POLITECNICO DI TORINO

Corso di Laurea
in Matematica per l'Ingegneria

Tesi di Laurea

Blockchain e piattaforme decentralizzate user-rewarding

Relatore
prof. Danilo Bazzanella
firma del relatore

. . . . . .

Candidata
Elena Pitino
firma della candidata

. . . . . .

Committente
SEA - Soluzioni Eco Ambientali s.r.l.

Anno Accademico 2021-2022

Indice

Abstract

La blockchain è una tecnologia rivoluzionaria, uno strumento in grado di decentralizzare un gruppo di utenti e renderlo autonomo da qualsiasi forma di autorità centrale. Tra i vari campi di applicazione travolti dalla potenza di questa tecnologia, quello aziendale ha subito una delle più forti influenze. Lo scopo di questo lavoro è analizzare come la blockchain può rivoluzionare il modo di gestire un'azienda, coordinandone i meccanismi interni e incentivando i comportamenti corretti dei dipendenti. L'idea nasce dalla collaborazione con SEA, Soluzioni Eco Ambientali Srl, una società a responsabilità limitata specializzata in igiene ambientale. Ciò che la contraddistingue è la costante ricerca di mezzi e tecnologie innovative, improntate sulla sostenibilità ambientale e al rispetto delle persone. Alla base di questo rispetto c'è la volontà di voler investire nella salute dei suoi dipendenti, utilizzando la tecnologia blockchain come strumento innovativo. L'obiettivo è costruire un sistema decentralizzato, autonomo e autogestito in cui gli utenti possano sentirsi parte di una community, che condivide regole, comportamenti corretti, valori e obiettivi comuni.

Parte I

La tecnologia Blockchain

Capitolo 1

Introduzione

La tecnologia blockchain viene considerata una *Disruptive Technology*, ovvero uno strumento dirompente e distruttivo. In quanto tale, ha il potere di rivoluzionare il mondo digitale e rendere gradualmente obsolete le istituzioni preesistenti.

Nella prima parte dell'elaborato verrà esaminata nel dettaglio la struttura di una blockchain, a partire da alcuni cenni di crittografia. Lo sviluppo di questa tecnologia nasce dall'esigenza di creare un sistema di scambio digitale libero dal controllo di un'autorità centrale di garanzia. Per fare questo, la blockchain viene concepita come un dataset distribuito, ovvero un elenco infinito di transizioni anonime. I dati al suo interno vengono racchiusi in blocchi, collegati da una struttura a catena e inseriti attraverso opportuni protocolli di consenso. L'introduzione del concetto di consenso distribuito, grazie al quale avviene la validazione dei blocchi, ha condotto pian piano alla decentralizzazione di infinite applicazioni. In quest'ottica trova spazio lo scambio di qualsiasi asset digitali e la possibilità di poter decentralizzare potenzialmente ogni sistema digitale.

Tra i numerosi campi di applicazione, anche il mondo aziendale ha percepito la potenzialità di un'innovazione in questo senso. La ragione che spinge un'azienda a investire in questo strumento è la volontà di creare un'organizzazione altamente digitalizzata, in grado di gestire reparti di diversa natura e coordinare relazioni con altre imprese in mancanza di fiducia. La seconda parte dell'elaborato si focalizza su questo aspetto e, in particolare, sull'applicazione della tecnologia blockchain al contesto aziendale di SEA, una società specializzata in igiene urbana. L'intento di questa azienda è quello di creare un sistema per il walfare aziendale che controlli il livello di salute dei suoi utenti, incoraggiandoli a uno stile di vita attivo ed equilibrato. Per fare questo, verrà modellata una blockchain privata e stabiliti tutti gli strumenti necessari alla creazione di una *piattaforma decentralizzata user-rewarding*. La piattaforma verrà strutturata sulla base delle esigenze dei nodi della rete, verranno fissati degli obiettivi per i dipendenti, analizzati i dati in ingresso della blockchain e stabiliti gli standard necessari alla premiazione degli utenti più attivi.

Capitolo 2

Cenni di crittografia

2.1 Sistemi simmetrici e asimmetrici

La crittografia è uno strumento che ha origini antichissime, utilizzata per rendere indecifrabili messaggi a chiunque non fosse il destinatario. Lo scopo della crittografia è sempre stato quello di permettere la comunicazione in presenza di persone che non dovevano capire il messaggio.

I primi criptosistemi si basavano sullo scambio di una chiave segreta, che doveva avvenire nel modo più sicuro possibile. Inizialmente un criptosistema veniva costruito sulla base di un semplice algoritmo o di una permutazione. Con il tempo, sono nati dei sistemi sempre più complessi e macchinari sempre più sofisticati. L'avvento dei computer ha portato allo sviluppo su software dei moderni protocolli crittografici, con chiavi crittografiche molto lunghe e con algoritmi complessi, che prevedevano sia la sostituzione che la permutazione dei messaggi originali. Un sistema di questo tipo viene detto **simmetrico** poiché la chiave viene condivisa da una coppia di utenti e utilizzata sia per cifrare che per decifrare i messaggi scambiati. In un sistema di questo tipo gli utenti interagiscono a coppie e l'utente che riceve il messaggio è sicuro dell'identità del mittente. Tuttavia, quando il numero di utenti è consistente, il numero di chiavi che ogni utente deve condividere con gli altri cresce. La sicurezza del sistema è quindi compromessa dalla difficoltà di saper gestire così tante interazioni. Poiché ogni utente deve condividere una chiave una con tutti, il numero totale si trova dall'approssimazione:

$$\binom{n}{2} = \frac{n!}{2(n-2)!} = \frac{n(n-1)}{2} \sim \frac{n^2}{2}$$

Per questo motivo a questo sistema viene preferito quello a **asimmetrico**, o a chiave pubblica. In questi criptosistemi, ogni utente possiede due chiavi, una pubblica e una privata. La forza di questo tipo di criptosistema sta nel fatto che, se anche si è a conoscenza della chiave pubblica, è impossibile risalire alla privata, nonostante le due chiavi siano dipendenti. Ogni utente possiede una sola chiave privata con cui decifra tutti i messaggi e usa per cifrare la chiave pubblica dell'utente con cui deve interagire. In questo modo sono necessarie in tutto $2n$ chiavi in un sistema di n utenti, molte meno rispetto a quelle

richieste in un sistema simmetrico. Nonostante questo netto miglioramento, la crittografia a chiave pubblica non ha reso obsoleta quella simmetrica a causa della maggiore lunghezza delle chiavi e delle difficoltà che si possono riscontrare durante la decifratura.
Per definire al meglio un criptosistema sono necessari:

- Un alfabeto di simboli e caratteri Σ.
- Uno spazio delle chiavi, ovvero un insieme non vuoto K, che cambia in base alla tipologia di sistema scelto.
- Un insieme non vuoto P, formato da stringhe di elementi di Σ, detto dei messaggi in chiaro, o plaintext.
- Un insieme di messaggi cifrati C, o ciphertext, costruito come il precedente.
- Un insieme $E = \{E_k : k \in K\}$ di funzioni iniettive, dette di cifratura $E_k : P \to C$.
- Un insieme di funzioni $D = \{D_h : h \in K\}$, dette di decifratura $D_k : C \to P$, tali che $\forall k \in K$ esiste $h \in K$ tale che:

$$D_h(E_k(p)) = p, \forall p \in P.$$

2.1.1 RSA

Il più famoso sistema a chiave pubblica è l'RSA, pubblicato nel 1977 e rimasto il più usato per anni fino alla scoperta dei sistemi basati sulle curve ellittiche. Questo sistema crittografico è basato sull'elevata complessità computazionale della fattorizzazione in numeri primi. Un utente A:

1. Sceglie due numeri primi grandi distinti p e q.
2. Ne calcola il prodotto $N = p \cdot q$, e il valore della funzione di Eulero $\phi(N) = \phi(p) \cdot \phi(q) = (p-1)(q-1) = N - p - q + 1$.
3. Sceglie $e \in \mathbb{Z}^*_{\phi(N)}$ e calcola d tale che $e \cdot d \equiv 1 \bmod \phi(N)$.
4. Rende nota la chiave pubblica costituita dalla coppia (N, e).
5. Tiene segreta la chiave privata costituita dalla coppia $(\phi(N), d)$.

Quando altro utente vuole mandare un messaggio M deve cifrarlo attraverso una funzione unidirezionale dipendente dalla chiave pubblica di A, ottenendo:

$$C = f_A(M) = M^e mod N.$$

Poiché, per costruzione, $d \cdot e = 1 \bmod \phi(N)$, per decifrare il messaggio ad A basta utilizzare la funzione inversa basata sulla sua chiave privata d, così da ottenere il messaggio originale:

$$M = f_A^{-1}(C) = C^d mod N.$$

La decifratura funziona per il teorema di Eulero generalizzato.

Teorema 2.1.1 (di Eulero generalizzato)**.** *Sia N il prodotto di due primi distinti. Se $m \equiv 1$ mod $\phi(N)$, allora $a^m \equiv a$ mod N per ogni $a \in \mathbb{Z}$.*

In RSA l'utente A riesce a decifrare il messaggio perché:

$$f_A^{-1}(f_A(M)) = f_A^{-1}(M^e) = M^{e \cdot d} = M^{1+k\phi(N)} = M mod N.$$

Lo spazio dei messaggi in chiaro e dei messaggi cifrati è $\mathbb{Z}_N$ e lo spazio delle chiavi è il sottogruppo rispetto alla moltiplicazione degli elementi invertibili $\mathbb{Z}^*_{\phi(N)}$.

L'algoritmo si basa su un elevamento a una potenza nota (e), dentro lo spazio $\mathbb{Z}_N$, con N noto. Per decifrare bisogna essere capaci a fare l'operazione inversa, cioè calcolare efficientemente le radici e−esime dentro $\mathbb{Z}_N$, cosa non nota a meno di non conoscere $\phi(N)$. Questa è detta funzione di Eulero e rappresenta il numero di elementi della classe che hanno un inverso in modulo N. In quanto funzione moltiplicativa, $\phi(N) = \phi(p) \cdot \phi(q)$ e, poiché p e q sono due numeri primi, $\phi(p) = p - 1$ e $\phi(q) = q - 1$. Dunque, solo se nota la fattorizzazione è possibile calcolare $\phi(N) = (p-1)(q-1) = N - p - q + 1$, e la chiave segreta d.

Bisogna notare che, anche se a partire dalla conoscenza della fattorizzazione si arriva a rompere il sistema di cifratura, i due problemi non sono equivalenti. Non è noto un algoritmo che permetta di fattorizzare N a partire dalla rottura di RSA. Ciò non compromette la sicurezza dell'algoritmo, che ancora non risulta essere stato violato a partire dalla conoscenza della sola chiave pubblica (N, e).

2.1.2 Sistemi su curve ellittiche

L'introduzione della crittografia su curve ellittiche (ECC - Elliptic Curve Cryptosistems) nel 1985 ha rivoluzionato la crittografia a chiave pubblica. Sia p un numero primo, una curva ellittica viene definita come il luogo dei punti di $\mathbb{Z}_p$ che soddisfano un'equazione del tipo:

$$y^2 = x^3 + ax + b.$$

La sua rappresentazione nel continuo, in Fig. 2.1, (disegnando tutti i punti reali che verificano l'equazione) permette di capire come funziona la somma di due punti sulla curva. Poiché l'equazione è verificata in modulo p, con p ragionevolmente piccolo, la vera rappresentazione della curva è di tipo discreto, formata da uno spazio di $p + 1$ punti. Infatti, quando la retta passante per due punti non interseca la curva si introduce un punto all'infinito, che fa da elemento neutro. Dunque, a causa della loro struttura di gruppo, la somma di due punti fa parte dell'insieme di $p + 1$ punti che appartengono alla curva. Per esempio, la curva usata in Bitcoin è $y^2 = x^3 + 7$, definita in $\mathbb{Z}_{17}$, e risulta formata da 18 punti. Essa è mostrata in 2.2, insieme alla Tabella delle somme dei 18 punti delle curva.

Il motivo per cui le curve ellittiche sono così diffuse in crittografia sta nella complessità del cosiddetto Elliptic Curve Discrete Logarithm Problem (ECDLP), ovvero nel saper determinare k, dati P e $Q = kP$. I principali criptosistemi basati sull'aritmetica modulare hanno un sistema analogo che sfrutta questa difficoltà computazionale rendendo l'algoritmo nettamente più potente.

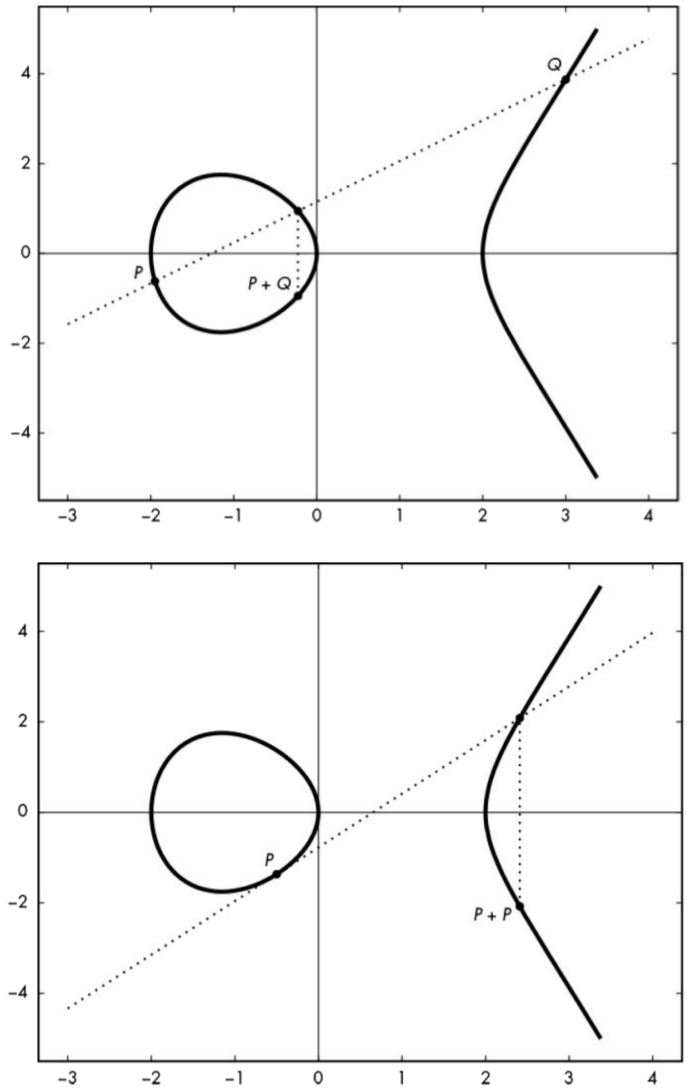
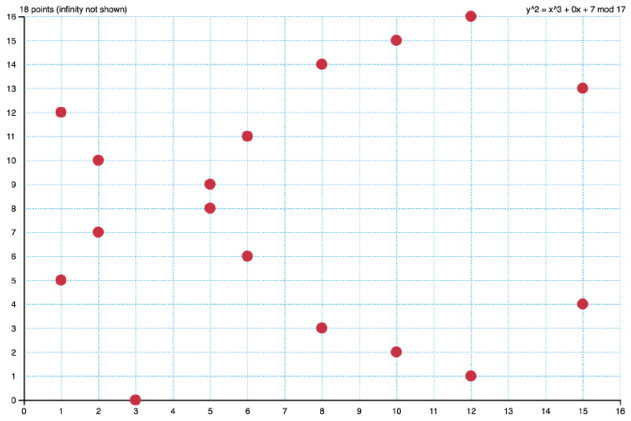


Figura 2.1. Somme di punti in curve ellittiche, Slide del corso *Blockchain e criptoeconomia*

Un **sistema simmetrico** di scambio chiavi che utilizza le curve ellittiche è, per esempio, quello di Diffie-Hellman, che, fissata una curva ellittica e un punto P sulla curva, si sviluppa in pochi passi.

