso anche di un singolo token garantisce equo diritto.

Obiettivo di una DAO: trasparenza delle transazioni finanziarie, democrazia, privacy ed anonimato

Fonte: Cryptonomist, https://cryptonomist.ch/2020/04/11/cosa-sono-dao-come-funzionano/

DAOs vs Organizzazioni Tradizionali

DAO	Organizzazione Tradizionale
Solitamente con struttura piatta e totalmente democratica	Solitamente con struttura gerarchica
Tutti i cambiamenti/azioni/proposte devono essere validate tramite voto da tutti i membri	A dipendenza della struttura, le decisioni possono essere prese da un solo membro come da più membri con votazione
Nessun intermediario che verifichi le regole e il sistema di voto	Regole e votazioni sono verificate e controllate da intermediario
I servizi offerti sono gestiti in maniera autonoma e decentralizzata (NO manipolazione)	Richiede l'intervento umano o il controllo di un'autorità centrale (SI manipolazione)
Tutte le attività sono trasparenti e totalmente pubbliche	Attività sono tipicamente private e limitate al pubblico
Initial Coin Offering (ICO) – clicca qui per approfondimenti	Initial Public Offering (IPO)

Fonte: Ethereum, https://ethereum.org/en/dao/

Altri Utilizzi

Clicca qui per vedere utilizzi aggiuntivi

Tracciabilità della catena di approvvigionamento

- Migliorare la sicurezza alimentare: origine dei prodotti, destinazione, ora e luogo (Walmart)
- Autenticazione parti di aerei: rende più semplice controllare l'origine, la qualità delle parti usate degli aerei (SITA)
- Riduzione della contraffazione: tracciabilità e prova di autenticazione dei prodotti. I clienti possono ricevere certificati contenenti tutte le informazioni dei prodotti (LVMH)

Arte Digitale (NFT)

- Non-fungible token (NFT) sono dei certificati che attestano l'autenticità, l'unicità e la proprietà di un oggetto digitale (immagine, video, canzone,…). I token vengono registrati in una blockchain e non possono essere scambiati tra loro ne copiati.
- Gli NFT possono essere anche usati per certificare pezzi di arte digitale

Gestire la tua Identità digitale

- Okta e SecureKey stanno lavorando per costruire soluzioni d'identità digitale mediante l'utilizzo della blockchain
- Gli utenti possono decidere quali informazioni personali condividere
- Prevenire frodi su scambio identità (bagarinaggio)
- Tracciare l'andamento di studenti per migliorare l'istruzione
- Votazione elettorale digitale

Automazione della gestione dei contenuti

- Tracciare copyright, semplificando il tracciamento delle royalties, il loro pagamento tutto automaticamente (Sony Music)

Fonte: UBP – Decoding Blockchain; InsiderMarketing, https://www.insidemarketing.it/glossario/definizione/nft/

Universo investibile

Criptovalute & Stablecoin

- Possibilità di investire in **Criptovalute & Stablecoin** direttamente nei DEX regolamentati
- Long-only Active funds, Prodotti strutturati,
  Hedge Fund (Arbitrage, Quant..)

Cripto ETPs

- Autorizzate negli USA da fine Settembre 2021
- Seguono il valore della criptovaluta di riferimento

Investimenti in società coinvolte nel settore

- Molte società stanno investendo nella tecnologia Blockchain

Blockchain Fondi & ETFs

- Venture Capital Funds
  Private Equity Funds

Fonte: UBP – Decoding Blockchain & https://time.com/nextadvisor/investing/cryptocurrency/how-to-invest-in-crypto-without-buying-any-crypto/

