# Feasibility Study of the Usage of Blockchain Technology in Online Privacy Protection

*Ben Folk-Sullivan, Department of Computer Science, Earlham College, Richmond, IN, 47374*

## Abstract

In the modern day, a lot of private information people want to protect can easily find its way onto the internet. Blockchain Technology is a computer design architecture created to keep information secure and immutable. To find a way to better protect private information, this study explored the feasibility of using a blockchain system to protect online privacy. This study focuses on regulating access to browser cookies by online web-servers. Before a web-server can access a cookie, a blockchain network will authenticate the web-server's permissions. Request Latency and Request Scale change with the number of nodes in the blockchain network will be used to determine this set-up's feasibility.

## Introduction

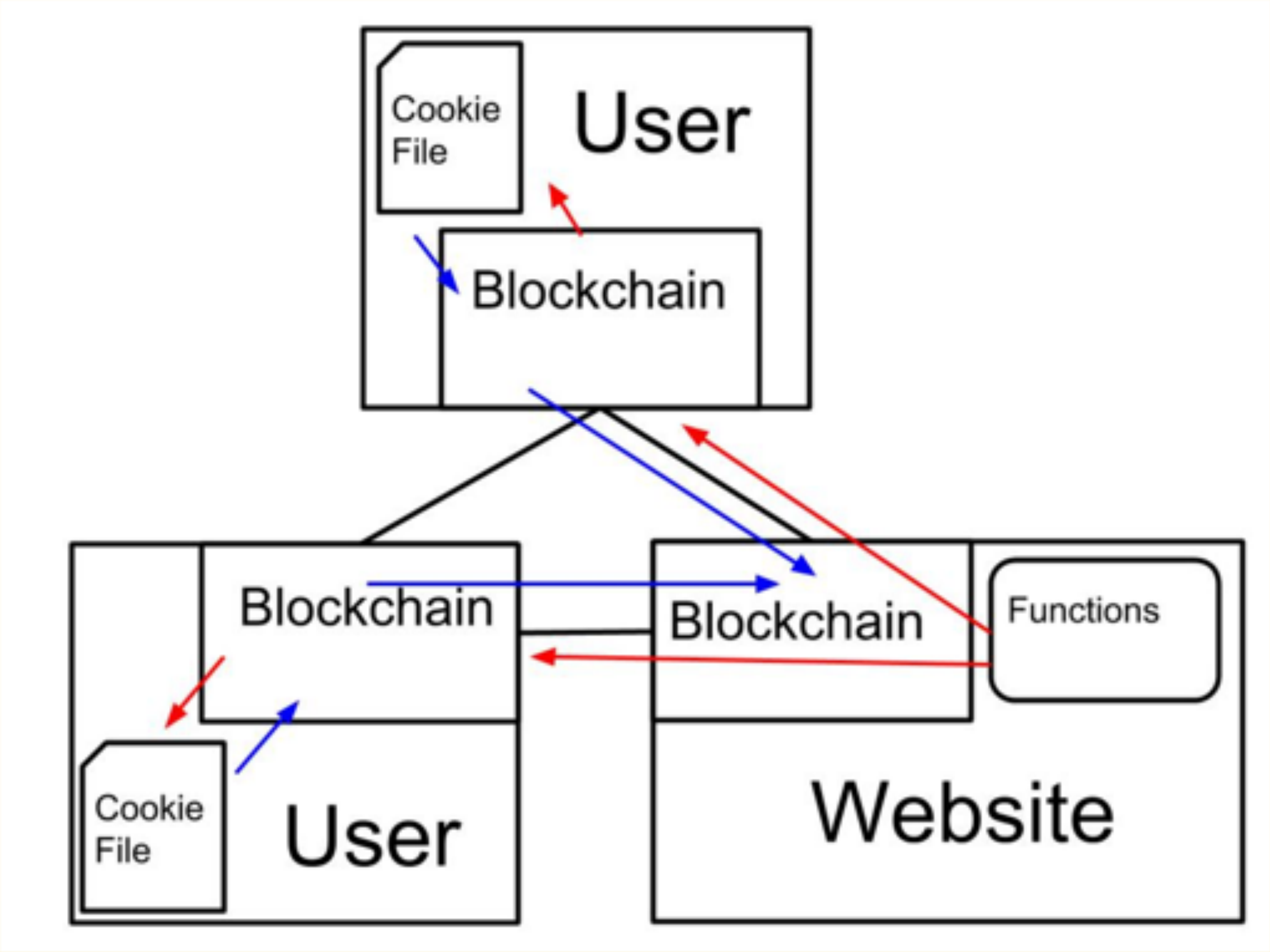
Users on the Internet of Things leave clear, detailed histories of themselves on both their own databases and those of dozens of websites and Internet Service Providers (ISPs). They have no control over this information or the profiles made from them, and the information has turned into a good traded and sold among companies to improve their marketing campaigns and revenue streams. In a very real way, the average internet user is turning into a corporate product.[1][2]

One of these pieces of information are cookies. Stored on a user's computer, these cookies are still in many cases mandatory, requiring onerous effort from the user to control and manage them. Third parties, such as internet advertisers, have evolved the cookie system so that they can track the user's activity across multiple websites.

