Signposts

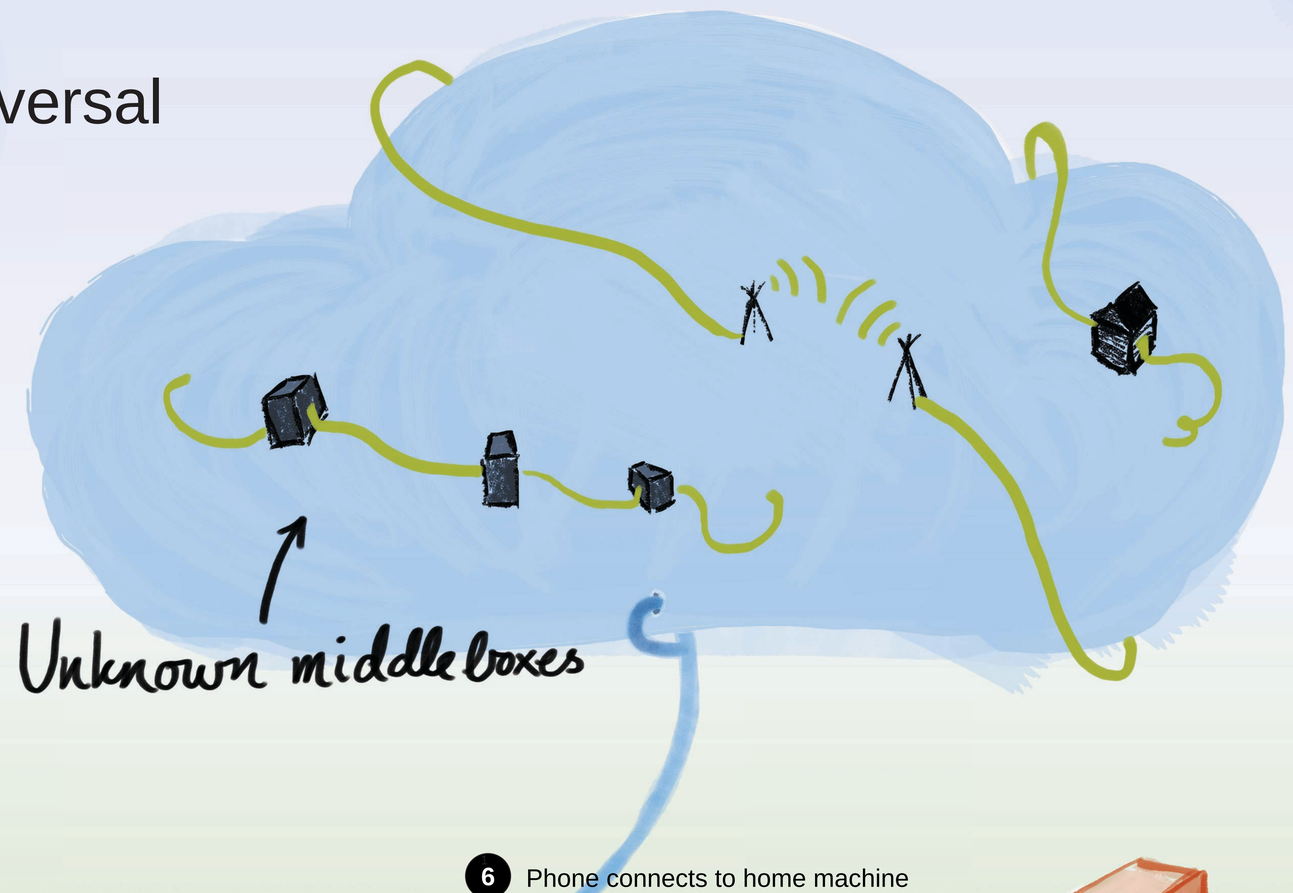
Signposts provides users with a secure, simple mechanism to establish and maintain communication channels between their personal cloud of named devices.

Signpost names exist in the DNSSEC hierarchy, and resolve to secure end-points when accessed by existing DNS clients.

Signpost clients intercept user connection intentions while adding privacy and multipath support. **Signpost** servers co-ordinate clients to dynamically discover routes and overcome the middleboxes that pervade modern edge networks.