Conclusioni

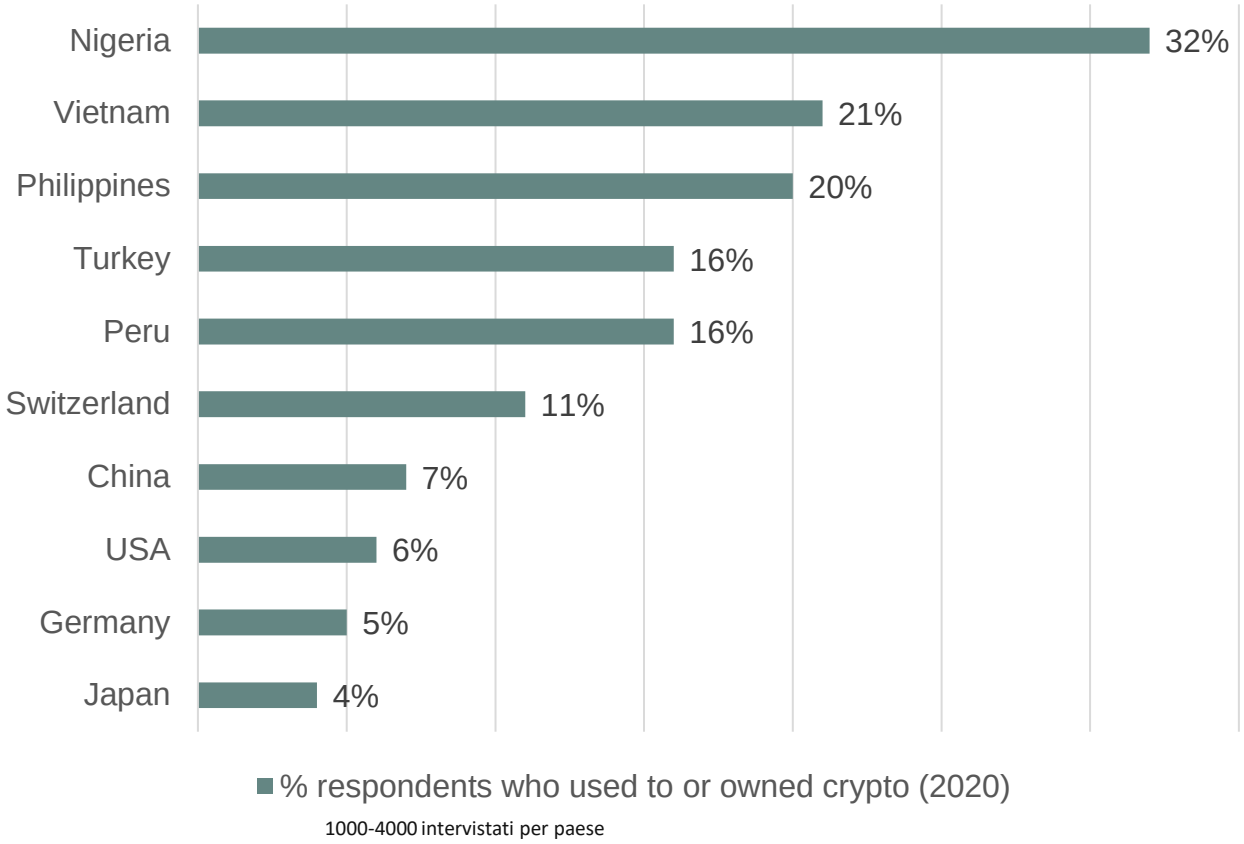
- **Short Term**
  - **Blockchain:** il **sentimento collettivo sulla blockchain è in aumento**, insieme alle implementazioni significative nei settori pubblico e privato. Le **applicazioni della tecnologia blockchain sono svariate** e crediamo che sia importante capire quali saranno le società in ritardo e quelle che invece decideranno di cavalcare l'onda. «Come è già successo per Internet, probabilmente assisteremo alla creazione di un misto di società native della blockchain e di società che adottano la tecnologia per migliorare i propri processi aziendali esistenti e per **affrontare nuove opportunità** di mercato generate da queste nuove capacità.» (Morgan Stanley)
  - **Criptovalute**: crediamo che sia un asset **ancora investibile e con un potenziale di crescita interessante**. È un mercato ancora relativamente **inefficiente**, ricco di **arbitraggi** da sfruttare. Nel mercato, ci sono già molte piattaforme (qualcuna sarà destinata a scomparire – *hype and reality*) che ti permettono di investire nella maggior parte delle sfaccettature di questo mondo (futures, swaps, prodotti strutturati, HF,…). Il rischio maggiore sono le **regolamentazioni restrittive** dei governi che potrebbero improvvisamente cambiare le carte in tavola → ***Piatto ricco mi ci ficco, ma investor's tourism beware! Potrebbe rivelarsi in buona parte un Momentum Trade***
- **Long Term**
  - **Blockchain:** rivoluzionaria!
  - **Criptovalute:** non le vediamo scomparire, ma sicuramente saranno **molto più regolamentate**, rendendo perciò il loro mercato **molto più efficiente** e dei **ritorni inferiori**. L'avvento delle Central Bank Digital Currencies (**CBDC**) e delle **Programmable Money**.

