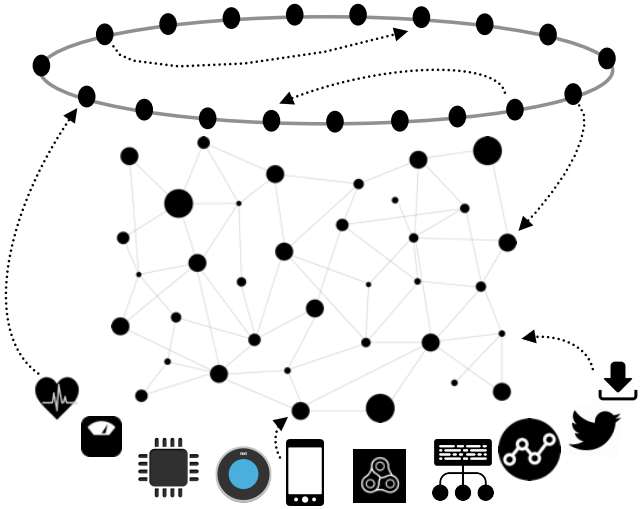
ETH zürich

Towards Blockchain-based Auditable Storage & Secure Sharing of IoT Data



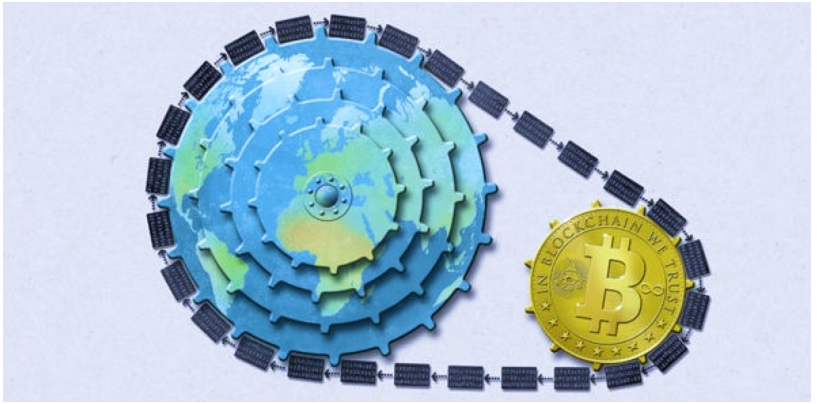
Hossein Shafagh, Lukas Burkhalter, Anwar Hithnawi, Simon Duquennoy

Summer School on Real-world Crypto and privacy, June 2017

Trust in the Internet

- How things started → Trust the goodness in people
- Certification Authorities
- Few powerful corporations control the majority of data in the Internet → lack of control and ownership
- Edge computing on the rise → Data in Proximity
- How can we empower users with data ownership and fine-grained access control?

Blockchain



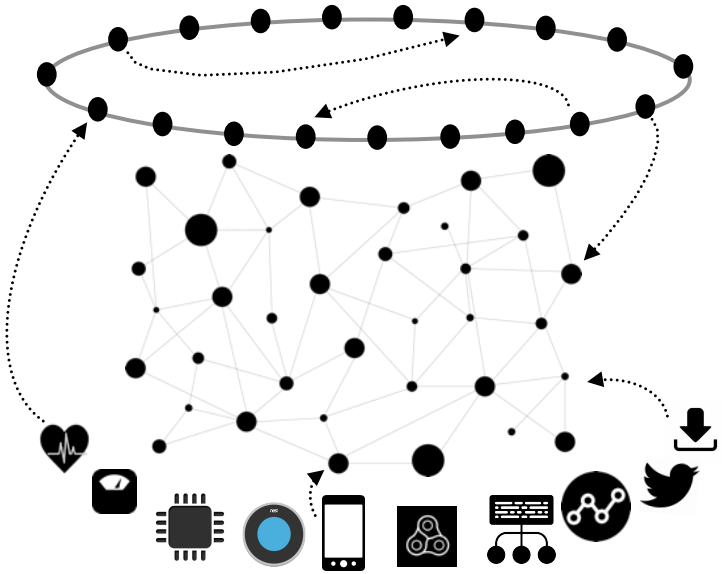
- Distributed ledger
- Bootstrapping trust
- No single point of trust
- Cryptocurrencies: Bitcoin, Zcash, Ethereum
- Altchains: DNS, File-storage, voting, publishing, copy right, supply chain

