UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

DIPARTIMENTO DI INGEGNERIA

MECCANICA E INDUSTRIALE

Corso di Laurea

in Ingegneria Gestionale

BLOCKCHAIN E CRIPTOVALUTE:

aspetti tecnici, pratici e studio della volatilità

Relatore: Chiar.mo Prof. Roberto Franzoni

Laureando:

Andrea Alberti

Matricola n. 723574

Anno Accademico 2020 - 2021

A coloro che mi hanno sostenuto sempre,
la mia famiglia.

BITCOIN

A PEER-TO-PEER ELECTRONIC CASH SYSTEM

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

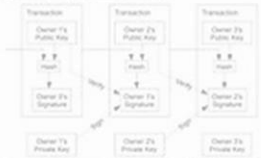
We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party. What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank. We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp

Server The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added. To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one. New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free. The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.

As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.

It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent. The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1. The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind. We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late. The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction. The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = \frac{z q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point.

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \cdot (1 - (q/p)^{(z-k)})$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z. q=0.1 z=0 P=1.0000000 z=1 P=0.2045873 z=2 P=0.0509779 z=3 P=0.0131722 z=4 P=0.0034552 z=5 P=0.0009137 z=6 P=0.0002428 z=7 P=0.0000647 z=8 P=0.0000173 z=9 P=0.0000046 z=10 P=0.0000012 q=0.3 z=0 P=1.0000000 z=5 P=0.1773523 z=10 P=0.0416605 z=15 P=0.0101008 z=20 P=0.0024804 z=25 P=0.0006132 z=30 P=0.0001522 z=35 P=0.0000379 z=40 P=0.0000095 z=45 P=0.0000024 z=50 P=0.0000006

Solving for P less than 0.1%... P < 0.001 q=0.10 z=5 q=0.15 z=8 q=0.20 z=11 q=0.25 z=15 q=0.30 z=24 q=0.35 z=41 q=0.40 z=89 q=0.45 z=340

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org

INDICE

INTRODUZIONE

Negli ultimi anni l'interesse per il mondo delle criptovalute è cresciuto moltissimo. Molte società che operano in ambito cripto hanno concluso importanti accordi di sponsorizzazione nel mondo dello sport e dello spettacolo e più recentemente sono apparse in tv le prime pubblicità riguardo ad esse. Per questo motivo il numero di persone che parla di blockchain, Bitcoin, Ethereum ed altro è sempre maggiore. Tuttavia, esistono dei falsi miti come la credenza che queste rappresentino una facile fonte di guadagno. Per questo motivo è necessario approcciarsi in modo sostenibile a questo settore, studiando le basi tecnologiche che lo governano, in modo da comprenderne potenzialità e limiti. Solo a questo punto è possibile passare alla valutazione di un eventuale investimento in questa nuova tecnologia.
L'obiettivo di questa tesi è proprio quello di illustrare i principi fondamentali di funzionamento della blockchain e delle criptovalute, senza troppi tecnicismi e attraverso l'uso di analogie per un'esposizione semplificata dei punti più complessi. Successivamente vengono esposti aspetti pratici per l'interazione con le criptovalute e uno studio sulla loro volatilità. L'argomento è inoltre trattato nel modo più neutrale possibile, esponendone sia le opportunità che i limiti e le debolezze. Infatti, come tutte le tecnologie, criptovalute e blockchain vanno valutate sulla base del valore fondamentale, non facendosi offuscare dall'aspetto emotivo dettato dall'andamento del mercato.

L'elaborato è diviso in tre capitoli. Nella prima parte sono illustrati i principi di funzionamento della blockchain e delle criptovalute. In particolare, inizialmente è trattata la tecnologia blockchain, parlando nel dettaglio di ogni suo componente e fornendo degli esempi della sua implementazione, in ambito finanziario e non solo. In seguito, sono esposti i concetti di criptovaluta e protocollo, partendo dal più diffuso e "antico", Bitcoin, fino ad arrivare al computer decentralizzato Ethereum e al progetto italiano di Algorand. L'obiettivo di questa parte è quello di evidenziare le diverse modalità di utilizzo della blockchain da parte di ciascun protocollo, analizzando vantaggi e svantaggi dei singoli casi.

Nel secondo capitolo della tesi sono presentate a livello pratico, le fasi di acquisto, conservazione e vendita delle criptovalute, per coloro che convinti dalla bontà della tecnologia decidano di investirvi del capitale.

Infine, nel terzo e ultimo capitolo è riportato uno studio sulla volatilità del settore cripto confrontato con settori più tradizionali, come quello azionario e obbligazionario. L'obiettivo di questo capitolo è quello di illustrare i rischi finanziari che si corrono entrando in questo mondo, causati soprattutto dalle dimensioni ancora ristrette e dall'altissima speculazione che viene fatta al suo interno.

Alla fine della lettura, sarà possibile avere un'idea chiara dei complessi meccanismi crittografici e tecnologici che consentono alla blockchain di funzionare e si conosceranno diverse modalità di utilizzo di tale tecnologia, con un approfondimento su Bitcoin, Ethereum e Algorand. Inoltre, verranno compresi il significato e le potenzialità di uno degli ambiti in forte sviluppo, la DeFi. Infine, sarà possibile avere indicazioni riguardo alle procedure di investimento e al rischio finanziario associato al mercato delle criptovalute.

CAPITOLO UNO

1. BLOCKCHAIN E CRIPTOVALUTE

C'è una grande confusione sui concetti di blockchain e di criptovalute: in alcuni casi si fa riferimento a bitcoin parlando della tecnologia blockchain, in altri si menziona la blockchain parlando delle criptovalute in generale. Tuttavia, questi termini indicano cose molto diverse seppur connesse tra loro. Per fare chiarezza nella distinzione è possibile fare un'analogia con il web.

- I siti web sono una tecnologia per condividere informazioni.
- La blockchain è una tecnologia per registrare le informazioni.
- I motori di ricerca sono il modo più diffuso di usare la tecnologia dei siti web.
- Le criptovalute sono il modo più diffuso di utilizzare la tecnologia della blockchain.
- Google è il browser più famoso.
- Bitcoin è la criptovaluta più diffusa.

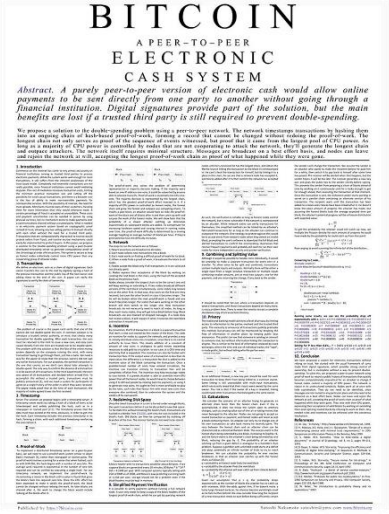
Al fine di analizzare più approfonditamente le differenze, nei capitoli successivi vengono trattati singolarmente, prima la blockchain e successivamente le criptovalute.

1.1 Blockchain

1.1.1 Breve storia

La prima idea di blockchain nasce nel 1991 ad opera di Haber e Stornetta, due ricercatori che introducono un sistema a blocchi protetto crittograficamente, con l'obiettivo di effettuare una marcatura temporale di documenti digitali. Tuttavia, questa tecnologia rimane inutilizzata e il brevetto scade nel 2004. In quello stesso anno, Hal Finney introduce un sistema chiamato Reusable Proof of Work. Il sistema funziona così: riceve un token non fungibile e in cambio crea un token firmato crittograficamente, che può

essere trasferito da persona a persona. Questo sistema risolve il problema della doppia spesa, ma viene poco utilizzato. Alla fine del 2008 viene pubblicato il White Paper di Bitcoin *(figura 1[1])*, ad opera di Satoshi Nakamoto, che descrive la blockchain come la conosciamo oggi. Questo sistema prevede ancora una volta un algoritmo PoW, ma risolve il problema della doppia spesa tramite un protocollo P2P generalizzato per la verifica delle transazioni. Nel 2009 viene minato il primo blocco Bitcoin da Satoshi Nakamoto e sempre Satoshi il 12 gennaio 2009 effettua la prima transazione di 10 bitcoin verso Hal Finney. Nel 2013, Vitalik Buterin, co-fondatore di Bitcoin Magazine inizia a sviluppare una nuova blockchain sulla quale è presente una funzionalità detta smart contract. Gli smart contract sono dei programmi eseguiti sulla blockchain che consentono, ad esempio, di eseguire transazioni solo quando determinati requisiti sono soddisfatti. Questa nuova catena, conosciuta come Ethereum, è quindi programmabile e su di essa vengono costruite delle Decentralized Applications tra cui casinò, socials ed exchange. Ad oggi Bitcoin ed Ethereum dominano il mondo delle blockchain, ma molte nuove proposte sono emerse e stanno guadagnando terreno rapidamente, come Terra, Cronos e Algorand.


BITCOIN

A PEER-TO-PEER ELECTRONIC CASH SYSTEM

Figura 1 - White Paper Bitcoin.

1.1.2 Definizione

“La blockchain, letteralmente “catena di blocchi” *(figura 2[2])*, è una struttura dati decentralizzata, condivisa e crittograficamente immutabile. Tale struttura serve da registro digitale di tutte le informazioni che in essa vengono inserite e suddivise in “blocchi” di dati. L’inserimento e la validazione di tali transazioni sono delegati a un meccanismo di consenso, distribuito su tutti i nodi (in alcuni casi solo quelli autorizzati) della rete stessa. Per semplificare il concetto, in poche parole:

[1] Fonte: https://drakemall.com/it/products/bitcoin-whitepaper-poster.
[2] Fonte: https://www.fkie.fraunhofer.de/de/leistungsportfolio/lernlabor-cybersicherheit/blockchain.html.

> "*La Blockchain non è altro che una sorta di libro di mastro, distribuito e gestito da una rete di computer, ognuno dei quali ne possiede una copia"*[3].

L'aggiunta di ogni nuovo blocco alla catena deve passare attraverso un preciso protocollo basato sul consenso tra questi computer (nodi). Una volta autorizzata l'eventuale aggiunta del blocco, ogni nodo aggiorna la propria copia, senza che ci sia più alcuna possibilità di modificare i dati una volta inseriti e validati".

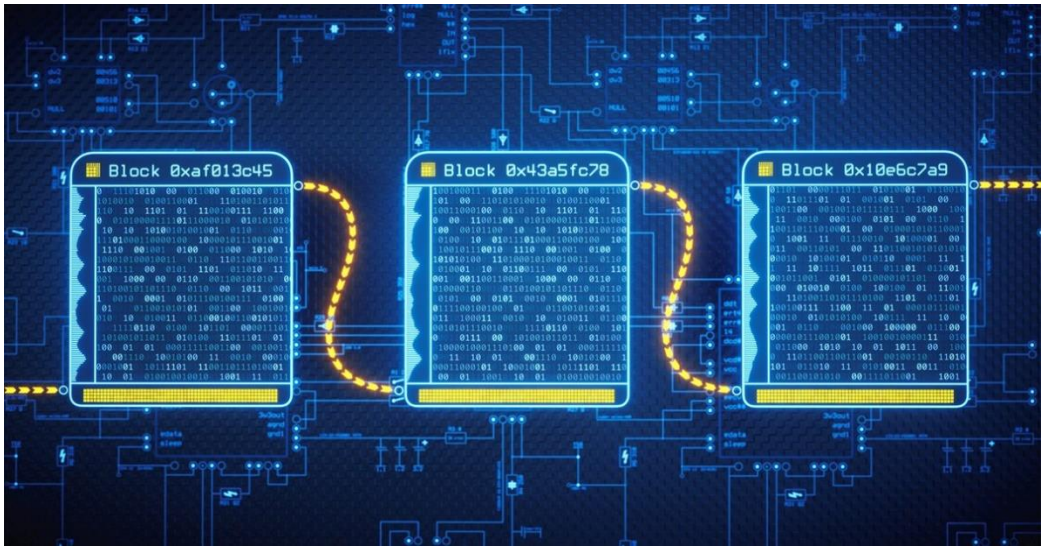


Figura 2 - La blockchain

1.1.3 Tipologie di blockchain

Esistono due tipologie di blockchain, permissionless e permissioned.

La blockchain permissionless (o pubblica), ovvero "senza autorizzazione", è un registro pubblico la cui proprietà non appartiene a nessuno. Chiunque può contribuire all'aggiornamento dei dati su di esso, tramite l'aggiunta di blocchi e ciascun partecipante al network può contribuire a garantirne la sicurezza e l'immutabilità. Le decisioni vengono prese tramite un algoritmo di consenso e in un sistema di questo tipo non può esistere alcun tipo di censura, infatti, non è presente un ente centrale in grado di

[3] Comandini G., Da Zero alla Luna. La Blockchain: quando, come, perché sta cambiando il mondo, Palermo, Dario Flaccovio Editore S.r.l., Marzo 2020, pp. 47, https://www.lafeltrinelli.it/da-zero-alla-luna-quando-libro-gian-luca-comandini/e/9788857910307, consultato il 28 Novembre 2021.

bloccare le transazioni effettuate dai partecipanti. Gli elementi fondamentali sono i nodi, i quali si occupano di verificare che le transazioni siano corrette, se lo sono non hanno potere di bloccarle e vengono aggregate per formare un blocco. Esempi di Blockchain pubbliche sono Bitcoin ed Ethereum.

La blockchain permissioned (o privata), ovvero “con autorizzazione” è di proprietà di un determinato attore della rete. Questo può decidere se consentire l’accesso alla rete ad un nodo oppure negarlo e decide la posizione che i vari attori assumono nella rete. È anch’essa costituita da un registro che viene distribuito, ma la grande differenza con una blockchain permissionless è che viene distribuito solo ai nodi scelti dal proprietario. Quest’ultimo ha anche il potere di decidere chi ha il diritto di verificare le informazioni, aggiungerle al blocco e successivamente alla blockchain. Una struttura di questo tipo va quindi a centralizzare una tecnologia che fa della decentralizzazione la propria forza. Un esempio di blockchain di questo tipo è la cosiddetta *blockchain del consorzio:* 10 aziende si accordano per la costituzione di una blockchain nella quale condividere, ad esempio, le fatture. Tuttavia, se l’azienda 7 ha rapporti solo con le aziende 3,4,5 è possibile “tagliare fuori le altre aziende” e condividere le fatture solo con queste tre.

1.1.4 Il blocco

Da questa prima illustrazione della blockchain e dal suo stesso nome si capisce come l’elemento fondamentale di tale struttura sia il blocco, ma che cosa è un blocco? Il blocco può essere visto come un insieme di dati che vengono identificati da una stringa alfanumerica univoca, detta Hash (trattata successivamente), che permette a chiunque di verificare l’autenticità del blocco. Infatti, una volta trovato l’hash, il blocco viene aggiunto alla blockchain e chiunque può verificare la correttezza della stringa che lo identifica. I blocchi sono concatenati perché nei dati inclusi in un blocco è presente anche l’hash del blocco precedente. Per come è fatta la funzione di hash, cambiando un solo dato in input, cambierebbe totalmente la stringa in output, quindi una modifica dei dati produrrebbe un hash diverso dal precedente, evidenziando l’alterazione del blocco. Ma quindi, a causa della concatenazione, se qualcuno volesse modificare un blocco, dovrebbe poi modificare anche tutti i successivi e calcolarne l’hash. Considerando che il calcolo dell’hash è un’operazione molto onerosa, non risulta conveniente

modificare blocchi già confermati. Nei dati del blocco, oltre all'hash sono incluse le transazioni. Infatti, affinché queste possano essere considerate valide, è necessario siano incluse in un blocco minato, ovvero con un hash corretto e verificabile. Vediamo adesso più nel dettaglio la composizione di un blocco *(figura 3*[4]*).* La struttura di quest'ultimo elemento è divisibile in 2: *header e body.* Il *body* contiene le transazioni, mentre l'*header* è formato da una serie di dati tra i quali:

- *Hash*: stringa alfanumerica associata all'intero contenuto del blocco;
- *Timestamp*: data e ora in cui il blocco è stato prodotto;
- *Height*: numero del blocco;
- *PrevHash*: hash del blocco precedente;
- *Transaction Volume*: volume di criptovaluta movimentato;
- *Size*: dimensione del blocco in KB.

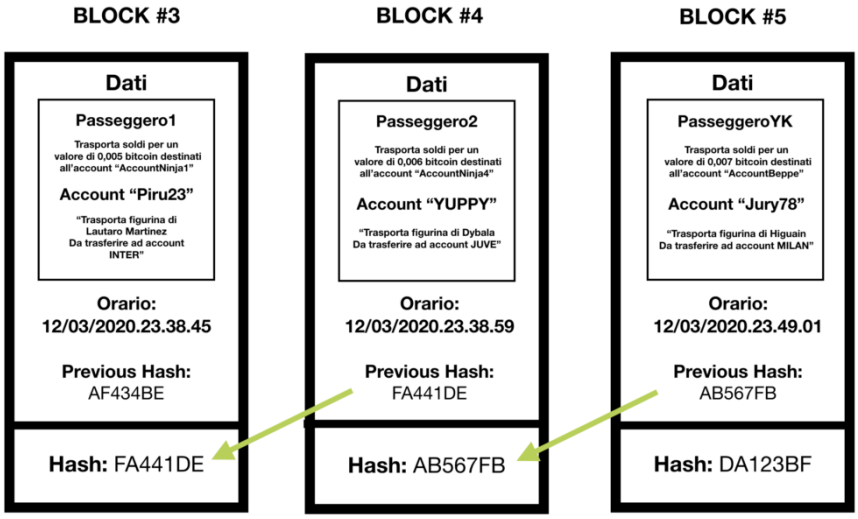


Figura 3 – La struttura del blocco

L'elemento crittografico che garantisce l'immutabilità del blocco, come accennato precedentemente è l'hash, ma cos'è questa stringa? Con questo termine si indica una funzione crittografica che si caratterizza per:

- Irreversibilità (dato l'output è impossibile risalire all'input);
- Determinismo (dato un input, lasciandolo costante l'output sarà sempre uguale);

[4] Fonte: https://knobs.it/blockchain-cose-un-blocco-e-come-fatto/.

- Lunghezza fissa (dipende dalla tipologia, l'SHA-256 ha 256 bit);
- Effetto valanga (una piccola variazione in input produce un'enorme variazione in output).

Queste caratteristiche garantiscono che un blocco verificato e inserito nella blockchain resti immutabile in eterno. Il meccanismo che conferisce alla catena, la caratteristica di immutabilità, è tratto più nel dettaglio nel paragrafo *"immutabilità della blockchain"*.

1.1.5 Le caratteristiche principali della blockchain

1.1.5.1 Decentralizzazione e trasparenza

Una delle principali caratteristiche della blockchain è senza alcun dubbio la decentralizzazione. Per capire bene cosa significhi questo termine e quali conseguenze porta con sé, è opportuno fare un confronto con un sistema centralizzato, come quello finanziario attuale. Il centro del sistema attuale è la BCE che si occupa di gestire le transazioni, prendere decisioni e verificare tutto ciò che riguarda la valuta fiat: l'euro. Tutti i dati sono tenuti in un database centrale gestito dalla banca stessa, per questo è necessaria una grande fiducia nei confronti del corretto operato della BCE, da parte di tutti gli attori del sistema economico-finanziario. La rivoluzione della blockchain consiste nel rompere totalmente questo paradigma, per passare ad una gestione **decentralizzata**, ovvero condivisa da tutti i nodi della rete. In questa tecnologia non esiste più un ente centrale attraverso cui devono passare le informazioni, dotato del potere di prendere decisioni su di esse, ma le informazioni vengono condivise tra tutti i nodi della rete. Una volta che queste sono state verificate e approvate, vengono registrate in un blocco e aggiunte alla blockchain. Questa catena di blocchi viene poi inviata a tutti i nodi della rete e grazie ad una serie di algoritmi crittografici diviene immutabile ed eterna. La blockchain è quindi salvata sui server dei milioni di nodi che vi partecipano ed è consultabile on-line da chiunque voglia farlo. Poiché i dati su di essa salvati sono immutabili, è possibile osservare qualsiasi operazione svolta su di essa, indipendentemente da quanto è datata. In questo modo è garantita anche la **trasparenza** delle operazioni. La principale differenza risiede quindi nella collocazione del potere decisionale. In un modello centralizzato spetta ad un ente centrale, non c'è quindi la necessità di raggiungere il consenso fra più parti, che invece è necessario nella blockchain. Questo problema è noto come "*problema dei generali bizantini"*, e consiste

nel dover condurre più soggetti diversi a prendere la medesima decisione rispetto ad una determinata situazione, nell'ipotesi in cui, tra di essi, sono presenti soggetti che possono fallire e soggetti malevoli che possono cercare di portare gli altri a decisioni errate. Questo problema è stato risolto dalla blockchain tramite gli algoritmi di consenso.

1.1.5.2 L'algoritmo di consenso

> "Un algoritmo di consenso è un meccanismo che permette a utenti o dispositivi di coordinarsi in un contesto distribuito. Deve garantire che tutti gli agenti nel sistema possano concordare su una singola fonte di verità, anche se alcuni agenti falliscono. In altre parole, il sistema deve essere *Byzantine fault-tolerant."*[5]

In un sistema centralizzato l'informazione passa da un punto centrale, il quale ha il potere di decidere su di essa. In un sistema decentralizzato invece, non esiste un punto centrale con il potere decisionale, ma il potere è distribuito tra i vari nodi del sistema e al fine di decidere riguardo un'informazione, è necessario un algoritmo che consenta ai vari utenti di raggiungere il consenso su di essa. Nella blockchain quando si parla di potere, si fa riferimento alla possibilità di decidere riguardo all'aggiunta o meno di un blocco alla catena. Poiché per quanto visto prima, una volta aggiunto un nuovo elemento alla catena, questa non può più essere modificata e diviene immutabile, è fondamentale garantire la correttezza di ciascun blocco che viene aggiunto. Questa funzione è svolta dall'algoritmo di consenso, il quale, oltre a creare un meccanismo che consente di verificare la correttezza del blocco, sceglie anche chi ha il diritto di aggiungere il blocco alla catena una volta che è stato verificato. Quest'ultimo punto non è da sottovalutare, infatti chi ha questo diritto ha un potere enorme: potrebbe decidere quali transazioni il mondo può vedere e quali invece non potranno mai essere viste.

[5] What is a blockchain consensus algorithm, Binance Academy, aggiornato al 18 Agosto 2021, https://academy.binance.com/it/articles/what-is-a-blockchain-consensus-algorithm, consultato il 29 Novembre 2021.

Esistono diversi algoritmi di consenso ma tutti sono caratterizzati da tratti comuni:

- **Richiesta di garanzia** (una sorta di valore) a colui che vuole fare da validatore del blocco, in modo tale da dissuaderlo dall'agire in modo disonesto. Lo "stake" può consistere in potenza computazionale, criptovalute o anche reputazione.

- **Ricompensa** erogata al validatore, in cambio dell'attività svolta. Può essere composta dalle fees delle transazioni del blocco e/o da una quantità fissata di criptovaluta.

- **Trasparenza:** è fondamentale la ricerca della trasparenza dell'attività, in quest'ottica l'algoritmo di consenso dovrebbe rendere costosa la produzione dei blocchi ma molto facile la verifica in modo tale da smascherare eventuali imbrogli.

- Rendere più conveniente seguire le regole rispetto a barare.

I principali metodi di consenso utilizzati sono la Proof of Work (PoW) e la Proof of Stake (PoS).

1.1.5.2.1 Proof of Work e Mining:

È il primo algoritmo di consenso creato ed è adottato attualmente dalle 2 principali blockchain: Bitcoin ed Ethereum, anche se quest'ultima sta per passare ad un consenso di tipo PoS. La garanzia richiesta dalla PoW consiste in potenza computazionale per la risoluzione di complessi problemi matematici, al fine di decretare colui che avrà il diritto di generare un nuovo blocco. Per quanto riguarda la ricompensa, questa è data sia dalle fees delle transazioni incluse nel blocco, sia dall'erogazione di una quantità di criptovaluta a colui che per primo risolve il problema. In questo tipo di consenso è più conveniente agire secondo le regole, rispetto a infrangerle, in quanto il mining richiede costi energetici e investimenti in hardware molto elevati. Pertanto, colui che venisse beccato a trasgredire le regole non verrebbe ricompensato e dovrebbe sostenere costi enormi.

Hash	00000000000000000090ec83aef111e64d18de540effb87c5209160b4ea4501
Confirmations	91,512
Timestamp	2020-03-04 22:10
Height	620208
Miner	F2Pool
Number of Transactions	2,392
Difficulty	15,486,913,440,292.87
Merkle root	731af657f676d7c4db69a092a1f54905ac6ead7d03021ffdfacf6c6f82618351
Version	0x20800000
Bits	387,067,068
Weight	3,998,618 WU
Size	1,332,656 bytes
Nonce	1,833,475,282
Transaction Volume	4107.84315750 BTC
Block Reward	12.50000000 BTC
Fee Reward	0.12933880 BTC

Figura 4 - header di un blocco Bitcoin

Per approfondire il funzionamento della PoW è necessario comprendere e definire i principali elementi che sono presenti nella figura 4[6], che rappresenta l'header di un blocco della blockchain Bitcoin.

- *Merkel root*: hash di tutti gli hash di ogni singola transazione;
- *Version*: indica la versione del software utilizzato;
- *Weight*: misura per confrontare le dimensioni di transazioni diverse tra loro in proporzione al limite della dimensione del blocco;
- ***Difficulty***: valore matematico che esprime la difficoltà nel trovare un hash valido per il blocco. È funzione del numero di zeri iniziali dell'hash;
- ***Bits:*** valore target rispetto al quale l'hash del blocco deve essere minore o uguale, affinché il blocco possa essere verificato e accettato dalla rete. In altre parole, è il numero di zeri;
- ***Nonce***: valore fondamentale in quanto è l'unico valore che il miner può variare al fine di far variare l'hash e trovare così l'hash richiesto dal target;

[6] Fonte: https://www.blockchain.com/btc/block/00000000000000000090ec83aef111e64d18de540effb87c5209160b4ea4501.

Come accennato prima la Proof of Work richiede come garanzia l'impiego di potenza computazionale da parte di colui (miner) che vuole creare (minare) il blocco. In particolare, il miner deve svolgere il cosiddetto **processo di mining.** Questo processo consiste nel trovare l'hash del blocco il cui valore risulti minore o uguale al valore target fissato nel record bits. Tipicamente il valore target prevede un determinato numero di zeri che devono precedere l'hash del blocco. Per la struttura della funzione di hash, non è possibile partendo dall'hash, risalire al contenuto che l'ha generato, ciò significa che l'unico modo di trovare un output che rispetta i vincoli è procedere per tentativi, continuando a variare il Nonce. Maggiore è il numero di 0 e quindi di elementi dell'hash che dobbiamo indovinare maggiore è la difficulty, il numero di nonce da provare e quindi il tempo impiegato per trovarlo.

> Per meglio comprendere questa affermazione è necessario capire come è fatto un hash: la tipologia di funzione usata dalla blockchain è l'SHA-256, cioè una funzione che restituisce in output una sequenza di 256 bit "0" e "1". Questi bit vengono convertiti in 64 caratteri, a ciascuno dei quali vengono quindi assegnati 4 bit, usando così una codifica esadecimale che consente di rappresentare 16 diversi elementi, dallo 0 alla f. Cercare un hash che, ad esempio, sia minore o uguale ad un valore che inizia con dieci "0" e poi tutti "9", significa trovare quell'input che genera un hash in output che ha almeno i primi 40 bit (10 x 4) uguali a quello target. La probabilità di trovare un tale valore scegliendo a caso il nonce, tanto più bassa quanto è maggiore il numero di zeri. Il numero di tentativi con diversi input che bisogna fare, prima di arrivare al risultato cercato e quindi il tempo impiegato, crescono al crescere del numero di zeri.
>
> Un esempio numerico che chiarifica il concetto è il seguente: si immagini di avere un'ampolla con 10.000 bigliettini, ciascuno dei quali contiene un numero, da 1 a 10.000. Bisogna pescare un biglietto e se il numero estratto è inferiore a 100, si vince una bicicletta. La probabilità che questo possa avvenire è 100 su 10.000, ovvero l'1%. Se il regolamento cambia e, al fine di vincere, è necessario pescare un numero minore di 10, le

probabilità di farlo crollano allo 0,1%. Poiché in formato binario, più sono gli zeri iniziali, più il numero è piccolo, appare evidente che al crescere del numero di “0”, la probabilità di scegliere il nonce corretto si riducono. Questo è il meccanismo attraverso il quale viene regolata la difficoltà di minare un blocco in alcune blockchain PoW, come quella di Bitcoin.

Il motivo per il quale, al fine di variare l’output l’unico modo possibile è agire sul nonce, è che tutti gli altri dati contenuti nel blocco sono già determinati e invariabili (non posso, ad esempio, modificare le transazioni o il timestamp, o il PrevHash). Il primo miner che risolve il problema riceve una ricompensa in criptovaluta e le fees relative alle transazioni incluse nel blocco, dopo che anche tutti gli altri nodi della rete hanno verificato l’intera blockchain e il blocco in questione, questo è stato aggiunto alla blockchain e una copia aggiornata di quest’ultima è stata scaricata dai nodi. La sicurezza nella PoW è garantita dalla funzione di hash: il calcolo del valore che rispetta il target richiede tantissimo tempo e tentativi, mentre la verifica di correttezza è immediata, infatti, dato il nonce e gli altri dati è possibile calcolare l’hash in una frazione di tempo infinitesimale.

1.1.5.2.2 Proof of Stake

L’algoritmo di consenso PoS nasce come alternativa al PoW. In questo modello di consenso il minatore viene rimpiazzato dal validatore, il mining lascia il posto allo staking (depositare la criptovaluta in un determinato portafoglio) e la criptovaluta non viene più minata ma bensì forgiata. Al contrario di quanto avviene nel PoW, non è richiesto un hardware in grado di apportare grande potenza di calcolo, in quanto la scelta del validatore del blocco avviene tramite un’estrazione. Questa è effettuata tra tutti coloro che hanno messo in staking, ovvero depositato presso un determinato wallet, le proprie monete. La probabilità di essere selezionati dipende da molti criteri, il principale è la quantità di criptovaluta depositata. Questa funge da garanzia e da incentivo a comportarsi in modo onesto. Qualora un validatore cercasse di comportarsi in modo scorretto perderebbe il proprio deposito. La ricompensa a colui che valida il blocco è costituita dalle sole fees delle transazioni in esso contenute e la sicurezza è garantita da due principali elementi: diversificazione dei criteri di scelta e facilità per i

nodi di verificare la correttezza dell'operato del validatore. I due sono strettamente collegati, infatti, essendo i criteri di scelta del validatore molteplici, è vero che chi ha più monete depositate ha più probabilità di essere estratto, ma non può averne la certezza, quindi, il validatore non può essere sempre lo stesso (anche perché verrebbe meno la decentralizzazione della blockchain). Poiché ad un validatore ne segue uno diverso, questo verificherà in modo semplice l'operato del precedente e qualora risulti scorretto perderà le criptovalute depositate.

1.1.5.2.3 PoW o PoS: confronto

In conclusione, è possibile affermare che non esiste l'algoritmo di consenso perfetto, ma ognuno ha dei pregi e dei difetti. Nelle seguenti righe è presente un confronto tra i limiti di Pos e PoW.

I limiti della PoW:

- **Consumo elettrico:** per come la Proof of Work funziona, il dispendio energetico nel calcolo dell'hash è molto elevato.

- **Vulnerabilità al 51% attack:** qualora un miner riuscisse a detenere il controllo del 51% della potenza computazionale riuscirebbe di fatto a controllare la blockchain. Per quanto riguarda invece la PoS un validatore dovrebbe detenere il controllo del 51% delle monete e questo è molto difficile, sia perché in caso di grande domanda il prezzo della moneta salirebbe molto, sia perché pochi sceglierebbero di utilizzare un sistema che è risaputo essere controllato da un'unica persona.

I Limiti della PoS:

- **Rich get richer:** più monete si hanno e si possono depositare, più sono le ricompense ottenute (pagate in criptovaluta) e quindi più monete si guadagnano.

- **Tendenza alla Centralizzazione:** un sistema come la PoS, in cui la probabilità di essere selezionati come validatore è direttamente proporzionale alla quantità di

moneta che si deposita e nei quali generalmente, sono previsti dei limiti minimi di ingresso, piccoli detentori di moneta tenderanno a delegare le proprie monete a detentori maggiori, accentrando di fatto il potere nelle mani di pochi grandi validatori. In quest'ottica il vantaggio maggiore potrebbe essere tratto dai grandi exchange, questi infatti consentono ai loro utilizzatori di depositare le proprie criptovalute in staking pools, con il rischio che si generi un sistema centralizzato in cui il controllo è nelle mani degli exchange che diventerebbero le "nuove banche". Per quanto riguarda la Proof of Work, anche in questa tipologia di consenso si sta verificando una sorta di accentramento dovuto ai grandi costi energetici e di hardware per il mining, che ha portato alla creazione di molto mining pools. Tuttavia, il rischio di centralizzazione sembra più remoto per questa tipologia rispetto alla Proof of Stake.

1.1.5.3 Sicurezza della blockchain

Come visto sopra, la blockchain offre sicurezza e inalterabilità dei dati in essa contenuti, tramite l'utilizzo della crittografia. Inoltre, offre anche una soluzione al problema del consenso distribuito, tramite l'adozione di opportuni algoritmi. Tuttavia, è necessario risolvere un altro problema, quello dell'**autenticità e integrità delle transazioni,** ovvero garantire che ciascun utente possa spendere solo le proprie criptovalute e che la quantità che decide di spendere non venga in alcun modo alterata. La soluzione è data dalla **crittografia a chiave pubblica**. Per capire di cosa si tratta è importante chiarire inizialmente cosa è la crittografia, capire il funzionamento della crittografia a chiave privata, analizzare le modalità di applicazione del sistema a chiave pubblica e solo alla fine, nel paragrafo "*Le transazioni"*, potrà essere analizzato nello specifico come avviene una transazione di criptovaluta.

