ELABORATO D'ESAME:
SIMPLECRYPTO

Alunno: de Cillis Mirko

Classe: 5° AI

Docente Tutor: Cirulli Nicola

Scuola: ITIS "On. Jannuzzi"

Anno Scolastico: 2020/2021

Sommario

TEMA A 3
IL CONTESTO 3
Introduzione 3
Il Progetto… 3
…e come si distingue dagli altri 4
Come funziona? 4
ANALISI DEL PROBLEMA 5
Gestione del Progetto 5
Ipotesi 6
Modello Concettuale e Logico del Database 6
Modello Concettuale 6
Modello Logico 6
Diagramma degli Strumenti 7
Protocolli e Servizi di Riferimento 8
Strumenti Utilizzati 8
Sicurezza dei Dati 9
Diagrammi delle Sequenze 10
Schermate del progetto 11
LE BLOCKCHAIN 13
Introduzione 13
Definizione 13
La Network delle Blockchain 13
Hash 14
Crittografia Asimmetrica 14
L'elemento base: i Blocchi 15
I Protocolli di Consenso 15
Proof of Work (PoW) 15
Proof of Stake (PoS) 16
Smart Contract 17
Ethereum 17
La Finanza Decentralizzata… 18
… e la Sostituzione del Sistema Centralizzato 18
Conclusioni 19
Fonti 20

TEMA A

Dato il crescente distacco sociale causato dalla pandemia in corso, il candidato sviluppi un sistema che offra la possibilità di creare occasioni di incontro, scambio di idee o ludiche al fine di offrire un'alternativa basata sulle nuove tecnologie come luogo di scambio culturale e sociale.

Analizzando la realtà di riferimento e fatte le opportune ipotesi aggiuntive ritenute interessanti, il candidato individui una possibile soluzione che a suo motivato giudizio sia la più idonea per sviluppare i seguenti punti:

1. *il progetto, anche mediante rappresentazioni grafiche, dell'infrastruttura tecnologica ed informatica necessaria a gestire il servizio nel suo complesso ed in particolare facendo riferimento ai seguenti aspetti:*
    a. *l'infrastruttura di comunicazione in termini di caratteristiche dei canali, degli apparati e dei protocolli, che permette di trasmettere le segnalazioni dei cittadini ad un sistema di gestione centralizzato;*
    b. *le caratteristiche generali dei componenti hardware e software del sistema sia a livello centrale che a livello del cittadino segnalante;*
    c. *il problema della sicurezza dei dati e della loro accessibilità;*
    d. *eventuali tecnologie che possano aiutare nello sviluppo della soluzione proposta;*
2. *il progetto della base di dati e/o dell'applicazione per la gestione delle informazioni relative agli interventi da effettuare e alle segnalazioni dei cittadini: si richiede in particolare il modello concettuale e il modello logico;*
3. *il progetto di massima del software (sito web, app, applicazione desktop), che implementi, con appropriati linguaggi a scelta lato client o lato server, un segmento significativo dell'applicazione.*

IL CONTESTO

Introduzione

Da un decennio a questa parte sta crescendo l'importanza di un nuovo tipo di moneta: le criptovalute, cioè monete virtuali utilizzate per effettuare transizioni di denaro da un conto all'altro, in modo veloce e senza provvigioni troppo onerose. Inoltre, viene garantita anche la privacy dei due interlocutori perché i conti non sono direttamente riconducibili ai proprietari. La differenza sostanziale che distingue queste valute dalle classiche è il fatto che sia decentralizzata.

Si parla infatti di finanza decentralizzata (Decentralized Finance, DeFi) in cui non c'è un sistema centrale che raccoglie e gestisce le operazioni: tutto viene regolato automaticamente da una rete di computer che salva le transazioni in blocchi di dati. La struttura dati fondamentale per la DeFi è la blockchain.

Dalla prima nascita del Bitcoin, nel 2008, sono nate tante altre criptovalute che si differenziano tra loro principalmente per servizi, sicurezza e privacy offerti. Tutte queste monete alternative al Bitcoin vengono chiamate altcoin.

Il mercato delle criptovalute cresce sempre di più: a maggio 2021, il market cap[1] del Bitcoin è di circa 1100 mld $[2], più di 700 volte il market cap di Google nello stesso periodo (1.5 mld)[3]. Il sistema decentralizzato e il valore intrinseco delle criptovalute attraggono sempre più gente, desiderosa di investire nel nuovo sistema o – più semplicemente – di speculare sull'andamento ancora molto volatile di questo mercato. Infatti, il valore delle monete virtuali non è stabilito da un ente centrale: è il mercato stesso ad apprezzarle. Ciò attrae principalmente investitori a lungo termine, chi desidera liquidare il proprio investimento dopo anni.

Il Progetto...

Per quelli che invece non vogliono mettere a rischio il proprio capitale, ma che comunque vogliono entrare nel mondo delle criptovalute, viene presentato SimpleCrypto.

Con questo servizio totalmente gratuito e open source, chiunque può tentare investimenti su qualsiasi criptovaluta desideri e simulare l'andamento del suo investimento in tempo reale. Così l'utente può mettere in pratica le conoscenze che sta acquisendo su questo mercato senza rischiare di perdere soldi per davvero.

Il servizio permette anche agli utenti di comunicare tra loro in una sezione community. Qui chiunque potrà pubblicare un post sulle proprie considerazioni riguardo il mercato o riguardo questa o quella criptovaluta.

La piattaforma è disponibile online all'indirizzo SimpleCrypto.

...e come si distingue dagli altri

Il progetto è molto simile a CryptoSpaniards, un simulatore online di investimenti in criptovalute. Le differenze sostanziali sono le seguenti:

1. SimpleCrypto ha una sezione community in cui gli utenti possono comunicare tra di loro;
2. Nella sezione community non ci saranno i "mi piace" ai post e ai commenti;
3. I dati degli utenti e i loro investimenti non sono accessibili agli altri utenti, rispetto a CryptoSpaniards;
4. Viene salvato l'andamento dei portafogli e delle criptovalute solo degli ultimi 3 giorni.

La possibilità di comunicare agevolmente con gli altri utenti della piattaforma contraddistingue SimpleCrypto dagli altri servizi.

Inoltre, a differenza di altri social, la sezione community non prevederà i "mi piace". L'obiettivo è quello di avere utenti attivi, così i partecipanti (gli utenti) possono solo lasciare commenti per i post che ritengono importanti e degni di nota. Si ottiene così una comunità di persone che dialoga attivamente, anche nel modo in cui "decide" quali possono essere i post più interessanti. I post più discussi saranno anche quelli più conosciuti. Si apriranno discussioni, anziché lasciare la parola solo a chi pubblica e limitarsi a essere d'accordo con il "mi piace".

Come funziona?

SimpleCrypto è diviso in due macro sezioni, indipendenti l'una dall'altra:

- Sezione Community, dove tutti possono condividere i propri pensieri ed idee sulle criptovalute;
- Sezione Portafoglio, in cui l'utente compra o vende criptovalute e vede l'andamento del proprio investimento.

In entrambi i casi, per poter usare la piattaforma bisogna effettuare la registrazione.

Per acquistare una criptovaluta, basta semplicemente selezionarla nel mercato e indicare l'importo, in euro, di quanto si desidera acquistare. All'utente verrà poi associato il corrispondente valore nella moneta scelta. Per esempio, se si decide di acquistare 40.000€ in Bitcoin, verrà assegnato all'utente circa 1 BTC. Il portafoglio seguirà e traccerà l'andamento delle monete scelte. Lo stesso procedimento vale per quanto riguarda la vendita di criptovalute.

Postare un messaggio nella community è semplicissimo. L'importante è che il messaggio non superi i 255 caratteri. I post possono essere commentati. Il feed della community può essere ordinato in base ai post più recenti o per quelli con più commenti.

ANALISI DEL PROBLEMA

Gestione del Progetto

Nello sviluppo del progetto informatico si è rivelato estremamente utile organizzare il lavoro per scandire le attività da svolgere in tempi prefissati. È stato quindi gestito il lavoro con il metodo Kanban per scandire in modo agile tutte le attività. In particolare, è stato usato il servizio online Trello per applicare questo metodo di project management.