- L'utente A sceglie a caso k_A e calcola $P_A = k_A P$, che invia a B;
- Analogamente, B sceglie k_B e invia $P_B = k_B P$ ad A.
- Una volta ricevute le rispettive chiavi pubbliche, A calcola $K = k_A P_B$ e B $K = k_B P_A$.



+	∞	(1,5)	(1,12)	(2,7)	(2,10)	(3,0)	(5,8)	(5,9)	(6,6)	(6,11)	(8,3)	(8,14)	(10,2)	(10,15)	(12,1)	(12,16)	(15,4)	(15,13)
∞	∞	(1,5)	(1,12)	(2,7)	(2,10)	(3,0)	(5,8)	(5,9)	(6,6)	(6,11)	(8,3)	(8,14)	(10,2)	(10,15)	(12,1)	(12,16)	(15,4)	(15,13)
(1,5)	(1,5)	(2,10)	∞	(1,12)	(5,9)	(15,13)	(2,7)	(12,1)	(8,14)	(6,6)	(6,11)	(10,15)	(8,3)	(15,4)	(12,16)	(5,8)	(3,0)	(10,2)
(1,12)	(1,12)	∞	(2,7)	(5,8)	(1,5)	(15,4)	(12,16)	(2,10)	(6,11)	(8,3)	(10,2)	(6,6)	(15,13)	(8,14)	(5,9)	(12,1)	(10,15)	(3,0)
(2,7)	(2,7)	(1,12)	(5,8)	(12,16)	∞	(10,15)	(12,1)	(1,5)	(8,3)	(10,2)	(15,13)	(6,11)	(3,0)	(6,6)	(2,10)	(5,9)	(8,14)	(15,4)
(2,10)	(2,10)	(5,9)	(1,5)	∞	(12,1)	(10,2)	(1,12)	(12,16)	(10,15)	(8,14)	(6,6)	(15,4)	(6,11)	(3,0)	(5,8)	(2,7)	(15,13)	(8,3)
(3,0)	(3,0)	(15,13)	(15,4)	(10,15)	(10,2)	∞	(8,14)	(8,3)	(12,16)	(12,1)	(5,9)	(5,8)	(2,10)	(2,7)	(6,11)	(6,6)	(1,12)	(1,5)
(5,8)	(5,8)	(2,7)	(12,16)	(12,1)	(1,12)	(8,14)	(5,9)	∞	(10,2)	(15,13)	(3,0)	(8,3)	(15,4)	(6,11)	(1,5)	(2,10)	(6,6)	(10,15)
(5,9)	(5,9)	(12,1)	(2,10)	(1,5)	(12,16)	(8,3)	∞	(5,8)	(15,4)	(10,15)	(8,14)	(3,0)	(6,6)	(15,13)	(2,7)	(1,12)	(10,2)	(6,11)
(6,6)	(6,6)	(8,14)	(6,11)	(8,3)	(10,15)	(12,16)	(10,2)	(15,4)	(1,5)	∞	(1,12)	(2,10)	(2,7)	(5,9)	(3,0)	(15,13)	(12,1)	(5,8)
(6,11)	(6,11)	(6,6)	(8,3)	(10,2)	(8,14)	(12,1)	(15,13)	(10,15)	∞	(1,12)	(2,7)	(1,5)	(5,8)	(2,10)	(15,4)	(3,0)	(5,9)	(12,16)
(8,3)	(8,3)	(6,11)	(10,2)	(15,13)	(6,6)	(5,9)	(3,0)	(8,14)	(1,12)	(2,7)	(5,8)	∞	(12,16)	(1,5)	(10,15)	(15,4)	(2,10)	(12,1)
(8,14)	(8,14)	(10,15)	(6,6)	(6,11)	(15,4)	(5,8)	(8,3)	(3,0)	(2,10)	(1,5)	∞	(5,9)	(1,12)	(12,1)	(15,13)	(10,2)	(12,16)	(2,7)
(10,2)	(10,2)	(8,3)	(15,13)	(3,0)	(6,11)	(2,10)	(15,4)	(6,6)	(2,7)	(5,8)	(12,16)	(1,12)	(12,1)	∞	(8,14)	(10,15)	(1,5)	(5,9)
(10,15)	(10,15)	(15,4)	(8,14)	(6,6)	(3,0)	(2,7)	(6,11)	(15,13)	(5,9)	(2,10)	(1,5)	(12,1)	∞	(12,16)	(10,2)	(8,3)	(5,8)	(1,12)
(12,1)	(12,1)	(12,16)	(5,9)	(2,10)	(5,8)	(6,11)	(1,5)	(2,7)	(3,0)	(15,4)	(10,15)	(15,13)	(8,14)	(10,2)	(1,12)	∞	(8,3)	(6,6)
(12,16)	(12,16)	(5,8)	(12,1)	(5,9)	(2,7)	(6,6)	(2,10)	(1,12)	(15,13)	(3,0)	(15,4)	(10,2)	(10,15)	(8,3)	∞	(1,5)	(6,11)	(8,14)
(15,4)	(15,4)	(3,0)	(10,15)	(8,14)	(15,13)	(1,12)	(6,6)	(10,2)	(12,1)	(5,9)	(2,10)	(12,16)	(1,5)	(5,8)	(8,3)	(6,11)	(2,7)	∞
(15,13)	(15,13)	(10,2)	(3,0)	(15,4)	(8,3)	(1,5)	(10,15)	(6,11)	(5,8)	(12,16)	(12,1)	(2,7)	(5,9)	(1,12)	(6,6)	(8,14)	∞	(2,10)

Figura 2.2. Curva di Bitcoin, Slide del corso *Blockchain e criptoeconomia*

In questo modo entrambi gli utenti condividono la stessa chiave segreta $K = k_A k_B P$, pur non conoscendo la chiave privata scelta dall'altro.

In un **sistema a chiave pubblica** sulle curve ellittiche, invece, scelto un punto G della curva, ogni utente:

- sceglie un numero casuale d che fa da chiave privata;
- calcola il prodotto dG come chiave pubblica, così che risalire alla privata sia equivalente all'ECDLP.

Quasi tutti gli algoritmi crittografici si adattano all'utilizzo di questo strumento, rendendo la crittografia basata su curve ellittiche più efficiente e potente di tutte le alternative. Basti pensare che criptosistemi con chiavi a 256 bit sono molto più forti di RSA con chiavi a 4096 bit. Quello che rende i sistemi basati sulle curve ellittiche complessi da utilizzare è la cifratura del messaggio. Infatti, nei cifrari classici un testo viene diviso in

blocchi e codificato ottenendo una sequenza di numeri interi, così da poter essere visto come un elemento di $\mathbb{Z}_N$ e quindi cifrato e decifrato. Nei sistemi su curve ellittiche è necessario trasformare una sequenza di numeri interi in un punto della curva,cosa che avviene attraverso algoritmi di codifica probabilistica.

2.2 Firme Digitali

Nei sistemi a chiave pubblica chiunque può cifrare un messaggio. Diventa quindi necessario validarlo, attraverso una firma digitale.

Dati due utenti, A e B, siano f_A e f_B le funzioni che rappresentano le loro chiavi pubbliche, unidirezionali e difficili da invertire, a meno di non conoscere le chiavi private dei due utenti, f_A^{-1} e f_B^{-1}. Lo schema generale che l'utente A può applicare per firmare un documento M, è mandare a B $f_B(M)$, cosa che tuttavia non garantisce l'identità di A. Infatti, essendo f_B la chiave pubblica di B, chiunque potrebbe spacciarsi per A e firmare documenti a suo nome. Per questo motivo, il protocollo generale prevede anche l'invio da parte di A della coppia $(f_B(f_A^{-1}(s_A)), s_A)$, dove s_A è un testo che contiene i dettagli dell'invio e può essere visto come la firma digitale di A. In questo modo B, applicando $f_A f_B^{-1}$ può verificarne il contenuto. La firma è quindi personalizzata, un terzo utente non può spacciarsi per A perché ha bisogno della funzione privata f_B^{-1} per ottenere $f_A^{-1}(s_A)$. L'unica conseguenza di questa scelta è il rischio che lo stesso utente B possa riutilizzare la firma di A. Per questo motivo, si tende a far dipendere ogni firma dal messaggio mandato attraverso una sua impronta $h(M)$, ovvero mandando la coppia $(f_B(f_A^{-1}(s_A||h(M))), s_A)$.

2.2.1 Firma digitale con RSA

RSA è un cripto sistema basato sull'utilizzo di una chiave pubblica e di una privata e quindi si presta bene al sistema di firma digitale. Ogni utente ha a disposizione una chiave pubblica costruita sulla base della fattorizzazione scelta, quindi l'unica complicazione è data dal fatto che lo spazio dei messaggi è diverso, perché dipendente dalle chiavi ottenute ($\mathbb{Z}_{N_A}$ per l'utente A e $\mathbb{Z}_{N_B}$ per B) così come le rispettive funzioni di cifratura e decifratura. Il processo di firma si compone dei seguenti passaggi.

- A sceglie un numero $s_A \in \mathbb{Z}_{N_A}$ e lo rende pubblico perché costituisce la sua firma digitale.
- Manda quindi a B il messaggio M e $m_A = f_B(f_A^{-1}(s_A))$.
- B verifica che $f_A(f_B^{-1}(m_A)) = s_A$ e che quindi la firma sia di A.

Questo processo funziona solo nel caso in cui $N_A < N_B$. Se $N_A > N_B$ il protocollo è leggermente diverso.

- A sceglie un numero $s_A \in \mathbb{Z}_{N_A}$ e lo rende pubblico.
- Quando scrive il messaggio aggiunge la firma $m_A = f_B(f_A^{-1}(s_A mod N_B))$.
- B verifica che $f_A(f_B^{-1}(m_A)) = s_A$ e che quindi la firma sia di A.

Anche in questo caso l'unico utente che può appropriarsi della firma di A è B, perché ha a disposizione $f_B(f_A^{-1}(s_A))$ e, di conseguenza, l'unica soluzione è nuovamente far dipendere la firma dal messaggio.

2.2.2 Firma digitale con curve ellittiche

Anche i criptosistemi pubblici su curve ellittiche hanno, vista la loro struttura, un sistema di firma digitale associato. Sia dato un punto G su una curva di N punti, in modo da poter scegliere una chiave privata d e calcolare il punto $P = dG$ da utilizzare come chiave pubblica.

- Il mittente calcola l'impronta del messaggio in chiaro $h = h(M)$ (attraverso una funzione hash h unidirezionale).
- Sceglie a caso un valore $k \in \mathbb{Z}_N$.
- Calcola il punto della curva $kG = (x, y)$.
- Fissa $r = x$ mod N e calcola $s = (h + rd)k$ mod N.

La firma digitale è costituita dalla coppia (r, s). La firma è personalizzata perché solo A è in grado di calcolare s, che dipende dalla chiave privata d, Inoltre, B non può riutilizzare la firma di A perché dipendente dall'impronta del messaggio mandato. L'unica complicazione è data dal fatto che il processo di verifica non è immediato, ma si svolge in pochi passaggi.

- L'utente B calcola l'inverso di s: $w = s^{-1} = k/(h + rd)$.
- Calcola $u = wh$ e $v = wr$.
- Ottiene il punto $Q = uG + vP$, con $P = dG$.

Se l'utente che ha ricevuto il messaggio riesce ad ottenere tutte le informazioni corrette, la prima componente di Q coincide con r e la firma è valida:

$$Q = uG + vP = whG + wr(dG) = \Big(\frac{kh}{h + rd} + \frac{krd}{h + rd}\Big)G = kG = (x, y)$$

2.3 Funzioni Hash

Le funzioni hash sono alla base di tutti i protocolli crittografici, servono per condensare gruppi di transazioni in blocchi e collegarli tra loro, creando effettivamente una blockchain. Una hash viene definita come una funziona matematica che prende in input dei dati e restituisce un'impronta (detta hash o digest) di lunghezza fissata (di solito 160, 256, 384 o 512 bit).

Sia dato, quindi, un alfabeto, ovvero un insieme Σ, e sia Σ^* l'insieme di tutte le parole di lunghezza arbitraria ottenibili da Σ. Una funzione hash è un'applicazione, con n fissato:

$$h : \Sigma^* \longrightarrow \Sigma^n.$$

Quando il dominio di una funzione hash è finito, la funzione è detta di compressione. Le funzioni hash sono di particolare interesse poiché godono dell'effetto valanga, ovvero producono impronte molto diverse, anche con input molto simili. Infatti, sono progettate per essere unidirezionali (one-way), ovvero difficili da invertire: l'unico modo per ricreare i dati di input dall'output è andare per tentativi. Questo garantisce l'immutabilità dei dati che vengono crittografati e per questo motivo, all'interno della blockchain, il loro principale utilizzo è quello di collegare e condensare gruppi di transazioni in blocchi.

Inoltre, possedere o essere in grado di calcolare l'hash di un documento o di un testo, è parte di molti protocolli crittografici, per una serie di motivi:

1. Si può dimostrare di non aver modificato un documento, provando di essere in grado di calcolare in momenti diversi la stessa impronta.

2. Zero-Knowledge Proof: si può dimostrare di essere in possesso di un documento senza mostrarne il contenuto. L'impronta servirà poi come prova di immutabilità.