1.1.5.3.1 Crittografia a chiave privata: Il cifrario di Cesare

Quando si parla di crittografia si fa riferimento a una serie di tecniche che consentono di "nascondere" il contenuto di un messaggio e comunicarlo agli altri attraverso un canale non sicuro, nel quale oltre che dal destinatario, il messaggio potrebbe essere intercettato da parti estranee. Affinché questo possa avvenire in modo sicuro ed

efficace è necessario che il sistema di cifratura sia dotato di un **algoritmo** e di una **chiave** (o due, a seconda del sistema che si utilizza). L'algoritmo è l'insieme dei "passaggi" da seguire per cifrare o decifrare il messaggio originario, mentre la **chiave** rappresenta quell'informazione senza la quale non è possibile decifrare il messaggio anche se si è a conoscenza dell'**algoritmo** utilizzato. Per chiarire meglio di cosa si tratta è possibile fare un esempio: **Il Cifrario di Cesare** *(figura 5[7])***.** Questo sistema è stato uno dei primi metodi di crittografia a chiave privata e fu inventato da Giulio Cesare. Il funzionamento consisteva nell'associare a ciascuna lettera del messaggio originale, la lettera dell'alfabeto che si otteneva traslando di x posizioni la lettera originaria. Per ricondursi al concetto esposto prima, l'algoritmo è: "associa alla lettera in posizione x, quella in posizione x + chiave", la chiave è il numero di posti di traslazione. Chi conosce l'algoritmo ma non la chiave non può decifrare il messaggio.

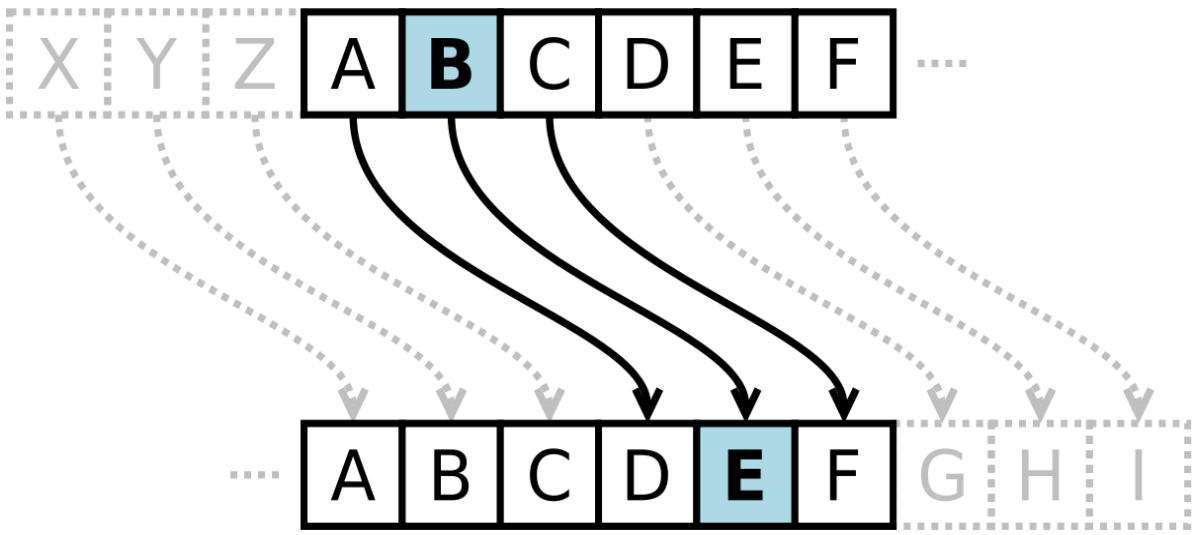


Figura 5 - Cifrario di Cesare in Chiave 3

Volendo applicare un sistema di questo tipo alla blockchain ci si troverebbe davanti a due grandi problemi. Il primo è la *vulnerabilità della chiave*, in quanto al più, posso disporre di un numero di chiavi pari al numero di lettere nell'alfabeto e quindi sarebbe molto facile risalire alla chiave noto l'algoritmo. Il secondo è rappresentato dalla necessità di comunicare la chiave a chi riceve il messaggio e deve decifrarlo. Questa, infatti, deve essere comunicata in anticipo, perché se il canale di comunicazione è non sicuro, non è possibile farlo attraverso esso. Tuttavia, non sempre è possibile comunicare la chiave anticipatamente, basti pensare a due persone che non si conoscono,

[7] Fonte: https://it.wikipedia.org/wiki/Cifrario_di_Cesare#/media/File:Caesar3.svg. Cepheus.

abitano in parti diverse del mondo e hanno bisogno di comunicare. Per risolvere questo problema si è passati ad un **sistema di cifratura a chiave pubblica** (o doppia chiave).

1.1.5.3.2 Crittografia a chiave pubblica

Questo sistema si basa su due chiavi, una chiave pubblica e una chiave privata dotate delle seguenti caratteristiche:

- La chiave pubblica discende dalla privata e non è possibile, data la chiave pubblica risalire a quella privata;
- Un messaggio cifrato con chiave pubblica può essere letto con chiave privata e viceversa;

- La chiave pubblica viene comunicata a tutti, mentre quella privata va tenuta al sicuro e non va diffusa per nessun motivo.

Figura 6 - Crittografia a chiave pubblica A → B.

Nella *figura 6*[8] è riportato il funzionamento di questo sistema quando due soggetti, A e B vogliono scambiarsi un'informazione tramite la rete. A scrive il messaggio, cifra il messaggio usando la chiave pubblica di B che è facilmente reperibile in quanto condivisa da B, ne fuoriesce il testo criptato. B riceve il testo e per le caratteristiche delle chiavi potrà decifrarlo usando la propria chiave privata e avere la certezza che nessun altro potrà farlo a meno che sia in possesso di tale chiave (**riservatezza del**

[8] Fonte: https://www.criptoinvestire.com/come-funziona-la-crittografia-nelle-blockchain.html.

messaggio). Se invece fosse B a dover comunicare qualcosa ad A basterebbe svolgere il passaggio inverso, riportato in *figura 7*[9]*.*

Figura 7 - Crittografia a chiave pubblica B --> A

Per usare una metafora, la chiave pubblica può essere vista come un lucchetto e la chiave privata come la chiave che apre il lucchetto. A potrebbe fabbricare tanti lucchetti e distribuirli, a quel punto B potrebbe prendere una scatola, metterci un messaggio e chiuderla con il lucchetto. La scatola potrebbe essere presa da chiunque, ma solo chi possiede la chiave che lo apre, cioè A, può leggere il contenuto del messaggio. Quello appena illustrato è il modo più semplice di applicazione della crittografia a doppia chiave e mostra come è possibile garantire la **riservatezza** di un messaggio. Tuttavia, questo metodo crittografico può fare molto di più "giocando con le chiavi". I problemi a cui è possibile dare una soluzione sono **autenticità** (garantire che il mittente del messaggio sia realmente A) **e integrità** (garantire che il messaggio non sia stato in alcun modo manomesso)**.** La loro risoluzione è possibile tramite le modalità illustrate nella *figura 8*[10]*.*

[9] Fonte: https://www.criptoinvestire.com/come-funziona-la-crittografia-nelle-blockchain.html.
[10] Elaborata su: https://www.alnitak74.net/articoli/SicurezzaInformatica/crittografia.html.

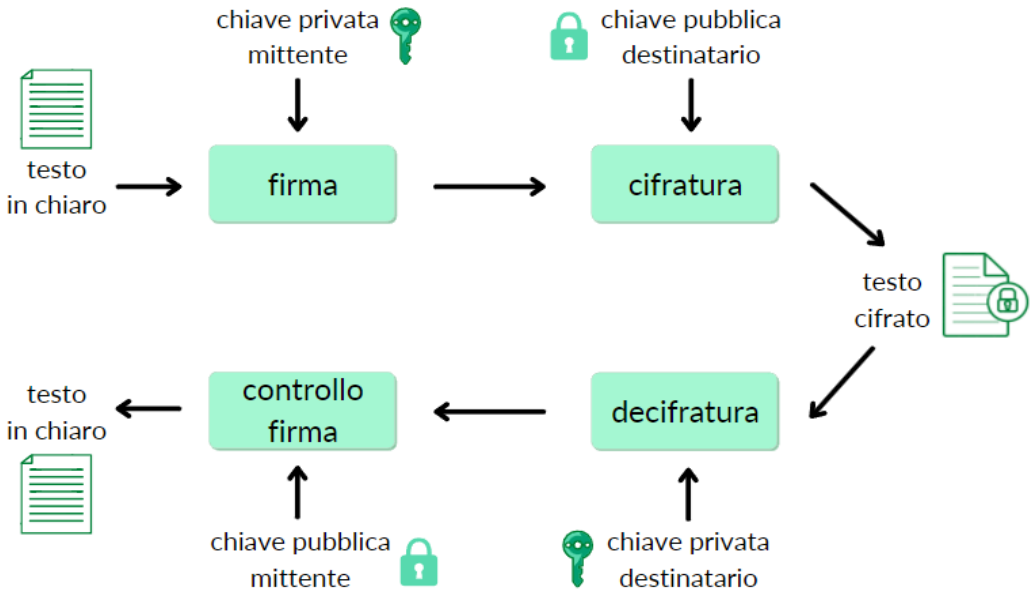


Figura 8 - Cifratura complessa a chiave pubblica

A cifra il proprio messaggio con la propria chiave privata e successivamente cifra il tutto usando la chiave pubblica di B. Quando il messaggio arriva a B, questo lo apre innanzitutto usando la propria chiave privata e successivamente apre la parte risultante usando la chiave pubblica di A. In questo modo si ha la garanzia che solo A può aver inviato quel messaggio, perché è l'unico ad avere la chiave privata usata per cifrarlo. Contemporaneamente si mantiene la riservatezza perché solo B può aprire il messaggio cifrato con la chiave pubblica B. Per ultima cosa viene garantita anche l'integrità del messaggio, perché chiunque l'avesse voluto modificare avrebbe dovuto essere a conoscenza della chiave privata di A.

1.1.5.4 Immutabilità della blockchain

La blockchain è crittograficamente immutabile, ovvero grazie alla crittografia in essa implementata, è quasi impossibile alterare le informazioni nella catena, una volta che vengono verificate dai nodi della rete. Questo avviene grazie alla funzione di hash, che lega indissolubilmente i blocchi contenenti le transazioni. Nel paragrafo "Il Blocco" è trattata la struttura del blocco della catena ed è fondamentale per capirne l'immutabilità. Riassumendo, ciascun blocco è costituito da un insieme di dati e, al fine di poter passare al processo di verifica da parte dei nodi, con conseguente aggiunta alla blockchain, deve preventivamente essere minato. Minare un blocco significa trovarne

l'hash e poiché in ciascun blocco viene incluso l'hash del blocco precedente si crea un legame che non può più essere alterato. Per le caratteristiche della funzione di hash, infatti, variando l'input varierebbe anche l'hash in output. Ad esempio, supponiamo esista una blockchain con 101 blocchi, dal numero 0 al numero 100. Se qualcuno provasse a modificare il contenuto del blocco 90, eliminando ad esempio una transazione, il suo hash cambierebbe. Ma allora anche l'hash del blocco 91 dovrebbe cambiare, perché ha in input l'hash del blocco 90. Ogni cambiamento verrebbe quindi immediatamente rilevato e corretto. Questo meccanismo crittografico garantisce quindi l'immutabilità della blockchain.

1.1.6 Le transazioni

Nella sezione "*Sicurezza della blockchain"* è esposto il concetto di crittografia e sono analizzati i sistemi a chiave pubblica e chiave privata. La crittografia usata per garantire le transazioni sulla blockchain è quella a chiave pubblica, la quale però viene implementata in un modo leggermente diverso da quelli visti. Infatti, l'obiettivo non è più quello di "nascondere" un messaggio, ma quello di garantire che una transazione sia effettuata dal reale proprietario delle criptovalute in oggetto e che questa non possa essere alterata. I messaggi nel sistema Blockchain, quindi, vengono inviati non criptati, e in questo sistema la crittografia viene utilizzata solo per firmare digitalmente i messaggi, ovvero le transazioni.

Per inviare un ordine di transazione: M (messaggio), il mittente:

- "scrive il messaggio";
- esegue l'Hash del messaggio: H = SHA256(M)
- cifra H con la sua chiave privata per ottenere la firma: S = encrypt(H ; Kpriv)
- invia la firma S, il messaggio M, e la sua chiave pubblica Kpub (dalla Kpub discende l'indirizzo tramite l'hash function)

Per verificare che la firma S sia valida per la transazione M, i nodi:

- eseguono l'Hash del messaggio M: H = SHA256(M)

- decifrano S con la chiave pubblica del mittente: H’ = decrypt(S ; Kpub)
- verificano che H = H’. Se l’equazione è vera allora la firma è valida.[11]

In questo modo si ha la garanzia che la transazione sia stata effettuata realmente dal mittente, in quanto questo è l’unico proprietario della propria chiave privata e che il suo contenuto sia immutato. Infatti, cambiandone il contenuto verrebbe variato l’hash e quindi invalidata la firma S, composta dall’hash cifrato in chiave privata. Questo è il medesimo meccanismo di implementazione della **firma digitale** dei documenti *(figura 9).*[12]

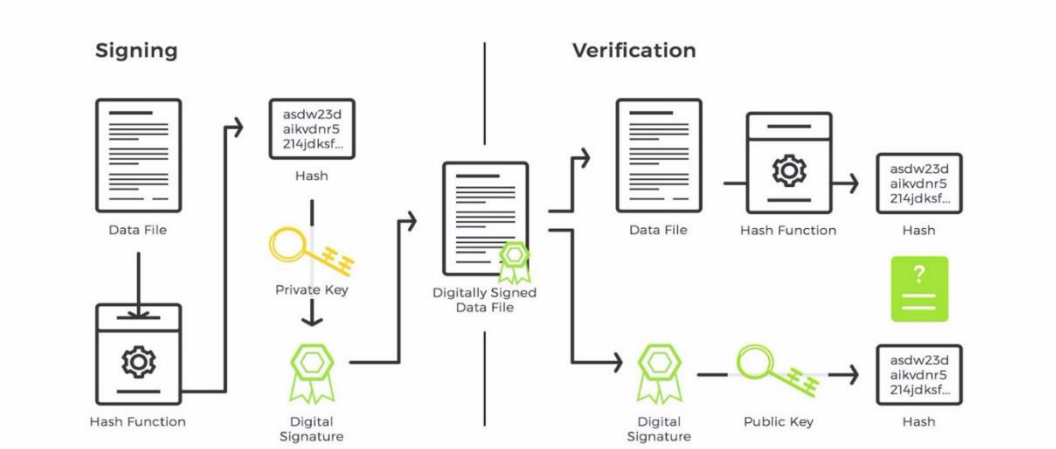


Figura 9 - Rappresentazione processo firma digitale

1.1.7 I nodi

Facendo un piccolo riassunto, finora si è visto che la blockchain è una tecnologia che permette di salvare delle informazioni, che vengono suddivise in blocchi, sottoposte ad una procedura di verifica (consenso) da parte dei **nodi** e infine aggiunta a questa catena di blocchi (registro) condivisa, decentralizzata e crittograficamente immutabile. A tal proposito vengono trattati nei precedenti capitoli cosa è un blocco, cosa è il consenso, cosa sono le informazioni (con riferimento particolare alle transazioni) e come funziona la crittografia alla base (hash e chiave pubblica). Resta da capire cosa sono i **nodi**.

[11] Firma di una transazione in bitcoin, 10bitcoin, http://www.10bitcoin.it/firma-transazione-bitcoin/, consultato il 01/12/2021.
[12] Fonte: https://knobs.it/chiave-pubblica-chiave-privata/.

> “Un nodo è, in generale, un punto di connessione fisico o virtuale dove è possibile creare, inviare e ricevere tutti i tipi di dati e informazioni. Quindi, dal punto di vista della tecnologia blockchain, i nodi sono costituiti da tutti quei computer che sono connessi alla rete e che eseguono il software responsabile di tutto il suo funzionamento”.[13]

Data la definizione generale di nodo di una blockchain, è importante sottolineare che esistono molti tipi diversi di blockchain e, in ciascuna di esse, i nodi possono avere funzioni diverse. Parlando della rete Bitcoin, diventare un nodo è facile e per farlo basta scaricare e avviare il software **Bitcoin Core** sul proprio computer. In questa rete esistono diverse tipologie di nodo:

- **Full Nodes**: sono i nodi che garantiscono **sicurezza** e **robustezza** all’intera rete. Questi scaricano e memorizzano una copia sempre aggiornata dell’intera Blockchain Bitcoin, verificano le transazioni tramite le regole del consenso e trasmettono le transazioni e i blocchi. Inoltre, controllano che le regole del protocollo bitcoin siano rispettate. Ad esempio, verificano che la dimensione del blocco sia minore di 1MB, che le firme delle transazioni siano valide e che non ci siano problemi di double spending. In caso contrario rigettano il blocco e impediscono la sua aggiunta alla blockchain. È necessario siano dotati di un software come Bitcoin core che si occupa di quanto detto. Essere un Full Node ha i seguenti requisiti:

    - Desktop o laptop con una versione recente di Windows, Mac OS X o Linux;
    - 200GB di spazio libero sul disco;
    - 2GB di memoria (RAM);
    - Connessione a internet ad alta velocità con upload di almeno 50 kB/s;
    - Connessione illimitata o con alti limiti per l’upload. I full nodes possono raggiungere o superare 200 GB/mese per l’upload e 20 GB/mese per il download. Inoltre, c’è la necessità di scaricare ~200GB nel primo utilizzo del full node;
    - Essere attivo almeno sei ore al giorno;

[13] Cos’è un nodo, Bit2me Academy, https://academy.bit2me.com/it/cos%27%C3%A8-un-nodo/, consultato il 02/12/2021.

Si contano circa 9700 full nodes pubblici attivi, tuttavia sono presenti anche molti nodi nascosti, ovvero nodi che usano VPN o browser nascosti come Tor.

- **Super Nodes:** sono full nodes visibili pubblicamente. Sono sempre disponibili 24/7 a chiunque voglia comunicare. Sono fondamentali in quanto trasmettono l'informazione all'interno della rete, fungendo sia da fonte di informazioni, sia da bridge tra nodi. È probabile che un Super Node richieda più potenza di calcolo di un nodo nascosto.

- **Nodi di data mining:** sono dei nodi completi i quali, oltre ad eseguire Bitcoin core eseguono anche il software di Mining, come ad esempio BTCMiner. Possono essere rappresentati da una solo persona (solo miner) oppure da gruppi che si uniscono e solo l'amministratore si registra come nodo (mining pools).

- **Nodi Leggeri:** sono nodi che non scaricano l'intera blockchain e che ricevono informazioni da verificare dai super nodi. Non contribuiscono quindi alla sicurezza della rete. Essendo leggeri sono eseguiti su tablet e smartphone.

È fondamentale la differenza tra mining nodes e full mining nodes. Infatti, i mining nodes acquistano costose attrezzatture hardware per effettuare il mining. Una volta trovato l'hash del blocco, questo potrà essere aggiunto alla blockchain solo dopo la verifica e l'approvazione degli altri full nodes.

Altre blockchain fanno uso del **Master Nodes**, che oltre alle funzioni dei nodi sopra citati ha anche diritti di voto e svolge altre funzioni nella blockchain.

1.1.8 Cos'è il Fork in una blockchain

Molte volte in ambito blockchain si sente parlare di Fork. Tecnicamente parlando non è altro che una modifica al codice del software che i nodi scaricano nel proprio computer, fatto con l'obiettivo di migliorare il protocollo della criptovaluta. La conseguenza a questa modifica è che viene generata una nuova versione della blockchain. Questa può essere compatibile o meno con la versione precedente a seconda dell'importanza

della modifica che viene apportata. Per fare un esempio pratico: in Bitcoin la comunità di nodi può proporre delle modifiche da apportare a Bitcoin Core. Se queste modifiche vengono accettate da parte del team di Bitcoin Core, il software viene aggiornato e i nodi possono decidere se scaricarne o meno la versione aggiornata. Non tutti gli aggiornamenti sono fondamentali, quindi non è richiesto ai nodi un cambiamento continuo della versione di Bitcoin Core. Ci sono però modifiche così importanti da richiedere un aggiornamento del software per continuare a lavorare sulla nuova blockchain. Proprio in questi due casi si verifica il fork, che può essere **soft fork** o **hard fork.**

Figura 10 - Soft fork nodi

Il **soft fork** si verifica quando l'aggiornamento resta retrocompatibile con la vecchia blockchain. In questo caso i nodi aggiornati e quelli non aggiornati posso continuare a comunicare. Fino a quando tutti i nodi non sono aggiornati, coesistono due blockchain (*figura 11*[14]), una aggiornata e una non aggiornata. Quest'ultima tenderà a sparire nel tempo, quando tutti i nodi faranno l'upgrade alla versione successiva del sistema. Nella *figura 10*[15], in giallo sono rappresentati i nodi vecchi, mentre in verde quelli aggiornati. Come si può vedere, la comunicazione fra loro è possibile.

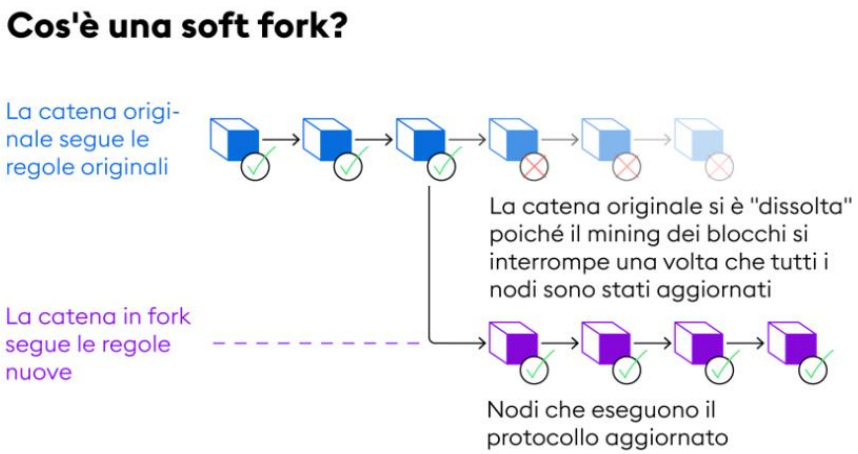


Figura 11 - Soft fork

[14] Fonte: https://www.bitpanda.com/academy/it/lezioni/come-funzionano-le-hard-fork-e-le-soft-fork/.
[15] Fonte: https://academy.binance.com/it/articles/hard-forks-and-soft-forks.

L'**hard fork** si verifica quando l'aggiornamento è fondamentale per il funzionamento della blockchain. In questo caso i nodi aggiornati e quelli che non lo sono, non possono più scambiarsi informazioni (*figura 12*[16]). Si creeranno due blockchain diverse che continueranno ad esistere contemporaneamente (*figura 13*[17]). La prima blockchain utilizza la versione vecchia del software, la seconda usa la versione aggiornata e sarà seguita dai nodi aggiornati. Bitcoin Cash, hard fork di Bitcoin, mostra come la catena originaria possa tranquillamente continuare a vivere. Chi crede nel nuovo progetto aggiorna il software, mentre chi è contrario continua a lavorare con il software vecchio. Nell'hard fork ciò che avviene, è che chi detiene token della valuta sulla blockchain originaria, troverà, al momento del fork, una pari quantità di token della nuova criptovaluta gratuitamente. Per questo motivo l'hard fork è oggetto di forti interessi speculativi.

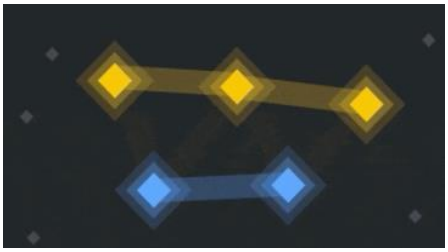


Figura 12 - Hard fork nodi

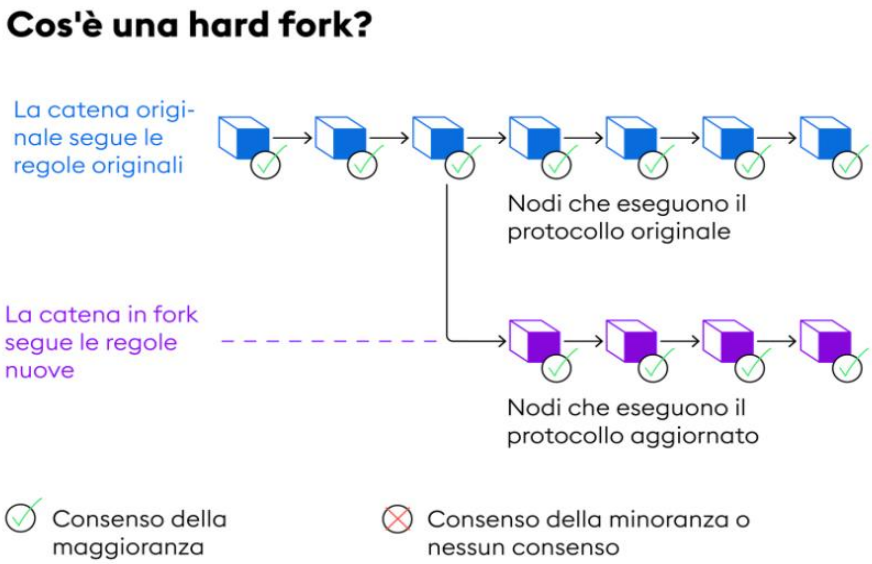


Figura 13 - Hard fork

1.1.9 Errori: Orphan block e Stale block

La blockchain risulta essere una tecnologia molto stabile e apparentemente priva di errori. Tuttavia, possono capitare delle situazioni, dovute principalmente a ritardi della

[16] Fonte: https://academy.binance.com/it/articles/hard-forks-and-soft-forks.
[17] Fonte: https://www.bitpanda.com/academy/it/lezioni/come-funzionano-le-hard-fork-e-le-soft-fork/.

rete, che possono portare a dei malfunzionamenti. I due principali errori sono **stale block** e **orphan block.** Lo **stale block** si verifica quando due blocchi vengono minati quasi contemporaneamente. In questo caso il miner 1 mina il blocco A numero 234000 e lo passa ai nodi per essere verificato. Mentre non è ancora stato processato da tutti i nodi, il miner B mina il blocco B con lo stesso numero 234000 e lo passa ai nodi. Ci si trova in una situazione nella quale una parte dei nodi lavora sul primo blocco e una parte sul secondo. Successivamente, un altro miner mina il blocco C numero 234001 collegato a uno dei due precedenti, ad esempio A. In questo caso il blocco C (dopo la verifica dei nodi) viene aggiunto alla catena. Poiché è sempre la catena più lunga a prevalere, la catena A-C diventa quella ufficiale e il blocco B viene ignorato. Le transazioni incluse in B non vengono perse, ma recuperate successivamente. Colui che ha creato tale blocco non avrà diritto a nessuna ricompensa nel sistema Bitcoin, mentre avrà comunque una reward in Ethereum.

Il caso dello stale block è anche una dimostrazione pratica di come l'algoritmo di consenso e la regola di prevalenza della catena più lunga, risolvano il problema dei generali Bizantini, facendo convergere l'intero sistema di nodi sulla scelta unanime di quale è la blockchain principale.

Un **Orphan block** si verifica quando un blocco viene minato, ma i blocchi parenti non sono ancora stati aggiunti alla catena. Una situazione di questo tipo può avvenire in caso di ritardi nel processo di verifica, ma dal 2015, in Bitcoin non è più possibile grazie ad un aggiornamento del software. Questi blocchi comunque non andavano persi, ma conservati in dei pools di blocchi orfani e recuperati successivamente alla convalida dei blocchi parenti. Nella *figura 14*[18] sono rappresentate le due situazioni di errore.

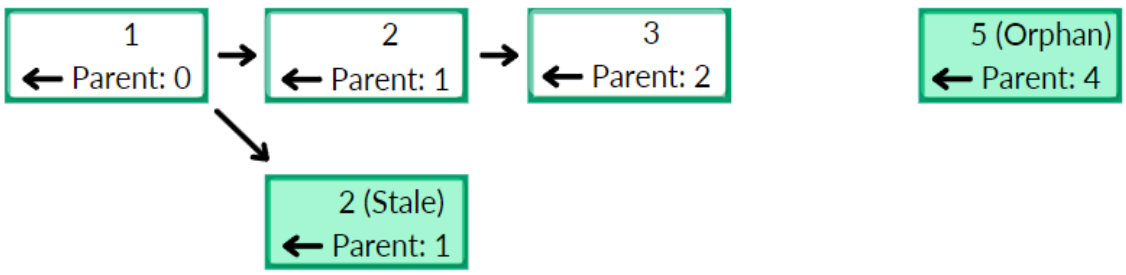


Figura 14 - Stale e Orphan block

[18] Fonte: https://medium.com/@blockchain101/confirmation-times-stale-blocks-reverse-transaction-double-spending-and-the-51-attack-in-simple-bd65a32d32b3.

1.1.10 Attacchi alla rete

Per quanto la blockchain riesca a risolvere molteplici problemi e abbia dimostrato di essere in grado di garantire una grande efficienza e sicurezza, non è priva di rischi. Infatti, ci sono degli attacchi a cui non è immune. Di seguito sono riportati i principali.

- **51% Attack:** questa tipologia di attacco è stata già accennata nei limiti del Proof of Work. È infatti un attacco che caratterizza solo tale algoritmo di consenso in quanto in una blockchain PoS, non è possibile. Questo attacco si verifica quando un miner (o un insieme di miners in accordo) riesce a prendere possesso del 51% della potenza di calcolo della rete. In questo caso sarebbe in grado di minare blocchi più velocemente di chiunque altro e quindi, sarebbe di fatto in grado di governare la blockchain. Un'applicazione concreta di ciò che potrebbe fare è rappresentata dal **double spending**, ovvero dalla possibilità per il miner malevolo, di poter spendere soldi che aveva già precedentemente speso. Questo tipo di attacco si verifica nei seguenti passi: il minatore dotato del 51% di hashrate si disconnette dalla rete e inizia a minare la propria copia della blockchain. Questa sarà collegata all'hash dell'ultimo blocco disponibile nella chain principale, che chiamiamo P. A questo punto effettua una transazione sulla chain principale, ad esempio acquista una Ferrari e riceve la macchina. Nel frattempo, sta minando la propria blockchain personale, la quale sarà formata da un numero di blocchi maggiore rispetto a quella pubblica minata dagli altri minatori. A questo punto il miner "cattivo" pubblica la propria copia della blockchain, che essendo più lunga verrà considerata quella giusta, perché ha richiesto più lavoro. Questa verrà verificata e aggiunta alla chain principale, facendo scomparire la transazione che aveva effettuato prima. Il truffatore si trova adesso oltre che con la Ferrari, anche con i soldi che aveva già speso. Con il 51% attack, oltre al double spending è possibile bloccare transazioni o addirittura raggiungere il "monopolio di mining". Infatti, con il 51% della potenza di calcolo, è possibile ottenere tutte le ricompense, rendendo inutile il mining per i restanti minatori.

  Un attacco di questo tipo è possibile solo per chain piccole, per quelle grandi come Bitcoin sarebbe estremamente costoso e non redditizio, poiché questo causerebbe un crollo del valore della criptovaluta stessa.

- **Attacco DDoS**

  “Un attacco DDoS (Direct Denial of Service) è un tentativo di paralizzare il nodo di una blockchain, inondandolo con un volume elevato di traffico.” [19]È un attacco molto comune in quanto di facile realizzazione e coinvolge vari ambiti informatici, non solo la blockchain. Ad esempio, nel caso di un sito Web, viene inviato al server un numero enorme di richieste per un determinato periodo di tempo, impedendo alle richieste legittime di ricevere le risorse di cui hanno bisogno. Nel caso di un nodo blockchain, vengono inviati enormi volumi di transazioni piccole o non valide allo scopo di impedire l’elaborazione di transazioni legittime. Le blockchain più diffuse sono spesso bersagliate da attacchi di questo tipo, ma adottano delle contromisure valide che permettono di annullarne, o comunque ridurne gli effetti. Il DDoS non comporta alcuna perdita di moneta, ma semplicemente un blocco temporaneo della rete.

- **Ignoranza**

  Nonostante le vulnerabilità mostrate sopra, le blockchain sono per lo più crittograficamente sicuri e a prova di hacker. Il pericolo più grande è rappresentato dagli esseri umani, infatti, milioni e milioni di criptovalute sono continuamente rubate tramite diversi stratagemmi online. I principali furti avvengono quando le persone affidano le proprie password o le proprie chiavi private a siti online con standard di sicurezza nulli, per la paura di dimenticarsele. In altri casi, (che sembrano assurdi ma che sono più frequenti di quanto si possa credere) le persone, ignorando l’importanza della chiave privata, la cedono a estranei che le contattano sui social con la promessa di farle diventare milionarie. Quest’ultimo punto fa capire quanta mancanza di conoscenza ci sia sulla blockchain, sulla crittografia e in generale sulla gestione in sicurezza delle proprie criptovalute. Oltre al miglioramento dal punto di vista tecnico è quindi (e soprattutto) fondamentale una corretta divulgazione e formazione pratica all’interno di scuole, università e pubblica amministrazione. È inoltre necessaria una semplificazione delle procedure per accedere a questo mondo, prima che si possa pensare ad una adozione di massa.

[19] Valeri M., *Attacchi alla blockchain: cause, conseguenze e contromisure,* in “Malware e attacchi hacker, Cybersecurity360, 1 Marzo 2019, https://www.cybersecurity360.it/nuove-minacce/attacchi-alla-blockchain-cause-conseguenze-e-contromisure/, consultato il 30/11/2021.

1.1.11 La blockchain nel mondo reale

Finora la Blockchain è stata associata esclusivamente alle criptovalute, ma solo perché l'impulso principale alla sua diffusione è avvenuto con la nascita di Bitcoin e grazie al contesto economico-finanziario del 2008. Non bisogna però commettere l'errore di considerare la blockchain e Bitcoin come un'unica cosa. La blockchain è una tecnologia a sé stante e grazie alle sue caratteristiche, trova molti altri ambiti di applicazione oltre a quello delle criptovalute:

- **Settore trasporti**: per capire come la blockchain potrebbe essere applicata a questo settore è possibile fare degli esempi concreti. Il primo riguarda il *noleggio di un'automobile:* il cliente compra l'automobile e inizia a pagare le rate. Se questa operazione fosse gestita tramite smart contract su blockchain, qualora il cliente non paghi una rata lo smart contract ordinerebbe all'auto di non mettersi in moto e quindi il cliente non la potrebbe utilizzare. Un ulteriore esempio può essere questo: un cliente compra un biglietto del treno delle ore 9:00. Lo smart contract congela l'importo e rilascia il biglietto al cliente. Quando il treno arriva, alle 9:00, i soldi vengono inviati alla compagnia. Se invece il treno fa ritardo, verrà sbloccata solo una parte di importo e l'altra restituita al cliente come rimborso per il disservizio. A sua volta, tramite lo smart contract sarebbe possibile per la compagnia del treno, risalire al motivo del ritardo e prendere le contro misure per evitare si verifichi nuovamente.

