A Blockchain-based Method for Decentralizing the ACME Protocol to Enhance Trust in PKI

Elie F. Kfoury[1], David Khoury[2], Ali AlSabeh[1], Jose Gomez[1], Jorge Crichigno[1], Elias Bou-Harb[3]

[1] University of South Carolina, SC, USA
[2]American University of Science and Technology, Beirut, Lebanon
[3]The University of Texas at San Antonio, TX, USA

Agenda

- Introduction
- Public Key Infrastructure (PKI)
- ACME Protocol
- Background on Blockchain
- Proposed System
  - Domain Control Verification
  - Secure Session Establishment
- Results
- Conclusion and Future Work

Introduction

- Critical data is constantly sent across the globe through diverse technologies and protocols
  - Internet of Things (IoT)
  - E-Commerce
  - E-Government
  - Instant Messaging (IM)
  - Conversational media (Voice over IP/LTE)
- Many applications are facing deployment issues due to the lack of proper security and privacy measures
- IoT has not been widely adopted by organizations due to security challenges, specially client authentication

Public Key Infrastructure (PKI)

- Most existing systems are secured through a Public Key Infrastructure (PKI) with a trusted third-party Certificate Authority (CA)
- The PKI/CA infrastructure depends on its **trust model**
- Unfortunately, trust in CA remains a critical challenge (e.g., Diginotar, Comodo)
- A major reason for having trust problems with CAs is centralization
  - Denial of Service (DoS)
- Acquiring certificates from CAs can be cumbersome as the domain name verification is done through a collection of ad-hoc mechanisms

ACME Protocol

- Automated Certificate Management Environment (ACME) protocol has been proposed to automate the certificate issuance process
  - Used by “Let’s Encrypt” CA
- Deploying an HTTPS-enabled website is complicated, expensive, and error-prone for server operators
  - Installation of a certificate in a web server requires the server to use a key generation software
  - Manually follow steps to configure and validate the control of the domain name
- ACME only solved the automation issue, but the trust concerns remain as ACME requires a trusted CA