In questa metodologia, gli oggetti di lavoro sono rappresentati visivamente su una lavagna Kanban (detta Kanban Board), consentendo ai membri del team di vedere lo stato di ogni lavoro in qualsiasi momento.

Tutti i compiti da svolgere vengono posti su una lavagna. Ogni compito è rappresentato da una card e le card vengono suddivise in più colonne in base allo stato di avanzamento di quella task. Per questo progetto, nella lavagna Kanban ci sono le colonne:

- ToDo: è la lista di tutte le attività che devono ancora essere prese in carico. È una lista di tutte le cose da fare per il progetto;
- Current Sprint: è una lista ridotta di cose da fare in un certo lasso di tempo. Vengono prese alcune delle attività dalla lista ToDo, e queste devono essere portate a termine entro una certa scadenza;
- Doing: sono le attività su cui si sta lavorando in questo momento. Devono essere al massimo 2, per non poter lavorare su più cose contemporaneamente;
- Done: sono le attività definitivamente completate.

Nella lista ToDo possono essere aggiunte continuamente card in base alle esigenze: altre funzionalità, correzioni di bug, perfezionamenti di alcune parti del progetto.

Infatti, con le lavagne Kanban risulta molto semplice monitorare visivamente lo stato e l'avanzamento delle attività.

Nella figura 1 un esempio della lavagna Kanban durante lo sviluppo del servizio.

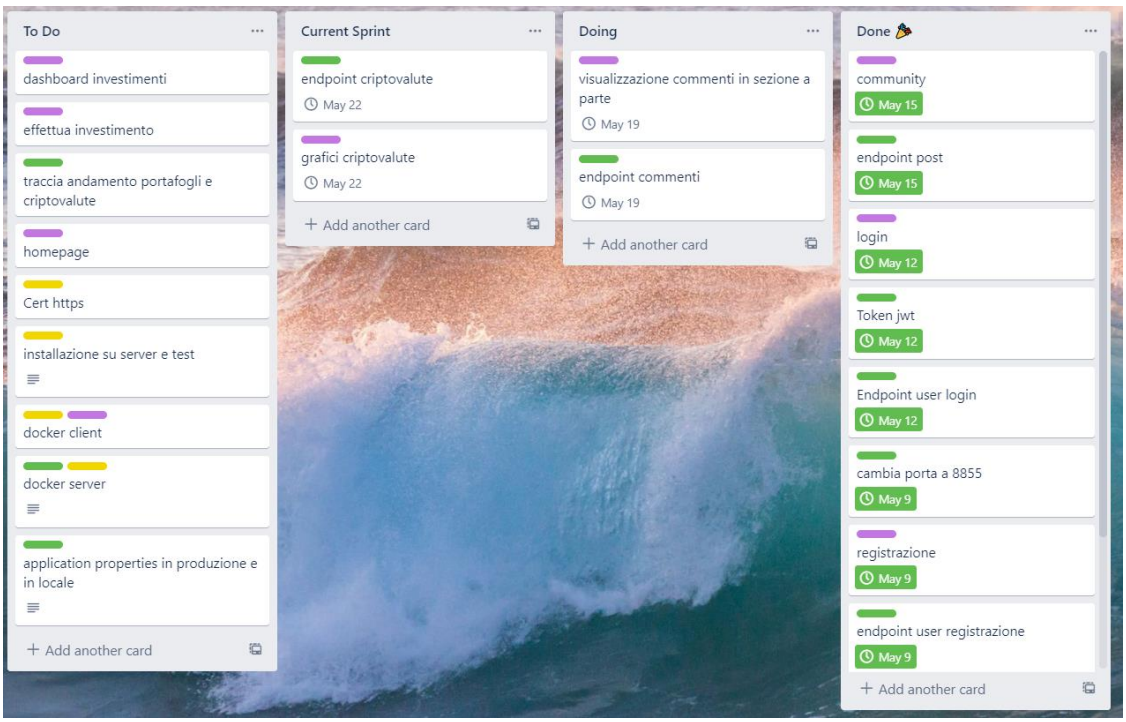


Figura 1

SimpleCrypto è suddiviso in tre progetti:

- Lato Server[4]: scritto in Java, con framework Spring, serve a elaborare le richieste dell'utente e a gestire le connessioni al server;
- Lato Client[5]: scritto in JavaScript, con framework React, per l'interfacciamento user friendly all'utente;
- Orchestrator[6]: permette di far comunicare il client con il server sul sito online e di aggiungere i certificati per la connessione sicura HTTPS.

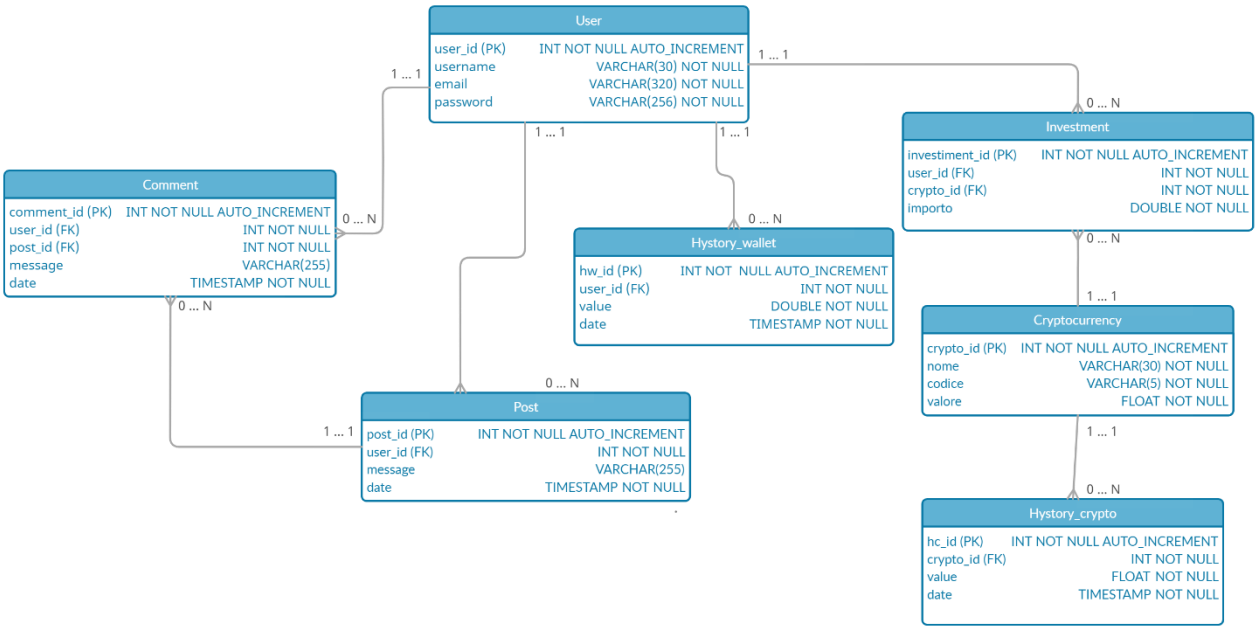
I codici di entrambi i progetti sono open source e consultabili online su GitHub.

Ipotesi

- Ci sarà un numero limitato di criptovalute disponibili all'acquisto;
- I valori degli investimenti degli utenti e l'andamento delle criptovalute verranno salvati nel DB per 3 giorni;
- Non c'è limite al numero di post e commenti;
- La tabella *Cryptocurrencies* contiene il valore attuale della moneta; quando viene aggiornato il valore viene copiato in *Hystory_Crypto* con la relativa data;
- Periodicamente, vengono prelevati da una API i prezzi delle criptovalute per aggiornare Cryptocurrencies. Nello stesso momento, viene calcolato il valore del portafoglio di ogni singolo utente e salvato in Hystory_wallet con la data in cui sono stati aggiornati;
- L'investimento in una criptovaluta da parte di un utente non sarà la somma di più righe, ma verrà aggiornato il dato creato al primo investimento.

