Dipartimento di Matematica e Informatica
Università degli Studi di Cagliari

ABCDE: Metodo di Ingegneria del Software per creare dApp

Lodovica Marchesi

lodovica.marchesi@unica.it

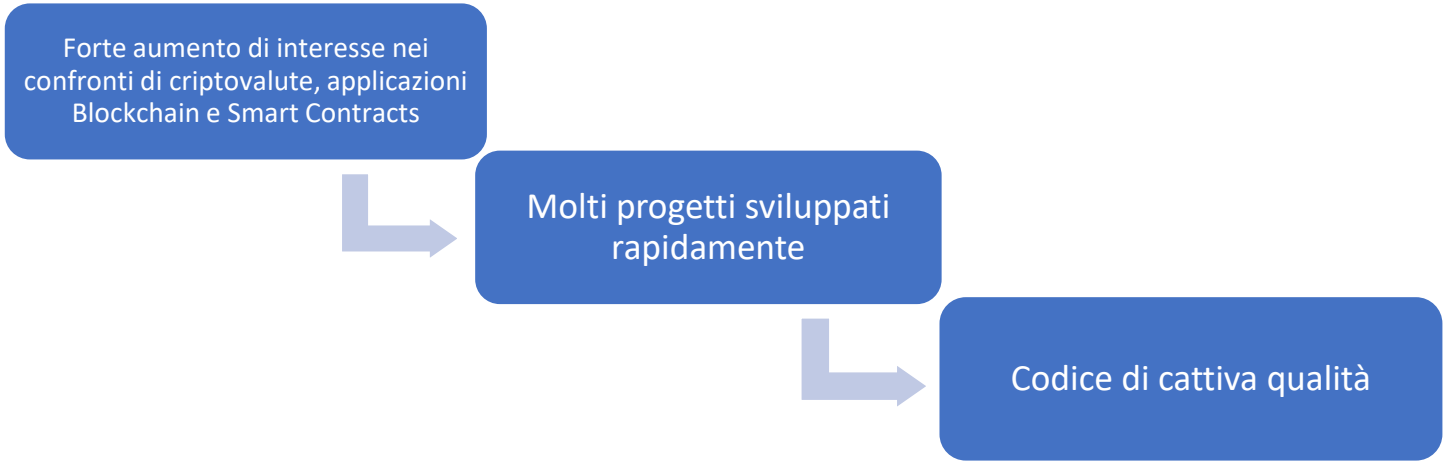
Blockchain permissioned, DEFI e loro applicazioni

Online, 24 Febbraio 2021

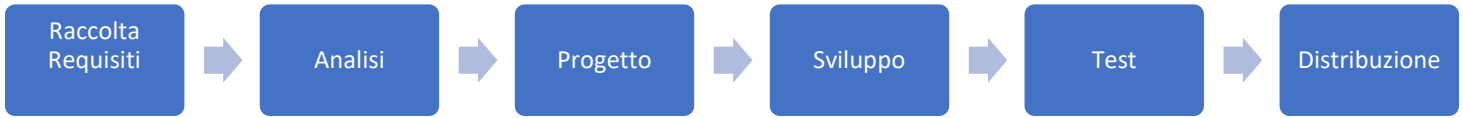
ABCDE – metodo di ingegneria del software per creare dApp

- Agile BlockChain Dapp Engineering
- Ingegneria del Software
  - Metodologie di Sviluppo Sw
- Agile
  - Sw di qualità in tempi brevi
  - Basato su tecniche Agili (ad es. User Stories, sviluppo iterativo e incrementale basato su di esse, …)
- dApp
  - Applicazione Decentralizzata
  - Gira su Blockchain

ABCDE – metodo di ingegneria del software per creare dApp



ABCDE :



Un sw nuovo e peculiare

- Lo scenario blockchain ha introdotto
  - nuovi concetti: address, gas, oracle, …
  - nuovi requisiti: immutabilità, difficoltà nell'aggiornamento del software, …

