Homework 9

Cyril Renevey, Lukas Pestalozzi, Joey Zenhäusern, Leonardo Wirz

December 1, 2017

Problem A

The bitcoin's prices from the last three years were downloaded on [1]. The generalized hyperbolic distribution was not found for Python (only the hyperbolic distribution was implemented in scipy.stats), and either was it in the standard libraries of Matab. We used a custom code can be found on [2]. There are two function, one to find the parameters fitting the distribution and the second is the probability density function. The log return of prices is define as follow :

$$R = \log(\frac{V_t}{V_y})$$

With V_t = today's value and V_y = yesterday's value.
First figure show the fitted distribution and the corresponding histogram and the second shows the same in a logarithmic scale.

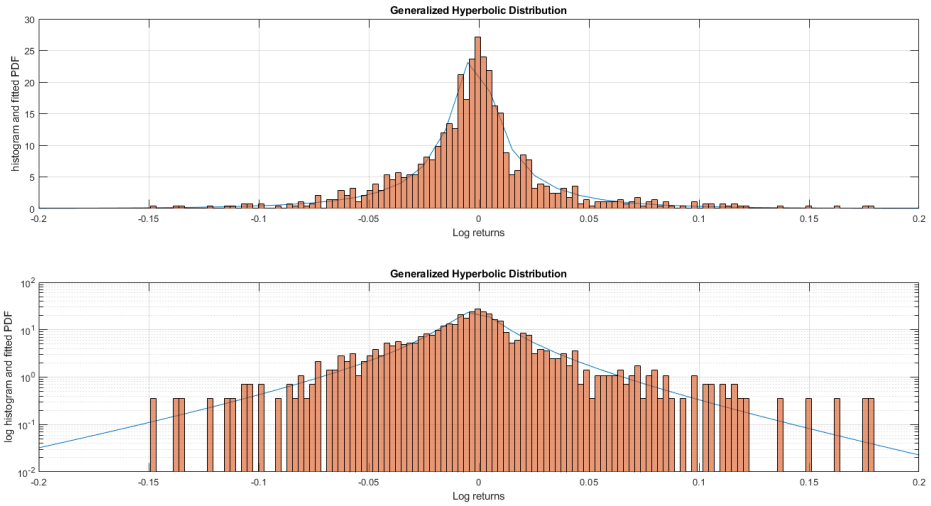

Figure 1: fitted PDF on log returns.

The main problem seems to be on the top of the histogram on values near 0, the histogram goes higher than the fitted distribution on those values. Both figures suggest that the fit is quite good but could be better. The fit appears reasonable also in the tails.

Problem B

The simple neutral evolutionary model is implemented in the jupyter notebook *problem-b.ipynb*. Executing the Algorithm with parameters $\mu = 7/N$, $N = 10^5$, $m = 1$ and 200 iterations we can verify that the marketshare of the initial species (in our case bitcoin) also shows a rough linear decrease, as shown in the lecture. The exact decrease cannot be reproduced due to unkown parameters for N and m, but it is fair to confirm the results of the lecture in light of the graph produced by our algorithm.

Problem C

Prove that RPCA will fail if 30% of the validators are faulty.
We assume, a "faulty" validator exhibits byzantine faults (malicious behavior, eg. they collude with each other with the goal to make RPCA "fail").

"The final round of the RPCA requires a minimum percentage of 80% of a server's UNL agreeing on a transaction. All transactions that meet this requirement are applied to the ledger, and that ledger is closed, becoming the new last-closed ledger"[3]. So trivially, if more than 20% of the validators are faulty (and never agree to a transaction), ripple never approves any transaction. This makes the system unusable and therefore RPCA will fail if 30% of the validators are faulty, since $30\% > 20\%$.
Note that 80% of the validators have to collude to be able to control perfectly which transactions are approved (they even may include non-valid transactions).

Problem D

First of all, a smart contract is a computer protocol which goal is to facilitate, verify and secure the terms of a contract, without intermediary agents (such as lawyer, banks, etc). Ethereum is a public blockchain-based platform which allows the creation of various smart contracts. The currency of the platform is the cryptocurrency Ether, it helps proceeding the financial smart contracts.
We will analyze the typical hedging contract proposed in the course, which is as follow :

- Wait for party A to input 1000 ether.
- Wait for party B to input 1000 ether.
- Record the USD value of 1000 ether, calculated by querying the data feed contract, say this is $x.
- After 30 days, allow A or B to "reactivate" the contract in order to send $x worth of ether (calculated by querying the data feed contract again to get the new price) to A and the rest to B.

We will look at the two different situations, the one where A can "reactivate" and the one where B can. Let α_t be the price of 1 Ether in $ at time t and $t = 0$ the initial time where we first recorded the price of Ether α_0. In this case we have $x = 1000/\alpha_0$. Let's first look at the case where A can reactivate : if A exercises its right its payoff would be $x \cdot \alpha_{30} - x \cdot \alpha_0$ Ether at $T = 30$ days (we neglect the role of the discount rate in our case). This payoff would be negative in the case $\alpha_{30} < \alpha_0$ thus A wouldn't exercise. For this reason the payoff of A at T is : $V_{30} = (x \cdot \alpha_{30} - x \cdot \alpha_0)^+ = x(\alpha_{30} - \alpha_0)^+$ which is the payoff of a long position on a European call option written on the Ether price with maturity $T = 30$ days and strike $K = \alpha_0$. B would thus have the short position.
In the case where B can reactivate, we have, following a similar reasoning, that its payoff is $V_{30} = x(\alpha_0 - \alpha_{30})^+$ which is the payoff of a short position on a European call option written on the Ether price with maturity $T = 30$ days and strike $K = \alpha_0$. A would thus have the short position.

References

[1] Bitcoin charts. https://www.quandl.com/data/BCHARTS-Bitcoin-Charts-Exchange-Rate-Data. Accessed: 2017-12-01.

[2] Matlab code library. https://ch.mathworks.com/matlabcentral/fileexchange/50219-flexible-distributions-toolbox. Accessed: 2017-12-01.

[3] David Schwartz, Noah Youngs, and Arthur Britto. The ripple protocol consensus algorithm. https://ripple.com/files/ripple_consensus_whitepaper.pdf, 2014. Accessed: 2017-11-29.