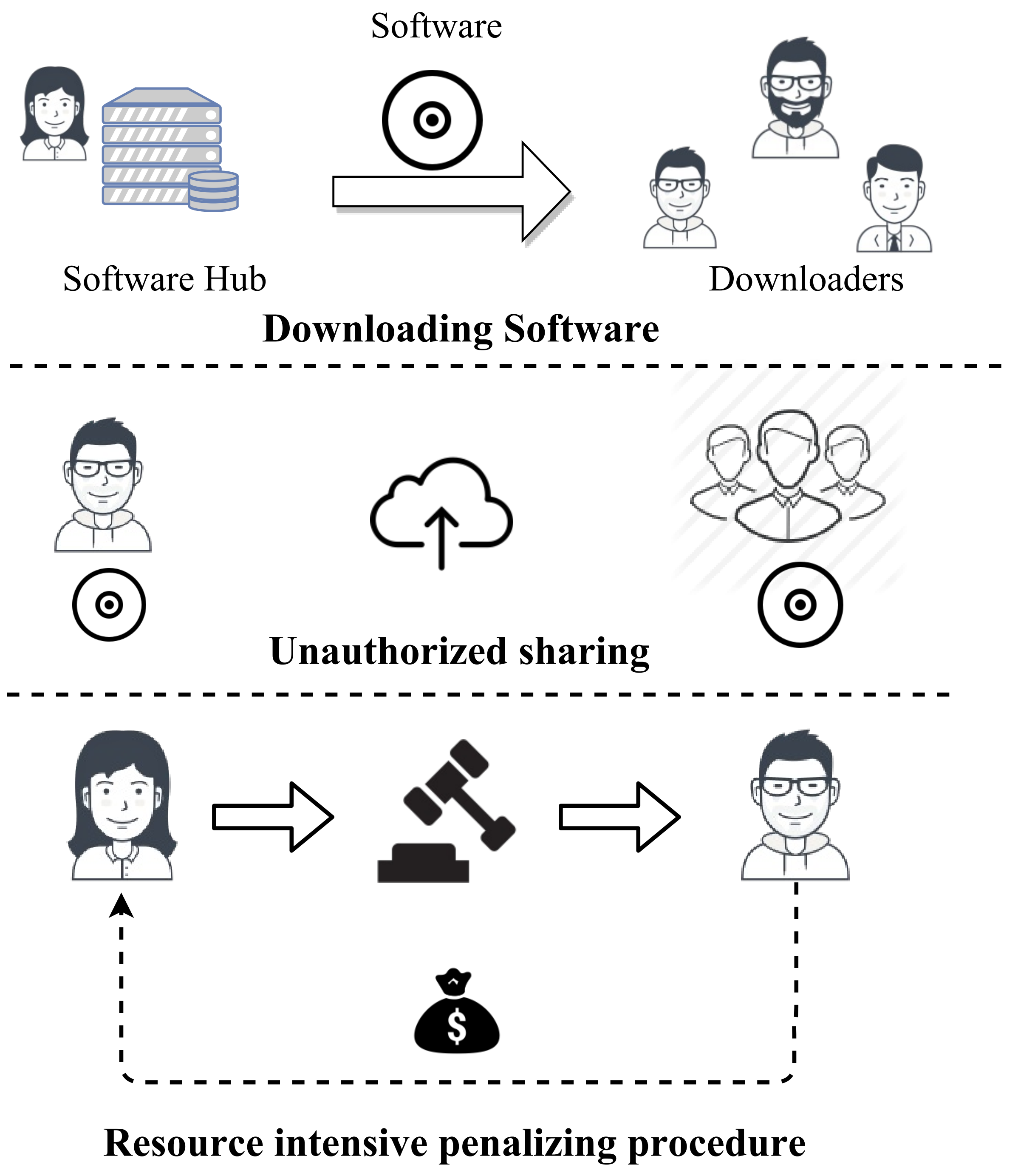
CERIAS
The Center for Education and Research in Information Assurance and Security

