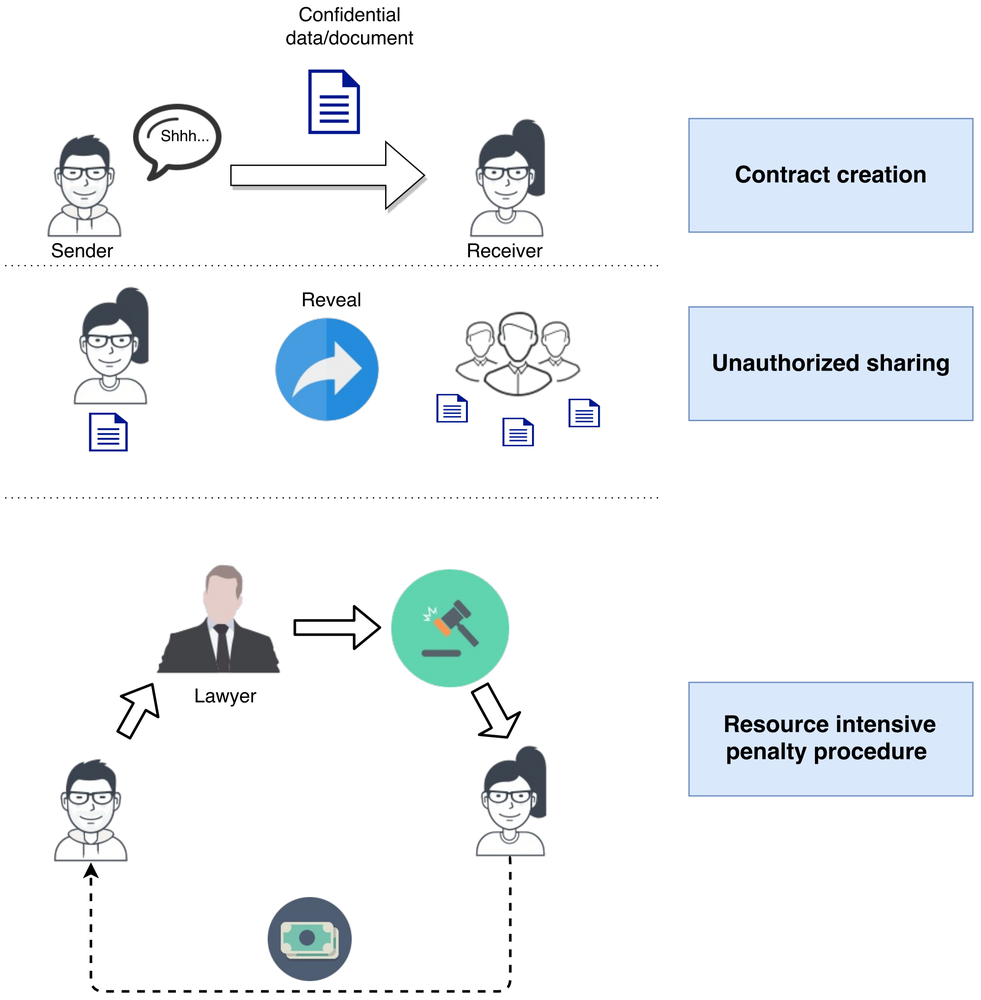
CERIAS

The Center for Education and Research in Information Assurance and Security

SmartNDA: Realizing Non-Disclosure Agreement using Bitcoin Penalty

Aniket Kate, Easwar Vivek Mangipudi, Krutarth Rao
Purdue University

(1) NDA - Present Scenario



Wastage of resources including money and time

(2) New Approach: Building Blocks

Robust Watermarking

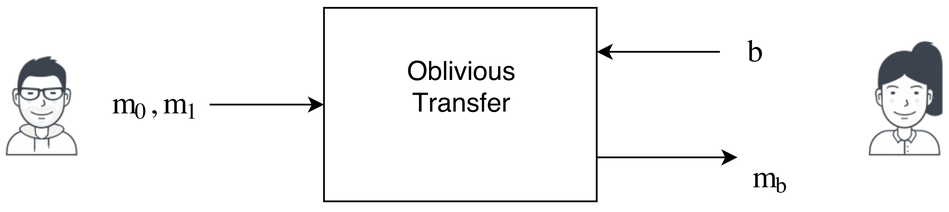
- Create two versions of the document
- Robust Watermark cannot be removed without destroying the document

Time-locked Bitcoin Deposits

- The Receiver (Deposit creator) cannot withdraw the funds until the end of the pre-defined period
- The Sender, if has access to the Receiver's signing-key can withdraw the funds at any point of time

Oblivious Transfer (OT)