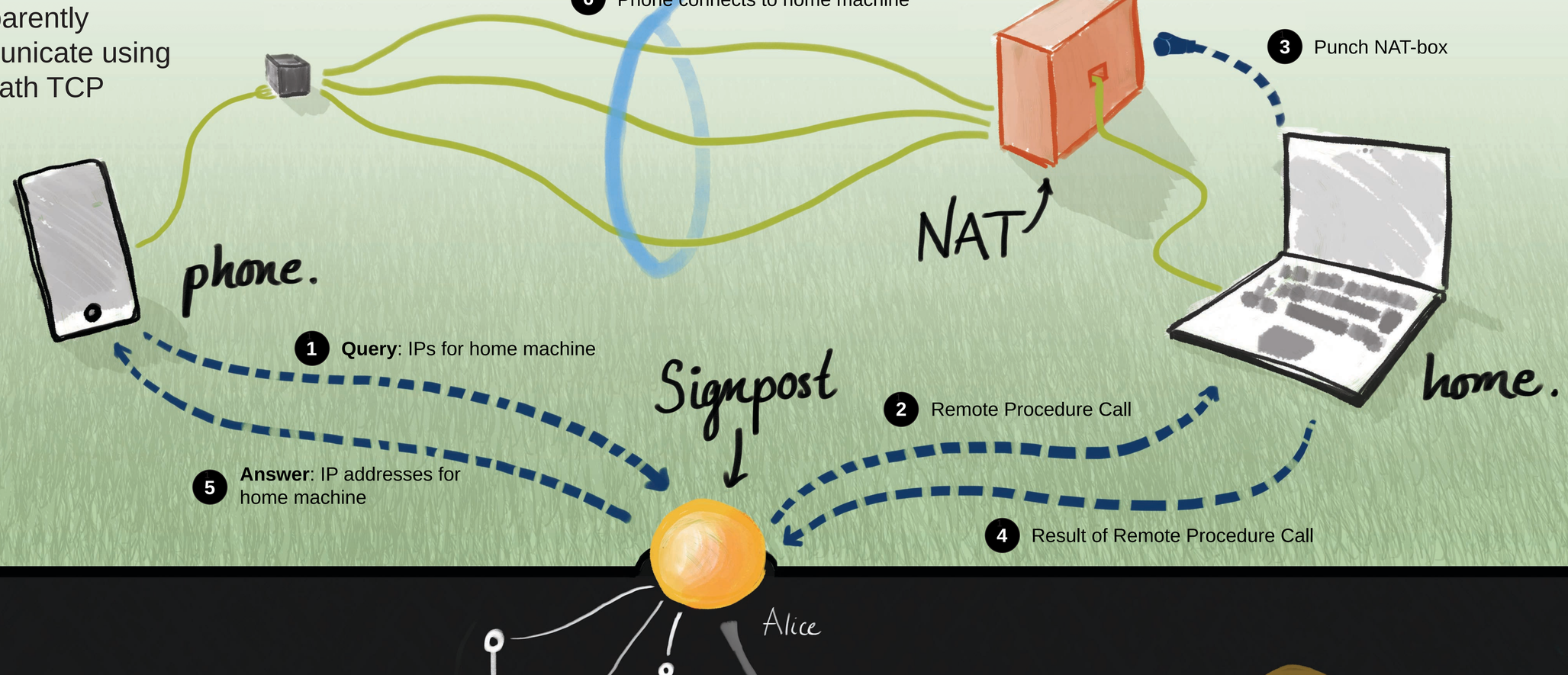
Middlebox traversal

Using a tactics engine, Signposts automatically traverses the middleboxes between your devices