Secure Software Distribution using Crypto-augmented Smart Contracts

Aniket Kate, Easwar Vivek Mangipudi, Krutarth Rao
Purdue University

(1) Sofware Distribution and Piracy



Wastage of resources including money and time

(2) New Approach: Building Blocks

Robust Watermarking

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

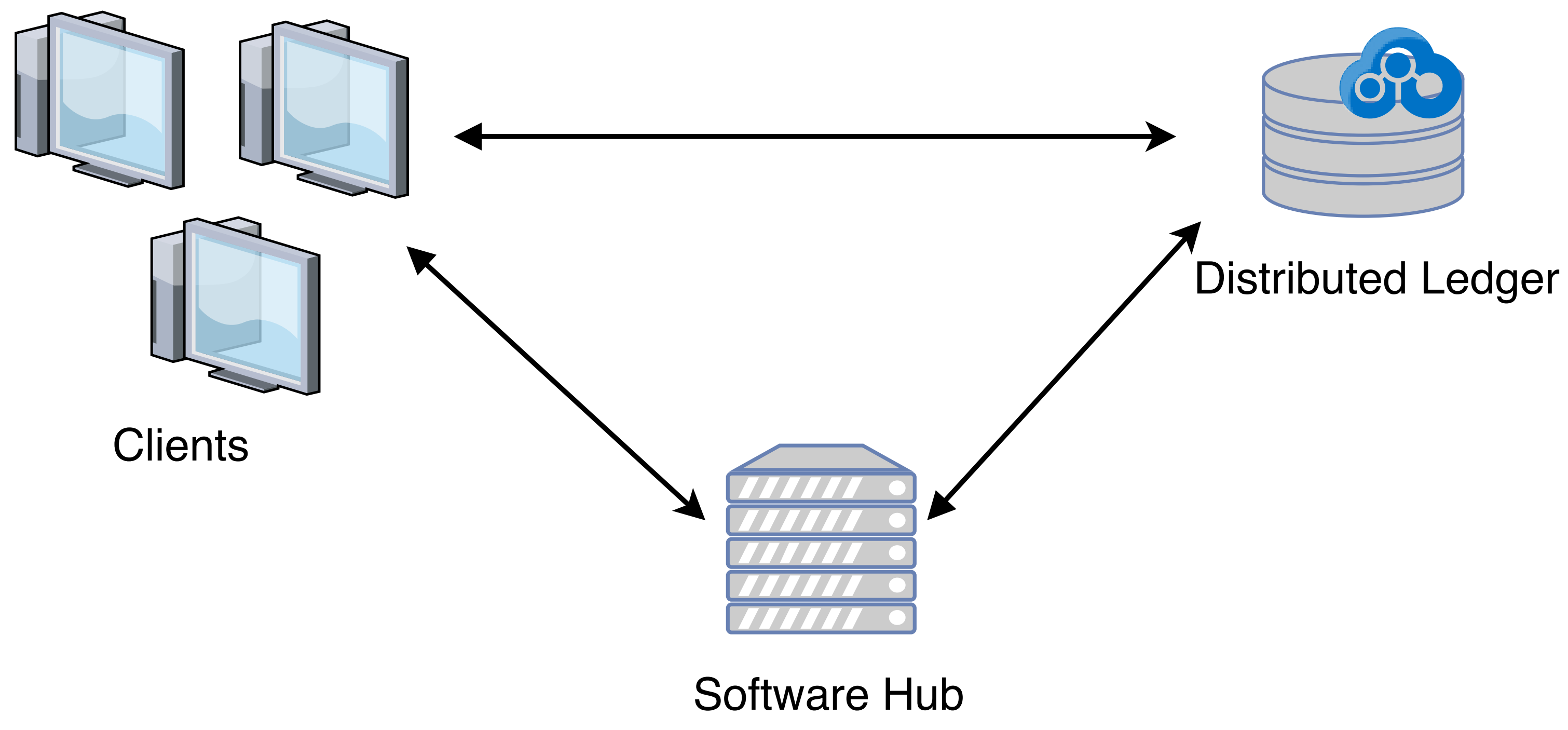
Time-locked Bitcoin Deposits

- 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

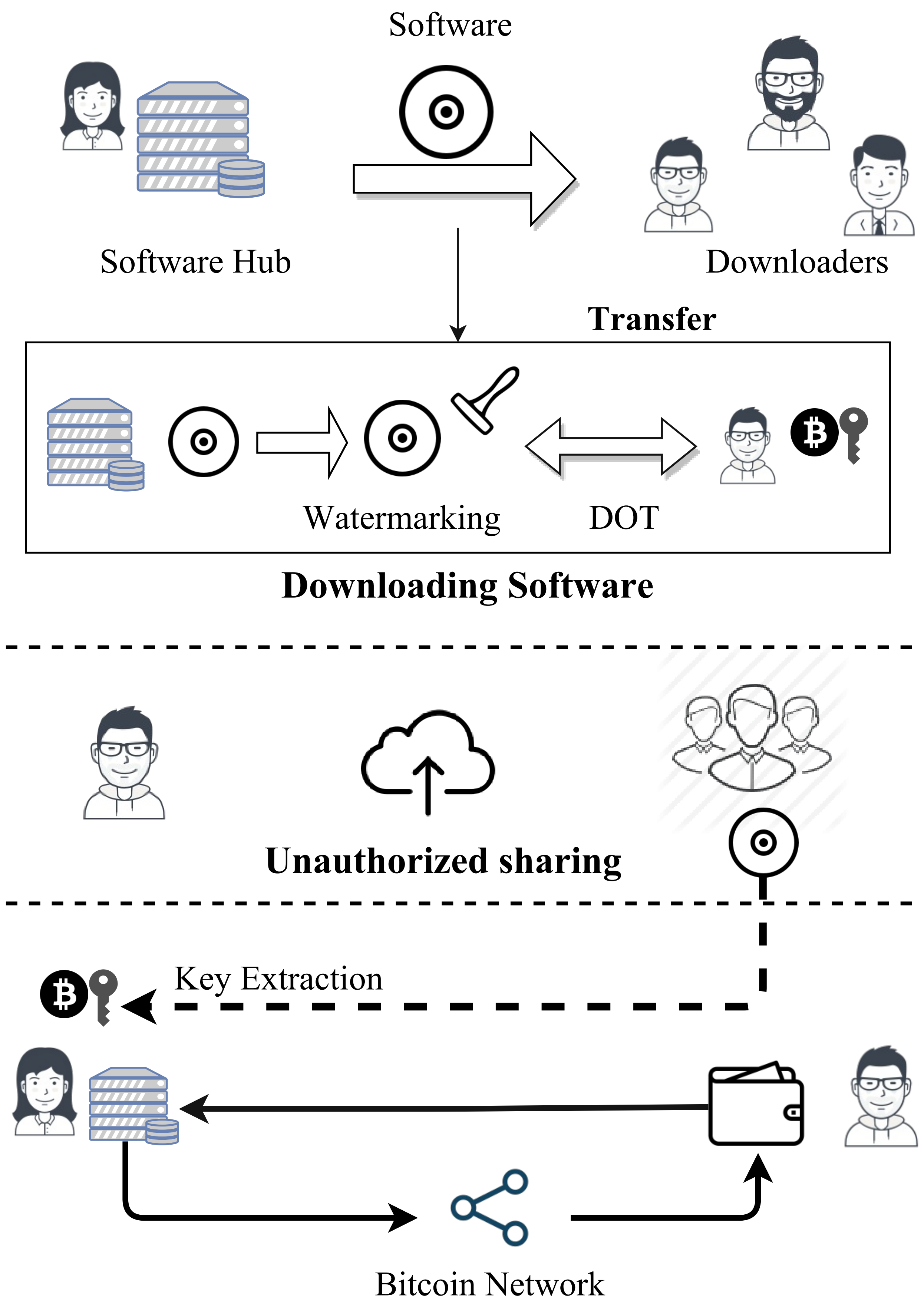
(3) Network



