The article discusses the use of Blockchain technology as a solution to prevent Distributed Denial of Service (DDoS) attacks. IoT devices have a weak security configuration due to which they can be easily hacked and made a part of the botnet to launch DDoS attack. The centralized client/server model of the Internet causes the entire system to fail due to the failure of a single server thus facilitating DDoS attacks. A Blockchain solution will replace login credentials with public key cryptography making it difficult to scan and compromise devices. User’s private key will become necessary to communicate with other devices. By limiting the authority to install firmware to the manufacturer using his private key, the chances of installation of malware would become almost none. Storing public keys on the Blockchain will help IoT devices to authenticate login requests. Blockchain can thus establish a secure P2P network wherein the attacker will not be able to publish DDoS attack launch instructions. In addition, there are other ways to use blockchain to prevent DDoS attacks. Companies like Blockstack, Namecoin, Nebulis are working towards building a decentralized DNS system. Another way is to re-engineer the entire structure of the internet to make it a decentralized model. A blockchain may itself be a victim of DDoS Sybil attack, but already there exist solutions to prevent direct DDoS risks for blockchain.

My views:

This paper proposes a Blockchain technology based solution for the prevention of DDoS attacks. I learned a lot about DDoS attacks and DNS as prerequisites to this paper. I feel that implementing a blockchain solution for DDoS attack is like **fighting fire with fire**, a decentralized solution to a decentralized attack. I plan to read more on it, especially the Gladius whitepaper.