UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

Blockchain for good

Relatore:

prof. Di Nunzio Giorgio Maria

Laureando:

Zago Giovanni

1226024

Correlatore:

dott. Fabio Pallaro

ANNO ACCADEMICO: 2021/2022

Data di laurea: 19 Settembre 2022

Indice

Introduzione

Il presente elaborato riassume il percorso svolto nel tirocinio presso la sede di Padova di Sync Lab srl, da Giugno ad Agosto 2022.

L'azienda

Logo azienda SyncLab srl

> Sync Lab è una Innovative Company attenta ai paradigmi della trasformazione digitale che realizza prodotti e soluzioni per diversi mercati quali: sanità, industria, energia, telco, finanza e trasporti & logistica.
> L'offerta di consulenza specialistica, sintesi di circa 20 anni nel settore IT, e la forte competenza in diversi domini tecnologici, aiutano il cliente a dominare i nuovi trend e le sfide che ne derivano, quali: GDPR, Big Data, Cloud Computing, IoT, Mobile e Cyber Security.
> In questo scenario Sync Lab si posiziona come uno dei più importanti system integrator nel panorama italiano delle aziende ICT[1].

L'azienda è stata fondata nel 2002 a Napoli come *software house*, ma presto si sposta nell'ambito *Information and Comunication Technology* (ICT). Oggi conta 6 sedi in tutta Italia, oltre 300 dipendenti e più di 150 clienti, tra diretti e finali, tra cui importanti aziende come UniCredit, Intesa San Paolo, H&M, Sky, Fastweb, Vodafone.

[1] https://www.synclab.it/about.php

Il progetto

Il progetto nasce come proposta per contrastare il problema della speculazione nel campo della carità. Spesso abbiamo letto o sentito parlare di associazioni *no-profit* che non hanno ricevuto il denaro dato loro in beneficenza perchè, nel percorso dalle tasche del donatore alle casse dell'associazione, qualcuno ha trattenuto per sé una parte del ricavato. La domanda che dà origine al progetto è quindi: **non è possibile, con le moderne tecnologie, evitare i passaggi di mano, dove qualcuno potrebbe trattenere per sé soldi destinati ad associazioni che operano a favore di persone che vivono diverse situazioni di disagio?**

Sempre più persone preferiscono donare in modo digitale: le donazioni su Facebook o su Instagram, l'IBAN per i bonifici o le proposte di donazione di PayPal sono solo degli esempi di nuove modalità per aiutare chi ha bisogno. Anche molti *influencer* vivono grazie alle donazioni spontanee dei loro *follower*, utilizzando piattaforme come Patreon, che garantiscono una donazione periodica ed automatica.

Una delle tecnologie che ha visto un notevole sviluppo e crescente interesse negli ultimi anni è la **blockchain**. Il suo utilizzo più noto al grande pubblico è quello delle cryptovalute (chiunque al giorno d'oggi ha sentito parlare almeno dei Bitcoin), ma questa è solo una delle infinite applicazioni possibili di questa rivoluzione.

Nel corso del progetto si è voluto provare ad utilizzare la blockchain per uno scopo diverso e meno noto: la **beneficenza**. L'intenzione è quella di eliminare il fattore umano -facilmente soggetto ad errori più o meno colposi- nel viaggio del denaro dal donatore al ricevente. Le transazioni su blockchain sono infatti criptate e tracciabili: si può quindi mantenere l'anonimato del donatore senza rinunciare alla tracciabilità della donazione. Come vedremo meglio più avanti, ogni transazione è scolpita in un blocco e la rete di blocchi garantisce la non modificabilità della storia delle transazioni.

Il personale interesse per il progetto scaturisce dall'interrogarmi sugli utilizzi che facciamo di ogni strumento, più o meno informatico che sia . La tecnologia avanza e troppo spesso la si vede andare solo nel verso della produzione, della monetizzazione. Si potrebbe quasi arrivare a credere che il progresso tecnologico lasci indietro chi ha meno possibilità educative ed economiche. Questo progetto ha l'intenzione di portare la modernità a ser-

vizio di chi ha più bisogno. Grazie alla decentralizzazione non solo si possono eliminare gli intoppi classici del denaro che passa tra troppe mani, ma si può rendere più veloce e trasparente la beneficenza, conferendole una maggior garanzia di eticità.

Grazie al confronto con l'azienda ospitante, infine, sono arrivato alla realizzazione vera e propria dello **Smart Contract**. Il team aziendale mi ha accompagnato a conoscere meglio il mondo delle blockchain e grazie all'esperienza di tirocinio ho potuto verificare che, volendo, il nuovo che avanza può aiutare anche l'inclusione e non solo la capitalizzazione.

Aspetti etici

Ho voluto inserire in questo elaborato anche una parte che muova dei timidi passi sull'analisi etica della blockchain, concentrandomi in particolare sui casi d'uso considerabili eticamente "corretti". L'intenzione di usare questo strumento come sigillo di garanzia etico non è infatti originale, ma già esiste in diversi settori: dalle miniere di cobalto della Repubblica Democratica del Congo alla *sharing economy*.

Lo studio (lontano dall'essere esaustivo) considera alcuni aspetti particolarmente interessanti per un uso etico della blockchain: la tracciabilità e la decentralizzazione. Questi sono stati analizzati partendo da criteri classici dell'etica finanziaria e sociale, ponendo al centro di tutto la persona umana e il denaro come mezzo, non come fine. Molti altri aspetti sarebbero di altrettanto interesse: il consumo energetico, l'open source, gli hackeraggi, solo per fare alcuni esempi. Tuttavia si è deciso di soffermarsi solo sui due aspetti prima esposti perché quelli più vicini all'intenzione del progetto.

Il criterio base della riflessione è qui riassunto:

> Lo smarrimento dell'orizzonte metafisico; la perdita della nostalgia di Dio nel narcisismo autoreferenziale e nella dovizia di mezzi di uno stile di vita consumistico; il primato assegnato alla tecnologia e alla ricerca scientifica fine a se stessa; l'enfatizzazione dell'apparire, della ricerca dell'immagine, delle tecniche di comunicazione: tutti questi fenomeni devono essere compresi nei loro aspetti culturali e messi in rapporto con il tema centrale della persona umana, della sua crescita integrale, della sua capacità di comunicazione e di relazione con gli altri uomini, del suo continuo interrogarsi sulle grandi questioni che attraversano l'esistenza[2].

Ciò che muove la riflessione è quindi un esplicito principio antropocentrico, dove i mezzi sono intesi al servizio dell'uomo e non viceversa. Tutto ciò che *schiavizza* l'uomo e

[2]Pontificio Consiglio della giustizia e della pace. *Compendio della dottrina sociale della Chiesa*. Libreria Editrice Vaticana, 2005, n 554.

ne diventa dominatore non è, di conseguenza, eticamente corretto, ma piuttosto qualcosa che svia dal corretto utilizzo degli strumenti che noi stessi creiamo.

Capitolo 1

Nozioni di base

1.1 Blockchain

1.1.1 L'origine: i Bitcoin

Il 1 Novembre 2008 viene pubblicato il primo *white paper* di Satoshi Nakamoto, lo pseudonimo usato dell'inventore (o dagli inventori) della tecnologia Bitcoin: *Bitcoin: A Peer-to-Peer Electronic Cash System*[3]. Nel *paper* l'anonimo autore presenta la sua idea: una moneta elettronica che non abbisogna dell'approvazione centralizzata e a prova di *double-spending*[4], i Bitcoin.

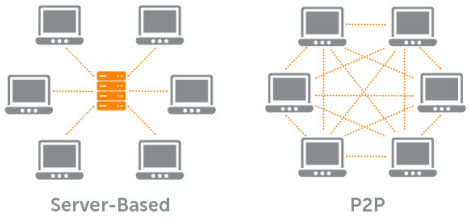

Figura 1.1: Visualizzazione grafica di una rete client-server e di una rete peer-to-peer
Fonte: http://john-ee.com

Il concetto base è quello di costruire una tecnologia capace di registrare tutte le transazioni in modo immodificabile, decentralizzato e sicuro. La tecnologia *peer-to-peer* si presta a quest'idea, essendo costitutivamente democratica e non gerarchica. Nella tecno-

[3]Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 1 Nov. 2008. URL: `https://bitcoin.org/bitcoin.pdf` (visitato il 07/2022).

[4]Col termine *double-spending* si identifica una truffa che consiste nello spendere due o più volte lo stesso titolo valutario. Storicamente gli istituti finanziari si sono occupati di fermare questa truffa, ma Satoshi Nakamoto propone una tecnologia che la impedisca in modo automatico.

logia client-server infatti c'è un sistema (il server) sempre attivo in attesa di richieste da soddisfare; una sorta di saggio del monte al quale porre le proprie domande. Il client non deve fare altro che scalare il monte (fuor di metafora, inviare la richiesta) ed attendere la risposta del server/saggio. La tecnologia peer-to-peer, al contrario, è più simile ad un villaggio dove ognuno possiede alcune informazioni: tutti sanno qualcosa e nessuno possiede la conoscenza totale. Dentro a questo secondo paradigma nasce la blockchain.

Ogni nuova transazione viene proposta da un singolo utente, chiamato nodo A, a tutti i nodi. Questi creano un blocco che contiene tra le altre la transazione proposta dal nodo A e il blocco viene valutato. Se il 51% dei nodi approva il blocco, questo viene scritto definitivamente nella blockchain ed ora anche il blocco B (destinatario) può accedere alla transazione.

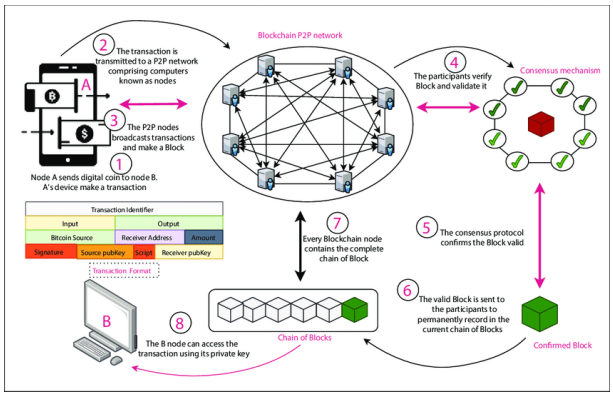

Figura 1.2: Visualizzazione grafica delle operazioni standard di una blockchain
Fonte: https://www.researchgate.net/ by Md Ashraf Uddin

In questo modo, dal 12 Gennaio 2009, data in cui Satoshi Nakamoto per primo inviò 10BTC, la rete dei Bitcoin permette lo scambio della cryptovaluta. Ad ogni transazione, i nodi che per primi la approvano (i *miners*) ricevono una ricompensa in BTC, calcolata in base ad un algoritmo scritto dal creatore stesso, che diminuisce il valore della ricompensa man mano che aumentano i BTC in circolazione, impostando il tetto massimo in circolo a 21 milioni di monete. Questo tetto non può essere superato nemmeno tramite il *double spending*, poiché il sistema Bitcoin garantisce la "potatura" dei rami nati da questa truffa.

