Scalability:
A communication perspective

French-Japanese Workshop on Blockchain technologies
and application to digital trust

Quentin Bramas

Université de Strasbourg

Slides available on https://bramas.fr

November, 14th, 2023, Keio University, Tokyo

Who am I ?

カンタ　　ブラマス

Quentin Bramas,

Associate Professor in Strasbourg, France

I work on Blockchain, BlockDAG

And also in distributed algorithms:

- mobile autonomous robots
- routing protocols
- dynamic graphs

Scalability ?

- Consensus protocol
- Storage
- Throughput
- Latency
- …

Two of my work on Scalability

- Consensus Protocol
- Throughput / Application

Scalability of the consensus protocol

Two main category of blockchains:

- permisionless (Bitcoin, …):

  PoW, Arbitrary number of participants, very slow

- permisionned, consortium (RedBelly, …):

  DBFT, limited number of validators, fast

First Work: Proof-of-Interactions

First Work: Proof-of-Interactions

Main goal: replacing proof-of-work, to reduce energy consumption.

First Work: Proof-of-Interactions

Main goal: replacing proof-of-work, to reduce energy consumption.

Idea: use the interactions between the participants to elect the next block writer.

First Work: Proof-of-Interactions

Main goal: replacing proof-of-work, to reduce energy consumption.

Idea: use the interactions between the participants to elect the next block writer.

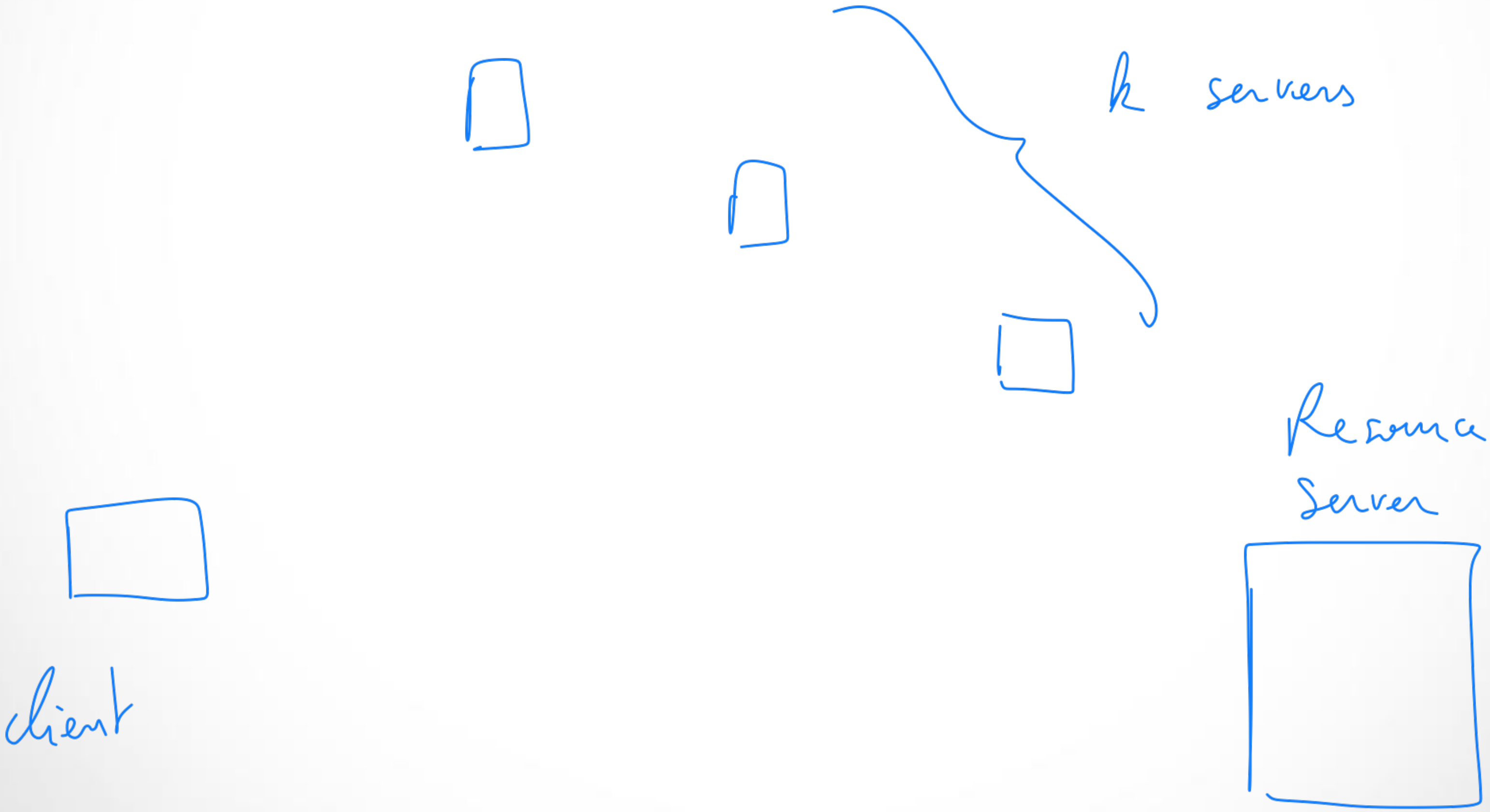
Current limitation: fixed set of participants, but can be very large.

