CleanFreak

ATOS challenge 2017

Authors :
DUSSIEUX Xavier & CUSSET Julien

Bordeaux INP
ENSEIRB-MATMECA
November 29, 2016

Contents

1 Introduction **3**

2 Use Cases **4**

2.1 Adding a signature 4

2.2 Preventing a virus infection 4

2.3 Use case diagram 4

3 Actors and incentives **5**

3.1 Developers and independent users 5

3.2 Contributors 5

3.3 Miners 5

3.4 Overview diagram 6

3.5 Valuing the tokens 6

4 Interests **7**

4.1 Interest for CleanFreak-based antivirus users 7

4.2 Interest for CleanFreak-based antivirus designers 7

5 Technical Feasibility **7**

6 Conclusion **7**

7 Glossary **8**

1 Introduction

Security in computer science has always been an endless cat and mouse game : hackers search for new infections while cybersecurity companies aim to spot them, and make their own research in order to prevent malicious behaviours. Due to the Internet thrive and the constant renewing of technologies, coping with those threats is becoming more and more difficult. According to Microsoft Security Intelligence Report, more than 16 million households have had serious virus problem for the past 2 year, while the 'Conficker Virus' remains the most widespread virus with almost 9 million infections until now.

Would it be possible to make Internet users collaborate to deal with malicious programs such as viruses?

As a matter of fact, an 8-year old technology could help settle it : the Blockchain. Historically built to make financial transactions in a public, decentralized way and under cover of pseudonymity, the Blockchain technology is nowadays booming, being considered by some as the most innovating technology since Internet.

In this presentation, we explain how the Blockchain could enable to design antiviruses using a decentralized, public and collaborative virus database that can automatically adapt to the latest infections.

2 Use Cases

2.1 Adding a signature

Let's say Alice is a photographer looking for a photo editing software. She browses the Internet and find an attractive free editor on a web platform, and decide to download it. A few moments later, her CleanFreak-based antivirus detects a virus from the software such as infected files propagation. The antivirus then tries to contain the threat by moving the files to quarantine, and scan them to extract the virus signature. In order to prevent other users from this infection, the Alice's antivirus issues a request to the CleanFreak blockchain to add the virus signature into the collaborative database. The other users of the blockchain then check that the signature corresponds to a real virus infection (avoid false positives) which is unknown to the database before computing the proof of work. The first user to resolve the proof of work will be rewarded with a certain amount of CleanFreak tokens shared with all the latest collaborators who detected new viruses. At the end of the process, the new virus signature is included in the blockchain.

2.2 Preventing a virus infection

A few minutes later, Bob, who also use a CleanFreak-based antivirus, tries to download the same software. After a quick scan using the CleanFreak virus signatures database, he will be informed that the file he wants to download is infected by a virus. Therefore he will look for an other editing software that is declared safe.

2.3 Use case diagram

The figure 1 below sums up these two use cases.

