Blockchain registries - the future of protocol operations

Alexander Pelov (a@ackl.io)
Protocols need registries that scale

• Protocols and the need for protocol codes
  – CoAP
    • Content-Format
  – CoOL
    • Structured Identifiers
      – IANA allocates SID range to Registrar
      – Registrar allocates sub-ranges to modules
      – (optional) modules can publish the identifiers and the corresponding SIDs (a SID file)
Problem

If no control – a greedy person can allocate all IDs
Blockchain

• Immutable, trustable registry
  – E.g. bitcoin – once a transaction has passed it stays in the blockchain forever
  – 80 bytes of “comment”

• Cheap, tamper-proof public databases
  – Land registries (Hunduras, Greece)

• Solution
  – Use blockchain to allocate the IDs
  – Open question: pricing
    • Pay for each allocated ID?
SIDs

• For SIDs
  – IANA allocates 1 000 000 SIDs for BITCOIN allocation
  – IANA creates an account
    • When a person wants to allocated a range of 100 SIDs, the person pays 1 bitcoin to the IANA SID account and in the comment enters the SID range
  – The SID range is then allocated forever
    • If a consequent transaction is made, it is invalid
  – IANA aggregates once monthly and publishes the information (BITCOIN blockchain is the reference)
• With the money – pay for infrastructure / open-source development of SID tools / charity
Thanks!

- Generalize to other registries
  - Content-Format
  - ...

Alexander Pelov (a@ackl.io)