Letteralmente "catena di blocchi", la blockchain è un **registro condiviso ed immutabile** che facilita la registrazione e la tracciabilità delle transazioni. Nella blockchain,

ogni utente possiede tutta la catena delle transazioni fin dall'origine e può approvare o meno le nuove transazioni.

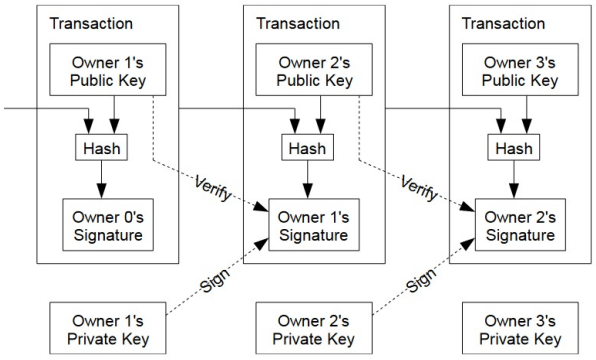

Figura 1.3: Struttura delle transazioni Bitcoin nel *white paper* originale

La transazioni, schematizzate nell'immagine qui sopra, vengono registrate in questa catena di blocchi, identificati dall'*hashing* del timestamp e per questo unici. L'approvazione di ciascuna transazione non ha più bisogno di un ente centrale (p.es. la nostra banca che, alla nostra richiesta di fare un bonifico, garantisce che quella somma è presente nel nostro conto corrente e può essere spostata nel conto del destinatario), ma sarà la *community* ad approvare la transazione, attraverso lo storico delle transazioni (inciso in modo immodificabile nella blockchain) e la risoluzione della *proof-of-work* (che vedremo in modo più approfondito nel seguito).

1.1.2 L'interesse per la blockchain

Nell'ultimo decennio l'attenzione si è spostata dai Bitcoin verso la blockchain in quanto tecnologia che rende possibile la loro esistenza. Il progetto di Satoshi Nakamoto è *open-source*, quindi chiunque ha la possibilità di studiare e capire lo sviluppo di questa tecnologia, replicandola. L'interesse crescente non è dovuto solo ad una sorta di passione irragionevole per il nuovo che avanza, ma nasce soprattutto grazie alle molteplici applicazioni. Sono nate in questi anni blockchain alternative (a volte chiamate *altchain*, per sottolineare la loro alternatività rispetto a Bitcoin), le cui funzionalità non sono limitate alle sole cryptovalute, ma permettono nuovi modi d'uso. Le caratteristiche di queste blockchain promettono sviluppi presenti e futuri in campi come l'economia e la finanza, la gestione della democrazia, il *cloud computing* e la sanità.

Per comprendere i vantaggi dell'utilizzo della blockchain negli ambiti appena elencati, solitamente se ne sottolineano la decentralizzazione, l'immutabilità, la trasparenza e la sicurezza. Lo stesso fa questo elaborato.

Decentralizzazione

Quando ciascuno di noi deve fare un bonifico bancario, la garanzia che non verserà più denaro di quanto non ne abbia depositato nel proprio conto corrente è data dall'istituto finanziario di riferimento. Se voglio versare una cifra superiore a quella totale che possiedo, la banca non permetterà il bonifico, perché ha verificato che non dispongo di sufficiente liquidità. Questa è la **centralizzazione**: ogniqualvolta un singolo ente, piccolo o grande che sia, è il garante della legittimità di un'azione, l'approvazione si dice centralizzata. Una fetta importante della nostra società si basa su questo principio: non solo gli istituti bancari, ma anche la sanità, lo SPID, l'istruzione etc. Se voglio verificare il titolo di studio di un candidato, mi devo rivolgere all'istituto che l'ha rilasciato; solo questo può garantirmi la veridicità del titolo esposto. Persino le elezioni si basano sui risultati che ogni seggio segnala, in modo piramidale dalla base fino alla capitale.

La blockchain rovescia questo paradigma, spostando l'approvazione dall'ente centralizzato alla *community*. Ogni nodo della blockchain possiede tutte le informazioni necessarie per dare o meno il consenso. Riprendendo l'esempio del bonifico, se voglio donare una certa quantità di cryptovalute, non c'è nessun ente che verifica la mia disponibilità nel wallet, ma (in modo anonimo) sono tutti i nodi della blockchain che verificano lo storico delle transazioni ed accertano che ho i fondi necessari per la transazione. Come vedremo tra poco riguardo la sicurezza, proprio la necessità dell'approvazione del 51% della rete rende questo passaggio estremamente difficile da intercettare ed hackerare. Oltre a rendere strumentalmente difficile un'approvazione "fasulla", la decentralizzazione distribuisce anche l'interesse per delle transazioni oneste. Se un singolo dipendente di un istituto bancario disonesto e con delle spiccate capacità informatiche può effettuare dei spostamenti a suo favore, in una blockchain i singoli nodi hanno nei loro interessi che le transazioni rispettino le norme. Per assurdo, si dovrebbe creare un interesse comune a più della metà dei nodi, per poter falsificare una transazione.

Immutabilità

Come abbiamo già detto, ogni nodo della blockchain possiede tutto lo storico della stessa. Per questo si può dire che ogni transazione è scolpita in modo definitivo ed immutabile, una volta approvata. Un blocco ha scritte al suo interno un certo numero di transazioni e questo blocco è posseduto, in copia, da tutti gli utenti della *community*. Falsificare un blocco non sarebbe quindi sufficiente, ma si dovrebbero modificare quasi 7000 nodi, degli oltre 13000 raggiungibili[5].

Seppur esista quindi una via per modificare la blockchain, questa non è nella sostanza percorribile e questo garantisce, *de facto*, l'immutabilità.

Trasparenza e privacy

Oltre ad essere immutabile, la blockchain è consultabile in qualsiasi momento. Esistono diversi modi di cercare un particolare *smart contract*, una transazione o qualsiasi movimento registrato in un blocco. Il tutto senza ledere la privacy degli utenti: ciascuna operazione (e ciascun *wallet*) è infatti registrata tramite un indirizzo univoco. Limitandoci all'uso delle transazioni di cryptovalute, ogni nodo ha un proprio indirizzo grazie al quale si possono verificare tutte le transazioni fatte; quest'ultimo però non ha nulla a che fare con l'identità della persona fisica che lo possiede: l'unico modo per collegarli è che sia l'utente a rendere pubblico il proprio indirizzo.

Di fatto, ogni account ha 3 "chiavi": privata, pubblica e l'indirizzo. La chiave privata è un numero compreso tra 0 e $2^{256} - 1$. Questa è personale e irrecuperabile, se smarrita le proprie cryptovalute sono perse per sempre. Attraverso delle funzioni di hashing si ottengono la chiave pubblica e, successivamente, l'indirizzo. Le funzioni di hashing usate sono univoche e non invertibili: dalla chiave privata è sempre possibile recuperare la chiave pubblica e l'indirizzo (per questo deve essere tenuta segreta), mentre non è possibile il contrario.

Anche la privacy è decentralizzata: nessun governo, ente o altro può avere un mandato per ottenere l'identità dietro ad un certo indirizzo. Le blockchain sono infatti sovragovernative e non hanno nessun ente centrale sul quale fare pressione per conoscere l'identità di un singolo nodo.

[5]Fonte: https://www.bitrawr.com/bitcoin-node-map, ultima visita: 26/7/2022.

Questa è, tra le altre, una delle ragioni dell'iniziale diffidenza verso le cryptovalute: la loro riservatezza le ha rese uno strumento adatto allo scambio di denaro a fini illeciti, come i pagamenti per il traffico di droghe o di persone nel dark web, oppure i riscatti per i computer sequestrati da virus etc. Le cryptovalute sono però un semplice strumento e come tale non hanno una intenzione, né positiva né negativa, ma è solo l'uso che se ne fa che assegna un valore etico.

Sicurezza

Uno dei punti centrali delle blockchain è la sicurezza, tanto che Satoshi Nakamoto stesso nel suo *white paper* sottolinea quest'aspetto dei Bitcoin. Alcuni tratti di questo aspetto sono già stati trattati nei paragrafi precedenti: in questo paragrafo si cercherà di elencarli in modo ordinato e di sviluppare gli approfondimenti annunciati.

La sicurezza è, evidentemente, proporzionale alla difficoltà di manomettere la blockchain. Le principali manomissioni possibili sono essenzialmente due, una riferita al passato della blockchain e una al futuro: modificare la blockchain così da poter modificare i wallet propri o altrui e il *double spending* (o altre forme fraudolente di *mining*). Per il primo rischio, abbiamo già trattato l'argomento parlando di immutabilità della blockchain.

Il *double spending* si presenta come un problema intrinseco alla moneta virtuale: a meno di stampare denaro falso, non è possibile pagare tramite mezzo fisico due diversi servizi con la stessa moneta, poiché il primo servizio possiede il denaro che potrei usare per pagare il secondo. Nella moneta virtuale, invece, sembra essere più facile questa frode: i tempi di pagamento, l'assenza di un codice invece presente sulle banconote e molti altri fattori possono far pensare che pagare due servizi con la stessa moneta digitale sia possibile. Di seguito un elenco sintetico dei principali cyberattacchi verso la blockchain.

Race attack Il *race attack* consiste nello sfruttare il lasso di tempo che passa dalla richiesta di una transazione Bitcoin alla sua accettazione. L'hacker invia due transazioni in rapida successione, in modo da ottenere il servizio A prima che il pagamento sia accettato e il servizio B con un reale pagamento. Un'alternativa è che il servizio B altro non sia che il suo stesso *wallet*, per cui ottiene il servizio A in modo, di fatto, gratuito. Questa prima falla si supera semplicemente attendendo l'approvazione della transazione prima di fornire il servizio, come un commerciante che non fa debito agli sconosciuti.

Finney attack Simile al *race attack*: in questo caso il *miner* prima di avviare la transazione per il servizio A, pre-registra un blocco con una transazione (tipicamente verso sé stesso). Ricevuto il servizio A, sostituisce il blocco della transazione col blocco minato, così da non pagare il servizio.

Oltre alla bassa probabilità che un singolo *miner* sia scelto per approvare una transazione, anche in questo caso è sufficiente attendere l'approvazione prima di fornire il servizio.

51% attack Già accennato prima, questo attacco consiste nel possedere metà+1 della potenza di calcolo, chiamata *hashrate*. Così facendo si aumentano le possibilità di vincere la competizione per l'approvazione di un blocco, arrivando a centralizzare il controllo. Questo tipo di attacco è semplicemente sconveniente per chiunque lo voglia praticare: possedere un tale *hashrate* andrebbe a distruggere il profitto della truffa, portando i costi al di sopra del guadagno.

Ad oggi si stima che la top tre per *hashrate*[6] sia composta da FoundryUSA (20.5% del totale), F2Pool (17.4%) e AntPool (15%). Diventa quindi impossibile oltre che controproducente per un singolo (o anche per un gruppo) tentare questo attacco.