IoT Ecosystem

- Time-series data
- 3x tiers:
  - Low-power IoT devices
  - Gateway (IP-connectivity)
  - Backend (Cloud)
- Stove-piped architecture
- Isolated data silos
- Tied to lifespan of service

Design Requirements

- **R1** Decentralized, resilient, auditable access control management
  - ownership, secure sharing
- **R2** Secure data storage
  - confidentiality, integrity, authenticity
- **R3** IoT compatible
  - time series, single write, multiple read



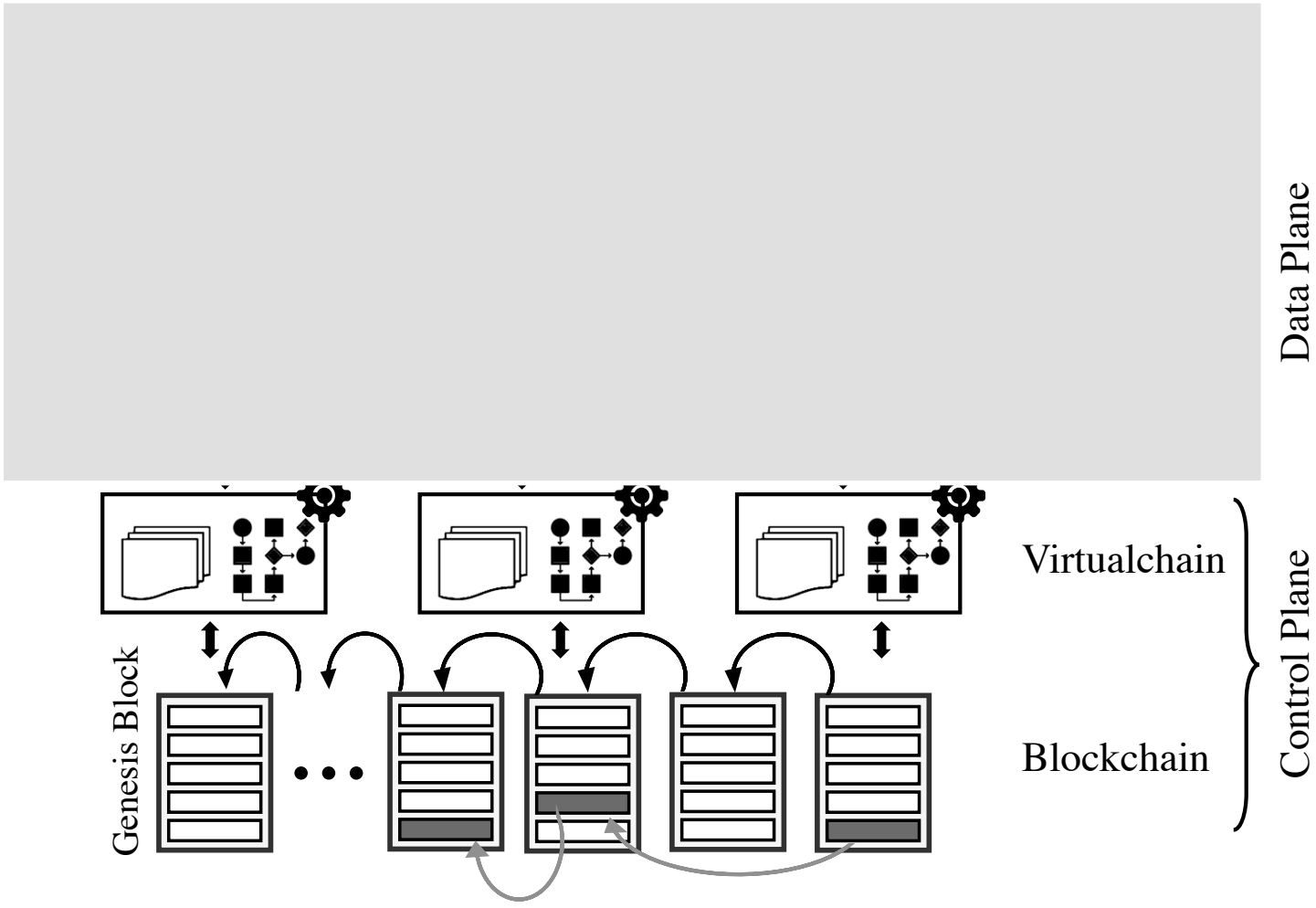
Data plane
(DHT, Cloud)