Takeaway

Non bisogna sottostimare questo tipo di tecnologia, in quanto ha le basi per rivoluzionare l'economia e la società del futuro. Nonostante ci siano già numerose piattaforme, società, DAO e criptovalute, siamo solamente all'inizio del processo di trasformazione. Per questa ragione, come tutte le cose nuove, è molto difficile individuare i vincitori ed i vinti.

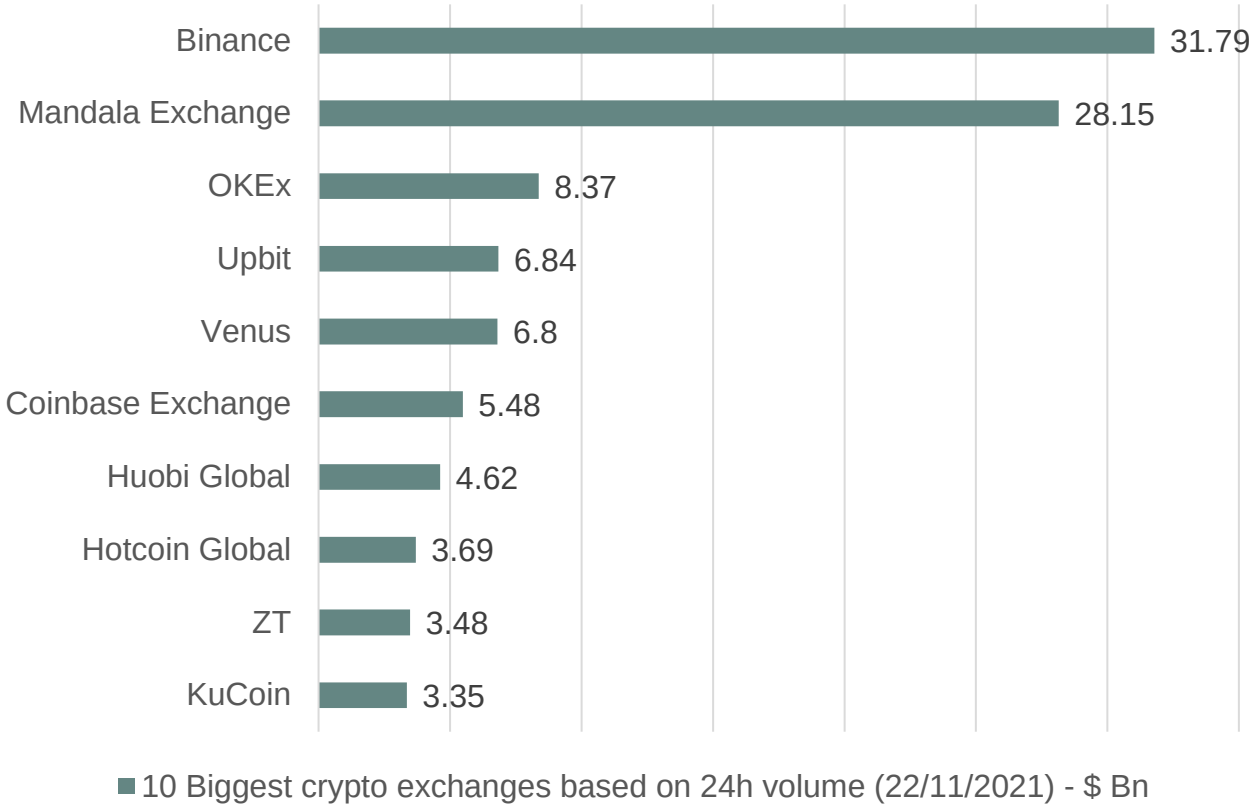
Fonte: Morgan Stanley (https://www.morganstanley.com/im/publication/insights/investment-insights/ii_theedgeblockchain_it.pdf)

Quanto è comune il mondo crypto?