Modello Concettuale e Logico del Database

Modello Concettuale



Modello Logico

Tabella	Attributi	Chiavi	Tipo
User	user_id	PK	int not null auto_increment
	username		varchar (30) not null
	email		varchar (320) not null
	password		varchar (256) not null
Investment	investment_id	PK	int not null auto_increment
	user_id	FK	int not null
	crypt_id	FK	int not null
	importo		double not null
Cryptocurrency	crypto_id	PK	int not null auto_increment

	nome		varchar (30) not null
	codice		varchar (5) not null
	valore		float not null
Hystory_crypto	hc_id	PK	int not null auto_increment
	crypto_id	FK	int not null
	value		float not null
	date		timestamp not null
Hystory_wallet	hw_id	PK	int not null auto_increment
	user_id	FK	int not null
	value		float not null
	date		timestamp not null
Post	post_id	PK	int not null auto_increment
	user_id	FK	int not null
	message		varchar (255) not null
Like_post	lp_id	PK	int not null auto_increment
	user_id	FK	int not null
	post_id	FK	int not null
Comment	comment_id	PK	int not null auto_increment
	post_id	FK	int not null
	user_id	FK	int not null
	message		varchar (255) not null
Like_Comment	lc_id	PK	int not null auto_increment
	user_id	FK	int not null
	comment_id	FK	int not null

Diagramma degli Strumenti

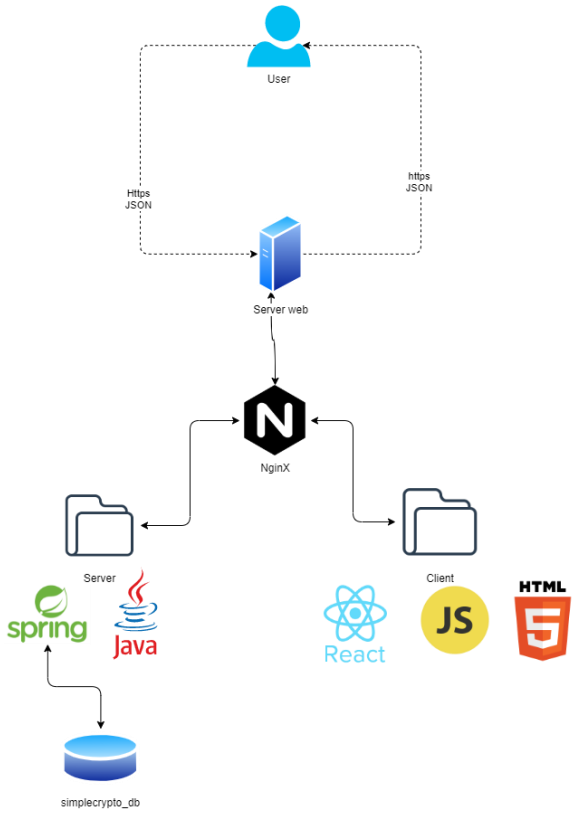


Figura 2

Il servizio si compone di un lato client e uno server. Il lato server, gestito con il framework Java Spring, consente di gestire le richieste al DB e restituisce le informazioni richieste. Su Spring vengono dichiarati e gestiti gli endpoint dell'API. Il client è semplicemente una interfaccia grafica semplificata all'API, creata usando il framework JavaScript React. Le chiamate al server vengono gestite dal web server Nginx. Il modo in cui ogni parte comunica con gli altri viene mostrata graficamente nella figura 2.

Tutti gli strumenti e i servizi sul server sono gestiti e installati con Docker. Questo sistema automatizza il deployment (implementazione) delle applicazioni in modo semplice e veloce, senza la necessità di una Virtual Machine.

Protocolli e Servizi di Riferimento

La trasmissione delle pagine del sito si baseranno sul protocollo HTTP, usato proprio per questo tipo di comunicazioni. Necessariamente, la trasmissione di dati (il login o l'invio di un post) e la ricezione dei dati (valori delle criptovalute, post nella community) verranno gestite con i metodi http:

- POST per l'invio di nuovi dati, per esempio la registrazione di un nuovo utente;
- PUT per l'aggiornamento di dati nel database, ad esempio nel caso in cui si voglia aggiornare l'importo di un investimento;
- GET per la ricezione dei dati, ad esempio i post della community.

La connessione sicura al sito viene accertata dal tool open source gratuito Certbot che genera certificati per abilitare l'HTTPS sui siti online.

Per ottenere i cambi di valuta delle criptovalute vengono chiamati i dati dalla API dalla piattaforma di scambio criptovalute Binance.

Strumenti Utilizzati

Per il lato client è stato utilizzato il framework di JavaScript React. la gestione del server e delle chiamate al database è stata scritta in Java con il framework Spring.

Il database è gestito dal DBMS MySQL. In particolare, il framework Spring permette di creare molto facilmente le tabelle definendo le entità con delle semplici classi. Ad esempio, il codice per definire l'entità degli utenti è:

```
1.
2.  @Entity
3.  public class User {
4.      @Id
5.      @GeneratedValue (strategy = GenerationType.AUTO)
6.      private Integer id;
7.
8.      @NotEmpty
9.      @Column (length = 30, nullable = false)
10.     private String username;
11.
12.     @NotEmpty
13.     @Column (length = 320, unique = true, nullable = false)
14.     private String email;
15.
16.     @NotEmpty
17.     @Column (length = 60, nullable = false)
18.     private String password;
19.
20.     ...
21.
22. }
23.
```

Così definisce l'entità *user* con gli attributi:

- *id* integer not null auto_increment;
- *username* varchar(30) not null;
- *email* varchar(320) not null unique;
- *password* varchar(60) not null.

Anche per quanto riguarda le query, Spring offre una interfaccia semplificata. Anziché scrivere a mano ogni singola query, permette di crearle agilmente semplicemente in base al nome del metodo che si va a dichiarare.

```
1.
2.  public interface UserRepository extends CrudRepository<User, Integer> {
3.
4.      User findByEmail(String email);
5.
6.      User findByUsername(String username);
7.  }
8.
```

Questa interfaccia definisce due funzioni:

- *findByEmail* con cui si ottiene l'utente corrispondente alla mail passata come parametro;
- *findByUsername* con cui si ottiene l'utente corrispondente all'username passato come parametro.

Ad esempio, il calcolo per determinare l'andamento dell'investimento di un utente in un dato momento, verrà facilmente gestito con Spring. Piuttosto che usare una query come:

```
1.
2.  INSERT INTO hystory_wallet (user_id, date, value)
3.  VALUES (1, CURDATE(),
4.    (SELECT SUM(C.value * I.importo)
5.    FROM investment I INNER JOIN cryptocurrency C ON I.crypto_id = C.id
6.    WHERE I.user_id = 1)
7.  );
8.
```

Viene scritto molto più semplicemente – calcolando in un colpo solo l'andamento di tutti gli utenti – in codice Java:

```
1.
2.  ...
3.  users.forEach(user -> {
4.      final float[] current_wallet = {0};
5.      user.getInvestments().forEach(investment -> {
6.          current_wallet[0] += investment.getImporto() *
    investment.getCryptocurrency().getValore();
7.      });
8.      HistoryWallet hw = new HistoryWallet(user, current_wallet[0]);
9.      historyWalletService.save(hw);
10. });
11. ...
12.
```

Infine, c'è da implementare il sistema per aggiornare il valore delle criptovalute ogni 5 minuti. I dati vengono chiamati dal lato server verso una API esterna di Binance. Affinchè questa cosa venga gestita automaticamente dal server, viene chiamato un servizio che, periodicamente, preleva i dati dalla API, aggiorna quelli attuali nel server e rimuove quelli più vecchi di 3 giorni.

```
1.
2.  @Scheduled(fixedRateString = "300000")
3.  public void getCryptoValues() {
4.      utils.updateValues();
5.  }
6.
```

Sicurezza dei Dati

La prima misura preventiva considerata prevede la protezione dei dati sensibili dell'utente. Cifrare la password è estremamente importante per garantire la sicurezza di chi fa uso della piattaforma.