The guided tour puzzle

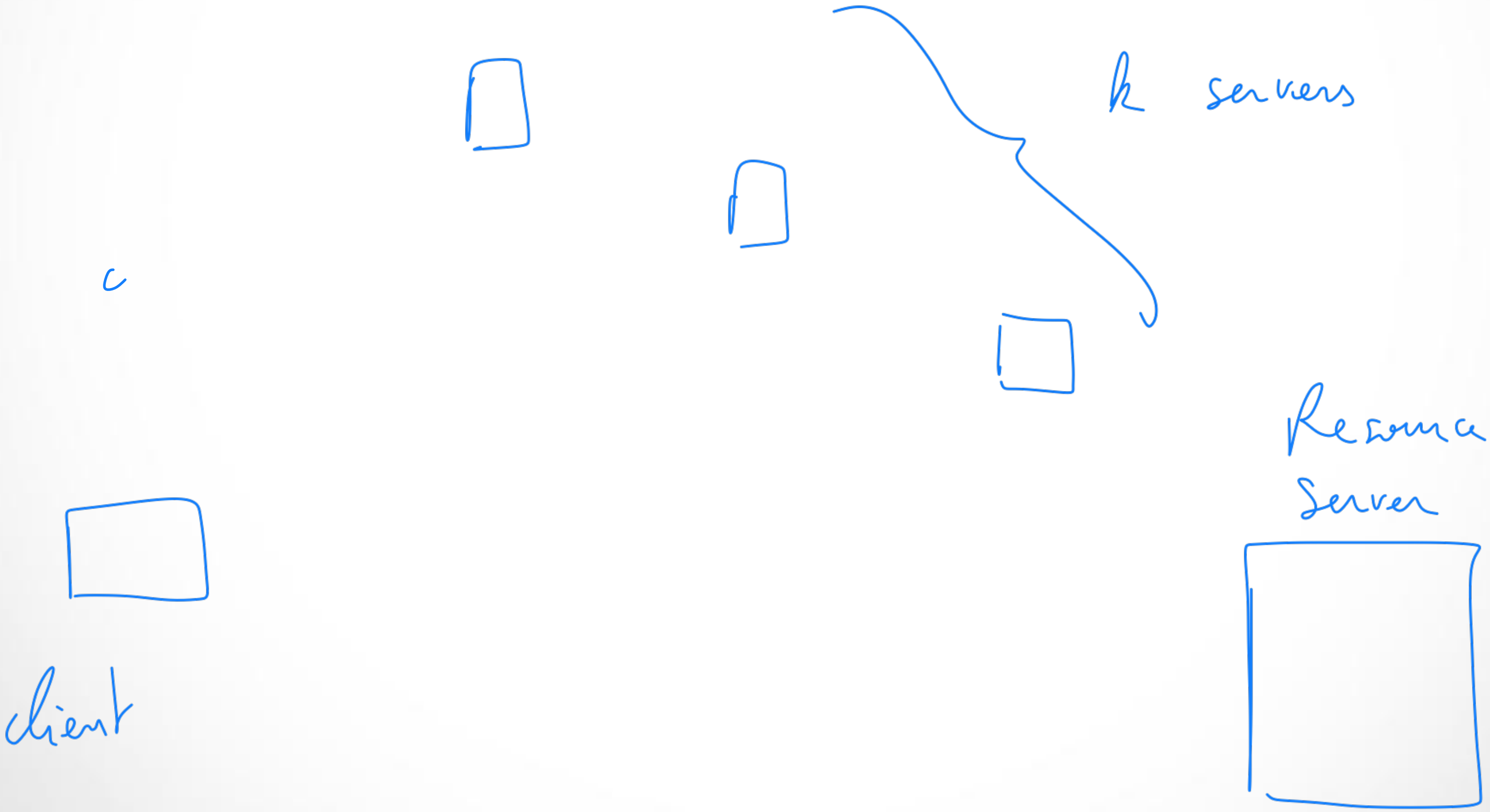
Mehmud Abliz and Taieb Znati. *A Guided Tour Puzzle for Denial of Service Prevention.*
In Proceedings of the Annual Computer Security Applications Conference (ACSAC) 2009