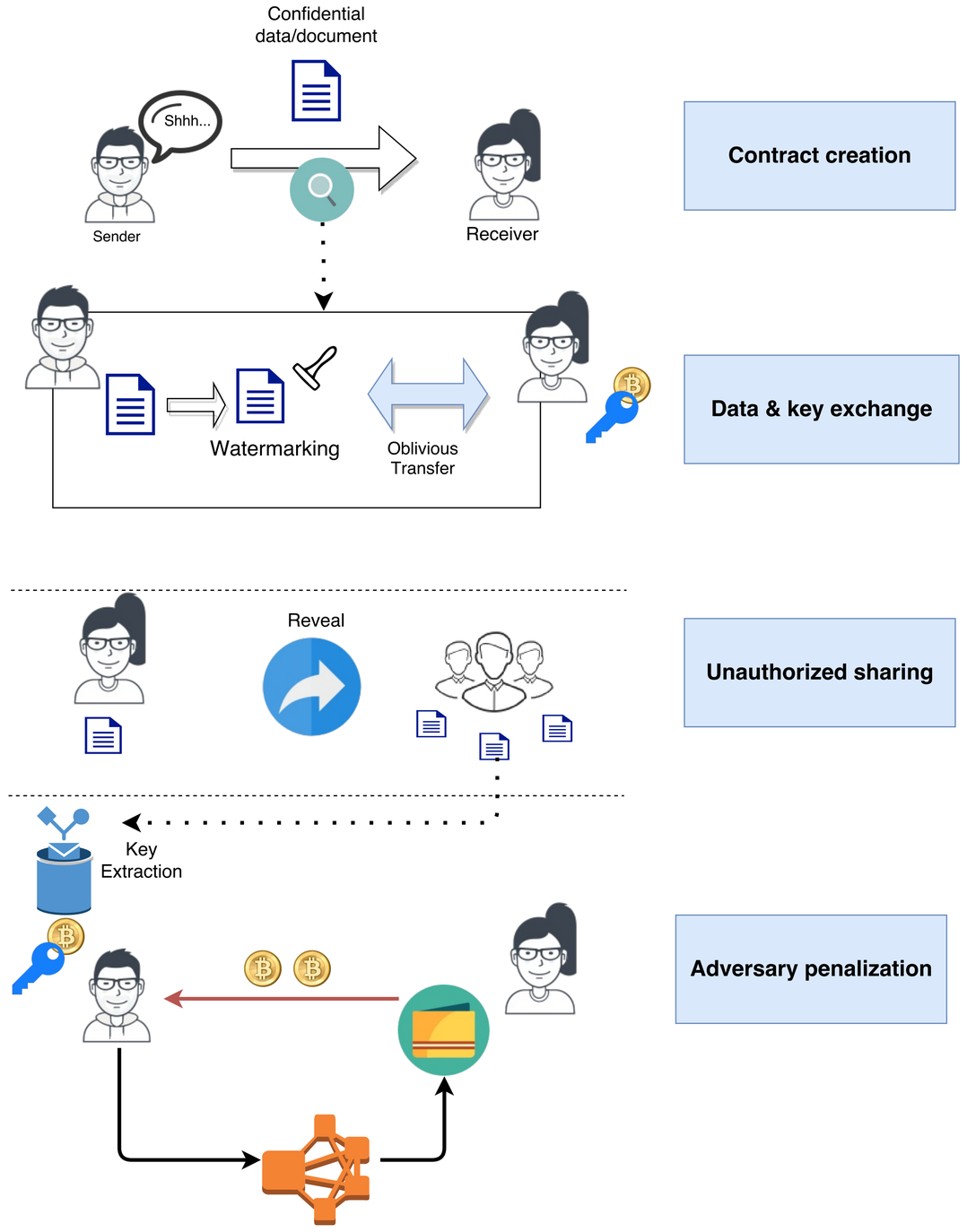
- Oblivious Transfer is performed between the parties for the transfer of the document
- Receiver's choice for the bit for the Oblivious Transfer corresponds to the Signing-key



(3) Smart NDA

- The Receiver makes a **Time Locked Bitcoin Deposit** using a *Signing-Key*
- The Sender makes Watermarked copies of the document
- The Receiver receives one watermarked copy through **Oblivious Transfer** using her Signing Key

(4) Protocol and Penalization procedure



Aim: Instantaneous Penalty.

- The Sender can extract the Signing key from the revealed document
- The Sender then proceeds to transfer the Bitcoin deposit funds to his account using the obtained Signing key
- The Transaction is instantaneous

(5) Features

- Any unauthorized disclosure is penalized instantly
- No third party is involved
- Trust is achieved through the innate properties of the Blockchain of Bitcoin, Oblivious Transfer and Watermarking

(6) Implementation

- As proof of concept and for performance analysis. Images were used as documents while using Cox scheme for watermarking
- Protocol is fast, no run of the protocol takes more than 10 seconds

CERIAS®

PURDUE UNIVERSITY