La password viene cifrata con il metodo bcrypt. Questa funzione di hashing si basa innanzitutto sull'aggiunta di un salt, ovvero un additivo casuale alla password vera e propria, così da rendere l'hash diverso anche con la stessa stringa. Un esempio di hash bcrypt è:

```
$2a$10$N9qo8uLOickgx2ZMRZoMyeIjZAgcfl7p92ldGxad68LJZdL17lhWy
```

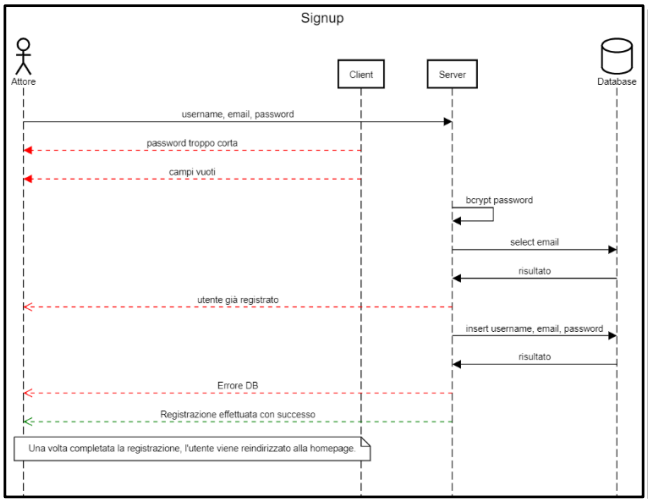
Dove:

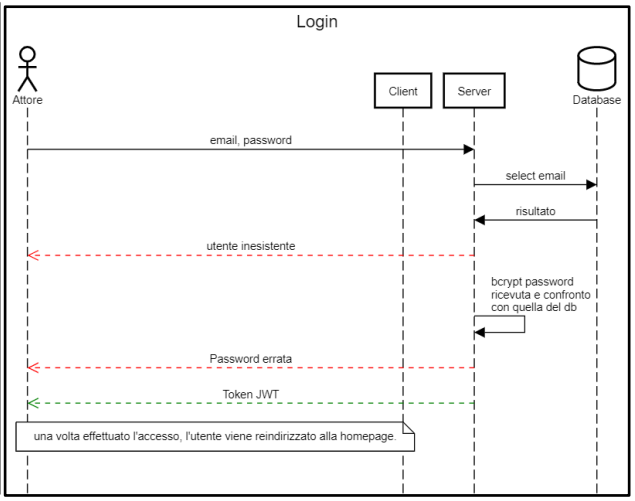
- `$2a$` indica che è stato utilizzato la funzione bcrypt;
- `10$` è il costo. Se il costo aumenta, la velocità di creazione dell'hash diminuisce, ma anche la velocità a cui gli hacker possono indovinare la password diminuisce;
- `N9qo8uLOickgx2ZMRZoMye`, ovvero i 22 caratteri successivi, è il sale di 128 bit;
- `IjZAgcfl7p92ldGxad68LJZdL17lhWy`, i restanti 31 caratteri, è il valore dell'hash risultante di 184 bit.

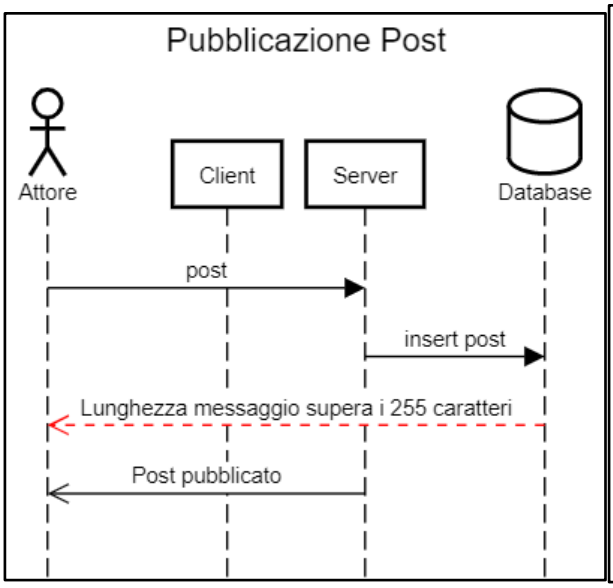
Quando l'utente tenta di accedere, viene usato un metodo apposito che preleva il sale dalla password salvata nel database e la usa per cifrare la password inserita in fase di accesso. Se i due hash corrispondono, la password è corretta.

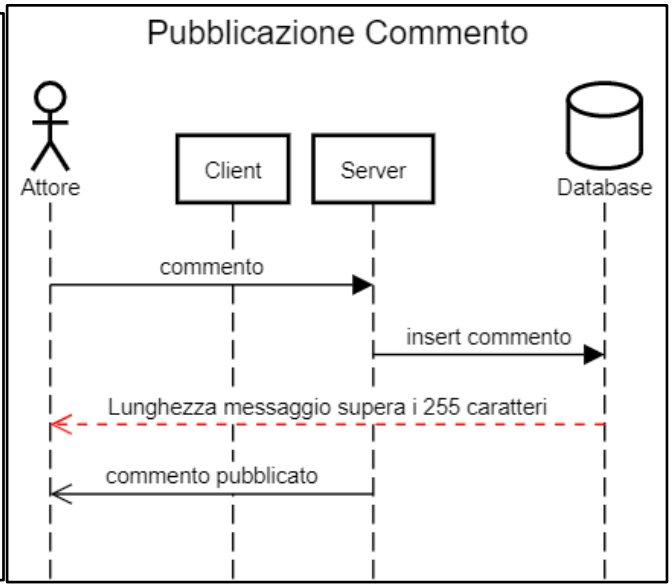
Un altro aspetto importante per la sicurezza del servizio è la protezione dell'accesso alle API. Per esempio, solo alcune api sono pubbliche e accessibili da tutti. Se voglio pubblicare un post devo essere registrato: quindi l'endpoint API per pubblicare un post non deve essere pubblica. Per risolvere questo aspetto, viene aggiunto all'header della chiamata al server l'intestazione "X-Auth" in cui viene passato il token JWT ricevuto in fase di login. Solo se il token è valido e non è scaduto il server elabora la richiesta.