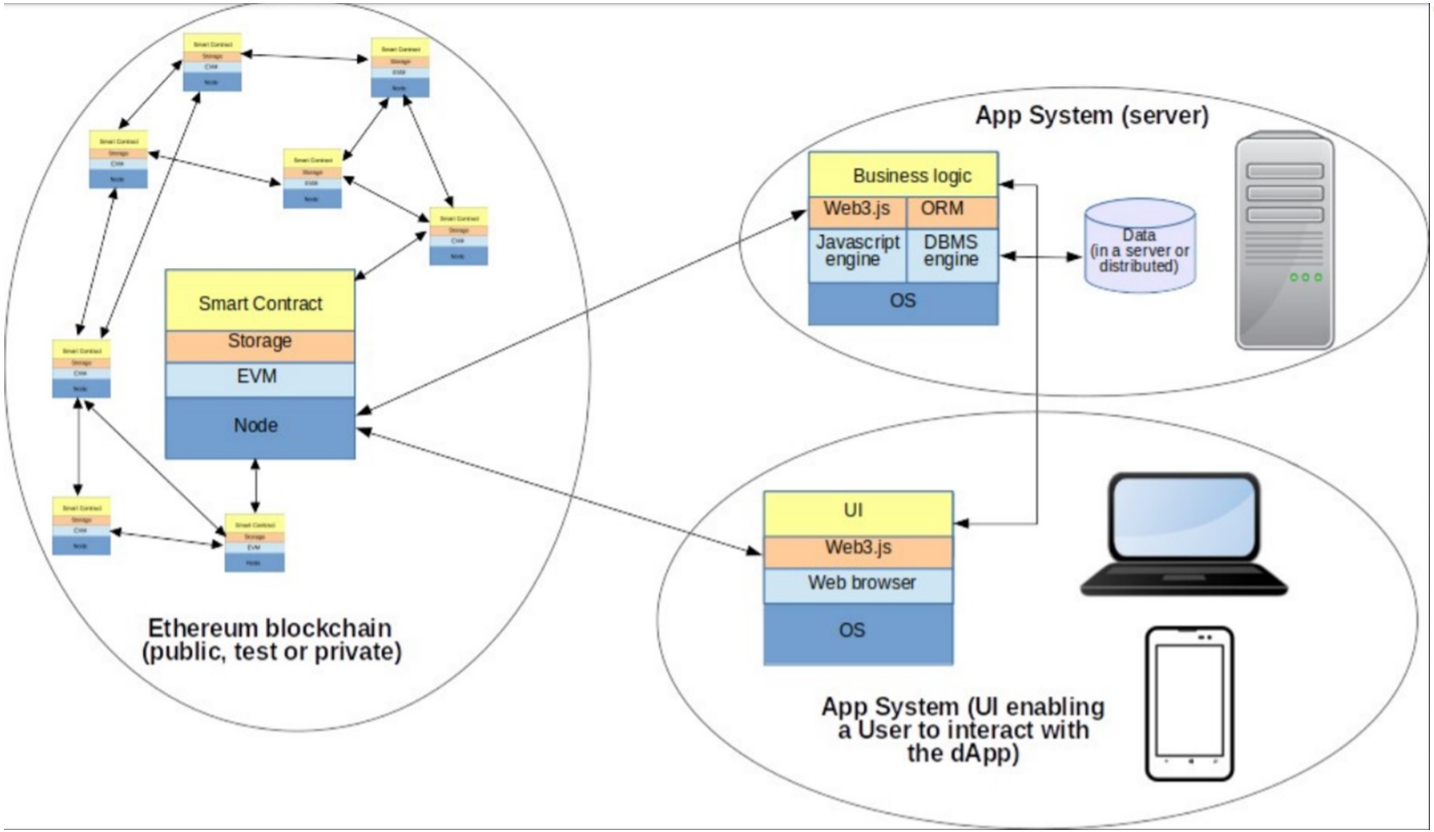
- Gli Smart Contracts:
  - sono eseguiti su tutti i nodi della blockchain
  - la loro esecuzione ha il forte vincolo che tutti gli output e le modifiche di stato devono essere uguali in tutti i nodi
  - non possono accedere direttamente al mondo esterno

