# Transparent Certificate Revocation for CBE Based on Blockchain

Qin Wang[3], Rujia Li[1,2], Qi Wang[1], David Galindo[2]

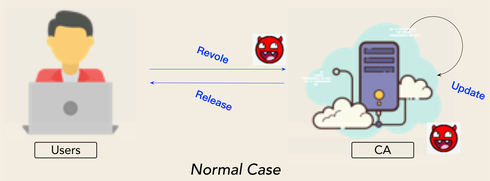
1. Southern University of Science and Technology; 2.University of Birmingham; 3.Swinburne University of Technology

## Introduction

Certificate-based encryption (CBE) [1] achieves the certificate revocation through centralized CA. However, CA's malicious revocation may indirectly make user's decryption fail.

## Problem

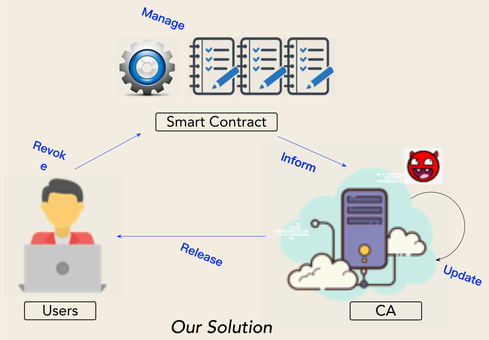
- CA: arbitrary revocation.
- CA: revocation repudiation.
- CA: lack of incentives.




*Normal Case*

## Solution

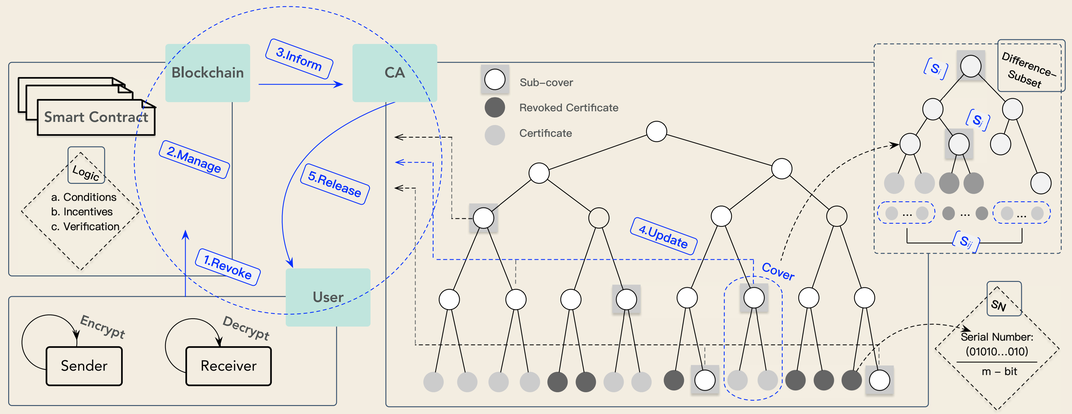
The smart contract is involved as an agent to prevent the CA from maliciously revoking certificates.




*Our Solution*

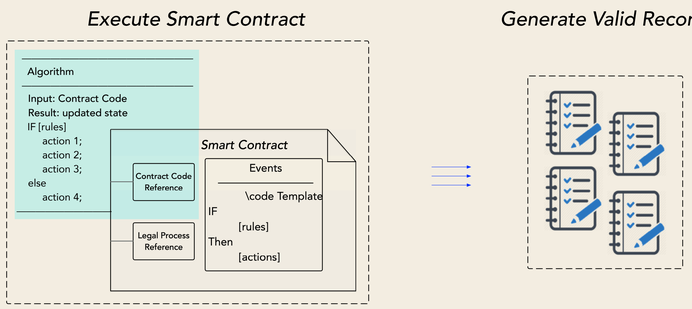
## Protocol

A generic CBE construction includes five algorithms: *Key Generate*, *Set Key*, *Certificate*$^\star$, *Encrypt*, *Decrypt*, in which we emphasize the enhancement of the *Certificate*$^\star$ protocol.




*Blockchain-based CBE Model*

- **(1) Request.** The user sends the revocation requests to a smart contract (SC).
- **(2) Manage.** The SC (1) stores the revocation conditions. (2) sets the incentive policies. (3) verifies the eligibility of revocations.




- **(3) Inform.** The SC informs CA by sending the approval to CA.
- **(4) Update.** The CA updates certificates revocation information through a binary tree (the difference sub-cover approach [2]).
- **(5) Release.** After a successful revocation, the leaves in the subset will be pushed back to users for further decryption.

## Properties

- **[Transparency]**. Revocation data and conditions are transparent.
- **[Accountability]**. Revocation requests are globally auditable.
- **[Non-repudiation]**. CA cannot deny her illegal revocations.
- **[Automation]**. Revocation operations are automatically executed.
- **[Deterrence]**. CA with the illegal revocations will be punished.

## Future work

- The scalability issue inherited from the blockchain.
- The privacy issue in the revocation.

## References

[1] Gentry, Craig. "Certificate-based encryption and the certificate revocation problem." In Crypto. pages 272-293, Springer, 2003.

[2] Naor, Dalit, Moni Naor, and Jeff Lotspiech. "Revocation and tracing schemes for stateless receivers." In Crypto. pages 41-62, Springer, 2001.