

Dumbchain

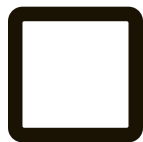
Minimal blockchain simulation

Progetto per : Programmazione 3 e Lab.

Studente: Alessio Maddaluno (0124/1455)

Cos'è Dumbchain

Dumbchain è un'implementazione minimale per la simulazione di un nodo di una generica blockchain. Offre:



Inserimento di blocchi
diretto o tramite miner pool



Ripristino di uno stato
precedente della catena



Controllo dell'integrità della
catena



Una GUI indipendente per
analizzarne le funzionalità

Dumbcoin GUI

Interact directly with the DumbChain

transaction value

Add TX

transaction value

Add TX

Blockchain Integrity : **VALID**

Validate

Restore

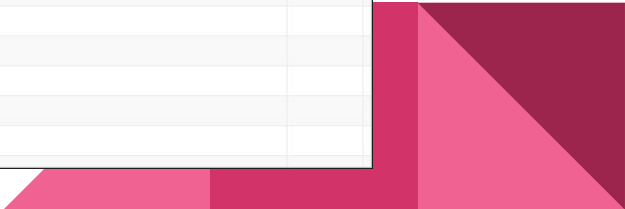
Reset

Miner's block state: 0/5

block id

Mine Block

Id	Hash	Previous Hash	Nonce	#Tx	Block Id	Hash	Value
0	000e5498c6be4f...	0	1811	1	0	901131d838b17aac0f7885b81e03cbd9f5157a00343d30ab22083685ed1416a	GENESIS
1	000678d06e77b7...	000e5498c6be4f...	1306	5	1	559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08dfdfdd	A
2	000189e8c09f9f1...	000678d06e77b7...	5084	5	1	df7e70e5021544f4834bbbee64a9e3789fbc4be81470df629cad6ddb03320a5c	B
					1	6b23c0d5f35d1b11f9b683f0b0a617355deb11277d91ae091d399c655b87940d	C
					1	3f39d5c348e5b79d06e842c114e6cc571583bbf44e4b0ebfda1a01ec05745d43	D
					1	a9f51566bd6705f7ea6ad54bb9deb449f795582d6529a0e22207b8981233ec58	E
					2	58bb119c35513a451d24dc20ef0e9031ec85b35bfc919d263e7e5d9868909cb5	AA
					2	fc686c314491e1f68bf1899fc54b2327353c44dd1ab4ed56538ef623edd1e866	BB
					2	a56362a10c816abf206d72cb914e2d5ca454eb9c7e744f88b1a1422c379e9942	CC
					2	92f089f2a70df5d960aac7c83dac8bc454c2cb1fa9a8e3061a8f6a84f338fd21	DD
					2	bd43c62d6ccc0ceb731444123576f0ee21f5f66bfd673edacd95e5e724b4fa6	EE



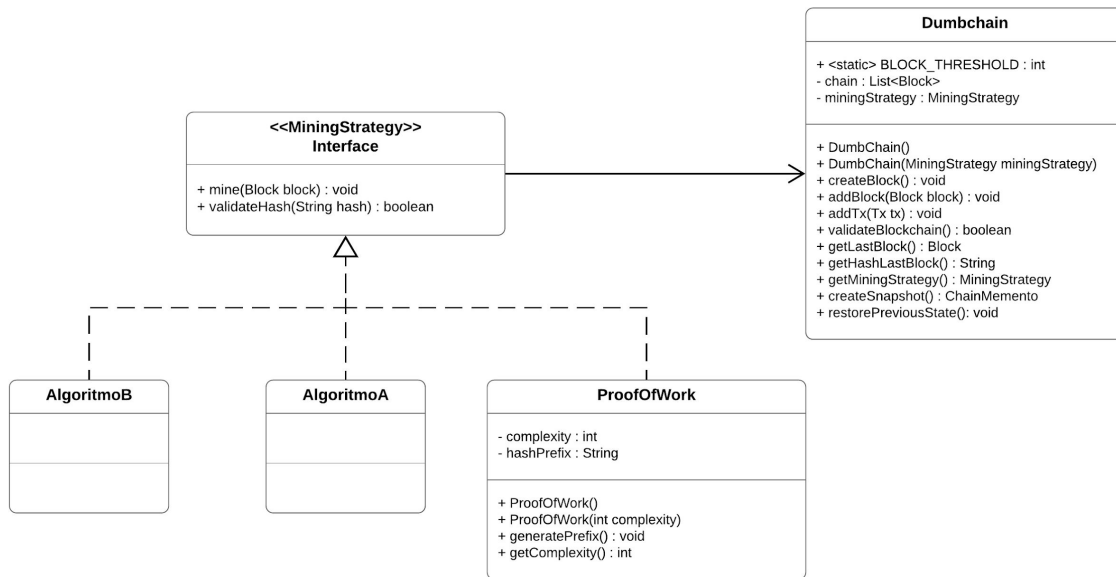
Design Pattern utilizzati

L'intero progetto è realizzato utilizzando i seguenti pattern:

- **Strategy** - *Indipendenza algoritmi di mining*
- **Builder** - *Interfaccia semplificata per la creazione di blocchi*
- **Memento** - *Ripristino dello stato precedente della catena*
- **MVC** - *Gestione modulare per l'interfaccia grafica*
 - *Il Model relativo all'MVC è un implementazione di un facade rispetto al package "dumbchain"*