Architettura dApp

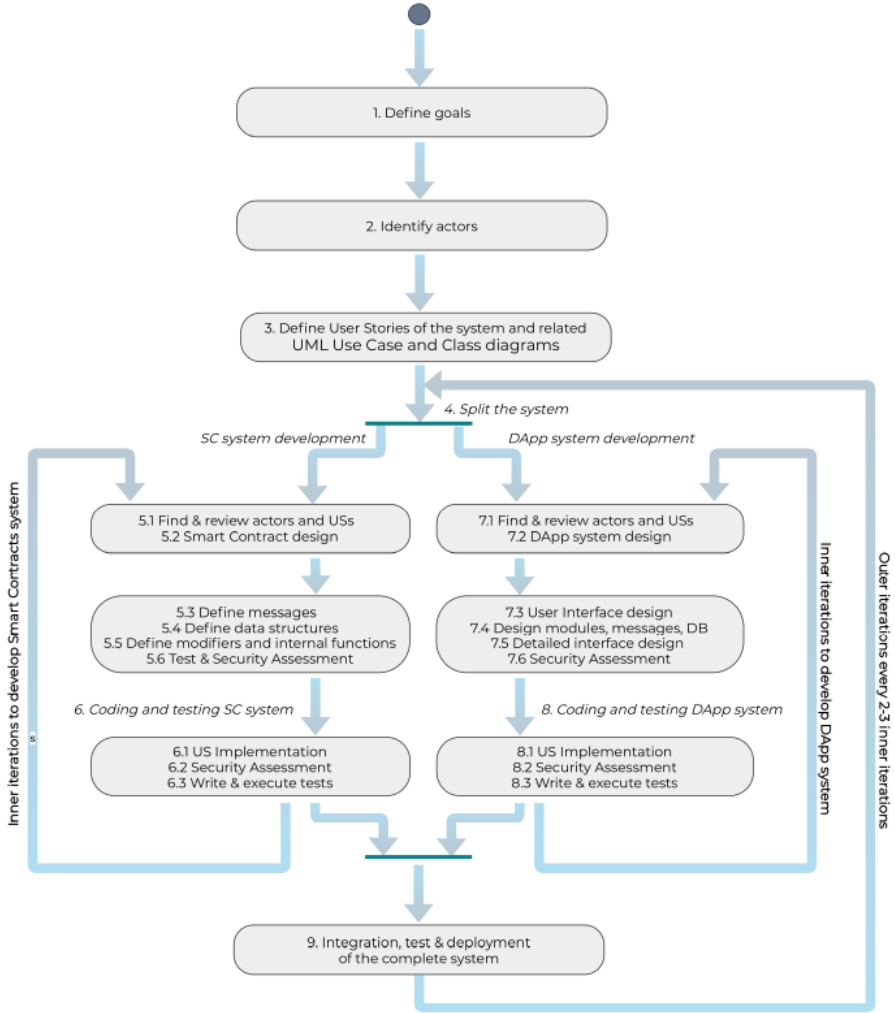
- SISTEMA INTERNO
- Sistema BC, composto dagli SC
- Interagisce col mondo esterno solo attraverso le transazioni
- Ha attori, riconosciuti tramite il rispettivo indirizzo
- Può inviare transazioni ad altri contratti o inviare soldi

- SISTEMA ESTERNO:
- Sistema SW in esecuzione su dispositivi mobili e/o su server, che scambia informazioni con utenti e dispositivi esterni
- Interagisce col primo, inviando transazioni e ricevendo i risultati
- Aggiunge l'interfaccia agli SC

Architettura dApp



Processo ABCDE



Checklists: Sicurezza

- Gli SC sono progettati per gestire e trasferire anche quantità significative di denaro (in criptovaluta, ma scambiabile con denaro reale).
- E’ necessario che raggiungano correttamente i loro scopi, ma è anche fondamentale che la loro esecuzione sia sicura contro gli attacchi.
- Il nostro approccio prevede di eseguire una checklist di sicurezza, da eseguire durante e alla fine dell'attività del progetto e dopo la codifica.
- L'obiettivo è verificare che venga applicato a tutti i pattern di sicurezza a problemi noti. Garantire un elevato livello di sicurezza del sistema, insieme al minor costo possibile di implementazione e manutenzione.