- **Beneficienza**: le caratteristiche di trasparenza e tracciabilità della blockchain la rendono uno strumento molto valido per scongiurare truffe o errori nelle donazioni. Una delle più importanti iniziative in questa direzione è quella della BCF, Binance Charity Foundation. Binance è uno dei più grandi exchange di criptovalute al mondo e la BCF è un ente no-profit che mira a garantire che il 100% della somma donata in beneficienza arrivi realmente al destinatario finale. Tutto questo è realizzato senza intermediari e quindi con delle fees nulle. Un'altra applicazione di "blockcharity" è quella dell'italiana Helperbit. Questa si occupa di raccogliere fondi in bitcoin per aiutare coloro che sono stati colpiti da calamità naturali, come terremoti e tsunami.

- **Supply Chain:** i network logistici attuali hanno grossi limiti di trasparenza ed efficienza. Questo perché si basano ancora sulla fiducia ed è ancora lontano dal garantire un'integrazione adeguata tra le compagnie e le parti coinvolte. La blockchain può risolvere la gran parte dei problemi e può avere moltissime applicazioni nell'ambito logistico. Potrebbe essere usata per il tracciamento della provenienza, tracciamento dei parametri critici (blockchain e IoT possono tracciare le condizioni dei prodotti durante il trasporto), prevenzione dei prodotti contraffatti (la blockchain consente di tracciare l'origine di ogni parte del prodotto finale).

Questi sono solo alcuni casi di applicazione concreta della blockchain al mondo reale. Altri settori possono infatti essere e-commerce, prova di identità, proprietà intellettuale e raccolta fondi.

1.1.12 I limiti della blockchain

La blockchain è in grado di garantire decentralizzazione, sicurezza e immutabilità di ciò che viene in essa inserito, tuttavia non può verificarne la veridicità. In altre parole, c'è grande difficoltà nel rendere ciò che è **off chain, in chain.** Nulla vieta ad un soggetto malintenzionato di inserire un'informazione errata sulla blockchain e venderla per vera. Questo rappresenta un grosso limite di questa infrastruttura tecnologica. Questo problema viene in parte risolto dagli **oracoli**, dei sistemi che si occupano di inserire dati esterni all'interno della blockchain, tramite procedimenti in grado di rendere immutabile e veritiero l'inserimento dei dati. In questo modo c'è la certezza che ciò che è contenuto nella blockchain è realmente ciò che viene detto essere. Ad esempio, tramite uno smart sensor e quindi l'IoT[20], è possibile verificare senza possibilità di inganno se una porta in un determinato momento era aperta o meno, o se un treno è arrivato in ritardo. Un altro limite sta proprio nel suo grande vantaggio, la decentralizzazione. Per garantire la sicurezza nella blockchain, servono molti nodi che operano nella verifica delle transazioni e nel controllo del rispetto del protocollo. Questo potrebbe rendere la blockchain, nonostante i suoi grandi vantaggi, di difficile implementazione per piccole società che non dispongono di molti dispositivi connessi che

[20] IoT: Internet of Things. Termine che indica la capacità degli oggetti (things) di creare una rete di comunicazione tra di loro.

possono funzionare da nodi. Un terzo grosso limite è dato dalla difficoltà di creazione e implementazione di tale tecnologia. Sono infatti necessarie grandi conoscenze in ambito informatico e tecnologico per l'utilizzo di un sistema basato su blockchain e attualmente non ci sono molti mezzi per creare interfacce adatte ad un pubblico meno esperto. Infine, un grande ostacolo alla diffusione della blockchain è dato dal contrasto con il GDPR per quanto riguarda la **privacy.** Riassumendo ciò che caratterizza il GDPR potrebbero essere utilizzate tre parole: centralizzazione, limitazione e rimovibilità. Infatti, il GDPR conferisce ai residenti dell'UE diritti al trattamento dei dati personali, tra cui: diritto alla cancellazione dei dati quando non sono più necessari, diritto a richiedere la correzione di dati errati, diritto a limitare l'elaborazione dei dati quando ne viene contestata l'accuratezza. Riassumendo invece la blockchain in tre parole potrebbero essere utilizzate: decentralizzazione, distribuzione e immutabilità. Il sistema attuale e la blockchain si basano quindi su principi opposti, pertanto per consentire la diffusione della blockchain è necessario trovare una soluzione a questi problemi.

1.2 Criptovalute

1.2.1 Definizione

La criptovaluta, come dice il nome, è una forma di denaro digitale basato sulla crittografia, che consente agli individui di trasmettere valore in un contesto digitale. Le principali caratteristiche delle criptovalute possono essere ricondotte a quelle dell'infrastruttura tecnologica su cui si basano, la blockchain. Tra di esse troviamo infatti la crittografia e la decentralizzazione. Quest'ultima in particolare, permette di evidenziare la differenza tra un sistema come PayPal e il sistema delle criptovalute. Il fatto che sia decentralizzata significa che non esiste un ente centrale dotato di potere decisionale, quindi non esiste un singolo soggetto in grado di prendere decisioni riguardo a cosa può essere approvato o meno e non esiste un server centrale in cui tutti i dati vengono salvati. Questo rende le criptovalute resistenti alla censura e maggiormente sicure in caso di attacchi hacker ai server, i dati non sono infatti salvati in un unico luogo ma una copia di essi è detenuta da ogni nodo della blockchain.

1.2.2 Il Bitcoin

1.2.2.1 La nascita

L'idea di Blockchain risale al 1991, ma la Blockchain come la conosciamo oggi nasce nel 2008 e si diffonde molto velocemente grazie al contesto economico-finanziario di quegli anni, nel quale la **fiducia** nel sistema finanziario era ai minimi. La grande rivoluzione della Blockchain sta proprio nella non necessità di fiducia. Per capire però il significato di questo termine è necessario guardare alla storia dello scambio di valore. A partire dall'8000 a.C. in Mesopotamia nascono le prime forme di baratto, queste avevano due grandi limiti: difficoltà di incontro tra domanda e offerta e impossibilità di frazionare certi beni oggetto di scambio. A partire dal 5000 a.C. si iniziano a standardizzare i beni di scambio, usando grano, sale e conchiglie, il tutto fino al 2000 a.C. anno in cui si introducono i primi oggetti metallici il cui valore è dato dal peso. È proprio in questo contesto che inizia a nascere un grandissimo problema: **la fiducia**. Non tutti potevano disporre di bilance per verificare il peso degli oggetti di scambio, quindi affinché lo scambio potesse avvenire era necessario fidarsi di colui con cui il rapporto stava avvenendo. Quest'ultimo poteva imbrogliare facilmente sul peso e ottenere più

di quanto gli fosse dovuto. Grazie a questa situazione iniziano a nascere delle primordiali forme di banche: piccoli templi apponevano il loro timbro, certificando il peso e quindi il valore dell'oggetto metallico usato nello scambio. Traslando tutto ai giorni nostri, l'attuale sistema finanziario (e non solo) è totalmente basato sulla fiducia. La maggior parte della ricchezza è depositata nelle banche e quindi di proprietà di questi enti che la utilizzano per generare ricavi, in parte utilizzati per erogare servizi ai depositanti. Tutte le transazioni che vengono effettuate passano da una **terza parte intermediaria** (le banche) che si occupa di gestirle e autorizzarle. Le decisioni sono prese a livello centrale e il registro di tutto ciò che avviene è depositato presso l'istituto e da essa gestito. Tuttavia, l'attuale sistema non si è sempre mostrato infallibile, basti pensare al fallimento di grandissime banche, fra tutte Lehman Brothers nel 2008, con conseguenze distruttive per l'economia mondiale. Proprio in quegli anni cresce il bisogno di avere una nuova tecnologia che consenta di rimuovere la necessità di fiducia in un terzo e che riesca a garantire sicurezza e trasparenza. Il tutto si concretizza con la pubblicazione del White Paper di Bitcoin, il 31 ottobre 2008 (un mese dopo il fallimento di Lehman Brothers) ad opera di Satoshi Nakamoto e con la creazione del primo blocco, nel quale è incisa la frase "*Chancellor on brink of second bailout for bank*".
Nel White Paper, Nakamoto afferma di aver risolto il più grande problema delle valute digitali dell'epoca, il double spending, attraverso un sistema basato sulla crittografia e sulla PoW, che connette direttamente due soggetti senza alcun bisogno di intermediari.

1.2.2.2 Il double spending

Il double spending è una situazione nella quale un soggetto ha la possibilità di usare più volte le stesse monete per effettuare delle transazioni. Il metodo esposto da Satoshi per la prevenzione del double spending prevede la creazione di un registro distribuito (blockchain) sul quale vengono annotati tutti i trasferimenti di moneta, la cui sicurezza è garantita dall'algoritmo di consenso PoW. Grazie alla crittografia su cui si basa, tutto ciò che viene annotato nel registro diventa immutabile e questo garantisce che chiunque effettui una transazione, una volta che questa è aggiunta al registro non possa più modificarla. Poiché la transazione è presente nel registro e non esiste modo di eliminarla (a meno si verifichi un 51% attack), chiunque può verificare che le monete

che vengono inviate non siano già state spese. Il problema del double spending viene quindi risolto. Il punto più importante da capire è che questo metodo di prevenzione è efficace solo nel momento in cui la transazione viene inserita nella blockchain. Pertanto, al fine di non incorrere in una doppia spesa è fondamentale aspettare che la transazione venga aggiunta. Per fare un esempio pratico: Bob deve pagare un piatto di pasta al ristorante di Alice, quindi effettua la transazione in bitcoin verso l'indirizzo del wallet di Alice. Poiché le transazioni prima di essere aggiunte alla blockchain, devono essere inserite in un blocco e verificate dai nodi della rete, passerà del tempo dal momento del pagamento all'effettiva aggiunta alla catena. Se Alice accetta la transazione prima che questa venga aggiunta rischia di incorrere nel problema della doppia spesa, ovvero rischia di non ricevere i soldi di Bob perché quest'ultimo, scaltramente, li ha inviati anche ad un proprio indirizzo bitcoin. Se questa transazione viene approvata prima rispetto a quella effettuata nei confronti di Alice, questa non riceverà il denaro.

Riassumendo, la blockchain e bitcoin propongono una soluzione realmente valida al double spending, tuttavia è fondamentale che chiunque sia disposto ad accettare pagamenti in bitcoin, attenda l'aggiunta della transazione alla blockchain prima di accettarla.

1.2.2.3 Il protocollo Bitcoin

È importante fare chiarezza, quando si parla di bitcoin, riguardo al significato dei termini ai quali si sta facendo riferimento. Il sistema Bitcoin si può dividere in due elementi fondamentali: il bitcoin con la "b" piccola, che indica la criptovaluta e il Bitcoin con la "B" grande che indica il protocollo Bitcoin. Quest'ultimo definisce le regole della blockchain Bitcoin ideata da Satoshi Nakamoto. Infatti, ciascuna catena può adottare regole diverse per quanto riguarda il **consenso**, ***l'halving***[21] e il meccanismo di **reward**. Quello Bitcoin è trattato nel dettaglio nelle righe successive. Bitcoin è basato su un algoritmo di **consenso** Proof of Work e quindi sul mining dei blocchi. Circa ogni due settimane devono essere prodotti 2016 nuovi blocchi, mediamente 1 ogni 10 minuti. Se il numero di blocchi si discosta dall'obiettivo, il sistema provvede a adeguare

[21] *Halving:* evento nel quale viene dimezzata la ricompensa erogata al miner che mina un nuovo blocco.

la difficoltà di creazione del blocco, aumentandola se sono stati creati più blocchi o diminuendola nel caso opposto. In generale più sono i miners operanti sulla rete, più la potenza di calcolo sarà maggiore e quindi la difficoltà di risoluzione di un blocco viene aumentata. Il meccanismo di **reward** è strutturato in modo tale da erogare una determinata quantità di bitcoin al miner che risolve il blocco (oltre alla fees delle transazioni in esso incluse), immettendo così in circolazione nuova moneta. In particolare, chi ha inventato il sistema Bitcoin ha deciso di dare vita ad una "deflazione controllata" in quanto, ogni quattro anni, il numero di bitcoin erogati alla creazione di un nuovo blocco si dimezza. Questa procedura è chiamata **halving**. Ad esempio, fino al 2016 un blocco dava diritto a 25 BTC, fino al 2020 a 12,5 BTC, oggi invece dà diritto a 6,25 BTC. Questa procedura terminerà attorno al 2136 quando si arriverà a 21 milioni di bitcoin minati dal sistema, che rappresenta la supply massima di bitcoin. Raggiunta quella quantità non ci sarà più alcun modo di generare nuova moneta, garantendo a bitcoin la caratteristica della rarità. Successivamente al 2136 ci saranno altri modi di guadagnare per i miners, perché qualora queste figure venissero meno si bloccherebbe l'intero sistema. In generale, il protocollo Bitcoin offre grande **sicurezza**, tanto che non è mai stato attaccato con successo in 10 anni di storia. La **decentralizzazione** è un altro punto a favore del protocollo, nonostante negli ultimi anni sia diminuita con la creazione delle mining pools, a causa della grande quantità di potenza di calcolo richiesta per il mining. Il punto debole è la **scalabilità**, infatti il tempo tra la creazione di un blocco e l'altro è di dieci minuti e la dimensione del singolo blocco è limitata, con conseguente basso numero di transazioni contenibili. Per arginare questo problema sono nate soluzioni come Lightning Network.

1.2.2.4 Lightning Network[22]

La PoW causa, nei periodi di maggiore congestione, un forte incremento dei tempi e delle fees di transazione, infatti i miners aumenteranno la quantità di fees richieste al crescere delle domande di approvazione. Inoltre, il tempo di attesa per la convalida delle transazioni arriva in certi casi a raggiungere interi giorni. Questo è dovuto sia alla dimensione limitata dei blocchi, sia al fatto che i miners preferiranno inserire nel blocco le transazioni che permettono loro di corrispondere commissioni maggiori. Una

[22] Approfondimento LN: https://academy.binance.com/it/articles/what-is-lightning-network.

soluzione a questi problemi è la Lightning Network. Questa consiste in una rete, dotata di propri nodi e propri software diversi da quelli della mainnet, che ha però la caratteristica di comunicare con la blockchain principale. In questa rete vengono aperti dei canali di comunicazione diretti P2P, i quali consentono a due utenti si scambiarsi transazioni ad alta velocità, l'unico limite è la velocità della propria connessione internet. Le operazioni vengono immagazzinate in una sorta di smart contract e, una volta che sono state tutte eseguite ne viene caricato il solo saldo finale sulla chain principale, "liberandola" da tutte le singole transazioni effettuate tra le 2 parti. Questo consente di decongestionare la rete e riduce gli effetti sopracitati di tale fenomeno. Il prezzo da pagare per la grande velocità offerta da questa tecnologia è la decentralizzazione. Infatti, rispetto alla rete Bitcoin principale presenta una maggiore centralizzazione, dovuta al numero di nodi ristretto che partecipa a tale rete. Un esempio di utilizzo della LN potrebbe essere questo: Alice e Bob aprono il loro canale, nel quale entrambi hanno un saldo di 5 BTC. Alice potrebbe scrivere nel registro "*paga 1 BTC a Bob"*. Ora, Bob ha 6 BTC dalla sua parte, e Alice ne ha 4. Dopodiché, Bob potrebbe inviare 2 BTC ad Alice, aggiornando i saldi a 6 BTC dalla parte di Alice e 4 BTC da quella di Bob. Possono continuare così per molto tempo.
In qualsiasi momento, uno dei due può pubblicare lo stato corrente del canale nella blockchain. A quel punto, i saldi di ciascuna parte del canale verranno allocati on-chain ai rispettivi partecipanti.

1.2.2.1 Lo pseudonimato

Molto spesso bitcoin viene associato all'anonimato, tuttavia non è totalmente corretto. Il protocollo Bitcoin, grazie alla tecnologia blockchain, rende immutabile, eterno e visibile a tutti l'insieme di tutte le transazioni svolte da ciascun indirizzo. È vero che conoscere un indirizzo non significa conoscere il suo intestatario, infatti ciascun soggetto può deliberatamente decidere se intestarsi l'indirizzo utilizzando il proprio nome o più semplicemente un nome fittizio come avviene per le e-mail. Tuttavia, è anche vero che le operazioni svolte da ciascun indirizzo non sono anonime e nascoste, ma ad esso associate e pubbliche. Queste sono le ragioni per cui è più corretto parlare di "pseudonimato" garantito da Bitcoin e non un vero e proprio anonimato.

Un indirizzo è una stringa alfanumerica lunga tra i 26 e i 34 caratteri, dai quali vengono esclusi simboli come la “O” maiuscola e il numero 0 per evitare di incorrere in errori di digitazione *(Figura 15[23])*. Questa rappresenta una sicurezza ulteriore, quasi inutile, visto che la probabilità di digitare un indirizzo realmente esistente sbagliando dei caratteri è 1 su 4,29 miliardi. È quindi molto difficile perdere i propri bitcoin per aver sbagliato la digitazione dell’indirizzo di destinazione, poiché la digitazione non verrebbe proprio accettata.

Figura 15 - Indirizzo Bitcoin

[23] Fonte: wallet personale di bitcoin.

1.2.3 Ethereum

Come nel caso di Bitcoin, anche quando si fa riferimento al sistema Ethereum è importante fare chiarezza sui termini. Ethereum indica il protocollo mentre la criptovaluta che viene utilizzata per regolare le operazioni su di essa è l'Ether (ETH).

"Ethereum è una piattaforma informatica decentralizzata".[24]

In altre parole, può essere visto come un computer che non viene eseguito in un unico luogo ma su tanti nodi sparsi nel mondo. Pertanto, rispetto ai personal computer a cui siamo abituati è più lento, perché richiede la sincronizzazione e il consenso dei vari nodi della rete. Inoltre è più costoso perché per effettuare operazioni è necessario pagare delle fees ai miner. A prima vista sembrerebbe di aver fatto dei passi indietro, tuttavia prima di trarre una conclusione è necessario guardare anche il suo lato positivo. Infatti, la decentralizzazione, ovvero la possibilità di essere eseguito da milioni di nodi comporta dei vantaggi:

- Impossibilità di spegnerlo, resettarlo, distruggerlo o censurarlo. Tutto ciò che viene inserito nella catena è immutabile ed eterno. Per modificarlo sarebbe infatti necessaria l'approvazione della maggior parte dei nodi e, in ogni caso, ogni modifica resterebbe visibile a tutti. Per fare un esempio concreto, si immagini di giocare ad un gioco di carte collezionabili on-line e di aver acquistato per 100 euro la carta "Alice". Se la società proprietaria del gioco, decidesse per qualche ragione di eliminarla ci sarebbe il rischio di perdere i propri 100 euro. Se il tutto fosse spostato su blockchain, questo non sarebbe possibile in quanto un singolo individuo non può prendere decisioni, ma dovrebbe avere l'approvazione almeno del 51% dei nodi.

- Accessibilità a chiunque possegga una connessione internet e disponibilità di spazio per tutti gli utenti del mondo (2^256 indirizzi disponibili). Chiunque, collegandosi a *https://etherscan.io/* può vedere e analizzare tutto ciò che è successo sulla rete, con la certezza che ciò che vede è reale e in alcun modo alterato.

[24] What is Ethereum, Binance Academy, aggiornato al 18 Novembre 2021, https://academy.binance.com/it/articles/what-is-ethereum, consultato il 10/12/2021.

- Programmabilità. In quanto computer, Ethereum porta con sé la possibilità di essere programmato. Ciò significa che oltre a poter svolgere transazioni come avviene su Bitcoin, su Ethereum è possibile creare dei veri e propri programmi, come quelli a cui siamo abituati sui pc di casa, con la differenza che vengono eseguiti da milioni di nodi nel mondo. Questi programmi sono chiamati *smart contract* e le loro caratteristiche sono trattate nel paragrafo successivo.

- Creazione di token ERC-20. Grazie alla sua natura programmabile e agli smart contracts, è possibile creare dei token. Un **token** non è altro che un'informazione digitale rappresentativa di una qualche forma di diritto e registrata su un registro distribuito. Esistono due tipologie di token; ***token fungibili***[25] *e* ***token non fungibili***[26]**.** La loro creazione avviene scrivendo all'interno di uno smart contract le caratteristiche fondamentali dell'informazione da digitalizzare. Lo smart contract genererà questi token, che a questo punto possono essere scambiati su blockchain, ereditando tutti i benefici di quest'ultima. Tramite queste modalità è possibile *tokenizzare* beni del mondo reale, ovvero creare una versione digitale di beni reali, scambiabili sulla rete. Il grosso vantaggio di questa operatività sta nel rendere divisibili beni che normalmente non lo sono. Ad esempio, la tokenizzazione di un immobile consentirebbe anche a chi ha meno disponibilità economiche di acquistarne un pezzo. Seguendo questa logica, un giorno, chiunque potrebbe poter acquistare un pezzo della Gioconda. Riassumendo, i token nascono tramite smart contract su una blockchain che li supporta e non hanno una propria blockchain. Questa rappresenta la **differenza principale tra un token e una coin** (criptovaluta). Il primo nasce su blockchain esistente ed è quindi di facile creazione, la seconda nasce su una propria blockchain, richiedendo più lavoro e conoscenza. Sono esempi di Coin, bitcoin (con la "b" piccola) ed Ether (ETH).

[25]Token fungibili: sono quei token che possono essere sostituiti con qualcosa di identico. Ad esempio, le stablecoin, token digitali il cui valore replica quello della valuta Fiat a corso legale.
[26]Token non fungibili: categoria nella quale ciascun token è diverso da un altro, quindi non è possibile che ne esistano due uguali. esempi di applicazione sono l'implementazione dell'identità digitale e la tracciabilità della supply chain.

1.2.3.1 Lo Smart Contract

> *"Uno Smart Contract è semplicemente un programma eseguito sulla blockchain di Ethereum o qualsiasi altra rete che li supporti. È una raccolta di codice (le funzioni) e dati (lo stato) che risiede a un indirizzo specifico sulla blockchain."*[27]

Lo Smart Contract, pertanto, non è né smart né contract perché è semplicemente un codice (*figura 16*[28]). Tuttavia, deve il suo nome al fatto che si auto-esegue (smart) e è in grado di far rispettare degli accordi presi da due parti (contract). Sulla Blockchain Ethereum, lo Smart Contract è rappresentato da un proprio indirizzo ed è dotato di un proprio saldo. Gli utenti della rete possono interagirvi effettuando transazioni verso quell'indirizzo, una volta che il contract riceve la transazione si esegue automaticamente e genera un output sulla base di come questo è stato scritto. L'output viene salvato nella blockchain (o meglio, nella "macchina a stati" Ethereum). Poiché tutto ciò che è presente su Ethereum è pubblico e visibile a tutti, chiunque potrebbe leggere il codice del contratto con cui sta per interagire e verificare che non sia malevolo e per le caratteristiche della blockchain stessa, una volta aggiunto il codice diviene immutabile. Un esempio banale di smart contract potrebbe essere un codice che contiene la seguente istruzione: "quando qualcuno invia 1 ETH all'indirizzo genera come output la scritta "Hello World!"". A questo punto quando un utente invia 1 ETH all'indirizzo del contratto, questo in output darà "Hello World!" e chiunque potrà vedere il tutto sulla blockchain, tramite il sito https://etherscan.io/. Un altro esempio, più concreto, simile ad uno smart contract è rappresentato dai distributori automatici. Il distributore è preimpostato in modo tale da fare una determinata azione quando un consumatore immette un determinato input.

Figura 16 - Smart Contract in Solidity

[27] What is a smart contract, Binance Academy, aggiornato al 18 Novembre 2021, https://academy.binance.com/it/articles/what-is-ethereum#what-is-a-smart-contract, consultato il 10/12/2021.
[28] Fonte: https://www.researchgate.net/figure/An-example-of-a-smart-contract-written-in-Solidity_fig1_337603517.

Quindi quando riceve 2 euro e il numero 32 in ingresso, il distributore verifica che i 2 euro siano corretti e se lo sono eroga il prodotto collocato nel posto 32. Tutto questo viene fatto in modo automatico e consente di rispettare un “accordo” tra il consumatore e il distributore stesso.
Le potenzialità degli smart contracts sono enormi e gli ambiti d’uso moltissimi. Per citarne uno basti pensare al mondo assicurativo, dove grazie all’integrazione tra Internet of Things e smart contracts sarebbe possibile rilevare eventuali comportamenti scorretti del conducente e agire di conseguenza. Ad esempio, un superamento dei limiti di velocità potrebbe portare lo smart contract ad aumentare il premio assicurativo.
Un altro ambito di utilizzo molto interessante e che si è sviluppato fortemente nel 2021 è quello della Decentralized Finance (DeFi), trattata nel paragrafo successivo.

1.2.3.1.1 I benefici dello smart contract

Lo smart contract e la blockchain hanno come principale aspetto di miglioramento dell’attuale sistema, l’incremento dell’efficienza. Infatti, per quanto visto sopra, le caratteristiche dello smart contract producono:

- **Automatizzazione** nell’esecuzione dei contratti, che consente di eseguire il contratto senza la necessità di una figura umana di intermediazione;

- **Trasparenza** delle obbligazioni contrattuali. Queste possono infatti essere lette da tutti i partecipanti della blockchain senza possibilità di essere ingannati;

- **Immutabilità** del codice. Questo garantisce che il contratto non possa essere cambiato di nascosto e resti esattamente ciò per cui i soggetti si sono impegnati;

- Possibilità di trovare un accordo in assenza di fiducia. Nel caso degli smart contract, infatti, l’unico elemento in cui questa viene riposta è il codice che, essendo un set di istruzioni, segue esattamente ciò che viene ad esso impartito di fare.

Questi aspetti, in termini di efficienza producono un forte risparmio di risorse (tempo) nelle fasi di negoziazione e sviluppo del contratto, accelerarne le prestazioni e ridurre le possibilità di eventuali controversie tra le parti.

1.2.3.1.2 I limiti dello smart contract

Dopo aver visto i punti di forza degli smart contract è importante analizzarne le criticità principali:

- **Irrevocabilità**, che potrebbe essere un problema nel caso in cui, per determinati motivi, si presentasse la necessità di interrompere il contratto. Infatti, i codici, una volta avviati si eseguono in modo automatico, senza possibilità di essere bloccati. Questo rende inutile il concetto di "parte inadempiente" in questa tipologia di contratto ma può creare dei problemi in certe circostanze. Le blockchain più complete stanno cercando di introdurre una "funzione di autodistruzione", con l'obiettivo di eliminare smart contract inutilizzati. Questa funzione deve essere attivata dal nodo creatore del contratto e potrebbe essere utilizzata anche per risolvere il problema di irrevocabilità.

- **Difficoltà di trasposizione** del linguaggio naturale in linguaggio per la stesura dello smart contract. Questo porta con sé due conseguenze, la prima è la necessità di un intermediario tra le parti in grado di trascrivere il contratto in linguaggio formale, qualora queste non siano in grado. La seconda si manifesta nel caso di problemi complessi. Infatti, non tutti i contratti possono essere facilmente trascritti in linguaggio di programmazione e inseriti in uno smart contract.

- **Problemi giuridici:** la caratteristica di decentralizzazione tende a globalizzare la blockchain in cui gli smart contract vengono inseriti. Questo potrebbe creare una duplice problematica, la prima consiste nella definizione del sistema giuridico da applicare, la seconda nella determinazione del giudice territorialmente competente.

Per questi motivi lo smart contract, attualmente, non può sostituire completamente i contratti normali. Tuttavia, la tecnologia è nata da poco e nei prossimi anni potrebbe subire grossi miglioramenti.

1.2.3.2 I problemi di Ethereum e relative soluzioni

Il principale problema di Ethereum è costituito dalla **scalabilità**. L'algoritmo di consenso utilizzato è infatti una PoW e quindi per eseguire le operazioni on-chain, queste devono essere inserite nei blocchi da parte dei miners. Questi ricevono come ricompensa le fees relative alle transazioni incluse e quindi saranno più propensi ad includere prima le operazioni che "pagano meglio". Questo, in momenti di grande congestione della rete porta ad un drastico aumento delle fees da pagare per ottenere la convalida e l'aggiunta alla catena delle proprie operazioni. Questo problema riguarda in parte anche Bitcoin, tuttavia, Ethereum è molto più congestionato rispetto a Bitcoin a causa della sua programmabilità. Infatti, moltissime organizzazioni hanno avuto la possibilità di creare i propri smart contract e i propri token sulla blockchain Ethereum, quindi nel corso degli anni "l'affollamento" della rete è aumentato esponenzialmente. Nella *figura 17*[29] è possibile osservare l'andamento delle commissioni medie pagate su Ethereum nel periodo giugno – novembre 2021. Le fees su Ethereum vengono dette Gas e vengono pagate in ETH. La loro unità di misura è un sottomultiplo dell'Ether, il Gwei, che corrisponde a 10^{-9} ETH.

Nei periodi di massima congestione si è arrivati a pagare centinaia di dollari per una singola operazione.

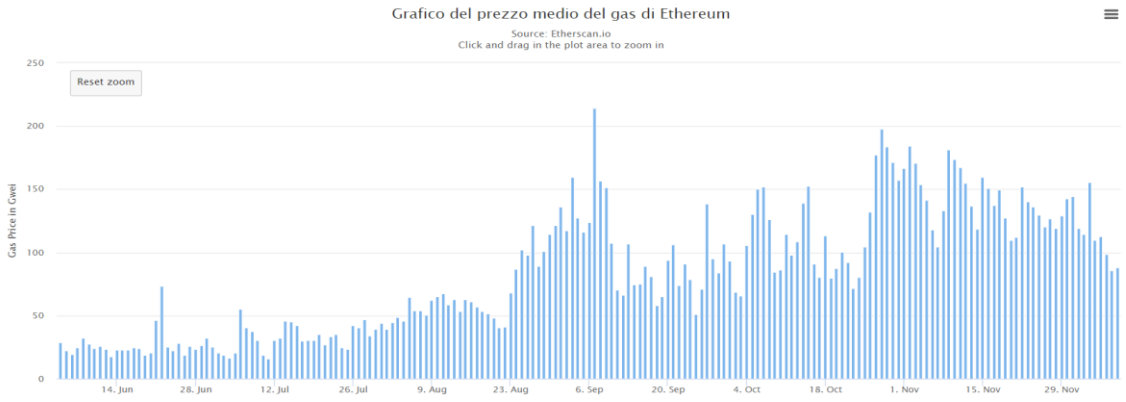


Figura 17 - Gas fees Ethereum

Un modo che la community di Ethereum ha deciso di provare per ridurre gli importi è la transizione ad un consenso Proof of Stake e l'utilizzo dello sharding. Tale passaggio

[29] Fonte: https://it.cointelegraph.com/news/ethereum-gas-fees-drop-as-daily-dex-and-defi-volumes-decline-.

è attualmente in corso, ma servirà ancora del tempo per giungere alla nascita di Ethereum 2.0. Una soluzione già esistente al problema della scalabilità, la quale verrà integrata con l'utilizzo della PoS e con lo sharding[30], sono i cosiddetti **Layer 2**.
L'idea alla base del layer 2 è quella di delegare transazioni di minore importanza a sistemi in grado di gestirle con costi inferiori e in grande quantità, per poi, qualora ce ne fosse bisogno, fare una transazione complessiva nella blockchain principale. Attualmente esistono molte alternative per implementare un layer 2, le due principali sono:

- **Sidechain**: è una vera e propria catena di blocchi, con un proprio algoritmo di consenso che garantisce la sicurezza delle transazioni. Ciò che la rende una sidechain è la presenza di un bridge che permette di trasferire assets in modo decentralizzato e sicuro da e verso la catena principale. Grazie a questa soluzione l'utente sposta i propri asset sulla sidechain, con una transazione sulla mainnet (pagando le fees della catena principale), ma una volta spostate può usufruire di transazioni rapide e sicure sul layer 2. Per garantire questo tipo di vantaggio, quest'ultimo è dotato di un algoritmo di consenso più centralizzato, infatti è necessario scendere a dei compromessi. Se la sidechain fosse sicura, decentralizzata e scalabile potrebbe essere infatti usata come blockchain principale, ma questo non è possibile. Le soluzioni di scalabilità di questo tipo più recenti portano con sé delle grosse novità, oltre al bridge. Infatti, sono nate proposte pienamente *EVM compatibili*[31], sulle quali possono essere eseguiti smart contract scritti per funzionare con Ethereum e, ancora, eseguiti applicativi di qualsiasi tipo come wallet pensati per funzionare con la blockchain principale.

- **Rollup:** questi sono dei sistemi che basano la propria sicurezza direttamente nella catena di blocchi principale e non in un proprio algoritmo di consenso. Possono essere visti come dei meccanismi che comprimono un numero grande di transazione in una sola, con un rapporto di riduzione solitamente di uno a cento. La compressione avviene grazie ad una struttura ad albero binario basato sulla funzione

[30] *Sharding:* creazione di canali paralleli alla chain principale per trasmettere informazioni.
[31] *EVM compatibile*: compatibilità con il mondo Ethereum, stesso linguaggio di scrittura (Solidity), interfaccia grafica familiare, possibilità di esecuzione dei programmi scritti per funzionare su Ethereum e stesso indirizzo che inizia con 0x…

di hash, il *Merkle Tree*[32]. Per le sue caratteristiche, quest'ultimo è molto utile per dimostrare che un "dato" esiste in un insieme, mentre è molto meno efficiente nel dimostrare che quel "dato" non esiste. Questo rappresenta un grosso problema, ad esempio un utente potrebbe aggiungere alle varie operazioni che vengono compresse, una transazione in cui si accredita valute di altri utenti. Verificare che una transazione di questo tipo non esista richiederebbe molto tempo. Le soluzioni a questo problema sono 2: **optimistic rollups** e **zero-knowledge rollups.** Nel primo caso si concede del tempo alla parte defraudata di dimostrare la frode, attraverso una Proof of Fraud. Questa viene inviata allo smart contract che, in caso di verifica dell'accusa, rimuove il batch dal rollup ed elimina i rollups successivi. Fino a che il ricorso non si esaurisce nessuno può prelevare soldi dal rollup verso la catena principale.