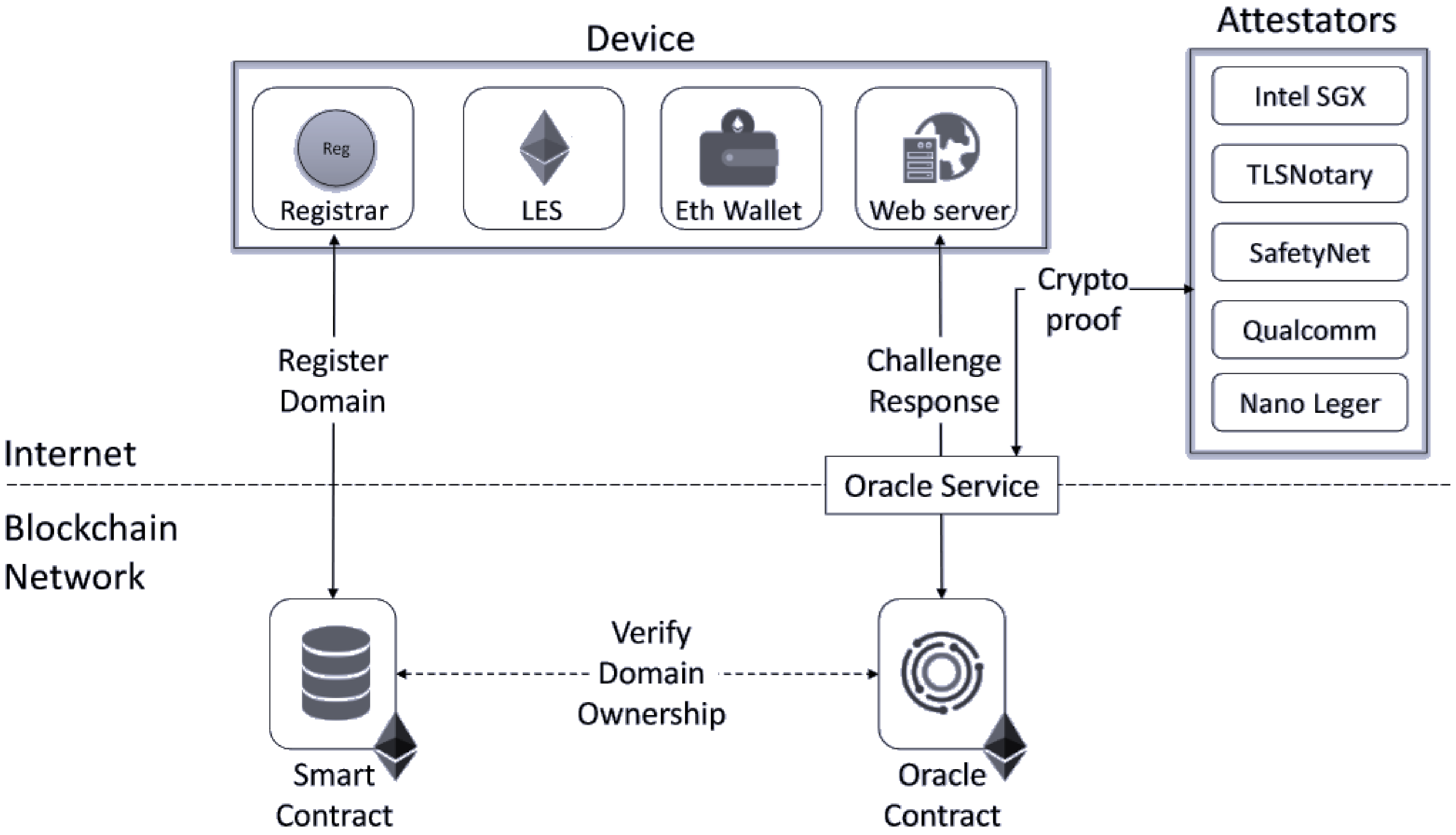
ACME Protocol

- The CA generates a random token and sends the token and list of challenges that the client (certificate’s requester) can complete to prove ownership of identifier
- The client selects the HTTP challenge, creates a file containing a token, and hosts it at a directory on the claimed server.
- Client informs the CA that challenge is complete
- The CA verifies that the file is present and that it contains the correct challenge response
- Client sends a Certificate Signing Request (CSR)
- CA issues the certificate