(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



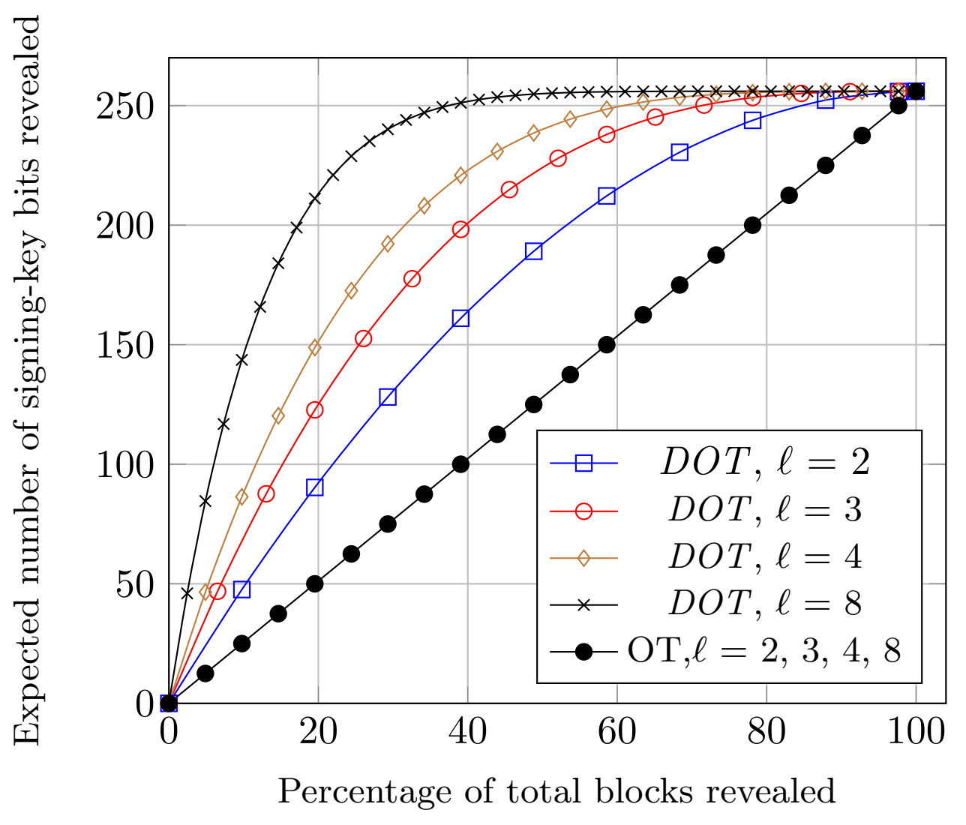
- The Hub owner extracts the Signing key from the revealed copy of the software
- She then proceeds to transfer the Bitcoin deposit funds to her account using the obtained Signing key
- The Transaction is instantaneous

(6) Features and Applications

- 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


Expected number of signing-key bits revealed
Percentage of total blocks revealed
DOT, $\ell = 2$
DOT, $\ell = 3$
DOT, $\ell = 4$
DOT, $\ell = 8$
OT, $\ell = 2, 3, 4, 8$