Negli zk rollups, invece, oltre al merkle tree viene aggiunta nella compressione una prova crittografica, che serve a dimostrare la correttezza delle informazioni compresse. Tale prova richiede molta energia ma è verificabile molto velocemente, indipendentemente dal numero di transazioni e account.

I rollups sono più sicuri rispetto alle sidechain, tuttavia a causa del tempo richiesto per la verifica di correttezza, consentono attualmente di fornire supporto alla chain principale solo nelle transazioni e non nell'esecuzione degli smart contract. I protocolli di finanza decentralizzata trovano quindi grande applicazione nei Layer 2 sidechain.

Esistono poi altri modi per la creazione di layer 2 come le State Channels, i Plasma, le Hybrid Solutions e i Validium. Ciascuna di queste si caratterizza per diverse prestazioni nei tre elementi del blockchain trilemma: scalabilità, sicurezza e decentralizzazione. Alcuni esempi sono riportati nella *figura 18*[33].

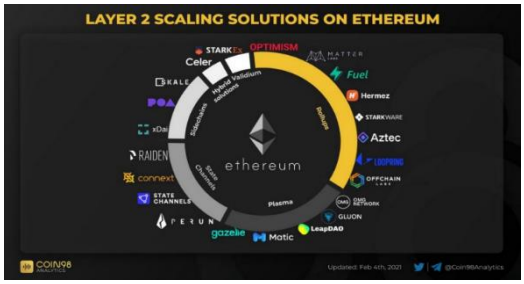


Figura 18 - I Layer 2

[32] Merkle tree: albero binario nel quale ciascun nodo è l'hash dei nodi figli. In questo modo il nodo padre di tutti sarà un hash che contiene tutti gli hash dei figli. Questo nodo padre è detto Merkle Root. Confrontando l'hash di un nodo con il valore che dovrebbe avere qualora fosse corretto, diventa possibile verificare la correttezza delle informazioni in esso contenute. Se il Merkle Root differisce dal valore corretto si scende nell'albero binario tramite i nodi il cui hash risulta errato, fino a trovare la fonte dell'errore. Approfondimento: https://academy.binance.com/it/articles/merkle-trees-and-merkle-roots-explained.

[33] Fonte: https://fabiocricri.medium.com/ethereum-soluzioni-layer-2-c85065234b84. Fabio Cricrì.

1.2.4 Il trilemma della Blockchain

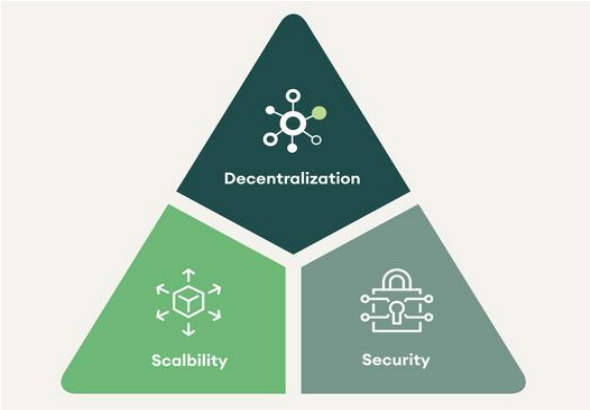


Figura 19 - Il trilemma della blockchain

Ricapitolando le caratteristiche di Bitcoin ed Ethereum si ha che il primo offre grande sicurezza, buon decentramento ma una bassa scalabilità, richiedendo dieci minuti tra la creazione di due blocchi. Il secondo, con il passaggio alla versione 2.0 offrirà una maggior scalabilità, ma dovrà rinunciare a un po' di decentramento e di sicurezza. Ciò che emerge è un **trade off** tra i 3 elementi fondamentali della blockchain: **scalabilità, sicurezza e decentralizzazione** (*figura 19*[34])**.** Questo problema è noto come **il trilemma della blockchain.** È opinione diffusa tra gli sviluppatori che creare una blockchain che sia dotata di tutti e tre gli elementi in modo efficace sia impossibile. Tuttavia, questa tesi non è mai stata dimostrata matematicamente, ma viene comunque utilizzata per esprimere le grandi difficoltà con le quali gli sviluppatori di blockchain si trovano giornalmente a combattere. Proprio partendo da questo problema e in particolare dalla volontà di dimostrare l'invalidità della suddetta tesi, Silvio Micali nel 2017 fonda Algorand.

1.2.5 Algorand

Algorand inizia il suo cammino nel 2017, dalla mente di Silvio Micali, professore italiano del MIT, specialista in crittografia e vincitore del premio Turing. L'obiettivo di Micali è quello di creare una blockchain che possa "rompere" il trilemma della blockchain, quindi essere sicura, decentralizzata e scalabile. La strategia usata da Algorand per raggiungere questo obiettivo è stata quella di creare un sistema permissionless con un nuovo algoritmo di consenso, il Pure Proof of Stake (PPoS). Inoltre, per restare al passo con le novità, la rete è dotata della possibilità di creare smart contract e quindi in grado di ospitare le loro applicazioni, con particolare attenzione alla DeFi. Proprio nell'ottica di permettere a numerosi progetti di finanza decentralizzata di costruire su Algorand, sono stati sviluppati strumenti che facilitano la loro implementazione e il loro funzionamento.

[34] Fonte: https://cvj.ch/en/focus/background/the-blockchain-trilemma/.

1.2.5.1 Pure Proof of Stake

Il Pure Proof of Stake è il cuore pulsante del sistema Algorand. Il suo fondatore Silvio Micali, in un'intervista fatta con Marco Montemagno afferma che "*grazie a questo meccanismo, Algorand è la prima Blockchain a smontare la tesi del trilemma, proponendo un sistema decentralizzato, sicuro e altamente scalabile*". Il PPoS si basa, in poche parole, su una lotteria nella quale vengono estratti a caso i soggetti che avranno il diritto di verificare e aggiungere nuovi blocchi alla catena. La **lotteria** funziona così: ogni volta che un blocco deve essere aggiunto, circa ogni 4 secondi, vengono pescati casualmente 1000 token tra i 10 miliardi creati. I soggetti che detengono questi token formano un comitato, questo decide sul prossimo blocco tramite un sistema a maggioranza qualificata. Il processo di estrazione è svolto crittograficamente ed è assimilabile a ciò che avviene con una slot machine: ogni utente, per ogni blocco da creare, "tira la leva" sul proprio pc e può vincere o meno. In caso di vittoria viene erogata una prova matematica (biglietto) che attesta la vincita. Questa prova viene propagata in rete dal vincitore insieme alla decisione sul blocco, quindi chiunque sa chi ha diritto di entrare nella commissione e cosa ha deciso. La PPoS è pertanto:

- **Scalabile** perché il tempo richiesto per effettuare l'estrazione è di un microsecondo;

- **Decentralizzata** perché l'estrazione è casuale e quindi chiunque ha più o meno la stessa probabilità di essere scelto. Questa aumenta all'aumentare del numero di token posseduti, tuttavia essendo estratti tra dieci miliardi, il vantaggio è minimo, se non addirittura trascurabile;

- **Sicura** perché non è possibile sapere a priori chi saranno i vincitori essendo la lotteria casuale. L'unica possibilità di conoscere i membri del comitato è in seguito alla pubblicazione in rete dei biglietti vincenti. Tuttavia, a questo punto è tardi per corrompere, perché ormai biglietto e opinione sul blocco sono già stati propagati nella rete e quindi non è più possibile farli sparire e cambiare la decisione.

Un altro grande beneficio derivante dal PPoS è il **consumo estremamente ridotto di energia.** Algorand è infatti la prima blockchain **carbon negative.**

Per quanto riguarda le **ricompense** il meccanismo è diverso da Ethereum e Bitcoin. Il sistema PPoS non necessità infatti né di lavoro, né di monete messe in staking. Di fatto la verifica dei blocchi non rappresenta un costo per coloro che vengono estratti. In linea di massima, quindi, non sarebbe necessaria alcuna ricompensa. Tuttavia, è stato stabilito che chiunque possieda almeno 1 Algo (criptovaluta nativa di Algorand) all'interno del wallet di Algorand, ha diritto a delle ricompense erogate in Algo e proporzionali al numero di coin possedute.

Per concludere, anche **l'evoluzione del protocollo** in Algorand è pensata per risolvere un problema, quello dei fork. Secondo la società infatti, un fork, specialmente nel caso in cui sia hard, potrebbe portare ad una frattura della comunità. Per risolvere il problema è stato introdotto il meccanismo di evoluzione riportato in *figura 20*[35].

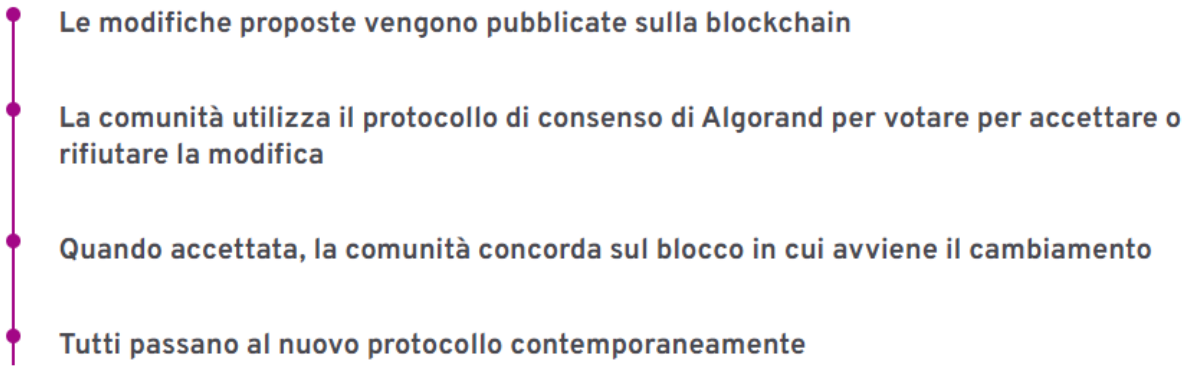


Figura 20 - Evoluzione protocollo Algorand

1.2.5.2 La tokenomics di Algorand

La distribuzione dei token Algo viene fatta secondo lo schema indicato nella *figura 21*[36]. Una parte della supply di dieci Bn viene riservata alla fondazione, che si occupa di sviluppare il progetto. Un'altra parte è erogata all'ecosistema, ovvero ai vari protocolli e applicazioni che decideranno di svilupparsi sulla blockchain Algorand. La voce relativa ai "partecipation incentives" fa riferimento ai token Algo che vengono erogati a coloro che impegnano i propri Algo nella governance del sistema, ovvero in quell'organizzazione che si occupa della gestione progettuale e della proposta e approvazione

[35] Fonte: https://www.algorand.com/technology/algorand-protocol.
[36] Fonte: https://www.algorand.com/technology/algorand-protocol.

delle modifiche. Parte della supply viene riservata alla società Algorand e una parte è allocata agli Early Baker. Questi ultimi sono coloro che hanno investito e creduto nel progetto fin dalle sue fasi iniziali, consentendone lo sviluppo. Il rilascio dei token è graduale e cresce nel corso degli anni fino al 2030, anno in cui la supply massima di 10 Bn verrà raggiunta. Un altro elemento innovativo pensato da Algorand consiste nell'implementazione dell'accelerated vesting: qualora la EMA[37] a 30 giorni superi la EMA a 30 giorni degli All Time High, il rilascio dei token viene incrementato rispetto al normale. Questo è fatto con l'obiettivo di contenere eventuali rallies di prezzo, allontanando così soggetti con intenti speculativi e attirando investitori che credono nel valore a lungo termine.

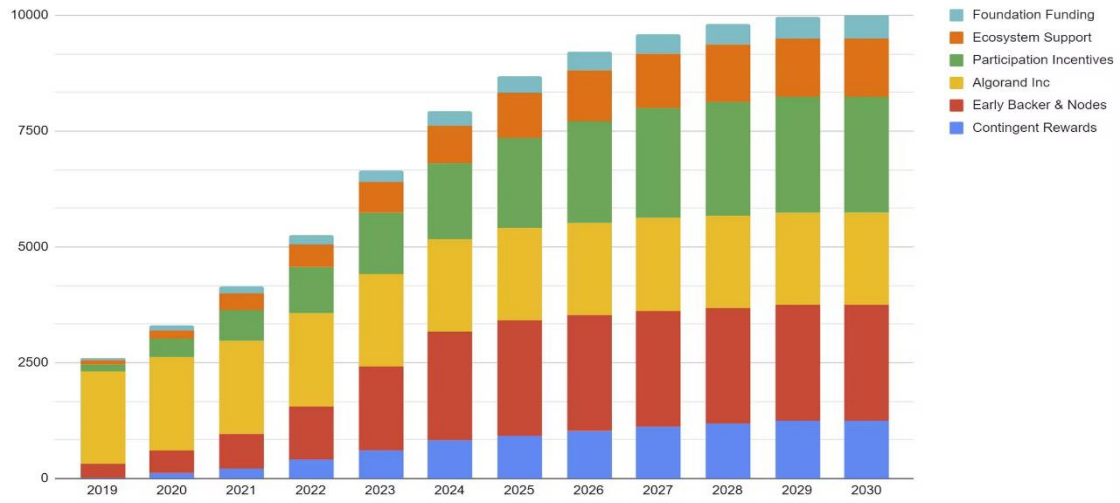


Figura 21 - Algodynamics a lungo termine

1.2.5.3 Progetto SIAE

Nel capitolo relativo alla blockchain, nella parte riguardante i casi d'uso, è citata la protezione dei diritti d'autore. La legge sul diritto d'autore sancisce che tale diritto sorge con la creazione di un'opera, senza che sia necessario alcun deposito. Il problema è dimostrare "chi" ha creato l'opera

Figura 22 - SIAE e Algorand

[37] EMA: media mobile esponenziale.

e “quando” questa è nata. La blockchain, grazie alle sue caratteristiche, permette di risolvere efficacemente ed efficientemente questi due problemi. Grazie agli smart contract, infatti, è possibile depositare al loro interno un hash e ottenere in output un NFT (Non Fungible Token). Se per generare l’hash vengono utilizzati i documenti legali necessari al riconoscimento del diritto d’autore, questo ne garantisce la proprietà. Infatti, cambiando anche solo il nome nei documenti, l’hash cambierebbe drasticamente, mostrando la contraffazione delle carte. Associando a tale hash, tramite smart contract un NFT, diventa possibile per il creatore dell’opera detenere i propri diritti e scambiarli su blockchain. Il risultato sarebbe una disintermediazione nella gestione dei diritti d’autore, garantendo al contempo sicurezza e maggior tutela della proprietà. Questa innovazione è stata prontamente colta dalla **SIAE**, la società italiana per la gestione del diritto d’autore, che ha stretto un accordo con **Algorand**. L’accordo, stipulato nel 2019 prevede la creazione di NFTs (*figura* 22[38]) rappresentativi dei diritti d’autore degli oltre 95.000 artisti che si affidano alla società. La prima tappa della collaborazione è stata raggiunta il 24 marzo 2021, con la creazione di 4.000.000 di NFTs sull’infrastruttura blockchain di Algorand. Questa partnership, insieme a molte altre, è testimonianza delle possibilità che la blockchain in generale è in grado di offrire.

[38] Fonte: https://www.siae.it/it/iniziative-e-news/siae-rappresenta-i-diritti-degli-autori-con-asset-digitali-creati-pi%C3%B9-di-4000000.

1.2.6 Schemi di truffa nel mondo delle criptovalute

Dal 2016 a oggi, sono cresciuti del 587% gli utilizzatori di cripto asset a livello globale. Questo incremento è stato accompagnato di pari passo da una crescente diffusione di scammer e truffatori. Essendo un mondo non ancora regolamentato interamente, non c'è alcuna protezione a livello legale e diventa quindi fondamentale la conoscenza dei principali schemi di truffa utilizzati per evitare di perdere i propri soldi. I principali metodi utilizzati dai truffatori sono due:

- **Lo Schema Ponzi**

  Questo schema truffaldino prende il nome da Charles Ponzi, immigrato italiano negli Stati Uniti. Nonostante nel tempo si sia sviluppato in varianti sempre più complesse, il ragionamento alla base è sempre lo stesso e si articola in quattro fasi. *(figura 23[39])*

  - Fase 1: vengono attirati i primi clienti con la promessa di alti rendimenti in poco tempo;

  - Fase 2: si pagano gli interessi promessi, facendo credere che il sistema funzioni veramente. In realtà il pagamento è fatto usando una parte del capitale iniziale;

  - Fase 3: la voce si diffonde e sempre più clienti investono soldi per ottenere i rendimenti elevati promessi. Si continuano a pagare i rendimenti dei clienti al tempo t, usando i soldi dei clienti che arrivano al tempo t+1;

  - Fase 4: quando il deflusso inizia a superare il potenziale afflusso, lo schema si interrompe, lasciando senza soldi gli ultimi arrivati. I soldi verranno incassati dai creatori del Ponzi e dai primi clienti, se hanno ritirato i soldi prima dell'interruzione dello schema.

[39] Fonte: https://www.riskcompliance.it/news/lo-schema-ponzi-le-red-flags-e-il-sistema-piramidale/.

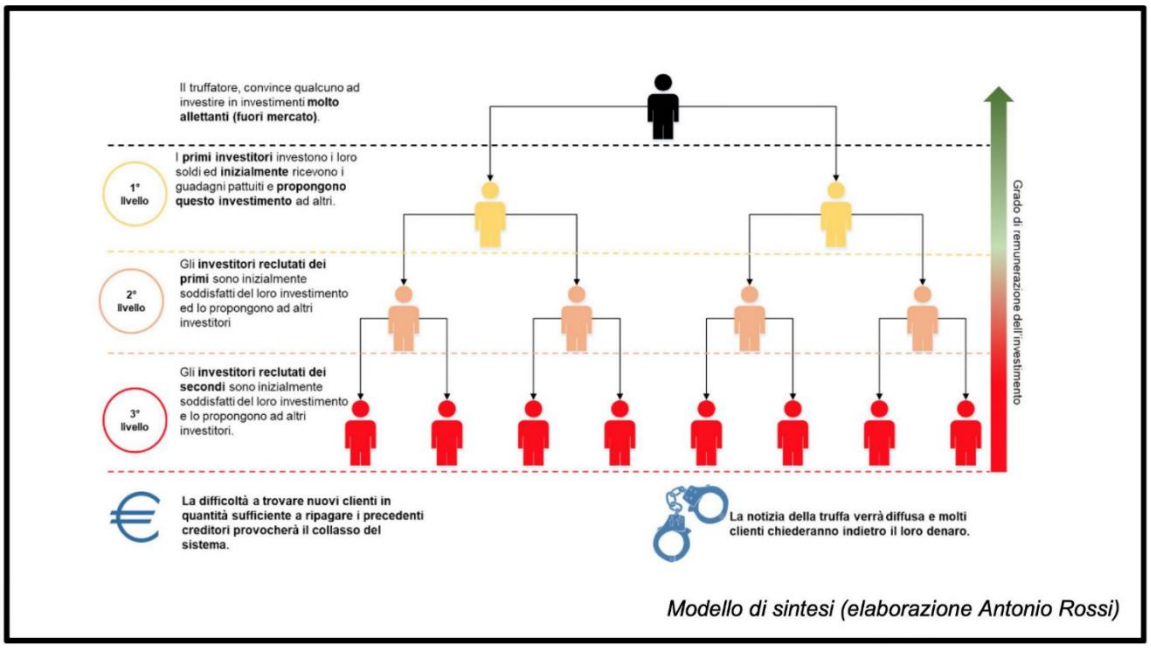


Figura 23 - Schema Ponzi

Tra le più grandi truffe effettuate con lo schema Ponzi possono essere citate **One-Coin**, che restò attiva dal 2014 al 2017, sottraendo circa 5 miliardi di dollari a 3 milioni di investitori e **BitConnect.** Questa prometteva un rendimento del 40% al mese tramite un trading bot e ha sottratto agli investitori circa 3,5 miliardi di dollari.

- **Il Rugpull**

  Un Rugpull, letteralmente “tiro del tappeto” è un metodo truffaldino che consiste nel far sembrare una situazione completamente normale e tranquilla, fino al momento in cui il tappeto viene tirato e coloro che vi sono sopra cadono e si fanno male. È un metodo tipicamente usato all’interno dei *liquidity pool* nella *DeFi*, entrambi trattati nel paragrafo successivo. Solitamente colui che ha intenzione di organizzare questa truffa, si comporta nel seguente modo: il tutto inizia tramite la creazione di uno smart contract, questo dovrebbe congelare al suo interno le monete, tuttavia, in questo caso, il malintenzionato si riserva una backdoor che consenta successivamente di prelevare le monete senza alcun intoppo. Successivamente crea un nuovo token e lo inserisce all’interno di un liquidity pool tramite lo smart contract creato, dando la possibilità a chi è interessato di tradarlo (scambiarlo) con un token di valore, ad esempio bitcoin o ETH. Nel momento in cui il truffatore si ritiene soddisfatto della quantità di valore accumulata, aziona la backdoor svuotando il pool.

A questo punto chi ha acquistato il token scam, si ritrova con un asset privo di valore, senza la possibilità di liberarsene, questo perché il pool è stato svuotato.

Seppur non esiste un metodo infallibile da usare al fine di non cadere in truffe, esistono delle regole generali che consentono di evitare la maggior parte delle situazioni scomode che possono capitare. La prima cosa da fare quando si interagisce con un progetto è chiedersi quale è il suo **scopo.** In particolare, bisogna capire come funziona, se la proposta è innovativa o se sta semplicemente cavalcando qualche tendenza. In quest'ultimo caso può essere si tratti di una truffa. In secondo luogo, è possibile, essendo la maggior parte dei progetti open-source, verificare il **codice sorgente** per chi ne ha le possibilità. Per chi invece non ha le conoscenze informatiche, diventa fondamentale verificare la presenza di **audit** effettuati da società diffuse e affidabili. Un ultimo punto è quello di verificare chi sono i **fondatori**. Se questi sono persone famose, con alle spalle altri progetti non dovrebbero esserci problemi, nel caso in cui questi siano anonimi, invece, le probabilità di truffe crescono.
In ogni caso, investire in un progetto cripto serio non comporta l'eliminazione di ogni tipo di rischio e la sicurezza di non perdere i propri soldi. Permane infatti un rischio finanziario dovuto alla grande speculazione che, al momento, aleggia attorno a questo mondo. Questa categoria di rischio è trattata più approfonditamente nel capitolo tre.

1.3 Altri ambiti d'uso della blockchain

1.3.1 La DeFi

La DeFi, letteralmente Decentralized Finance, è un nuovo modo di interpretare la finanza che è nata con la diffusione delle blockchain programmabili come Ethereum e in particolare con la creazione degli smart contract. Grazie a questa infrastruttura tecnologica, si differenzia dalla finanza tradizionale per la caratteristica di decentralizzazione. Non esistono più gli intermediari come le banche, il tutto è gestito tramite gli smart contract, con il grande vantaggio della riduzione delle commissioni di

intermediazione. In altre parole, si passa da un rapporto utente – intermediario ad un rapporto utente – contratto. Un confronto sintetico tra TradFi e DeFi è illustrato in *figura 24*[40].

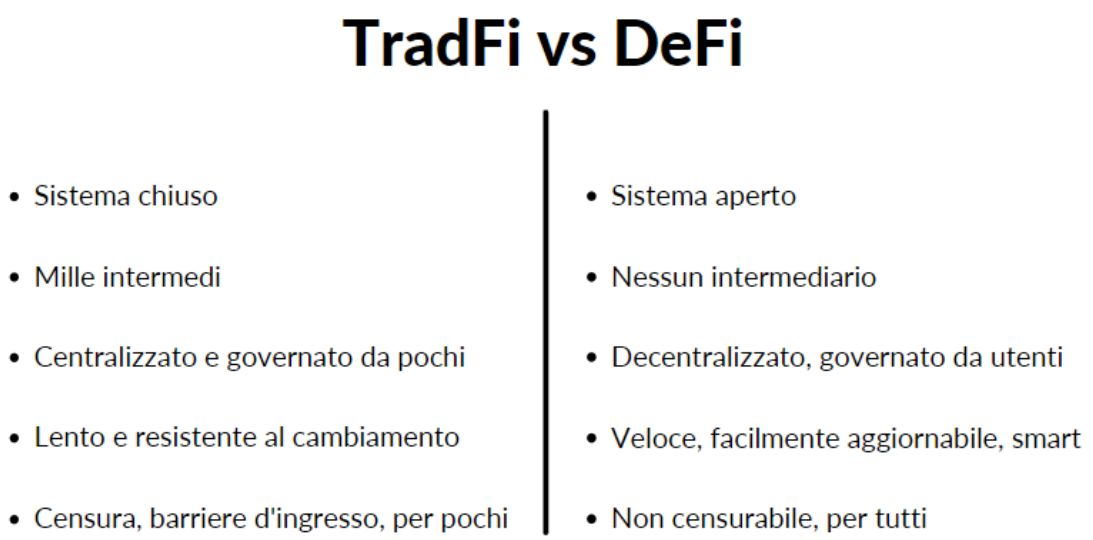


Figura 24 - TradFi VS DeFi

La finanza decentralizzata è un vero e proprio universo parallelo a quello tradizionale, costituita da un proprio ecosistema di servizi finanziari, erogati tramite delle decentralized applications costruite su smart contract. Negli ultimi due anni ha avuto un enorme sviluppo e sono nati una grande varietà di servizi, alcuni completamente nuovi, altri già diffusi nella finanza tradizionale. La struttura DeFi può essere rappresentata con la piramide in *figura 25*[41]. La base della piramide contiene i servizi di base, noti e utilizzati anche nella finanza tradizionale, ai quali, però, sono state apportate alcune modifiche e migliorie rese possibili dalla decentralizzazione e dalla disintermediazione. Più si sale nella piramide, più i servizi diventano "sperimentali" e usati solo da una piccola fetta di utenti. Questo significa che più ci si avvicina alla punta della piramide, più i rischi derivanti dall'utilizzo di tali sistemi aumenta, al contempo aumentano anche i possibili benefici.

Senza scalare troppo la piramide, per evitare di entrare in meccanismi e dinamiche complesse, in questo elaborato vengono descritti i servizi fondamentali alla sua base.

[40] Elaborato su https://drive.google.com/file/d/1ZPnmqyvk4_kCvnq02mwK-onroGHD6-_y/view.
[41] Elaborato su: https://drive.google.com/file/d/1ZPnmqyvk4_kCvnq02mwK-onroGHD6-_y/view.

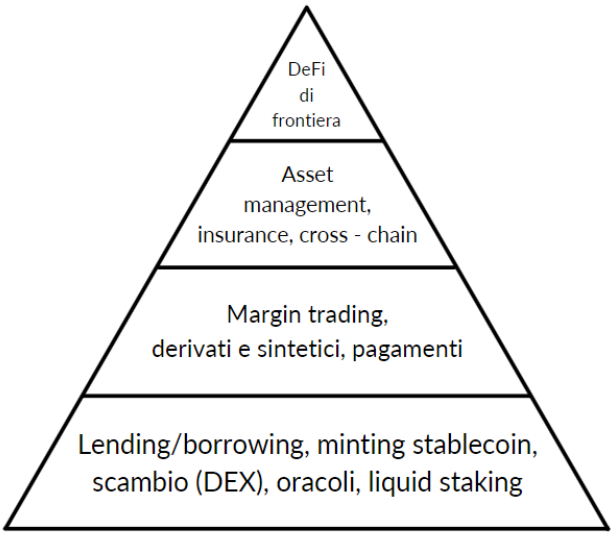


Figura 25 - I servizi finanziari sulla DeFi

- **I protocolli di lending / borrowing**

  Queste piattaforme permettono l'incontro tra due tipologie di utente, il Lender, ovvero colui che ha liquidità disponibile e la vuole prestare e il Borrower, ovvero colui che la chiede in prestito. Generalmente quest'ultimo deposita un collaterale in criptovaluta e ottiene in prestito delle stablecoin [42]che può usare in vari modi. Ad esempio, Bob ha dieci bitcoin, vorrebbe usarli per generare un rendimento senza però venderli, in modo da restarvi esposto. Va sulla piattaforma e chiede in prestito una stablecoin, (perché i rendimenti offerti in rete sulle stable sono solitamente superiori rispetto a quelli offerti su bitcoin), impostando un opportuno Loan To Value (LTV[43]). La differenza rispetto ad un sistema tradizionale è che non esiste alcun intermediario fra le parti, il tutto è gestito in automatico da uno smart contract, come illustrato in *figura 26*[44].

[42] Stablecoin: token generati tramite smart contract, il cui valore resta stabile. La stabilità è ottenuta replicando esattamente il valore della valuta Fiat scelta (euro, dollaro...).
[43] LTV: Valore percentuale che esprime il rapporto tra il valore preso a prestito e il valore del collaterale.
[44] Elaborato su: https://drive.google.com/file/d/1ZPnmqyvk4_kCvnq02mwK-onroGHD6-_y/view.

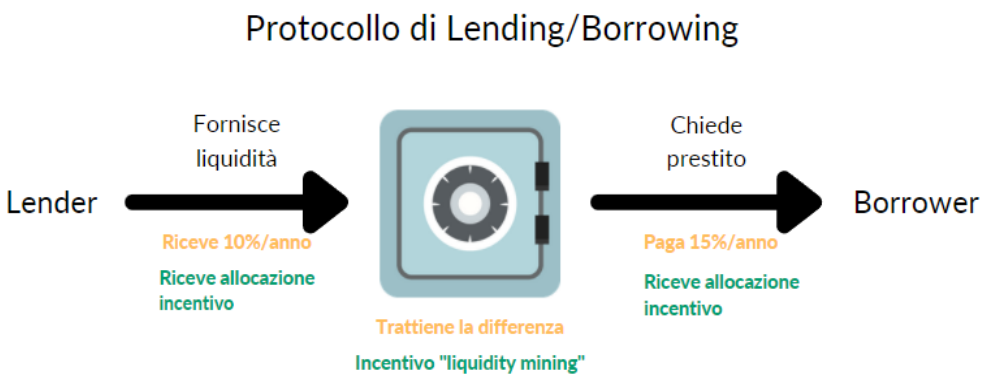


Figura 26 - Lending e Borrowing

Il funzionamento è semplice: colui che prende in prestito il denaro paga un interesse, questo è in parte trattenuto dallo smart contract e la restante parte viene erogata a colui che fornisce la liquidità. La differenza con il sistema tradizionale emerge qui, la presenza dello smart contract produce due effetti:

- L'APR[45] ottenuto dal lender è più alto, infatti non ci sono le commissioni da pagare all'intermediario. Questo trattiene solo una piccola parte degli interessi del borrower e lo usa per generare un altro vantaggio di cui entrambe le parti possono godere, il Liquidity Mining.

- **Liquidity mining:** è un incentivo erogato in token della piattaforma di lending / borrowing, ad entrambe le parti. Il suo valore (espresso attraverso l'APY[46]) è solitamente molto più alto dell'interesse maturato o pagato. Questo incentivo è un cosiddetto win-win. Tramite l'erogazione dei token la piattaforma attira nuovi depositi e nuove richieste di prestito, così facendo può detenere più interessi e al contempo erogare nuovi incentivi di liquidity mining. Ciò che si genera è un circolo virtuoso. La ricerca del liquidity mining da parte degli utenti è chiamata **farming[47].**

[45] APR: tasso di interesse annuo non considerando il reinvestimento dei profitti.
[46] APY: tasso di interesse composto annuo. Ottenuto tramite reinvestimento dei profitti ogni x periodo di tempo.
[47] Farming: ricerca dei migliori incentivi di liquidity mining.

- **Decentralized Exchange (DEX)**

  Sono delle piattaforme utilizzate per tradare, ovvero scambiare, un token con un altro. Si differenziano dagli exchange centralizzati come Binance in quanto, non utilizzano un meccanismo ad order book ma usano delle liquidity pool e degli AMM[48]. Il primo è un registro nel quale vengono registrate domanda e offerta di token, il trade avviene quando il prezzo delle due si incontra. Le liquidity pool, invece, contengono liquidità erogata dai liquidity provider e stabiliscono in automatico il prezzo del token tramite gli algoritmi dell'AMM. In questo caso, quindi, non è richiesto il match tra domanda e offerta, il tutto viene ancora una volta gestito automaticamente dagli smart contract.

  Il funzionamento del DEX è illustrato in *figura 27*[49].

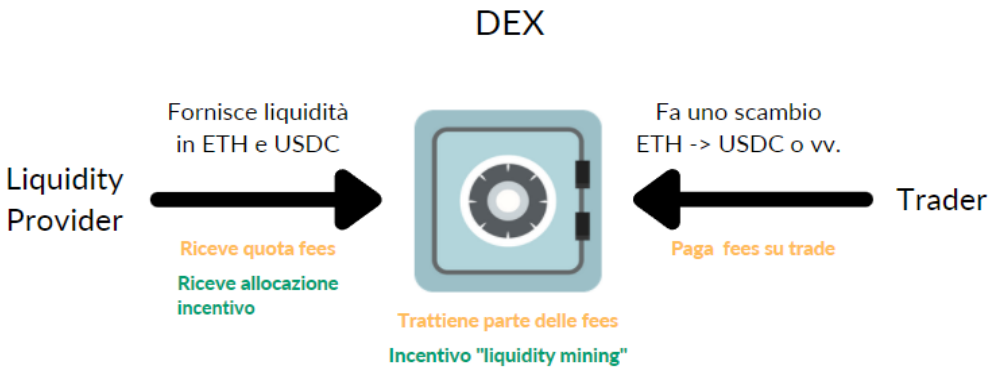


Figura 27 - Funzionamento del DEX

I liquidity provider depositano liquidità sottoforma di token LP. Questi sono token costituiti in egual peso da 2 criptovalute diverse, ad esempio ETH e USDT. I trader, ovvero coloro che desiderano scambiare una moneta con un'altra, eseguono lo scambio. Nell'esempio sarà possibile scambiare ETH per USDT e viceversa. Per fare ciò si pagano delle commissioni. Una parte delle fees è erogata a coloro che hanno fornito liquidità, l'altra invece è trattenuta dalla piattaforma e utilizzata per il liquidity mining. Gli incentivi di liquidity mining sono erogati solo ai liquidity provider, essi sono la parte più importante del DEX. Infatti, senza liquidità non sarebbe

[48] AMM: Automated Market Maker, è un protocollo che stabilisce i prezzi degli asset tramite formule matematiche.
[49] Elaborato su: https://drive.google.com/file/d/1ZPnmqyvk4_kCvnq02mwK-onroGHD6-_y/view.

possibile scambiare le monete e quindi nessun trader sarebbe invogliato a usare il protocollo.