The guided tour puzzle

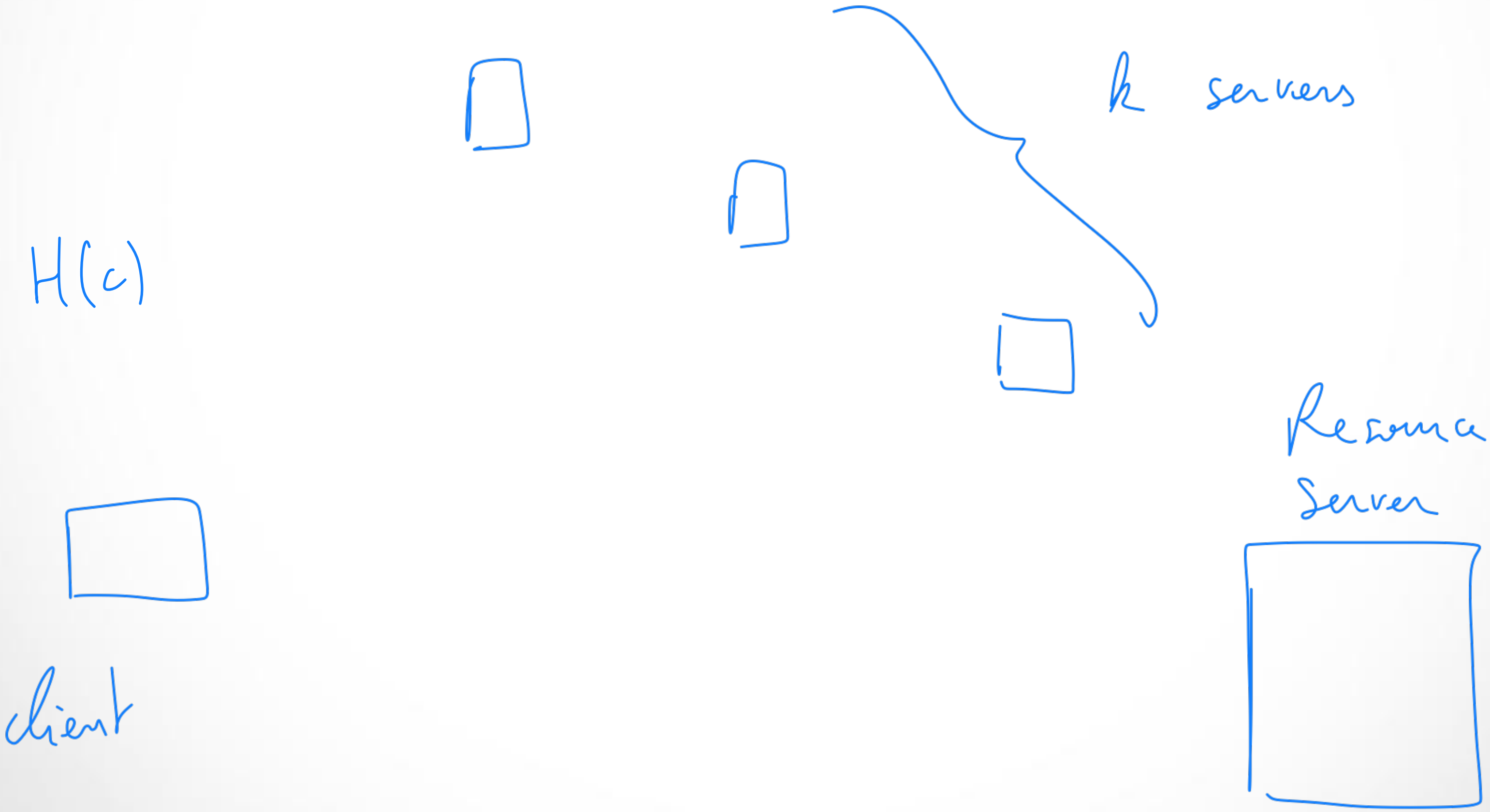
The guided tour puzzle