1.1.3 Ethereum

Figura 1.4: Logo Ethereum

Come per Bitcoin, anche Ethereum inizia la sua storia con un *white paper*, pubblicato da Vitalik Buterin, un giovane programmatore russo: *Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform*[7]. Già dal titolo si può intuire la sostanziale differenza rispetto a Bitcoin: se Nakamoto pensava ad una forma di scambio virtuale di denaro, Buterin invece immagina una vera e propria piattaforma decentralizzata dove chiunque possa sviluppare delle applicazioni con un linguaggio Touring-completo: **Solidity**. Buterin stesso, nell'articolo, descrive lo scopo di Ethereum:

[6]Frankfield, Jake. *51% Attack*. 14 Lug. 2022. URL: `https://www.investopedia.com/terms/1/51-attack.asp#toc-what-is-a-51-attack` (visitato il 07/2022).

[7]Buterin, Vidalik. *Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform*. 23 Gen. 2014. URL: `https://bitcoinmagazine.com/business/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211` (visitato il 07/2022).

> Ethereum does not intend to be a Swiss Army knife protocol with hundreds of features to suit every need; instead, Ethereum aims to be a superior foundational protocol, and allow other decentralized applications to build on top of it instead of Bitcoin, giving them more tools to work with and allowing them to gain the full benefits of Ethereum's scalability and efficiency.

Dal suo lancio ad oggi, Ethereum ha avuto molteplici aggiornamenti e nel 2022 avverrà *The Merge*[8], la fusione della piattaforma Ethereum 2.0 con l'attuale piattaforma, che eliminerà definitivamente la *proof-of-work* dalla blockchain.

All'interno della blockchain Ethereum ciascuno può avere uno o più profili, identificati da un numero esadecimale di 40 cifre, chiamato chiave pubblica, che identifica univocamente ciascuno di questi. La grande novità di Ethereum è proprio l'essere non soltanto una piattaforma di scambio di valute digitali, ma anche permettere lo sviluppo di applicazioni decentralizzate potenzialmente per qualsiasi scopo.

1.1.4 IOTA

Benché esuli dal tema principale di questo elaborato, merita almeno una menzione anche un nuovo tipo di blockchain, che ha rinunciato all'uso dei blocchi: le blockchain con tecnologia DAG (*Direct acyclic graph*).

I DAG sono grafi con una struttura tale che, partendo da un nodo A, non è possibile tornare allo stesso nodo seguendo gli archi del grafo. Ogni sequenza può passare solamente dal prima al dopo, senza mai poter tornare indietro. I DAG sono stati inventati prima della blockchain: sono già impiegati in problemi relativi all'elaborazione dei dati, allo *scheduling*, alla ricerca del percorso migliore per la navigazione etc.

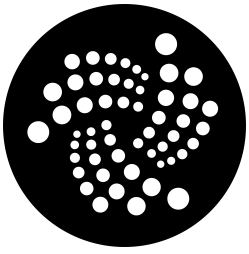

Figura 1.5: Logo IOTA

Il loro uso nella tecnologia in discussione consente di abbandonare l'idea dell'approvazione di blocchi contenenti più transazioni e di approvare invece le singole transazioni, che diventano i nodi del grafo, con una conseguente maggior velocità e il favorire le microtransazioni, scoraggiate invece dai tempi di approvazioni dei blocchi Bitcoin[9].

[8] Per maggiori informazioni, cfr. https://ethereum.org/it/upgrades/merge/

[9] Pagliari, Emanuele. *DAG applicato alla blockchain: la spiegazione e l'uso in IOTA*. 30 giu. 2019. URL: `https://cryptonomist.ch/2019/06/30/dag-blockchain-iota/` (visitato il 08/2022).

IOTA[10] è una cryptovaluta nata per l'*Internet of Things* (IoT, da cui il nome) che ha abbracciato questa struttura dati. In IOTA ogni nuova transazione deve approvare le due transazioni precedenti (non ancora approvate) diventando così *miner* di sé stessa. Questo consente, potenzialmente, una scalabilità infinita e l'assenza di tasse per l'immissione di nuove transazioni.

1.2 Forme di consenso

Le forme di consenso sono uno dei punti più importanti all'interno dello sviluppo della blockchain. Quando una transazione viene proposta, tutti i nodi concorrono all'approvazione del nodo proposto: solo chi lo approva, infatti, viene ricompensato. Questa corsa all'approvazione viene vinta in base ad alcune regole: le forme di consenso, appunto. La blockchain propone alcune sfide per poter poi approvare il nodo proposto e i primi a risolverle ricevono la ricompensa per aver minato un nuovo blocco.

Storicamente Bitcoin introduce la prima modalità di approvazione: la **Proof-of-work**, ancora oggi in uso nella blockchain di Nakamoto. Da allora sono nate alcune alternative; Ethereum (soprattutto dopo il *The Merge*) ha scelto la **Proof-of-stake**. Altre proposte stanno nascendo su *altchain*, come la **Proof-of-history** per la cryptovaluta Solana o altre prove ancora in fase di sviluppo. In questo elaborato approfondiamo la pioniera (*proof of work*) e la scelta di Ethereum, per poi elencare brevemente nuove alternative e le loro caratteristiche.

1.2.1 Proof-of-work

Storicamente la prima forma di consenso su blockchain, in uso ancora oggi su Bitcoin, la *proof-of-work* (PoW) consiste nella risoluzione, da parte dei computer dedicati al *mining*, di complessi calcoli. Questi puzzle crittografici non richiedono logica o un particolare ragionamento, ma piuttosto la generazione di quante più soluzioni possibili. Per questo le schede grafiche si sono presto rivelate ottimali per il *mining*: l'alta parallelizzazione fa di esse lo strumento adatto a generare quante più soluzioni possibili.

Seppur la PoW funzioni da più di un decennio e abbia reso la rete Bitcoin una rete sicura, questa non è priva di alcuni limiti. Primo fra tutti l'alto consumo energetico

[10]Popov, Serguei. *The Tangle*. 30 Apr. 2018. URL: `https://www.allcryptowhitepapers.com/iota-whitepaper/` (visitato il 08/2022).

che richiede: per ricevere la ricompensa, il *miner* deve avere più potenza di calcolo dei suoi avversari, quindi un consumo energetico maggiore. Gli strumenti richiesti, inoltre, non sono alla portata economica di chiunque. Questa forma di consenso ha di fatto generato una barriera di ingresso al *mining* su Bitcoin (e, nei primi tempi, anche su Ethereum), barriera aggirata tramite le *mining pool*, che di fatto rischiano di intaccare la decentralizzazione.

1.2.2 Proof-of-stake

Dati i limiti della PoW, non ultime la lentezza e il muro d'ingresso, nel 2011 nel forum BitcoinTalk[11] nasce la proposta di una diversa forma di validazione: la *proof-of-stake* (PoS). L'anno successivo, ad opera di Sunny King e Scott Nadal viene pubblicato il *white paper* anche per la PoS[12]. L'idea era ancora embrionale e si basava sul concetto di *coin age*. Scrivono gli autori:

> In a simple to understand example, if Bob received 10 coins from Alice and held it for 90 days, we say that Bob has accumulated 900 coin-days of coin age.
>
> Additionally, when Bob spent the 10 coins he received from Alice, we say the coin age Bob accumulated with these 10 coins had been consumed (or destroyed).

La *coin age* non è quindi legata unicamente alla disponibilità economica, ma piuttosto alla fedeltà al progetto. Acquistare una grossa quantità di cryptovalute significa credere nel progetto, ma lo stesso vale per chi ne acquista un quantità minore ma la detiene per lungo tempo. Questa forma di consenso, quindi, non impone una barriera d'ingresso basata sulla potenza di calcolo o sulla disponibilità economica del singolo.

Chi "blocca" parte delle sue cryptovalute per creare il proprio *stake* è chiamato *validator*. La scelta dei *validators* per il singolo blocco può essere casuale o basata sulla dimensione dello *stake*, ma è in ogni caso più democratica rispetto alla PoW, che invece potrebbe (nel caso assurdo che un singolo *miner* possedesse il 51% della potenza di calcolo) scegliere sempre la stessa persona. Il rischio della centralizzazione nella PoS è scongiurato dal costo della validazione: se si viene scelti, lo *stake* viene ridotto dal costo.

Il grosso vantaggio della PoS è la non necessità di una grande potenza di calcolo. Chiunque con un computer con sufficiente memoria per poter avere tutta la blockchain e

[11] https://bitcointalk.org/index.php?topic=27787.0

[12] King, Sunny e Nadal, Scott. *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. 19 Ago. 2012. URL: `https://decred.org/research/king2012.pdf` (visitato il 07/2022).

una connessione ad internet 24 ore su 24 può partecipare ed essere scelto come *validator*. L'incentivo ad un comportamento corretto è lo ***slashing***: un comportamento fraudolento porta alla perdita di una percentuale o della totalità dello *stake*, senza ottenere la ricompensa per la validazione.

Nemmeno la PoS è però priva di limiti, prima fra tutti la maggior possibilità di essere scelto per chi ha un capitale maggiore. Possiamo immaginare la scelta come l'estrazione di un nome da un cappello con i bigliettini di tutti i partecipanti. Ciascun partecipante paga un tassa per ogni bigliettino col suo nome. Chiaramente chi ha maggior disponibilità economica sarà scelto con più probabilità; ma man mano che i suoi biglietti vengono estratti, anche chi è meno abbiente ha sempre più possibilità di essere scelto.

Delegate PoS Come si può intuire dal nome, in questa forma di consenso lo *stake* non è personale, ma viene delegato a dei validatori selezionati. Potremmo paragonare questa forma a delle elezioni, con una parte del proprio *stake* al posto del voto.

Liquid PoS Questa *proof* è simile alla *delegate PoS*, con la differenza che le monete affidate ad un altro *validator* non vengono bloccate, ma possono continuare ad essere usate.

1.2.3 Forme di consenso alternative

Proof of history

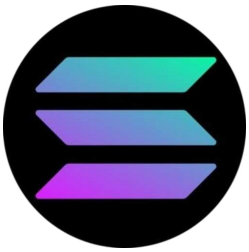

Figura 1.6: Logo Solana

Proof of History is a sequence of computation that can provide a way to cryptographically verify passage of time between two events. It uses a cryptographically secure function written so that output cannot be predicted from the input, and must be completely executed to generate the output. The function is run in a sequence on a single core, its previous output as the current input, periodically recording the current output, and how many times its been called.

> The output can then be re-computed and verified by external computers in parallel by checking each sequence segment on a separate core[13].

Usando la crittografia SHA256, la *proof-of-history* basa la validazione sull'ordine cronologico dei blocchi, usando l'output del blocco $n-1$ come input per il blocco n. Per la stessa ragione, tutti i blocchi già validati possono essere verificati da terze parti. Inoltre, questa forma di consenso non è parallelizzabile e quindi non preferisce chi dispone di potenza di calcolo maggiore.

Figura 1.7: Logo Idena

Proof of person Questa forma di consenso, a differenza delle altre, si basa unicamente sulla centralità della persona. Il progetto Idena[14] cerca di portare il fondamento chiave della democrazia nella blockchain: una persona, un voto. La *proof-of-person* attraverso alcune challenge (chiamate *flip puzzles*) da risolvere periodicamente, in modo sincrono e in tempi brevi, punta a creare una identità virtuale unica per ogni persona. Questi *flip puzzles* sono dichiarati a prova di AI e il progetto mette in palio premi per chi dovesse riuscire a sviluppare un'AI capace di risolverli con una precisione minima del 71%.

