Summary\_of\_authLedger

The study proposes a domain authentication system based on blockchain technology known as AuthLedger. The drawbacks of current systems have been discussed in detail. The current Public Key Infrastructure (PKI) authentication is mainly dependent on Certificate Authorities (CA) which have to be trusted by domain owners as well as operators. There is a disparity of rights between users and CAs. Methods such as Domain Name System Security Extensions (DNSSEC) and Certificate Authority Authorizations (CAA) are trust-based and are prone to single point of failure. The study sets up the threat model describing various malicious adversaries and their capabilities. The AuthLedger consists of five entities – CA, Domain Name Server (DNS), Browser Extention, Validating Authority, Blockchain. The domain authentication procedures are based on time and count and are described in detail. Rules have been formulated to prevent misbehavior of validator nodes as well as clients which also include incentives to promote node honesty and attract more nodes to join the system. Lastly, the research describes the implementation prototype with the help of Ethereum smart contracts and Solidity language.

My views:

This paper presented a very novel system for domain authentication. The most important characteristic of the system is that it does not rely on third parties making it one of its kind.