Decentralized Robinson List

A. Cirillo[1] A. Mauro[1] D. Pennino[2] M. Pizzonia[2] A. Vitaletti[3]
M. Zecchini[3]

3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems, September 25th 2020

[1]Fondazione Ugo Bordoni

[2]Engineering Department
Roma Tre University

[3]Department of Computer, Control and Management Engineering
La Sapienza - University of Rome

Introduction

Robinson List

User contact information are precious gold to marketing strategists.

- End of 2019, 44% scam calls (Source: first Onion)
- Americans lost nearly $9 billion from phone scams in 2018 (Source: First Orion)
- Between 2017 and 2018, scam calls increase by 300%

Robinson List

- *Robinson Lists* are an opt-out list of people who do not wish to receive marketing calls.
- At the same time, it is a tool to provide marketing operators with a more transparent market.
- Centralized service existing in a various countries (e.g. Belgium, UK, Canada, Australia, ...)

Robinson List

- The Italian Robinson List is the *Registro Pubblico delle Opposizioni* (RPO) and it is managed since 2011 by Fondazione Ugo Bordoni.
- Today the RPO manages 1.5Mln records but it is expected to handle 100Mln records by 2021 (due to the introduction of mobile phones).

Why Decentralized Robinson List?

The purpose of this work is the design and evaluation of the RPO as a fully-decentralized service on top of a blockchain technology.

- Empower Citizens giving them fully control of their choices

Why Decentralized Robinson List?

The purpose of this work is the design and evaluation of the RPO as a fully-decentralized service on top of a blockchain technology.

- Empower Citizens giving them fully control of their choices
- Reduce maintenance cost

Why Decentralized Robinson List?

The purpose of this work is the design and evaluation of the RPO as a fully-decentralized service on top of a blockchain technology.

- Empower Citizens giving them fully control of their choices
- Reduce maintenance cost
- It is possible to show cryptographic proof of the subscriber option.

Why Decentralized Robinson List?

The purpose of this work is the design and evaluation of the RPO as a fully-decentralized service on top of a blockchain technology.

- Empower Citizens giving them fully control of their choices
- Reduce maintenance cost
- It is possible to show cryptographic proof of the subscriber option.
- Transnational deployment