3. Proof of Work: è il protocollo che prende parte alla validazione dei blocchi di molte blockchain. Poiché ottenere una specifica hash richiede un numero di tentativi arbitrari, si può creare un sistema grazie al quale dimostrare di aver svolto un lavoro.

Una coppia di elementi $(a, b) \in \Sigma^*, a \neq b$, tale che $h(a) = h(b)$ si dice collisione. L'inviolabilità di una funzione hash dipende dalla complessità nel saper determinarne delle collisioni.

- h(x) si dice unidirezionale se, data un'impronta z, è un problema computazionalmente intrattabile ricavare x tale che $h(x) = z$.

- h(x) si dice debolmente priva di collisioni se per $a \in \Sigma^*$ fissato, determinare b tale che $h(a) = h(b)$ è un problema computazionalmente intrattabile.

- h(x) si dice fortemente priva di collisioni se determinare una qualsiasi collisione (a, b) è un problema computazionalmente intrattabile.

Le funzioni hash non agiscono sul messaggio originale, ma quest'ultimo viene predisposto all'algoritmo attraverso alcuni passaggi. In particolare, il testo che si vuole crittografare viene suddiviso in blocchi della stessa lunghezza. Se il messaggio in ingresso risulta più corto si fa il *padding* del messaggio, ovvero si inseriscono dei valori casuali negli ultimi blocchi. Dopo di che, sui singoli blocchi agiscono man mano delle funzioni one-way, a seconda dell'algoritmo di riferimento. Le più note e sicure funzioni hash sono:

1. MD5 (Message Digest 5)
   Una delle prime funzioni hash è MD5, realizzata nel 1991 per migliorare la precedente MD4. Diventata ben presto vulnerabile, viene usata oggi in molte applicazioni web, nella memorizzazione delle password nei server. Per evitare di memorizzare la password dei singoli utenti, viene salvata una copia codificata con MD5 da usare come confronto durante i login successivi.
   Il testo da cifrare viene diviso in 4 blocchi da 32 bit, ognuno dei quali subisce 16 operazioni, così da produrre impronte a 128 bit. L'algoritmo agisce per un totale

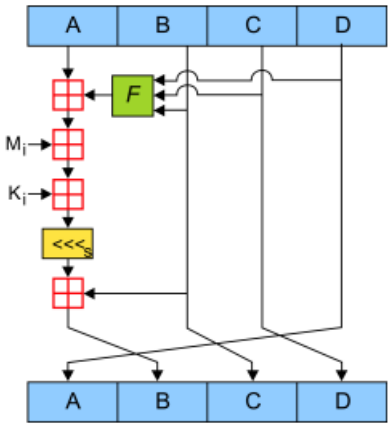


Figura 2.3. MD5, Slide del corso *Blockchain e criptoeconomia*

di 64 volte sul messaggio di partenza. In particolare, su ogni blocco viene applicata una funzione non lineare F in relazione a una costante K_i, ogni volta differente.

2. RIPDEM
   Un'altra hash usata da molte criptovalute è RIPDEM-160, nata nel 1994, la cui versione più nota produce impronte a 160 bit. Questa hash prende in ingresso un input multiplo di 512 bit diviso in parole di 32 bit. Vengono quindi usate operazioni in modulo 2^{32} sui cifrati parziali. L'algoritmo agisce per un totale di 5 round. In particolare, una funzione di compressione agisce parallelamente su due rami, attraverso 16 step ciascuno, per un totale di 80 step nell'intero algoritmo.

3. SHA (Secure Hash Algorithm)
   Le funzioni SHA sono una famiglia di 5 funzioni crittografiche sviluppate nel 1993 dalla National Security Agency e pubblicate dal NIST (National Institute of Standards and Technology) come standard federale del governo degli USA. La prima (SHA-1) produce un digest di 160 bit, gli altri 4 algoritmi sono indicati come SHA-2 e producono digest di 224, 256, 384 e 512 bit. La funzione SHA-256 fa parte della famiglia di SHA-2 e opera su stringhe di lunghezza multipla di 512 bit. L'algoritmo opera con parole da 32 bit e, anche in questo caso, effettua quindi delle operazioni modulo 2^{32} per 64 round.

4. SHA-3
   Il 2 novembre del 2007 il NIST annunciò un concorso pubblico per stabilire un nuovo standard crittografico [9]. La competizione ha portato allo sviluppo di SHA-3, dichiarato nel 2015 come nuovo standard. L'algoritmo deriva della famiglia di primitive crittografiche Keccak e, a differenza del predecessore SHA-2, è una hash di tipo sponge con un numero variabile di round, che fornisce digest di lunghezza arbitraria, di solito di 224, 256, 384 o 512 bit. L'algoritmo si compone di una prima

fase di cicli che assorbono i blocchi del testo iniziale (la fase a spugna, ”sponge”) e di una seconda fase di spremitura (”squeezing”), che produce digest di lunghezza arbitraria.

Capitolo 3

La tecnologia Blockchain

3.1 L'origine

La blockchain è una tecnologia innovativa che nasce con l'esigenza di decentralizzare alcuni sistemi informatici, tutelare la privacy dei suoi utenti e automatizzare processi per mezzo di smart contract.

Il suo approccio rivoluzionario permette di gestire protocolli che non sono dipendenti da un'autorità centrale, un ente necessario per creare scambi tra sconosciuti, tra i quali manca fiducia reciproca, così da avere un garante per le transizioni. Che sia una banca, lo stato, o qualsiasi tipo di organizzazione, il ruolo dell'autorità centrale non sempre ha un impatto positivo. Può mettere a rischio la privacy dei suoi utenti o costituire una minaccia alla sicurezza dell'intera rete. Un sistema informatico basato su un'autorità centrale si dice centralizzato, ed è facile da attaccare perché compromesso dalla sicurezza del solo server centrale dell'autorità. L'obiettivo che sta alla base della nascita della blockchain è la volontà di creare di una rete decentralizzata, di utenti che non si conoscono, non si fidano l'uno dell'altro ma sono in grado di scambiarsi operazioni e transazioni in modo sicuro e che, quindi, godono degli stessi diritti.

Non a caso questa tecnologia è nata anche in risposta a una rivoluzione sociale ed economica iniziata già nei primi anni 90. In quegli anni molti informatici sentirono l'esigenza di muoversi nel mondo digitale in maniera quanto più anonima possibile, difendendo la loro privacy (attraverso l'uso della crittografia) e creando una criptomoneta digitale, anonima e distribuita, per sfuggire all'autorità e ai costi di transizioni delle banche centrali. Con il tempo le stesse necessità hanno mosso diverse realtà digitali ad adottare questa tecnologia, dando luogo a una vera e propria rivoluzione industriale.

In base al tipo di pubblico a cui si presenta questa tecnologia, la blockchain può essere:

- pubblica (permissionless): blockchain le cui transazioni sono consultabili liberamente e alle quali chiunque potenzialmente può partecipare.

- privata (permissioned): blockchain la cui rete peer-to-peer è composta da una cerchia ristretta di utenti. Di solito, costruiscono blockchain private tutte quelle organizzazioni aziendali che puntano alla decentralizzazione dei propri sistemi.

La distinzione si basa principalmente sul numero di utenti, e sulla modalità di partecipazione alla blockchain e comporta diverse scelte strutturali. Nelle blockchain pubbliche la rete è molto più ampia e costituita da utenti che non si fidano l'uno dell'altro. Questo richiede una maggiore sicurezza dei protocolli interni, cosa che non è strettamente necessaria nel caso delle blockchain private.

3.2 Un dataset distribuito

Con l'obiettivo di creare di una rete decentralizzata, la blockchian è stata concepita come un dataset distribuito, che prende il nome di Distributed Ledger Techonology, perché duplica e archivia i dati in suo possesso in diversi nodi di una rete. Le conseguenze più dirette di questa scelta sono due:

1. Trasparenza e immutabilità: i dati all'interno sono immodificabili ed estremamente al sicuro. La presenza di infinite copie garantisce un controllo immediato e verificabile di tutte le operazioni. Una volta registrata una transazione su blockchain, non può essere modificata o cancellata. Le transazioni sono quindi irreversibili. Questa abilità della blockchain di prevenire l'alterazione delle transazioni già confermate fa sì che venga definita immutabile.

2. Resistenza agli attacchi: a differenza del modello centralizzato, la Distributed Ledger Techonology si basa su un modello decentralizzato. Non esiste un singolo punto di attacco, ma è necessario compromettere contemporaneamente la sicurezza di tutti i nodi coinvolti.

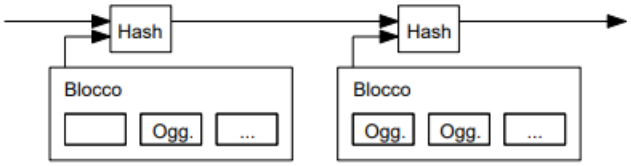


Figura 3.1. Struttura blockchain, Bitcoin: A Peer-to-Peer Electronic Cash System [2]

La blockchain è detta così a causa della sua struttura. Gli utenti non dispongono di un singolo file, ma i dati sono divisi in blocchi, collegati tra loro da una struttura a catena in Fig. 3.1. Ogni blocco punta al precedente attraverso il calcolo reiterato di funzioni hash, grazie le quali poter ricostruire la catena. Il fatto che i dati siano distribuiti in maniera trasparente in una rete decentralizzata, rende necessario l'utilizzo della crittografia, sia per tutelare la privacy degli utenti che per garantire transazioni sicure attraverso firme digitali. In questo modo si ottiene una struttura dati non modificabile. L'immutabilità, combinata con gli algoritmi di consenso, garantisce al sistema estrema sicurezza.

3.3 Struttura blocchi

I dati memorizzati nella blockchain sono transazioni da un utente a un altro. Ogni blocco è formato da un body, che contiene le transazioni, e un header, che contiene sette campi di gestione:

1. Il magic number, relativo alla blockchain alla quale appartiene il blocco.
2. Il numero della versione del blocco.
3. L'hash dell'header del blocco precedente.
4. L'hash del Merkle Root, ovvero l'hash di tutte le transazioni del blocco.
5. Il timestamp del blocco corrente.
6. Il valore del target in forma compatta, necessario per validare il blocco, detto Bits.
7. Il Nonce, un valore che viene inserito in modo casuale durante il protocollo di validazione.

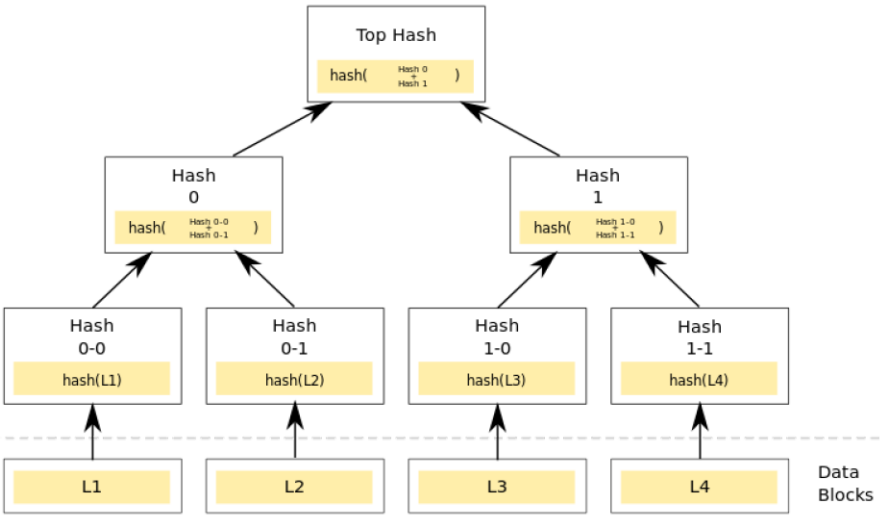


Figura 3.2. Merkle Root, Slide del corso *Blockchain e criptoeconomia*

Questa struttura garantisce l'immutabilità della catena. Se ci fosse anche solo una variazione di un bit in una transazione di un blocco, allora cambierebbe il Markle Root del blocco (che si trova nell'header) e di conseguenza la hash dell'header del blocco seguente.

Per risalire a una data transizione basta ripercorrere il Merkle Root, oppure costruire un cammino alternativo attraverso il Merke Tree. Il Merkle Tree permette di risalire a una transazione con un cammino più breve, che ha una lunghezza proporzionale al logaritmo del numero delle transizioni. La verifica di una transazione avviene attraverso

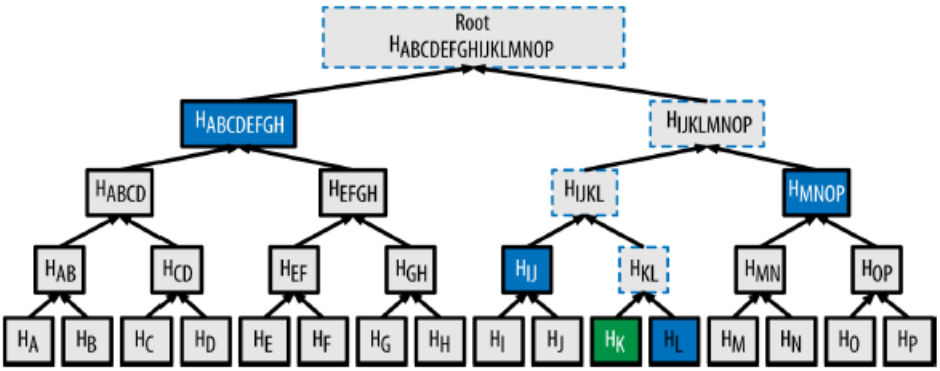


Figura 3.3. Merkle Tree, Slide del corso *Blockchain e criptoeconomia*

il simple-payment-verification. Grazie a questo protocollo, un utente può permettersi di non memorizzare l'intera blockchain ed essere comunque certo che tutti i dati siano corretti. Basta farsi mandare tutte le hash intermedie (in blu in Fig. 3.3) che collegano la transazione da verificare all'ultimo blocco inserito, di cui si possiede l'header e ripercorrere verticalmente il Merkle Tree. Questo tipo di verifica permette di distinguere gli utenti della rete in due categorie:

- Full node: utente che memorizza l'intera blockchain e quindi tutte le transizioni al suo interno.
- Light node: utente che memorizza solo gli header di tutti i blocchi. Chi gioca questo ruolo può verificare autonomamente una transizione appoggiandosi a un full node, attraverso il simple-payment-verification.