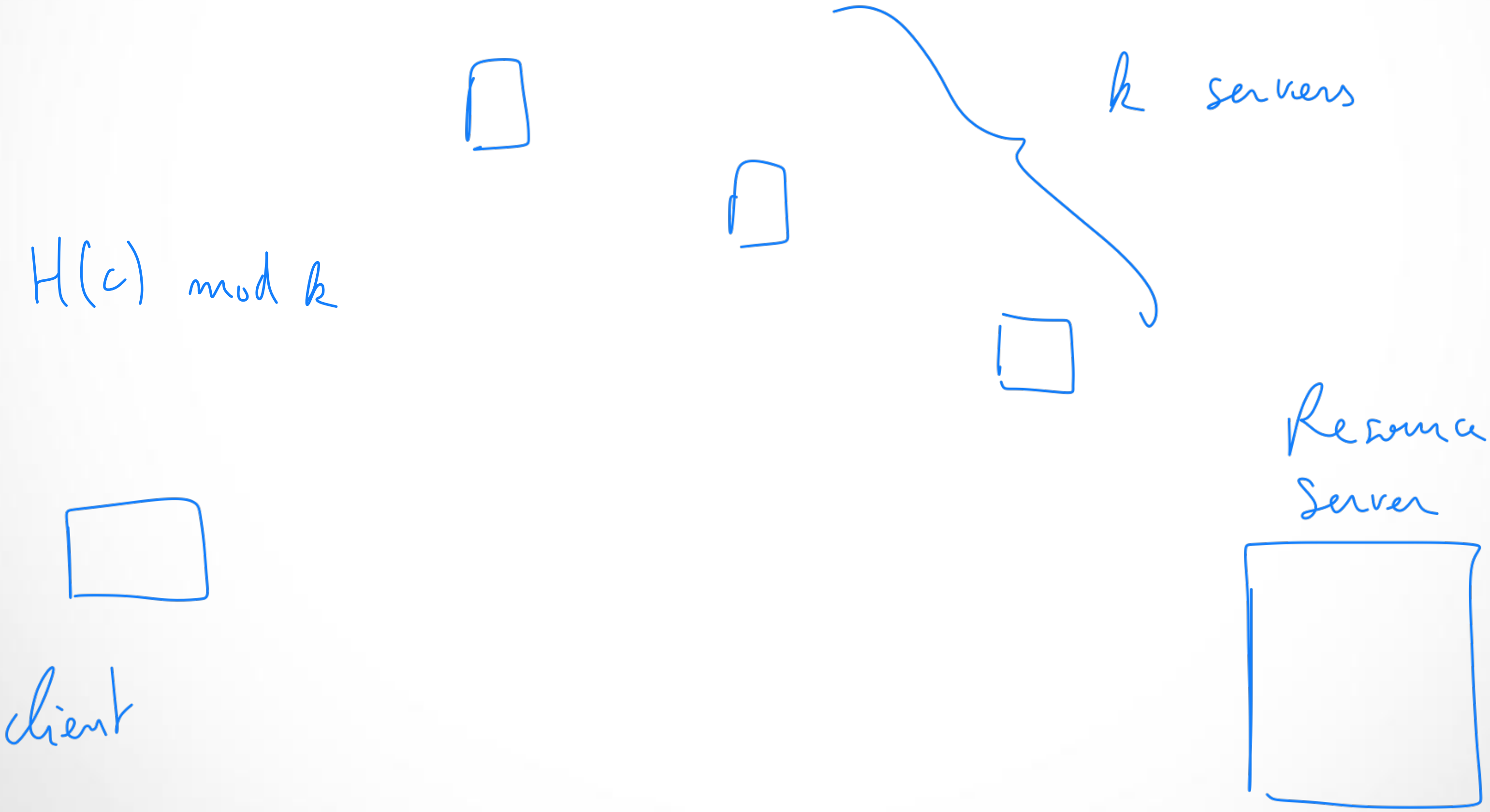
The guided tour puzzle



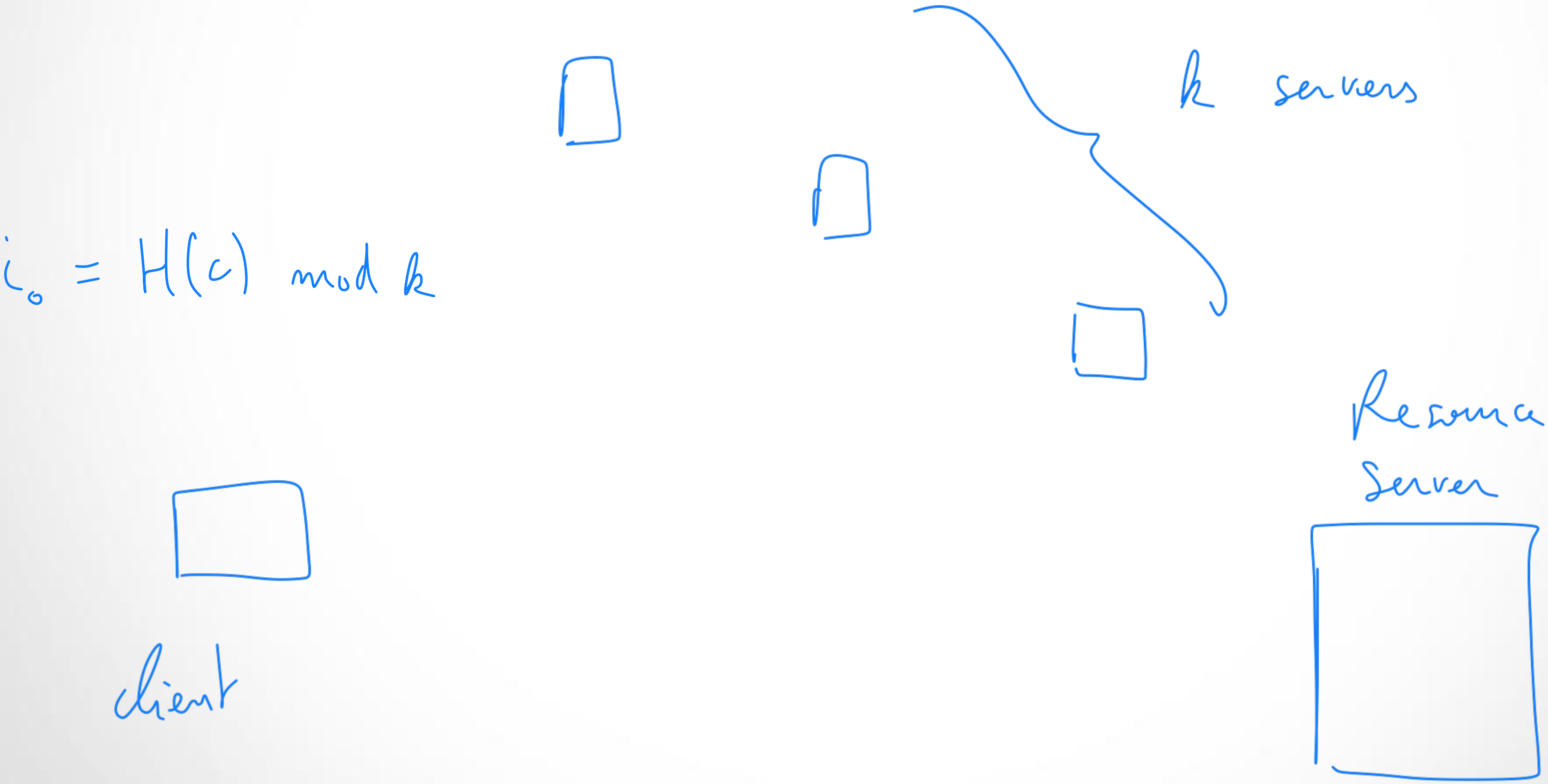
The guided tour puzzle



