Concept/ Idea:

- Main goal: Increase web surfing security by creating a blockchain of secure and trusted websites hosted under a secure server
- By doing so, we prevent users to be redirected to malicious websites from their current webpage. In fact, the server will be hosting a database of secure links. If a website is not registered on this database of secure websites, it will be impossible to be redirected to this webpage, therefore protecting the user from navigating to this potentially malicious site.
- There are two advantages to such an implementation: security and cost. Using the blockchain structure, websites that fall under the server are pre-validated by the server, therefore guaranteeing their security/ authenticity. Since the server will validate the website by authenticating its information beforehand, the websites won't need a SSH to guarantee their secureness and save the cost of buying a certificate for themselves.
-

- How do we justify the owner of the website is valid?

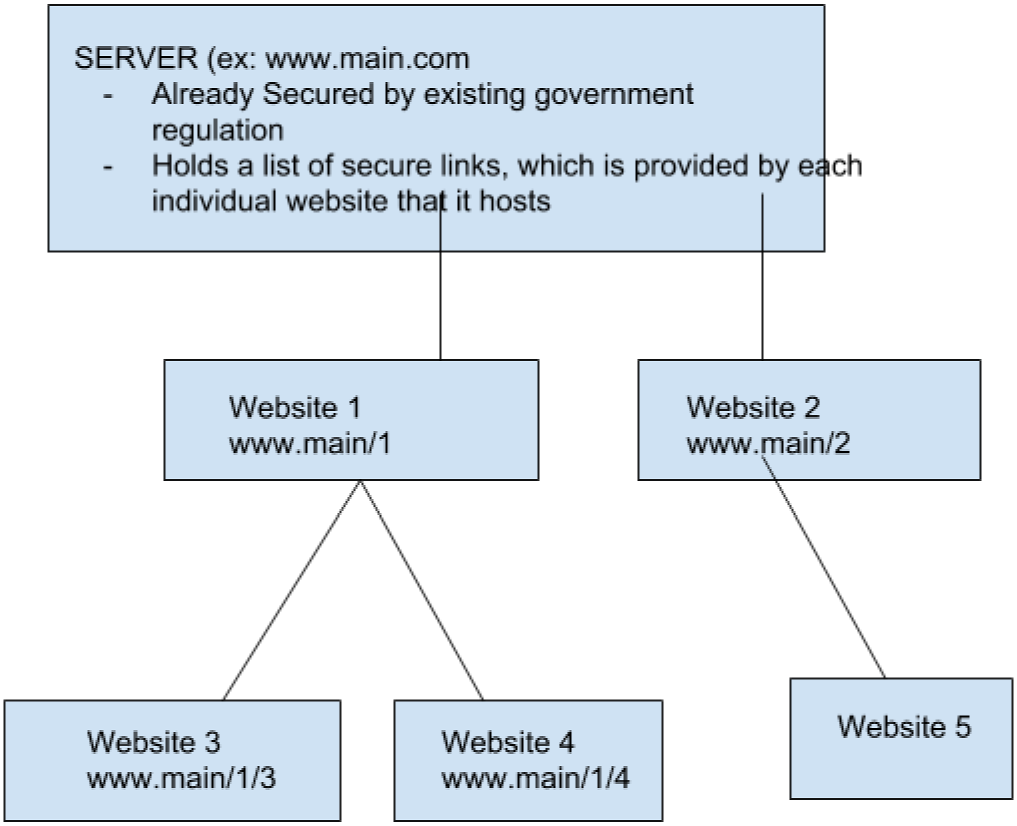
By adding more information, such as business license and corporate juridical person which is authorized by the government.

Why do we use private chain?

Because administrator who has password could edit. Even if others extend the blockchain, it is invalid and cannot be followed.

What is the prospect?

We plan to upload the certification number into the public chain so that anyone could see and verify that the website is safe.


SERVER (ex: www.main.com
- Already Secured by existing government regulation
- Holds a list of secure links, which is provided by each individual website that it hosts
Website 1
www.main/1
Website 2
www.main/2
Website 3
www.main/1/3
Website 4
www.main/1/4
Website 5

Design:

If someone want to register a company, the government will assign a unique number("password") to the company. And the number could be used to establish a private blockchain, which could verify the legal role of the owner.

Server initiates the block by sending message to IOTAS including "password", url "www.aaaaa.com" , certification number "4653643543(regulation number), and trusted list. Everytime the server want to extend the blockchain, it sends messages including its keyword and new website "www.aaaaa.com/1223.php" to be added in order to extend the chain. After receiving the response, the server stores each "root" for searching for the record.

After the chain is established, users could input the domain name and then the browser runs our library. To be specific, the browser tells the server get message from IOTAs and then check the website. If the website is included in smart contract, the browser will be redirected to the website, otherwise the browser denies users' request because of lack of trust.