3.4 Le transizioni

Quello che compone il corpo di ogni blocco è un elenco di transizioni, passaggi da un nodo a un altro di criptomoneta, o di qualsiasi asset digitale, in maniera del tutto anonima e sicura.
Quando un utente vuole fare una transazione:

1. Crea una coppia di chiavi, una pubblica e una privata mediante un fissato ECC (Elliptic Curve Cryptosistems).
2. Calcola il suo indirizzo di riferimento, associato alla chiave pubblica, detto input Address. Una volta creato, può fare una transazione solo se precedentemente ha ricevuto del denaro su quell'indirizzo.
3. Scrive la transazione, fissando l'indirizzo di output del destinatario.

4. Firma digitalmente la transazione mediante e l'Elliptic Curve Digital Signature Algorithm (ECDSA).

Chi riceve la transazione è in grado di verificare l'indirizzo di provenienza grazie alla firma del mittente.

L'Indirizzo si ricava dalla chiave pubblica, attraverso un algoritmo che utilizza alcune tra le più note funzioni hash. L'utilizzo di un indirizzo e non della chiave pubblica rende molto difficile inviare la transazione all'utente sbagliato e non permette di risalire in alcun modo alla chiave privata. Inoltre, rende il processo molto più sicuro, perché in questo modo la chiave resta segreta fino a che l'utente non spende nuovamente la criptomoneta ricevuta. In quel momento, pubblica la sua chiave pubblica e utilizzando la sua chiave privata dimostra di essere il legittimo proprietario della criptomoneta che andrà a spendere.

Oltre alle transazioni regolari che compongono una blockchain, in base al meccanismo di validazione esistono altri tipi di transazioni:

- In alcune blockchain la prima transazione di ogni blocco ha un unico input, cioè non corrisponde a un output precedente. Esso è detto coinbase e ha come output l'indirizzo di chi ha validato il blocco.

- Inoltre, alcuni progetti blockchain prevedono per ogni transazione da validare il pagamento di una fee, ovvero di una tassa. Essa rappresenta l'importo che un utente è disposto a pagare per vedere realizzata la propria operazione.

3.5 Protocolli di consenso

La tecnologia blockchain ha introdotto nel mondo digitale il concetto di consenso distribuito, ovvero degli algoritmi per mettere d'accordo una rete di utenti che non si fidano gli uni degli altri.

Un sistema blockchain può essere descritto come un sistema first-to-file: se un'entità spende simultaneamente gli stessi fondi, inviandoli a due utenti diversi, solamente la transazione che viene confermata per prima sarà processata. Senza l'utilizzo della tecnologia blockchain, queste due transizioni potevano essere contemporaneamente valide, poiché era impossibile determinare quale fosse avvenuta prima senza un'autorità centrale, rischiando di incorrere nel cosiddetto double-spending. Oltre al rischio di double-spending, i dati di un blocco, una volta approvato e registrato, non possono essere alterati senza che vengano modificati tutti i blocchi successivi ad esso. Per questo motivo, il processo di validazione deve essere gestito e progettato in modo da trovare il consenso di tutta la rete ed evitare errori. Regolare il processo di validazione consente inoltre di gestire il problema della scalabilità di una blockchain, ovvero il numero massimo di transizioni che possono avvenire in un dato intervallo temporale.

Gli utenti che partecipano agli algoritmi di consenso sono chiamati *miner* e possiedono una copia aggiornata della blockchain. Hanno il compito di controllare l'integrità dei dati e raccoglierli in un blocco da validare. La validazione avviene a seguito della vincita di una sfida, data dal protocollo di consenso, ma può essere anche automatica a seconda del progetto blockchain. Quando si parla di criptovalute, i miner sono invogliati a partecipare

ai protocolli di validazione, poiché ricompensati attraverso la coinbase. L'algoritmo di mining premia chiunque arrivi per primo alla soluzione del problema, che riceverà l'intera quantità di bitcoin estratti in quello specifico blocco della Blockchain, e le commissioni di transazione del blocco.

Quando due blocchi vengono inseriti simultaneamente si genera una biforcazione della catena, anche detta *fork*. Quando si crea una fork, entrambi i blocchi vengono considerati momentaneamente validi. Ogni blockchain risolve in maniera differente la creazione di una biforcazione, implementando algoritmi di consenso che spingono tutta la community a minare su uno qualsiasi dei due rami della catena. L'incentivo è dato dal fatto che le transazioni contenute nei blocchi abbandonati non saranno mai validate, impedendo ai miner di ottenere la ricompensa per aver minato tali blocchi e le relative fee. Di conseguenza, appena in una delle due biforcazioni viene validato ed aggiunto un nuovo blocco, i miner tenderanno a minare sul ramo più lungo. In casi come questi la divisione della catena è un fenomeno quasi casuale, che viene risolto rapidamente in base all'algoritmo di consenso.

Il termine biforcazione viene usato anche nei casi in cui avviene una vera e propria divisione della rete decentralizzata. Può accedere che un gruppo di utenti proponga il cambiamento di un protocollo, o veda nel progetto nuove prospettive. In assenza di un'autorità centrale e per la natura stessa della blockchain, un gruppo di utenti può decidere di emanciparsi e creare un progetto blockchain parallelo. In casi come questi la biforcazione può essere di due tipi:

- Soft fork: una parte degli utente adotta un protocollo nuovi, permettendo a chi mantiene il vecchio software di continuare a operare regolarmente.
- Hard fork: nasce un nuovo progetto blockchain che condivide però con la catena originale tutti i blocchi fino al momento della fork.

Il protocollo di consenso viene scelto dagli sviluppatori in base alle esigenze e alla grandezza della community che deve mettere d'accordo.

Proof of Work

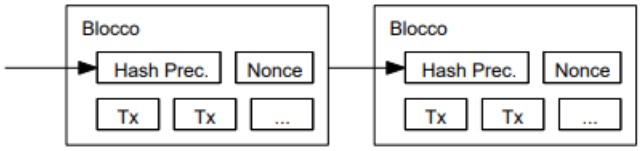


Figura 3.4. PoW, Bitcoin: A Peer-to-Peer Electronic Cash System [2]

Il protocollo più famoso per mettere d'accordo una rete di utenti priva di un'autorità centrale è la Proof of work (PoW). Esso è strutturato in modo che un utente possa

dimostrare di aver fatto un lavoro in maniera semplice e immediata, ma nel contempo dimostrando alla community impegno e responsabilità.

L'algoritmo utilizza la Zero Knoledge Proof, che grazie alle funzioni hash permette a una rete di utenti di trovare un sistema di verifica immediato. La dimostrazione da presentare per validare un blocco non è altro che l'hash dell'header del blocco precedente. La prova in questione consiste nell'aggiungere al testo di riferimento uno o più caratteri, sotto il nome di *nonce*, in modo che l'hash risulti minore di un certo target. Per la natura stessa delle funzioni hash la prova è puramente lasciata al caso e può essere superata solamente per tentativi. Data la casualità del problema, è possibile stimare il tempo impiegato a produrre la PoW, e quindi, scegliere adeguatamente il target in modo da regolare il tempo di validazione di un blocco.

La prima applicazione della PoW è avvenuta nel 1997 grazie ad Adam Back, che propose l'Hashcash, per limitare le email spam e gli attacchi di denial of service [1]. Il protocollo prevede che un utente, prima di mandare una mail o chiedere l'accesso a un servizio, debba dimostrare alla rete di aver svolto un lavoro. Esso non è altro che l'hash, usando SHA-1 a 160 bit di un header che contiene data, ora, indirizzo IP e indirizzo mail, al quale aggiungere un nonce, scelto in modo che l'impronta inizi con 20 zeri. La probabilità di ottenere un target corretto è molto bassa e servono in media 2^{20} tentativi. Nelle applicazioni più recenti si utilizzano funzioni hash più complesse.

La PoW può essere eseguita da processori con hardware specifico, gli ASIC (Application Specific Integrated Circuit), che eseguono calcoli matematici molto complessi. Possono essere eseguiti sia da privati che da aziende, le Mining Pool.

Proof of Stake

Il secondo più importante protocollo di consenso è la Proof of Stake. Letteralmente, è una prova di interesse, che chi vuole validare il blocco ha in quanto possessore di una grande quantità di criptomoneta. In questo modo, non è più necessario affidarsi a dispendiosi protocolli crittografici, ma i validatori vengono scelti direttamente dal sistema in maniera casuale e con probabilità proporzionale alla loro ricchezza. In particolare, i criteri usati per scegliere i validatori sono:

- Random, usando quindi metodi probabilistici.
- Anzianità, usata come unità di misura e definita come il prodotto tra la quantità di moneta posseduta per il numero di giorni in cui sono state conservate. In questo modo, l'anzianità torna a zero subito dopo aver fatto da validatore e decade se il tempo di possesso diventa troppo grande.
- Velocità, intesa come unità di misura dell'utilizzo più che del solo possesso.

Sulla carta, quindi, la PoS presenta molti miglioramenti rispetto alla PoW, tra i quali i minori consumi di energia e una maggiore velocità di validazione. Questo rende la blockchain molto più scalabile e le operazioni più veloci. Inoltre, i miner coinvolti nel processo sono molto più motivati poiché fanno parte della rete peer-to-peer in modo attivo.

L'unico difetto presente rispetto alla Proof of Work è la gestione delle fork, perché i miner non hanno nessuna posta in gioco. Infatti, nella PoW sono spronati a far crescere la catena in una sola direzione, a causa della perdita dei blocchi orfani. In questo caso, non costa nulla lavorare su entrambi i rami della biforcazione. Per evitare questo scenario si può fare un Checkpoint dell'intera blockchain, limitare la riorganizzazione dei blocchi ed eventualmente punire chi lavora su due rami contemporaneamente.

Delegated Proof of Stake

Un'evoluzione della PoS è rappresentata dalla Delegated Proof of Stake (DPoS), in cui il gruppo dei miner è ristretto a pochi utenti. Essi vengono eletti con un sistema di votazione in cui i voti sono pesati in base alla ricchezza posseduta. Di conseguenza, chi ha maggiore ricchezza, ha un potere decisionale superiore.

Gli utenti si dividono in producers, ovvero coloro che sono stati delegati alla validazione dei blocchi e in validatori (validators), composti da chi possiede un full node e, quindi, una copia della blockchain. Una volta eletto il gruppo di producers, un blocco viene inserito solo se trova il consenso di almeno 2/3 del gruppo ed è considerato valido da tutti i validatori.

Pure Proof of Stake

Un altro protocollo molto simile al precedente è dato dalla Pure Proof of Stake (PPoS). A differenza della PoS, il comitato di producers viene sorteggiato ogni volta che un blocco deve essere aggiunto alla blockchain. Questo sorteggio avviene costantemente e con probabilità proporzionale alla quantità di moneta posseduta. Una volta scelto, un utente dimostra alla rete di essere stato sorteggiato solo dopo aver validato il blocco, in modo da non subire attacchi o corruzioni.

Proof of Importance

La Proof of Importance (PoI) è un protocollo di consenso simile alla PoS, con la differenza che il fattore di interesse non si basa sulla quantità di moneta posseduta ma scambiata.

Proof of Autority

Un altro importante protocollo di consenso è la Proof of Autority (PoA). Anche in questo caso la validazione dei blocchi viene affidata a un gruppo ristretto di miner, scelti in base alla loro reputazione. A differenza della PoS un miner dimostra il proprio interesse implicitamente e rivelando la propria identità. Questo rende il protocollo molto più adatto a progetti privati, o con pochi utenti. Inoltre, dato il numero limitato di validatori, la blockchain risulta molto scalabile il meccanismo di validazione rapido. Sorgono comunque alcune difficoltà durante le elezioni dei nuovi producers, soprattutto a causa della necessità di mantenere uno standard coerente, che in una rete decentralizzata è difficile da trovare. Inoltre, essendo le identità di questi utenti note a tutta la rete, è molto più facile attaccare il sistema corrompendo alcuni di essi. Nella PoA per attaccare il sistema non serve avere la potenza di calcolo del 51% della rete, ma controllare il 51% dei validatori, indebolendo

la decentralizzazione della rete. Per questo motivo, la PoA è adatta soprattutto alle blockchain private (permissioned) e ai contesti aziendali, in cui esiste un'autorità centrale e la decentralizzazione non è strettamente necessaria.

Proof of Burn

In questo protocollo di consenso il modo per dimostrare interesse è eliminare, quindi bruciare, criptomoneta. Il processo è molto simile alle PoS nella modalità di sorteggio, poiché proporzionale alla moneta bruciata. Inoltre, rispetto alla PoW, dove si spende tempo ed energia per aumentare le probabilità di validare un blocco, in questo caso la prova di interesse è altrettanto immediata ma non richiede lo stesso spreco di risorse. Bruciare moneta è molto facile perché basta fare una transazione a un indirizzo per cui non è stata creata la chiave privata. In questo modo la criptomoneta non è del tutto persa ma è inutilizzabile e quindi bloccata nel sistema. Inoltre, l'atto di bruciare criptomoneta non deve essere considerato come uno spreco di risorse, bensì come un gesto che crea scarsità economica e quindi un aumento del valore nel mercato. L'unico rischio, come nella PoW è di bruciare troppa criptomoneta e poi non arrivare a validare un blocco, a seguito del quale il miner viene ricompensato.

3.6 Bitcoin

La prima grande vera applicazione della tecnologia blockchain è Bitcoin, la prima criptovaluta (BTC) con il maggiore valore economico sul mercato. Alla fine del 2008 un anonimo inventore, o un collettivo di persone, noto con lo pseudonimo di Satoshi Nakamoto, pubblicò un documento in cui presentava la creazione di una nuova criptomoneta digitale, anonima e decentralizzata [2]. Essa si presenta come un elenco infinito di transazioni tra utenti che non si conoscono e non si fidano l'uno dell'altro, ma che, grazie a questa innovativa tecnologia, sono in grado di scambiarsi criptomoneta senza l'ausilio di un'autorità centrale. "Da un punto di vista tecnico, il libro mastro di una criptovaluta come Bitcoin può essere pensato come un sistema di transizione tra stati, dove esiste uno "stato" che consiste nello stato di proprietà di tutti i Bitcoin esistenti e una "funzione di transizione tra stati" che prende uno stato e una transazione e produce un nuovo stato come risultato. Lo "stato" in Bitcoin è la raccolta di tutte le monete (tecnicamente, "output delle transazioni non speso" o UTXO) di cui è stato eseguito il mining e che non sono ancora state spese, dove ogni UTXO ha un taglio e un proprietario (definito da un indirizzo ricavato dalla sua chiave pubblica crittografata)" [3].