Control plane
(Blockchain)

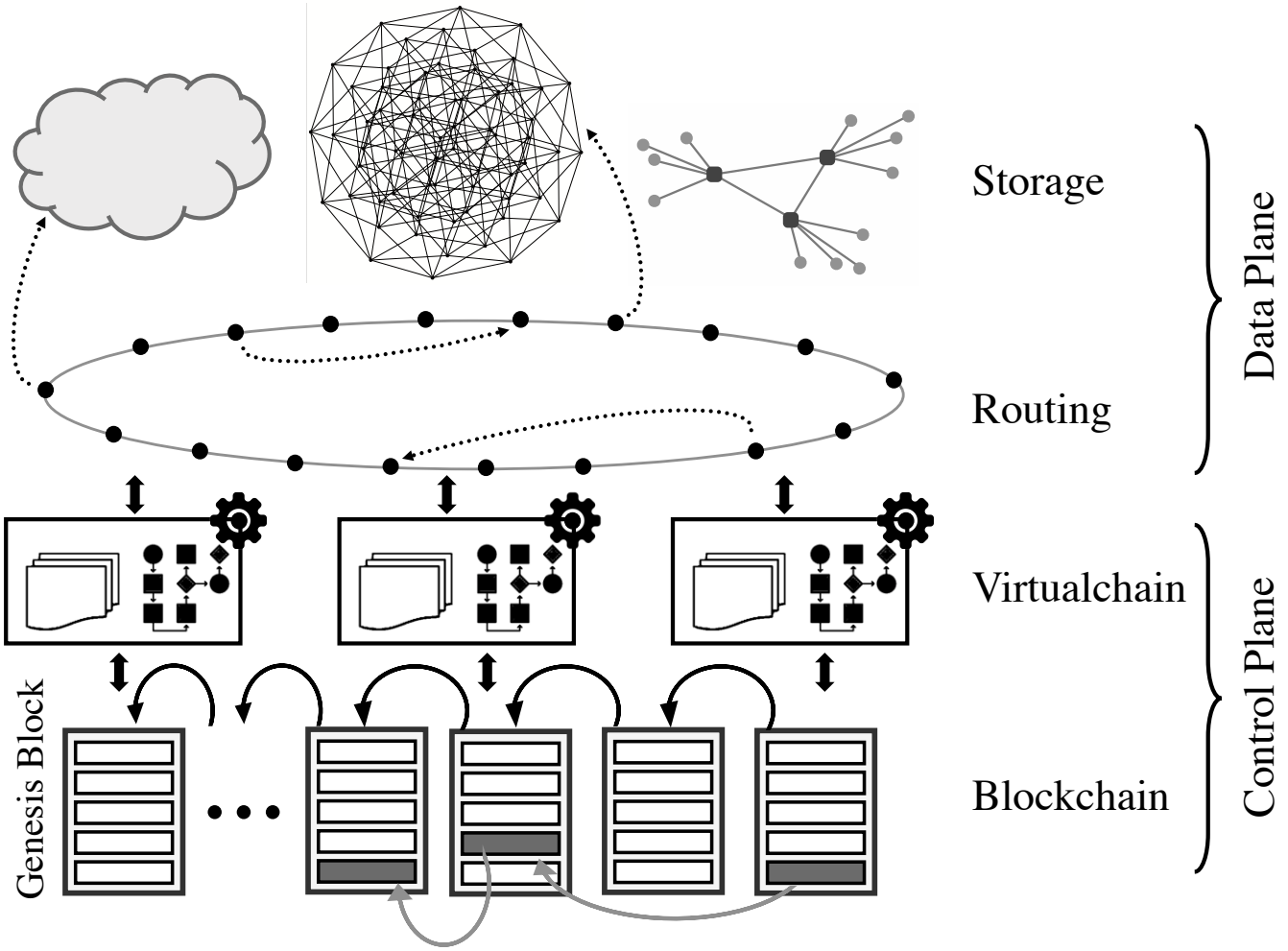
IoT devices &
Services

Design Overview

Design Overview



Design Overview



ETH zürich

Towards Blockchain-based Auditable Storage & Secure Sharing of IoT Data

dropletchain.github.io

@hossein_shafagh

Summer School on Real-world Crypto and privacy, June 2017