Problem Model and Requirements

Model

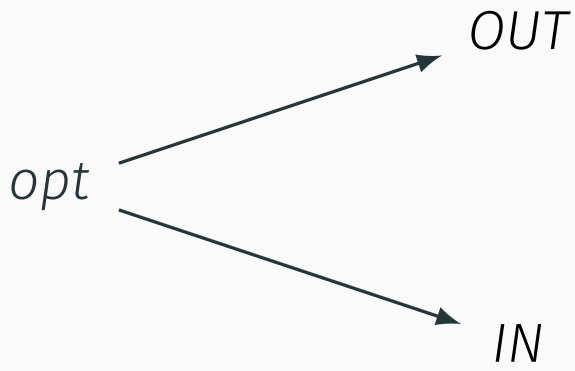
The Robinson List

$< tel, opt >$

Model

The Robinson List

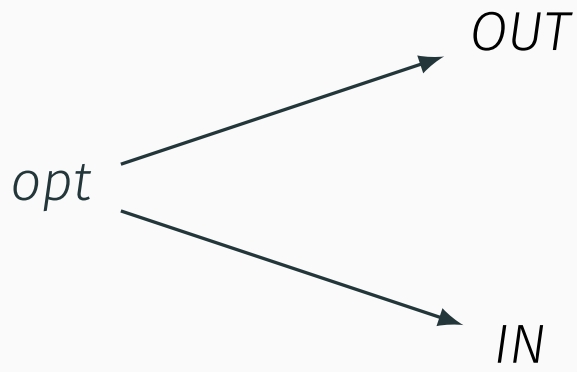
$< tel, opt >$



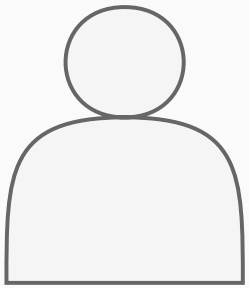
Model

The Robinson List

$< tel, opt >$



Actors

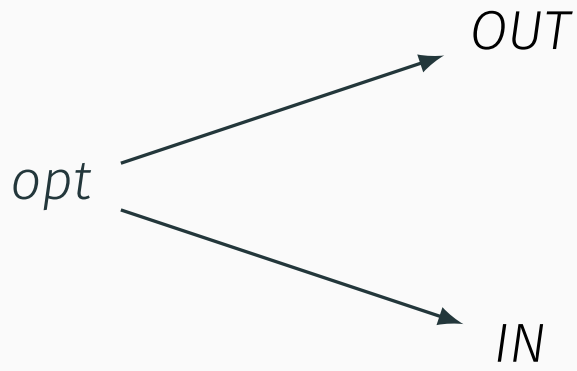


Subscriber

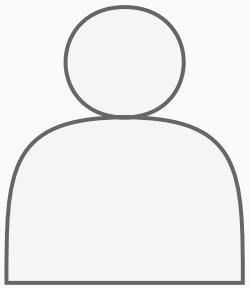
Model

The Robinson List

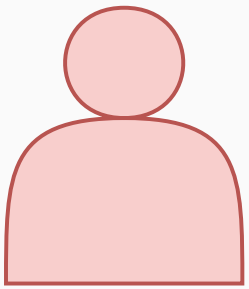
$< tel, opt >$



Actors



Subscriber

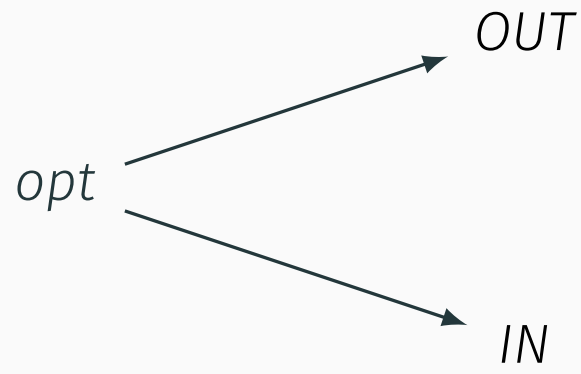


Operator

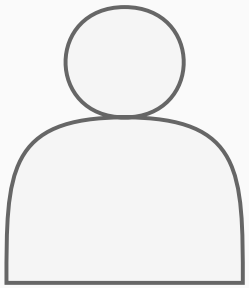
Model

The Robinson List

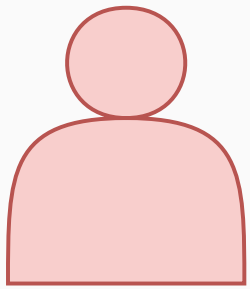
$< tel, opt >$



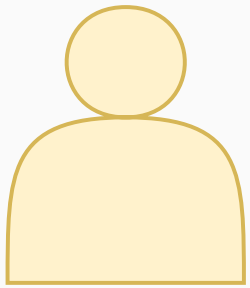
Actors



Subscriber



Operator



Initializer

Requirements

1. Each subscriber can own any number of records $< tel, opt >$

Requirements

1. Each subscriber can own any number of records $< tel, opt >$
2. Only the owner can update a record

Requirements

1. Each subscriber can own any number of records $< tel, opt >$
2. Only the owner can update a record
3. An operator can query the options of a given *tel*

Requirements

1. Each subscriber can own any number of records $< tel, opt >$
2. Only the owner can update a record
3. An operator can query the options of a given *tel*
4. The result of a query is equipped with a cryptographic proof

Requirements

1. Each subscriber can own any number of records $< tel, opt >$
2. Only the owner can update a record
3. An operator can query the options of a given *tel*
4. The result of a query is equipped with a cryptographic proof
5. No actor can change any other subscriber choice without his/her consent

Requirements

1. Each subscriber can own any number of records $< tel, opt >$
2. Only the owner can update a record
3. An operator can query the options of a given *tel*
4. The result of a query is equipped with a cryptographic proof
5. No actor can change any other subscriber choice without his/her consent
6. The system should always be available

Requirements

1. Each subscriber can own any number of records $< tel, opt >$
2. Only the owner can update a record
3. An operator can query the options of a given *tel*
4. The result of a query is equipped with a cryptographic proof
5. No actor can change any other subscriber choice without his/her consent
6. The system should always be available

Centralized solution

Requirements

1. Each subscriber can own any number of records $< tel, opt >$
2. Only the owner can update a record
3. An operator can query the options of a given *tel*
4. The result of a query is equipped with a cryptographic proof
5. No actor can change any other subscriber choice without his/her consent
6. The system should always be available