La blockchain utilizzata è pubblica e raggiunge il consenso tramite la PoW. Bitcoin utilizza SHA-256 e resetta periodicamente il livello di difficoltà in modo che tenere costante il tasso di creazione dei blocchi. Attualmente, il target di riferimento viene scelto e ricalibrato ogni 2016 blocchi, in modo da regolare l'ingresso di un blocco ogni 10 minuti nella catena. Per migliorare questo tempo, sono nati dei circuiti integrati specifici, detti ASICS (Applicatioon Specific Integrated Circuit) focalizzati sulla risoluzione della PoW con prestazioni veloci ed efficienti, seppur onerose in termini di costo energetico.

A seguito della validazione di un blocco vengono creati nuovi Bitcoin, con i quali vengono ricompensati i miner, in modo da inserire in modo sistematico altro valore all'interno della blockchain. Inizialmente la ricompensa per il miner stabilita da protocollo era di 50 BTC. Il protocollo di Bitcoin prevede che tale ricompensa sia dimezzata ogni 210.000 blocchi (circa ogni 4 anni). Nel 2020 c'è stato l'ultimo dimezzamento e da allora e per i prossimi 4 anni il compenso sarà 6.25 BTC. In questo modo il sistema di incentivi per i miner è diretto e proviene dall'interno. Se un utente vuole accelerare il processo di validazione per un'operazione urgente, può aggiungere una fee, ovvero una commissione in BTC, da attribuire al miner che validerà il blocco. La PoW che regola la validazione può essere modificata in modo da rendere il processo più o meno scalabile. Questo non solo rallenta l'inserimento delle operazioni di chi non paga le fee, ma agevola tutti quei circuiti specifici impiegati nella sola realizzazione della PoW. La tendenza alla nascita di Mining Pool rischiano di mettere la validazione dei blocchi in mano a pochi soggetti e rendere le rete sempre meno decentralizzata. Questo fa si che il progetto risulti poco scalabile e molto oneroso in termini di consumi elettrici.

3.7 Blockchain 2.0: Ethereum e le DApps

L'introduzione di concetti come i protocolli di consenso e gli asset digitali ha condotto pian piano alla decentralizzazione di molti altri mercati, espandendo il concetto di blockchain a qualcosa di più rivoluzionario del denaro elettronico. Queste sono state le premesse che hanno portato alla nascita di Ethereum, una piattaforma decentralizzata basata su una blockchain nata nel 2013, da un'idea dell'informatico Vitalik Buterin. In questo nuovo ecosistema è concesso lo scambio di valute personalizzate, dette token, che fungono da strumenti finanziari, asset non fungibili, derivati finanziari, e altre risorse digitali che possono rappresentare potenzialmente tutto. Inoltre, in questa nuova ottica trova spazio un'altra importante innovazione, ovvero la possibilità di poter stipulare dei contratti intelligenti, sistemi che trasferiscono asset digitali in accordo con regole pre-impostate. Per citare il whitepaper con cui questa tecnologia è stata introdotta nel mercato [3], "Ethereum permette tutto ciò attraverso la costruzione di quello che in sostanza è il definitivo protocollo astratto e fondante: una blockchain con un linguaggio di programmazione integrato e Turing completo, che permette a tutti di scrivere smart contract e applicazioni decentralizzate dove si possono creare le proprie regole arbitrarie per proprietà, formati delle transazioni e funzioni di transizione tra stati".

3.7.1 Gli Smart Contract

Ethereum e tutti i progetti ad essa ispirati aspirano, dunque, a un meccanismo decentralizzato che permetta di scrivere e stipulare dei contratti automatizzati, detti quindi 'smart'. Infatti, sebbene sia possibile programmare in Bitcoin, il linguaggio di programmazione da utilizzare necessita di un solito background crittografico ed è sottomesso ad alcune limitazioni che non permettono una totale autonomia. Per esempio, non è possibile programmare dei loop per evitare cicli infiniti durante la verifica delle transazioni.

Ethereum, invece, si basa su di un linguaggio di programmazione onnipotente e Turing-completo, chiamato Solidity, che si presta perfettamente a qualsiasi tipo di utilizzo. Il suo codice non è particolarmente ampio, ma riserva possibilità che vanno ben oltre la criptovaluta, ovvero la scrittura di veri e propri contratti, i quali a loro volta possono essere utilizzati per codificare funzioni di transizione di stato arbitrarie, permettendo agli utenti di creare potenzialmente qualsiasi sistema, semplicemente scrivendo la logica in poche righe di codice.

3.7.2 I Token

La visione di un mondo decentralizzato comprende la possibilità di poter scambiare, attraverso transizioni sicure, non solo criptomoneta, ma anche altri asset digitali: i token. Queste risorse digitali esistono anche nel mondo reale sotto forma di beni materiali con un valore specifico, come buoni pasto o punti che si possono collezionare e utilizzare in determinati contesti. Nell'universo blockchain sono un asset digitale che rappresenta un valore o un diritto. I token possono essere usati per fare acquisti, come riserva di valore e per accedere ai servizi specifici della piattaforma oppure come strumento di investimento. Si distinguono in tre categorie.

1. Utility token: Sono come degli asset digitale con un valore, danno diritto all'utilizzo di alcune feature su una piattaforma, a benefici o servizi premium. Possono essere utilizzati come delle azioni da parte degli utenti in contesti in cui bisogna prendere decisioni circa il futuro del progetto, ma non costituiscono una fonte di guadagno.

2. Security token: danno diritto di partecipazione al profitto della blockchain che li ha emessi. A differenza dei precedenti, vengono emessi durante le ICO (Initial Coin Offering) sotto forma di azione o quota di proprietà sul progetto su cui si va a investire. In questo modo chi li acquista ha diritto di voto sulle decisioni gestionale e, nel contempo, un guadagno proporzionale al successo della startup. Vengono quindi utilizzati anche quando si vuole investire in una nuova criptovaluta. In tal caso si configura come una sorta di vendita di una nuova criptovaluta a un determinato prezzo, che viene acquistata da chi si aspetta un aumento di valore nel tempo.

3. Payment token (coin), ovvero le criptomonete.

La distribuzione dei token si sviluppa in due fasi:

1. Fase iniziale di distribuzione, in cui si definisce chi detiene i token e quanti ne vengono lanciati sul network.

2. Fase normale di distribuzione, basata sulle regole e sui contratti della piattaforma.

Esistono diverse strategie per distribuire i token, che vengono scelte in fasi differenti e in base allo scopo del progetto di riferimento. Per esempio, nei progetti che hanno bisogno di investimenti, i token hanno anche un valore di mercato. Diversamente, nelle piattaforme di vendita, vengono usati solamente come merce di scambio o fonte di valore. Alcuni dei meccanismi di distribuzione più comuni sono:

- La vendita attraverso l'Initial Coin Offering (ICO).
- L'allocazione interna, avviene quando si vogliono spronare gli utenti a partecipare da subito attraverso un sistema di remunerazione. I token vengono quindi distribuiti a tutti gli utenti prima di lanciare il progetto blockchain.
- Airdrop passivo, una distribuzione gratuita o a costo nominale nei confronti degli utenti passivi.
- Airdrop interattivo, un'offerta gratuita agli utenti più attivi. Alcuni progetti hanno persino evitato la vendita dei token, lanciando e distribuendo i token direttamente nei wallet degli utenti.

Il metodo di allocazione viene stabilito dagli sviluppatori dell'idea, che ne hanno il pieno controllo. Nonostante questa libertà, bisogna considerare questo passaggio fondamentale. Non avere abbastanza token potrebbe creare difficoltà nel pagare alcune spese. Allo stesso modo, creare da subito un grande numero di risorse può concentrare tutta la ricchezza nelle mani di pochi e inflazionare i prezzi dei token. Quando viene creata una nuova moneta virtuale è obbligatorio stabilirne l'importo massimo. Una volta distribuita, l'ICO non dovrà mai superarlo. Il numero massimo di risorse che verranno create si dice Total Hard Cap e fa in modo che ci sia scarsità digitale e che, quindi, i token creati non perdano di valore.

3.7.3 Lo standard ERC-20

Sebbene Ethereum consenta agli sviluppatori di creare assolutamente qualsiasi tipo di applicazione senza limitazioni a tipi di funzionalità specifici, è tuttavia necessario standardizzare alcuni casi d'uso molto comuni per consentire agli utenti e alle applicazioni di interagire facilmente tra loro. Ciò include l'invio di unità di valuta, la registrazione di nomi, l'offerta di scambi e altre funzioni simili. ERC-20 è uno standard stabilito da Ethereum per scrivere gli smart contract relativi ai token. la sigla ERC è l'acronimo di Ethereum Request Comment e comprende una serie di documenti specifici e tecnici che riguardano la programmazione di uno smart contract. Prima della creazione dello standard, gli utenti dovevano riscrivere da capo il codice per la creazione di ogni token, con il conseguente carico di lavoro e rischi per la funzionalità e la sicurezza. Grazie a questo nuovo sistema, invece, è possibile mantenere delle basi riutilizzabili per più progetti senza dover ogni volta ripartire dall'inizio. I token generati da ERC-20 sono estremamente flessibili, possono essere utilizzati come utility token o security e ricoprire qualsiasi ruolo all'interno de progetto blockchain di riferimento. Per rispettare lo standard ERC-20, è indispensabile che un contratto includa sei funzioni:

- totalSupply: massimo numero di token che possono essere creati;
- balance0f: assegna un numero iniziale di token a qualsiasi indirizzo specificato, solitamente i creatori del token;
- transfer: trasferisce i token a chi li acquista

- transferFrom: invia token da una persona all'altra
- approve: verifica che uno smart contract possa distribuire token, in base alla fornitura restante (verifica necessaria per eseguire 3)
- allowance: verifica che un indirizzo abbia un saldo sufficiente per inviare token ad un altro indirizzo (verifica necessaria per eseguire 4)

Oltre a queste funzioni, è possibile personalizzare lo standard in base alle esigenze degli sviluppatori.

3.7.4 Le DApp

Ethereum è stato il primo ambiente che, grazie al suo linguaggio di programmazione e alla possibilità di scrivere smart contract, ha fornito agli sviluppatori gli strumenti per costruire le DApp, ovvero le prime applicazioni decentralizzate. Le DApp sono applicazioni:

- Decentralizzate: operano su un sistema computazionale distribuito (ovvero un insieme di computer dislocati in qualsiasi punto del globo)
- Open-source: gli smart contract e il codice con cui sono programmate è pubblico e può essere ripreso da altri per essere migliorato o adattato alle esigenze di un determinato scopo
- Autosostenibili. Non hanno bisogno di vendere spazi pubblicitari interni all'app per mantenersi. A seconda delle condizioni espresse dagli smart contract e dalle modalità del consenso distribuito, le DApp sono autosostenibili, sia finanziariamente che a livello di sviluppo. Solamente il completo abbandono del progetto da parte di sviluppatori e utenti finali determinerebbe la fine di una DApp.

Vengono classificate in tre categorie:

1. Tipo I. Sono tutte le DApp che hanno la propria blockchain, su cui eseguono tutti i protocolli. Bitcoin è la prima DApp blockchain mai esistita.
2. Tipo II. In questa classificazione troviamo quelle DApp che dipendono da una blockchain esterna. In questo caso, le DApp possono funzionare utilizzando i propri token o la blockchain su cui girano.
3. Tipo III. DApp di questo tipo utilizzano DApp di tipo II per il loro funzionamento. Generalmente, le DApp di tipo III utilizzano i token delle DApp di tipo II per svolgere le loro operazioni.

le DApp hanno molto in comune con le applicazioni tradizionali, sono formate dagli stessi elementi di base, la differenza sta nel modo in cui interagiscono con questi elementi. Il *frontend*, ovvero l'interfaccia utente ha le stesse caratteristiche tipiche delle applicazioni sul mercato, in grado di comunicare con gli utenti in modo chiaro e diretto. Il *backend* invece fa riferimento alla logica con cui si sviluppa un'applicazione e assume un significato del tutto diverso. In una DApp è formato da una serie di smart contract, che regolano il

funzionamento dei singoli comandi. In questo modo gli utenti sono sicuri che l'applicazione non farà nulla che non sia specificato chiaramente dagli sviluppatori.

A differenza delle applicazioni tradizionali, che funzionano sulla base di sistemi centralizzati e, i cui diritti sono nelle mani di un'autorità centrale, questa nuova generazione di applicazioni funziona in modo simile ad una blockchain. Tutti gli utenti sono parte attiva del sistema e, in quanto nodi pubblici, contribuiscono con le proprie risorse alla memorizzazione e alla crescita della blockchain. Questo garantisce non solo sicurezza e immutabilità dei protocolli che regolano il sistema, ma anche efficienza e continua automazione. La piattaforma sarà sempre in servizio poiché è impossibile rimuovere tutti i nodi dalla rete contemporaneamente. Inoltre, ogni volta che viene richiamato uno smart contract si genera un'immissione di dati nella blockchain. Questi dati vengono archiviati in modo crittografico e tutte le transazioni possono essere riviste pubblicamente nel blockchain explorer. Oltre a ciò, il fatto che una DApp funzioni su una blockchain significa che viene utilizzato un protocollo di consenso per verificare ogni interazione, così da garantire lo stesso livello di sicurezza e decentralizzazione di una blockchain [6].

Parte II

SEA Salute

Capitolo 4

L'obiettivo di SEA

SEA Soluzioni Eco Ambientali Srl è una Società a responsabilità limitata specializzata in igiene ambientale. Da anni fornisce una vasta gamma di servizi innovativi nell'ambito dell'ecologia urbana. Ciò che la contraddistingue è la costante ricerca di mezzi e tecnologie innovative, improntate sulla sostenibilità ambientale e al rispetto delle persone. La partnership con gli enti del territorio per la ricerca delle soluzioni più all'avanguardia ha portato a una collaborazione con il Politecnico di Torino. Infatti, anche il mondo aziendale ha percepito la potenza della tecnologia blockchain. Le aziende hanno oggi più chiara la necessità di digitalizzare i propri processi interni per fornire un'esperienza adeguata a clienti e dipendenti. In quest'ottica l'obiettivo di SEA non è solo quello di decentralizzare il loro servizio clienti ma fornire un servizio molto più attivo di gestione del personale. Questa scelta nasce dall'esigenza di tutelare i dipendenti a lungo termine, investendo nella loro salute e nel loro benessere psico-fisico. I collaboratori ecologici, per esempio, si occupano di igiene urbana e per questo sono costretti a uno stile di vita molto sedentario. Il fatto che il loro turno di lavoro si svolga interamente su un mezzo di trasporto ha un effetto a lungo termine su muscoli e articolazioni, esponendoli a fratture e contrazioni molto più frequentemente rispetto a chi adotta uno stile di vita attivo. L'obiettivo di SEA è quello di investire sulla loro salute, così da ridurre i giorni di malattia e le sostituzioni nel caso di infortuni. Più in generale, l'adozione di uno stile di vita sano fa parte dei valori che SEA vive e diffonde, sia all'interno del proprio gruppo che in ambito sociale, economico ed ambientale.

