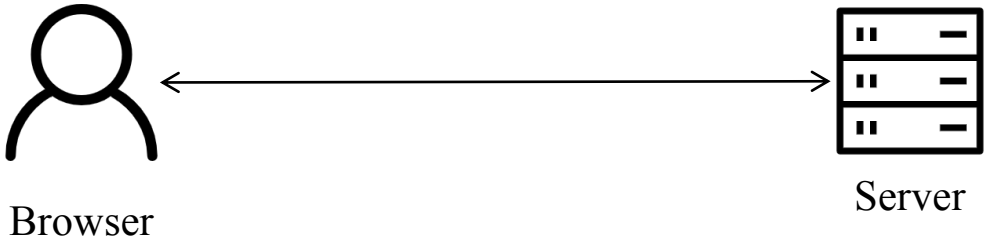
Ethereum-Based Certificate Transparency

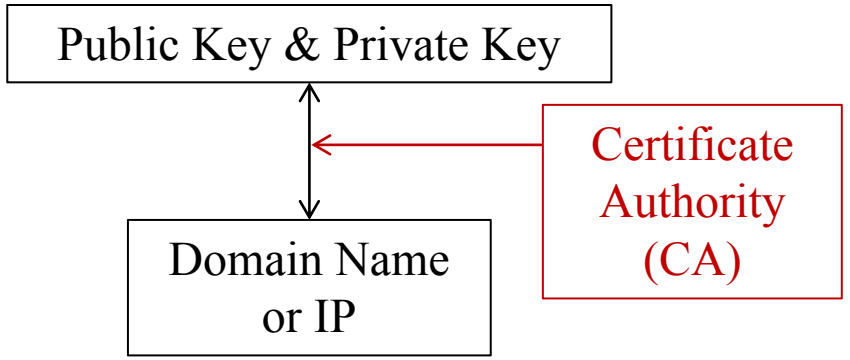
陈玄，三掌柜

Background

HTTP (Hypertext Transfer Protocol) → HTTPs (Hypertext Transfer Protocol secure)

SSL/TLS
(Secure Socket Layer/Transport Layer Security Protocols)





1. Ask for establish a secure SSL session
2. The server return certificate signed with the private key of a trusted Certificate Authority (CA).
3. Verify the certificate with public key
4. Establish SSL session with a symmetric key

Background

Currently, SSL/TLS heavily relies on Trusted Third Parties

How can we trust Third Parties? → IETF RFC 6962 - Certificate Transparency

↓

Append-Only Merkle Hash Tree

Build it on Blockchain! →

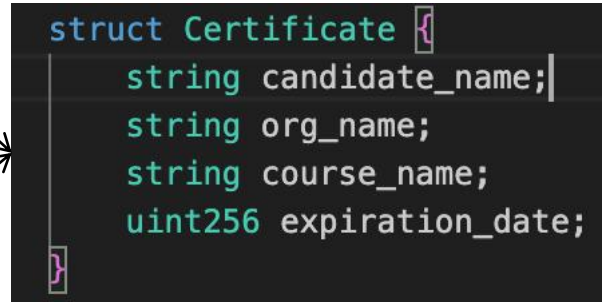
- Publicly auditable
- Misissued certificates

EthCT

EthCT: Implement Certificate Transparency on Ethereum

Generate

getData



Merkle Consistency Proofs have already been implemented by blockchain.

Next step: integrate with browsers

References

[1] Maulani, Giandari, Gunawan Gunawan, Leli Leli, Efa Ayu Nabila, and Windy Yestina Sari. "Digital certificate authority with blockchain cybersecurity in education." *International Journal of Cyber and IT Service Management* 1, no. 1 (2021): 136-150.

[2] Shen, Huajie, Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Kim-Kwang Raymond Choo. "Blockchain-based lightweight certificate authority for efficient privacy-preserving location-based service in vehicular social networks." *IEEE Internet of Things Journal* 7, no. 7 (2020): 6610-6622.

[3] Wang, Ze, Jingqiang Lin, Quanwei Cai, Qiongxiao Wang, Daren Zha, and Jiwu Jing. "Blockchain-based certificate transparency and revocation transparency." *IEEE Transactions on Dependable and Secure Computing* 19, no. 1 (2020): 681-697.

[4] Madala, D. S. V., Mahabir Prasad Jhanwar, and Anupam Chattopadhyay. "Certificate transparency using blockchain." *In 2018 IEEE International Conference on Data Mining Workshops (ICDMW),* pp. 71-80. IEEE, 2018.

[5] IETF RFC 6962 - Certificate Transparency. *Online,* https://datatracker.ietf.org/doc/html/rfc6962, (Accessed on: 2024-04)

[6] Create Your Own SSL Certificate Authority for Local HTTPS Development. *Online*, https://deliciousbrains.com/ssl-certificate-authority-for-local-https-development, (Accessed on: 2024-04)

Thanks for Listening!

陈玄
RA@SDS Fudan U, ETHPlanet Coordinator
chenxuan@fudan.edu.cn

三掌柜
Director of CSDN@Shanghai, Independent Developer
15290318915@163.com