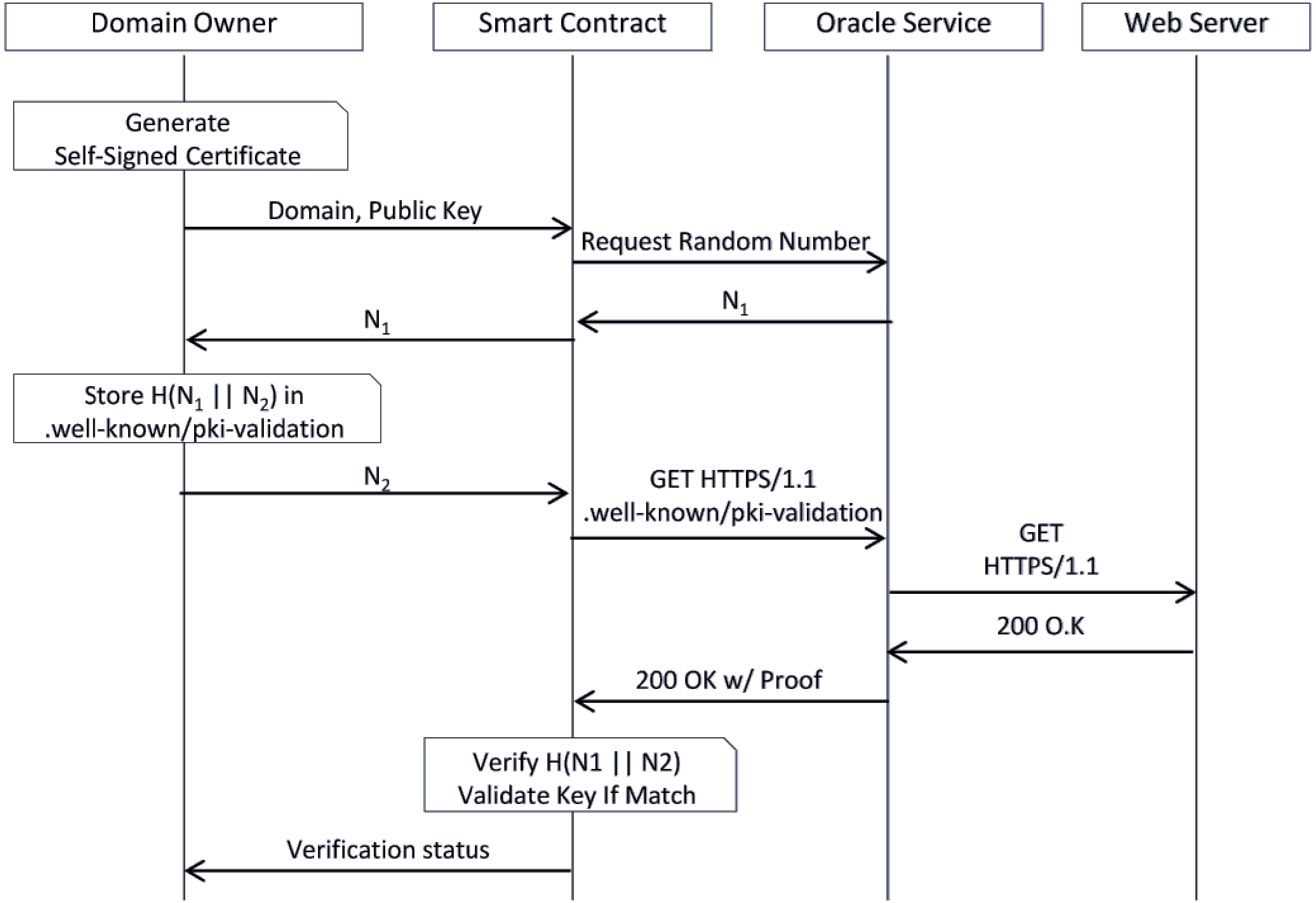
Background on Blockchain

- Emerging technology
  - Decentralized network
  - No single point of failure
  - Ensures data immutability
  - Cryptographic functions and Consensus algorithms
- The Ethereum Blockchain is an open-source featuring smart contract (scripting) functionality
- Smart contracts programming
  - Beyond digital currency, Decentralized applications (DApps)
  - Turing complete scripting language