The guided tour puzzle

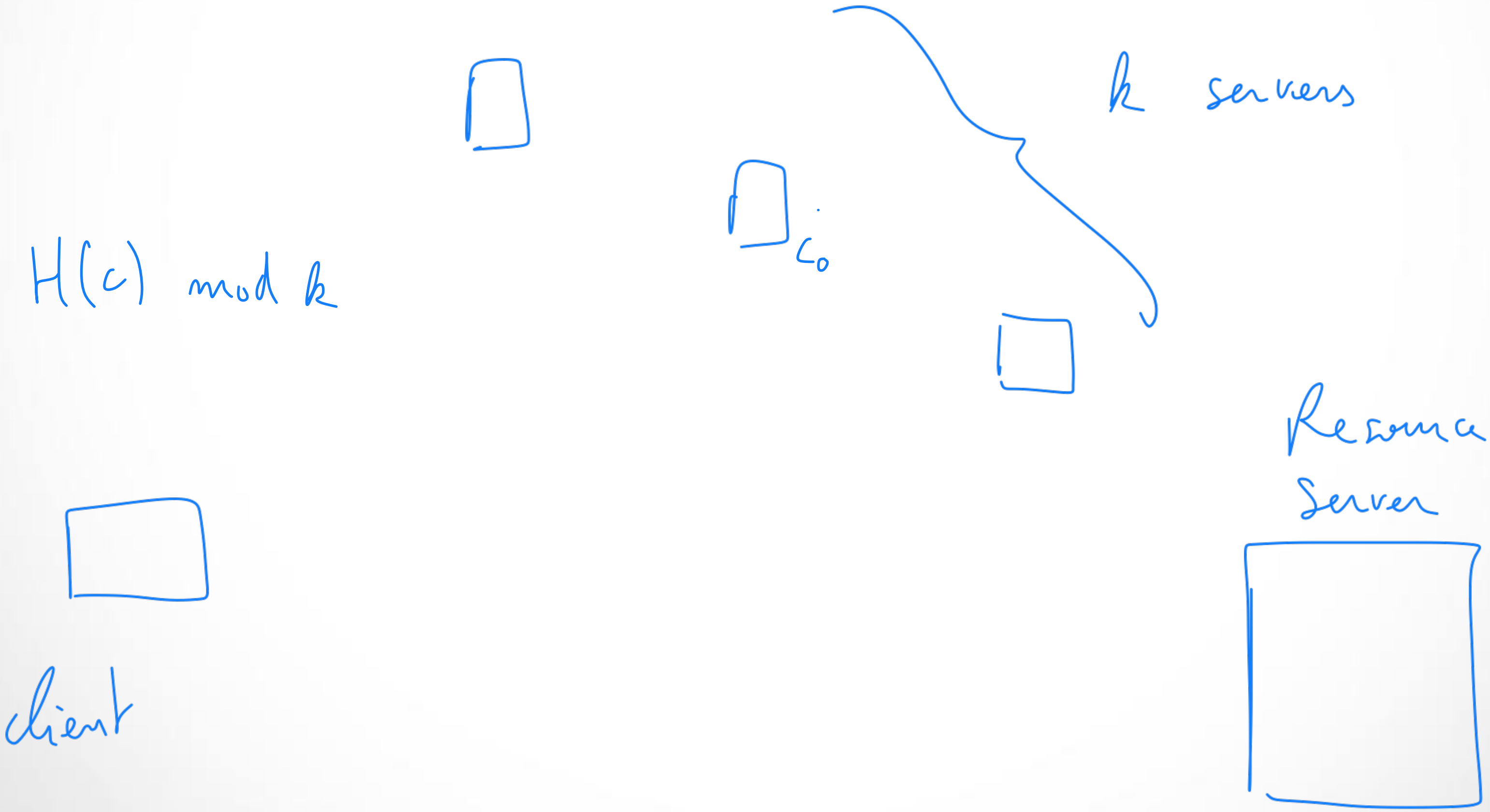


The guided tour puzzle