Il primo approccio a questo obiettivo è avvenuto nel 2019, con il Progetto promozione della salute in azienda Pyxis-SEA-Unito [10], in collaborazione con alcune studentesse e studenti della facoltà di Scienze della Nutrizione. Il programma forniva numerosi contenuti sull'importanza di un corretto stile di vita. Il materiale era organizzato in modo da offrire una panoramica generale e completa di tutto quello da sapere per migliorare lo stato di salute e le prestazioni lavorative: alimentazione, attività fisica, sonno, fumo. I dipendenti sono stati istruiti e indirizzati verso un corretto stile di vita attraverso delle pillole video. Ogni video si focalizzava su un profilo di salute su cui è utile agire, mettendo in evidenza errori più comuni, evidenze scientifiche ed effetti positivi di un intervento mirato. Tra i temi trattati il primo è stato "Sovrappeso e obesità". Un eccesso di peso, come in condizioni di sovrappeso e obesità, rappresenta un fattore di rischio importante per la salute: esso si

associa, infatti, a un aumentato rischio di sviluppo di malattie di tipo cardiovascolare e polmonare, nonché di diabete, ipertensione e di alcuni tumori. L'obesità è causata, nella maggior parte dei casi, da stili di vita scorretti, quali:

1. Un'alimentazione inadeguata, non bilanciata e ipercalorica.

2. Un ridotto dispendio energetico causato da scarsa attività fisica.

Questi sono stati la base di un percorso nutrizionale e fisico basato su piccole sfide quotidiane, come presentare un pasto completo e bilanciato o fare almeno un po' di esercizio ogni giorno. Inoltre, sono stati affrontati temi come la cura del sonno e il vizio del fumo, per responsabilizzare i partecipanti e renderli consapevoli dei rischi. Il programma ha riscosso un grande successo, i dipendenti si sono messi in gioco sfidando i propri colleghi al conseguimento di più obiettivi. In questo modo è stato possibile tenere traccia dei miglioramenti fatti e incentivare direttamente e attraverso un sistema di premiazione i partecipanti più attivi. Una volta terminato il progetto tuttavia è stato impossibile capire quali sono stati i frutti del lavoro svolto. Abbandonate le sfide quotidiane, i dipendenti non hanno avuto più alcun incentivo a mantenere uno stile di vita sano ed equilibrato, nonostante la grande spinta data dal progetto.

In quest'ottica l'utilizzo di un sistema decentralizzato come la blockchain può essere di grande aiuto e fornire un sistema di incentivi che rivoluzioni il modo di vivere il lavoro e lo sport. La grande sfida legata a questo progetto prevede un sistema che controlli i movimenti dei dipendenti, che diventano nodi di una blockchain e entrano a far parte di un sistema decentralizzato user-rewarding.

4.1 La Blockchain e il mondo del fitness

L'universo blockchain è entrato in contatto con il mondo dello sport amatoriale in risposta alla gestione dell'immensa quantità di dati sanitari erogati ogni giorno. Per dati sanitari non si intende solo informazioni sullo stato di salute di un utente ma dettagli sul suo stato fisico, raccolti da dispositivi indossabili e tracker di attività. Infatti, sempre più persone sono attente al proprio stile di vita e utilizzano la tecnologia per controllare i propri progressi. Basti pensare che il 52% degli utenti di smartphone acconsente alla raccolta di informazioni relative alla salute sul proprio telefono [4]. Tuttavia, quando un utente accetta di tenere traccia del proprio percorso di allenamento, acconsente contestualmente anche alla raccolta di informazioni sempre più dettagliate sul suo stato di salute: chilometri percorsi giornalmente, calorie bruciate, ore di sonno, frequenza cardiaca, informazioni sensibili che possono essere soggette a violazioni, vista la scarsa sicurezza di un dispositivo tracker. Questi dati vengono generati direttamente dai dispositivi in commercio e inseriti in un sistema centralizzato. Gli sviluppatori, quindi, di fatto li possiedono e monetizzano a partire da essi, vendendoli a multinazionali del mondo del sport senza il reale consenso dei consumatori.

La blockchain è in grado di risolvere il problema della sicurezza dei dati e della privacy in un modo che nessun'altra tecnologia può fare, rimettendo nelle mani dei consumatori il potere e i guadagni dei dati messi a disposizione della rete. La potenza di questo

strumento sta nella possibilità di poter costruire un ambiente tecnologico del tutto nuovo, decentralizzato, trasparente e controllato, in cui gli utenti sono un parte attiva del sistema. Quando un utente entra a far parte della blockchain viene ricompensato per il suo contribuito e possiede i dati che genera. Inoltre, molti sviluppatori di Blockchain hanno iniziato a riconoscere l'immensa opportunità che offre l'industria del fitness e hanno sviluppato diversi prodotti per il mercato, fin'ora dominato da grandi multinazionali come Fitbit, Apple e Polar Electro. Sull'orma di questi grandi progetti, è possibile creare un nuovo universo digital in cui gli utenti sono incentivati a mantenersi in forma e aiutati a proteggere i loro dati.

4.1.1 Lympo

Una delle maggiori applicazioni della blockchain in questo settore è rappresentata da Lympo, una startup blockchain costruita su Ethereum, che incentiva i propri utenti alla condivisione di dati sanitari e al mantenimento di uno stile di vita sano. Nasce inizialmente con l'obiettivo di collegare le persone ai migliori personal trainer, qualificandosi come una delle migliori 100 start up della tecnologia emergente in Europa, per poi entrare nell'universo blockchain all'inizio del 2018. L'obiettivo degli sviluppatori, un team di imprenditori nel settore dello sport, ingegneri informatici e consulenti esperti, era creare un ecosistema che mettesse in collegamento:

- Gli utenti che generano dati utilizzando dispositivi e applicazioni durante i loro allenamenti.
- Palestre, assicurazioni, medici, creatori di strumenti sportivi: soggetti che possono utilizzare i dati per migliorare le attrezzature, gli allenamenti, i programmi e i piani salute dei loro clienti.
- Aziende che analizzano dati, ovvero società di terze parti che sviluppano soluzioni sanitarie basate sui dati acquistati.

Lympo punta a diventare il punto di riferimento standard per tutte le parti interessate. Il suo successo non si basa sulla sola condivisione dei dati sanitari, ma sfrutta a pieno il boom del mercato della salute mobile (mHealth), che negli ultimi anni ha registrato un'enorme crescita. L'idea è quella di premiare gli utenti più attivi, coloro che utilizzano di norma queste applicazioni, ma che scelgono di entrare nell'universo blockchain con la consapevolezza di disporre del pieno controllo dei propri dati sanitari. Il meccanismo con cui un utente viene ricompensato per i dati messi a disposizione della piattaforma è al centro dell'ecosistema Lympo e si basa su dei token ERC20 Lympo (LYM) sulla blockchain Ethereum.
Nel whitepaper [4], il CEO di Lympo afferma: "L'obiettivo di Lympo è un token con un

valore reale a lungo termine, un caso d'uso reale che ispira le persone ad essere più sane e una adozione di massa indipendentemente dall'intera economia cripto. La nostra missione è far crescere Lympo verso una potente azienda e condurre una IPO (offerta pubblica iniziale) in futuro. In contrasto con le imprese tradizionali, vogliamo che la nostra comunità faccia parte di questo viaggio. Ed è per questo che il team ha preso la decisione di offrire un totale del 20% delle azioni Lympo ai nostri titolari di token". Infatti, gli utenti che detengono più di 10.000 LYM per la maggior parte del 2018 possono qualificarsi come azionisti della società e prendere parte al processo decisionale dell'azienda.
Come molte applicazioni blockchain, gli strumenti di cui si serve Lympo sono: i fitness wallet, il Marketplace creato per gli utenti della rete e una piattaforma di crowdfunding Lympo. Il portafoglio mobile di fitness Lympo è il cuore dell'ecosistema Lympo e funge da gateway per gli utenti a bordo. Permette di creare un profilo, compilare i dati sanitari e collegarsi agli sport preferiti e ai tracker sanitari dell'utente. Gli utenti ricevono ricompense in token LYM per condividere i propri dati. È l'unico veicolo di pagamento nell'ecosistema Lympo. L'app ha anche una funzione integrata che consente a istruttori e personal trainer di sfidare i clienti a raggiungere obiettivi individuali e ricevere token per i loro sforzi (Fig 4.1). Il marketplace Lympo elenca tutti i prodotti e servizi sulla piattaforma. Gli utenti possono spendere i propri token per trovare il miglior personal trainer, aggiungere funzionalità premium, acquistare alimenti sani, integratori e prodotti per la salute offerti dai partner Lympo. Infine, i token LYM possono essere utilizzati sulla piattaforma di crowdfunding Lympo per investire in aziende innovative del settore.
Nell'ecosistema Lympo tutti gli utenti hanno accesso ai dati generati sulla rete e al record delle transazioni precedenti. Tuttavia, i dati personali dell'utente non sono memorizzati nella blockchain stessa, ma sono mantenuti su server nella rete peer-to-peer. Ogni blocco della catena serve principalmente per il pagamento e lo scambio di dati. Tutti i dati on e off-chain sono protetti utilizzando protocolli crittografici e importati da diversi dispositivi IoT, come app di salute intelligenti, dispositivi indossabili e dispositivi elettronici di fitness, centri fitness e cartelle cliniche.

Figura 4.1. Sistema user-reward di Lympo, Lympo whitepaper [4]

Capitolo 5

La blockchain di SEA

Sull'orma di questi grandi progetti, l'obiettivo di SEA Salute è costruire una piattaforma decentralizzata user-rewarding, in cui gli utenti sono incentivati a condividere i propri dati sanitari e ricompensati per i loro sforzi attraverso un sistema di retribuzione in token.
La costruzione del sistema parte dalla scelta di una blockchain permissioned, i cui nodi della rete sono i dipendenti dell'azienda. La scelta di rendere privata la blockchain deriva dal rispetto della privacy di chi ne fa parte. Seppur i dati di ogni utente, infatti, siano crittografati, la blockchain si pone come un elenco di transizioni relative ai progressi fisici dei dipendenti, che vanno tutelati e rispettati. In questo modo, inoltre, il meccanismo di verifica di ogni blocco non viene affidato a dispendiosi protocolli di consenso. Nell'universo delle blockhain permissioned, infatti, si usa affidare il protocollo di validazione a una cerchia ristretta di utenti, in questo caso composta da un team interno al progetto, attraverso la proof of Autority. Questo algoritmo di consenso è basato sulla reputazione e sul valore dell'identità di un numero limitato e pre-selezionato di nodi validatori. Inoltre, non richiede una valuta nativa come il 'gas' di Ether ed è libero dal meccanismo di pagamento tipico dei protocolli di mining tradizionali. Questo consente alle imprese di mantenere la propria privacy e allo stesso tempo avvalersi dei vantaggi della tecnologia blockchain.

5.1 Fase di registrazione

Quando un dipendente entra a far parte del programma:

- Conferma le informazioni anagrafiche già presenti negli archivi SEA.
- Compila un test preventivo, con informazioni riguardo il suo stato di salute e di attività.
- Riceve i dati di un portafoglio digitale, dove collezionare i token aziendali.
- Riceve un dispositivo indossabile.

La fase di registrazione consiste principalmente nell'inserimento di alcuni dati sanitari di base e nel collegamento ufficiale ad un tracker di attività. A causa del trattamento dei

dati personali, non è possibile richiedere a un dipendente informazioni personali circa il suo stato di salute, come analisi del sangue o risultati di visite mediche. Il test preventivo si basa dunque su informazioni di base, oltre a quelle anagrafiche, come peso altezza, in modo da delineare gli obiettivi in modo generico e con il solo scopo di spronare l'utente al mantenimento di uno stile di vita sano. Una volta creato il profilo utente e il portafoglio digitale, ogni dipendente è in grado di monitorare da un'app mobile i propri progressi e tenere traccia degli obiettivi giornalieri raggiunti.

5.2 Sistemi IoT

Affinché il progetto funzioni a lungo termine, è necessario che i dati immessi nella blockchain siano quanto più veritieri possibili. L'oggettività dei dati in ingresso è un fattore da non sottovalutare, perché strettamente legata al meccanismo di retribuzione dei token e quindi al sistema interno della blockchain. Per il raccoglimento dei dati in ingresso sono necessari alcuni strumenti in grado di comunicare direttamente con la blockchain di SEA. Oggetti di questo tipo sono detti sistemi IoT (Internet of Things). L'IoT consente ai dispositivi su Internet di inviare dati a reti blockchain, con la fiducia e la sicurezza che caratterizza questa tecnologia. Per il progetto di SEA i dispositivi da integrare devono essere tali da avere un ingresso nella blockchain di dati veritieri e oggettivamente verificabili. Nonostante non manchino sul mercato applicazioni in grado di tenere traccia dell'allenamento fatto e della dieta seguita, il progetto non può permettere l'ingresso di queste informazioni, perché un utente potrebbe ingannare il sistema e approfittare degli incentivi aziendali. Per questa ragione, i dispositivi che devono comunicare con la blockchain devono prendere in ingresso informazioni direttamente dagli utenti e dai loro movimenti all'interno dell'azienda.

5.2.1 Dispositivi indossabili

I tracker di attività sono i principali strumenti da utilizzare, poiché fonte quotidiana di informazioni sul livello atletico degli utenti. Essi sono dotati di potenza ultra bassa, progettazioni molto compatte, materiali flessibili, impermeabilità e connettività affidabile. La distribuzione di questi strumenti all'intera rete blockchain permette un accesso regolare a due tipi di informazioni. Essi raccolgono sia informazioni circa lo stato di attività di un utente, come la distanza percorsa ogni giorno o le calorie bruciate, che alcune metriche per valutare lo stato di salute di chi li indossa.