1.3 Smart Contract

Uno *Smart Contract* (d'ora in poi, *sc*) ben si spiega attraverso la sua traduzione letterale: contratto intelligente. Tutti i contratti, di lavoro, noleggio o altro che siano, hanno una forma di base del tipo "Se ... Allora ...": se pago l'affitto, allora posso vivere nell'appartamento; se lavoro 40 ore a settimana, allora ricevo lo stipendio. Uno *sc* è la resa crittografica dei più classici contratti su carta che conosciamo. Oltre alla diversa forma di scrittura, uno *sc* è automatico, immutabile e letterale.

Immaginiamo uno *sc* d'affitto, dove grazie al pagamento concordato l'affittuario può godere dell'immobile. In un giorno stabilito del mese, lo *sc* avvia una transizione di denaro dal *wallet* dell'affittuario a quello del locatore. Questa transizione, a patto che l'affittuario

[13] Yakovenko, Anatoly. *Solana: A new architecture for a high performance blockchain v0.8.13.* URL: `https://solana.com/solana-whitepaper.pdf` (visitato il 07/2022).

[14] https://www.idena.io/it

abbia denaro a sufficienza, aggiorna la tessera per accedere al portone d'ingresso. Questo è l'automatismo: l'affittuario non deve fare il bonifico e il locatore non deve aggiornare i permessi di accesso, ma una volta concordati i termini, tutto avviene in automatico.

Immaginiamo che un giorno il locatore decida di alzare l'affitto, ma che nel contratto si fosse concordata una cifra non modificabile (in termini di programmazione, che non ci fosse una funzione *editRent()*): potrà solo ricontrattare, al termine legale dello *sc*, la cifra col locatore. Questa è l'immutabilità: tutto ciò che è scolpito nella blockchain, non può essere modificato.

Immaginiamo infine che il giorno pattuito per il pagamento l'affittuario non abbia denaro a sufficienza per pagare. Alla mezzanotte, la sua tessera perderà i diritti per aprire la porta dell'appartamento. Anche ammettendo che lo *sc* già preveda la possibilità di pagare 2-3 giorni dopo la data concordata, allo scadere di questi l'appartamento è da considerarsi libero e le clausole per il non pagamento già in atto. Questo è il significato dell'ultima caratteristica: gli *sc* non prevedono eccezioni oltre a ciò che è stato scritto nel loro codice.

DApp Abbreviazione di *decentralized application*, sono applicazioni decentralizzate basate sulla blockchain. Prima di Ethereum, le DApp potevano fare solo un numero limitato di operazioni, ma grazie a Buterin è possibile svilupparle sulla sua piattaforma per qualsiasi caso d'uso si possa immaginare.

EVM La *Ethereum virtual machine* è un software che permette di eseguire *real time* qualsiasi programma, indipendentemente dal linguaggio di programmazione, sulla blockchain Ethereum.

DAO La *Decentralized Autonomus Organization* è l'apice dell'uso delle DApp: vere e proprie organizzazioni la cui *governance* è decentralizzata e basata sul voto di tutti attraverso i token. Questa più di tutti è in forma di sviluppo. Essendo organizzazioni complesse e composte da moltissimi *smart contract*, esse hanno tutti i limiti della programmazione umana e l'immutabilità del codice in alcuni casi può rivelarsi un difetto, se un malintenzionato dovesse riuscire a trovare dei modi per arricchirsi tramite le funzionalità delle DAO (famoso il furto di 3,6 milioni di ETH nel 2016).

1.4 Web3

Internet of Things, intelligenza artificiale, decentralizzazione e un'enorme quantità di dati a disposizioni sono i principali attori del cambiamento attualmente in atto: il web3.

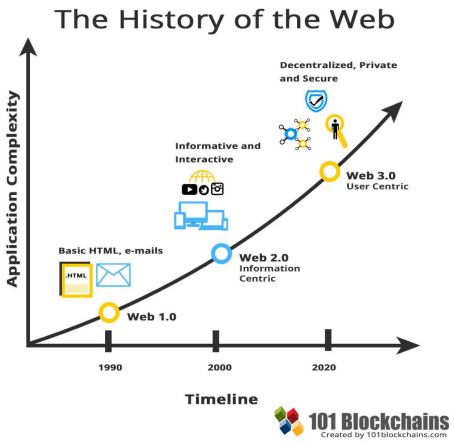

Figura 1.8: Grafico dello sviluppo del web
Fonte: https://101blockchains.com/web-3-0-examples/

Quella che potremmo chiamare la prima versione del web, il **web1**, si può rappresentare con la consultazione delle enciclopedie in biblioteca. Si poteva accedere a risorse statiche caricate grazie a competenze specifiche da parte dei primi *web developer*. Simbolo del **web2**, invece, sono i *social network*: la possibilità di interagire, caricare contenuti, partecipare attivamente alla vita del web sono tutte le caratteristiche del web che in larga parte ancora oggi viviamo.

La rivoluzione in corso, il passaggio verso il **web3**, è l'integrazione capillare del web in tutti gli ambiti della vita. Se il web2 ha permesso agli utenti di interagire, lo scopo del web3 è permettere l'interazione tra i dati, sviluppare la decentralizzazione e garantire la privacy.

Capitolo 2

Etica della blockchain

2.1 La necessità di un'etica della blockchain

Non è facile definire quali siano gli strumenti etici per una valutazione dell'uso della blockchain, tanti sono i suoi possibili usi. Ad una prima analisi si potrebbe pensare di usare le categorie dell'etica economica e finanziaria, ma queste risulterebbero insufficienti perché la blockchain è anche uno strumento democratico, uno strumento che propone una nuova famiglia di garanti, grazie alla decentralizzazione.

Risulta più che mai necessario porre dei confini, definire quali saranno i confini di questa riflessione. Anzi, prima di porre le fondamenta si rendere utile spiegare il perché di questo capitolo, lo *status quaestionis*. La bibliografia a riguardo al momento non è certamente paragonabile ad altri campi dell'etica che vantano migliaia di anni, ma l'interesse crescente per la tecnologia sta facendo crescere anche l'interesse etico[15], anzi la necessità di una riflessione etica:

> If blockchain technology can be reasonably expected to make a significant difference in society, then it deserves its own field of ethics, just like biotechnology, artificial intelligence, and nuclear technology[16].

Nell'articolo appena citato si elencano conferenze e lezioni accademiche interessate all'argomento, a porre delle basi per una nuova branca dell'etica. Si sottolinea come la

[15]Per approfondimenti: Hasan Jamil, *Blockchain Ethics: A Bridge to Abundance*, CreateSpace Independent Publishing Platform, 2018; Hyrynsalmi Sami, Hyrynsalmi Sonja M. & Kimppa Kai K., *Blockchain Ethics: A Systematic Literature Review of Blockchain Research*, in: *et al. Well-Being in the Information Society. Fruits of Respect. WIS 2020. Communications in Computer and Information Science*, vol 1270., Springer

[16]Orcutt, Mike. *Why it's time to start talking about blockchain ethics.* 10 Ott. 2019. URL: `https://www.technologyreview.com/2019/10/10/132652/why-its-time-to-start-talking-about-blockchain-ethics/` (visitato il 08/2022).

questione non sia strettamente legata alla finanza, all'etica o all'uso in mercati illeciti, ma alle potenzialità della blockchain, ai suoi sviluppi e a quali cambiamenti possa portare nella società. La domanda alla base dei vari interventi è la stessa: «Come possiamo modellare positivamente lo sviluppo di questa tecnologia?». Similmente, la questione si pone anche a livello di codice di condotta, deontologico.

> Ethical issues can occur whenever humans are involved in decision-making. This is the reason that many professions -such as law, medicine, and accounting- create ethical standards of conduct. Blockchain technology, though still a new field, has the potential to be as impactful upon people's lives as these established fields. For example, if Libra succeeds, it will potentially touch the lives of billions of people around the world. Accordingly, it is time to have the debate over the issues raised by human-influenced decisions in blockchain platforms[17].

La questione posta nell'articolo appena citato, citando l'esempio di Libra (la cryptovaluta di Meta), è la decentralizzazione: l'interrogativo insieme tecnico ed etico è se sia sufficiente l'immutabilità della blockchain a garantire per le decisioni prese dall'uomo, agente etico per eccellenza. Una questione tra le altre è quella propria dell'assenza di un'amministrazione centrale che può decidere ciò che è più o meno corretto, lasciando questa decisione in mano a un codice (scritto da uomini) e alla decentralizzazione: arricchirsi a danno di altri grazie ad un bug di uno *smart contract*, per esempio, è eticamente corretto? Più in generale, tutto ciò che è possibile fare è giusto sia fatto? Se fino ad oggi abbiamo conosciuto chi si sa muovere tra le pieghe della legge, al limite di ciò che è legale, in futuro potremo incontrare chi si sa muovere tra le pieghe dei codici.

D'altro canto, sempre sul caso d'uso di Libra, non manca chi pone dei dubbi riguardo la decentralizzazione, forse più pretesa che reale:

> Blockchain technology, like its predecessors the railroad and the Internet, will revolutionize the world. Although this new industry is rooted in the concept of decentralization, blockchains do rely upon certain agents of influence for decision-making purposes[18].

L'articolo cerca di mostrare come, a fronte della decentralizzazione tecnicamente implementata, le blockchain siano spesso in mano a piccoli gruppi di persone e aziende, che

[17] Neitz, Michele Benedetto. *Ethical Considerations of Blockchain: Do We Need a Blockchain Code of Conduct?* 21 Gen. 2020. URL: `https://sites.law.duke.edu/thefinregblog/2020/01/21/ethical-considerations-of-blockchain-do-we-need-a-blockchain-code-of-conduct/` (visitato il 08/2022).

[18] Neitz, Michele Benedetto. *The Influencers: Facebook's Libra, Public Blockchains, and the Ethical Considerations of Centralization.* 22 Nov. 2019. URL: `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3441981` (visitato il 08/2022).

di fatto hanno una forte influenza sull'andamento e sull'uso delle stesse. L'autore auspica una regolamentazione legale dell'uso delle blockchain, per contrastare il timore verso questa tecnologia da una parte e prevenire usi eticamente scorretti dall'altra. Chi possa o debba, tuttavia, regolare un'entità che manca di un organismo centrale identificabile in un certo territorio rimane una questione aperta.

2.2 Criteri etici

Constatata la necessità che si inizi a parlare di etica delle blockchain, vorrei affidarmi ad alcuni autori per porre delle basi di questa riflessione. Desidero iniziare chiarendo quali siano le fondamenta di questa riflessione, dal momento che nessuno strumento è in sè stesso buono o cattivo, tutto dipende dall'uso che se ne fa.