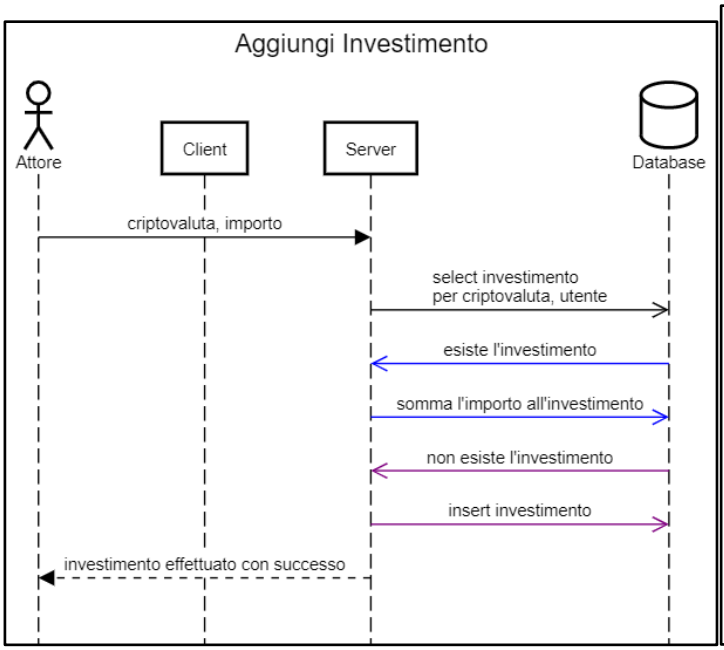
Diagrammi delle Sequenze

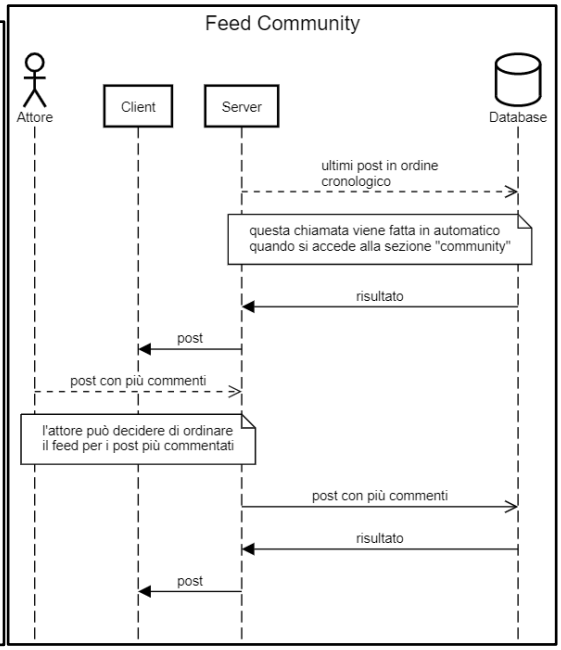






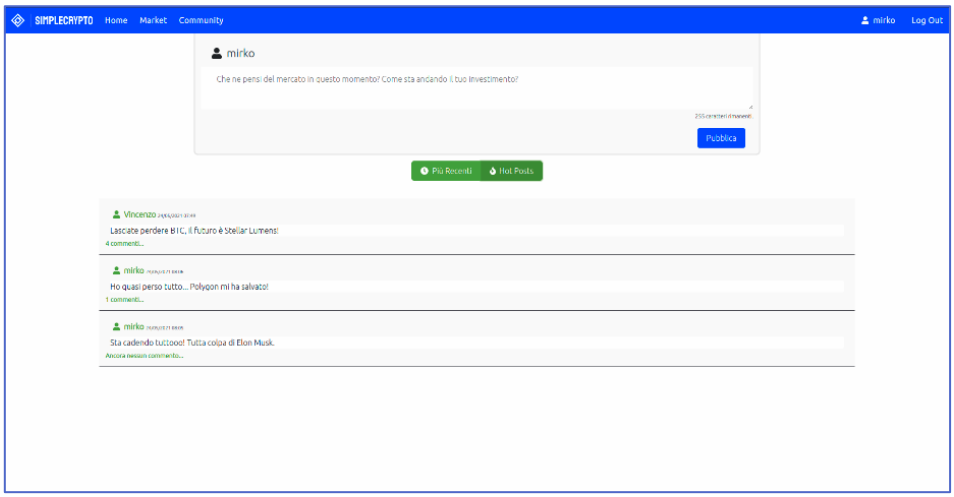




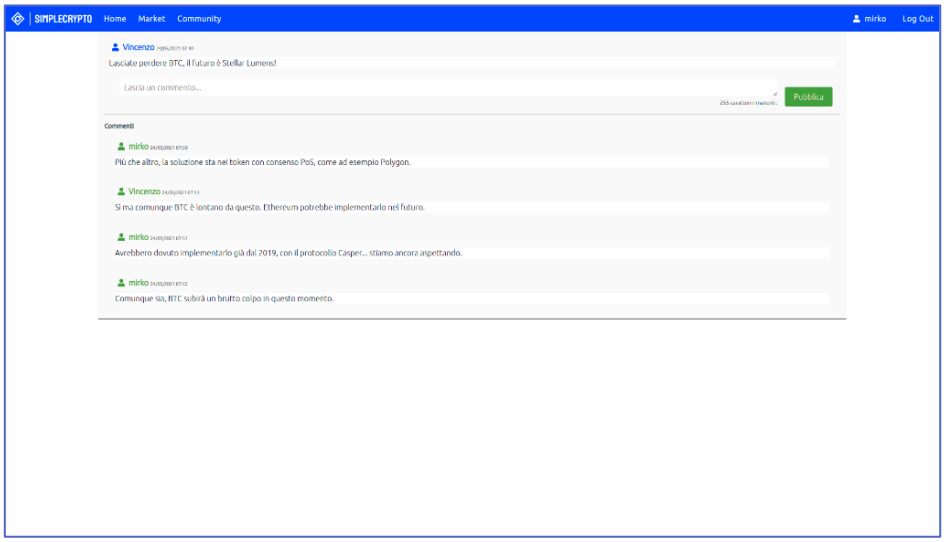


Schermate del progetto

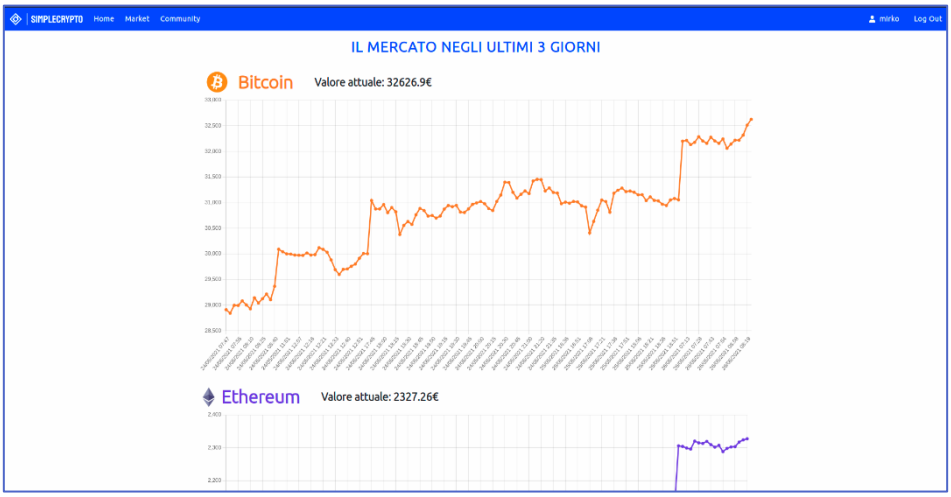
Sezione Community



Commenti sotto un post



Mercato negli ultimi giorni



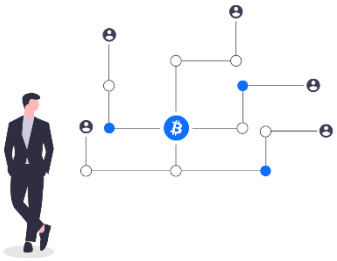
Investimento dell'utente

LE BLOCKCHAIN

Introduzione

Spesso la blockchain viene anche nominata "l'internet del futuro", perché è possibile creare applicazioni e sistemi decentralizzati, in cui non c'è un unico server che immagazzina i dati e gestisce gli accessi, ma al suo posto c'è una rete di computer che ha lo stesso onere.

Questa neonata tecnologia sta iniziando a prendere piede in molti settori, dalla finanza all'industria, dalle valute alla creazione di applicazioni fino al finanziamento di progetti innovativi. Il sistema ha tutte le carte in regola per introdurre un nuovo modo in cui possono essere realizzate le applicazioni.



Oltre alla decentralizzazione dei dati, un'altra importante ragione che ha determinato la nascita delle blockchain è stata la ricerca di un sistema libero dai condizionamenti e dagli errori umani. I computer all'interno di una rete blockchain si limitano a seguire le regole imposte dal sistema, eliminando del tutto fattori di rischio come la corruzione o la mancanza di imparzialità nelle scelte effettuate.

La blockchain è stata implementata per la prima volta nel 2008, con la pubblicazione del Bitcoin. Il suo primo impiego è stato come piattaforma per lo scambio di denaro tra utenti in maniera veloce, con commissioni basse e senza passare per un ente centrale, come una banca che trasferisce i soldi dal conto del mittente a quello del destinatario.

