BLOCKCHAIN-BASED DNS AND PKI TO RESOLVE ISSUES OF TRUST, SECURITY, AND CENSORSHIP IN THE CONTEXT OF THE IOT

Research project CSE3000 by Leon de Klerk (L.p.j.deklerk@student.tudelft.nl)
Supervised by M. Ayşen & Dr. Z. Erkin
April - July 2021

TU Delft

01 BACKGROUND

Main **components**:

- Domain Name System
- Public Key Infrastructure
- Internet of Things
- Blockchain

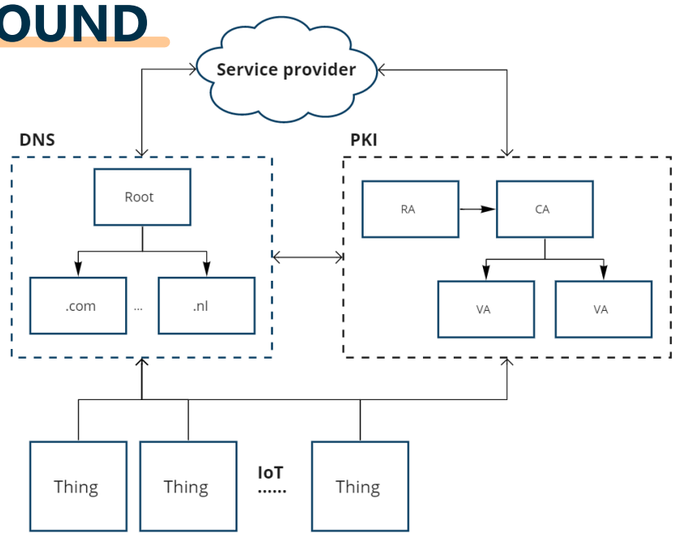

Fig. 1: Current system architecture

02 THE PROBLEM

DNS & PKI

- **Trust** in centralized authorities
- **Security** vulnerabilities
- Potential for **censorship**

IoT

- Low computational capabilities
- **Reliance**

Solution: build on **strong** points of **blockchain** to mitigate the issues of **trust**, **security**, and **censorship**

Blockchain

- Hardware requirements
- Participation
- **Scalability** & **speed**

Fig 2: NAME:WRECK banner[1]

03 METHODOLOGY

- Literature study
- [1] General introduction
- [2], [3] solutions overview
- Use of Google Scholar

Keywords

- "DNS", "Blockchain", "IoT", "PKI"
- "Trust", "Security", "Censorship"

04 SOLUTIONS

Non-blockchain-based

- Local recursive DNS [4],
- Secure Distributed DNS [5]
- mDNS [6]

- Address **one** dimension
- Lack in other dimensions
- **Trust** or **Security**

Blockchain-based

- Namecoin [7]
- Blockstack [8]
- Ethereum Name Services [9]
- EmerDNS [10]

- Leveraging **blockchain**, can address **multiple issues**
- **Blockchain** specific **issues**
- Required computing power

05 IMPROVEMENTS

Adoption

- **Integration** with current systems
- Existing blockchain

3 types of nodes

- **Regular**
- **Delegated**
- **Light**
- Address **IoT** constraints

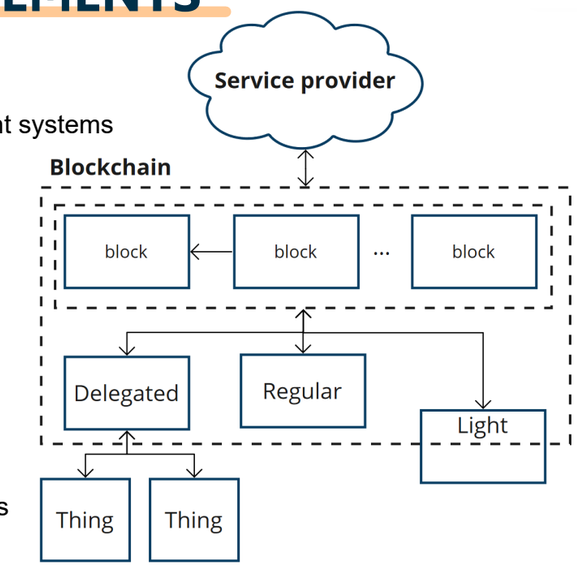

Fig 4: Proposed network architecture

06 FUTURE WORK

Open topics

- Technical implementation
- **Privacy** aspects
- User willingness
- Operator cooperation

References:
[1]: Ali, M.S., et al., Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Communications Surveys & Tutorials, 2019. 21(2): p. 1676-1717.
[2]: E. Karaarslan and E. Adiguzel, "Blockchain based dnsand pki solutions," IEEE Communications Standards Magazine, vol. 2, no. 3, pp. 52–57, 2018.
[3]: Faizan and A. Kupcu, "Improving pki, bgp, anddns using blockchain: A systematic review," arXiv pre-print server, 2020.
[4]: J. Salmela. Pi-hole - network-wide ad blocking.[Online]. Available: https://pi-hole.net/
[5]: C. Cachin and A. Samar, "Secure distributed dns," inInternational Conference on Dependable Systems andNetworks, 2004, 2004, pp. 423–432
[6]: S. Cheshire and M. Krochmal, "Multicast dns," RFC6762, February, Tech. Rep., 2013.
[7]: "Namecoin whitepaper." [Online]. Available: https://www.namecoin.org/resources/whitepaper/
[8]: M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Block-stack: Design and implementation of a global namingsystem with blockchains,"Last visited on, vol. 25, no. 2,2016
[9]: "Ethereum name services." [Online]. Available: https://docs.ens.domains/
[10]: "Emerdns." [Online]. Available: https://emercoin.com/en/emerdns

Footnotes:
1: https://www.forescout.com/research-labs/namewreck/
2: https://coinswitch.co/info/namecoin/what-is-namecoin