Nel suo libro *Eticonomia. La gestione dell'etica dell'economia, dell'impresa, del mercato, del business, della finanza, dei consumi, dell'ambiente*, Antonio Foglio esplicita il **principio personalista** e la necessità di un'etica in ambito economico:

> [...] fin dall'antichità l'economia ha avuto una connessione con l'etica: Aristotele, San Tommaso d'Aquino, Adam Smith, ecc. [...].
>
> L'economia è dunque etica non tanto per caratterizzazione che le viene attribuita, ma invece per sua esigenze intrinseche [...].
>
> L'etica fa dunque parte dell'economia, essa non è un *optional*; dell'etica in economia non se ne può fare a meno, come l'uomo non può fare a meno dell'aria per vivere; è infatti l'etica ad umanizzare l'economia, ad alimentare lo spirito partecipativo e collaborativo dei vari soggetti[19].

Come accennavo nella precedente sezione, non è però possibile limitare questa riflessione al solo ambito economico: è anche una rivoluzione umana e sociale, che cambia in un certo senso il modello autoritario a cui siamo abituati, distribuendo il potere decisionale. Questa rivoluzione, però, ha senso solo se favorisce il bene di tutti: la creazione di una nuova casta non migliorerebbe le condizioni della società, ma andrebbe solo a trasferire vecchi privilegi a nuovi gruppi. La rivoluzione in corso porta vero vantaggio solo tiene al centro il **bene comune**:

> Dalla dignità, unità e uguaglianza di tutte le persone deriva innanzi tutto il principio del bene comune [...]. Secondo una prima e vasta accezione, per bene comune s'intende ≪l'insieme di quelle condizioni della vita sociale che permettono sia alle collettività sia ai singoli membri, di raggiungere la propria perfezione più pienamente e più celermente≫.

[19] Foglio, Antonio. *Eticonomia. La gestione dell'etica dell'economia, dell'impresa, del mercato, del business, della finanza, dei consumi, dell'ambiente*. Franco Angeli, 2016, pp. 76-77, *passim*.

> Il bene comune non consiste nella semplice somma dei beni particolari di ciascun soggetto del corpo sociale. Essendo di tutti e di ciascuno è e rimane comune[...]. Come l'agire morale del singolo si realizza nel compiere il bene, così l'agire sociale giunge a pienezza realizzando il bene comune[20].

Riassumendo, l'analisi etica si baserà sui due principi appena esposti: bene comune e principio personalista.

2.3 Casi d'uso

Ora che sono stati chiariti i confini della riflessione proposta, possiamo introdurre una presentazione di alcuni casi d'uso della blockchain a baluardo di un desiderio di eticità e trasparenza. Questi esempi vogliono essere una concretizzazione di quanto appena esposto, di persone ed organizzazioni che hanno posto in essere il motto (mi sia concessa la licenza) «la blockchain è fatta per l'uomo e non l'uomo per la blockchain».

Miniere del Congo

Banca Etica presenta questo progetto, già citato in precedenza, in sviluppo nella Repubblica Democratica del Congo[21]: la blockchain è usata per registrare grazie ad un tag digitale, per ogni confezione sigillata di cobalto, il minatore, data e ora del confezionamento, quantità, luogo e tutti i dettagli che potranno essere verificati in qualsiasi momento ispezionando i blocchi. Questo strumento non solo permetterebbe di verificare eventuali furti o smarrimenti nel trasporto e nella vendita, ma di combattere il lavoro minorile e lo schiavismo, potendo verificare chi sono i minatori impegnati nell'estrazione e gli orari di confezionamento.

Giveth

Figura 2.1: Logo Giveth

"*Welcome to the Future of Giving*", questo lo slogan che si legge nella pagina principale di Giveth[22]. Il sito implementa su scala mondiale il progetto che questo elaborato presenta localmente. Ogni utente registrato alla piattaforma può proporre il proprio progetto o donare per altri già proposti. Oltre alle modalità classiche (login tramite mail e donazione con bonifico bancario), il sito propone il login tramite il proprio *wallet* e la

[20] Pontificio Consiglio della giustizia e della pace, *Compendio della dottrina sociale della Chiesa*, n. 164.

[21] https://www.eticasgr.com/storie/news-eventi/blockchain-etichetta-etica

[22] https://giveth.io/

donazione in cryptovalute (principalmente quelle sviluppate su blockchain Ethereum). Nel caso in cui un utente presenti il proprio progetto, non ha bisogno di essere accettato dagli amministratori, ma è la *community* a decidere chi merita fiducia e chi no.

Altri esempi

Figura 2.2: Logo UNICEF

UNICEF CryptoFound Anche UNICEF, nel 2019, apre alla possibilità di donare cryptovalute (solo Ether e Bitcoin) ai loro progetti[23]. Nella pagina dedicata, alla domanda sulla ragione di questa iniziativa, si legge: «Simply put: Transparency. Efficiency. Digital by Default». L'intento è così forte e chiaro che troviamo anche una pagina dedicata al tracciamento dei fondi ricevuti[24], grazie al quale si possono facilmente verificare gli ingressi, le uscite e le transazioni dei *wallet* che hanno deciso di donare a questo fondo. Indagini che, con le donazioni classiche, sono impossibili da fare seduti davanti alla propria scrivania.

Figura 2.3: Logo World Food Programme

Building blocks Il *World food programme*, lavorando dal 2015 sulla piattaforma di Ethereum, accetta donazioni in valuta digitale destinate all'assistenza umanitaria per il progetto *Building blocks*[25]

Elencare tutti gli esempi, oltre ad essere poco utile, renderebbe la lista molto lunga. Ne emerge che questo uso della blockchain si sta diffondendo e, come un bambino non può crescere senza qualcuno che gli trasmetta dei valori, allo stesso una rivoluzione di questa portata non può essere lasciata crescere senza porsi la questione etica che la riguarda.

2.4 Analisi etica

Come abbiamo visto, l'uso della blockchain può avere indiscutibili risvolti positivi sul piano socio-economico ed un impatto positivo sulla vita di moltissime persone. Viene quindi proposta ora una prospettiva sulle principali criticità etiche di questa rivoluzione.

[23] https://www.unicef.org/innovation/stories/unicef-cryptofund
[24] https://cryptofund.unicef.io/track#txs
[25] https://innovation.wfp.org/project/building-blocks

2.4.1 Blockchain

Immaginiamo un'azienda dove tutto è gestito tramite blockchain: i *curricula* sono la traccia su blockchain dei lavori passati di ciascun dipendente, le decisioni vengono prese tramite delle DAO, i contratti di assunzione e i pagamenti sono gestiti con degli *smart contract*[26]. Sembrerebbe l'azienda perfetta, dove -a patto di avere dei buoni programmatori- nulla può andare storto: le decisioni del consiglio di amministrazioni sono a disposizione dei dipendenti, lo stipendio arriva puntuale quando stabilito e nessuno può mentire sulle proprie referenze.

Ma cosa succederebbe se, in un precedente luogo di lavoro, il direttore avesse scritto una pessima lettera di raccomandazione ad un dipendente perché questo si è rifiutato di compiere qualcosa che non rientrava nelle sue mansioni o, peggio, di illegale? O se anche le cause fossero scritte su blockchain e non fosse quindi più possibile ottenere la riservatezza su alcune informazioni? Uno dei più importanti diritti da preservare, oggi più che mai, è quello alla riservatezza, alla privacy. Chi vorrebbe che il proprio vicino di casa, con un po' di pazienza, il mio address e una buona connessione, potesse vedere quanto ho guadagnato oggi al lavoro? Se l'uso della blockchain diventasse capillare, pur nelle migliori intenzioni, non garantirebbe il diritto alla riservatezza. Certo, sarebbe sufficiente tenere segreta la propria chiave pubblica o avere più indirizzi; ma una volta resi noti, tutto sarebbe consultabile.

D'altra parte però chi non vorrebbe avere la garanzia di ricevere il compenso pattuito, senza sorprese? La blockchain lo permette. O chi non vorrebbe avere uno strumento facile e sicuro per far votare tutti i dipendenti su una precisa scelta aziendale? La blockchain permette anche questo. I vantaggi di questa tecnologia sono molti e chissà quanti ce ne sono ancora da scoprire, ma a patto di compromessi. Compromessi che non è scontato accettare in qualsiasi ambito.

> However, the first ethical risk to be managed by blockchain advocates is that they not over-hype the technology's potential and then over-promise in terms of what it can deliver[27].

La sfera privata è qualcosa di essenziale per il rispetto e la valorizzazione dell'essere

[26]Per ulteriori approfondimenti, soprattutto riguardo a diverse prospettive etiche sull'argomento, cfr. Sharif, Monica M. e Ghodoosi, Farshad. *The Ethics of Blockchain in Organizations*. 2 Feb. 2022. URL: `https://link.springer.com/article/10.1007/s10551-022-05058-5#citeas` (visitato il 08/2022).

[27]Longstaff, Simon. *Blockchain: Some ethical considerations*. 16 Mar. 2019. URL: `https://ethics.org.au/blockchain-some-considerations/` (visitato il 08/2022).

umano: il diritto alla privacy contribuisce al più ampio diritto alla libertà di espressione, di essere. Un utilizzo smodato ed eccessivo della blockchain, pervasivo di tutti i campi della vita di una persona, andrebbe a ledere questo diritto. Certo, volendo affrontare la questione con una prospettiva a priori, con un'etica basata su virtù pre-esistenti le azioni dell'uomo, questa diventa una prospettiva perfetta. Anche usando un approccio deontologico, basato sui doveri, l'utilizzo pervasivo della blockchain è quasi auspicabile, non fosse che rende quasi impossibile cambiare vita a chi viene da una situazione più difficile e magari a suo modo burrascosa.

Il principio personalista, un'etica che guarda al benessere del singolo e del gruppo, esprime invece alcune perplessità rispetto a questi sviluppi, che rischiano di incatenare l'uomo dentro le sue stesse regole, ingabbiato in uno *smart contract* che lui stesso ha fatto e di cui ora è prigioniero. Ciò che in questa prospettiva diventa estremamente interessante è lo sviluppo delle *Decentralized People Organizations* (d'ora in avanti, DePo). Le DePo non sono una specifica tecnologia, ma piuttosto l'insieme di tutti gli ambiti dove l'esperienza umana è maggiormente coinvolta nell'uso di blockchain e ne può trarre vantaggio. Un esempio già citato di DePo è la trasparenza nelle decisioni dei consigli di amministrazione o dell'intera azienda/organizzazione, cambiando -non solo linguisticamente- la denominazione dei dipendenti da "risorse" a "persone".

> We conclude that in whole the implementation of blockchain technology in people operations processes can create a more ethical work environment. However, careful implementation is necessary and requires extensive examination of ethical implications in advance[28].

Come tutti gli strumenti, la blockchain non ha in sé stessa un intento etico, è il suo utilizzo che lo determina. Questa particolare rivoluzione può tuttavia garantire davvero un maggior rispetto del bene di ciascuno e di tutti, se trova il giusto indirizzo. Questa è l'intrinseca contraddizione dell'etica della blockchain: l'analisi etica della decentralizzazione presuppone un fondamento centralizzato. Un giudizio etico non può avere una base decentralizzata, dal momento che sono le fondamenta a sostenere la casa e non il contrario. A chi spetti questo compito forse è presto per dirlo. Se immaginiamo una DAO per decidere ciò che è giusto, con le attuali forme di consenso, si rischierebbe di schiacciare le minoranze. Magari, quando inventeremo nuove forme di consenso, anche le decisioni su ciò che è eticamente corretto potranno essere decentralizzate.