Definizione

Come riportato da *Blockchain. Tecnologia e applicazioni per il business*, uno dei libri su cui è fondata questa parte dell'elaborato (il libro è nominato alla lettera b delle fonti):

> *"La blockchain è un libro mastro (ledger) decentralizzato, strutturato come una catena di registri responsabili dell'archiviazione dei dati.*
>
> *Non è possibile modificare o rimuovere blocchi precedentemente aggiunti alla catena.*
>
> *In questo ecosistema, la crittografia e i protocolli di consenso garantiscono sicurezza e immutabilità.*
>
> *Il risultato è un sistema aperto, neutrale, affidabile e sicuro, dove la capacità di avere fiducia nel sistema non dipendono dalle intenzioni di nessun individuo o istituzione."*

Si può intuire come, stando alla definizione data, si tratta di una struttura dati immutabile e, a tal proposito, bisogna fare un distinguo.

La blockchain viene vista come un ledger digitale, in italiano "libro mastro". Un ledger è uno strumento utilizzato per registrare transazioni. Questo però lo distingue da un database: seppur entrambi vengono utilizzati per salvare i dati, mentre nel database è possibile inserire, cancellare e aggiornare dati, in un ledger si possono solo aggiungere informazioni.

Fatta questa distinzione, è chiaro che le blockchain non potranno rimpiazzare i database tradizionali. Questo perché i dati nel database possono essere modificati, a differenza della blockchain. Le due strutture dati sono state pensate per affrontare problematiche differenti.

La Network delle Blockchain

Un sistema, per essere decentralizzato come appena descritto, deve esserlo anche a livello fisico: la blockchain deve essere distribuita su una rete di macchine interconnesse.

Una blockchain è una rete peer-to-peer (P2P). Questo significa che:

- Tutti i nodi della rete sono ritenuti alla pari;
- Si ottiene un sistema decentralizzato, in cui le risorse sono distribuite. Se uno o più nodi vengono spenti, il sistema continua comunque a funzionare e ad offrire il servizio.

Hash

Un fattore determinante della sicurezza nelle blockchain, così come per la sequenzialità dei blocchi, è la funzione hash. Questa permette di creare un legame tra due blocchi consecutivi. Il suo ruolo nella blockchain verrà spiegato successivamente.

Viene usata per mappare dati di dimensione variabile in dati di dimensioni fisse. Una delle più usate è la funzione SHA256. Quello che rende importante queste funzioni è che:

- Lo stesso input genera sempre lo stesso output;
- Una minima variazione nell'input cambia drasticamente l'output;
- È una funzione unidirezionale: nonostante sia relativamente facile per un computer calcolare l'hash di un dato input, è invece molto complicato ottenere l'input a partire dall'hash.

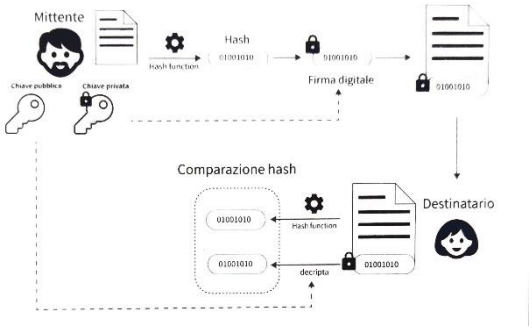


Figura 3

Con le funzioni hash vengono generate le cosiddette impronte digitali di un documento. Possono essere usati come prova del fatto che il documento non sia stato modificato: basta confrontare l'hash salvato con l'hash calcolato dal documento. Se i due hash combaciano, allora il documento si può ritenere valido e non corrotto. Nella figura 3 viene mostrato il meccanismo appena spiegato.

Crittografia Asimmetrica

Per comunicare nella rete è importante mantenere la segretezza dei messaggi trasmessi; devono essere quindi cifrati, ovvero trasformati in messaggi non comprensibili se non si conosce la chiave di lettura. Con alcune algoritmi di cifratura è possibile identificare il mittente oppure fare in modo che solo il destinatario sia in grado di leggere il messaggio decifrato. Per assicurare questo si usa la crittografia asimmetrica. Questo metodo di crittografia prevede l'utilizzo di due chiavi, in relazione matematica tra di loro:

- Chiave pubblica, che può essere condivisa con chiunque;
- Chiave privata, che deve rimanere segreta e non deve essere comunicata in rete.

I metodi di crittografia asimmetrica si basano sul fatto che è facile calcolare la chiave pubblica a partire da quella privata, quando viene generata la coppia di chiavi, ma lo stesso non vale nel momento in cui si conosce solo la chiave pubblica.

Senza entrare nel dettaglio del funzionamento di questi algoritmi, c'è da aggiungere che, oltre a quello che è stato spiegato riguardo l'impronta digitale di un documento, questo sistema di cifratura consente di assicurare l'identità del mittente: si tratta della firma digitale, che ha lo stesso significato della firma scritta a mano.

Gli utenti di una blockchain di monete digitali sono identificati da degli indirizzi. Un indirizzo non contiene criptovalute, ma è solo la destinazione o il mittente di una transazione. Il saldo collegato all'indirizzo viene calcolato a partire da tutte le transazioni registrate nella blockchain che coinvolgono quell'indirizzo.

Questo identificativo si ottiene secondo alcuni procedimenti matematici, a partire dalla coppia di chiavi asimmetriche:

1. Viene generata una chiave privata a partire da un numero casuale;
2. Dalla chiave privata si ottiene quella pubblica tramite un processo matematico;

3. La chiave pubblica passa attraverso alcuni algoritmi crittografici (principalmente di hash) per ottenere un indirizzo nella blockchain.

Con le criptovalute, le transazioni vengono gestite proprio con la chiavi asimmetriche: il mittente "firma" con la chiave privata la transazione a favore del destinatario; il destinatario potrà convalidarlo usando la chiave pubblica del mittente. Entrambi sono identificati dai rispettivi indirizzi.

L'elemento base: i Blocchi

I blocchi sono strutture dati aggiunti alla blockchain in modo sequenziale. Ogni blocco contiene una prova matematica, generalmente un hash, che ne assicura la successione al blocco precedente. Come mostrato nella figura 4, un blocco contiene i dati che deve immagazzinare e l'hash del blocco precedente. L'hash crea un collegamento inequivocabile tra il blocco corrente e quello che lo precede.

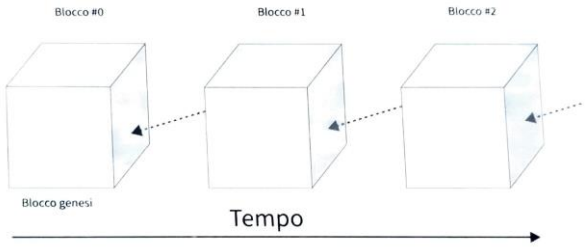


Figura 4

Per ogni nuovo blocco generato, l'hash del blocco precedente viene aggiunto all'input per calcolare l'hash del nuovo blocco. Quindi, se qualcuno tentasse di modificare o rimuovere delle informazioni all'interno di un blocco qualsiasi, finirebbe per ricalcolare l'hash che risulta da quel blocco, così come per tutti quelli successivi.

I Protocolli di Consenso

In una blockchain di cui chiunque può far parte, è impossibile fidarsi di ognuno dei nodi. "Fidarsi" vuol dire, in questo caso, dare per scontato che un blocco sia sicuro e non corrotto. Le reti blockchain si dicono infatti Trustless, non perché non si fidino tra di loro, ma perché è inequivocabile il modo in cui interagiscono.

Per determinare cosa è successo nella blockchain, ovvero qual è la sequenza di blocchi ritenuta valida, si procede attraverso un processo chiamato consenso. Questo è un accordo su ciò che è accaduto nella blockchain e deve essere raggiunto da tutti i nodi, i quali hanno ognuno lo stesso potere decisionale.

I nodi che aggiungono blocchi e garantiscono la validità delle transazioni sono i cosiddetti miner. Il mining consiste proprio in questo:

- Verificare che le transazioni siano valide;
- Raggruppare in blocchi le transazioni e verificare che il blocco ottenuto sia valido;
- Propagare i blocchi nella rete e aggiungerli alla catena di blocchi.

Con questo processo viene raggiunto il consenso distribuito e viene garantita la sicurezza del network.