Fitbit

Uno dei leader del settore è Fitbit [11], un'azienda che produce tracker di attività per fitness e benessere. Nel 2007, i suoi fondatori si resero conto che sensori e tecnologia wireless

avevano raggiunto un livello tale da poter offrire esperienze straordinarie nell'ambito del fitness e della salute. Così, decisero di creare un prodotto da indossare che avrebbe rivoluzionato il modo di concepire l'attività fisica. I loro prodotti sono progettati per adattarsi perfettamente alla vita di tutti i giorni e aiutare le persone a raggiungere qualsiasi obiettivo di salute e di fitness. Negli ultimi anni molte aziende hanno percepito la potenzialità di questa tecnologia e investito in un programma di benessere aziendale, con l'obiettivo di ridurre i costi sanitari e promuovere uno stile di vita sano. Fitbit si impegna da sempre a sostenere le aziende attraverso dei servizi personalizzati, aiutando i dipendenti a costruire abitudini sane attraverso l'attività fisica, il sonno, la gestione dello stress e l'alimentazione. Il servizio prende il nome di Fitbit Care e offre un'ampia selezione di tracker di attività e smartwatch da spedire direttamente ai dipendenti. Il monitoraggio dell'attività, del sonno e della frequenza cardiaca con i dispositivi Fitbit offre opportunità quotidiane di autoapprendimento e può portare a un cambiamento comportamentale positivo. Inoltre, il nuovo smarthwatch per la salute include un monitoraggio avanzato della salute, come la rilevazione della gestione dello stress, la salute del cuore, della temperatura cutanea e altro. Integrando un'esperienza sanitaria personalizzata, si aumenta il coinvolgimento dell'utente. Con Fitbit Care si ottiene un team dedicato al Customer Success, ovvero un programma personalizzato in grado di coinvolgere i dipendenti indipendentemente da dove si trovino e fornire loro valutazioni in tempo reale.

5.2.2 Dispositivi di vending

Durante il programma proposto dall'Università di Torino, tra i temi trattati, ha riscosso molto successo l'educazione alimentare. I dipendenti sono stati istruiti e indirizzati verso l'adozione di una dieta mediterranea e l'utilizzo di alimenti sani. Il progetto prevedeva alcune sfide e premiava chi riusciva a dimostrare impegno e determinazione nell'adozione di una corretta alimentazione. In un sistema blockchain la verifica di questo aspetto risulta molto complicata e rimessa a soli fattori umani. La mancanza di queste informazioni priverebbe il programma di un elemento fondamentale alla determinazione del benessere psico-fisico di un utente. Un'idea per incentivare uno stile di vita sano anche dal punto di vista alimentare è dotare alcuni cantieri SEA di distributori automatici personalizzati, con all'interno alcuni snack e cibi sani. Oltre ad elargire un servizio in più ai dipendenti, fornendo una valida alternativa ai classici snack, l'introduzione di questi dispositivi può diventare una parte attiva del meccanismo di user-rewarding, fornendo al sistema alcune informazioni circa le abitudini alimentari degli utenti. Questo processo può essere implementato attraverso diverse soluzioni, più o meno tecnologicamente avanzate.

Pagamenti Posless

POSLESS®

Una prima forma di comunicazione tra i distributori e la blockchain può essere data da un sistema di pagamento completamente digitalizzato. Permettendo ai dipendenti di pagare

attraverso i token ricevuti, è possibile scrivere una nuova tipologia di transazione all'interno della blockchain e acquisire nuove informazioni circa le abitudini alimentari degli utenti. Tra le aziende che si occupano di pagamenti Contactless, Qsave Elkey e Argentea hanno realizzato una rivoluzionaria soluzione per il mercato vending. In [7] viene presentato nel dettaglio questo meccanismo. "Grazie a un QR Code sarà possibile pagare tramite gli alternative payment in ogni distributore automatico. Il sistema in Fig. 5.2.2 , detto Bubble PosLess, si basa sullo standard PCI CPOD "Conctaless Payments on Commercial Of-The-Shelf, recentemente rilasciato dall'EBA (European Banking Authority) e consente di abilitare qualsiasi distributore automatico nell'accettazione di ogni tipo di pagamento effettuato con digital wallet. AMoney è un sistema multi-banca che permette di integrare tutti i provider di "alternative payments", come le criptomonete e di controllare in tempo reale le operazioni e le statistiche sui flussi in entrata attraverso un portale dedicato." In questo modo, ogni dipendente avrà un canale diretto con i distributori dell'azienda, e con transazioni immediate potrà usufruire di tutti i prodotti al loro interno.

Distributori Automatici Intelligenti

Un'alternativa del tutto digitalizzata al solo pagamento in criptomoneta è data dai distributori automatici intelligenti. In un progetto blockchain come quello di SEA, che punta a coinvolgere i dipendenti in tutte le fasi di raccolta dati, l'utilizzo di un distributore intelligente rivoluzionerebbe il meccanismo user-rewarding.
Negli ultimi anni la Intel [8] sta sviluppando dei distributori automatici basati su una tecnologia del tutto nuova, a vantaggio sia dell'azienda che dei clienti. L'esperienza utente comprende alta definizione, programmazione da remoto e un sistema di pagamento digitalizzato, che permette il pagamento in criptomoneta. Ma oltre ai consumatori, anche i

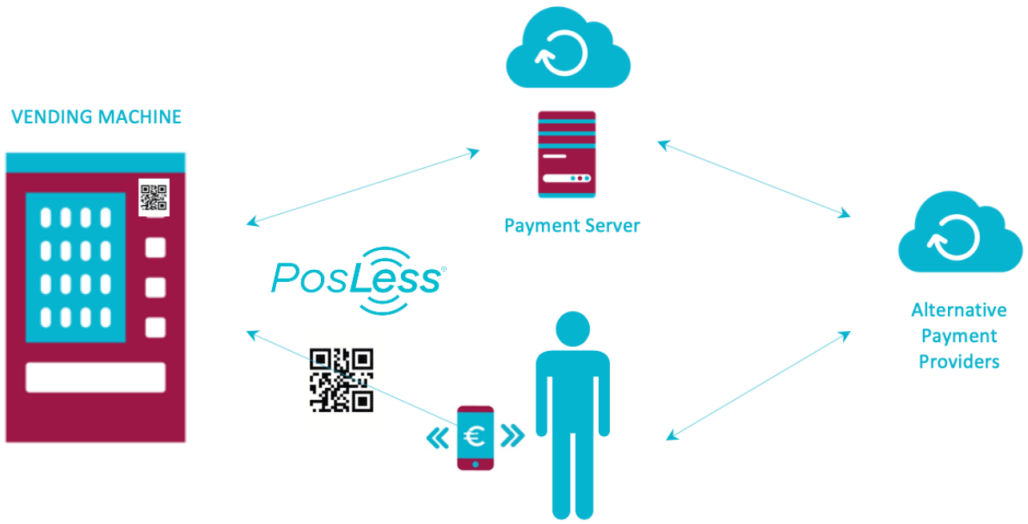


Figura 5.1. Sistema di Pagamento Posless, Sito ufficiale Elkey [7]

fornitori si troverebbero in una posizione favorevole, poiché in grado di comunicare con i clienti. Il sistema potrebbe essere in grado di inviare coupon direttamente dall'app mobile per incoraggiare i clienti all'acquisto di determinati prodotti e influenzarli con sconti e promozioni. Un sistema di questo tipo prevede, tuttavia, un investimento senza precedenti per il walfare aziendale. La soluzione certamente più realizzabile resta la prima, ovvero l'introduzione del pagamento Posless, così da non dover acquistare nuovi distributori ma semplicemente modificare quelli già presenti nei cantieri.

5.3 Dati in ingresso

Le informazioni raccolte dai dispositivi IoT costituiscono i principali dati in ingresso della blockchain e servono per delineare i profili aziendali. Quando un utente accede alla sua pagina personale dispone di una panoramica di come il sistema valuta il suo stato di salute, degli obiettivi raggiunti e delle transazioni fatte. Lo stato di salute viene valutato sulla base del benessere psico-fisico, senza sottovalutare fattori di rischio come stress e stanchezza. I dati in ingresso si dividono quindi in tre categorie:

1. Informazioni sull'attività dell'utente: la distanza percorsa in un giorno, i passi e le calorie bruciate, dati oggettivi e facili da verificare, sulla base dei quali assegnare i principali token aziendali.

2. Informazioni circa la salute dell'utente: frequenza cardiaca, variabilità del battito cardiaco, temperatura cutanea, livello di ossigeno nel sangue e battito cardiaco a riposo. Queste metriche si possono raccogliere direttamente dai braccialetti Fitbit, quindi non costringono i dipendenti a sottoporsi ad analisi o l'azienda ad invadere in qualche modo la loro privacy. A partire da questi valori si può calcolare un punteggio giornaliero di gestione dello stress, che dipende dal battito cardiaco, dalla quantità di esercizio fisico svolto e dalla qualità del sonno, rilevata sempre da questi dispositivi. Anche in questo caso, un punteggio positivo può portare all'assegnazione di un token.

3. Informazioni sull'alimentazione, sulla base dei token spesi per l'acquisto di cibi sani.

5.3.1 Informazioni sullo stato di attività

Una volta ricevuto e configurato il tracker di attività, ogni dipendente diventa ufficialmente un nodo della rete blockchain. Attraverso il tracciamento dei suoi movimenti fornisce al sistema i principali dati in ingresso della blockchain. Ogni dispositivo indossabile rileva di base gli stessi parametri:

1. Numero di passi

2. Distanza percorsa

3. Piani

4. Minuti di allenamento

5. Calorie bruciate

Questi valori sono consultabili sia dal dispositivo che da un'applicazione mobile, scaricabile da smartphone. L'interfaccia utente in Fig. 5.2 propone alcune informazioni circa lo stato di attività di chi indossa il dispositivo, con la possibilità di avere una panoramica sui progressi fatti ogni giorno e nel corso del tempo. Sulla base di queste informazioni, viene stabilito l'impegno di ogni utente e la sua attitudine all'attività fisica. Le informazioni ottenute sono la principale fonte di dati della blockchain, a partire dai quali vengono assegnati i principali token aziendali.
Alcuni dispositivi hanno anche la possibilità di rilevare:

- Il battito cardiaco;
- Le ore di sonno.

La frequenza cardiaca è particolarmente importante perché permette di valutare la salute del cuore. La rilevazione in tempo reale permette di capire i momenti di cardio e il livello di sforzo fatto durante gli allenamenti [11].

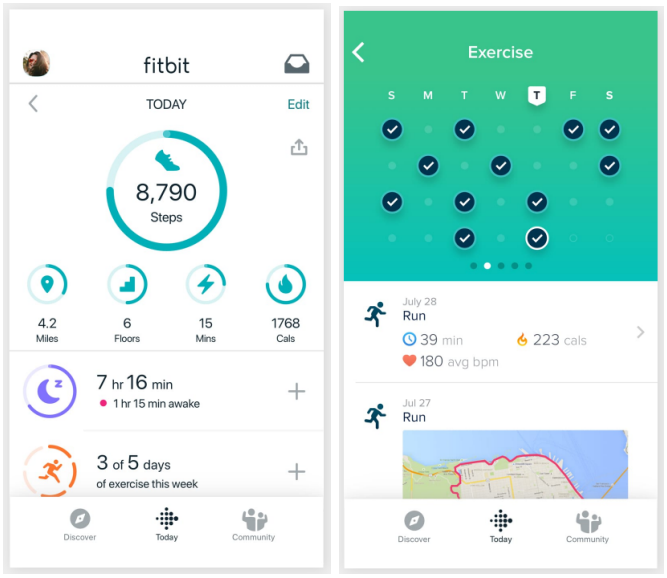


Figura 5.2. Stato di attività, Sito ufficiale Fitbit [11]

5.3.2 Informazioni sullo stato di salute

Con l'obiettivo di non spingere gli utenti del sistema oltre i loro limiti fisici, il sistema prevede anche la raccolta di informazioni mediche o sanitarie. Alcuni dispositivi, infatti, sono dotati di sensori in grado di calcolare i dati sanitari di chi lo indossa. Questi indicatori non sono destinati alla diagnosi o al trattamento di condizioni mediche e non devono essere utilizzate per finalità mediche. Sono piuttosto destinati a fornire informazioni che

possono aiutare a gestire il benessere dell'utente [11]. In base ai risultati ottenuti, inoltre, è possibile calcolare un intervallo personale, che si basa sulla media dei dati recenti, attraverso il quale analizzare le tendenze dei dati. Le metriche rilevate sono:

1. Frequenza respiratoria, ovvero il numero di respiri al minuto. Il corpo regola la frequenza respiratoria per ricevere una quantità di ossigeno sufficiente. Solitamente, la frequenza respiratoria è 12-20 respiri al minuto. I fattori che possono influenzare la frequenza respiratoria sono età, sesso, peso, condizioni di polmoni e cuore, ansia e febbre.

2. Variabilità del battito cardiaco (HRV). Essa varia da persona a persona e in base a età, sesso, sonno, ormoni, ritmo circadiano e altri fattori (ad esempio, caffeina o alcol, allenamento e stress). Gli studi dimostrano che una variabilità della frequenza cardiaca più alta è indice di una salute migliore. Un calo significato della variabilità della frequenza cardiaca potrebbe essere un segnale di stress, affaticamento o possibile malattia.

3. Temperatura cutanea, rilevata dal polso durante le ore di sonno. La temperatura cutanea è la temperatura sulla superficie della pelle. È normale che si verifichino variazioni della temperatura cutanea durante il sonno e da notte a notte. In generale, una variazione di questo fattore può simboleggiare l'insorgenza di febbre, anche se può essere determinata anche da fattori esterni, come cambiamenti significativi della temperatura ambiente.

4. Saturazione ossigeno (SpO2), che stima la quantità di ossigeno nel sangue. Di notte, il valore di SpO2 è più basso rispetto al giorno, perché la frequenza respiratoria è solitamente più lenta. Una corretta saturazione prevede dei livelli di ossigeno nel sangue costanti, sia durante l'allenamento che durante le ore di sonno.

5. Battito cardiaco a riposo (RHR). Il battito cardiaco a riposo solitamente va da 60 a 100 b/m, ma questo intervallo può variare in base a età e livello di allenamento. Può essere un indicatore importante del livello di allenamento e della salute cardiovascolare in generale. Di solito, le persone attive hanno un battito cardiaco a riposo più basso. Diversi fattori lo influenzano: stress, alcol o caffeina oppure febbre solitamente aumentano il battito cardiaco a riposo, mentre allenamento o meditazione lo abbassano.

5.3.3 Informazioni sulle abitudini alimentari

Per avere un quadro completo sullo stato di salute di un utente, l'ultimo elemento da analizzare riguarda la sua alimentazione. Come accennato, è impossibile tenere sotto controllo le abitudini alimentari di un utente. Di conseguenza, l'unico modo per ottenere informazioni concrete è attraverso l'utilizzo, in due contesti specifici, dei token aziendali.

- Con l'introduzione di distributori automatici personalizzati all'interno dei cantieri di SEA.

- Con l'organizzazione di eventi interni all'azienda, come dei mercati solidali, che promuovono la vendita di frutta e verdura a chilometro zero.