DLT solution

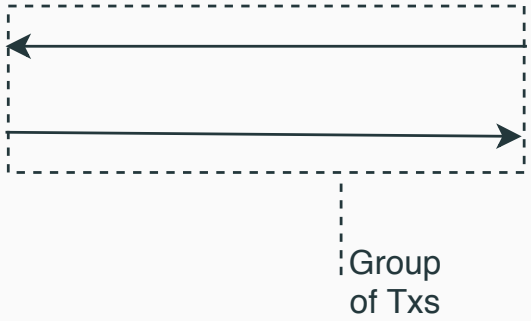
Solution

Ingredients

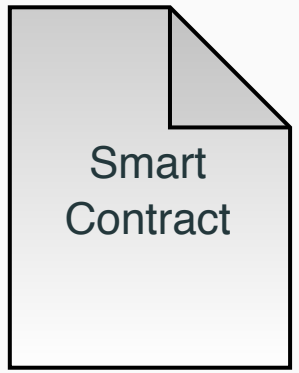
High Scalability

Wallet

Tokens



Group of atomic transactions

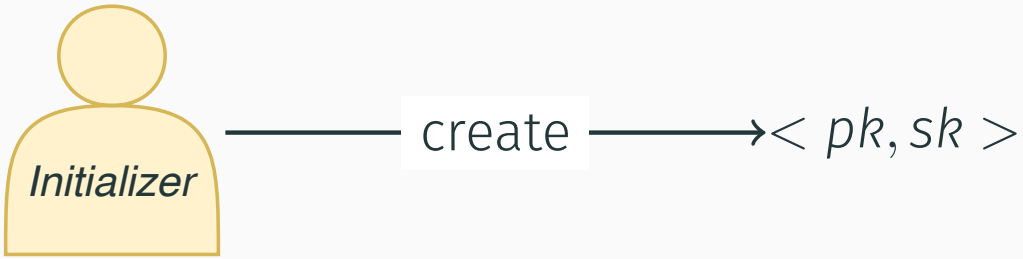


Smart Contract

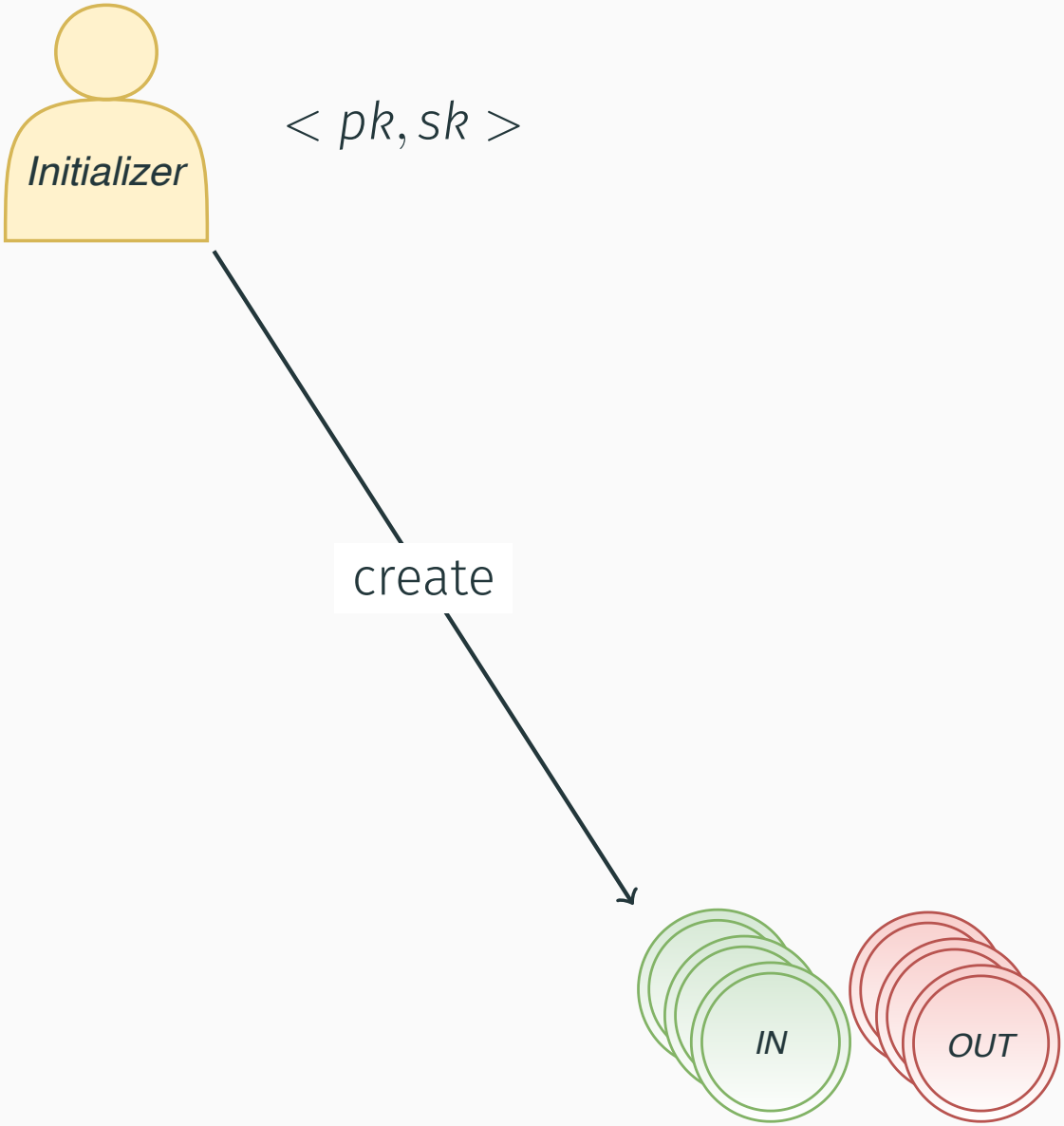
Main operations

- Robinson List Initialization
- Addition of a new telephone number t
- Option switching