Ci sono diversi algoritmi per raggiungere il consenso. I principali sono il Proof of Work (PoW) e il Proof of Stake (PoS).

Proof of Work (PoW)

Questo protocollo si basa sulla ricerca di un numero computazionalmente difficile da trovare ma, una volta trovato, risulta facile per gli altri nodi verificarne la correttezza. Il PoW si basa su algoritmi hash.

I miner competono tra di loro per risolvere un problema matematico complesso (un hash vincolato, che ad esempio deve iniziare con 19 zeri). L'unico modo per trovare una soluzione valida consiste nel provare tutte le combinazioni di input finché non si trova quella giusta. L'input della PoW deve essere il blocco precedente; per

ogni tentativo cambia il valore di un numero, il nounce, che viene aggiunto all'input dell'algoritmo per ottenere un risultato diverso.

Nel momento in cui un miner trova la soluzione e gli altri nodi la verificano, il miner si aggiudica il blocco e la ricompensa e il blocco viene aggiunto definitivamente nella blockchain.

La ricompensa è fondamentale per la blockchain, seppur in modo indiretto: incentiva i miner a generare nuovi blocchi e a mantenere il network sicuro. Il miner che crea un nuovo blocco viene ricompensato con tutte le commissioni delle transazioni contenute nel blocco più le monete messe in circolazione insieme al blocco.

PoW: Pro

Il vantaggio principale che si ottiene da questo algoritmo è l'immutabilità assicurata dalla difficoltà di modificare una transazione già registrata.

Se un malintenzionato vuole modificare una transazione inclusa in un blocco, deve essere in grado di ricalcolare la Proof of Work per tutti i blocchi seguenti prima che altri miner ne aggiungano un altro. Ad esempio, se l'utente deve manomettere una transazione avvenuta 8 blocchi prima, deve ricalcolare il PoW dei 7 blocchi successivi molto velocemente; dovrebbe avere una incredibile potenza di calcolo per far ciò.

PoW: Contro

- A causa dell'immensa potenza di calcolo necessaria per il PoW, c'è un enorme consumo di energia da parte di queste reti. Solo il Bitcoin consumava, nel 2018, lo 0.3% dell'elettricità mondiale[b].
- Questo sistema è difficile da scalare e ciò va a gravare sulla lentezza delle transazioni e le commissioni sempre più elevate;
- Le blockchain basate sul PoW sono vulnerabili a un attacco del 51%. Se un miner ottiene almeno il 51% della potenza di calcolo del network, sarebbe in grado di creare blocchi più velocemente rispetto alla parte restante. Questo significa che può modificare alcune transazioni e comunque salvare il blocco passando per valido. Nonostante questo, l'utente maligno non sarebbe comunque in grado di modificare vecchie transazioni.

Proof of Stake (PoS)

Rispetto al PoW che si basa sulla risoluzione di problemi matematici, nel protocollo Proof of Stake la creazione di un nuovo blocco viene affidata a un validator. Il validator viene scelto in anticipo in base alla quantità di criptovalute da loro possedute, definita come stake.

Nel PoS-mining non viene considerata la potenza di calcolo di un nodo, come nel PoW, bensì la quantità di token posseduti. Un utente può "puntare" i propri token per avere il diritto di confermare le transazioni di un blocco e ricevere la ricompensa. Lo staking consiste nel bloccare temporaneamente i propri token fino a quando non si conclude il processo di staking, ovvero la creazione e validazione di nuovi blocchi.

Se un utente malevolo coglie l'occasione nell'essere un validator per aggiungere informazioni false, sarà possibile risalire al malintenzionato e penalizzarlo intaccando il suo stake, quindi sottraendogli token.

Il protocollo è comunque equo nel confronto degli utenti: tutti hanno la possibilità di essere validator in base alla quantità di token posseduti rispetto al totale. Se un utente possiede il 5% del totale dei token della blockchain, avrà il diritto a essere un validator il 5% delle volte.

PoS: Pro

- Rispetto al PoW, richiede molta meno potenza di calcolo perché non c'è bisogno di fare calcoli complessi per salvare un blocco;
- È comunque a rischio attacco del 51%, ma l'attacker deve possedere almeno il 51% dei token. In una condizione del genere, l'utente maligno è meno incentivato ad attaccare. Infatti, il valore dei token da lui posseduti scenderebbe, causandogli una perdita significativa. Così non gli conviene attaccare la blockchain;

- È più economico in confronto al PoW in termini di costi per l'elettricità e per l'hardware. Di conseguenza, chiunque può entrare a far parte di una network con consenso PoS.

Smart Contract

Mettiamo caso di voler avviare una campagna di crowdfunding online: ci sarebbe bisogno di creare un sistema nel quale si propone il progetto da finanziare, una somma da raggiungere e una data entro la quale raggiungerla. Se la somma non viene raggiunta in tempo, il finanziamento viene annullato e i soldi dei benefattori vanno restituiti. Se invece si raggiunge la soglia in tempo, i soldi vengono sbloccati e dati al creatore del progetto, che potrà così iniziare a svilupparlo.

Per farlo, al giorno d'oggi, ci sono molte soluzioni, tra cui KickStarter, che fanno da intermediari tra ideatore e finanziatori. Il problema sta proprio nel modo in cui possono agire gli intermediari: bisogna in pratica fidarsi di loro. I rischi possono essere i seguenti:

- Si comporta in modo malevolo, chiudendo la piattaforma con i soldi del nostro progetto ancora bloccati;
- Possono essere attaccati da hacker;
- Sono lenti e costosi.

A tal proposito sono stati introdotti gli Smart Contract. L'obiettivo degli smart contract è proprio quello di sottoscrivere un contratto e di soddisfarne le condizioni in modo automatico, minimizzando i rischi descritti precedentemente.

Per fare un altro esempio, gli smart contract vengono usati anche con le criptovalute. In questi contratti vengono definite le modalità con cui si trasferiscono monete da un conto all'altro, come viene calcolato il saldo di un conto e viene anche tenuto il conto delle monete in circolazione.

Questo tipo di contratto viene salvato e mandato in esecuzione nelle blockchain. Il meccanismo di consenso della blockchain vincola il contratto e assicura che venga rispettato. Nel momento in cui le condizioni del contratto vengono rispettate, lo smart contract esegue automaticamente delle azioni specifiche; nel caso del crowdfunding, provvederà immediatamente a trasferire i soldi sul conto dell'ideatore del progetto. Lo smart contract stesso provvederà a inviare o restituire i soldi, senza che ci si affidi a terzi.

Nelle blockchain, gli smart contract sono legati al concetto di token, che rappresentano una risorsa all'interno della blockchain. Questa risorsa può essere qualsiasi cosa, come un mezzo di scambio di valore (coin), per ottenere diritti di utilizzo di un servizio, per entrare a far parte di una società, e tanti altri utilizzi.

Ethereum

Sulle potenzialità di questo strumento si basa la blockchain Ethereum. L'idea alla base di Ethereum è proprio quella di creare una blockchain che potesse eseguire programmi generici, come se tutta la rete che si viene a creare fosse un computer globale dove i programmi vengono eseguiti in modo decentralizzato.

In Ethereum ci sono degli standard che identificano alcune funzionalità degli smart contract: in questo modo, si possono creare molto più facilmente le applicazioni, perché viene già definito cosa è necessario. Questi standard vengono chiamati Ethereum Request for Comment (ERC). Gli standard principali sono ERC 20 e ERC 721.

Standard ERC 20

Questo standard è quello usato principalmente per creare token in Ethereum. È lo standard di riferimento per creare criptovalute basate su Ethereum. Uno smart contract che implementa questo standard deve includere almeno le funzioni definite dallo standard, tra cui:

- Total supply: una funzione che definisca il numero totale di token in circolazione;
- Balance of: una funzione che definisca i token posseduti da un indirizzo (il saldo di un conto);
- Transfer: una funzione per trasferire i token da un indirizzo a un altro.