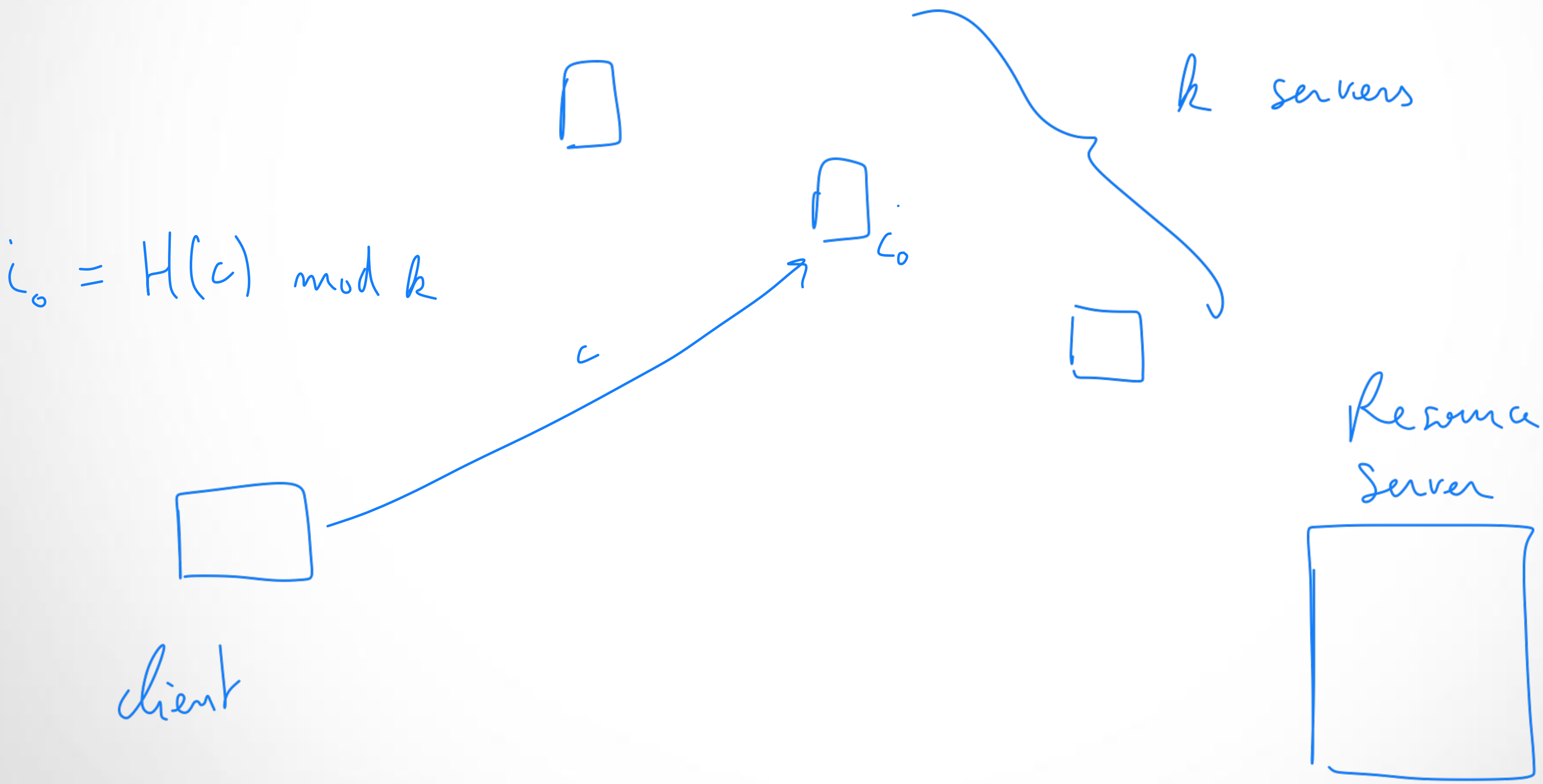


The guided tour puzzle

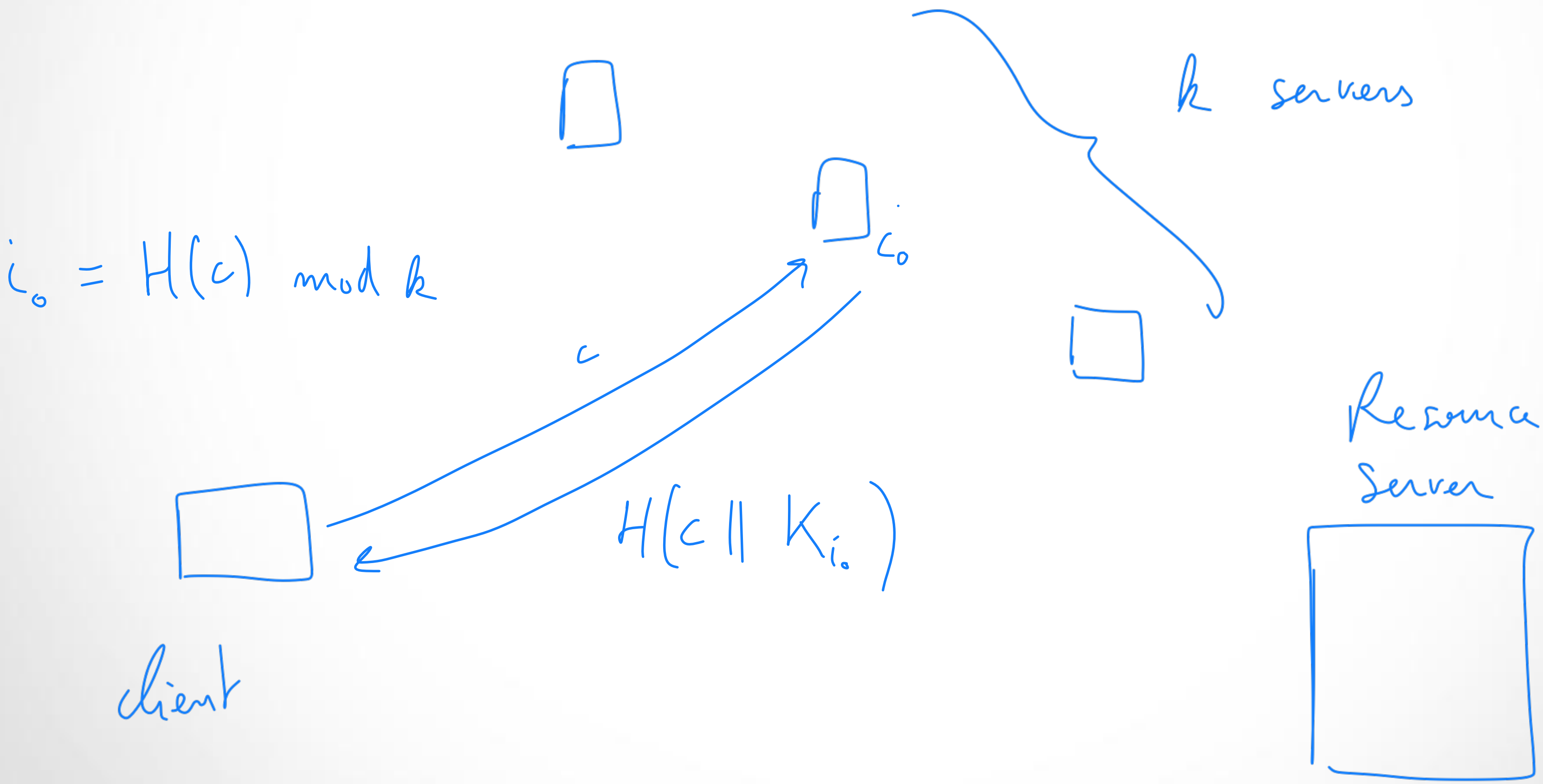
$i_0 = H(c) \bmod k$



