Attività Propedeutica alla Prova Finale

AGENT-BASED SIMULATION OF A BLOCKCHAIN: STUDY OF MALICIOUS BEHAVIOURS

Presentata da
EDOARDO ROSA

Indice

Introduzione

Qui il testo dell'introduzione alla tesi. Generalmente l'introduzione non dovrebbe superare le 2/3 pagine e dovrebbe essere scritta solo alla fine.

Capitolo 1

Blockchain

Blockchain systems, since 2008, year of Bitcoin white paper, have received a lot of attentions from whom is interested in building products and services and who want to invest in those assets.

A blockchain is a fully-distributed, peer-to-peer software network which makes use of cryptography to securely host applications, store data and transfer digital assets that could represent real-world assets; this technology can be thought as a append-only master ledger that is publicly available and is not controlled by a central authority.

Technically speaking a blockchain is a grown list of records, called blocks, which are linked using cryptographic techniques and widely used by cryptocurrencies.
There is no actually a formal definition of blockchain technology that is generally accepted but is possible to defined it using the Bitcoin as model and its application in cryptocurrencies.

Bitcoin's blockchain was presented by Sathosi Nakamoto in 2008 to solve the problem of build and using a decentralized protocol to implement digital currency without the need of a trusted authority or central server and avoid double-spending from malicious players.

Another definition of blockchain is provided by Vitalik Buterin, co-founder of Ethereum:

"A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong cryptoeconomically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol

specifies.“

This definition is interesting since do not mention financial terms, particular use cases, specific consensus protocols or algorithms but do not take into consideration aspects like decentralization and communication.

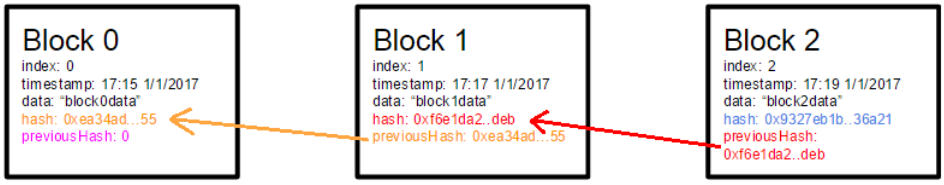
1.1 Structure

A blockchain is commonly composed in:

- Blocks
- Protocols
- Nodes

1.1.1 Blocks

A block in a single record that forms the growing list of records.



Blocks are linked using cryptography and by design are resistant to data modification. Cryptography provides authentication and verification and is used to conjure a secure computing environment out of many nodes without central authority or single owner.
Each block contains a cryptographic hash of the previous block, a timestap and the data to store in a permanent way.

Each block contains a cryptographic hash of the previous block,[6] a timestamp, and transaction data (generally represented as a merkle tree root hash). By design, a blockchain is resistant to modification of the data. It is ”an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way”.[8] For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority.

Though blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.[9]

Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin.[1] The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications.[1][3] Qui una breve descrizione del contenuto del capitolo o, eventualmente, testo introduttivo alle sezioni che seguono

1.2 Prima Sezione

Qui il testo della prima sezione. Questa è una parola in *corsivo*, questa invece è una parola in **grassetto** e questa è una parola in `monotype`.

Questo è un paragrafo centrato!

Dimensione del testo:

Testo Testo Testo Testo Testo Testo

Qui una citazione bibliografica [1].
Qui un link `www.google.it`

1.2.1 Prima Sottosezione

Qui l'esempio di un elenco puntato:

- Primo elemento,
- Secondo elemento,
- Terzo elemento.

Qui l'esempio di un elenco con un sotto-elenco:

- Primo elemento,
  - Primo elemento del sotto-elenco
  - Secondo elemento del sotto-elenco
- Secondo elemento,
- Terzo elemento.

Qui infine l'esempio di un elenco numerato

1. Testo
2. Testo
3. Testo

1.3 Seconda Sezione

Qui l'esempio di una formula matematica:
$G = \gamma \frac{m_1 m_2}{r^2}$

1.4 Terza Sezione

Qui il riferimento ad una sezione utilizzando una label: Sezione 1.3
Qui la definizione di due paragrafi con titoli.

Titolo 1 testo del paragrafo

Titolo 2 testo del paragrafo, con una nota a piè di pagina[1]

[1] Questo è il testo della nota, in cui si può *utilizzare* qualunque stile di **formattazione**

Capitolo 2

Capitolo con Immagini e Codice

Introduzione al capitolo

2.1 Prima sezione del secondo capitolo

Qui di seguito un'immagine. Tutte le immagini devono essere inserite nella cartella `images`

Figura 2.1: Testo della didascalia

Qui invece il testo con il riferimento all'immagine: Figura 2.1.

Qui un'immagine con due sotto-immagini:

(a) Didascalia prima figura

(b) Didascalia seconda figura

Figura 2.2: Didascalia globale

Altri tipi di riferimenti: Figura 2.2 oppure 2.2b.

2.2 Seconda sezione con codice sorgente

Il codice sorgente può essere inserito mediante un link al file del codice sorgente, in questo caso il file con il codice va inserito nella cartella `code`.

Capitolo 3

Titolo

3.1 Titolo della sezione

3.1.1 Titolo della sottosezione

Conclusioni

Qui il testo delle conclusioni alla tesi. Non deve essere un riepilogo di quanto fatto nella tesi ma piuttosto le conclusioni raggiunte relative al lavoro svolto.

Ringraziamenti

Qualora lo si desideri è possibile inserire qui il testo dei ringraziamenti alle persone che hanno contribuito in qualche modo al percorso che ha portato al lavoro di tesi.

Bibliografia

[1] Autore1, Autore2, *Titolo dell'opera*, Editore, Anno.

[2] Autore1, Autore2, *Titolo dell'opera*, Editore, Anno.

[3] Autore1, Autore2, *Titolo dell'opera*, Editore, Anno.