- **Liquidity pool:** è l'elemento fondamentale alla base degli exchange decentralizzati. Può essere visto come una vera e propria piscina, all'interno della quale vengono depositate coppie di token, con un peso solitamente del 50% ciascuno. Ciascun pool è rappresentativo di una diversa coppia di token. Il deposito dei token al suo interno è effettuato dai liquidity provider. Questi depositano un token LP, formato come detto sopra e in cambio ottengono una ricompensa doppia, le fees pagate dai trader e il liquidity mining. Il tutto viene fatto restando esposti ai token che compongono la coppia, che quindi possono portare ad un profitto o ad una perdita. Un elemento da non sottovalutare è la cosiddetta impermanent loss, in quanto questa può costituire una perdita pesante per il provider.

1.3.1.1 Impermanent loss e slippage

L'impermanent loss è così chiamata perché è solo una perdita temporanea di liquidità, il cui valore può variare nel tempo, portandone a volte anche all'annullamento. La perdita diventa permanente solo nel momento in cui la liquidità viene prelevata dal liquidity pool e ciò che ne determina l'importo è la variazione del prezzo di un token rispetto ad un altro. Come da *figura 28*[50], sull'asse delle ascisse è riportato questo dato percentuale, mentre su quello delle ordinate è presente il valore dell'impermanent loss.

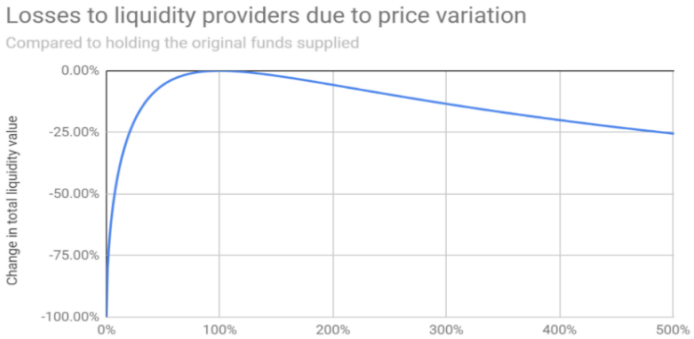


Figura 28 - Impermanent Loss

[50] Fonte: https://eidoohelp.zendesk.com/hc/it/articles/360051871372-Cos-%C3%A8-l-Impermanent-Loss-.

Un esempio numerico di quanto detto: Pippo deposita un token LP formato da ETH e USDT, al momento del deposito ETH vale $1000 e USDT $1. Al momento del prelievo ETH vale $4000 e USDT non è cambiato. Ciò significa che la variazione relativa dei due token è stata del 400% (400% dovuta a ETH e 0% dovuta a USDT). Cercando questo valore in ascissa e salendo fino alla rispettiva ordinata è possibile stimare la perdita impermanente, che nell'esempio è del 20% circa.
Vediamo ora un esempio più approfondito per capire quale è la causa alla base della possibile perdita: si ipotizza l'esistenza di un pool ETH / USDT. Il valore del primo è $1000, il secondo vale invece $1, in totale il pool vale $980.000, è quindi formato da 490 ETH e 490.000 USDT. Pippo deposita 10 ETH e 10.000 USDT, per un valore totale di $20.000 equamente divisi tra i due token, di conseguenza detiene il 2% del pool, il cui valore ammonta a $1.000.000. Si ipotizzi ora un aumento del 20% del prezzo di ETH sugli exchange tradizionali. Poiché il valore di ETH nel pool non può risentire delle variazioni esterne, il valore di ETH al suo interno non è ancora cambiato. Alice si accorge di questo e decide di acquistare ETH dal pool per rivenderlo sugli exchange tradizionali e trarne profitto, quindi acquista $10.000 di ETH in USDT. Questo causerà delle variazioni sulle quantità nel pool, che vengono determinate tramite una formula. La formula usata è detta **formula del prodotto costante**, in altre parole la variazione nel numero di token deve essere tale da mantenere il loro prodotto costante. In altre parole:

$$N.Token\,X \ * \ N.Token\,Y \ = \ K$$

Applicando questa formula, ciò che avviene nel pool è questo:

- prodotto costante = 500 (N. ETH) * 500.000 (N. USDT) = 250.000.000
- nuovo numero USDT = 500.000 + 10.000 = 510.000
- nuovo numero ETH = 250.000.000 / 510.000 = 490,2
- ETH rilasciati = 500 – 490,2 = 9,80

Alice ha di fatto acquistato 9,80 ETH per $10.000 ad un prezzo medio di $1.020 (2% **slippage**[51]) e può rivenderlo all'esterno per $1.200, ottenendo così un profitto. Questo comportamento ha portato ad una nuova composizione del liquidity pool, ora è composto da 490,2 ETH e 510.000 USDT. Se Pippo decide di ritirare adesso la liquidità fornita, avendo il 2% del totale diviso equamente tra ETH e USDT, ottiene 9,80 del primo e 10.200 del secondo. Il valore totale ritirato è quindi pari a (9,80 * $1.200) + $10.200 = $21.960. Se invece Pippo avesse tenuto i propri soldi senza depositarli avrebbe ora 10 ETH ($12.000) e 10.000 USDT ($10.000), quindi $22.000. Ricapitolando:

- Pippo ha depositato $20.000
- Pippo ha ritirato $21.960
- Se non avesse depositato avrebbe $22.000

Quindi apparentemente ha registrato un profitto di $1.960, ma se avesse tenuto i propri soldi senza depositarli avrebbe guadagnato $2.000. La differenza tra questi due valori è **l'impermanent loss**, ovvero quella perdita che Pippo ha sostenuto a causa delle variazioni reciproche di prezzo dei token depositati nel liquidity pool.

1.3.1.2 I rischi della DeFi

La DeFi offre moltissime possibilità, tuttavia è fondamentale, prima di utilizzarla, essere consci dei rischi che essa comporta. La DeFi è un insieme di applicativi costruiti su smart contract, che offrono diversi servizi, dai più tradizionali a quelli più innovativi ed estremi. Poiché tutto è basato sugli smart contract, i **rischi** della DeFi sono quelli ad essi associati. Tra questi abbiamo la **presenza di bug**, causati da un codice scritto male, che espongono lo smart contract ad un attacco hacker, con il rischio che i fondi in esso congelati vengano prosciugati. Una soluzione a questo problema può essere la verifica di audit effettuati sullo SC, da parte di società affidabili e conosciute del settore. Un altro rischio è associato al **rugpull**, spiegato nei capitoli precedenti. Un possibile rimedio può essere quello di controllare i creatori dello SC, qualora il team

[51] Slippage: variazione % del prezzo d'acquisto reale rispetto a quello atteso dovuto a dinamiche interne di un AMM.

sia composto da persone influenti nel mondo blockchain e con progetti di successo alle loro spalle, il rischio di un rugpull è basso. Un ultimo rischio può essere quello di **insolvenza**. Questa situazione si può presentare nel caso in cui lo smart contract non funzioni in modo efficiente e non liquidi in tempo le posizioni dei debitori. In altre parole, il collaterale crolla così rapidamente di valore, che il valore erogato in prestito arriva a superare il valore del collaterale che dovrebbe garantirlo. In una situazione di questo tipo, la liquidità nello SC è inferiore rispetto a quella fornita dai provider, i quali corrono quindi il rischio di non poter prelevare i propri depositi. Poiché una situazione di questo tipo è più probabile tanto più è alta la volatilità del collaterale, è possibile limitare il rischio fornendo liquidità a protocolli con limiti conservativi di Loan To Value e smart contract rodati, che non hanno mai presentato problemi di questo tipo.

2. ASPETTI PRATICI

Anche per chi conosce le basi teoriche del funzionamento della blockchain e delle criptovalute, l'aspetto pratico relativo all'acquisto, alla conservazione e alla vendita, può risultare complesso. I modi più diffusi per entrare in possesso di criptovalute per la prima volta sono l'acquisto su exchange centralizzato e l'acquisto tramite broker CFD. Ciascuno ha i propri svantaggi e i propri vantaggi, riguardo a sicurezza, velocità e aspetto legislativo, tuttavia la più grande differenza sta nel possesso fisico dell'asset. L'exchange consente a colui che acquista di ottenere il possesso fisico dell'asset, mentre tramite il broker CFD si acquisisce uno strumento finanziario che replica l'andamento della criptovaluta, senza però entrarne in possesso fisicamente. Seppur possedere fisicamente la criptovaluta comporti dei rischi, soprattutto legati alla sua gestione e alla sua conservazione, offre anche molte possibilità di guadagno. Esempi di ciò che è possibile fare possedendola fisicamente sono la messa in staking e, più in generale, l'utilizzo in DeFi. Per questi motivi, in questa sezione vengono approfonditi tramite esempi pratici, l'acquisto delle criptovalute tramite gli exchange, la loro gestione nei wallet e gli aspetti relativi alla vendita. Nelle *figure 29 e 30*[52] è riportata la classifica delle principali piattaforme di scambio, secondo CoinMarketCap, tra questi verrà trattato approfonditamente Binance.

Figura 29 – Classifica exchange

Figura 30 - Classifica exchange

[52] Fonte: https://coinmarketcap.com/it/.

2.1. L’acquisto

La prima fase da affrontare è quella della **registrazione**. Al fine di garantire la sicurezza, i principali exchange richiedono di completare il KYC (Know Your Costumer). Le informazioni richieste sono i dati anagrafici, il paese di residenza, l’indirizzo e un documento di riconoscimento. Per verificare la correttezza di quanto inserito, viene richiesto anche di effettuare un video per il riconoscimento facciale. Infine, è necessario inserire la propria mail e scegliere la password. Una volta svolti tutti i passaggi richiesti, si potrà accedere alla schermata principale dell’exchange. Da questa schermata sarà possibile accedere a tantissime funzioni offerte dalla piattaforma *(figura 32*[53]*),* tuttavia, prima di iniziare è fondamentale impostare il 2FA, ovvero il 2 factors authentication. Questo è un meccanismo di sicurezza che oltre alla password, richiede un’ulteriore informazione al fine di permettere l’accesso. Le informazioni possono essere quelle riportate in *figura 31*[54]. Uno strumento molto utile è Binance Authenticator. Questo genera un codice di 6 cifre, che cambia ogni 30 secondi e al fine di eseguire l’accesso, oltre a fornire e-mail e password, è necessario anche inserire tale codice. In caso contrario l’accesso non è permesso.

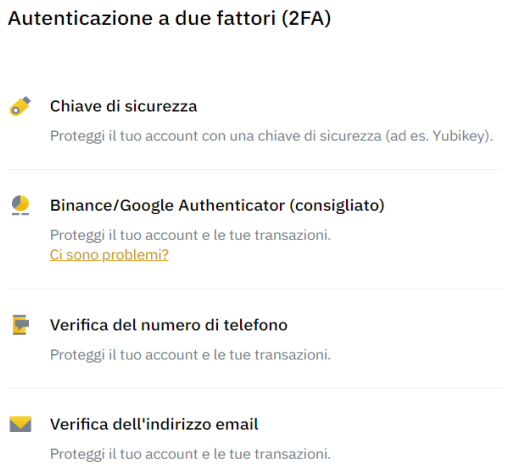


Figura 31 - Elementi 2FA

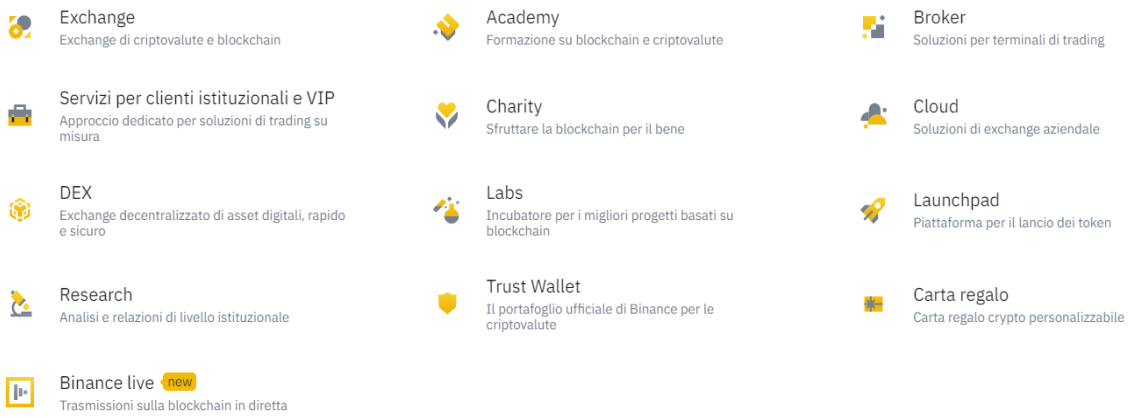


Figura 32 - I servizi di Binance

[53] Fonte: applicazione Binance.
[54] Fonte: applicazione Binance.

Una volta completata la fase preliminare di registrazione e di messa in sicurezza dell'account, al fine di procedere con l'acquisto della criptovaluta, è necessario **depositare** la valuta fiat. Nella *figura 33* è riportata la schermata di deposito di Binance. Sono disponibili più modalità, la più usata è quella tramite carta bancaria, attraverso la quale il deposito avviene istantaneamente. Su altri exchange, come FTX, sono supportati anche i bonifici SEPA, che a differenza del deposito con carta non richiedono commissioni, ma impiegano più tempo. Qualora si disponga già di alcune criptovalute, è possibile effettuare un deposito direttamente in valuta digitale, senza passare dalla moneta fiat. In questo caso, il passaggio è totalmente diverso e le informazioni da inserire sono riportate in *figura 34*[55]:

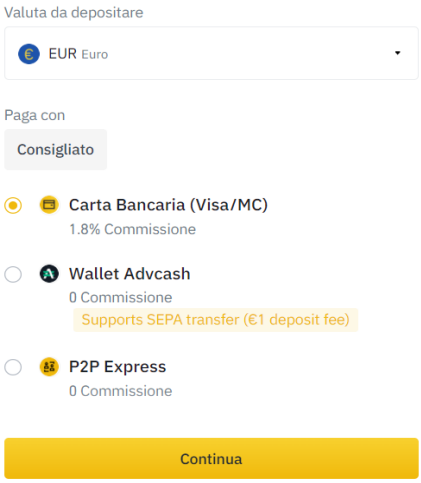


Figura 33 - Deposito Fiat

1. Scegliere la blockchain attraverso la quale eseguire la transazione e indicare la cripto che si vuole depositare. Infine, copiare l'indirizzo del deposito;
2. Spostarsi nel luogo in cui si detengono le cripto da inviare, avviare un prelievo verso l'indirizzo copiato al punto 1;
3. Attendere che la transazione venga confermata dalla blockchain. I tempi variano a seconda della rete che si utilizza e dalle politiche dell'exchange;
4. Se il deposito va a buon fine, l'importo depositato verrà accreditato nella sezione wallet dell'exchange.

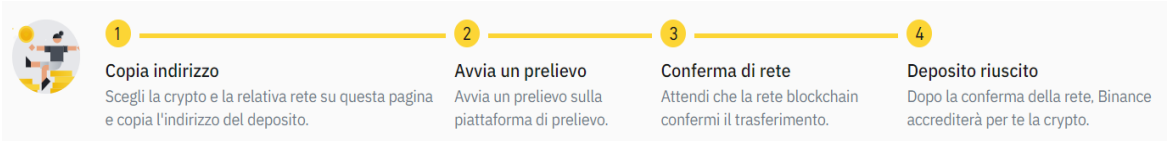


Figura 34 - Deposito Crypto

Una volta che sul conto è presente liquidità sottoforma di valuta fiat, per convertirla in criptovaluta è necessario andare nella sezione di trading del sito. In questa sezione sono presenti le varie coppie di valuta disponibili. Ad esempio, la coppia EUR / USDT,

[55] Fonte: https://accounts.binance.com/it/register?return_to=aHR0cHM6Ly93d3cuYmluYW5jZS5jb20vaXQvbXkvd2FsbGV0L2V4Y2hhbmdlL2JhbGFuY2U=.

permette di comprare EUR utilizzando USDT, oppure di vendere EUR e ottenere il controvalore in USDT. L'interfaccia grafica è riportata in *figura 35, 36 e 37*[56].

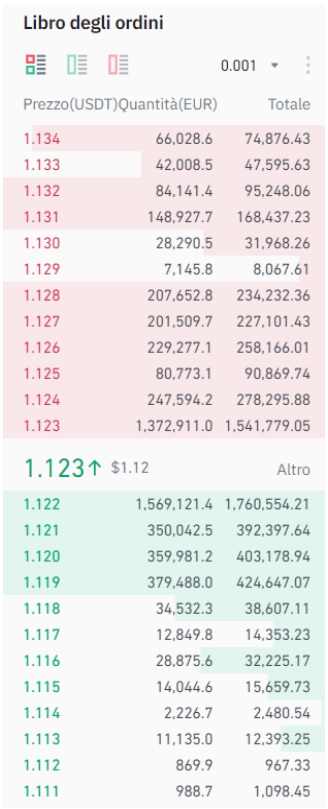


Figura 35 - Order Book

Figura 36 - Schermata vendita

Figura 37 - Schermata Acquisto

La *figura 35* mostra l'order book dell'exchange. I dati in rosso rappresentano il prezzo in USDT al quale gli utenti sono disposti a vendere i propri EUR. Ad esempio, se tale valore fosse 1,123, significherebbe che vendendo 1.000 EUR si otterrebbero in cambio 1.123 USDT. I dati in verde invece, rappresentano il valore in USDT al quale gli utenti sono disposti a comprare EUR. Se questo valore fosse 1,113, con 1.000 USDT si otterrebbero 898,45 EUR. Quando il valore in "compra" e quello in "vendi" combaciano, avviene il trade. Solitamente, operazioni di questo tipo richiedono delle commissioni, il cui valore dipende dall'exchange e dalla coppia tradata.

L'utente che ha depositato EUR e vuole entrare in possesso per la prima volta di criptovaluta deve cercare la coppia EUR / USDT e nella schermata "vendi" *(figura 36)*, inserire il prezzo al quale è disposto a vendere e la quantità di EUR che vuole vendere. Quando il trade risulta confermato, vede nel proprio wallet gli USDT appena acquistati.

[56] Fonte: interfaccia grafica web Binance.

Procedendo con lo stesso ragionamento, cercando la coppia USDT / BTC, può acquistare bitcoin tramite USDT. Può talvolta accadere che una coppia di scambio non sia disponibile sull'exchange. In questo caso è necessario passare attraverso degli scambi intermedi. Ad esempio, possiedo X e voglio Z ma la coppia X / Z non è disponibile. Cerco Y e vedo che sono disponibili sia X / Y che Y / Z. Allora vendi X e acquisto Y, poi tramite Y acquisto Z.

Dopo aver depositato denaro e aver comprato criptovaluta, è consigliato, per una questione di sicurezza trattata dopo, prelevare la liquidità dall'exchange. È possibile prelevare direttamente la criptovaluta, oppure convertirla in valuta fiat e prelevare quest'ultima. I processi sono diversi e illustrati successivamente.

- **Prelievo di valuta fiat**
  Questo caso si presenta quando un soggetto vuole ritirare parte dei depositi in euro, perché ne ha bisogno o perché semplicemente ha registrato una plusvalenza e decide di prendere profitto. L'interfaccia di prelievo è riportata in *figura 38*[57]. Binance offre la possibilità di prelevare sulla carta usata per il deposito oppure di inviare il denaro direttamente al conto corrente.

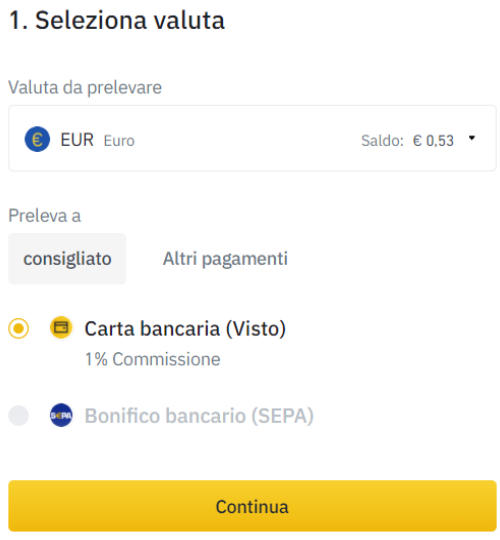


Figura 38 - Prelievo fiat

Figura 39 - Prelievo crypto

[57] Fonte: interfaccia grafica web Binance.

- **Prelievo di criptovaluta**

  La criptovaluta, ovviamente, non può essere inviata direttamente al conto bancario, tuttavia ci sono due diverse modalità disponibili per il prelievo.

  Il primo è il prelievo su **Binance card** (*figura 40*[58]). Questa carta è erogata gratuitamente da Binance agli utenti che ne fanno richiesta. Gira su circuito Visa e non ha alcuna commissione amministrativa o di elaborazione. Inoltre, restituisce all'utente una percentuale di cashback variabile, sulla base della quantità di BNB (criptovaluta di Binance) posseduti. Rispetto alle normali carte a cui si è abituati, offre la possibilità di "contenere" criptovalute. Nel momento in cui si utilizza la carta per pagare in negozio, questa effettua automaticamente la conversione in valuta fiat della criptovaluta disponibile.

Figura 40 - Binance card

  Il secondo metodo consiste nell'invio di criptovaluta ad un **wallet,** un portafoglio elettronico per la detenzione in sicurezza di criptovaluta (si rinvia al paragrafo successivo). La schermata di prelievo è riportata in *figura 39*[59]. I passaggi da seguire sono i seguenti: scegliere la criptovaluta da prelevare, inserire l'indirizzo del wallet al quale inviarla e immettere le informazioni richieste per autorizzare il prelievo. La cosa fondamentale da verificare è che il wallet supporti la rete impostata al momento del prelievo. In caso contrario si corre il rischio di perdere, senza possibilità di recupero, le proprie criptovalute. Una cosa da aver ben chiara è che non tutti i token supportano tutte le blockchain e, se anche il token supporta una determinata blockchain, è possibile utilizzarla solo se l'exchange lo consente. Ad esempio, ETH può essere trasferito usando la rete Ethereum (che ha commissioni elevate), oppure la rete Solana, oppure la Binance Smart Chain (BSC), che si caratterizza per commissioni molto basse. Binance supporta la BSC, mentre FTX no. Poiché ciascuna rete ha le proprie fees, è fondamentale, quando si acquistano criptovalute, considerare anche questo aspetto. Per concludere, è opportuno precisare che non tutti i token supportano tutte le blockchain. Ad esempio, Ether può essere trasferito

[58] Fonte: https://www.google.com/search?q=binance+card&sxsrf=AOaemvI9Rpm_HL6Ldx0Z-A8UogRdlmx1ug:1642886436004&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjE_LHzpMb1AhWTQuUKHQVACWsQ_AUoAXoECAEQAw&biw=1536&bih=764&dpr=1.25#imgrc=DT8VhFcXoMLubM.
[59] Fonte: interfaccia grafica web Binance.

usando più reti, mentre bitcoin solo usando la blockchain Bitcoin e sostenendone i relativi costi e i relativi tempi.

2.2 La conservazione

Le criptovalute sono risorse digitali scambiate tramite la rete. Come tutto ciò che è in rete, sono soggette a molti rischi, soprattutto legati ad attacchi hacker alle vulnerabilità delle piattaforme su cui vengono depositate. Al fine di conservare e utilizzarle in sicurezza, è possibile seguire alcuni accorgimenti.

- Il primo è l'utilizzo di un **PC ad uso esclusivo**, con il quale si utilizzano solo le criptovalute e non si naviga su siti internet che non si conoscono, per evitare il rischio di malware. Inoltre, è fondamentale non collegare tale PC a reti Wi-Fi pubbliche, per evitare il rischio di attacchi esterni. Anche il sistema operativo è importante, statisticamente Mac OS e Linux, sono meno vulnerabili ad attacchi esterni rispetto a Windows.

- **Credenziali**: è importante utilizzare password forti e molto diversificate fra di loro. Per salvarle è possibile usare dei password manager, come quello offerto da Trezor, che consentono di accedere a tutte le password tramite una Master Password e l'utilizzo dell'autenticazione a due fattori. Riguardo quest'ultima, è importante notare che quella che fa uso degli SMS è la meno sicura. Una 2FA più sicura è rappresentata da app come Authy o Google Auth, che generano un codice a 6 cifre, che varia ogni 30 secondi e senza il quale non è possibile accedere ai servizi sui quali sono depositate le criptovalute.

- Utilizzare siti famosi e certificati dagli enti regolatori in materia di sicurezza.

- Non lasciare le criptovalute sugli exchange, ma depositarle in wallet offline, che possono essere hardware o software.

2.3.1 Il wallet: cos'è e quali sono le diverse tipologie

Il wallet è uno strumento che consente di interagire con la rete blockchain. Contrariamente a quanto si crede, infatti, il wallet non contiene fisicamente la criptovaluta, bensì le informazioni necessarie a movimentarle. In particolare, ogni wallet ha una coppia di chiave privata e pubblica e un indirizzo derivato da quest'ultima. Le criptovalute sono "salvate" sulla blockchain, il saldo di criptovalute che un utente vede nel proprio wallet non è altro che la differenza tra le transazioni inviate verso l'indirizzo del wallet e quelle inviate dal wallet all'esterno. Per inviare le proprie criptovalute al wallet, basta effettuare un'operazione di prelievo come sopra descritto, usando come address quello del wallet. L'ammontare di ogni singola transazione, per la costruzione del saldo, è facilmente reperibile dall'intera blockchain. Tramite la chiave privata è possibile autorizzare ciascuna transazione e attraverso questa, è possibile recuperare le proprie criptovalute in caso di problemi al wallet.
Esistono diverse tipologie di wallet:

- Software wallet
  Questa tipologia si caratterizza per la connessione a internet e comprende:

  - Web wallet: per utilizzarli basta utilizzare un'interfaccia browser, senza alcun bisogno di scaricare applicativi o estensioni. Generalmente in questa tipologia di wallet, la gestione della chiave privata è affidata all'ente che offre il servizio di custodia. Questo rappresenta un aspetto positivo per chi è inesperto, ma anche un grosso rischio, infatti le chiavi private sono esposte ad un attacco da parte di soggetti malevoli. Appartengono a questa categoria gli exchange wallet, come quello di Binance.

  - Desktop wallet: come suggerisce il nome, un desktop wallet è un software scaricato ed eseguito localmente sul proprio PC. Al contrario dei web wallet, questi garantiscono la gestione delle proprie chiavi private all'utente. Quando un desktop wallet viene scaricato, questo genera un file chiamato "wallet.dat", salvato localmente sul PC. Al suo interno sono presenti le informazioni relative alle chiavi pubblica e privata, per questo va protetto con una propria password. Ogni volta che si effettua l'accesso al portafoglio, la password viene richiesta *(figura*

52) A questo punto ci sono due modi per fare un backup del wallet, salvare la password associata al file dat e il file stesso, oppure esportare la chiave privata associata al wallet. È importante notare che al fine di utilizzare le informazioni contenute nel file dat. Questo deve essere salvato sul dispositivo sul quale viene eseguito il desktop wallet. Questo processo di backup è fondamentale, perché così facendo, potrai accedere ai tuoi fondi da altri dispositivi, nel caso in cui il tuo computer smettesse di funzionare o diventasse in qualche modo inaccessibile. In generale, i desktop wallet possono essere considerati più sicuri della maggioranza di versioni web, ma è importante verificare che il computer sia privo di virus e malware prima di creare e usare uno wallet per criptovalute. Un esempio di desktop wallet è Metamask desktop *(figura 41 e 42[60]).*

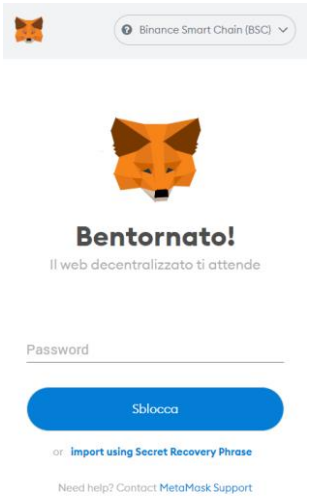


Figura 42 - Accesso a Metamask

Figura 41 - Interfaccia Metamask

- Mobile App wallet: funzionano in modo analogo ai desktop wallet, con la differenza che sono stati progettati per funzionare su mobile. Grazie alla disponibilità di fotocamere sugli smartphone, gli indirizzi vengono spesso rappresentati tramite QR-code. Per questo motivo sono molto utili per eseguire operazioni giornaliere, come i pagamenti, rendendoli una valida soluzione per spendere criptovalute

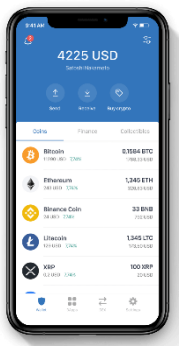


Figura 43 - Trust Wallet

[60] Fonte: interfaccia estensione browser Metamask.

nel mondo reale. Esempi di mobile wallet sono Trustwallet *(figura 43[61])* e Metamask. Quest'ultimo è molto utilizzato nella DeFi.

Tuttavia, proprio come i computer, i dispositivi mobili sono vulnerabili ad app malevoli e all'infezione da parte di malware. Pertanto, si consiglia di proteggere il wallet mobile con una password e di eseguire il backup delle chiavi private (o seed phrase) nel caso in cui lo smartphone si perda o si rompa.

- Hardware wallet: sono dispositivi elettronici che tramite un generatore di numeri casuali (RNG) generano chiavi pubbliche e private. Contrariamente a quanto avviene con i wallet online, questi dispositivi non sono connessi a Internet e le chiavi non lasciano mai il dispositivo. Esempi di hardware wallet sono il Ledger (figura 44[62]) e il Trezor. Quando si invia una transazione con il Ledger, questa è firmata direttamente internamente al dispositivo e la chiave usata resta sempre custodita al suo interno. Per questo motivo, questi dispositivi offrono un livello di sicurezza superiore ai precedenti, per contro sono meno user-friendly e l'accesso ai fondi non può essere fatto in un qualsiasi momento. Inoltre, l'acquisto di un hardware wallet rappresenta un costo per l'utente, pertanto sono consigliati a coloro che hanno intenzione di detenere a lungo le criptovalute, o a chi ne possiede una grande quantità.

Figura 44 - Wallet Ledger

- Paper wallet: è un pezzo di carta su cui vengono stampati fisicamente un indirizzo e la sua chiave privata sotto forma di QR code. La scansione di questi codici permette di eseguire transazioni di criptovalute. Pertanto, questi wallet sono altamente resistenti ad attacchi informatici online e possono essere considerati come un'alternativa ai wallet offline. Tuttavia, presenta numerosi punti deboli, che lo rendono ormai obsoleto. Il principale punto debole dei paper wallet è che non consentono di inviare fondi parzialmente, ma solo l'intero saldo in una volta sola. Ad esempio, si immagini di avere un paper wallet al quale sono state inviate 5 transazioni da 2 BTC, per un totale di 10 BTC. Per spenderne solo 2, è necessario prima inviare

[61] Fonte: https://trustwallet.com/.
[62] Fonte: https://www.amazon.it/stores/Ledger/Ledger/page/0D6ED38C-E09F-4DBB-96E9-7B51E71E94EC.

tutte e 10 le monete a un altro tipo di wallet (ad es., un desktop wallet), e da lì spendere i 2 BTC. In seguito, bisogna riportare gli 8 BTC a un nuovo paper wallet.

Indipendentemente dal wallet che si decide di utilizzare (esclusi gli exchange wallet che le gestiscono per conto dell'utente) si pone il problema *della gestione della chiave private.* Tipicamente la chiave è rappresentata da 24 parole *(figura 45*[63]), grazie alle quali è possibile accedere al wallet ed entrare in possesso di tutto ciò che vi è all'interno. Il modo migliore di conservarla è su un supporto offline, ad esempio cartaceo. Qualora si opti per quest'ultimo, è consigliato aggiungere una parola a scelta alle 24 reali, in modo tale che se qualcuno dovesse entrare in possesso del foglio, non riesca comunque ad accedere ai fondi in esso contenuti. La cosa fondamentale è comprenderne l'importanza e qualunque sia il modo scelto per conservarla, cercare di farlo sempre con la massima sicurezza, facendo sì che nessuno ne possa entrare in possesso.