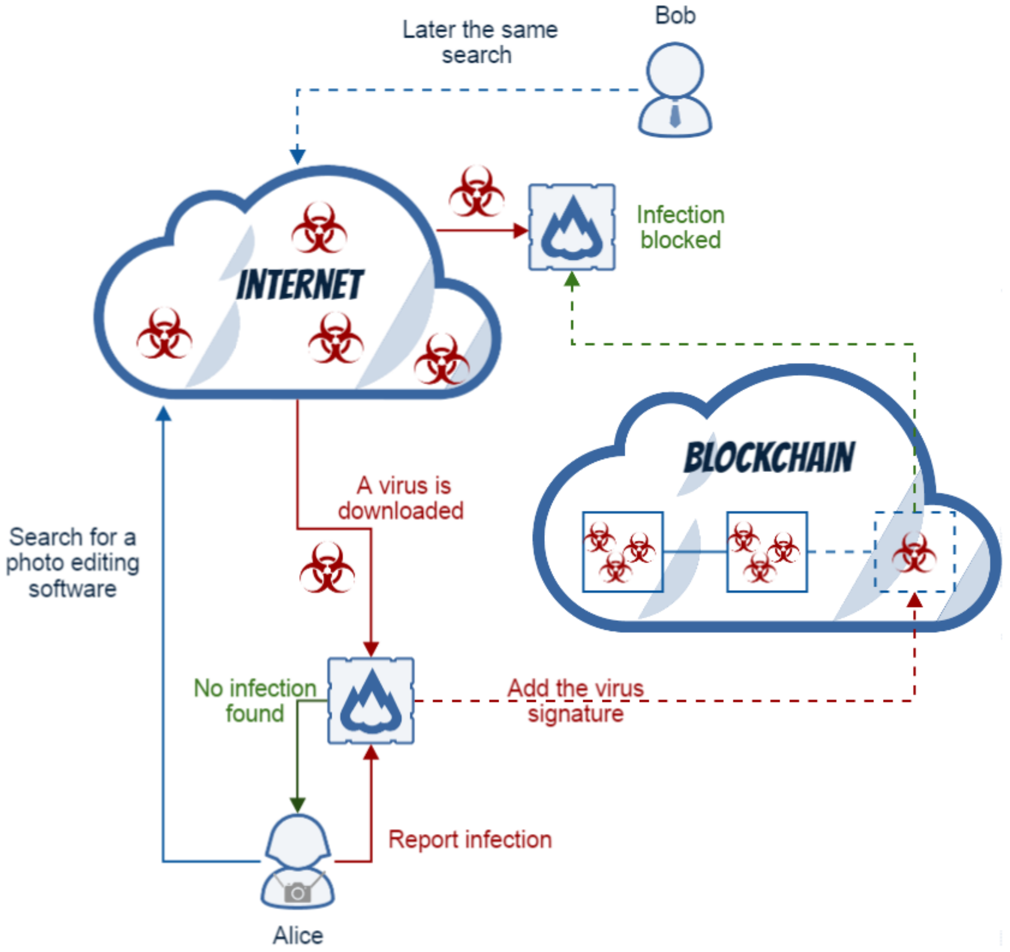

Figure 1: Basic use cases diagram

3 Actors and incentives

So as to encourage users to contribute to the CleanFreak database supply, the mining reward and financial model have been slightly adapted from the original Bitcoin blockchain description. In order to make the contribution attractive, half of the reward is given to the miners who resolved the proof of work first, while the other part will be distributed among the suppliers.

These tokens would be used to buy full versions of any CleanFreak-based antivirus. The price fixed could be symbolic since the objective is to value the tokens and ensure the collaboration attractiveness.

Based on this incentive aspect, we could imagine 3 kinds of users in this blockchain that are developped in the following subsections.

3.1 Developers and independent users

A public platform (similar to the blockchain.info) would allow anyone to watch statistics about CleanFreak tokens such as their value, the amount distributed, ... It would also enable developers to have access to the virus database and help them develop their own CleanFreak-based antivirus.

3.2 Contributors

As a collaborative platform, CleanFreak needs users called contributors who can add virus signatures to the blockchain in order to improve the protection provided by every CleanFreak-based antivirus. For each virus signature added to the blockchain, a reward is given to the contributor.

3.3 Miners

In order to prevent users from arbitrary modifying the blockchain, some users called miners invest computational power in the resolution of the proof of work of a block. Then, if a user wants to modify a block included in the blockchain, they will have to compute all the proves of work again from the later blocks before a new block is included. Indeed, users only trust the longest version of the blockchain since it is the most difficult one to corrupt. As an incentive, miners who solve the proof of work first are rewarded with tokens since they ensure the integrity of the blockchain's content.

3.4 Overview diagram

The figure 2 gives an overview of the protection and the different actors involved in the CleanFreak blockchain .

