Decentralized, peer-to-peer IoT

MANAGE IOT DEVICES WITH BLOCKCHAIN BASED, DECENTRALIZED SYSTEMS

How we are?

- Group of open source developers
- We develop Streembit and other free, open source tools
- We participate in the W3C standardization process

The problem

Addressing scalability and high availability requirements does not come cheap for businesses, and it's an even more pressing problem for SMEs and start-ups that need to build up their infrastructure from scratch. Currently, the centralized, client-server model is the dominant software paradigm. Cloud-based centralized platforms such as Amazon AWS or Microsoft Azure are expensive systems despite appearing initially low cost.

Centralized cloud-based solutions also make government surveillance easier. Software centralization that makes government surveillance easier weakens security by creating a convenient target for cyber-criminals. Users feel that centralization by a handful of solution providers poses a threat to profitability, business continuity, security and privacy. No wonder an increasing number of computer users and businesses are turning away from conventional, centralized, client-server software solutions. The evidence for this is the growing popularity of decentralized, blockchain-based systems such as the Bitcoin blockchain and Ethereum.

The Problem

Problems with proprietary, closed source client-server systems

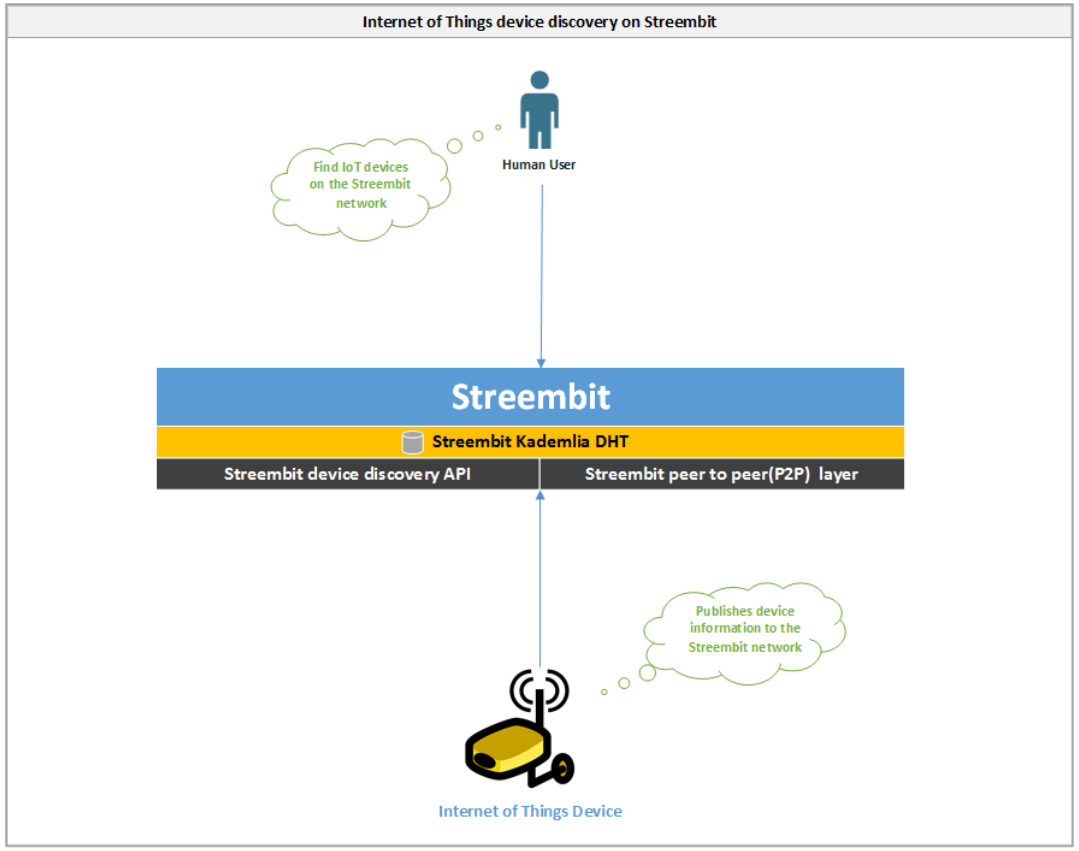
- Security and Privacy
- Occupations - certain professions such as lawyers, journalists need a secure communication tool
- Politics - Incoming communication legislation such as the UK Investigatory Powers Bill
- Lack of standards
- Mitigate the risk of inside job hacking

The solution

One possible solution is using decentralized, pee-to-peer systems to move away from the cloud.