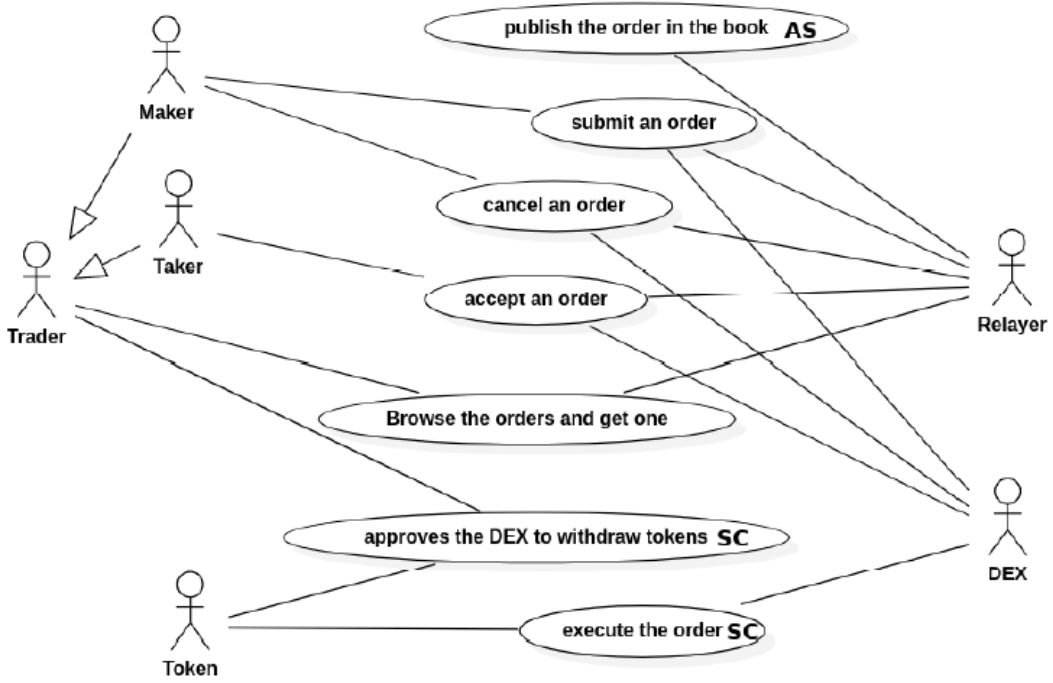
Checklists: Risparmio di Gas

- GAS:
  - Meccanismo attraverso cui le blockchain Etherum-like gestiscono l’esecuzione degli SC
  - Corrisponde a una frazione della valuta utilizzata da quel dato BC
- l'ottimizzazione è fondamentale non solo per risparmiare denaro, ma anche per evitare attacchi DOS o l'interruzione indesiderata dell'esecuzione per esaurimento del GAS
- Il nostro approccio fornisce una lista di 24 pattern

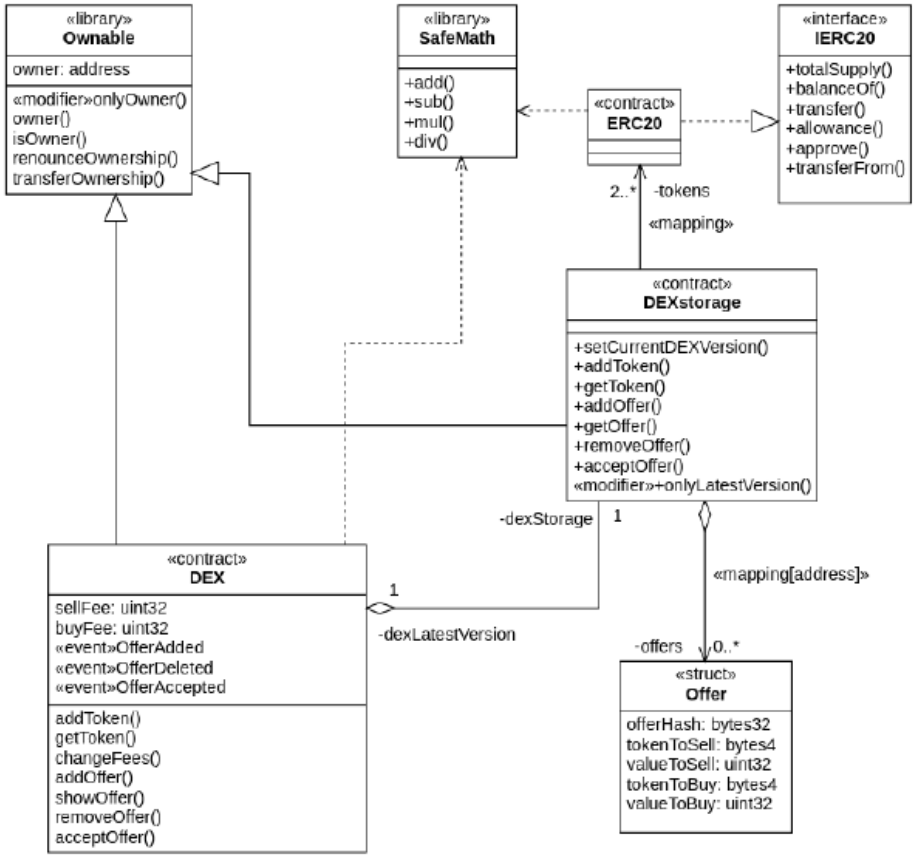
UML

- ABCDE integra lo sviluppi incrementale e iterativo con strumenti più formali
- Modellazione completa utilizzando diagrammi UML
- UML: Unified Modeling Language, è un linguaggio di modellazione e di specifica basato sul paradigma orientato agli oggetti.
- E' costituito da una collezione organizzata di diagrammi correlati, costruiti componendo elementi grafici con significato formalmente definito, elementi testuali formali, ed elementi di testo libero.
- Ha una semantica molto precisa e un grande potere descrittivo.
- Abbiamo dovuto estenderli per rappresentare concetti tipici di questo contesto