[28]Sharif e Ghodoosi, *The Ethics of Blockchain in Organizations*.

2.4.2 Blockchain e filantropia

Quanto fin qui detto lascia intuire le implicazioni nel singolo settore della filantropia.

Ad oggi, il 60% della popolazione globale non ha fiducia che le organizzazioni no-profit portino a termine i loro progetti senza intascarsi parte delle donazioni[29]. La blockchain può venire incontro a questi dubbi, grazie alla trasparenza e alla tracciabilità, come già fanno le organizzazioni qui presentate. Altri vantaggi sono la riduzione dei *middlemen*, la (attuale) bassa tassazione su questo tipo di transazione e l'immediatezza. Sembra quasi una tecnologia che possa soddisfare appieno i bisogni di questo ambito.

L'uso di blockchain e *smart contract*, inoltre, ridurrebbe il numero di volontari necessari per la burocrazia di queste organizzazioni, contrastando le conseguenze del calo di volontari al quale stiamo assistendo in questi anni e destinando sempre più persone al volontariato vero e proprio, più che alla burocrazia che gli è necessaria.

Le problematiche da affrontare sono però altrettante e pongono dubbi non trascurabili. Prima fra tutti, la curva di apprendimento delle cryptovalute è ancora uno scoglio difficilmente superabile per molte persone. La volatilità del loro valore fa temere che, donati 10'000€ ad un'associazione, questa domani ne possieda molti meno. Anche la legislazione globale sta muovendo i primi passi in questo ambito e non è per niente facile prevedere il suo esito. Infine, benché queste donazioni chiudano le porte ai *middlemen*, aprono le finestre per l'hackeraggio internazionale, che come abbiamo già visto potrebbe infilarsi in modo del tutto "legale" nelle pieghe dei codici, deviando le donazioni senza possibilità che un qualsiasi ente possa decidere la validità di quella transizione a posteriori.

In conclusione, le ragioni per credere in questa tecnologia sono tante, ma un eccesso di cieca fiducia può inesorabilmente portare a dei nuovi problemi, rendendo di fatto inutile questa rivoluzione.

[29]Busolli, Luca. *Blockchain e beneficenza*. 23 Dic. 2021. URL: `https://affidaty.io/blog/it/2021/12/blockchain-ebeneficenza/` (visitato il 08/2022).

Capitolo 3

Gli strumenti per il progetto

In questo capitolo presento gli strumenti utilizzati per lo sviluppo del progetto: dai software ai framework usati. Per qualcuno di essi ho dovuto fare delle scelte, legate a ciò che poteva meglio adattarsi al progetto e anche alla sicurezza dello stesso.

3.1 IDE

L'*Integrated Developement Enviroment* (IDE) è un software che aiuta gli sviluppatori nella fase di sviluppo e debugging. Per il progetto si sono resi necessari due IDE differenti, per la programmazione frontend e quella su blockchain.

3.1.1 VS Code

Figura 3.1: Logo Visual Studio Code

Visual Studio Code (VS Code) è un editor di codice sviluppato da Microsoft. È stato usato per la programmazione frontend in Angular, per il suo aiuto con gli errori di sintassi, gli *snippet* e soprattutto la possibilità di fare *local hosting*, fondamentale per testare una web app. VS Code permette inoltre di sincronizzare la cartella di lavoro con una *repository* su GitHub, per una più facile gestione delle versioni del progetto.

3.1.2 Remix

La scelta dell'IDE per la programmazione su blockchain è caduta su Remix, un IDE sviluppato dalla *community* ufficiale di *ethereum.org*, completamente *open-source*[30]. L'IDE,

[30]https://github.com/ethereum/remix-ide

in questo progetto usato nella versione web, permette il *deploy* dello *smart contract* su reti di test e su reti ufficiali.

Figura 3.2: Logo Remix

Nel primo caso, Remix fornisce 15 account, ciascuno con 100 Ether da poter usare per testare le chiamate a funzione. Anche il test delle funzioni è semplificato dall'uso di questo IDE: dopo aver deployato lo *smart contract*, infatti, vengono messe a disposizione le chiamate con relativi argomenti in un'interfaccia intuitiva.

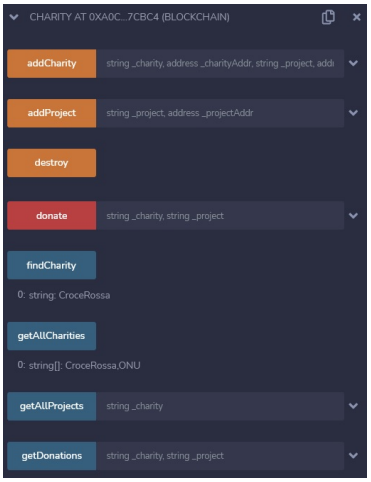

Figura 3.3: GUI per le chiamate a funzione su Remix

Nel caso si stiano usando gli account a disposizione, l'eventuale prezzo è pagato in automatico; se si opta per un *deploy* su blockachain, invece, il pagamento deve essere approvato di volta in volta dal proprio *wallet*, per questo progetto collegato alla rete di test Kovan.

3.2 Tecnologie usate

3.2.1 Spring framework

Figura 3.4: Logo Spring

Spring[31] è un *framework open source* per lo sviluppo su piattaforma Java. Nello specifico per questo progetto ho approfondito lo studio di **Spring Boot**, uno sviluppo di Spring. La differenza fondamentale è la possibilità di quest'ultimo di eseguire una web app senza bisogno di un

[31] https://spring.io/

web server esterno (nelle versioni precedenti, infatti, si doveva ricorrere a Tomcat, Jetty o altri web server).

Spring Boot permette di programmare applicazioni web CRUD[32]. Nella fase iniziale di studio di linguaggi e framework ho sviluppato alcuni server REST[33] usando come database PostgreSQL[34] per la sua semplicità d'uso, la GUI e un primo studio affrontato nel percorso universitario.

La scelta di non creare un backend

Nelle prime settimane di tirocinio, come accennato sopra, ho studiato -anche grazie all'aiuto del tutor e del team aziendale- gli strumenti che avrei poi usato per lo sviluppo del progetto, partendo da ciò che è meno vicino all'utente finale (il backend) fino al frontend, ciò che l'utente vede dell'intero progetto.

Arrivato il momento di decidere il modello vero e proprio, insieme al tutor aziendale ci siamo posti una questione: **è davvero necessario un backend?**

La questione, non banale, riguardava in particolare l'aspetto della sicurezza. Il backend sarebbe servito per un database degli account e delle transazioni avvenute. Chiaramente lo storico delle transazioni sarebbe un doppione: tutto ciò che succede sulla blockchain è pubblico e visibile; l'unico vantaggio poteva essere quello di legare la donazione non solo all'address ma alla persona fisica che decide di donare. Fin dall'inizio si era però deciso di mantenere la privacy del donatore, quindi anche questo possibile sviluppo sarebbe stato contrario ai principi del progetto, oltre che ridondante.

Passando all'aspetto della sicurezza, sviluppando un backend avrei creato una vulnerabilità in più: se qualcuno riuscisse ad accedere con le credenziali di un'associazione potrebbe cambiare l'address di un progetto benefico col proprio. Una volta intascate delle donazioni, sarebbe difficile se non impossibile riavere quelle donazioni, non essendoci un ente centrale di garanzia. Lo *smart contract* è invece nativamente scolpito su blockchain che, come abbiamo già visto, assicura tra l'altro immutabilità e sicurezza. L'accesso viene gestito comunicando col *wallet*, che implementa una sua sicurezza (trattando criptovalute,

[32]CRUD è l'acronimo di Create Read Update Delete, le operazioni base di un server. Indica quindi un'applicazione web capace di interagire in modo elementare con un database.

[33]REST definisce un insieme di principi di architettura per lo sviluppo di un sistema. Spesso legato al web, si basa sui seguenti principi: identificazione risorse, utilizzo metodi HTTP, risorse autodescrittive, collegamenti tra risorse e comunicazione *stateless*.

[34]https://www.postgresql.org/

per altro, questi livelli di sicurezza sono spesso molto alti), fornendomi una protezione dell'utente già sviluppata e testata.

L'implementazione di un backend si sarebbe quindi rivelato un doppione di qualcosa che già esiste (lo storico delle transazioni) oltre che una possibile falla nella sicurezza. Insieme col tutor aziendale abbiamo quindi deciso di lavorare solo su blockchain e frontend, avendo comunque a disposizione tutte le funzionalità necessarie ed evitando una possibile vulnerabilità del progetto.

3.2.2 Solidity

Solidity[35] è un linguaggio di programmazione staticamente tipizzato progettato per lo sviluppo di *smart contract* su Ethereum. Per lo sviluppo del progetto ho scelto questo linguaggio di programmazione (benché non sia l'unico capace di comunicare con Ethereum) per la sua specificità e perché già in un uso nell'azienda ospitante.

3.2.3 Angular

Figura 3.5: Logo Angular

Angular[36] è un framework open source rilasciato per la prima volta nel 2016 (col nome AngularJS), basato su Typescript, sviluppato principalmente da Google. È un framework supportato da una *community* di milioni di persone e largamente usato nella programmazione frontend. Permette lo sviluppo di web app eseguite direttamente nel proprio browser, anche in rete locale.

Ho usato un toolkit in particolare: **Angular Material**[37], una serie di componenti pensati per semplificare la creazione di siti accessibili e moderni.

web3.js vs ethers.js

Insieme allo sviluppo dell'interfaccia per la web app è necessario comunicare con lo *smart contract*: esistono principalmente due librerie per questo scopo, in JavaScript: web3[38] e ethers[39]. Nessuna delle due è significativamente migliore dell'altra: hanno aggiornamenti costanti, popolarità simile e documentazione ancora giovane, confrontata con

[35] https://soliditylang.org/
[36] https://angular.io/
[37] https://material.angular.io/
[38] https://web3js.readthedocs.io/en/v1.5.2
[39] https://docs.ethers.io/ethers.js/v3.0/html/

quella di altre librerie più "adulte". Nonostante ether.js si mostri più performante grazie alla sua dimensione più contenuta e faciliti il testing con test già scritti, ho scelto di usare web3.js per due ragioni: è sviluppata dal team ufficiale di Ethereum (ether.js è invece sviluppata e mantenuta da un singolo programmatore canadese) e, essendo stata pubblicata prima, ha una community di supporto più ampia.

3.3 MetaMask

Figura 3.6: Logo MetaMask

MetaMask[40] è un *cryptowallet* fondato nel 2016 per app distribuite (DApp) del Web3 e NFT, gestito da ConsenSys. È un *wallet* non fisico, utilizzabile come estensione dei principali web browser. Si collega, oltre alla rete principale Ethereum, ad alcune reti di prova, dove è possibile acquistare e scambiare Ether senza costi reali. Per il progetto ho usato la rete di test Kovan e la criptvaluta KovanETH, facilmente acquistabile gratuitamente grazie ad alcuni *tool* messi a disposizione del team di sviluppo.