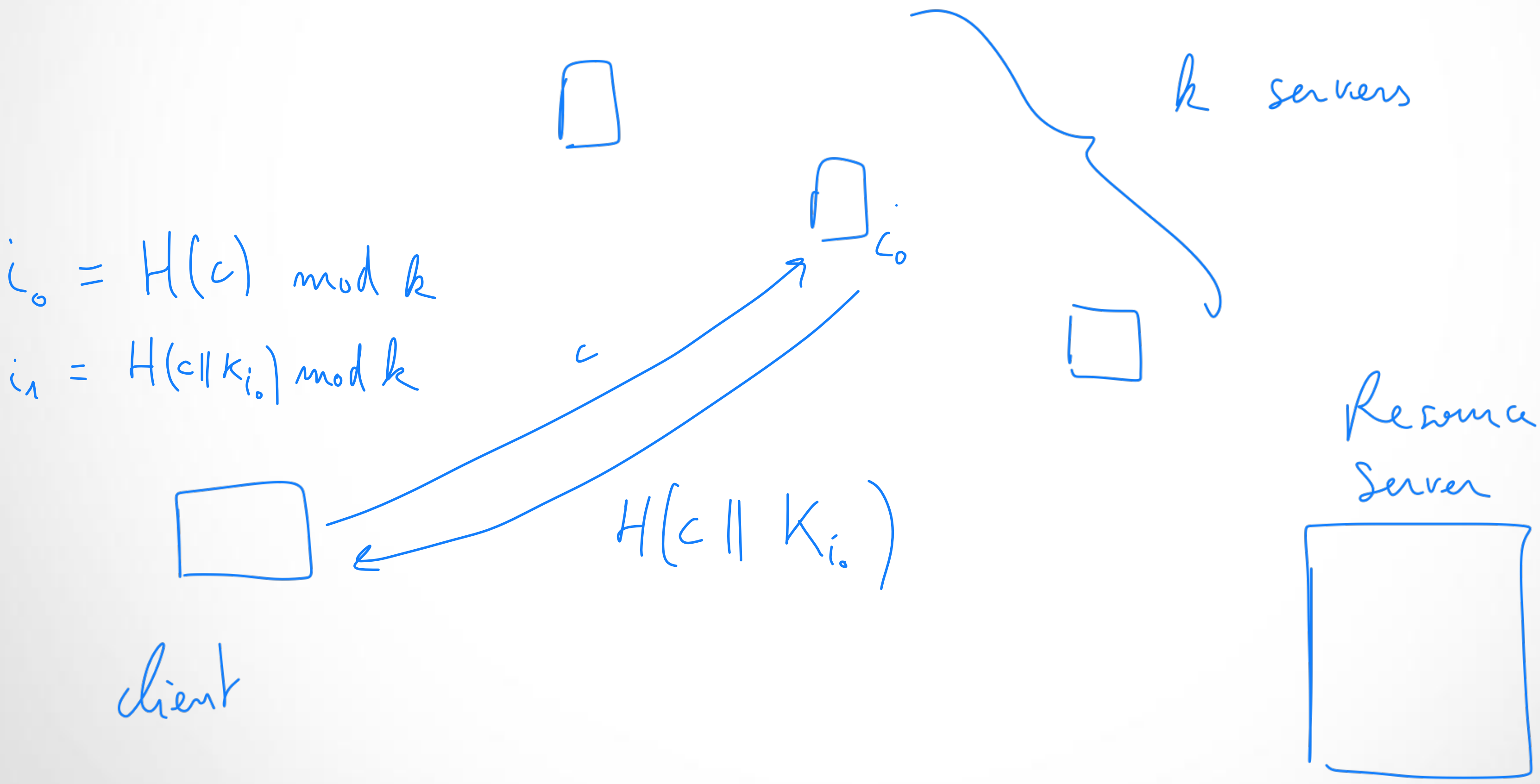
The guided tour puzzle



The guided tour puzzle