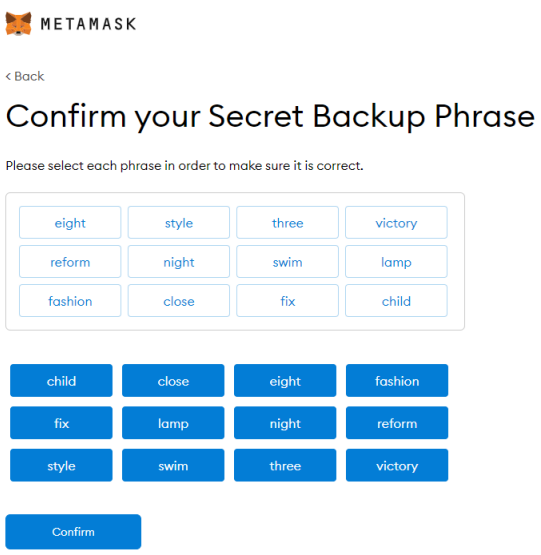


Figura 45 - Seed phrase Metamask

2.3 La vendita

La vendita di criptovalute è un meccanismo molto semplice. Tutto ciò che l'utente deve fare è eseguire inversamente i passaggi svolti durante l'acquisto. In altre parole, è sufficiente recarsi nella schermata di trading, cercare la coppia d'interesse e vendere

[63] Fonte: interfaccia Metamask.

la criptovaluta per ottenere una valuta stabile ed eliminare la propria esposizione alla volatilità, il tutto in pochi secondi. La valuta scelta come scambio può essere una valuta a corso legale, ma non è l'unica possibilità. Infatti, negli ultimi anni si sono sviluppati dei token particolari chiamati stablecoin. Questi, tramite diversi metodi replicano il valore della valuta fiat a cui sono ancorati. Ad esempio, BUSD, la stablecoin di Binance, replica esattamente il prezzo del dollaro, rappresentando così un bene rifugio dall'estrema volatilità del mercato cripto. Se un utente ha bisogno di denaro da spendere nel mondo reale, può decidere di vendere le criptovalute in cambio di EUR, se invece l'intenzione è quella di coprirsi dalla possibilità di un bear market, prendere profitto, o ancora, quella di chiudere una posizione su un progetto che non ritiene abbastanza valido, può farlo ottenendo stablecoin. Il vantaggio di detenere queste ultime è rappresentato dal fatto che sono prontamente disponibili per essere riutilizzate e che, rispetto alla valuta fiat, sono presenti in un numero molto superiore di coppie di trading. Le operazioni di vendita possono essere fatte in un qualsiasi istante e in qualsiasi giorno della settimana, il mercato delle criptovalute è infatti aperto 24/7. Questo, insieme ad altri fattori come la supply limitata, rendono tale mercato molto volatile, con le conseguenze positive e negative del caso. Le opportunità di guadagno sono molte, ma non bisogna fare l'errore di sottovalutare i rischi. Sono milioni le persone che decidono di investire in criptovalute i risparmi di una vita, credendo nella possibilità di ottenere guadagni facili. La maggior parte di esse perde tutto, finendo per trovarsi in una situazione economica estremamente spiacevole. Nel prossimo capitolo, con l'obiettivo di esporre concretamente i rischi che queste comportano, viene fatto uno studio della volatilità delle principali criptovalute. Inoltre, per offrire un termine di paragone, viene riportato un confronto tra il mercato delle criptovalute e quelli tradizionali.

CAPITOLO TRE

3. INVESTIMENTI E VOLATILITÀ DELLE CRIPTOVALUTE

3.1 Titoli scelti e loro descrizione

Le tipologie di asset per le quali, nelle pagine seguenti, verrà analizzata la performance con particolare attenzione alla volatilità registrata sono criptovalute, indici azionari, indici obbligazionari e indici del mercato real estate.

Criptovalute: quelle utilizzate ai fini dell'analisi sono tre. Le prime due sono quelle a maggior capitalizzazione di mercato, ovvero *bitcoin (BTC)* ed *Ether (ETH)*, che rappresentano anche quelle più stabili. La terza è una criptovaluta molto conosciuta e altrettanto volatile, *Dogecoin (DOGE).*

Indici azionari: sono stati utilizzati un indice rappresentante il mercato europeo, uno che riguarda il mercato statunitense e per concludere un indice globale.

Euro Stoxx 50: è il principale indice blue-chip europeo per l'Eurozona, fornisce una rappresentazione blue-chip dei leader del dei settori industriali dell'area. L'indice copre 50 titoli di 8 paesi dell'Eurozona: Belgio, Finlandia, Francia, Germania, Irlanda, Italia, Paesi Bassi e Spagna.

S&P 500: è ampiamente considerato come il miglior indicatore singolo di azioni statunitensi a grande capitalizzazione. L'indice comprende 500 aziende leader e copre circa l'80% della capitalizzazione di mercato disponibile.

S&P Global 1200: offre un'esposizione efficiente al mercato azionario globale, catturando circa il 70% della capitalizzazione di mercato globale. È costruito tramite la composizione di sette indici principali, molti dei quali sono leader accettati nelle loro regioni. Questi includono S&P 500® (US), S&P Europe 350, S&P TOPIX 150 (Giappone), S&P/TSX 60 (Canada), S&P/ASX All Australian 50, S&P Asia 50 e S&P Latin America 40.

Indici obbligazionari: sono stati utilizzati un indice globale contenente obbligazioni statali e uno che riguarda le obbligazioni emesse dalle società.

S&P Global Developed Sovereign Bond: è un indice completo, ponderato in base al valore di mercato, concepito per replicare la performance dei titoli denominati in valuta locale emessi pubblicamente dai paesi sviluppati per i loro mercati nazionali.

iShares global corporate bond ETF: è un fondo che mira a replicare il più fedelmente possibile, l'andamento di un indice composto da obbligazioni societarie investment grade di emittenti dei mercati emergenti e sviluppati.

Indice real estate: è stato utilizzato lo *Stoxx Global 1800,* il quale comprende le principali 1800 società globali che sono classificabili nel settore Real Estate.

3.2 Assunzione di distribuzione normale

Le analisi sono effettuate sui rendimenti giornalieri di ciascun asset, in un periodo che va dal 01/01/2016 al 03/10/2021, per un totale di 2103 osservazioni. La distribuzione dei rendimenti ipotizzata è quella Gaussiana. Questa distribuzione, come noto, non permette una perfetta approssimazione dell'andamento dei vari asset. Per questo motivo, di seguito, è riportata un'analisi di normalità, che ha l'obiettivo di evidenziare in che modo ciascun asset si discosta dall'ipotesi distributiva adottata. In particolare, vengono calcolati i valori di curtosi e asimmetria, con l'obiettivo di valutare la possibilità del verificarsi di eventi non prevedibili dalla distribuzione normale. Infine, è riportato un QQ Plot, per evidenziare anche graficamente la differenza tra la distribuzione reale dei rendimenti e quella normale.

Nella *figura 47*[64] è riportato l'istogramma delle frequenze dei rendimenti giornalieri di **bitcoin**, confrontato con le frequenze di una distribuzione normale caratterizzata dalla stessa media e deviazione standard di quella di BTC. La prima cosa che si vede è la maggior concentrazione dei rendimenti di BTC nell'intervallo tra -0,94% e 1,55%.

[64] Figure da 46 a 77 (eccetto 73) elaborate personalmente.

Questa evidenza è ribadita anche dall'indice di curtosi, che assume un valore di 7, contro lo 0 della distribuzione normale. Per quanto riguarda la simmetria invece, i rendimenti di bitcoin registrano un indice di asimmetria pari a -0,1, molto simile a quello di una distribuzione normale. I rendimenti di bitcoin, quindi, tendono a concentrarsi intorno al valore medio, infatti la probabilità che si verifichi un rendimento compreso tra $\mu + \sigma$[65] e $\mu - \sigma$ è del 78% nel caso reale, contro il 68% nel caso di ipotesi distributiva normale. In questo senso, l'ipotesi effettuata potrebbe apparire come conservativa, infatti la probabilità di un rendimento inferiore a $\mu - \sigma$ è superiore nel caso normale. Tuttavia, c'è un altro fenomeno da considerare, quello dei rendimenti estremi, sia positivi che negativi. Infatti, mentre nella distribuzione normale la probabilità che si verifichino è remota, nel caso reale, è molto più elevata. Il problema è visibile guardando al Q-Q plot riportato in *figura 46*. Infatti, si vede come, nella parte iniziale e in quella finale, i rendimenti di BTC si discostino notevolmente da quelli di una distribuzione normale. Nel momento in cui si accetta l'ipotesi Gaussiana, questo fattore deve essere preso in considerazione in quanto rappresenta un rischio per gli investitori. Ad esempio, se un soggetto volesse conoscere la probabilità di perdere più del 10% in un solo giorno, stando alla distribuzione normale sarebbe lo 0,5%, mentre in realtà, stando ai dati storici, sarebbe tre volte superiore.

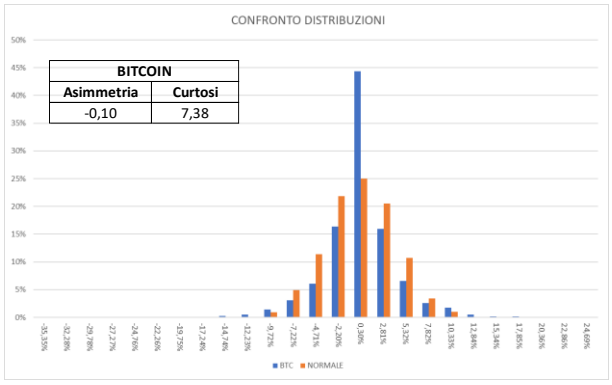


Figura 47 - Distribuzione bitcoin

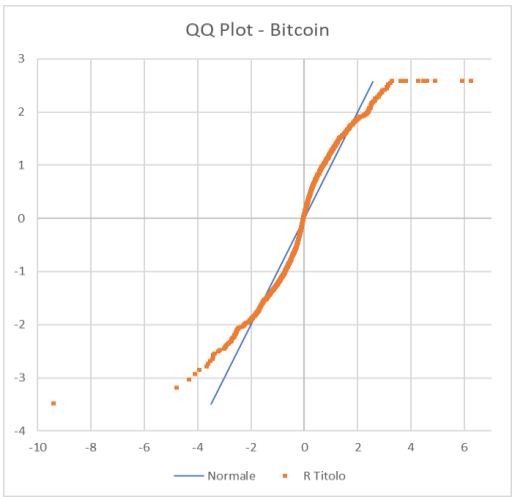


Figura 46 - QQ plot bitcoin

Per quanto riguarda **Ether**, la situazione è molto simile a quella illustrata parlando di bitcoin. Nella *figura 49* c'è una tendenza dei rendimenti a concentrarsi attorno alla

[65] μ e σ: indicano rispettivamente il valore atteso e la deviazione standard dell'insieme di dati considerato.

media e l'indice di asimmetria è simile a quello di una distribuzione normale. In particolare, in questo caso è positivo, pertanto ETH presenta una coda più lunga sul lato destro della distribuzione, quello dei rendimenti positivi. Infine, come si vede in *figura 48,* ancora una volta si verifica il problema dei rendimenti estremi.

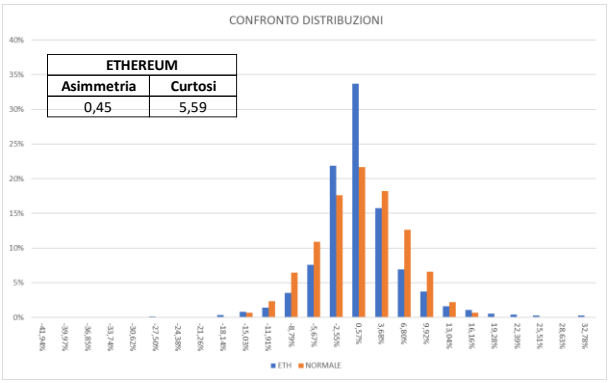


Figura 49 - Distribuzione Ether

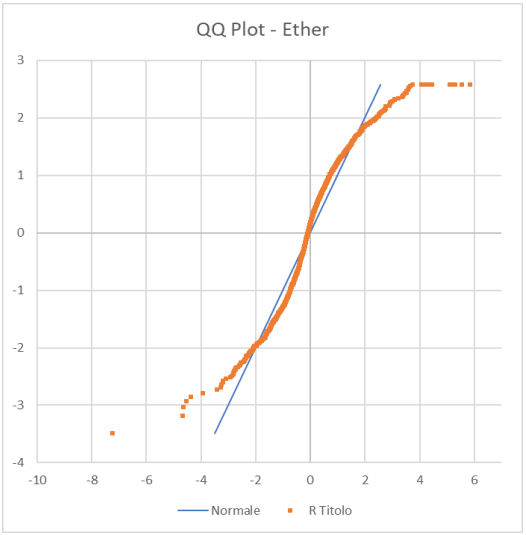


Figura 48 - QQ plot Ether

Le cose cambiano nel caso di una valuta più volatile come **Doge**. Sia dall'indice di curtosi, sia dall'asimmetria (*figura 51)*, appare un forte allontanamento dalla distribuzione normale. Un valore di 525 nell'indice di curtosi comporta un grandissimo accentramento dei valori della distribuzione attorno al valore medio. In una situazione come questa, l'utilizzo di un'ipotesi distributiva normale, genera dei valori molti diversi da quelli reali. Tuttavia, un'analisi più approfondita, mostra che assumendo tale ipotesi, si otterrebbe una valutazione conservativa del rischio. Infatti, come detto prima, in una distribuzione normale il 68% dei rendimenti cade tra μ + σ e μ – σ, mentre nella distribuzione reale di Doge, questo accade nel 91% dei casi. Inoltre, l'alto valore di asimmetria positiva, comporta un allungamento della coda destra. Questo significa che i rendimenti la cui probabilità di accadimento viene sottovalutata dall'ipotesi di normalità, sono positivi e quindi non comportano un rischio di perdita per l'investitore. Numericamente parlando, la probabilità che un rendimento sia inferiore a μ – 2,576 *σ è del 0,28% nel caso reale, contro lo 0,5% del caso normale, mentre la probabilità che il rendimento superi μ + 2,576*σ è doppio nel caso reale rispetto a quello normale. A testimonianza dell'influenza dei rendimenti molto positivi sui valori degli indici, in *figura 51* sono riportati i valori di curtosi e asimmetria, ottenuti imponendo un limite massimo del 50% al rendimento giornaliero. Un problema che invece resta presente è quello dei

rendimenti estremi, che richiedono, per la valutazione del rischio complessivo, l'introduzione di opportune misurazioni (*figura 50*).

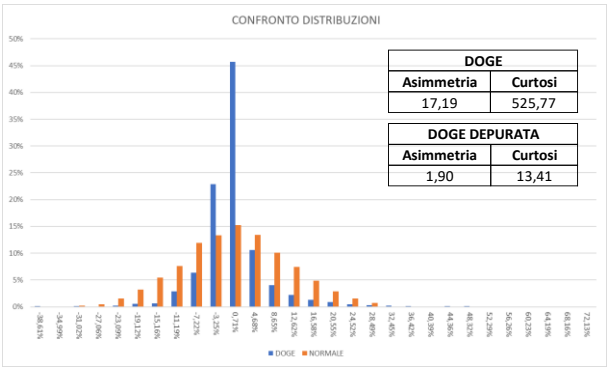


Figura 51 - Distribuzione Doge

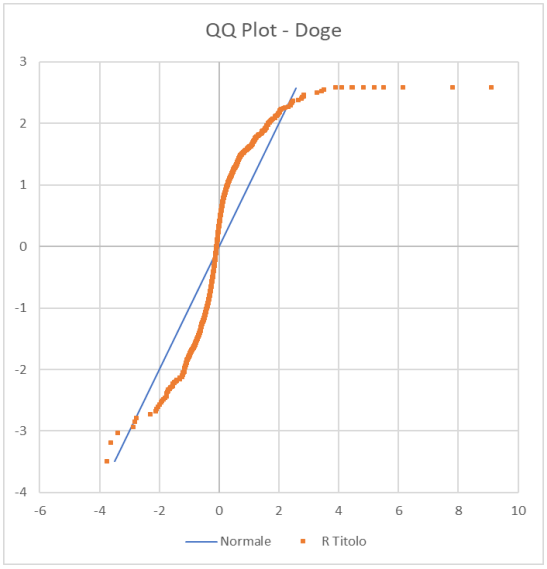


Figura 50 - QQ plot Doge

Gli indici azionari, presentano tutti più o meno le stesse caratteristiche. In particolare, sono caratterizzati sia da un elevato valore di curtosi, sia dalla presenza di un forte discostamento dalla normalità nei pressi dei rendimenti più elevati in termini assoluti. Rispetto alle criptovalute, l'asimmetria è sempre negativa, sintomo di rendimenti negativi che tendono a protrarsi di più rispetto a quando dovrebbero fare in una distribuzione normale.

La grande concertazione dei rendimenti attorno alla media, è dovuto ad una determinata scelta presa riguardo ai dati. Poiché le criptovalute sono un mercato aperto 24/7, mentre il mercato tradizionale non lo è, nei giorni di chiusura del mercato, il valore di ciascun asset è stato supposto uguale all'ultima quotazione disponibile. In questo modo, nei giorni di chiusura il rendimento dell'asset è pari allo 0%. In ogni caso, come per le criptovalute, può essere accettata l'ipotesi di distribuzione normale, ma è fondamentale aver chiara la presenza della possibilità di rendimenti, che la distribuzione normale non avrebbe potuto prevedere, soprattutto nei casi estremi. Nelle figure di seguito riportate, sono trattati **Euro Stoxx 50** *figura 52 e figura 53),* **S&P 500** *(figura 54 e figura 55)* e **S&P Global 1200** *(figura 56 e figura 57)*.

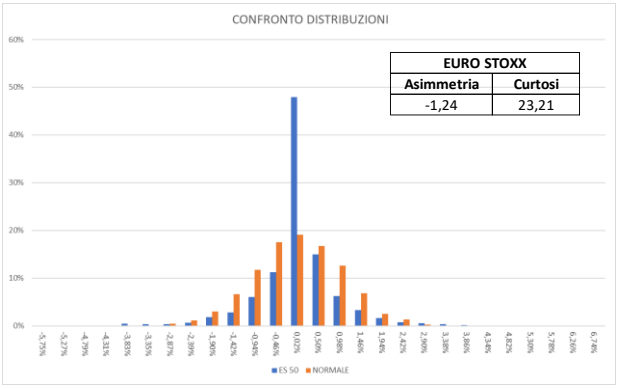


Figura 53 - Distribuzione Euro Stoxx 50

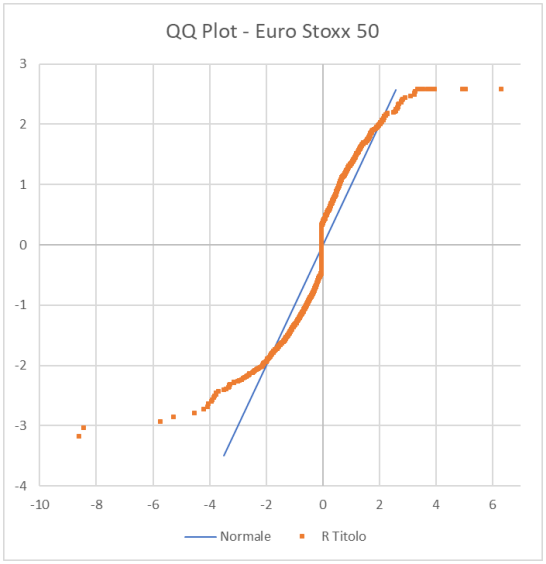


Figura 52 - QQ Plot ES 50

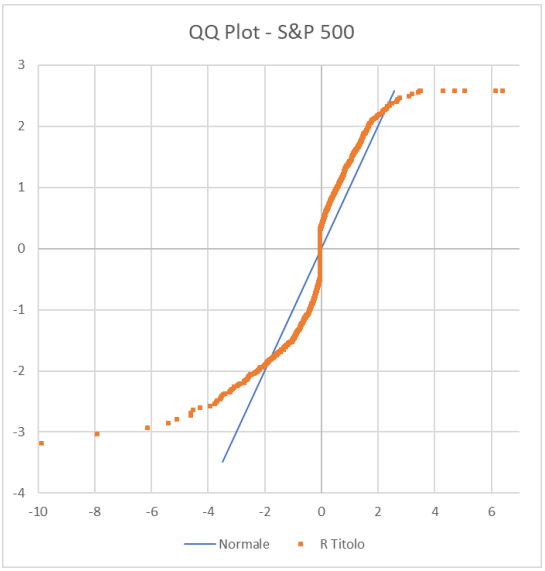


Figura 54 - QQ Plot S&P 500

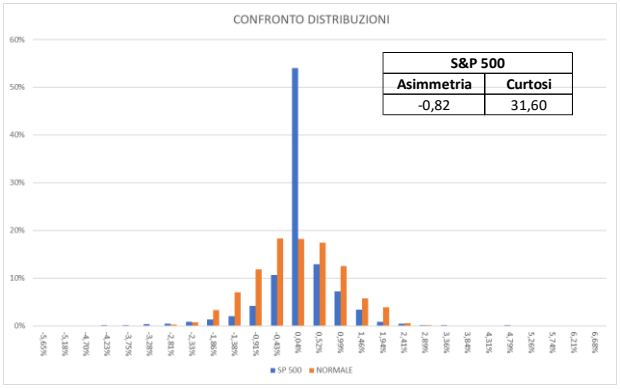


Figura 55 - Distribuzione S&P 500

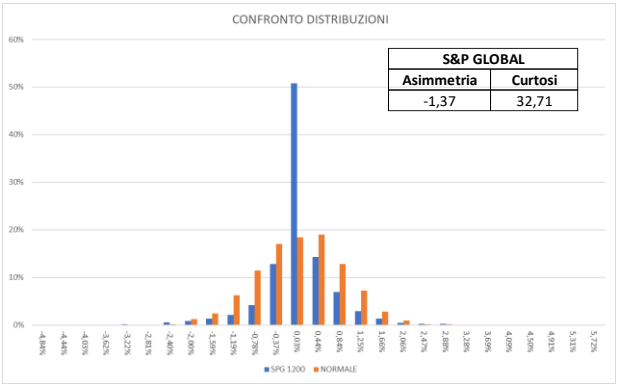


Figura 57 - Distribuzione S&P Global 1200

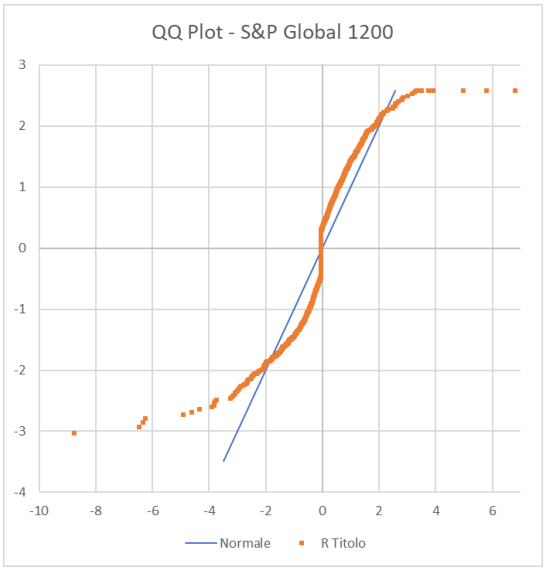


Figura 56 - QQ Plot S&P Global 1200

Per quanto riguarda gli indici obbligazionari e quello riguardante il real estate, la distribuzione dei rendimenti è piuttosto simile e non si discosta molto dalle situazioni del mercato azionario. L'unica differenza che si può notare è un maggior valore negativo della simmetria. Questo può portare una sottostima del rischio dei rendimenti negativi, quindi è importante evidenziare questo fatto e tenerne conto nel momento in cui si va a valutare la scelta degli asset sulla base del rischio di ognuno. Nelle figure seguenti sono riportate le analisi dei 2 indici obbligazionari, **S&P Global Sovereign** (*figura 58 e 59)* e **iShares Global Corporate** *(figura 60 e 61)* e dell'indice reale estate, lo **Stoxx Global 1800** *(figura 62 e 63)*.

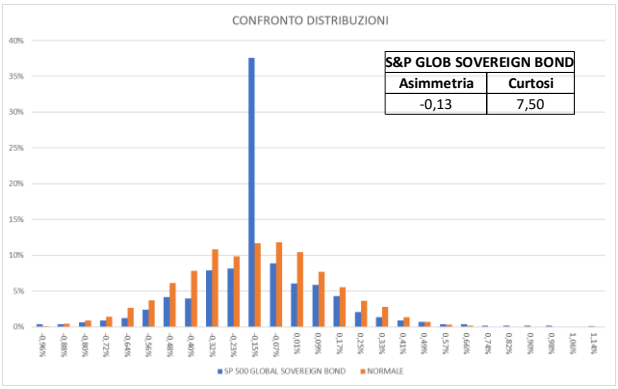


Figura 59 - Distribuzione S&P Global Sovereign Bond

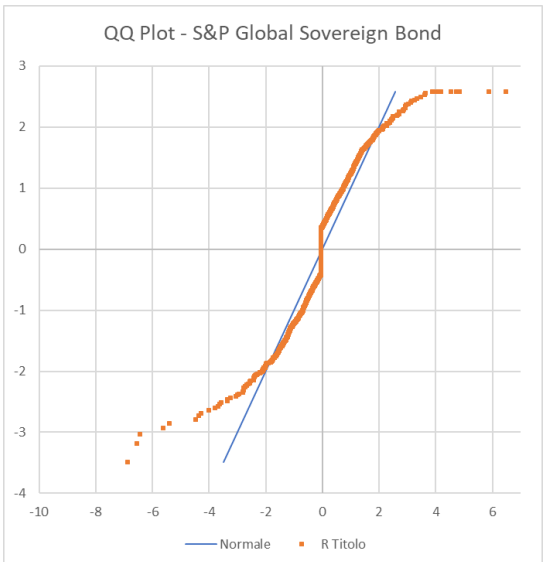


Figura 58 - QQ plot S&P Global Sovereign Bond

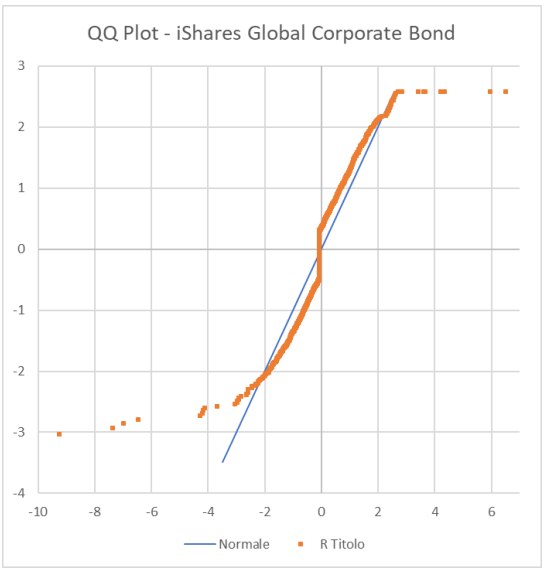


Figura 61 - QQ Plot iShares Global Corporate Bond

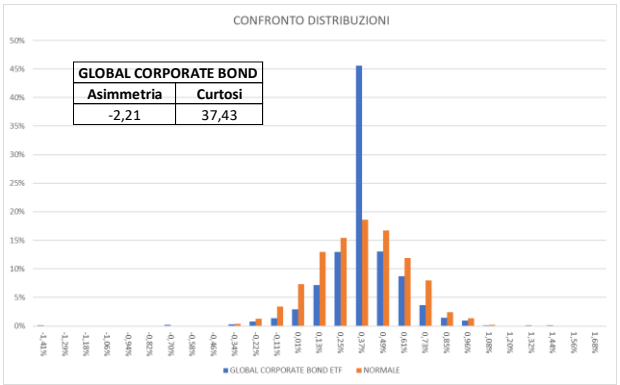


Figura 60 - Distribuzione iShares Global Corporate Bond

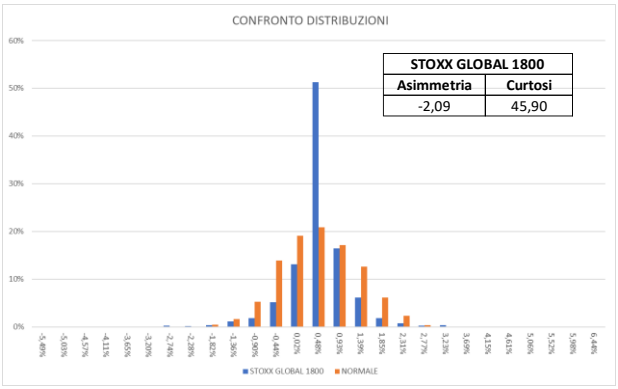


Figura 63 - Distribuzione Stoxx Global 1800

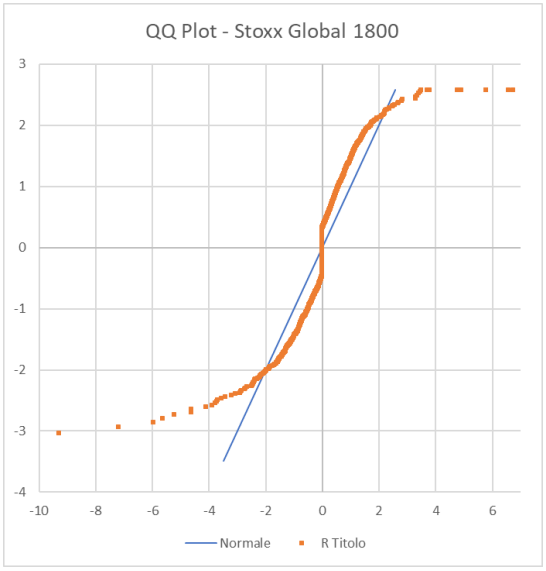


Figura 62 - QQ Plot Stoxx Global 1800

3.3 Gli indicatori di rischio assoluto

In questo capitolo, con il termine **rischio** ci si riferisce al **rischio finanziario**, ovvero alla possibilità che l'investimento, in una data futura, abbia un valore diverso a quello iniziale a causa delle oscillazioni del mercato. In generale, esistono diversi indicatori che consentono una misura quantitativa del rischio di un asset finanziario.

Una prima valutazione della rischiosità di un asset può essere fatta tramite il calcolo del range dei rendimenti. In *figura 64* sono riportati i rendimenti massimi e minimi giornalieri degli strumenti in analisi. In verde è rappresentato il valore del rendimento massimo registrato nel periodo considerato, in rosso quello minimo. Più una colonna è ampia, più l'asset è volatile e quindi rischioso. Da un primo sguardo al grafico, si può arrivare alla conclusione che le criptovalute rappresentano un investimento molto più rischioso del mercato azionario e a sua volta quest'ultimo è più rischioso di quello obbligazionario. Inoltre, anche all'interno del settore cripto stesso, le differenze sono molto marcate, ad esempio, Doge mostra un rendimento massimo svariate volte superiore a quello di BTC e ETH. Tuttavia, un'analisi di questo tipo è molto superficiale, infatti è molto influenzata dai rendimenti estremi, i quali possono essersi verificati una sola volta e non tiene conto della probabilità storica del verificarsi di un determinato livello di rendimento. Per questo motivo, le informazioni ricavabili da questa prima

analisi rappresentano un'indicazione generale, la quale necessità di un ulteriore approfondimento.

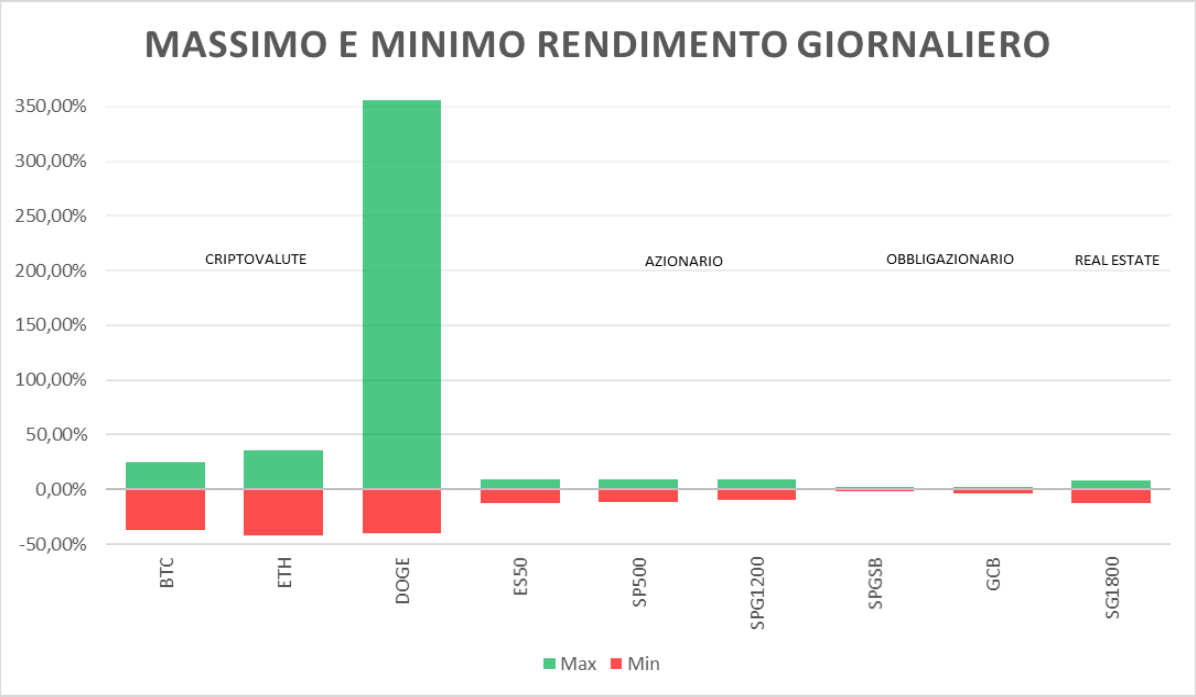


Figura 64 - Confronto rendimento massimo e minimo

Un indicatore molto utilizzato per valutare il rischio di un investimento è la deviazione standard (σ). Questa tiene conto di ciascun rendimento maturato nel periodo di tempo considerato, restituendo così una misura della variabilità del valore dell'asset. In altre parole, la deviazione standard esprime quanto un rendimento tende mediamente a discostarsi dalla media, in eccesso e in difetto. Ad esempio, se un titolo su un orizzonte settimanale ha μ = 5% e un σ = 10% significa che è lecito aspettarsi un rendimento settimanale compreso tra -5% e 15%. Nella *figura 65* è riportato un confronto tra le deviazioni standard dei vari asset.