Standard ERC 721

Questo standard viene implementato per descrivere la funzionalità di token non fungibili (in inglese Non Fungible Token, NFT). Il concetto di fungibilità è correlato a quello di interscambio. Una banconota da 10€ è perfettamente interscambiabile con un'altra da 10€; lo stesso oggetto ha lo stesso valore. Ma questa cosa non vale nella valutazione degli immobili: ogni casa o terreno ha una estensione diversa, caratteristiche diverse, si trova in condizioni diverse, ecc. Questo significa che non si può sostituire una casa con un'altra, ognuna ha la sua peculiarità.

La creazione di NFT permette di trasportare il concetto di unicità anche nel mondo dei beni digitali. La NBA sta applicando questo concetto vendendo video di highlights delle partite di basket. La piattaforma NBA Top Shot consente di comprare, vendere e scambiare questi video, detti "moments". L'unicità dei moments è assicurata proprio dai NFT collegati a essi: a ogni video corrisponde un token che ne assicura la rarità. Infatti questi token vengono prodotti in modo limitato e la scarsità dei beni digitali è sempre verificabile grazie alla blockchain.

Chi possiede il token sa di avere l'unica copia "originale" e immutabile, proprio perché scritta per sempre nella blockchain.

La stessa cosa sta avvenendo anche con l'arte e la vendita di "quadri digitali" resi unici grazie alla NFT. Si tratta della NFT Art. Sarebbe come avere il quadro della Gioconda oppure vederlo in una immagine al computer, solo che anche la versione originale è digitale. Ad esempio, attraverso questo meccanismo il famoso meme di Internet Nyan Cat è stato venduto all'asta per mezzo milione di dollari.

La Finanza Decentralizzata…

Quando si parla di blockchain, si pensa subito al sistema delle criptovalute e dello scambio di monete che ne deriva. Nonostante sia solo uno dei possibili impieghi di questa struttura dati, rimane tra le più importanti e rivoluzionarie. Stiamo parlando della Decentralized Finance – DeFi – e non è basata su un sistema centrale che controlla le transazioni; tutto è gestito automaticamente dalla rete di computer che salva i dati nella blockchain.

La DeFi altro non è che una rete P2P di macchine che scrivono le transazioni nella blockchain. Come spiegato precedentemente, questa struttura rende impossibile modificare blocchi precedenti, per cui è assicurata la sicurezza dei dati salvati. Le transazioni, le operazioni e i blocchi vengono calcolati e controllati a fondo prima di essere aggiunti alla catena, così da non aggiungere transazioni malefiche o inconsistenti. Chi registrerà la transazione nella blockchain avrà il compito di calcolare e scrivere il saldo risultante.

Inoltre, le transazioni che avvengono in una blockchain hanno commissioni molto inferiori a quelle di una banca. Per trasferire i Bitcoin, ad esempio, si può pagare una tassa che nel peggiore dei casi può ammontare a 10 centesimi. Non importa l'ammontare del trasferimento: la commissione è in un certo senso una ricompensa per chi registrerà la transazione; più è alta la provvigione, prima verrà salvata la transazione.

Tutte le operazioni che richiedevano un ente centrale adesso possono operare senza di essa. La sicurezza del proprio conto e la verifica delle transazioni sono affidati ai proprietari dei conti. E non solo: tutto questo avviene abbattendo i tempi e i costi dei trasferimenti.

… e la Sostituzione del Sistema Centralizzato

Come dice Satoshi Nakamoto, il creatore del Bitcoin:

> *"Il problema alla base delle valute convenzionali è dovuto alla quantità di fiducia necessaria per far funzionare il sistema. Dobbiamo fidarci del fatto che le banche non svalutino la moneta, ma purtroppo la storia è piena di momenti in cui questa fiducia non è stata rispettata.*
>
> *Dobbiamo fidarci del fatto che le banche conservino i nostri soldi, ma spesso sono scoppiate bolle legate al credito bancario, e solo una frazione dei soldi era effettivamente in possesso*

della banca. Dobbiamo riporre in queste istituzioni la nostra fiducia in termini di privacy, e fidarci del fatto che i ladri d'identità non svuotino i nostri conti correnti."

Non si può sicuramente mettere in discussione l'affidabilità delle banche, ma non si può dire lo stesso quando si parla di sicurezza informatica. Per quanto possano essere attrezzate, i loro server saranno sempre esposti al rischio di essere attaccati da hacker e malintenzionati. In aggiunta, il loro sistema di credito può mettere a repentaglio i tuoi risparmi se dovesse scoppiare una bolla nel mercato.

A questo punto potremmo dire non c'è bisogno delle banche come intermediari:

- Senza un ente centralizzato che può elargire crediti a chi ne ha bisogno, i risparmi saranno al sicuro;
- L'utilizzo della blockchain consente di avere dati pubblici ma anche sicuri, praticamente impossibili da modificare. Per alterarli, bisognerebbe attaccare molti dei nodi della blockchain. Al contrario, è più facile attaccare un solo obiettivo, il server della banca centralizzata;
- Le transazioni vengono fatte abbattendo costi di commissione e i tempi di trasferimento;
- Il conto diventa semplicemente un codice hash, che può essere la chiave pubblica dell'utente che ha eseguito il trasferimento. Questo va a rafforzare la privacy, perché non c'è una diretta correlazione tra utente e conto;
- Di conseguenza, ogni utente può crearsi più conti. Il conto non è altro che la coppia di chiavi pubblica e privata, per cui basta solo creare una nuova coppia per aprire un altro conto.

Per ricevere o inviare soldi, è sufficiente che sulla transazione venga apposta una firma con la chiave privata del mittente e indicare come destinatario la chiave pubblica dell'utente a cui voglio inviare denaro. Chiunque potrà verificare chi ha autorizzato la transazione, ma non si può sapere chi sia il proprietario di quel conto.

Conclusioni

In questo elaborato è stato presentato il progetto SimpleCrypto che consente di simulare investimenti in alcune delle criptovalute più scambiate del momento. Lo scopo è di entrare nel mercato delle criptovalute e seguirne l'andamento senza rischiare i propri soldi.

Oltre a questo, gli utenti possono confrontarsi tra di loro nel motivare le proprie decisioni economiche. Verranno premiate le conversazioni più coinvolgenti, ovvero i post con più commenti. Tutto ciò senza avere la possibilità di lasciare "like" come nella maggior parte delle community, con l'obiettivo di favorire una discussione tra gli utenti.

Dopodiché è stata fatta una panoramica del progetto sotto un aspetto tecnico: le ipotesi, il modello concettuale del database alla base del progetto, gli strumenti utilizzati, la risoluzione di alcuni problemi presentati nel corso dello sviluppo dello stesso.

Una volta approfondito l'aspetto tecnico di SimpleCrypto, ci si è spostati sulla tecnologia alla base delle criptovalute, la blockchain. Di questa struttura dati, nata di recente, è stato descritto il modello di rete su cui è basato, il sistema di validazione dei dati e i metodi di crittografia implementati per identificare gli utenti della rete e per la sicurezza dei dati stessi.

Infine, è stata fatta una considerazione sui possibili sviluppi futuri della blockchain. In particolare, la più interessante riguarda un nuovo modo di trasferimento di denaro abbattendo i costi di commissione e i tempi di trasferimento. Si tratta della finanza decentralizzata, il modello su cui si basano tutte le criptovalute. La finanza decentralizzata consentirebbe di togliere la banca come intermediaria per le transazioni, riducendo soprattutto i rischi di errori umani o di attacchi informatici.

Fonti

a. *Bitcoin Facile*, di Christian Palusci.
b. *Blockchain. Tecnologia e applicazioni per il business*, di Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi.
1. Il market cap è il valore di mercato totale delle azioni di una società, ovvero il valore di tutte le azioni esistenti. Indica dunque quanto denaro ha racimolato un'azienda tramite la vendita di azioni nel mercato. (Fonte: Wikipedia)
2. Bitcoin market cap 2013-2021 | Statista
3. Alphabet Market Cap | ycharts.com
4. https://github.com/MirkodeCillis/simplecrypto-server
5. https://github.com/MirkodeCillis/simplecrypto-client
6. https://github.com/mirkodecillis/simplecrypto-orch