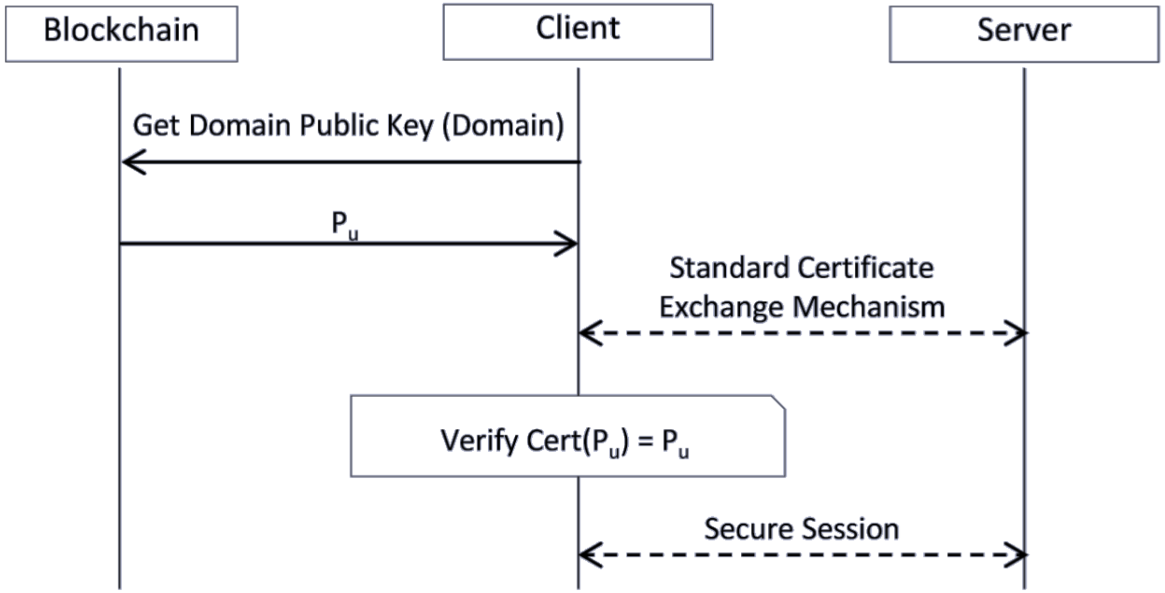
Proposed System



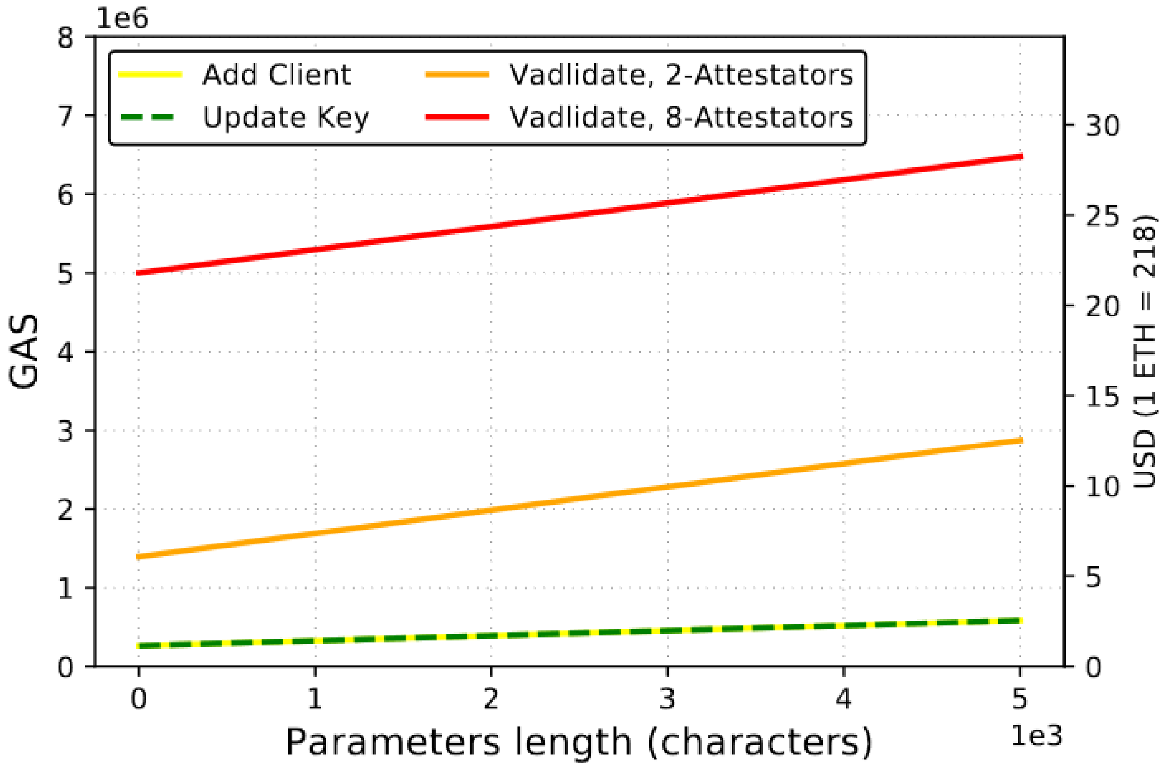
Domain Control Verification



Secure Session Establishment


Blockchain
Client
Server
Get Domain Public Key (Domain)
P_u
Standard Certificate Exchange Mechanism
Verify Cert(P_u) = P_u
Secure Session

GAS/USD Requirements



Conclusion and Future Work

- Blockchain-based method that decentralizes the ACME protocol by combining elements of the PKI/CA model with Blockchain technology
- It aims at resolving the trust concerns of the existing PKI/CA infrastructure
- The method eliminates the need for a trusted CA in the domain verification process and resolves DDoS attacks targeting single points of failures.
- Results showed that the solution is efficient in terms of transaction costs
- For future work, we intend to develop the session establishment software module as a plug-in to be integrated in major browsers
- Additionally, we aim at solving the client authentication problem.

Acknowledgement

- Thanks to the National Science Foundation (NSF)!
- Activities in the CI Lab at the UofSC are supported by NSF, Division Of Graduate Education (DGE) #1822567

Thank You

- Contact info for further questions
  - ➢ ekfoury@email.sc.edu
  - ➢ dkhoury@aust.edu.lb

- CyberInfrastructure Lab (CI Lab) website
  - http://ce.sc.edu/cyberinfra/