Multipath

Signposts allows processes to transparently communicate using multipath TCP



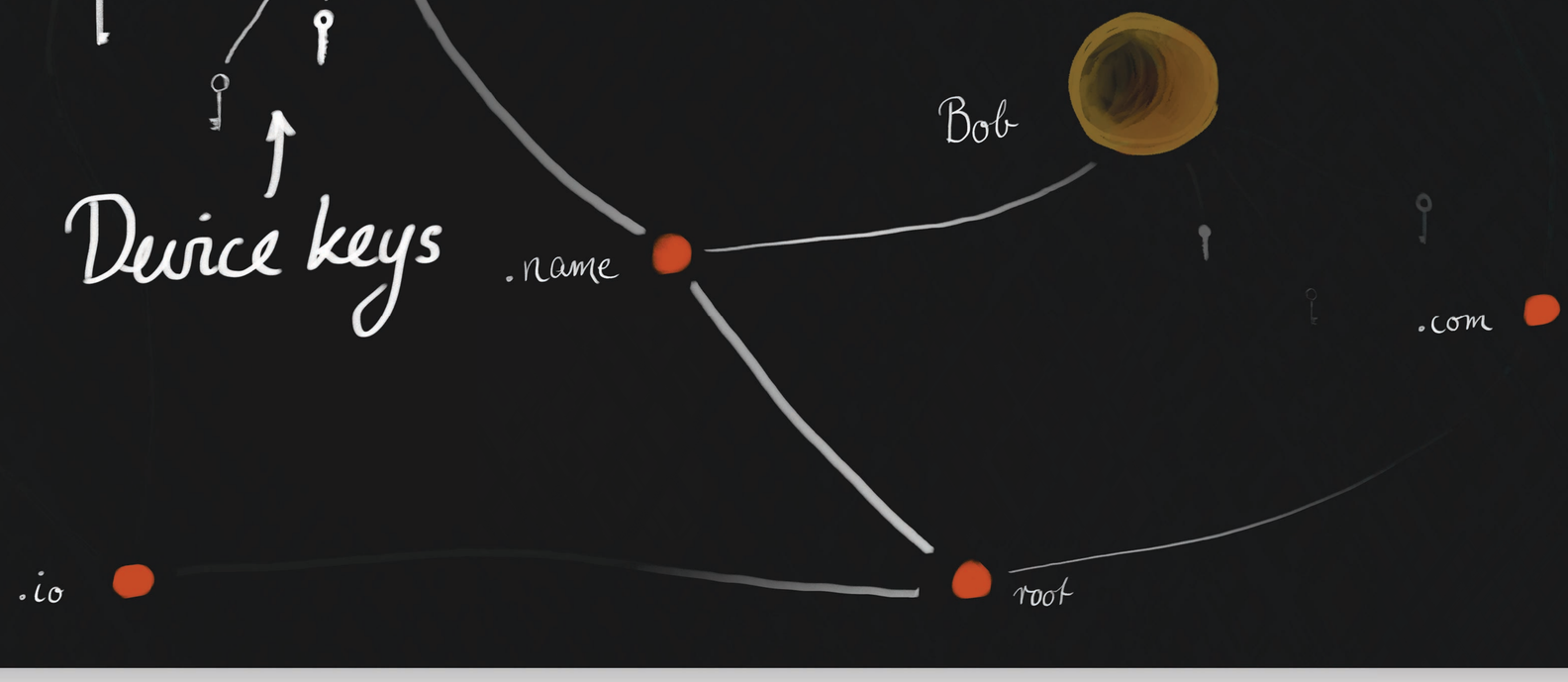
1. Alice's **phone** makes a DNS request
2. The **signpost** server makes a remote procedure call to Alice's **home machine**, which is behind her home router. In this case the remote procedure call instructs the machine to perform a NAT punch
3. The **home machine** performs the NAT punch, allowing the phone to connect to it
4. The home machine replies to the signpost server with information that will permit Alice's phone to use the tunnel created by the NAT punch. This will allow Alice's phone to connect to the home server. The signpost server uses this information to maintain a list of IP addresses related to Alice's home machine.
5. The signpost server then returns a list of possible IP addresses and further instructions to Alice's phone
6. Alice's phone finally connects to the home machine using one of these ip addresses

Secure identity

Signposts is built on top of DNSSEC.

DNSSEC gives both the connecting device, and the device being connected to, a verifiable identity.

DNSSEC is also used to derive secrets (e.g., PEM or X.509) for initiating encrypted communication between devices.



Andrius Aucinas, Jon Crowcroft, Sebastian Probst Eide, Steve Hand, Anil Madhavapeddy, Andrew W. Moore, Richard Mortier, Haris Rotsos, and Narseo Vallina-Rodriguez

UNIVERSITY OF CAMBRIDGE
EPSRC Engineering and Physical Sciences Research Council
horizon DIGITAL ECONOMY RESEARCH
Research Councils UK Digital Economy Transforming Business and Society
The University of Nottingham
UNITED KINGDOM · CHINA · MALAYSIA