Bitcoin

Project specifications

Bitcoin is a digital currency using peer-to-peer technology to operate in a node network without central authority or bank. *Transactions* recording coin transfers are verified by a decentralized system based on strong cryptography. A distributed ledger based on *blockchain* tecnology records a public history of transactions which malicious attackers cannot change if honest nodes control a majority of CPU power.

Bitcoin is described in a large number of publications available online, among which Satoshi Nakamoto's original 2008 paper [Nak08] and the "Ethereum white paper" [But14, p. 1 to 10].

Assignment

Develop and implement in Java a model of bitcoin circulation in a network of nodes representing independent agents and miners, and featuring no centralized authority. The model should address at least some of the interesting features of the blockchain idea for preventing double spending of coins. No need to capture the full complexity of real life, so simplifying assumptions are welcome. The system should allow running simulations where bitcoins are transferred between agents and transactions are validated by miners competing in constructing blockchains. Different blockchains may emerge during simulation and the longest should survive as the system evolves. Malicious agents and miners may also be comprised in the picture in order to verify the robustness of the model.

The project should come with a short report including:

- an abstract description of the model, including a discussion of the adopted simplifying assumptions;
- a high level description of the system;
- a few examples of simulation showing the interesting features of the system;
- an appendix with the Java source code (which should be extensively commented).

References

[But14] Vitalik Buterin. *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014. https://ethereum.org/en/whitepaper/.

[Nak08] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. https://bitcoin.org/bitcoin.pdf.