[40] https://github.com/MetaMask

Capitolo 4

Overview del progetto

4.1 Struttura del progetto

Il confronto con un ambiente professionale è stato fondamentale per la definizione del prodotto finale. L'obiettivo generale era chiaro fin dall'inizio del tirocinio: un'**interfaccia per la beneficenza in cryptovaluta Ether**. Il tutor aziendale, dott. Fabio Pallaro, mi ha aiutato a definire la struttura e a scoprire gli strumenti necessari allo sviluppo. Insieme abbiamo definito il percorso di studio per raggiungere l'obiettivo e tre target a difficoltà crescente, da uno scheletro del progetto ad una piena implementazione[41]. Ciascuno step prevedeva miglioramenti lato *smart contract*, lato *frontend* o su entrambi i lati.

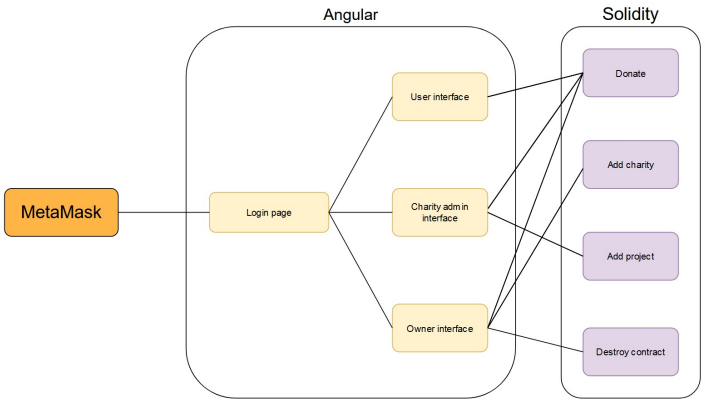

Figura 4.1: Schema generale del progetto

[41]Il progetto è stato interamente pubblicato ed è consultabile su GitHub. Esiste inoltre una prova funzionante della web app.
Smart contract: https://github.com/NonnoPinto/CharityCryptoDonation
Frontend: https://github.com/NonnoPinto/CharityCryptoDonation
Web app: http://nonnopinto.altervista.org/

Nella scrittura dello *smart contract* sono stati rilevanti come qualità centrali la solidità e la completezza. Solidity mette a disposizione un particolare tipo di funzione chiamato *modifier*; i *modifier* sono funzioni utili a modificare il comportamento di altre funzioni (vengono usati ad esempio per mettere dei limiti alle chiamate di funzioni, in base all'address che effettua la chiamata). Questo strumento è essenziale, data la natura pubblica della blockchain, per limitare l'uso illecito di funzioni e per assicurarsi che gli utenti possano accedere solo alle funzioni e alle variabili destinate a loro.

Per il frontend invece si è lasciato in secondo piano l'aspetto strettamente di design, cercando di implementare una *view* accessibile e sicura. Da console, infatti, è possibile avere accesso ad alcune variabili JavaScript ed è importante che nessuno possa, per esempio, sostituire l'address di un progetto no-profit col proprio: quei guadagni sarebbero, di fatto, irrecuperabili.

4.1.1 Versioni del progetto

Prima implementazione

Il primo "livello" da raggiungere era quello di uno *smart contract* funzionante ed accessibile tramite web app. Uno degli aspetti che sicuramente distingue maggiormente la prima versione dello sc dall'ultima pubblicata è la struttura dati usati. Avendo posto come obiettivo principale di questo primo step uno scheletro del progetto completo, lo sc implementava solamente la gestione degli address del proprietario e della singola associazione no-profit[42].

```
address payable owner;
address payable[] charityAddresses;
uint256 totalDonationsAmount;
```

Già nella prima versione troviamo, inoltre, alcuni modifier, qui un esempio.

```
modifier restrictToOwner() {
  require(msg.sender==owner, 'Method available only to owner');
  _;
}
```

[42]In Solidity, gli address sono per ovvie ragioni una primitiva, distinte in address e address payable. La differenza è che solo i secondi possono inviare e ricevere cryptovalute.

Il primo sc non era articolato o ricco di funzioni: permetteva di aggiungere una nuova associazione, di donare e di sapere quanto ciascuno avesse ricevuto fino a quel momento.

Il primo prototipo di view, dal canto suo, era una singola pagina HTML che, connessa a MetaMask, riconosceva l'address come proprietario o come utente e in base a questo permetteva di aggiungere nuove associazioni o solamente di donare. L'obiettivo di questo primo target era approfondire le API di MetaMask e Web3.js, obiettivo non scontato in quel momento.

Seconda implementazione

Dopo aver raggiunto uno scheletro funzionante, si è deciso di rendere più completo lo sc, permettendo a ciascuna associazione di avere più progetti, da aggiungere in modo autonomo.

Come anticipato, la grossa differenza sta nella struttura dati, studiata per cercare un equilibrio tra efficienza e ridondanza. Uno dei difetti della blockchain, infatti, è la lentezza nell'approvazione di un blocco: una chiamata con *fee* può richiedere anche 15-20 secondi per la sola approvazione: questo tempo aumenta con l'aumentare della complessità della funzione e con esso aumenta il costo dell'operazione. D'altra parte, però, un'eccessiva ridondanza di dati può portare inconsistenza, oltre ad essere fonte di errore nella gestione della memoria.

```
1 // Charity mapping
2 mapping(string => address) charityToAddr;
3 mapping(address => string) addrToCharity;
4 // Charities array
5 string[] charitiesArr;
6 // Mapping one charity to many projects
7 mapping(string => project[]) charitiesMap;
```

Come si può vedere, ho deciso di implementare un dizionario *two-way* ed in generale di sfruttare questo tipo di struttura, per poter accedere facilmente al nome delle associazioni e dei progetti, evitando di dover lavorare gli address in JavaScript, dove sarebbero stati più vulnerabili. Le alternative considerate sono state l'ordinamento delle associazioni man mano che vengono inserite, ma Solidity ha ancora una gestione incompleta delle stringhe

e avrebbe reso la cosa complessa, oltre che forzata in un linguaggio che non ha ancora sentito la necessità di implementare una libreria dedicata (si consideri, a titolo esplicativo, che alla versione attuale di Solidity -v0.8.17- il ritorno di un array di stringhe è in fase sperimentale). L'alternativa era la ricerca sequenziale e questa, immaginando qualche migliaio di associazioni e di progetti, è stata subito scartata. Proprio a causa di questa incompletezza nella gestione delle stringhe -nel confronto con linguaggi di programmazione più adulti come C++, Java, Python etc- anche il solo confronto tra stringhe non è semplice ed è stato implementato usando funzioni crittografiche fornite dal TeamKeccack[43].

In questa versione, inoltre, ogni associazione (dopo essere stata aggiunta dal proprietario) può liberamente aggiungere i suoi progetti. Lo *sc* controlla che non vengano usati due volte lo stesso nome o lo stesso address nella stessa associazione.

Il lato frontend è stato invece riscritto da zero e articolato in più pagine, aggiungendo il profilo dell'amministratore di un'associazione no-profit (si veda lo schema riportato in figura 4.1). Oltre al *routing*[44], questa versione raccoglie alcuni errori e li segnala all'utente, come l'assenza dell'estensione per accedere al proprio *wallet* o l'importo della donazione superiore a quanto si possiede.

A solo scopo esplicativo, si riportano qui sotto tre *snippet* dell'ultima implementazione. Il primo inizializza le variabili secondo le API di web3.js, il secondo è la richiesta a MetaMask degli account connessi e l'ultimo è la chiamata della funzione di donazione.

```
1 web3: Web3 = new Web3(Web3.givenProvider);
2 charityETH = new this.web3.eth
3         .Contract(charity_abi, contract_address);
```

```
1 this.access = await this._connectionService
2         .web3.eth.requestAccounts();
```

```
1 let weiAmount = this._connectionService.web3.utils
2         .toWei(this.data.amount);
3 this._connectionService.charityETH.methods
4         .donate(this.data.charity, this.data.project).send(
```

[43] https://keccak.team/keccak.html

[44] Il routing è, in Angular, la navigazione tra pagine.

```
5           {from: this._connectionService.access,
6            value: weiAmount});
```

Complessivamente, la web app fin qui sviluppata implementa in modo sufficientemente sicuro tutte le funzioni necessarie per l'obiettivo posto. Sono presenti altre funzioni per ulteriori sviluppi, di cui parleremo tra poco.

4.2 Analisi del progetto

4.2.1 Problemi riscontrati

I due linguaggi di programmazione usati e la struttura complessiva del progetto hanno presentato alcune difficoltà, legate alla formazione fin qui ricevuta.

La struttura del progetto

Il progetto, pur avendo dimensioni estremamente contenute, richiede un lavoro su tre fronti diversi con codici sorgente che abbisognano di un'organizzazione. Questa è stata la prima difficoltà: gestire un progetto su più fronti. Nel corso del triennio è stato raro dover affrontare progetti di queste dimensioni, che non fossero invece settorizzati, cioè concentrati su un singolo aspetto della programmazione o dell'ingegneria del software più in generale. Nel corso del tirocinio ho invece dovuto implementare la comunicazione tra MetaMask, Solidity e Angular, il tutto in un progetto complessivamente di grandi dimensioni, rispetto all'esperienza fin qui accumulata. Pur conscio che progetti simili siano la norma, anzi forse da considerarsi come piccoli progetti nell'informatica dei nostri giorni, la formazione del triennio mi ha fornito gli strumenti per affrontarlo ma non l'esperienza.

La programmazione

Dopo aver deciso di non sviluppare un backend, mi sono concentrato sullo studio di Solidity e di Angular. Il primo linguaggio, adeguatamente studiato, non ha rappresentato un ostacolo per l'implementazione: è lineare e generalmente simile alla OOP affrontata nel corso del triennio.

L'unica difficoltà è stata la gestione di un caso molto particolare: un utente che, con un *wallet* con almeno un address connesso alla web app, apra la pagine con un altro address, non connesso. Questo dovrebbe reinviare la pagina di accesso, ma non succede;

rimane l'accesso con l'ultimo address collegato. Anche confrontandomi con un dipendete dell'azienda, specializzato nelle blockchain, non ho trovato una soluzione, perché il cambio non viene in alcun modo segnalato da MetaMask e sembra quindi non sia possibile venirne a conoscenza. Il problema è comunque secondario perché si tratta solo di un cambio di address dello stesso *wallet* e si può ragionevolmente presupporre che sia posseduto da un singolo utente. Inoltre, le operazioni vengono effettuate dall'address connesso e non da quello -disconnesso- aperto in quel momento. La richiesta dei profili connessi restituisce un *array* di indirizzi, non solo l'address in quel momento aperto in MetaMask.

Un altro problema a cui non ho trovato soluzione, nemmeno dopo ricerche e confronti col team, è la maschera di collegamento con MetaMask. Essendo un'estensione del browser, è possibile attivarlo direttamente dalla sua icona. L'azione di collegamento col proprio indirizzo, invece, apre una nuova finestra. Questo può creare dei dubbi sull'autenticità dello stesso: una nuova scheda è infatti facile da replicare, rubando così i dati dell'utente. Analizzando il problema, mi sono accorto di due cose: prima di tutto il comportamento non dipende dal tipo di funzioni usate quanto piuttosto dal browser; su altri browser la stessa azione richiamava direttamente l'estensione. Il secondo aspetto che mi ha concesso di sorvolare sulla questione è che l'estensione riceve ugualmente la richiesta ed è possibile, in caso di giustificata diffidenza, chiudere la nuova scheda ed accettare il collegamento direttamente dall'estensione del browser (che, contrariamente alla finestra, non è possibile duplicare).