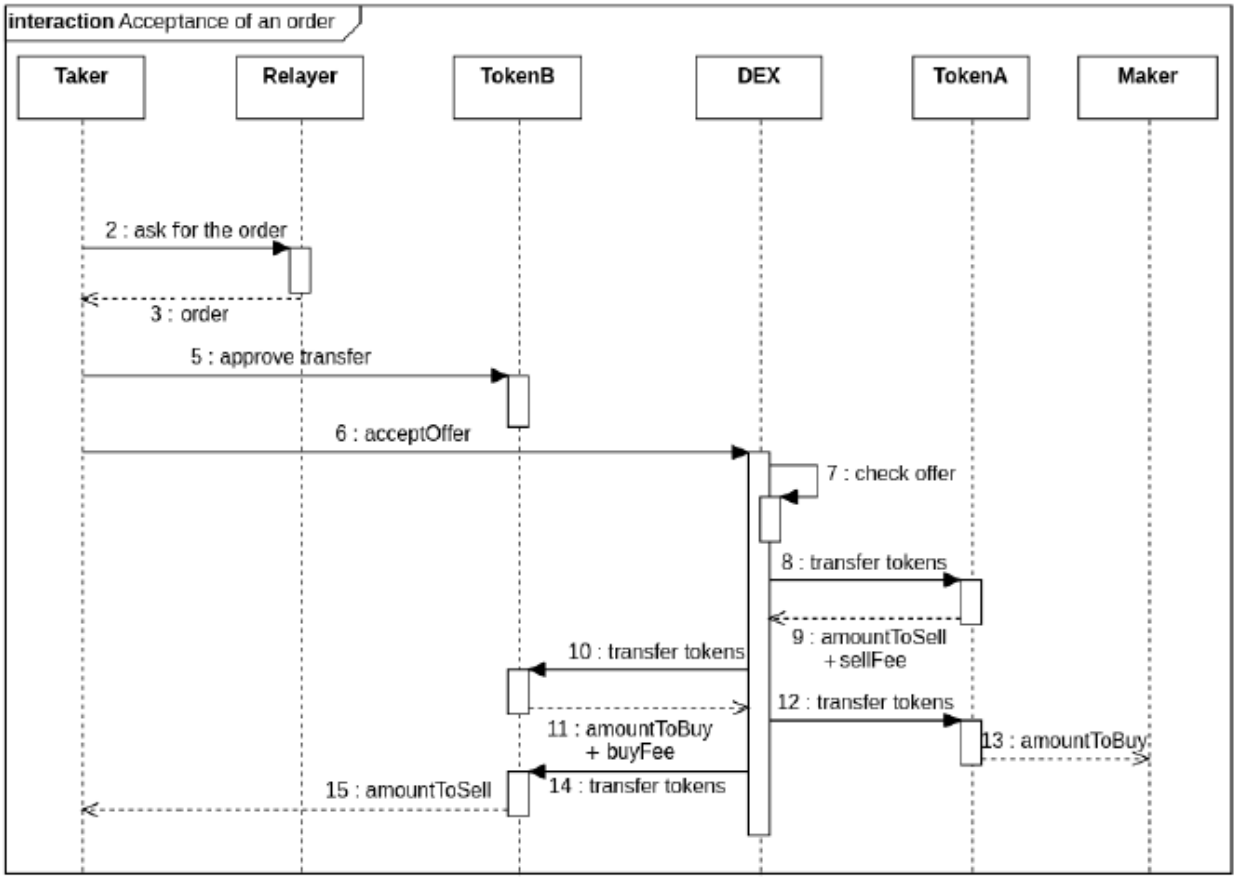
UML: Use Case diagram



UML: Class Diagram



UML: Sequence Diagram



Conclusioni

• Crediamo che il metodo ABCDE possa essere davvero prezioso per le aziende blockchain e le startup ICO egli sviluppatori di dApp, che potrebbero sviluppare un vantaggio competitivo utilizzandolo sin dall'inizio dei loro progetti di sviluppo

• Oltre alla sua semplicità, presenta una sorta di utile tutorial step-by-step per la corretta applicazione delle linee guida e dei modelli discussi

• Deriva dalla nostra esperienza nello sviluppo di dApp e dall’esperienza di imprese di cui siamo consulenti