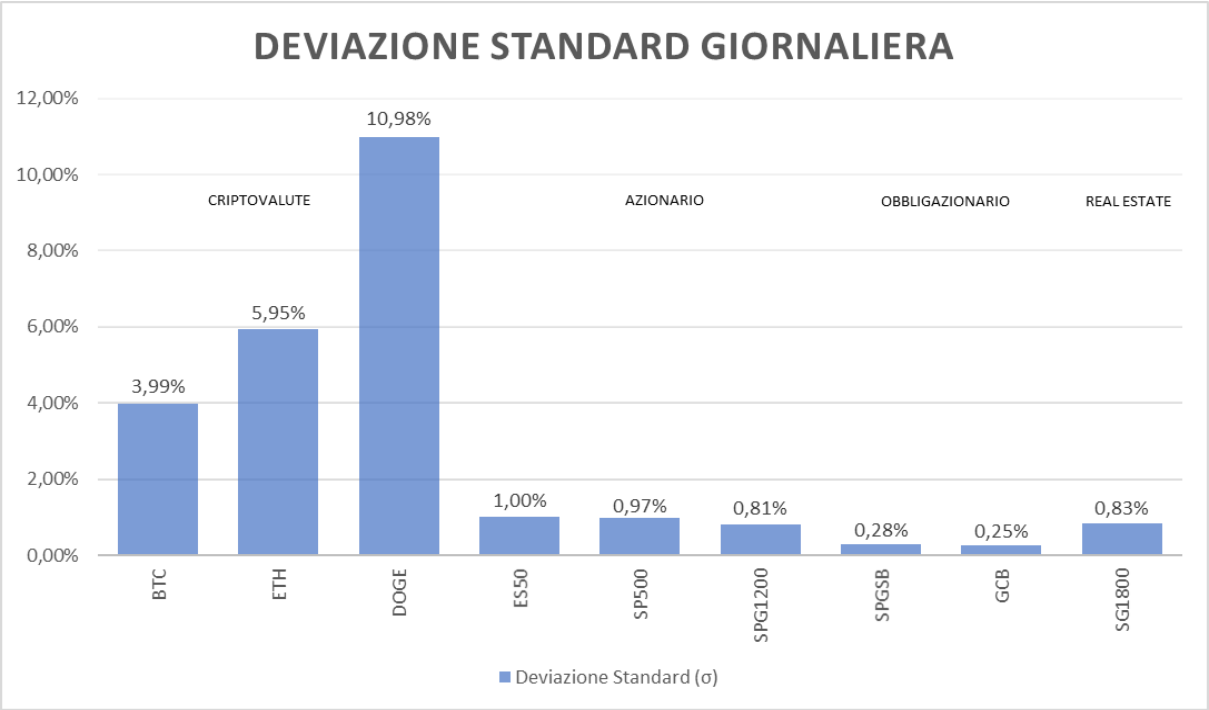


Figura 65 - Deviazione Standard

Dall'analisi del grafico è possibile vedere come le criptovalute siano caratterizzate da un rischio molto più elevato rispetto agli altri asset. Come era possibile aspettarsi, quelli meno rischiosi sono quelli obbligazionari, ma ciò che emerge maggiormente è che il mercato delle criptovalute si caratterizza per un livello di rischio mediamente otto volte superiore a quello associato ad un mercato già molto volatile come quello delle azioni. In particolare, una deviazione standard giornaliera del 10,98% su DOGE, significa che in un anno il suo valore potrebbe subire una variazione del 210% attorno alla media. BTC, che è considerata la criptovaluta più sicura e stabile, ha una deviazione standard giornaliera del 4%, in altre parole, tenuto conto di un rendimento medio dello 0,30%, 10.000 euro in BTC, in un giorno, possono mediamente diventare un valore compreso tra 9.630 euro e 10.400 euro. Per contro, investendo gli stessi 10.000 euro nell'indice S&P 500, questi varierebbero mediamente tra 9.908 euro e 10.100 euro. Tuttavia, è importante sottolineare che mentre la volatilità delle criptovalute si riferisce ad un singolo asset, quella dell'azionario è espressa facendo riferimento ai rendimenti di un indice, il quale tende a diminuire la volatilità delle azioni prese singolarmente.

Assumendo l'ipotesi di distribuzione normale dei rendimenti giornalieri e usando il concetto di deviazione standard, è possibile calcolare la perdita potenziale di un asset, in un determinato periodo di tempo e con un dato livello di probabilità. Questo indicatore è noto come Value at Risk (VaR) ed è molto utilizzato in finanza, infatti è molto facile

da interpretare. Guardando alla *figura 66*, si vede che ovviamente il VaR rispetta quanto già mostrato dalla deviazione standard, aggiungendo però delle informazioni. In particolare, i dati in figura sono stati calcolati usando un orizzonte temporale giornaliero e una confidenza del 99,5%. Prendendo ad esempio BTC, si vede che il VaR è pari al 10,06%. Questo significa che investendo 10.000 euro in bitcoin, la massima perdita giornaliera che un investitore può aspettarsi nel 99,5% dei casi è pari a 1.006 euro. Le osservazioni che possono essere fatte al VaR sono due:

- Se la distribuzione non è perfettamente normale, i valori possono risultare anche significativamente diversi. A questo proposito in *figura 76* sono riportati i valori del VaR al 99,5% non utilizzando i parametri di una distribuzione normale, bensì i dati storici reali. Da tale grafico si vede come, a causa del problema dei rendimenti estremi, l'assunzione di normalità tende a sottovalutare il VaR. L'unica eccezione è quella di DOGE e trova giustificazione nella forte asimmetria positiva e nei rendimenti negativi contenuti in valore.

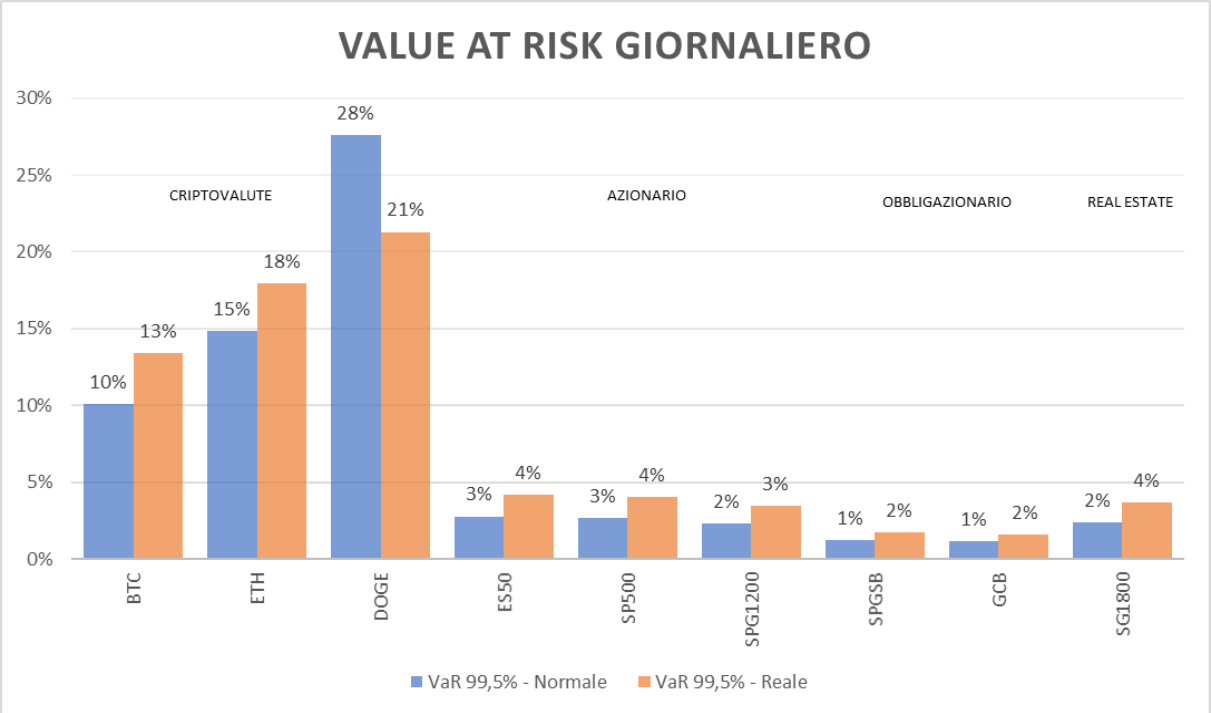


Figura 66 - Value at Risk

- Restituisce la massima perdita plausibile nel 99,5% dei casi, ma nel 0,5% delle situazioni rimanenti non fornisce alcuna misura del rendimento che potrebbe

verificarsi. Pertanto, questo potrà essere poco inferiore al VaR, ma anche molto più grande. Per dare una stima della perdita possibile in questi casi, in *figura 67* è riportato lo shortfall risk. Questo è calcolato come valore atteso dei rendimenti inferiori al Var ed è interpretabile come il rendimento medio nello 0,5% dei casi in cui il Value at Risk non viene rispettato. Guardando alla figura, si capisce come il rischio associato al mercato cripto sia grande, rispetto a quello relativo all'investimento in mercati tradizionali. Infatti, uno shortfall risk del 30%, sta ad indicare la possibilità, seppur remota che un capitale di 100.000 euro vada incontro ad una riduzione di 30.000 euro in un solo giorno.

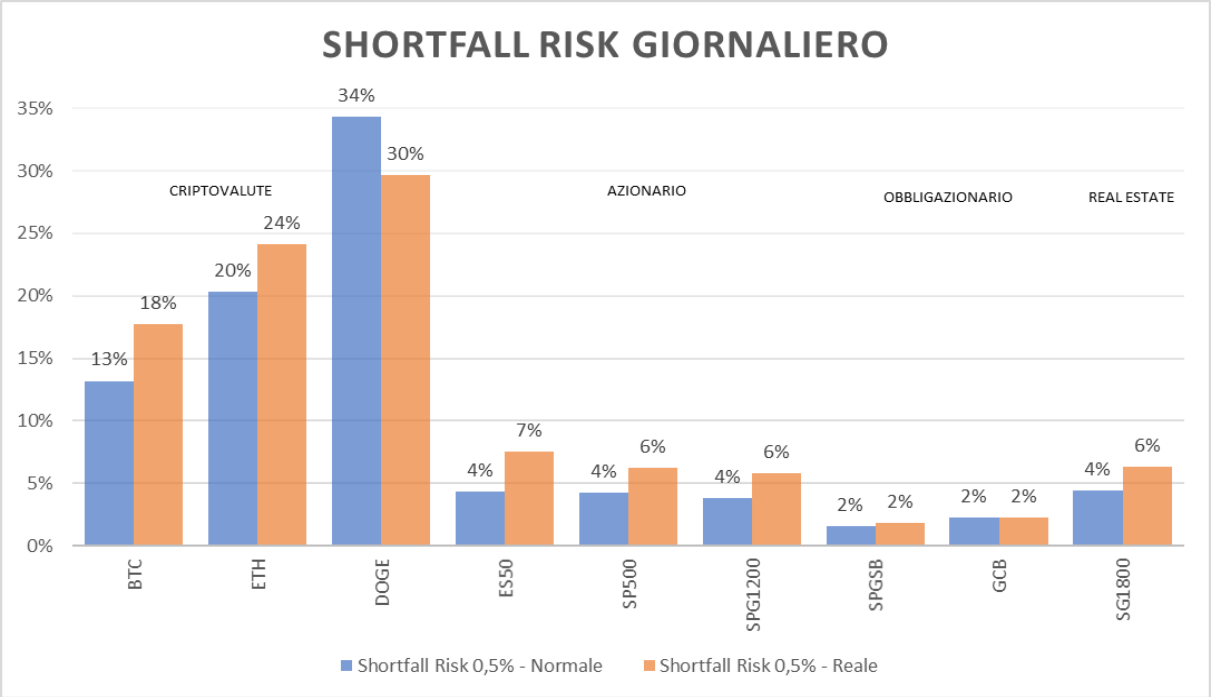


Figura 67 - Shortfall risk

Sebbene la deviazione standard sia un ottimo indicatore del rischio di un investimento, è spesso criticata per il fatto che considera con uguale peso, sia i rendimenti negativi che quelli positivi. Questi ultimi non rappresentano una perdita per l'investitore, quindi potrebbero esser considerati non negativi e non dovrebbero influire sulla valutazione relativa alle possibili perdite. Ad esempio, due titoli dotati di una deviazione standard simile, potrebbero essere completamenti differenti a livello di possibili perdite. Il primo potrebbe avere molti più rendimenti positivi, mentre il secondo molti rendimenti negativi, ma entrambi sono considerati in egual modo dalla deviazione standard e questo porterebbe ad una valutazione del rischio non focalizzata sulle possibili perdite. Per

questo è stata introdotta una nuova misura di quest'ultimo, il Downside Risk (*figura 68*). Questo indicatore è molto simile alla deviazione standard, tuttavia non considera lo scarto di ciascun rendimento dalla media, bensì da un valore target di rendimento. Nella figura questo target è lo 0%, in altre parole il valore del downside risk, esprime la deviazione standard dallo 0 dei soli rendimenti negativi, trascurando gli effetti sul rischio di quelli positivi. Per capire se le informazioni trasmesse sono diverse a quelle ottenute tramite l'analisi della deviazione standard, è possibile confrontare i dati del downside risk con i valori di μ - σ, riportati sempre in *figura 68*. Ciò che emerge è che la deviazione standard tende a sovrastimare il rischio, soprattutto su quegli asset dotati di asimmetria positiva, quindi caratterizzati da maggiori rendimenti positivi. Seppur questa analisi mostri ancora una volta come le criptovalute incorporino un maggior rischio, il divario con il mercato finanziario tradizionale, risulta ridotto dal downside risk, sintomo del fatto che la loro grande volatilità è dovuta anche ai grandi rendimenti positivi maturati. Tuttavia, è necessario ricordare che questo mercato è ancora relativamente piccolo e molto più soggetto a forti interessi speculativi, che ne aumentano notevolmente la rischiosità.

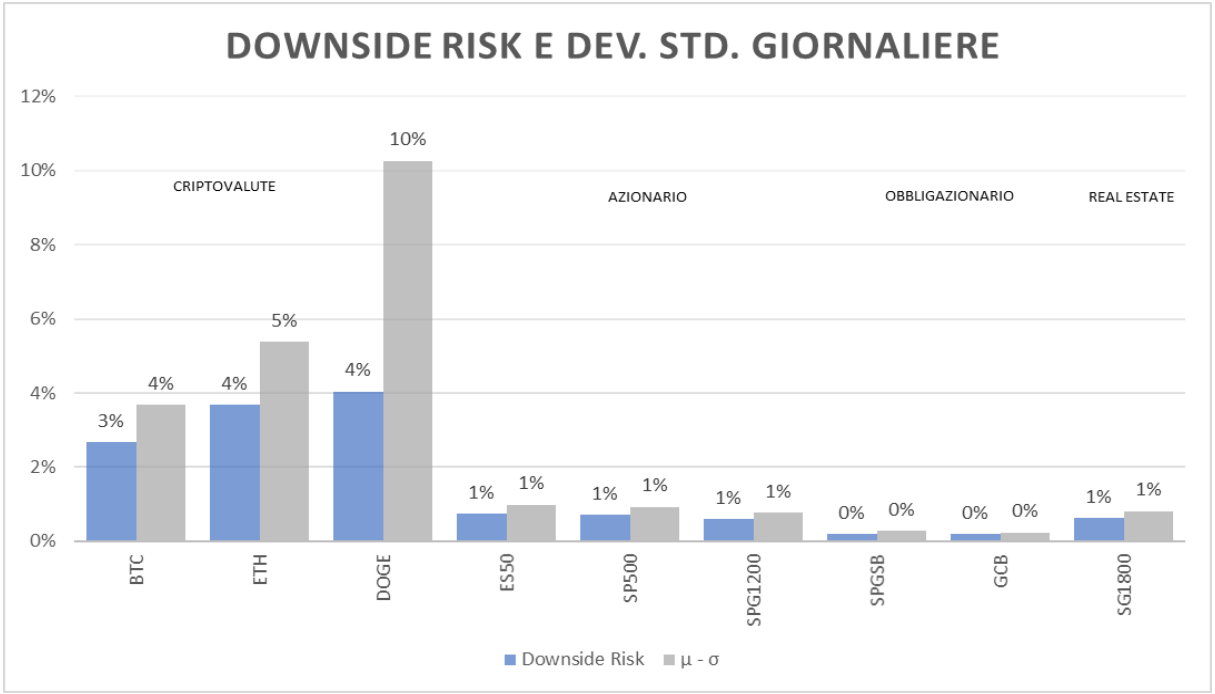


Figura 68 - Downside Risk VS Deviazione Standard

Gli indicatori di rischio riportati hanno dato risultati concordanti fra di loro. In tutti i casi le criptovalute sono risultate molto più rischiose di qualsiasi altro asset in analisi.

Tuttavia, la scelta di un investimento non è guidata solo dal rischio, ma anche dal rendimento che questo può produrre. Tipicamente ad un'alta rischiosità sono anche associati rendimenti maggiori e ciascun investitore ha la piena libertà di decidere il livello di rischio a cui esporsi ed accettarne i relativi rendimenti. Nella *figura 69* sono riportati i rendimenti reali e quelli teorici di ciascun asset. I rendimenti reali sono calcolati come variazione percentuale del prezzo giornaliero, dal 01/01/2016 al 03/10/2021, quelli teorici sono ottenuti tramite la formula del rendimento composto, basandosi sul rendimento medio giornaliero. La prima cosa che emerge è che i rendimenti teorici e reali nelle criptovalute sono totalmente diversi. Questo mostra l'impatto che i rendimenti estremi hanno sul valore medio, quindi l'importanza di avere indicatori di rischio basati anche sui soli rendimenti negativi. L'altro dato che emerge è che il rendimento di BTC, ETH e DOGE è di molto superiore a quello degli altri asset. Al fine di effettuare una scelta tra diversi asset, quindi, diventa necessario confrontarli considerando sia il rischio, sia il rendimento. Nel prossimo paragrafo viene effettuato un confronto tra i vari asset usando degli indicatori di rendimento corretti per il rischio.

ASSET	BTC	ETH	DOGE	ES50	SP500	SPG1200	SPGSB	GCB	SG1800
Rendimento Reale 2016 - 2021	10998%	360486%	143488%	28%	116%	84%	17%	32%	33%
Rendimento Teorico 2016 - 2021	59599%	14043603%	314629240%	42%	139%	97%	18%	33%	43%

Figura 69 - Confronto rendimenti

3.3.1 Confronto generale

Gli indicatori corretti per il rischio che verranno analizzati sono l'indice di Sortino e l'indice di Sharpe. Nella *figura 70,* sono riportati gli **indici di Sharpe** di ciascun asset, calcolato annualizzando la media e la deviazione standard giornaliere, calcolate sul periodo 2016 – 2021. Il valore dell'indice di Sharpe esprime il rendimento prodotto per unità di rischio, quindi maggiore è meglio è. Da questa analisi emerge come le criptovalute generino un rendimento corretto per il rischio maggiore rispetto agli altri asset. Quindi, nonostante queste siano caratterizzate da un valore di rischio molto più grande degli altri mercati, il rendimento che queste sono in grado di generare lo è ancora di più. In altre parole, per chi è disposto ad accettare la volatilità del mercato cripto, potrebbe ottenere un vantaggio rispetto a chi decide di investire, ad esempio, nell'azionario.

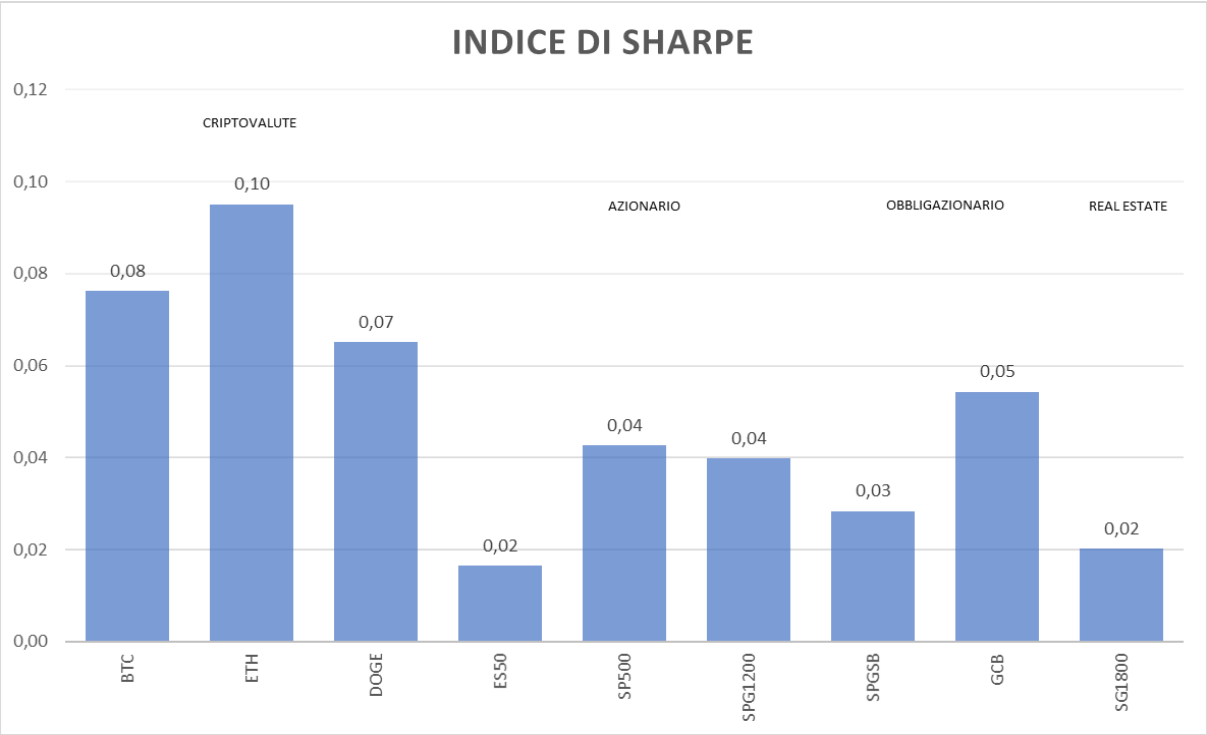


Figura 70 - Indice di Sharpe

Dai dati rappresentati, si vede come ETH sia l'asset più performante in termini di rendimento aggiustato per il rischio, in particolare il suo indice di Sharpe è il 150% superiore a quello dell'indice S&P 500 e il 25% superiore a quello di BTC. L'ES50 è quello con il minor valore, questo significa che non è in grado di ripagare in modo adeguato, il rischio che si corre detenendolo. Nel caso di titoli dotati di un indice di Sharpe molto simile, diventa importante effettuare delle analisi approfondite, maggiormente concentrate sul rischio. Infatti, lo Sharpe si basa sulla deviazione standard, pertanto porta con sé il limite dell'uguale peso attribuito ai rendimenti negativi e a quelli positivi. Per questo, molto spesso l'indice di Sharpe viene valutato insieme anche all'**indice di Sortino** *(figura 71)*. Quest'ultimo non utilizza la deviazione standard, bensì il downside risk. Quindi il valore dell'indice di Sortino è influenzato dalla sola variabilità dei rendimenti negativi, per questo tra due asset dotati di medesimo indice di Sharpe, è da preferire quello con un maggior indice di Sortino. Nei casi analizzati, si nota come sia l'indice di Sortino che quello di Sharpe, risultino maggiori nel caso del Global Corporate Bond rispetto all'Euro Stoxx 50. In effetti, guardando alla *figura 69*, il rendimento dei GCB è stato superiore rispetto a quello dell'ES50. Quindi sarebbe stato più remunerativo un investimento nel primo, rispetto ad un investimento in quest'ultimo e, addirittura, il rischio corso sarebbe stato inferiore. Analizzando invece il caso dell'SPGSB, si vede

come l'indice di Sortino risulta ancora una volta maggiore di quello dell'ES50, ma il rendimento in *figura 69* non lo è. Questo perché un indice superiore, non implica un rendimento superiore, bensì dice che il rendimento maturato non è stato molto buono rispetto al rischio che è stato corso. In effetti, VaR e Shortfall Risk dell'ES50 sono circa 3 volte superiori a quelli dell'SPGSB. Tuttavia, non sempre queste informazioni risultano corrette, soprattutto nel momento in cui si ha a che fare con asset caratterizzati da grandi movimenti estremi. Guardando alla *figura 69*, il grande divario tra rendimento teorico e reale nelle criptovalute, mostra come il rendimento medio sia fortemente influenzato dai rendimenti estremi. In questi casi, gli indici di Sortino e Sharpe risultano elevati per come sono costruiti, ma al fine di valutare correttamente l'investimento è importante considerare attentamente i parametri di rischio sopra riportati, come il Var, lo Shortfall risk e il Downside Risk.

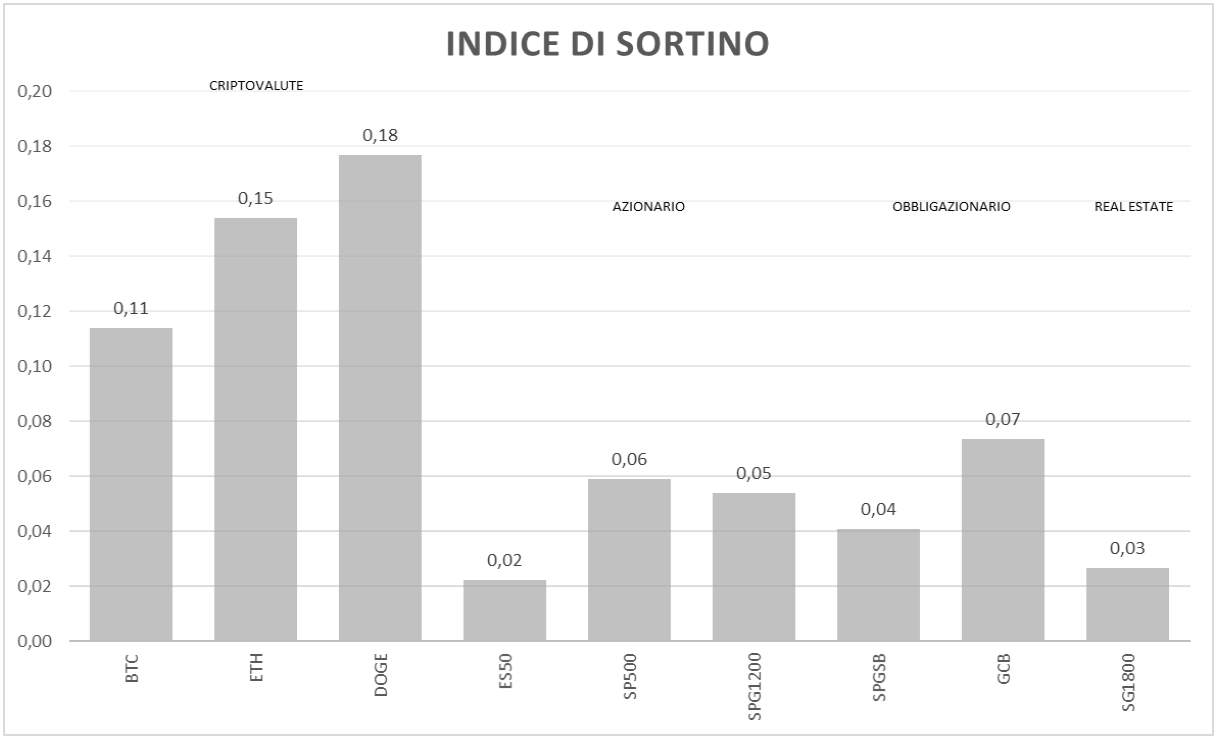


Figura 71 - Indice di Sortino

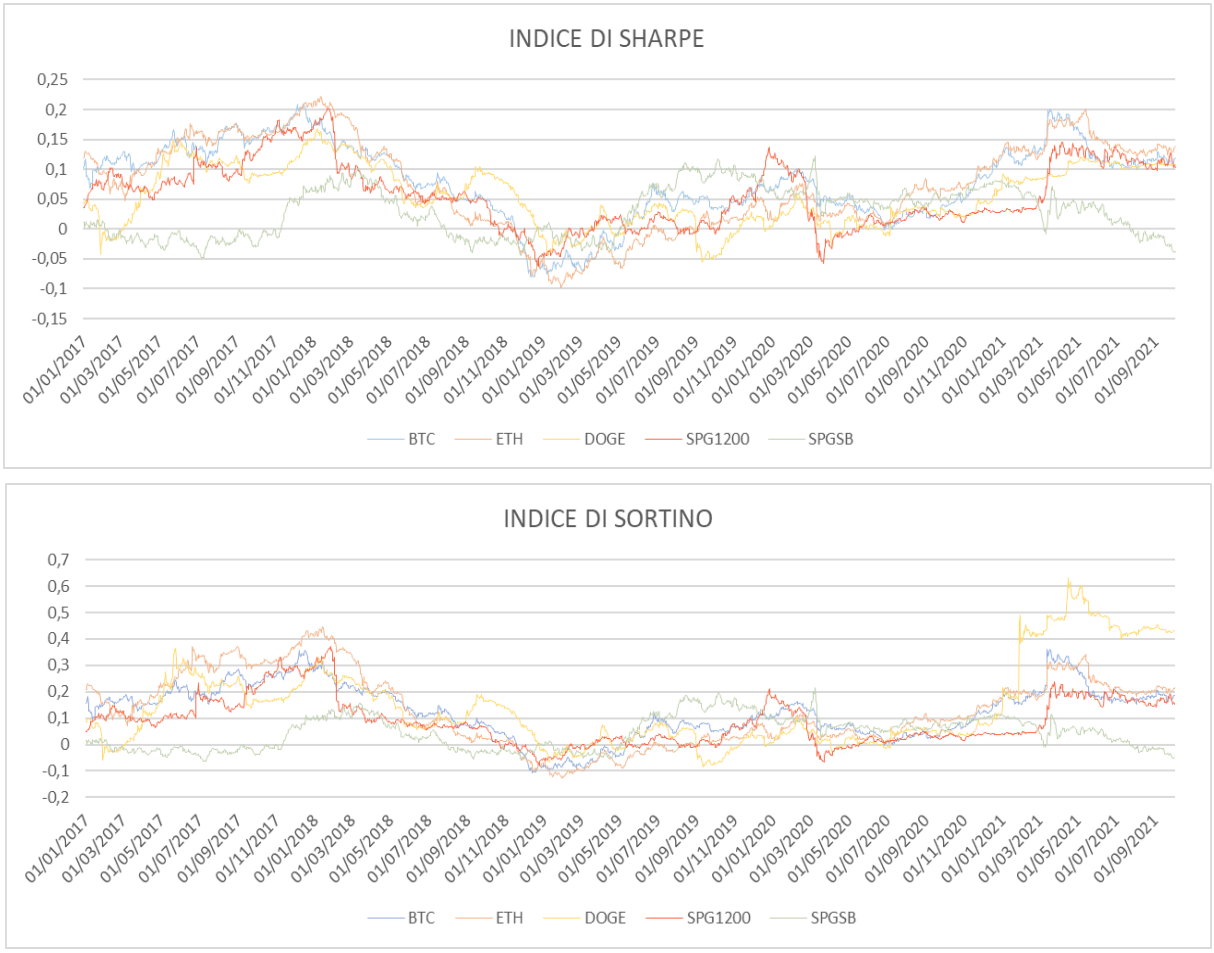


Figura 72 - Indice di Sharpe e Sortino dinamici

Per concludere, nella *figura 72* sono riportati gli indici di Sharpe e Sortino dinamici giornalieri, calcolati su orizzonte annuale. Questi consentono di ottenere informazioni aggiuntive rispetto agli omonimi indicatori statici. Infatti, consente di vedere come i valori sono cambiati nel corso del tempo, mostrando quale asset ha performato meglio rispetto al rischio, nei diversi periodi di tempo. Si vede come non sempre i rapporti migliori sono stati quelli associati alle criptovalute, soprattutto nel periodo 2019 – 2020, il quale coincide con una fase di stallo delle cripto, in seguito al crollo del 2018. Tuttavia, considerando interamente i 4 anni, il rendimento corretto per il rischio del mercato cripto è stato superiore a quello dei mercati tradizionali. Infine, si vede come il valore dell'indice di Sortino associato a DOGE sia aumentato incredibilmente nell'aprile 2020, assumendo un valore doppio rispetto agli altri. Guardando alla *figura 73*[66] si vede come proprio nella settimana del 12 aprile 2020, il prezzo di DOGE ha registrato un fortissimo

[66] Fonte: https://it.tradingview.com/chart/.

incremento, che ha causato una forte alterazione degli indicatori statistici ad esso relativi.

Questa è un ulteriore prova dell'imprevedibilità che un mercato emergente come questo può riservare. Infatti, è facilmente manipolabile da colore che detengono grandi quantità di criptovalute e questo fa sì che i prezzi possano subire variazioni enormi anche i pochissimi minuti, causando talvolta grandi perdite agli investitori.

Figura 73 - Prezzo settimanale DOGE

3.4 Analisi del rischio relativo

L'obiettivo di questa parte è capire se c'è possibilità, diversificando gli asset, di creare un portafoglio efficiente che contenga sia le criptovalute che gli altri asset, quindi un portafoglio che consenta di massimizzare l'indice di Sharpe. In altre parole, l'obiettivo è trovare quella combinazione di asset che consenta di ridurre al minimo il rischio e massimizzare il rendimento. A questo proposito è fondamentale ricordare che il rischio finanziario può essere diviso in due categorie: il **rischio specifico** e il **rischio sistemico**. Il primo è quello che si cercherà di ridurre in questo paragrafo tramite diversificazione, il secondo invece non può essere ridotto in questo modo, in quanto rappresenta l'esposizione del titolo a fattori macroeconomici che influenzano la performance del portafoglio a prescindere dal numero di assets inseriti. Il rischio specifico può

essere stimato attraverso i vari indicatori visti precedentemente, in particolare nella creazione del portafoglio si utilizzerà la deviazione standard. Il rischio sistematico è invece espresso dal coefficiente Beta del modello CAPM. Nella *figura 74* sono riportati i valori Alpha, Beta ed R^2 dei singoli asset, utilizzando come indice di mercato l'SP500 nel periodo 01/01/2016 – 03/10/2021 e come rendimenti quelli giornalieri.

Asset	α	β	R^2
BTC	0,28%	0,66	2,55%
ETH	0,53%	0,90	2,15%
XRP	0,484%	0,84	1,01%
DOGE	0,68%	0,91	0,64%
ES50	-0,01%	0,64	37,95%
SP500	0,00%	1,00	100%
SPG1200	0,00%	0,80	90,94%
SP500B	0,015%	-0,02	0,45%
SPGSB	0,01%	-0,04	2,32%
GCB	0,01%	0,02	0,39%
SG1800	-0,01%	0,62	51,74%
SPCRE	-0,014%	0,89	58,55%

Figura 74 - Coefficienti Alpha, Beta e R^2

Il coefficiente α indica la capacità dell'asset di produrre rendimenti in eccesso rispetto al mercato, in altre parole il suo valore è ottenuto come differenza tra il rendimento giornaliero prodotto dall'asset e quello di equilibrio secondo il CAPM. Per questo motivo, maggiore è il suo valore, meglio è. Il coefficiente Beta, invece, misura il rischio sistematico, in particolare da una misura della sensibilità dell'asset alle oscillazioni di mercato.