Con Angular e, più in generale, con i linguaggi per il frontend ho riscontrato maggiori difficoltà. TypeScript, HTML e CSS sono stati un grosso ostacolo per il raggiungimento dell'obiettivo. La loro logica è molto diversa da quella della OOP, il debugging vive principalmente nella console del browser invece che nell'IDE e in generale richiede un tipo di programmazione diverso da quello che ho potuto apprendere nel percorso di studi.

Spesso ho avuto bisogno di cercare aiuto online o nel team di sviluppatori frontend dell'azienda. Inoltre, confrontandomi con loro al termine del tirocinio, hanno confermato l'impostazione non del tutto corretta del lato frontend, in particolare riguardo le *best practice* e le scelte grafiche per la web app.

4.2.2 Punti di forza

Il principale punto di forza del progetto è stata l'azienda ospitante. Il tutor aziendale, come tutto lo staff, è sempre stato disponibile al confronto e ad aiutarmi, anche con colloqui che hanno impiegato una buona quantità di tempo. La comunicazione con il team è sempre stata veloce ed efficace, e mi ha consentito di venire a capo dei problemi, dopo essermi rivolto a loro, in modo semplice. Tutto questo in un clima sereno e con un "patto" chiaro: l'aiuto non sostituiva l'autoapprendimento, ma veniva in soccorso di problemi più complessi del previsto. Il progetto, inoltre, risponde alle esigenze presentate all'inizio dell'elaborato e si presta a mostrare un'applicazione reale anche dei criteri etici esposti.

Grazie a questo progetto ho potuto approfondire temi interessanti e in parte legati agli studi fatti, come lo sviluppo di un backend con *farmework* moderni, il frontend e la blockchain, il tutto in un ambiente di lavoro positivo e abituato alla presenza di tirocinanti. É stata particolarmente utile anche la riflessione etica, che mi ha dato l'occasione di indagare campi interdisciplinari che conoscevo ancora poco.

Da un punto di vista tecnico, infine, seppur il progetto non sia originale, le offerte simili sono ancora limitate e ho trovato particolarmente stimolante l'approfondimento di qualcosa che sta ancora muovendo i primi passi, in particolare l'uso della blockchain come backend. I *cloud* distribuiti non sono una novità, appunto, ma aver sostituito un *database* -con tutte le sue potenzialità e la sua solidità- con Ethereum è stata l'occasione per utilizzare al meglio una struttura dati che non è stata preconfezionata da decenni di studi.

4.3 Eventuali sviluppi futuri

L'intenzione è sempre stata di implementare un sistema didattico, più che professionale o destinato al grande pubblico. Questo lascia ampio margine di miglioramento. Il terzo step di cui parlavo nella sezione 4.1 ingloba tutte le possibili modifiche future. Sicuramente un primo cantiere che rimane aperto è quello grafico: avendo dovuto apprendere le basi della programmazione frontend non sono riuscito a curare maggiormente il lato visivo, che rimane carente.

L'intero progetto è stato sviluppato su Rete di test Kovan e non comunica con le altre reti. Sarebbe sicuramente uno sviluppo importante implementare la possibilità di funzionamento in due o più reti e magari anche in quella ufficiale Ethereum. A questo proposito, si potrebbe inserire il cambio da Ether a Euro (o Dollari Americani).

Ci sarebbe anche un'altra modifica molto interessante, più da un punto di vista concettuale che tecnico. Il primo progetto dell'associazione, insieme all'associazione stessa, deve essere inserito dal proprietario del contratto. Questa è di fatto una forma di centralizzazione. Sarebbe forse più corretto e coerente che ciascuno possa aggiungersi come nuova associazione e che la sua credibilità cresca in base a quanta gliene viene concessa dalla *community*.

Un'ultima implementazione per un maggiore livello di sicurezza è la limitazione dell'accesso alle pagine del proprietario del sito e degli amministratori delle associazioni no-profit ai normali utenti. Questa non è stata fatta fin da subito perchè la scelta della *landing page* è basata sull'address collegato e quindi, anche approfittando della criticità sui profili presentata prima, un utente potrebbe al massimo vedere l'interfaccia del proprietario, senza poterla usare.

Capitolo 5

Conclusioni

Gli obiettivi di questo elaborato erano principalmente due: lo sviluppo del progetto presentato e, tramite questo, un abbozzo di analisi etica della blockchain. Entrambi sono stati a mio parere raggiunti ed entrambi possono essere ulteriormente sviluppati e approfonditi.

La decentralizzazione, nodo della tecnologia in sé, è anche la questione che più di tutte rimane in sospeso. Nel progetto non è stata sviluppata la possibilità di aggiungere autonomamente la propria associazione anche per ragioni etiche: cosa accadrebbe se venisse aggiunta una finta organizzazione e la web app venisse usata come metodo di pagamento per traffici illeciti? Non avendo una registrazione necessaria, non esiste un registro centrale degli iscritti e l'unica strada percorribile è quella di leggere tutte le transazioni avvenute nello *smart contract*, cosa che sicuramente rallenterebbe le ricerche di pagamenti illeciti.

La questione che soggiace a questo quesito etico è una delle più classiche domande che si possono porre alla piramide dell'autorità: **chi controlla i controllori?**

In un sistema assolutamente decentralizzato nessuno controlla il controllore, perché non esiste un controllore; esiste però ciò che la maggioranza ritiene giusto, o quantomeno non sbagliato. Riprendendo il manuale di Foglio:

> La finanza etica intende valutare e selezionare gli investimenti anzitutto in base all'impatto sociale ed ambientale, quindi alle possibili *performance* e rese economiche. [...] [Considera quindi] il denaro come un importante mezzo per la realizzazione e la crescita dell'uomo; pertanto si propone di usarlo in modo socialmente responsabile con un preciso ordine di priorità[45].

[45] Foglio, *Eticonomia. La gestione dell'etica dell'economia, dell'impresa, del mercato, del business, della finanza, dei consumi, dell'ambiente*, p. 494.

Ciò che possa essere fonte di sviluppo o meno per l'uomo, a questo punto, diventa una scelta della maggioranza e, come spero di aver mostrato attraverso lo sviluppo del progetto e le scelte implementative che ho dovuto fare, non è una questione che possa avere una risposta banale.

Da un punto di vista tecnico, il progetto mi ha certamente permesso di imparare nuovi *framework* e linguaggi di programmazione. L'aspetto però che più di tutti reputo di vero apprendimento e crescita è quello dell'ambiente aziendale: tutto lo sviluppo si è mosso dentro un ambiente di lavoro reale, con i tempi e le necessità che questo richiede. Solo per citare alcuni esempi: non c'era un docente che avesse già fatto il mio stesso lavoro e che potesse guidarmi, ma esistevano colleghi che conoscevano i pezzi con cui comporlo, lasciando nelle mie mani lo sviluppo del quadro complessivo. Oppure, gli aspetti che venivano discussi negli incontri settimanali col tutor non erano meramente tenici, il mio studio di ciò che è necessario era il punto di partenza, non il traguardo. Gli incontri di allineamento servivano a porre questioni sull'accessibilità da parte dell'utente, sulla sicurezza, su casi limite da prevedere. Questi aspetti erano per me semi-sconosciuti e per questo l'ambiente del tirocinio è stato formativo, almeno al pari dello sviluppo in sé.

Desidero concludere con ciò che ho personalmente trovato di maggiore interesse sotto l'aspetto di sviluppo tecnologico: la possibilità, un domani, di possedere tutte le informazioni in un registro distribuito. Anche per questo ho deciso di non implementare un backend: pur con tutti i limiti già esposti, la condivisione dei blocchi potrà essere a mio avviso una vera rivoluzione tecnologica, sociale ed umana.

Fonti

Bibliografia

Foglio, Antonio. *Eticonomia. La gestione dell'etica dell'economia, dell'impresa, del mercato, del business, della finanza, dei consumi, dell'ambiente*. Franco Angeli, 2016.

Pontificio Consiglio della giustizia e della pace. *Compendio della dottrina sociale della Chiesa*. Libreria Editrice Vaticana, 2005.

Articoli

Buterin, Vidalik. *Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform*. 23 Gen. 2014. URL: https://bitcoinmagazine.com/business/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211 (visitato il 07/2022).

King, Sunny e Nadal, Scott. *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. 19 Ago. 2012. URL: https://decred.org/research/king2012.pdf (visitato il 07/2022).

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 1 Nov. 2008. URL: https://bitcoin.org/bitcoin.pdf (visitato il 07/2022).

Neitz, Michele Benedetto. *Ethical Considerations of Blockchain: Do We Need a Blockchain Code of Conduct?* 21 Gen. 2020. URL: https://sites.law.duke.edu/thefinregblog/2020/01/21/ethical-considerations-of-blockchain-do-we-need-a-blockchain-code-of-conduct/ (visitato il 08/2022).

— *The Influencers: Facebook's Libra, Public Blockchains, and the Ethical Considerations of Centralization*. 22 Nov. 2019. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3441981 (visitato il 08/2022).

Popov, Serguei. *The Tangle*. 30 Apr. 2018. URL: https://www.allcryptowhitepapers.com/iota-whitepaper/ (visitato il 08/2022).

Sharif, Monica M. e Ghodoosi, Farshad. *The Ethics of Blockchain in Organizations*. 2 Feb. 2022. URL: https://link.springer.com/article/10.1007/s10551-022-05058-5#citeas (visitato il 08/2022).

Yakovenko, Anatoly. *Solana: A new architecture for a high performance blockchain v0.8.13*. URL: https://solana.com/solana-whitepaper.pdf (visitato il 07/2022).

Sitografia

Busolli, Luca. *Blockchain e beneficenza*. 23 Dic. 2021. URL: https://affidaty.io/blog/it/2021/12/blockchain-ebeneficenza/ (visitato il 08/2022).

Frankfield, Jake. *51% Attack*. 14 Lug. 2022. URL: https://www.investopedia.com/terms/1/51-attack.asp#toc-what-is-a-51-attack (visitato il 07/2022).

Longstaff, Simon. *Blockchain: Some ethical considerations*. 16 Mar. 2019. URL: https://ethics.org.au/blockchain-some-considerations/ (visitato il 08/2022).

Orcutt, Mike. *Why it's time to start talking about blockchain ethics*. 10 Ott. 2019. URL: https://www.technologyreview.com/2019/10/10/132652/why-its-time-to-start-talking-about-blockchain-ethics/ (visitato il 08/2022).

Pagliari, Emanuele. *DAG applicato alla blockchain: la spiegazione e l'uso in IOTA*. 30 Giu. 2019. URL: https://cryptonomist.ch/2019/06/30/dag-blockchain-iota/ (visitato il 08/2022).