IDC recently concluded that block-chain technologies could be key tools for confirming data origin and accuracy, tracking updates and establishing true data authority for millions of different data fields. The block-chain is a solid model for establishing an audit trail, in addition to transferring and monitoring distinct entities that represent items of value. As a result, block-chain has the potential to serve as a foundation for improving the authenticity and accuracy of business and government records, and Internet of Things devices.

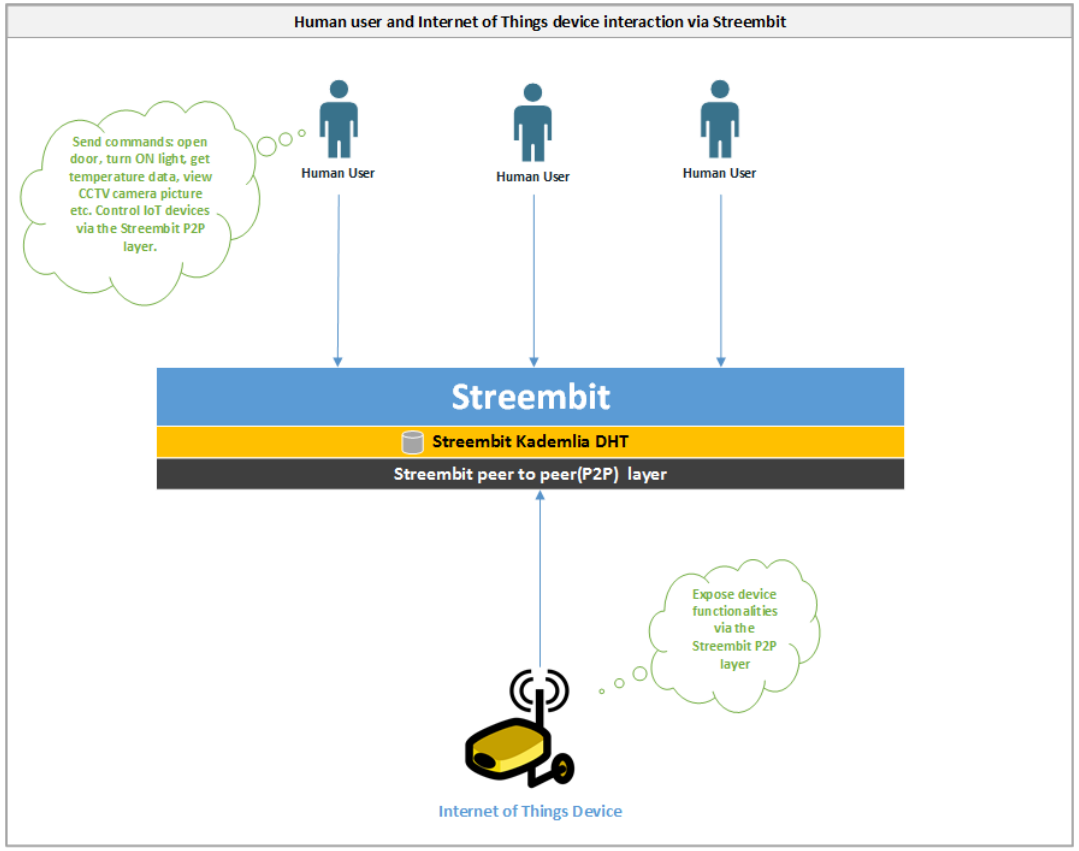
Device Discovery



Control Internet of Things devices

- The Internet of Things devices and human users communicate with each other directly in a peer to peer manner
- The data is end to end encrypted between the human user and IoT device. The encryption key is shared only between the user and device – never with any third parties.
- The device exposes functionalities via the decentralized network and user interface using W3C WoT standards
- The user interacts with the device via the Streembit P2P layer and UI. For example, opening a door, turning ON a light, controlling motor speed, getting temperature data, viewing CCTV pictures etc. all peer to peer, without a centralised solution and via the Streembit user interface.