Blockchain is a new technology developed for digital currency. Every member of a system work together to maintain a unified, publicly accessible ledger of their transactions. This ledger is made up of a chain of immutable entries, or blocks, are that are linked by cryptographic hash keys, and serves as a way to ensure the legitimacy of all transactions. No transactions through this system can be conducted with falsified resources by hostile parties.

This study was conceived as a way to investigate using blockchain technology to protect and regulate access to the cookies stored on a user's computer.

This study will use a series of servers all linked together in a blockchain network. One of these servers will be acting as an internet 'user' while the rest will act as internet website. When the user goes to a website, it will want to personalize its display for the user, based off an internet cookie-file stored on the user's system, the personal storage space of the computer that is not connected to the network itself. To access this cookie, the blockchain network will verify that the website currently has permission to access this file. Once permission is established, the website will pass several functions over to the user, who will run them on the cookie. The result of these functions is then passed back to the website. This structure will still allow permission entities to tailor a user's experience based off their personal information, while still keeping the information itself safely secured on the user's systems.



## Experiments

Each experiment can have 3 types of nodes. A user node, a valid website, and a malicious website.

Two values are measure in the experiment: Request Latency, and Request Response.

- Request Latency: How long it takes the blockchain to approve of a transaction.
- Request Response: How many website are requestining to access the User's cookie file.

There are seven experiments divided into three experiment groups. Group 1 has a blockchain network of two nodes. Group 2 has a blockchain network of four nodes. Group 3 has a blockchain network of eight nodes. All experiments have 1 user node.

- Group 1: 2 nodes total
  - Exp1: 1 valid node, 0 malicious nodes.
  - Exp2: 0 valid modes, 1 malicious node.
- Group 2: 4 nodes total
  - Exp1: 3 valid nodes, 0 malicious nodes.
  - Exp2: 2 valid nodes, 1 malicious nodes.
- Group 3: 8 nodes total
  - Exp1: 7 valid nodes, 0 malicious nodes.
  - Exp2: 5 valid nodes, 2 malicious nodes.
  - Exp3: 3 valid nodes, 4 malicious nodes.

## Design

Using the multichain program[3], multiple nodes are linked up together into a network, with one node labeled as a website and all other nodes as users. Each node has a blockchain module that is connected to all the other members of the network.

When the website first asks a user for permission to access its cookie, and the user accepts, the user will generate a blockchain item pair. This item is then transfered to the website. When the website makes subsequent requests of the user, the blockchain system will check to see it has the appropriate key and that it matches its pair on the user's database. These two items cannot be transfered away from either the user or the website.

The website will request to access a cookie on a user's system, trading over a key through the blockchain network. The blockchain will evaluate this key, checking to see if it is legitimate. If it is, the website will then pass over the function it intended to run on the cookie. The user's systems will run those functions on the cookie, and pass the result back to the website. The website then loads the webpage, customized for the user based on the output.

The setup of this structure allows for all parties to benefit. Websites will still be able to customize themselves to their users, and advertisers will still have access to browsing data across multiple platforms, and can thus better target their interests. The personal information of users will be protected and guarded from hostile actors, as the data itself becomes blackboxed. The only things seen by other individuals is the output of their functions.

## Further Work

This study is incomplete, but there are several ways it can be taken in the future. The experiments and ideation were made with an eye towards the small scale and practical, future studies could scale up the experiments to include hundreds of servers, further testing how effective this idea structure could be.

Another direction this study can be taken is to explore failure management. The security of blockchain technology is already well tested and explored. However, how the system can handle and recover from security failures, which this is not immune to, can be explored. How this security effects transaction overhead and whether it would be feasible would be valuable research.

## References

**[1]** Elisa Bertino, Kim-Kwang Raymond Choo, Dimitrios Georgakopolous, and Surya Nepal. 2016. Internet of Things (IoT): Smart and Secure Service Delivery. ACM Trans. Internet Technol. 16, 4, Article 22 (Dec. 2016), 7 pages. https://doi.org/10.1145/3013520

**[2]** Jan Henrik Ziegeldorf, Óscar García-Morchón, and Klaus Wehrle. 2014. Privacy in the Internet of Things: Threats and Challenges. Security and Communication Networks 7 (2014), 2728–2742.

**[3]** Gideon Greenspan. 2015. multichain program version 1.0.6. https://www.multichain.com/

## Acknowledgements

Thank you to Ajit Pai for being a better teacher adviser than I deserve and trying to help me out. Thank you to my parents and sister, who have and will continue to support me through everything. Thank you to David Barbella, Xunfei Jiang, and Charlie Peck for making my time as a computer science major enjoyable.

Thank you to Earlham College for 4.5 years of memories