Secure Software Distribution using Crypto-augmented Smart Contracts

Aniket Kate, Easwar Vivek Mangipudi, Krutarth Rao
Purdue University

(1) Software Distribution and Piracy

- Robust Watermarking
  - Create two versions of the software
  - Robust Watermark cannot be removed without destroying the software

- Time-locked Bitcoin Deposits
  - The Downloader cannot withdraw the funds until the end of the pre-defined period
  - The Sender (Software Hub Owner), if has access to the Downloader’s signing-key can withdraw the funds at any point of time

- Doubly Oblivious Transfer (DOT)
  - Doubly Oblivious Transfer is performed between the parties for the transfer
  - Downloader’s choice for the bit for the Oblivious Transfer corresponds to the Signing-key

(2) New Approach: Building Blocks

- Resource intensive penalizing procedure
  - Wastage of resources including money and time

- Unauthorized sharing

(3) Network

- Any unauthorized distribution is penalized instantly
- No third party is involved

Other Applications using the protocol:

- Data Custodianship
- Social media file sharing
- Non Disclosure Agreements

(4) Protocol

- The Downloader makes a Time Locked Deposit using a Signing-Key
- The Hub makes Watermarked copies of the software
- The Downloader receives one watermarked copy through Doubly Oblivious Transfer using his Signing Key

(5) Protocol and Penalization procedure

- The Hub owner extracts the Signing key from the revealed copy of the software
- She then proceeds to transfer the Bitcoin deposit funds to her account using the obtained Signing key
- The Transaction is instantaneous

(6) Features and Applications