

Sikorka

Ethereum Meets The Outdoors!

Lefteris Karapetsas

20/09/2016 – Devcon2 - Shanghai

Who Am I



- Ethereum core developer since 2014, C++ core, Solidity
- Contributor to The DAO.
- Interest in compiler design, AI and smart contracts

What is Sikorka?



What is Sikorka?

A System that:

- Facilitates deploying smart contracts in real world locations
- Enables smart contracts to interface with the environment
- Provide “Proof Of Presence”, that a user is indeed present in a location.

Potential Applications

- Loyalty programs offering discounts to people visiting specific locations
- Proving attendance in a location for official purposes. e.g.: Administrative, Corporate
- Augmented Reality Games

Proof Of Presence

Using mobile phones and software:

- Use mobile geolocation data
- Use a challenge question/answer
- Analyse video data at deployment and compare to image feed at interaction

Proof Of Presence

Using specialized hardware:

- Use scannable QR codes
- RFID tags/readers
- Special hardware deployed on location offering e.g.: bluetooth communication

How Sikorka Works

- Deployed contracts have to follow a specific interface
- System allows users to search for sikorka contracts around them
- Interaction with the contract happens thanks to the ABI and only after providing Proof Of Presence

Contract Interface

```
/**
 * @param _name           A name to give to the contract
 * @param _latitude       The latitude part of the geolocation coordinates
 * @param _longitude       The longitude part of the geolocation coordinates
 * @param _question       The Proof Of Presence challenge question
 * @param _answer_hash    A sha3 hash of the answer to the challenge question
 */
function SikorkaBasicInterface(
    string _name,
    uint _latitude,
    uint _longitude,
    string _question,
    bytes32 _answer_hash
) {
    name = _name;
    latitude = _latitude;
    longitude = _longitude;
    question = _question;
    answer_hash = _answer_hash;
}
```

Contract Interface

Proof Of Presence modifier needed for all user contract interaction

```
/**
 * Require Proof Of Presence for the function to be executed
 * @param _latitude      User's current latitude
 * @param _longitude     User's current longitude
 * @param _answer        The answer to give to the challenge question
 */
modifier need_pop(uint _latitude, uint, _longitude, string _answer) {
    if (sha3(_answer) != answer_hash) {
        throw;
    }
    if (distance(_latitude, _longitude, latitude, longitude) > 1) {
        throw;
    }
    _;
}
```

Contract Interface

Owner should change the challenge question periodically

```
/**
 * Change the challenge question/answer combination
 *
 * @param _question      The new question
 * @param _answer_hash  The hash to the answer
 */
function change_question(string _question, bytes32 _answer_hash) only_owner {
    question = _question;
    answer_hash = _answer_hash;
}
```

Example Contract

```
/**
 * Constructor
 *
 * @param _tokens_to_reward    The number of tokens to reward to each
 *                             user who successfully interacts with
 *                             the contract
 * @param _round_duration     The number of seconds this token round
 *                             will last
 */
function DiscountTokens(
    string _name,
    uint _latitude,
    uint _longitude,
    string _question,
    bytes32 _answer_hash,
    uint _tokens_to_reward,
    uint _round_duration
) SikorkaBasicInterface(
    _name,
    _latitude,
    _longitude,
    _question,
    _answer_hash) {

    tokens_to_reward = _tokens_to_reward;
    token_round_end = now + _round_duration;
}
```

Example Contract

```
/**
 * Claim discount tokens for the shop!
 *
 * @param _latitude    User's latitude coordinate
 * @param _longitude   User's longitude coordinate
 * @param _answer      The answer to the challenge question.
 */
function claimToken(uint _latitude, uint _longitude, string _answer)
    need_pop(_latitude, _longitude, _answer) {

    // User already got their discount tokens for this round
    if (balances[msg.sender] != 0) {
        return;
    }
    balances[msg.sender] += tokens_to_reward;
}
```

Demo Video

Advertising contracts offering discounts to users visiting locations around Berlin

Further Work

- Integrate the light client with the mobile app
- Finish and publish the mobile app in Android
- Improve Proof of Presence
- Integrate with an existing wallet for account management
- Integrate with an existing identity system

Thank you

Thank you for your attention. Any Questions?

For updates:

- Follow **@lifterisjp** on Twitter/Github
- Website <http://sikorka.io> coming soon!