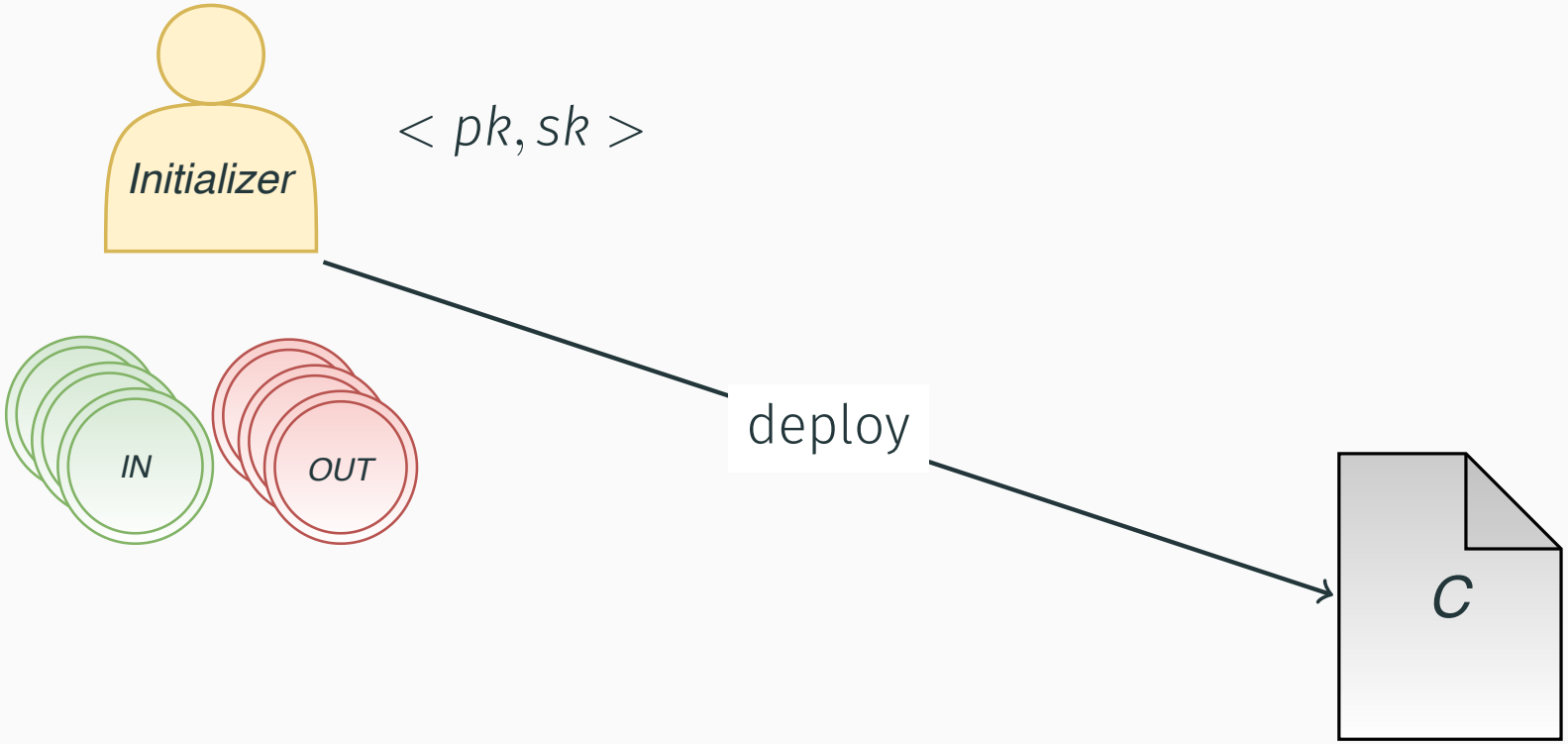
Robinson List Initialization



Robinson List Initialization

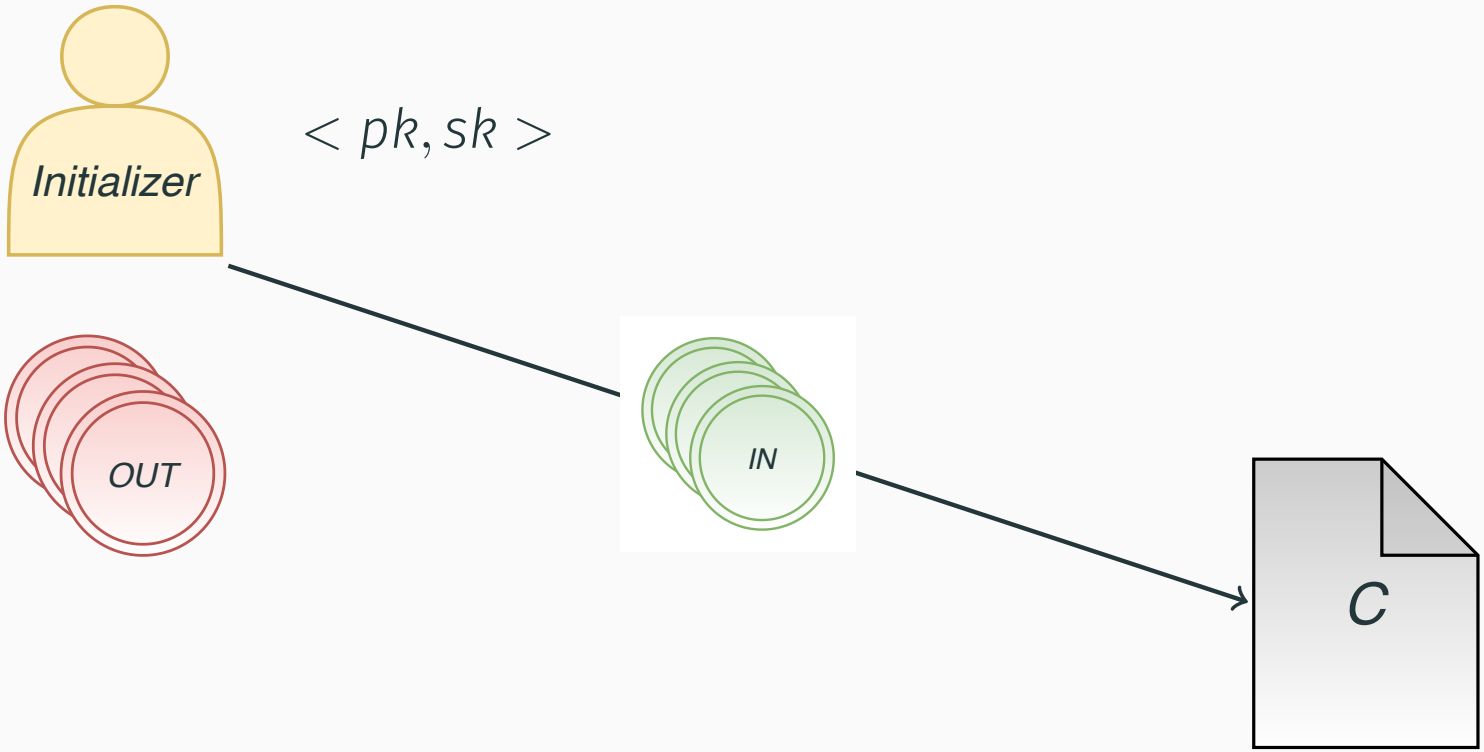


Robinson List Initialization

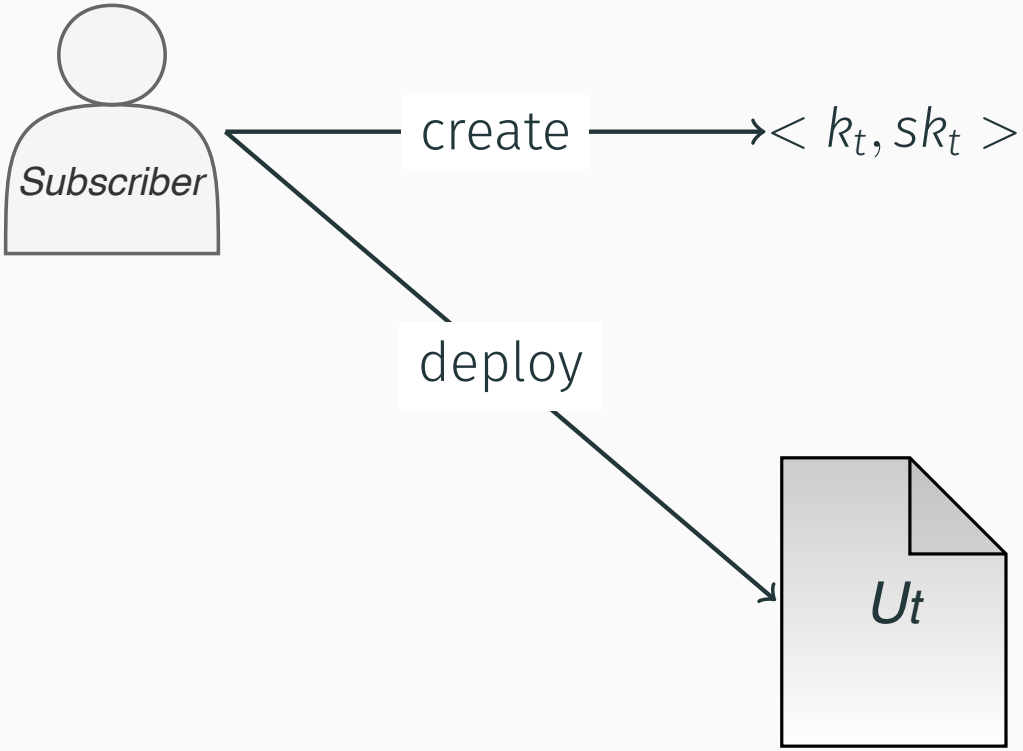


C checks whether the switch operation is well-formed. The switch operation is a group of transaction where (1) transfers 1 *OUT* token to *C* (2) transfers 1 *IN* token from *C* or viceversa.

Robinson List Initialization