Per la valutazione del rischio specifico è necessario osservare le deviazioni standard, ma soprattutto la tabella di correlazione tra i vari asset, con l'obiettivo di valutare eventuali opportunità di diversificazione.

Nella *figura 75* sono indicati la media, la deviazione standard e i coefficienti di correlazione annualizzate per ciascun asset. Questi ultimi si ottengono dal confronto tra il comportamento dei rendimenti di due asset e assumono valori compresi tra -1 e +1: più ci si avvicina al limite negativo, più l'andamento del rendimento degli assets si muove in direzioni opposte, viceversa, più ci si avvicina al limite positivo, più la direzionalità dei rendimenti è la stessa. Il valore 0 sta ad indicare un movimento dei rendimenti di ciascun titolo che risulta indipendente da quelli dell'altro.

ASSET	BTC	ETH	XRP	DOGE	ES50	SP500	SPG1200	SP500B	SPGSB	GCB	SG1800	SPCRE	μ mensile	σ mensile
BTC	1,00												9,14%	21,86%
ETH	0,56	1,00											16,96%	32,57%
XRP	0,36	0,35	1,00										15,56%	44,56%
DOGE	0,34	0,27	0,26	1,00									21,43%	60,12%
ES50	0,12	0,09	0,08	0,05	1,00								0,50%	5,49%
SP500	0,16	0,15	0,10	0,08	0,62	1,00							1,24%	5,30%
SPG1200	0,16	0,14	0,10	0,07	0,76	0,95	1,00						0,97%	4,43%
SP500B	0,02	0,03	0,02	0,01	-0,01	-0,07	-0,01	1,00					0,43%	1,35%
SPGSB	0,06	0,06	0,03	0,02	-0,20	-0,15	-0,10	0,53	1,00				0,24%	1,53%
GCB	0,05	0,05	0,04	0,02	0,06	0,06	0,16	0,80	0,76	1,00			0,41%	1,36%
SG1800	0,10	0,08	0,07	0,04	0,57	0,72	0,78	0,22	0,13	0,36	1,00		0,51%	4,55%
SPCRE	0,11	0,09	0,07	0,05	0,48	0,77	0,74	0,13	0,01	0,22	0,91	1,00	0,70%	6,19%

Figura 75 - Correlazione, media e dev. std. vari assets

La correlazione fra criptovalute stesse appare positiva e inferiore a uno, il che significa che creando un portafoglio di sole criptovalute, si otterrebbe una riduzione del rischio tramite la diversificazione. Per quanto riguarda i valori tra criptovalute e indici azionari, questi risultano positivi ma molto vicini allo zero. Questo suggerisce un comportamento dei rendimenti delle valute digitali che tende a muoversi in una direzione indipendente da quello dell'azionario. Ancora una volta un portafoglio cripto – azionario consentirebbe di raggiungere un buon grado di diversificazione. Infine, la correlazione tra criptovalute, obbligazionario e real estate assume caratteristiche molto simile a quelle già citate per l'azionario. I valori della deviazione standard esprimono l'elevata rischiosità che un portafoglio di sole criptovalute potrebbe avere, dall'altra parte, un portafoglio che le contenga consente anche dei rendimenti impensabili usando altri strumenti. Per questo motivo, nel paragrafo successivo sono presentati la ricerca del portafoglio ottimale usando il modello di Markowitz e un confronto tra portafogli con diverse composizioni.

3.5 Esempi di portafogli diversificati

Nella figura 76 è riportata una rappresentazione della frontiera efficiente. Questa è stata ottenuta con l'ausilio del risolutore di Excel, massimizzando l'indice di Sharpe, sotto il vincolo di impiego del 100% del capitale. Inoltre, all'interno del grafico è riportato il posizionamento, a livello di rischio – rendimento, dei singoli asset componenti il portafoglio. Questo consente di avere una visualizzazione grafica dei vantaggi che la creazione di un portafoglio differenziato può fornire. In particolare, si nota come un portafoglio costituito solamente da DOGE, possa garantire il maggior rendimento, tuttavia porta con sé anche un alto livello di rischio. Al grafico è stata aggiunta una nuova criptovaluta, Ripple, che consente di visualizzare bene i vantaggi della diversificazione. Infatti, a parità di rischio, è possibile ottenere un rendimento più elevato rispetto a quello che XRP potrebbe fornire. La stessa situazione vale per bitcoin e per quasi tutti gli altri assets. Quello che più si avvicina alla frontiera efficiente è ETH, questo dimostra la bontà di questo asset al suo livello di rischio. Infine, è stato collocato sul grafico è stato collocato un portafoglio costituito solo da criptovalute, il quale si colloca quasi sulla frontiera efficiente e consente di ottenere un rendimento molto elevato.

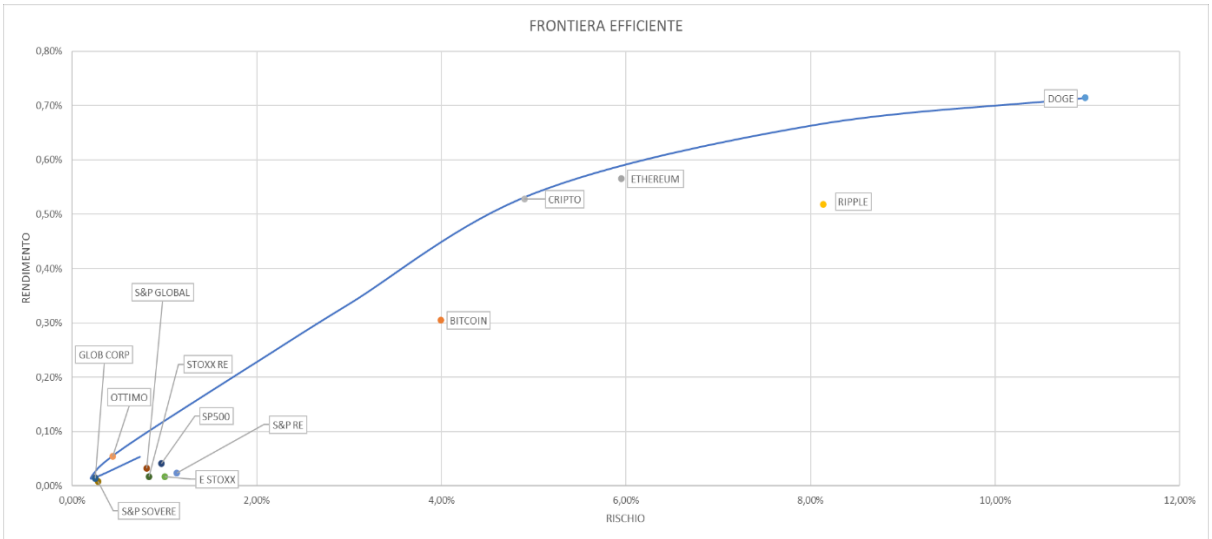


Figura 76 - Frontiera efficiente

Nella *figura 77* è riportato un confronto quantitativo tra 5 esempi di portafoglio scelti. Il primo è un portafoglio ugualmente suddiviso: 25% criptovalute, 25% azionario, 25% obbligazionario e 25% real estate. Inoltre, all'interno di ciascuna classe il peso di ogni asset è il medesimo. Il secondo è il portafoglio ottimale di Markowitz, ovvero quel portafoglio che massimizza l'indice di Sharpe, ottenuto tramite il risolutore di Excel. Il terzo

e il quarto sono costituiti rispettivamente da BTC e SP500 e consentono di visualizzare quanto la diversificazione può aiutare ad aumentare l'indice di Sharpe. L'ultimo è un portafoglio costituito da sole criptovalute, ottenuto massimizzando l'indice di Sharpe, sotto il vincolo di utilizzare solo questa tipologia di asset.
I valori di media, deviazione standard, indice di Sharpe e beta, sono espressi rendendo mensili i valori giornalieri. In particolare, al fine di non sovrastimare l'indice di Sharpe, la media è stata resa mensile usando la formula del rendimento semplice, ovvero moltiplicando per 30 il valore giornaliero. La deviazione standard invece è ottenuta moltiplicando per la radice quadrata di 30 il valore giornaliero.

ASSET	BILANCIATO	OTTIMO	BTC	SP500	CRIPTO
BTC	6,25%	1,23%	100,00%	0,00%	20,14%
ETH	6,25%	3,81%	0,00%	0,00%	51,38%
XRP	6,25%	1,02%	0,00%	0,00%	14,10%
DOGE	6,25%	1,12%	0,00%	0,00%	14,38%
ES50	8,25%	0,00%	0,00%	0,00%	0,00%
SP500	8,25%	10,20%	0,00%	100,00%	0,00%
SPG1200	8,25%	0,00%	0,00%	0,00%	0,00%
SP500CB	8,25%	75,52%	0,00%	0,00%	0,00%
SPGSB	8,25%	0,00%	0,00%	0,00%	0,00%
GCB	8,25%	7,10%	0,00%	0,00%	0,00%
SG1800	12,50%	0,00%	0,00%	0,00%	0,00%
SPC1500	12,50%	0,00%	0,00%	0,00%	0,00%
MEDIA	4,41%	1,64%	9,14%	1,24%	15,83%
DEV. STD.	7,79%	2,41%	21,86%	5,30%	26,84%
SHARPE	0,57	0,68	0,42	0,23	0,59
BETA	0,59	0,15	0,66	1,00	0,85
RENDIMENTO	33327%	15699%	10998%	116%	210561%

Figura 77 - Confronto portafogli

- **Portafoglio bilanciato**: questa composizione del portafoglio consente un rendimento medio del 4,41% mensile ed espone ad un rischio quantificabile nel 7,79%. In altre parole, un portafoglio di questo tipo, potrebbe fornire un rendimento annuo composto del 68% ed una deviazione standard attorno al 27%.

- **Portafoglio ottimale**: questo offre un rendimento medio del 1,64%, mentre ha una deviazione standard del 2,41%. Annualizzando i dati usando, ancora una volta il rendimento composto, si avrebbero $\mu = 22\%$ e $\sigma = 8\%$. Questo portafoglio rappresenta quindi un'opzione di investimento per coloro che non sono molto propensi al rischio, ma che ricercano comunque un buon rendimento.

- **Portafoglio BTC e SP500**: l'indice di Sharpe di questi due portafogli, mostra come ha poco senso un investimento in essi. Infatti, offrono un rendimento per unità di rischio che è il minore fra tutti. In particolare, soffermandosi sul portafoglio 100% BTC, si vede come il portafoglio cripto, sia in grado di offrire un maggior rendimento ed un livello di rischio poco superiore grazie alla diversificazione.

- **Portafoglio cripto**: questo portafoglio contiene solo criptovalute. Il peso attribuito ad ognuna è stato calcolato tramite il risolutore di Excel, cercando la massimizzazione dell'indice di Sharpe e con il vincolo di sole criptovalute inserite in portafoglio. I valori che si ottengono tramite l'annualizzazione composta sono i seguenti: $\mu = 483\%$ e $\sigma = 93\%$. Il rendimento offerto è notevole, dall'altra parte il rischio da correre è altrettanto elevato, soprattutto considerando che tramite l'annualizzazione della deviazione standard il suo valore viene tipicamente sottostimato. In conclusione, un portafoglio di questo tipo è consigliato a coloro che hanno un elevato livello di propensione al rischio.

Nell'ultima riga, ovvero la riga "rendimento" è riportato il rendimento reale che il portafoglio avrebbe registrato, qualora questo fosse stato creato il primo giorno del 2016 e mantenuto tale fino al 3 ottobre del 2021. Si vede come il portafoglio ottimale ha registrato un rendimento molto superiore a quelli di BTC e SP500, inoltre è riuscito a produrre un rendimento che ha accorciato la distanza con il portafoglio bilanciato, esponendo l'investitore ad un livello di rischio molto più basso.

CONCLUSIONE

Dall'elaborato emerge che la blockchain rappresenta una tecnologia rivoluzionaria, nel senso che rompe completamente l'elemento su cui l'attuale sistema economico – finanziario si basa, la fiducia. Ad alto livello il suo funzionamento è piuttosto semplice, la blockchain permette di salvare delle informazioni suddividendole in blocchi e sottoponendole ad una procedura di verifica da parte dei nodi. Se quest'ultima viene superata, il blocco viene aggiunto alla catena, la quale è immutabile ed una sua copia è depositata presso ogni nodo della rete, conferendole la proprietà di decentralizzazione. A livello tecnico, queste caratteristiche sono rese possibili da un algoritmo di consenso, che sceglie colui che ha il diritto di aggiungere un blocco e dall'implementazione di varie tecniche della crittografia. I principali metodi utilizzati sono le funzioni di hash e i sistemi crittografici a doppia chiave. Le prime consentono di garantire l'immutabilità della catena, legando indissolubilmente tra loro gli elementi fondamentali, i blocchi. I secondi, invece, garantiscono la sicurezza delle transazioni, consentendo solo al proprietario di movimentare i propri pacchetti di informazioni. La blockchain offre quindi, al netto dei suoi limiti, una soluzione trasparente, decentralizzata e crittograficamente sicura per il salvataggio, la condivisione e il trasferimento delle informazioni.

Per quanto riguarda le criptovalute, emerge come queste non siano altro che dei "file", che risiedono sulla blockchain e che si promettono di svolgere le funzioni di una valuta, usufruendo però dei vantaggi offerti dalla tecnologia su cui si basano. In particolare, queste non richiedono la presenza di un ente terzo che le custodisca, che ne verifichi l'autenticità o che ne abiliti il trasferimento, in quanto tutte queste funzioni sono garantite dalla blockchain e dal protocollo di ciascuna criptovaluta.

Blockchain e criptovalute sono quindi cose distinte, che non devono essere confuse. La prima è una tecnologia, le seconde sono uno dei modi di utilizzarla. Sempre nell'elaborato sono infatti esposte altre modalità di utilizzo della blockchain, alcune che consentirebbero un netto miglioramento dell'efficienza in ambito logistico, assicurativo e nel settore della beneficienza, altri sono invece relativi all'ambito finanziario. Proprio in quest'ultimo rientra la Decentralized Finance, che propone un modo tutto nuovo di interpretare la finanza, completamente disintermediato, che consente l'annullamento delle commissioni di intermediazione e la loro distribuzione ai soggetti che interagiscono con tali sistemi. Questa nuova interpretazione della finanza presenta numerosi rischi, come il crollo del valore degli asset digitali o errori (più o meno volontari) nella

scrittura degli smart contracts. Proprio per questo, riguardo l'aspetto della finanza in generale e degli investimenti è emersa la necessità di un buon livello di conoscenza sia a livello pratico che a livello di gestione del rischio. Le criptovalute, infatti, richiedono una grande attenzione nella loro movimentazione, al fine di non sbagliare blockchain e indirizzo di invio e ricezione. Inoltre, la loro grande volatilità richiede un'attenta strategia nella gestione del rischio: un portafoglio con un eccesso di criptovalute potrebbe causare grandi perdite in un lasso di tempo anche molto breve. In conclusione, si è visto come, tramite l'aggiunta di una piccola percentuale di criptoassets in portafoglio, sia possibile raggiungere un valore dell'indice di Sharpe superiore, mostrando come le criptovalute rappresentino uno strumento di diversificazione rispetto ad azionario e obbligazionario.

La blockchain e le criptovalute hanno quindi le potenzialità per eliminare la necessità di fiducia e migliorare a livello di efficienza moltissimi processi logistici, finanziari e decisionali, tuttavia gli scogli da superare sono ancora molti. Uno di questi è sicuramente la necessità di una preparazione, già a partire dal livello scolastico, riguardo ai rischi che si corrono e al riconoscimento di eventuali truffe, che nel mondo cripto sono all'ordine del giorno. L'ostacolo più grande è però rappresentato dalla mancanza di una regolamentazione apposita per le criptovalute. Infatti, l'assenza di normative chiare non permette di stabilire le responsabilità e soprattutto nell'ambito della finanza decentralizzata, l'investitore non può tutelarsi in alcun modo. L'incremento nell'adozione delle criptovalute nel 2021 sembra aver finalmente convinto i regulators a impegnarsi nella creazione di apposite leggi e si prevede che nei prossimi anni queste saranno pronte. Quando questi scogli saranno superati, la blockchain riuscirà ad espandersi nel mondo reale e a rendere efficienti i macchinosi processi che oggi lo caratterizzano?

BIBLIOGRAFIA

Comandini G., *Da Zero alla Luna. La Blockchain: quando, come, perché sta cambiando il mondo*, Palermo, Dario Flaccovio Editore S.r.l., Marzo 2020, https://www.lafeltrinelli.it/da-zero-alla-luna-quando-libro-gian-luca-comandini/e/9788857910307, consultato il 28 Novembre 2021.

Finanza Viva, *Conoscere ed Investire in criptovalute. Scopri la finanza decentralizzata, gli NFT e la blockchain con l'unico manuale che ti insegna ad investire efficacemente in criptovalute*, s.l., Finanza Viva – My Publishing Empire ltd, Novembre 2021, consultato il 10 Gennaio 2022.

SITOGRAFIA

Nakamoto S., *Bitcoin: A Peer – to – Peer Electronic Cash System,* 31 Ottobre 2008, https://bitcoin.org/bitcoin.pdf, consultato il 06/12/2021.

Difference between blockchain and bitcoin, Binance Academy, aggiornato al 29 Aprile 2021, https://academy.binance.com/it/articles/difference-between-blockchain-and-bitcoin, consultato il 08/12/2021.

History of blockchain, Binance Academy, aggiornato al 24 Agosto 2021, https://academy.binance.com/it/articles/history-of-blockchain, consultato il 08/12/2021.

Capaccioli G. e Marciano D., *DLT & blockchain: tipologie e limiti,* in "Applicazioni reali, Educational", Affidaty, 16 Ottobre 2019, https://affidaty.io/blog/it/2019/10/dlt-blockchain-tipologie-e-limiti/, consultato il 07/12/2021.

Valsecchi V., *La classificazione delle blockchain: autorizzate e private*, in "Industry 4.0 & IoT", Spindox, 20 Giugno 2018, https://www.spindox.it/it/blog/la-classificazione-delle-blockchain/#gref, consultato il 07/12/2021.

Cavicchioli M., *In cosa consistono i blocchi della blockchain*, in “Blockchain”, The Cryptonomist, 15 Giugno 2020, https://cryptonomist.ch/2020/06/15/in-cosa-consistono-blocchi-blockchain/, consultato il 28/11/2021.

Bellini M., *Blockchain: cos’è, come funziona e gli ambiti applicativi in Italia*, in “Esperti e analisti”, Blockchain4innovation, 7 Febbraio 2021, https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/, consultato il 28/11/2021.

Blockchain; cos’è il nonce e perché è così importante, Knobs, https://knobs.it/blockchain-cose-il-nonce-e-perche-e-cosi-importante/, consultato il 28/11/2021.

Petrozzi D., *Funzioni hash: a cosa servono e perché dovresti conoscerle,* Eternal Curiosity, 12 Agosto 2014, https://eternalcuriosity.it/funzioni-hash-a-cosa-servono-e-perche-dovresti-conoscerle, consultato il 29/11/2021.

What is a blockchain consensus algorithm, Binance Academy, aggiornato al 18 Agosto 2021, https://academy.binance.com/it/articles/what-is-a-blockchain-consensus-algorithm, consultato il 29/11/2021.

Cannata C., *Sistemi decentralizzati vs sistemi centralizzati: vantaggi e applicazioni,* Wizkey, 16 Luglio 2019, https://www.wizkey.io/it/blog/sistemi-decentralizzati-vs-sistemi-centralizzati-vantaggi-e-applicazioni-2/, consultato il 29/11/2021.

Proof of work explained, Binance Academy, aggiornato al 24 Agosto 2021, https://academy.binance.com/it/articles/proof-of-work-explained, consultato il 29/11/2021.

https://www.blockchain.com/btc/block/000000000000000000090ec83aef111e64d18de540effb87c5209160b4ea4501, consultato il 29/11/2021.

Cos’è SHA-256, Bit2me Academy, https://academy.bit2me.com/it/algoritmo-bitcoin-sha256/, consultato il 29/11/2021.

Aaron, *Proof of stake*, in “Binance Academy”, https://academy.binance.com/en/glossary/proof-of-stake, consultato il 29/11/2021.

Cavalli S., *Proof of Work (PoW) vs Proof of Stake (PoS): la guida*, in “wiki”, The Cryptonomist, 5 Ottobre 2019, https://cryptonomist.ch/2019/10/05/proof-of-work-pow-vs-proof-of-stake-pos-la-guida/, consultato il 29/11/2021.

Rubino A., *Proof of Work: cos’è e la differenza con il proof of stake*, in “Criptovalute”, Blockchain4innovation, 5 Marzo 2020, https://www.blockchain4innovation.it/criptovalute/blockchain-cosa-sono-i-protocolli-pow-e-pos-e-a-cosa-servono/, consultato il 29/11/2021.

La Proof of Stake favorisce la centralizzazione e i ricchi, Cryptonews, aggiornato al 6 Giugno 2021, https://it.cryptonews.com/exclusives/fiat-like-proof-of-stake-chains-favor-centralization-rich-p-10579-it.htm#:~:text=L'acquisto%20di%20ETH%20non,con%20la%20Proof%20of%20Stake, consultato il 29/11/2021.

Chiave pubblica e chiave privata: cosa sono e a cosa servono su blockchain, Knobs, https://knobs.it/chiave-pubblica-chiave-privata/, consultato il 01/12/2021.

Firma di una transazione in bitcoin, 10bitcoin, http://www.10bitcoin.it/firma-transazione-bitcoin/, consultato il 01/12/2021.

Cos’è un nodo, Bit2me Academy, https://academy.bit2me.com/it/cos%27%C3%A8-un-nodo/, consultato il 02/12/2021.

What are nodes, Binance Academy, aggiornato al 20 Ottobre 2020, https://academy.binance.com/it/articles/what-are-nodes, consultato il 02/12/2021.

Come funzionano le hard fork e le soft fork, Bitpanda Academy, https://www.bitpanda.com/academy/it/lezioni/come-funzionano-le-hard-fork-e-le-soft-fork/, consultato il 10/12/2021.

Hard forks and soft forks, Binance Academy, aggiornato al 24 Agosto 2021, https://academy.binance.com/it/articles/hard-forks-and-soft-forks, consultato il 10/12/2021.

Pagliari E., *Registrato un blocco orfano sulla blockchain bitcoin (BTC),* in “Bitcoin”, The Cryptonomist, 28 Maggio 2019, https://cryptonomist.ch/2019/05/28/blocco-orfano-blockchain-di-bitcoin-btc/, consultato il 30/11/2021.

Cos’è il blocco orfano, Bit2me Academy, https://academy.bit2me.com/it/cos%27%C3%A8-un-blocco-orfano/, consultato il 03/12/2021.

Bai A., *Blockchain: come avviene un attacco al 51% in diretta*, in “Web”, Hardware Upgrade, 18 Maggio 2021, https://www.hwupgrade.it/news/web/blockchain-come-avviene-un-attacco-al-51-in-diretta-ve-lo-mostra-il-video-di-un-ricercatore_97813.html, consultato il 30/11/2021.

Valeri M., *Attacchi alla blockchain: cause, conseguenze e contromisure,* in “Malware e attacchi hacker, Cybersecurity360, 1 Marzo 2019, https://www.cybersecurity360.it/nuove-minacce/attacchi-alla-blockchain-cause-conseguenze-e-contromisure/, consultato il 30/11/2021.

Blockchain use cases, Binance Academy, aggiornato al 21 Ottobre 2020, https://academy.binance.com/it/articles/blockchain-use-cases, consultato il 01/12/2021.

Blockchain nella supply chain: casi di applicazione, The Procurement Magazine, 12 Febbraio 2020, https://www.theprocurement.it/innovazione/blockchain-supply-chain-casi-applicazione/, consultato il 04/12/2021.

Spagnolo E., *Blockchain, non solo Bitcoin: casi d’uso di una tecnologia “necessaria”,* in “Blockchain”, The Cryptonomist, 28 Agosto 2021, https://cryptonomist.ch/2021/08/28/blockchain-casi-duso-tecnologia/, consultato il 04/12/2021.

Dall'Ava M., *Come la blockchain sta cambiando il modo in cui il mondo vive e funziona,* in "Economia", Wired, https://www.wired.it/economia/business/2021/04/21/blockchain-cambiando-modo-vivere/, consultato il 02/12/2021.

What is cryptocurrency, Binance Academy, aggiornato al 12 Gennaio 2022, https://academy.binance.com/it/articles/what-is-cryptocurrency/, consultato il 12/01/2021.

Redazione, Soldi depositati in banca: non sono più i tuoi, a dirlo la legge, Notizieora, aggiornato al 24/01/2021, https://www.notizieora.it/affari/soldi-depositati-in-banca-non-sono-piu-i-tuoi-a-dirlo-la-legge/#:~:text=I%20soldi%20depositati%20in%20banca,propriet%C3%A0%20%C3%A8%20detenuta%20dalla%20banca.&text=Quando%20si%20deposita no%20i%20soldi,se%20ne%20perde%20la%20propriet%C3%A0, consultato il 02/12/2021.

Double spending explained, Binance Academy, aggiornato al 2 Dicembre 2021, https://academy.binance.com/it/articles/double-spending-explained, consultato il 03/12/2021.

What is Lightning network, Binance Academy, aggiornato al 24 Agosto 2021, https://academy.binance.com/it/articles/what-is-lightning-network, consultato il 11/12/2021.

@Wackerow*, Macchina Virtuale Ethereum (EVM)*, Ethereum.org, 22 Dicembre 2021, https://ethereum.org/it/developers/docs/evm/, consultato il 10/12/2021.

What is Ethereum, Binance Academy, aggiornato al 18 Novembre 2021, https://academy.binance.com/it/articles/what-is-ethereum, consultato il 10/12/2021.

Che cosa è Ethereum, Bitpanda Academy, https://www.bitpanda.com/academy/it/lezioni/che-cos-e-l-ethereum/, consultato il 10/12/2021.

Token vs criptovalute: differenze e potenzialità, Namirial, aggiornato al 16 Giugno 2021, https://focus.namirial.it/differenze-vantaggi-token-criptovalute/, consultato il 10/12/2021.

Redazione osservatori digital innovation, *Come funzionano i token blockchain e come si costruiscono,* in “Blockchain & Distributed Ledger”, Osservatori.net, 5 Febbraio 2020, https://blog.osservatori.net/it_it/token-blockchain-come-funzionano, consultato il 11/12/2021.

@Wackerow*, Introduzione agli smart contract,* Ethereum.org, 22 Dicembre 2021, https://ethereum.org/it/developers/docs/smart-contracts/, consultato il 10/12/2021.

What is a smart contract, Binance Academy, aggiornato al 18 Novembre 2021, https://academy.binance.com/it/articles/what-is-ethereum#what-is-a-smart-contract, consultato il 10/12/2021.

Bellini M., *Smart contracts: che cosa sono, come funzionano e quali sono gli ambiti applicativi,* in “Smart Contract”, Blockchain4innovation, 28 Dicembre 2018, https://www.blockchain4innovation.it/mercati/legal/smart-contract/blockchain-smart-contracts-cosa-funzionano-quali-gli-ambiti-applicativi/, consultato il.

Reghelin A., *Smart contract e blockchain: funzionamento, esempi e normativa,* in “Blockchain & Distributed Ledger”, Osservatori.net, 9 Luglio 2019, https://blog.osservatori.net/it_it/smart-contract-in-blockchain, consultato il 10/12/2021.

HR D., *Blockchain e smart contract: benefici e limiti,* Decahr, 22 Ottobre 2020, http://www.decahr.it/blockchain-e-smart-contract-benefici-e-limiti/, consultato il 10/12/2021.

Cavicchioli M., *Ethereum: forte calo del gas,* in “Ethereum”, The Cryptonomist, 8 Novembre 2021, https://cryptonomist.ch/2021/11/08/ethereum-forte-calo-gas/#:~:text=Essendo%20ancora%20una%20blockchain%20basata,per%20assicurarsi%20una%20convalida%20breve, consultato il 10/12/2021.

Bellacicca A., Ditroia M., *Blockchain layer 2: cos'è e come funziona la soluzione per incrementare velocità e scalabilità,* in "Industria 4.0", Blockchain4innovation, 4 Ottobre 2021, https://www.blockchain4innovation.it/mercati/industria4-0/blockchain-layer-2-cose-e-come-funziona-la-soluzione-per-incrementare-velocita-e-scalabilita/, consultato il 10/12/2021.

Carboni D., *DeFi, l'importanza del "second layer" per la democratizzazione,* in "Banche e Finanza", Blockchain4innovation, 23 Agosto 2021, https://www.blockchain4innovation.it/mercati/banche-e-finanza/defi-limportanza-del-second-layer-per-la-democratizzazione/, consultato il 11/12/2021.

Merkle trees and merkle roots explained, Binance Academy, aggiornato al 29 Aprile 2021, https://academy.binance.com/it/articles/merkle-trees-and-merkle-roots-explained, consultato il 11/12/2021.

Cricrì F., *Ethereum Soluzioni Layer 2,* Medium, 5 Giugno 2021, https://fabiocricri.medium.com/ethereum-soluzioni-layer-2-c85065234b84, consultato il 11/12/2021.

Cos'è il Trilemma Blockchain, tecno Babele https://www.tecnobabele.com/cose-il-trilemma-blockchain/2021-09-12/, consultato il 12/12/2021.

@Metapunks.world, *Why Algorand,* Medium, 3 Novembre 2021, https://medium.com/@metapunks.world/why-algorand-e7211775cf9d, consultato il 04/01/2022.

Montemagno M., Crypto e Dintorni – 4 chiacchere con Silvio Micali (Algorand), YouTube, 17 Giugno 2021, https://www.youtube.com/watch?v=Ia-wVqiZZFM, consultato il 13/12/2021.

Technology, Algorand, https://www.algorand.com/technology/algorand-protocol, consultato il 13/12/2021.

Long Term Algo Dynamics, Algorand, https://algorand.foundation/governance/algo-dynamics, consultato il 13/12/2021.

Fulco D., *Blockchain: come funziona il sistema adottato dalla SIAE per il diritto d'autore, in "*Legal", Blockchain4innovation, 14 Giugno 2021, https://www.blockchain4innovation.it/legal-2/blockchain-come-funziona-il-sistema-adottato-dalla-siae-per-il-diritto-dautore/, consultato il 10/12/2021.

Bellomunno C. e Camilotti L., *Un'idea per usare la Blockchain nella tutela del diritto d'autore,* in "Economia", Wired, 4 Novembre 2020, https://www.wired.it/economia/business/2020/11/04/blockchain-diritto-autore/, consultato il 13/13/2021.

Siae rappresenta i diritti degli autori con asset digitali: creati più di 4000000 di NFT sull'infrastruttura Blockchain di Algorand, Siae, 24 Marzo, 2021, https://www.siae.it/it/iniziative-e-news/siae-rappresenta-i-diritti-degli-autori-con-asset-digitali-creati-pi%C3%B9-di-4000000, consultato il 13/13/2021.

IMG Solution SRL, *Mercato criptovalutario: le truffe degli ultimi 10 anni analizzate da criptovalute24,* in "Economia", Ansa, 14 Giugno 2021, https://www.ansa.it/pressrelease/economia/2021/06/14/mercato-criptovalutario-le-truffe-degli-ultimi-10-anni-analizzate-da-criptovalute24_0b4f8d16-3009-4e42-816e-18ee31fce689.html, consultato il 10/12/2021.

Criptovalute: boom truffe in rete, il vademecum per evitarle e navigare in sicurezza, Adnkronos, 16 Settembre 2021, https://www.adnkronos.com/criptovalute-boom-truffe-in-rete-il-vademecum-per-evitarle-e-navigare-in-sicurezza_1elWRyoqlgYS5vOB-DgrbpR, consultato il 13/12/2021.

Schema Ponzi, Wikipedia, https://it.wikipedia.org/wiki/Schema_Ponzi, consultato il 13/12/2021.

Bel N., *I più famosi schemi piramidali del mondo crypto,* Cointelegraph, 10 Luglio 2020, https://it.cointelegraph.com/news/the-most-famous-financial-pyramids-in-the-crypto-world, consultato il 13/12/2021.

How to spot scams in decentralized finance, Binance Academy, aggiornato al 4 Gennaio 2022, https://academy.binance.com/it/articles/how-to-spot-scams-in-decentralized-finance-defi, consultato il 05/01/2022.

The Crypto Gateway – Investire in criptovalute, Che cos'è la DeFi e come funziona | corso di DeFi per principianti Ep.1, YouTube, 2 Dicembre 2021, https://www.youtube.com/watch?v=5Z69nvwd-dE, consultato il 15/12/2021.

Impermanent loss nelle liquidity pool, Etherevolution, 20 Agosto 2020, https://etherevolution.eu/impermanent-loss-nelle-liquidity-pool/, consultato il 16/12/2021.

What is the Metaverse, Binance Academy, aggiornato al 12 Gennaio 2022, https://academy.binance.com/it/articles/what-is-the-metaverse, consultato il 14 Gennaio 2022.

Meta, The Metaverse and how we'll build it together – Connect 2021, YouTube, 28 Ottobre 2021, https://www.youtube.com/watch?v=Uvufun6xer8, consultato il 17/12/2021.

Crypto wallet types explained, Binance Academy, aggiornato al 11 Novembre 2021, https://academy.binance.com/it/articles/crypto-wallet-types-explained, consultato il 20/12/2021.

Zhao C., Binance blog, *Centralization VS Decentralization*, data articolo 12/02/2019, https://www.binance.com/it/blog/all/centralizzazione-vs-decentralizzazione-301982828007075840, consultato il 02/12/2021.

“ *Ogni persona informata ha bisogno di conoscere il Bitcoin perché potrebbe essere uno degli sviluppi più importanti del mondo* “

Leon Louw

Voglio ringraziare il mio relatore, il Professor Roberto Franzoni. Mi ha seguito in questo importante momento della mia carriera universitaria con professionalità e disponibilità, sia nello svolgimento dello stage che nella stesura della tesi.

Alla mia famiglia che mi ha sempre sostenuto e supportato in questo percorso.
Ringrazio mia mamma Marica, mio papà Maurizio, mia sorella Chiara, mia nonna Nella, mio nonno Franco, mia zia Ilaria, mio zio Lorenzo, mia cugina Viola e la mia ragazza Veronica.