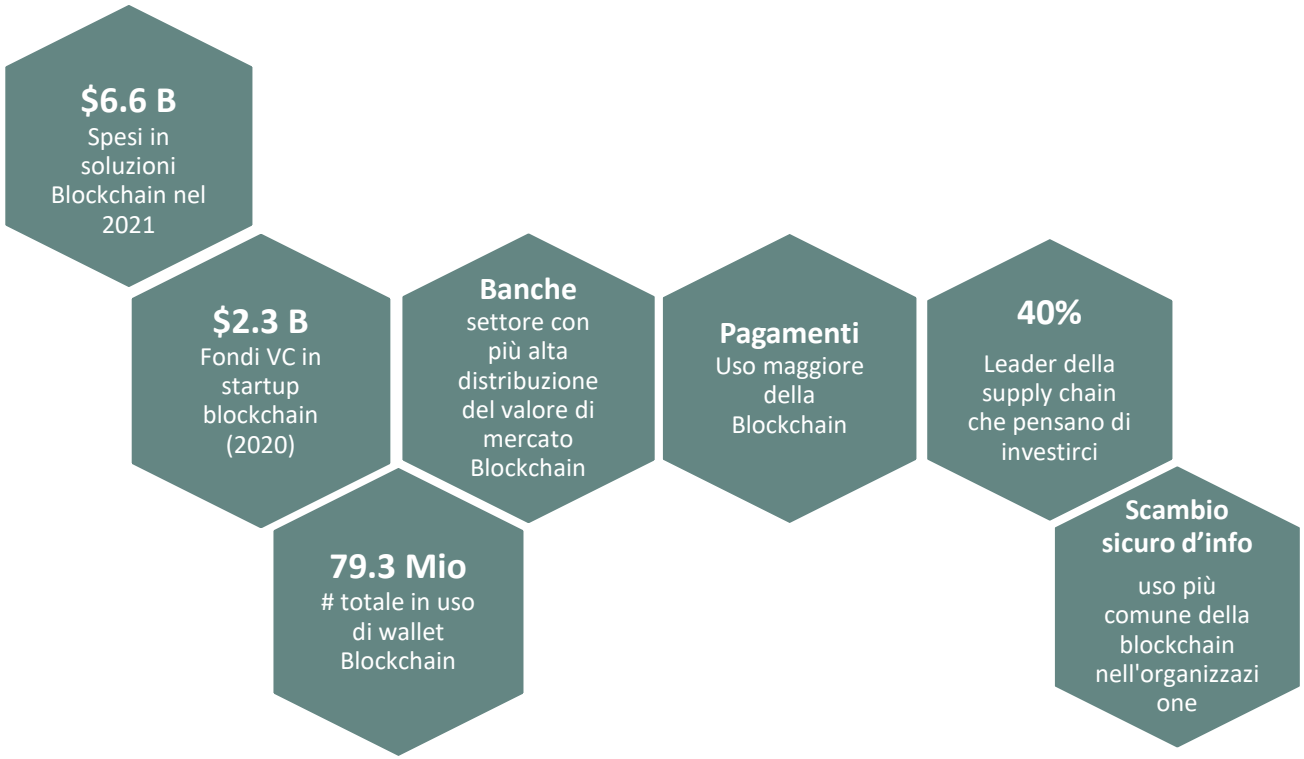
Fonte: Statista Global Consumer Survey

Quanto è comune il mondo crypto?