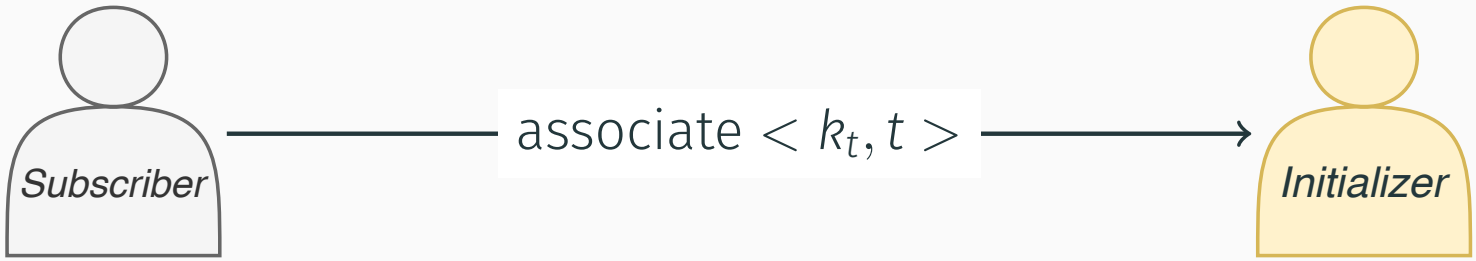
Addition of a new telephone number t



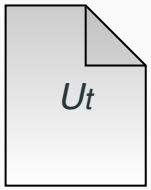
U_t is a standard contract template associate with each subscriber t. It has been designed to avoid exchange of tokens between subscribers in order to respect the *Option Constraint*, defined as follows:

For each telephone number t, the contract U_t contains only either only one *IN* token or only one *OUT* token.