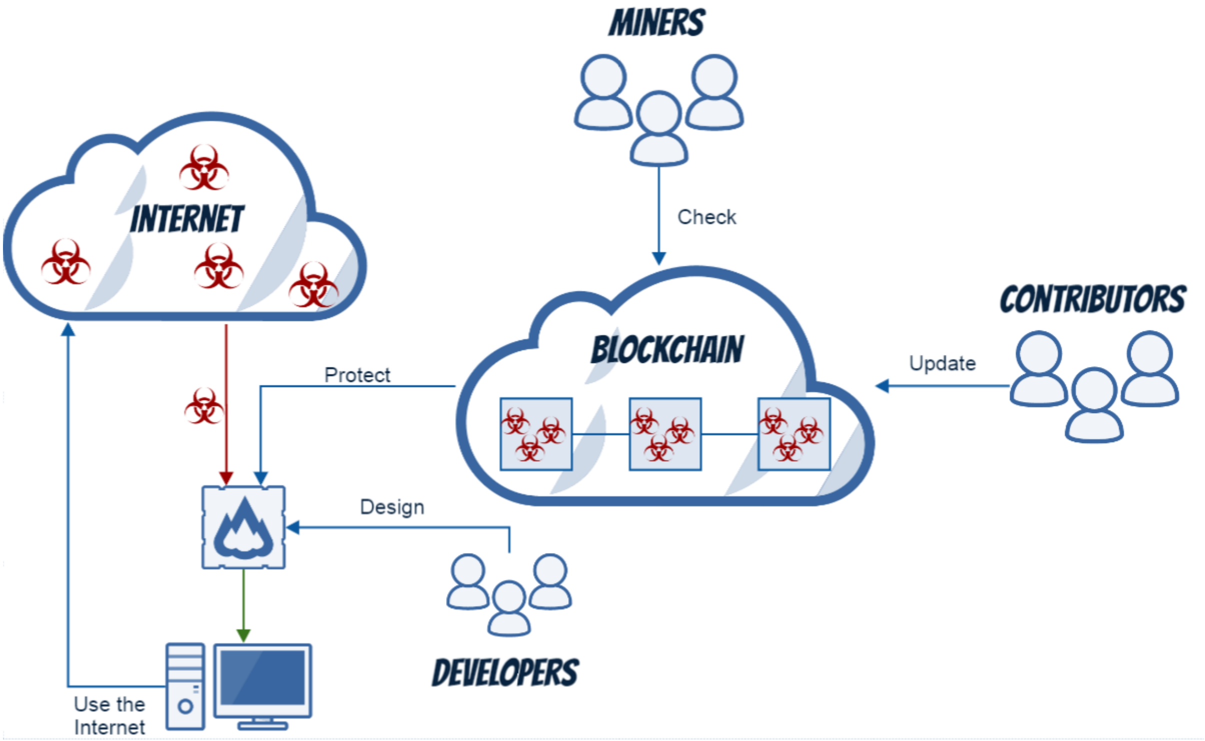

Figure 2: CleanFreak protection overview

3.5 Valuing the tokens

In order to value the tokens and make a living for the blockchain, an amount of token is required to get access to a CleanFreak based software. In exchange of tokens, an offline mode (which store the virus signatures on local disk) can be installed to protect the computer in case of down web connexion. This would become interesting only if CleanFreak is getting relatively popular. Nevertheless, this does not represent a new constraint since the blockchain already needs a widespread network to ensure the security of the virus database.

Eventually, the tokens should remain the only currency to purchase CleanFreak based software since it would give them some value and indirectly enhance the security of the database. Indeed, tokens of great value attract miners and contributors who will be able to exchange tokens with a fair exchange rate to common currencies. As the later are more involved in the network, both the volume of data and its integrity guarantee will increase. In the end, antivirus companies will provide users with stronger protection and other Internet users will be more likely to purchase their software.

4 Interests

4.1 Interest for CleanFreak-based antivirus users

- Collaborative and evolutive protection against latest threats
- Rewards for the participation in the whole Internet security

4.2 Interest for CleanFreak-based antivirus designers

- No need for virus database maintenance
- Collaborative and distributed virus database
- Possibility to add open-source or proprietary softwares
- Remuneration from the users despite the public aspect of the base

5 Technical Feasibility

The main technical difficulties in this project will be to detect new viruses whose signature is not included in the blockchain and ensure the automatic generation of a new virus signature in order for it to be added in the database. It is also necessary to equip all the nodes with a script that detect if it is a real virus to limit the integration of a false positives into the blockchain. In order to design a prototype in a short period of time, we will focus first on a specific type of malicious program (virus). The rest of the development will not be the hardest part technically speaking since we will rely on similar blockchain implementations such as the Bitcoin one.

6 Conclusion

To sum up, CleanFreak is a public and decentralized virus database preventing its users from being affected by the latest viruses. It is based on a blockchain technology rewarding both collaborators who bring new virus definitions to the base and miners investing computational power to ensure its integrity. Various antiviruses softwares could then use the base created to scan files and detect potential virus threats. A lot of things could be done to extend this project. For instance, the type of threats handled by the database could be more divers for a more efficient protection. We could even imagine an artificial intelligence based on the blockchain entries which would be able to detect potential threats that are not included yet. In this way, the CleanFreak project would only be the trigger of a bigger movement for a full collaborative protection.

7 Glossary

- CleanFreak

  We refer by ‘CleanFreak’ to the blockchain gathering all virus signatures used to scan and prevent virus infections.

- Proof of work

  Algorithm requiring great computational power used to prevent other users from arbitrary modification of the blockchain content.

- Miner

  User investing computational effort in the proof of work resolution (‘mining’ process).

- User

  We refer by ‘user’ to the nodes of the CleanFreak blockchain network. Every user is not a miner.

- Token

  Measure of cryptocurrency used to benefit from blockchain ‘privileges’ (using antivirus extensions with CleanFreak).