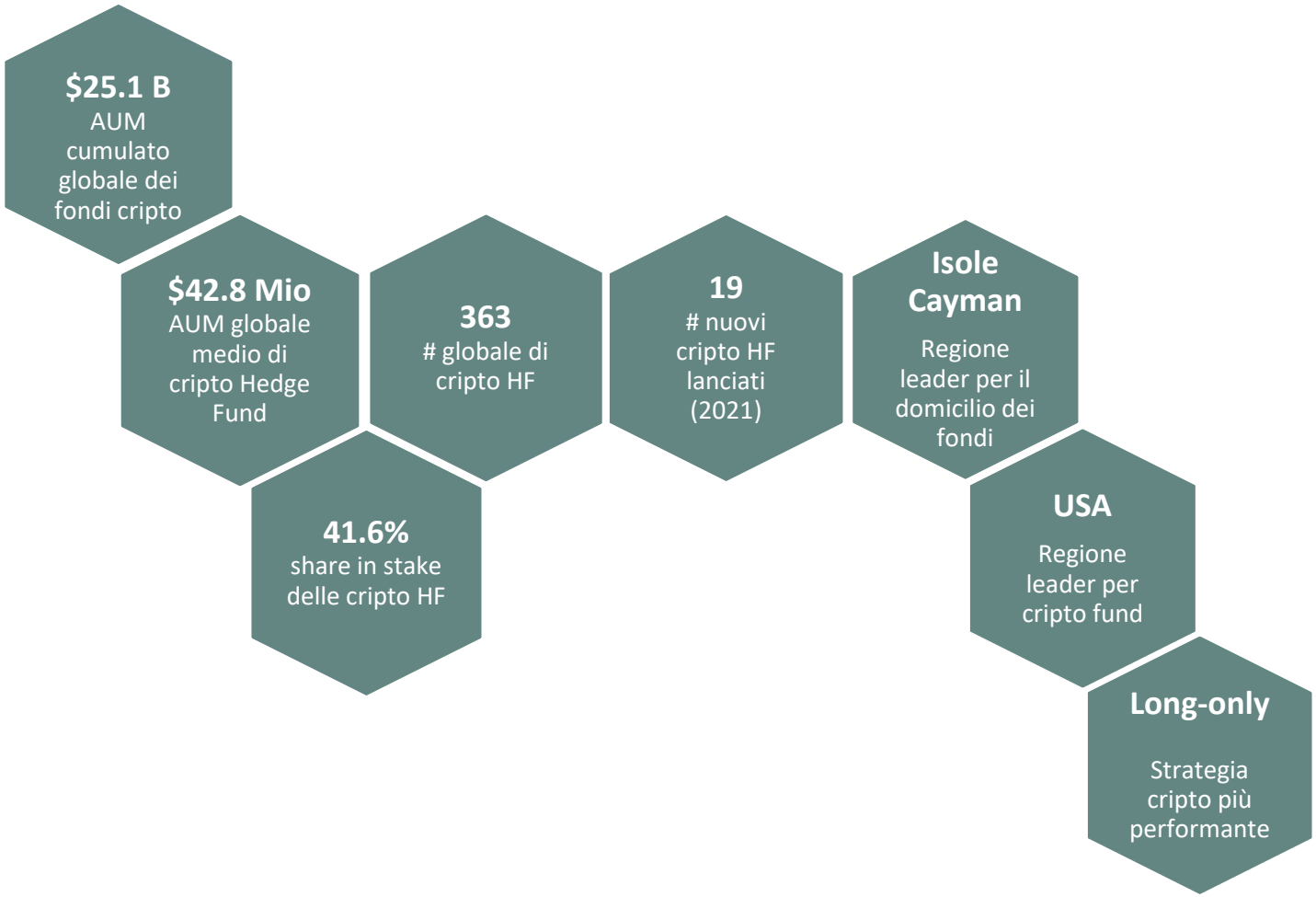
Fonte: Statista Global Consumer Survey, https://www.statista.com/statistics/864738/leading-cryptocurrency-exchanges-traders/