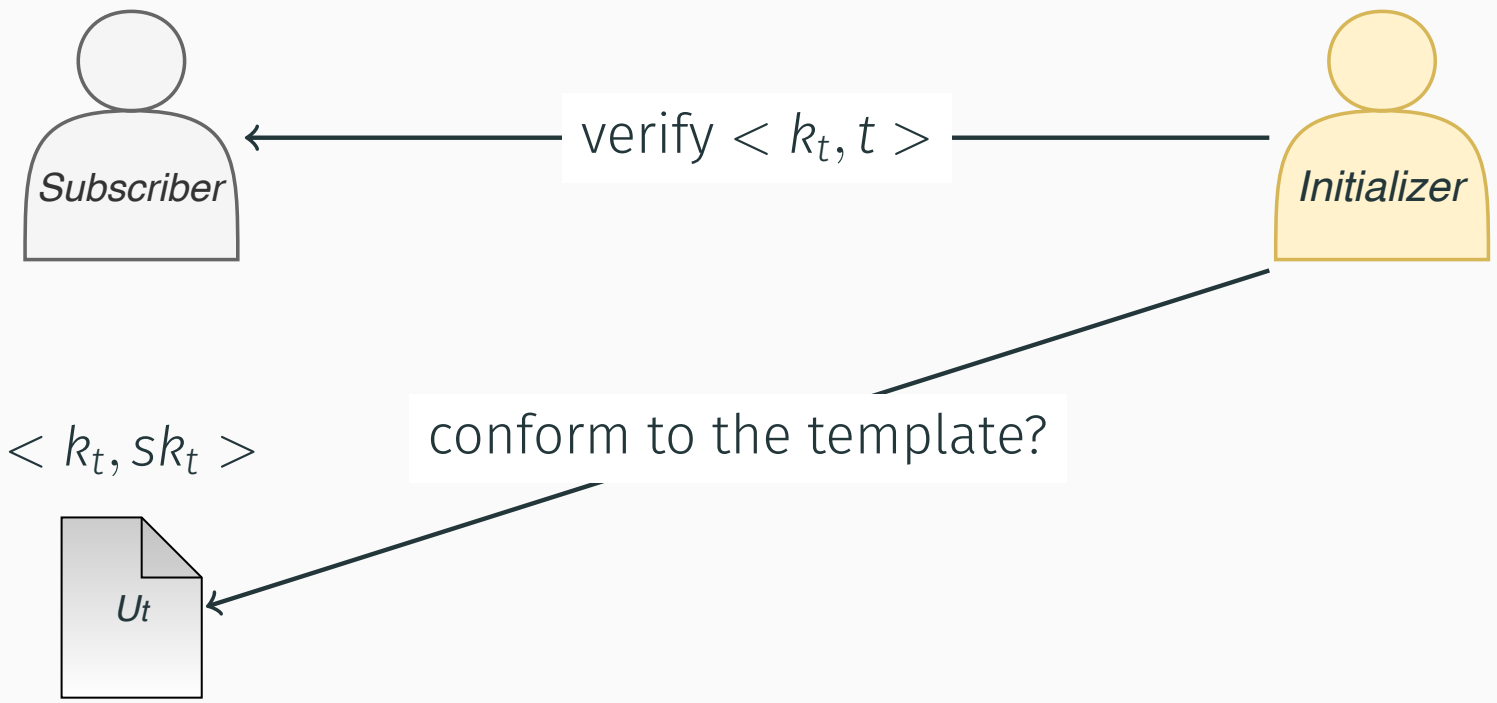
Addition of a new telephone number t



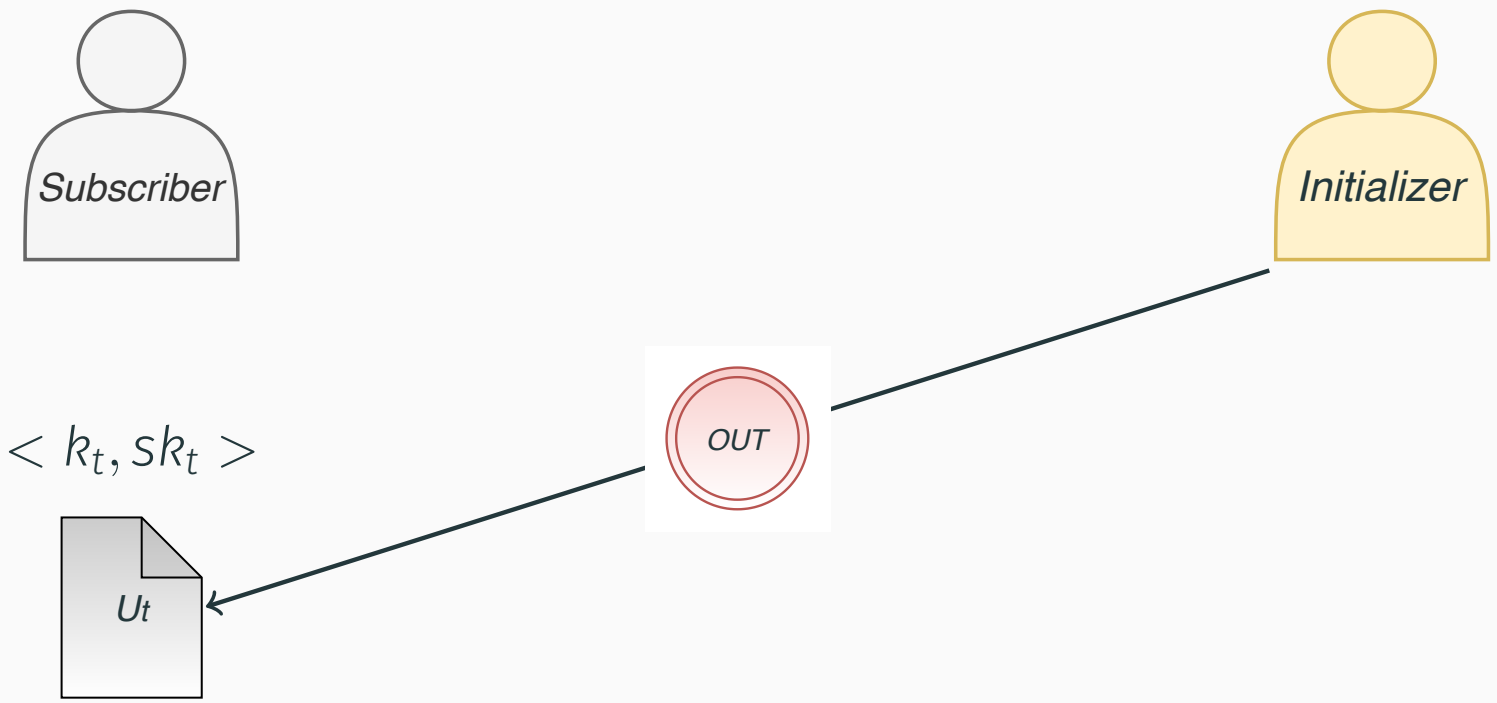
$< k_t, sk_t >$



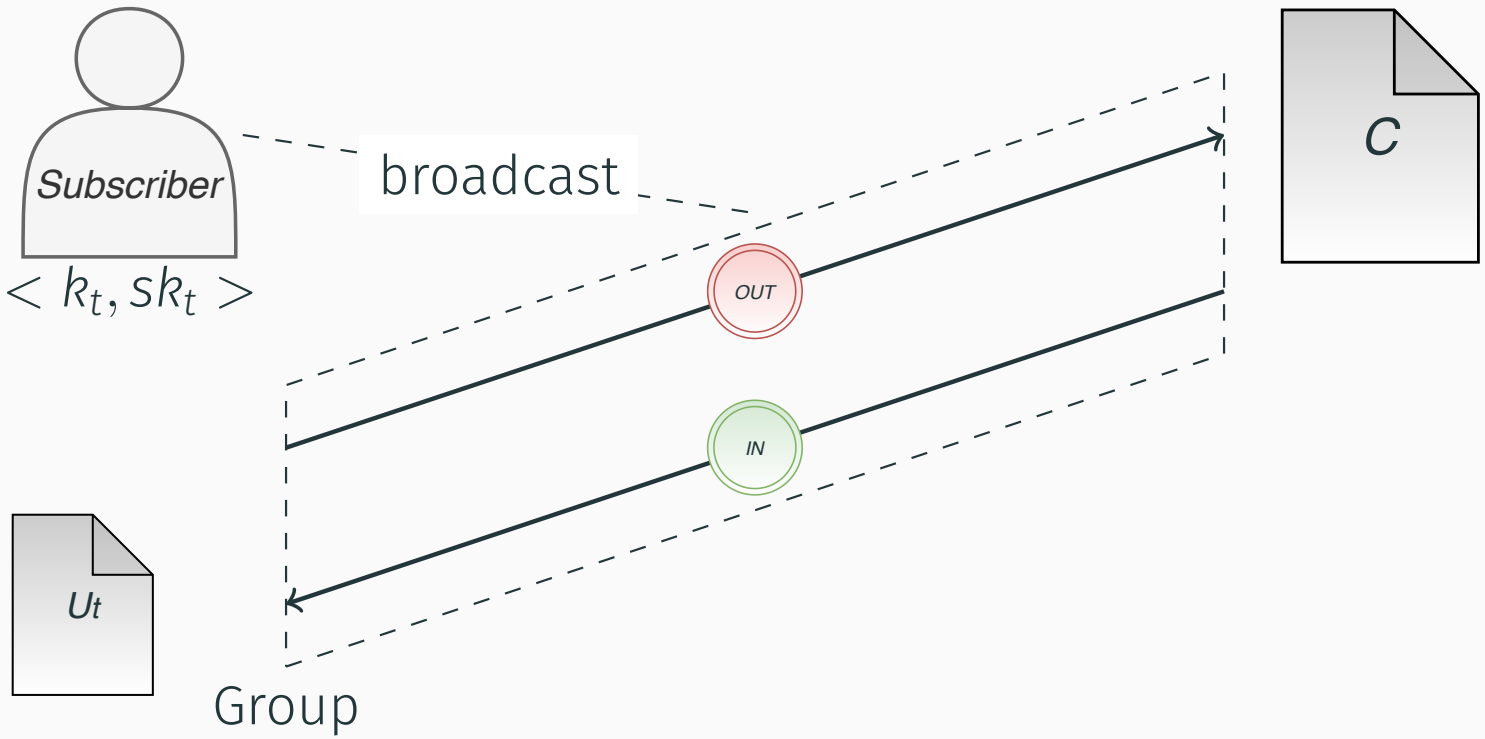
Addition of a new telephone number t



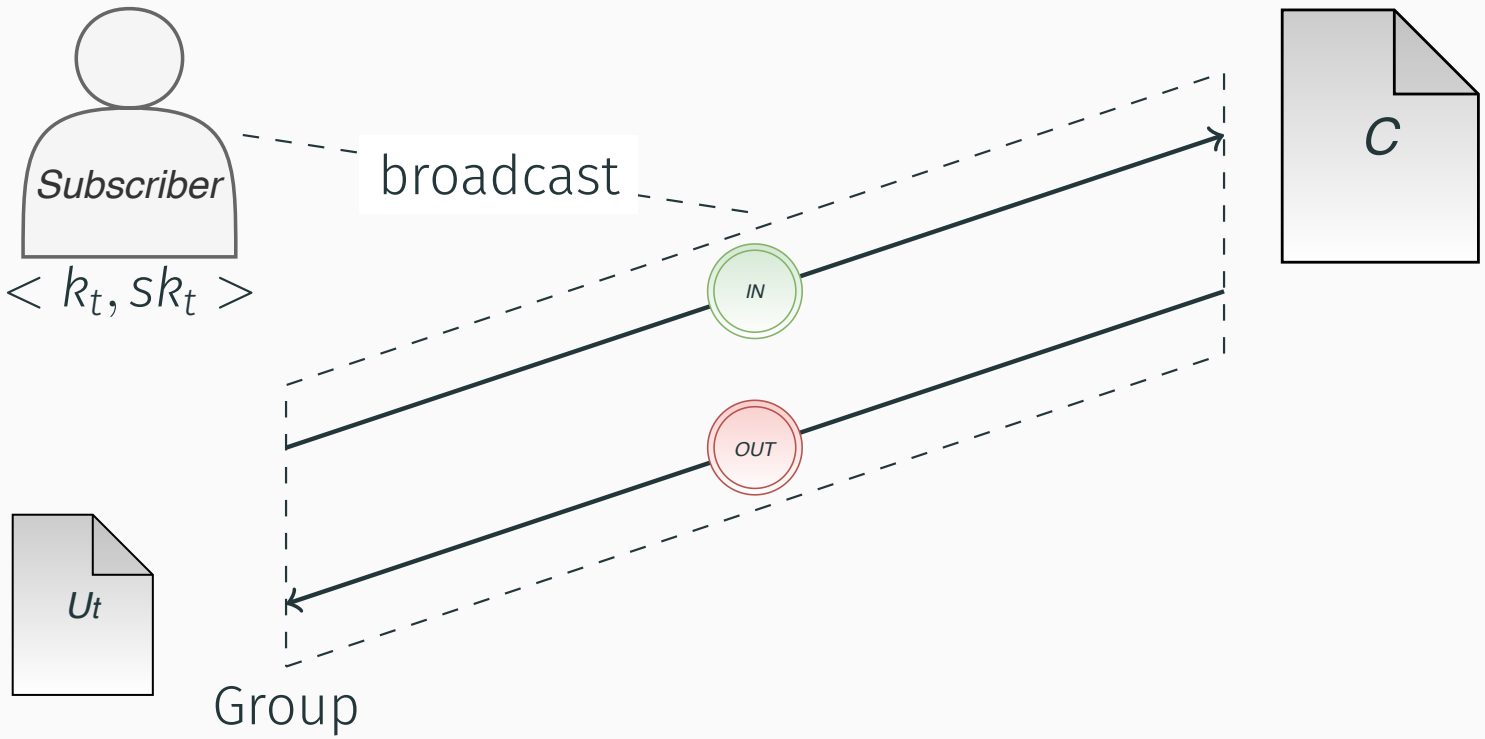
Addition of a new telephone number t



Option switching



Option switching



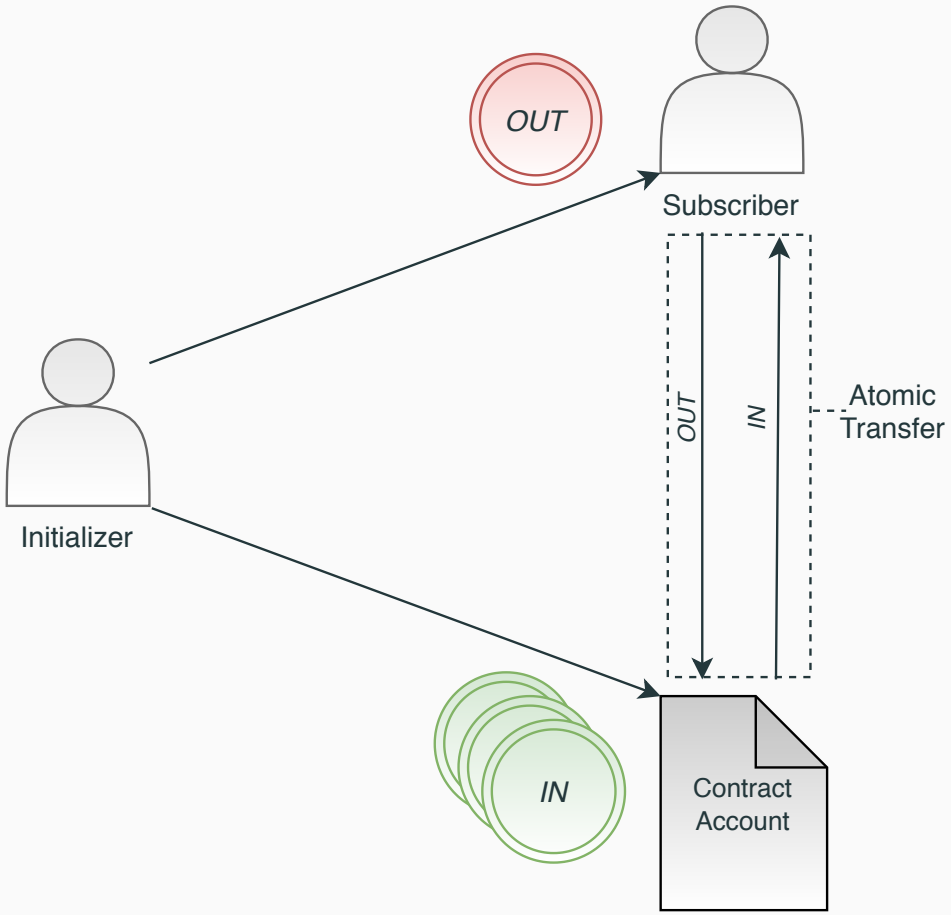
Proof of Concept and Evaluation

Proof of Concept (PoC)

PoC has been realized on *Algorand* because:

- It is one of the best performers in terms of transaction throughput and scalability
- It provides all the technological ingredients required for our application (Atomic Standard Asset, Atomic Transfer and Algorand Smart Contract)

Architecture



Performance Evaluation

- For creating 1000 subscribers' wallet and storing the association public key-phone number in a local database –> 2.67 seconds per user.
- For authenticating and initializing users –> 24 seconds per user.
- For swapping –> 6 seconds.
- For *pruning* the list of phone numbers provided by marketing operators:

Users	1000	500	100
Average	3,533582604	1,813632202	0,3662767768
Variance	0,04431163425	0,008486357303	0,001594493799

Privacy and Identity

Privacy

Subscriber choices are *personal data*. System needs to be complaint with *privacy regulation*, like GDPR.

Pseudoanonymization of personal information and data is widely used. In our scenario consists in not writing in-chain any association among the phone number and subscriber choices.

Only *operators*, and few other entities, needs to know both telephone number and choices