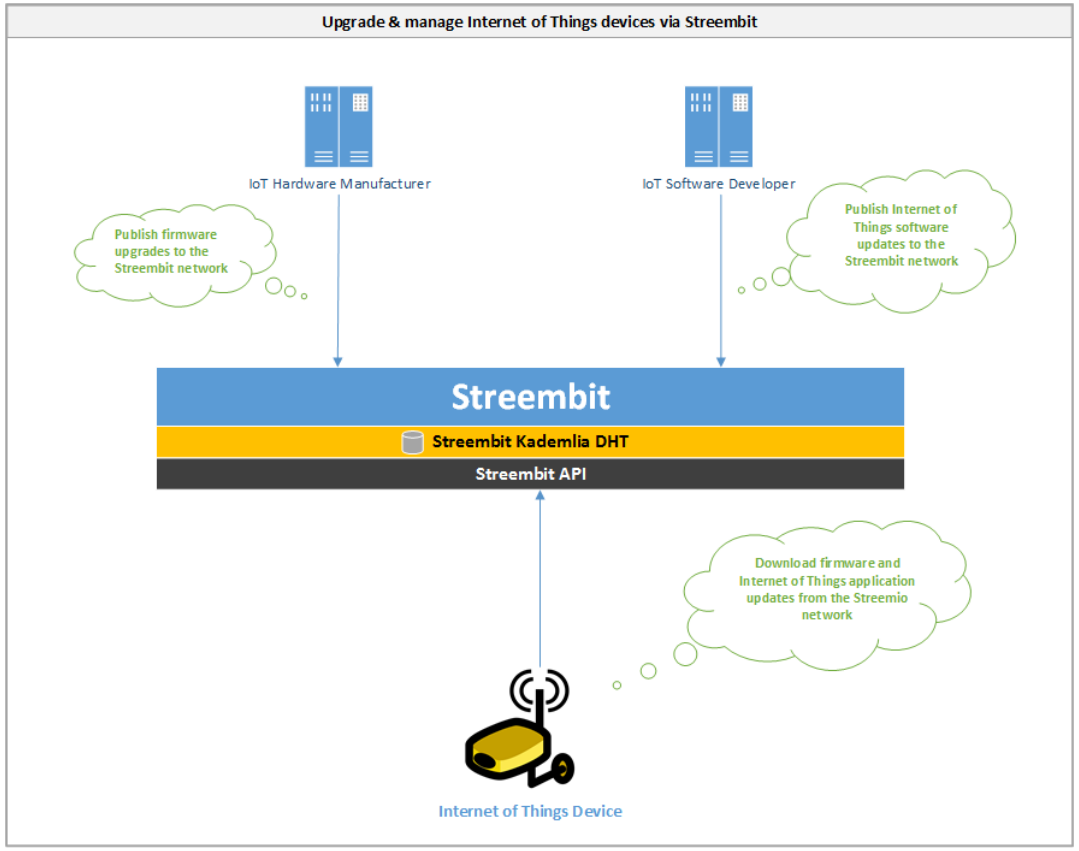
Control Internet of Things devices



Upgrade and manage IoT devices

- Hardware and software providers upgrade Internet of Things devices on the always up and running on decentralized networks.
- Internet of Things device manufacturers and software designers publishes firmware and software updates via the decentralized network.
- Ensure via strong PPKI security that the origin and data integrity of the updates by verifying the public key of the publisher.

Upgrade and manage IoT devices



Strong security

Based on PPKI, ECC cryptography

- Human users and Internet of Things devices use public/private key (PPK) infrastructure and PPK cryptography functions to secure messages
- Each actor of the system must generate a public/private key pair. (Typically keys are generated prior to configuring the device and will be burned into the devices' firmware).
- The device or user publishes the public key to other users of the system.
- The data integrity and authenticity of the messages is guaranteed with PPK signatures.
- Each session between users is secured with strong symmetric cryptography keys.
- All messages between users are secured with 128-bit and 256-bit AES symmetric encryption/decryption.
- The system uses elliptic curve Diffie Hellman (ECDH) key exchange algorithms to facilitate the exchange of session keys

Working on standards

We try to create an IETF standard for decentralized, peer-to-peer IoT.

https://github.com/streembit/DECOD/blob/master/protocol.md

Contact info

Tibor Zsolt Pardi

tzpardi@streembit.com

http://streembit.github.io/

Skype: zsolt.pardi