Blockchain – Alcuni dati

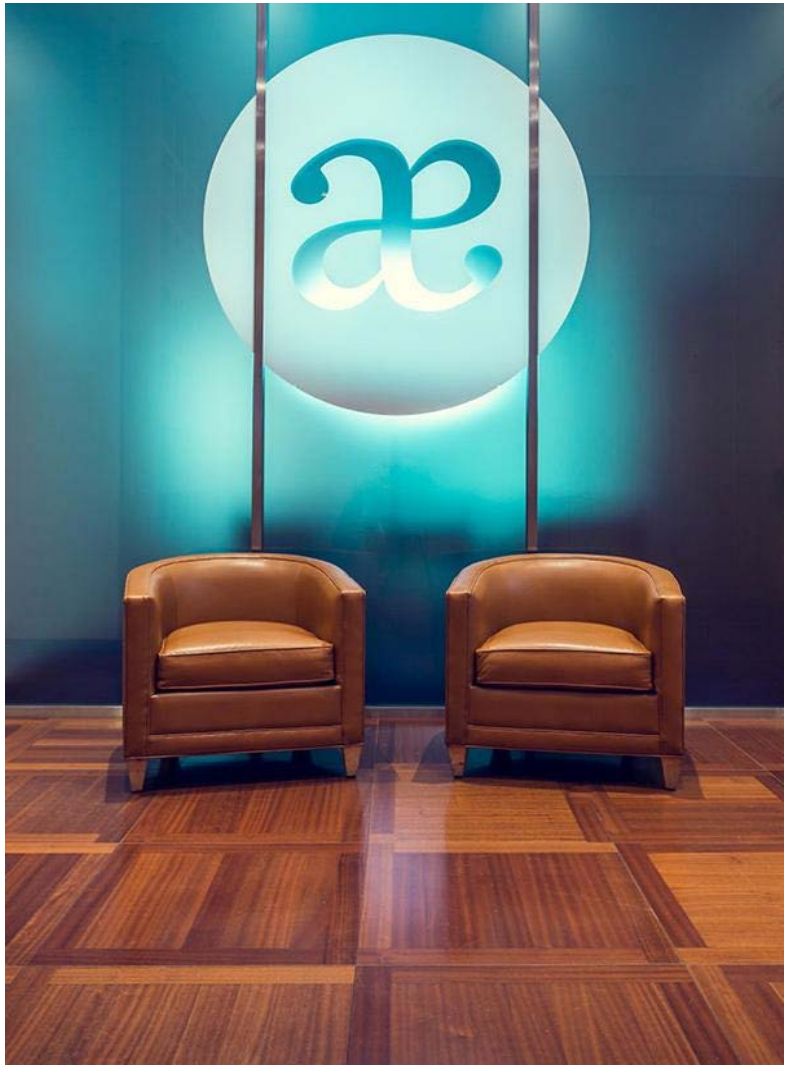


Fonte: Statista Global Consumer Survey (https://www.statista.com/topics/7573/crypto-funds/#dossierKeyfigures)

Fondi Cripto – Alcuni dati



Fonte: Statista Global Consumer Survey (https://www.statista.com/topics/7573/crypto-funds/#dossierKeyfigures)



Disclaimer

The information provided herein is intended to inform you of certain investment products and services offered by Aequitum SA.

This material is intended for your personal use and should not be circulated to any other person without our permission. Any use, distribution or duplication by anyone other than the recipient is prohibited. The views and strategies described herein may not be suitable for all investors and are subject to investment risks. Certain opinions, estimates, investment strategies and views expressed in this document constitute our judgment based on current market conditions and are subject to change without notice. Investors may get back less than they invested. The information contained herein should not be relied upon in isolation for the purpose of making an investment decision. More complete information is available, including product profiles, which discusses risks, benefits, liquidity and other matters of interest. For more information on any of the trade ideas and products illustrated herein, please contact Aequitum SA.

Past performance is no guarantee of future results.

Aequitum is the lighthouse, marking the safe course through the open seas of Wealth Management. It is a lean, bespoke, and independent solution, connecting deep experience with strategic vision, simplicity and analytical knowledge – here to guide your investment voyage to a secure harbour.

Aequitum SA
Via Vegezzi 6
CH-6900 Lugano

tel +41 (0)91 910 25 80
fax +41 (0)91 910 25 90

info@aequitum.com
aequitum.com

AEQUITUM