Identity management: possible enhancements

Binding phone numbers and public keys is an *Identity management* problem. With the current solution, the Initializer handles it, so we are using a centralized approach.

Identity management: possible enhancements

We wish to decentralize three tasks of the initializer:

1. Verification of bindings of telephone numbers to public keys

Identity management: possible enhancements

We wish to decentralize three tasks of the initializer:

1. Verification of bindings of telephone numbers to public keys
2. Storing the bindings into a private identity management database

Identity management: possible enhancements

We wish to decentralize three tasks of the initializer:

1. Verification of bindings of telephone numbers to public keys
2. Storing the bindings into a private identity management database
3. Reply to operator queries

Identity management: possible enhancements

We wish to decentralize three tasks of the initializer:

1. **Verification of bindings of telephone numbers to public keys**

The work[1] describes two approaches to perform this operation in a decentralized manner.

It selects randomly a committee of validators that is hard to predict. Each member performs the check autonomously and write in-chain the *proof* of the binding.

[1] Diego Pennino et al. *Binding of Endpoints to Identifiers by On-Chain Proofs*. 2020. arXiv: *2005.00794 [cs.DC]*.

Identity management: possible enhancements

We wish to decentralize three tasks of the initializer:

2. **Storing the bindings into a private identity management database**

Identity pairs $< t, k_t >$ can be easily stored on-chain but they cannot be plaintext due to *privacy regulations*.

Identity management: possible enhancements

We wish to decentralize three tasks of the initializer:

3. **Reply to operator queries**

We aim to define a scheme that allows to access identity pairs autonomously.

Operators can be added and removed dynamically.

Next steps

Next steps

We have showed motivations and the feasibility of the *Decentralized Robinson List*.

Open questions:

- Performance evaluation

Next steps

We have showed motivations and the feasibility of the *Decentralized Robinson List*.

Open questions:

- Performance evaluation
- Privacy

Next steps

We have showed motivations and the feasibility of the *Decentralized Robinson List*.

Open questions:

- Performance evaluation
- Privacy
- Remove the Initializer

Next steps

We have showed motivations and the feasibility of the *Decentralized Robinson List*.

Open questions:

- Performance evaluation
- Privacy
- Remove the Initializer
- Cross-border deployment

Next steps

We have showed motivations and the feasibility of the *Decentralized Robinson List*.

Open questions:

- Performance evaluation
- Privacy
- Remove the Initializer
- Cross-border deployment
- Analysis of other use cases

Next steps

We have showed motivations and the feasibility of the *Decentralized Robinson List*.

Open questions:

- Performance evaluation
- Privacy
- Remove the Initializer
- Cross-border deployment
- Analysis of other use cases
- Selective opt-in/opt-out

Thank you for the attention!