Con queste iniziative si spera di indirizzare sempre di più le scelte alimentari dei dipendenti. In entrambi i casi il sistema offre all'utente la possibilità di spendere i propri token e, allo stesso tempo, utilizza le informazioni in suo possesso, come gli acquisti settimanali, per ricompensare i clienti più fedeli, così da premiare i più entusiasti e incoraggiare gli altri.

Poiché i prodotti venduti arrivano da fornitori esterni, dovranno essere stipulati degli accordi tra SEA e le aziende. Quando un fornitore decide di partecipare al mercato, per esempio, raccoglie i token aziendali ottenuti dalle vendite su un portafoglio digitale e successivamente li riscatta con SEA attraverso dei servizi o degli sconti sull'igiene urbana.

Capitolo 6

Soluzioni user-rewarding

Il meccanismo di ricompensa della blockchain di SEA è il cuore del progetto e la vera novità che l'azienda vuole introdurre. Ogni giorno vengono immesse nuove informazioni all'interno della blockchain, per delineare il profilo di ogni utente. Queste informazioni vengono processate dal sistema, viene verificato il livello di attività, lo stato di salute e sulla base di obiettivi specifici l'utente viene o meno ricompensato. Il meccanismo retributivo si basa sull'utilizzo di appositi smart contract, che trasferiscono nel portafoglio digitale dell'utente degli asset digitali, i token aziendali. Questi vengono distribuiti ogni volta che un utente dimostra al sistema uno stato di salute positivo. Per creare il coinvolgimento necessario alla durata del progetto, gli obiettivi da raggiungere vengono posti come sfide da superare, così da creare tra la community SEA una sana competizione e un senso di connessione.

Esempio: Viene fissato un obiettivo comune a tutti i dipendenti, come una distanza minima da percorrere o un quantitativo di calorie da bruciare. Vengono quindi lanciate delle challenge, alla quale i dipendenti scelgono o meno di partecipare. Chi supera la sfida, inserendo nella blockchain i risultati ottenuti, viene ricompensato con token aziendali, inseriti nei portafogli digitali direttamente dalla piattaforma. La procedura è formata dai seguenti passi:

1. L'azienda lancia la sfida ai dipendenti;
2. L'utente sceglie di partecipare;
3. Viene registrato uno smart contract;
4. L'utente completa la sfida e invia i dati di tracciamento del dispositivo usato;
5. I token stabiliti dal contratto vengono spostati nel wallet dell'utente.

I token distribuiti sono gli elementi chiave di questo sistema, perché permettono alla community di ottenere dei premi concreti e allo stesso tempo universali, da utilizzare i modi diversi ma con lo stesso valore di base. Sono la principale forma di remunerazione della

blockchain e per questo vengono utilizzati come incentivo per la community di dipendenti di SEA. Vengono distribuiti all'interno del circuito attraverso degli standard noti.

Gli smart contract utilizzati nel meccanismo di remunerazione prevedono esclusivamente la distribuzione dei token SEA, di conseguenza lo standard più opportuno è il noto ERC-20. Il contratto viene stipulato dalla blockchain per i singoli utenti. Ogni volta che un utente accetta una sfida e si impone di raggiungere un determinato obiettivo, verrà chiamato lo smart contract predefinito. Il quantitativo di token in gioco verrà bloccato per tutta la durata della prova e, dopo che l'utente avrà raggiunto gli obiettivi specificati nel contratto, i token concordati verranno trasferiti nel portafoglio digitale di chi ha completato la sfida. Contestualmente al contratto relativo alla remunerazione, il servizio blockchain deve fornire anche un'autorizzazione degli utenti all'utilizzo dei propri dati personali con timestamp. Solamente in questo modo si possono garantire gli standard stabiliti dal Regolamento generale sulla protezione dei dati nell'Unione Europea (GDPR) [5].

Le sfide che ogni dipendente deve affrontare si dividono in base al tipo di dati in ingresso che l'utente sceglie di condividere

6.0.1 Obiettivi legati allo stato di attività

Le informazioni più importanti raccolte dal sistema riguardano lo stato di attività, a partire dalle quali nascono le sfide più impegnative per gli utenti della rete. Il progetto promosso dall'università di Torino raccomandava ai dipendenti 150 minuti di esercizio fisico a intensità moderata a settimana, o 75 minuti a intensità vigorosa e due sessioni di allenamento per il rafforzamento muscolare [10]. A partire da queste premesse viene costruita la challenge aziendale. Per incentivare chiunque scelga di partecipare, vengono creati tre sotto-obiettivi.

1. Svolgere 50 minuti di esercizio fisico a intensità moderata, o 15 minuti a intensità vigorosa

2. Svolgere 100 minuti di esercizio fisico a intensità moderata, o 30 minuti a intensità vigorosa

3. Svolgere 150 minuti di esercizio fisico a intensità moderata, o 75 minuti a intensità vigorosa

Quando un utente sceglie di partecipare autorizza il suo dispositivo indossabile a monitorare i suoi spostamenti e, al termine della settimana, ottiene una quantità di token proporzionale all'obiettivo raggiunto.

Può essere parte dell'attività fisica qualsiasi attività sportiva, ma anche semplici movimenti quotidiani come camminare, andare in bicicletta o ballare. Questo permette agli utenti di confrontarsi con i mezzi che hanno a disposizione, e dimostrare partecipazione al sistema nel modo che preferiscono. Inoltre, l'utilizzo dei dispositivi indossabili crea una competizione flessibile che può essere vissuta anche a distanza, fornendo ai nodi della rete un sistema di sfide da remoto.

6.0.2 Obiettivi legati allo stato di salute

I dispositivi indossabili sono in grado di rivelare, attraverso dei sensori specifici, alcune metriche sanitarie: frequenza respiratoria, variabilità del battito cardiaco, temperatura cutanea, saturazione ossigeno e battito cardiaco a riposo. Questi dati servono a dare una panoramica del livello di salute di un utente, per non sottovalutare fattori importanti come stress e stanchezza. A partire da questi valori alcuni dispositivi permettono di calcolare un punteggio giornaliero di gestione dello stress (Fig. 6.1), un modo analitico per valutare dei valori troppo generici da utilizzare per assegnare i token aziendali. Esso dipende dal battito cardiaco, dalla quantità di esercizio fisico svolto e dalla qualità del sonno, rilevata sempre da questi dispositivi. Il punteggio di gestione dello stress è basato su un sensore multi-percorso. Rileva, attraverso i dispositivi indossabili, piccoli cambiamenti elettrici chiamati risposte di attività elettrodermica sulla pelle (EDA) [11]. Il punteggio viene assegnato in base a tre elementi:

- La reattività: dati sulla frequenza cardiaca e sull'attività elettrodermica.
- L'equilibrio: un punteggio che deriva dall'importanza di trovare la giusta dose di attività fisica. Uno stile di vita sedentario può far aumentare i livelli di ormoni dello stress ma troppa attività può portare a stanchezza e stress fisico.
- Una regolare cura del sonno: dati sul riposo dell'utente.

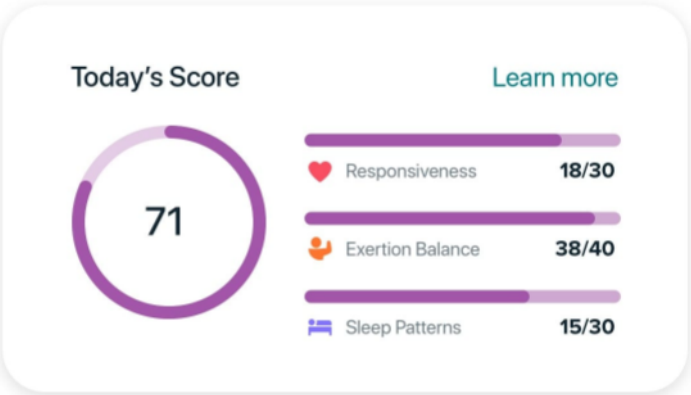


Figura 6.1. Punteggio giornaliero di gestione dello stress, Sito ufficiale Fitbit [11]

Nel meccanismo user-rewarding, ogni dipende partecipa indirettamente anche al raggiungimento di un stato di salute positivo. Quando un utente sceglie di condividere i dati rilevati dal suo tracker di attività, autorizza il sistema a prendere in ingresso queste informazioni ed elaborare un punteggio di gestione dello stress. Per superare questa sfida basta ottenere un punteggio superiore a un valore di soglia, così da dimostrare al sistema di essere in forma e ottenere così i token aziendali.

6.0.3 Obiettivi legati all'alimentazione

Questo tipo di challenge è legata al livello di utilizzo dei distributori automatici e alla partecipazione agli eventi aziendali. Fissare questi obiettivi serve per indirizzare le scelte alimentari degli utenti, incoraggiandoli a mangiare meglio in qualsiasi contesto.

A partire dai dati relativi alle vendite è possibile capire quali sono gli utenti più sensibili a un'alimentazione sana. La challenge legata a questo tipo di informazioni è strutturata come le precedenti, dura una settimana lavorativa e prevede la remunerazione in token per gli obiettivi raggiunti. Per ogni utente, il sistema conta il numero di acquisti nei distributori automatici e durante gli eventi aziendali e premia chi supera un valore di soglia. L'ottenimento di token rappresenta un rimborso parziale della spesa fatta e, dunque, un vero e proprio incentivo.

Quando verranno creati i token SEA, allora, con un'allocazione interna alcuni dovrebbero essere già distribuiti nei wallet degli utenti, così da promuovere da subito questo meccanismo.

6.1 I token SEA

Il sistema di remunerazione prevede il trasferimento di specifici asset digitali, i token aziendali SEA. Essi vengono erogati sotto forma di utility token, ovvero token con un valore specifico, che non portano a un guadagno diretto di chi li possiede ma vengono utilizzati esclusivamente come forma di pagamento. Per stimare la Total Hard Cap, ovvero la quantità massima di token da immettere nel sistema, bisogna considerare i tre scenari in cui i verranno distribuiti questi asset digitali.

1. Durante la fase iniziale di allocazione. Infatti, per raccogliere da subito informazioni circa le abitudini alimentari degli utenti, il progetto prevede un'allocazione interna. Quando un utente si registra nella blockchain il sistema trasferisce da subito una piccola quantità di token nel suo portafoglio digitale.

2. Al completamento di una challenge aziendale, basata sugli obiettivi del progetto SEA Salute.

3. In caso di acquisto, dai distributori automatici, durante gli eventi aziendali oppure dalla piattaforma online, il Marketplace SEA.

6.2 Il Marketplace

Il Marketplace è una piattaforma interna alla blockchain di SEA che permette di spendere i token aziendali collezionati dai dipendenti. Grazie a questo shop virtuale, infatti, gli utenti del sistema vengono spronati a raggiungere gli obiettivi fissati dal sistema e guadagnare con un meccanismo simile a una raccolta punti. Una volta raccolti, i token possono essere spesi direttamente dagli utenti all'interno dell'azienda attraverso i distributori automatici e gli eventi aziendali, oppure possono essere convertiti all'interno del Marketplace in:

1. Coupon e promozioni presso strutture convenzionate

2. Permessi e ore libere
3. Assicurazioni mediche e agevolazioni sanitarie
4. Sconti per eventi culturali

Poiché il progetto si basa sul benessere aziendale, tra i servizi offerti non mancheranno lezioni singole con personal trainer, abbonamenti in palestra e sconti presso i negozi di alimentari locali. Con lo stesso meccanismo i dipendenti potranno ottenere qualsiasi tipo di sconto, ingressi ridotti a cinema e musei, promozioni presso librerie locali e negozi convenzionati, e maggiori garanzie sanitarie. L'azienda o l'ente che accetta di fornire delle promozioni ai dipendenti, dovrà stipulare degli accordi interni con SEA, e attraverso convezioni e sconti sui servizi, riscattare il debito accumulato. Qualunque impresa locale può entrare a far parte della piattaforma e sponsorizzare i propri servizi ai dipendenti SEA, sia per risparmiare sull'igiene urbana, che per ottenere e fidelizzare nuovi clienti. Il ruolo di queste imprese in futuro potrebbe essere integrato all'interno della blockchain, permettendo loro di collezionare i token ottenuti in un portafoglio digitale e quindi di entrare a far parte del sistema user-rewarding.

Un'alternativa allo shopping online potrebbe essere convertire i token ottenuti in ore libere, così da premiare i dipendenti con del tempo per se stessi. In questo modo, gli utenti del sistema saranno incoraggiati a fare di più e mettersi sempre più in gioco nelle challenge aziendali.

Il marketplace dovrà offrire una panoramica di tutte queste opzioni, suggerendo quelle preferite dalla rete e personalizzando l'esperienza in base alle abitudini dell'utente. Quello che rende il progetto una vera novità nel mondo aziendale è l'approccio rivoluzionario dato da questa piattaforma. Infatti, non si configura semplicemente come uno shop online, ma come un terreno di esplorazione e comunicazione tra gli utenti del sistema. La blockchain rende la rete totalmente decentralizzata, gestita dai soli utenti, che hanno il pieno controllo dei loro dati. Sono quindi padroni anche della piattaforma di acquisto, attraverso dei sistemi di valutazione condivisibili e interattivi.

Riferimenti Bibliografici

[1] Adam Black. "Hashcash - a denial of service counter-measure". In: (2002). URL: http://www.hashcash.org/hashcash.pdf.

[2] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". In: (2008). URL: https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf.

[3] Vitalik Buterin. "Ethereum Whitepaper: A Next Generation Smart Contract & Decentralized Application Platform". In: (2013). URL: https://ethereum.org/it/whitepaper/.

[4] Tadas Maurukas Ada Jonuse Marius Silenskis. "Lympo Whitepaper". In: (2018). URL: https://whitepaper.io/document/111/lympo-whitepaper.

[5] Sito ufficiale della Commissione Europea. *The General Data Protection Regulation (GDPR)*. URL: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_it.

[6] The Cryptonomist. *DApp: cosa sono e come funzionano le applicazioni decentralizzate*. Sito visitato a Dicembre 2021.

[7] Elkey. *Il pagamento Posless*. URL: http://www.elkey.com/pagamenti-senza-pos/.

[8] Intel. *Intelligent Vending*. URL: https://www.intel.com/content/www/us/en/retail/retail-vending.html.

[9] NIST. NIST selects winner of secure hash algorithm (SHA-3) competition. URL: https://www.nist.gov/news-events/news/2012/10/nist-selects-winner-secure-hash-algorithm-sha-3-competition.

[10] SEA Salute. Sito visitato a Ottobre 2021. URL: https://www.seaeco.it/sea-salute.

[11] Fitbit: Prodotti e Tecnologia. Sito visitato a Dicembre 2021.