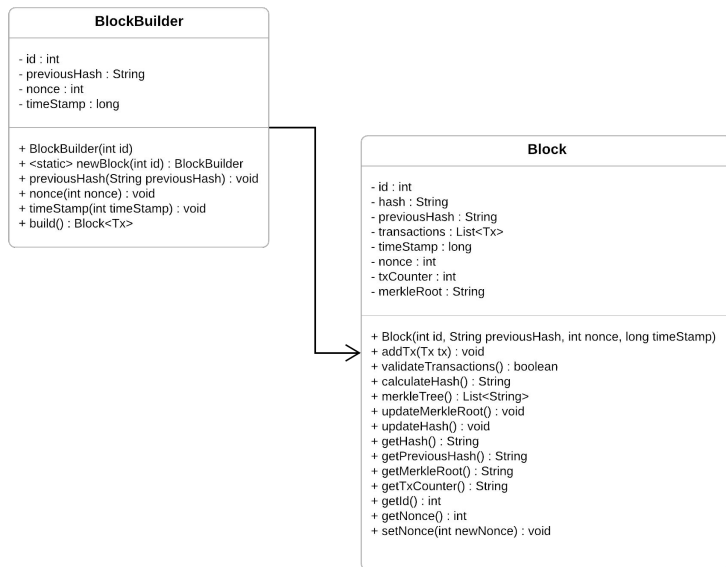
Strategy - Algoritmi di mining



È possibile aggiungere molto facilmente ulteriori algoritmi di mining di vario genere: *es. automining, proof of work gpu based etc..*

Perchè? Indipendenza dell'algoritmo di mining consente sperimentazione maggiore.

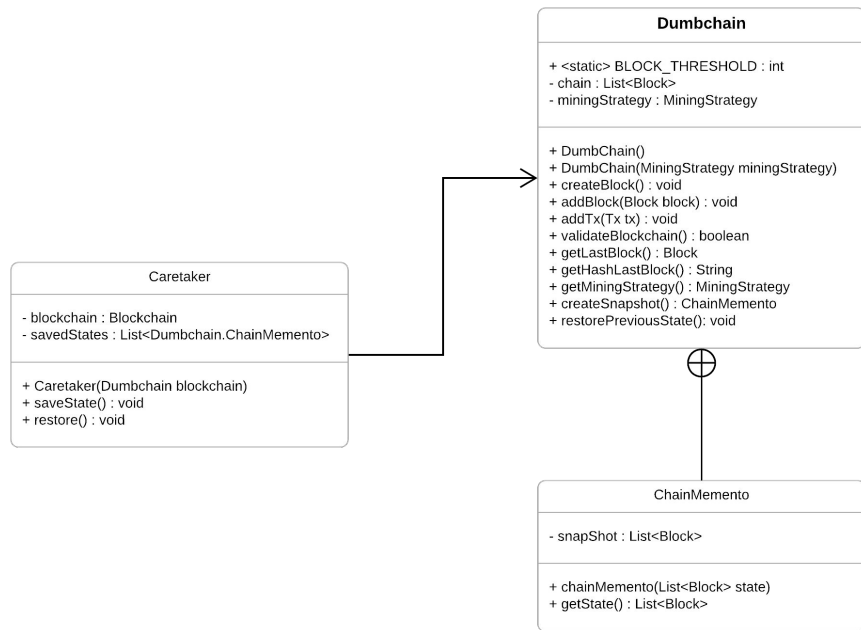
Builder - Interfaccia di creazione dei blocchi



Semplificare la creazione di blocco e contemporaneamente gestire possibili parametri di default consente di creare blocchi per test di funzionamento più specifici: *modificare parametri altrimenti derivati*.

Perché? Semplificazione gestione di parametri di default, maggior flessibilità per la creazione di blocchi

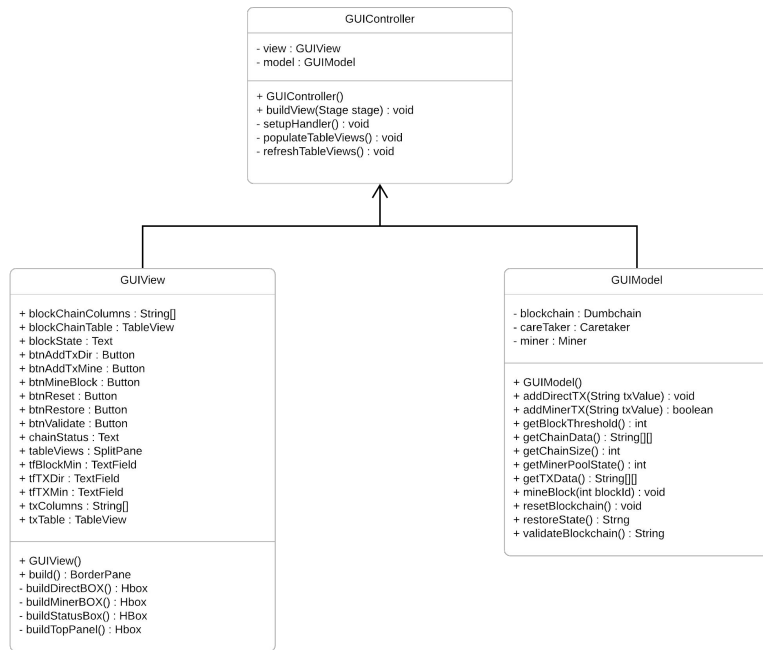
Memento - Ripristino stato precedente



Essendo uno strumento per imparare il funzionamento di una blockchain è possibile fare letteralmente un “CTRL+Z” per ritornare allo stato precedente.

Perché? Ripristinare lo stato precedente della blockchain è una caratteristica necessaria.

MVC - Modularità interfaccia grafica



Modularizzare la GUI oltre che migliorare la leggibilità consente di avere una view complementamente indipendente dal Model.

Perché? Pulizia del codice, modularità delle funzionalità

UML - Class Diagram