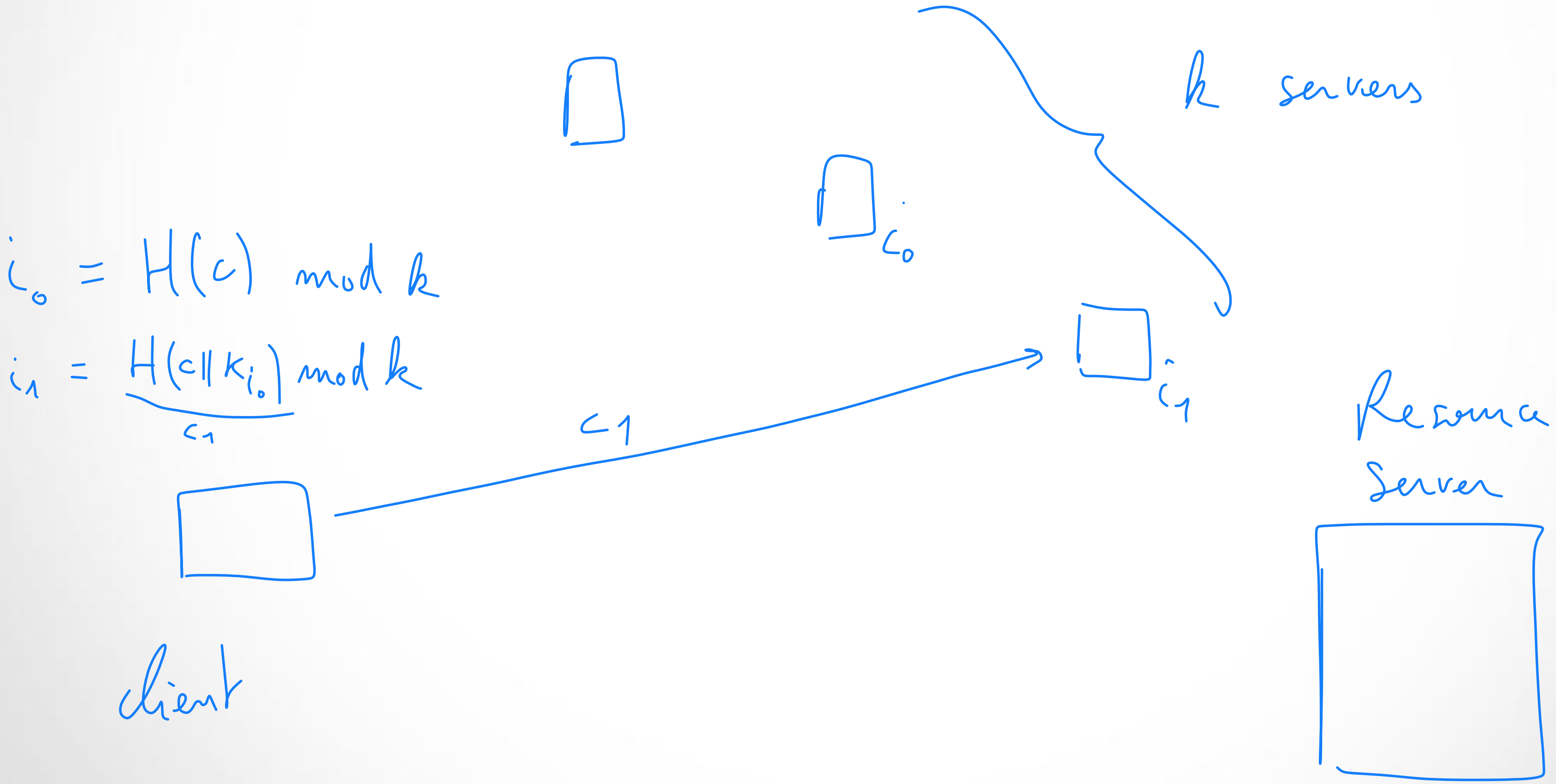
The guided tour puzzle



$i_0 = H(c) \bmod k$

$i_1 = H(c \| K_{i_0}) \bmod k$

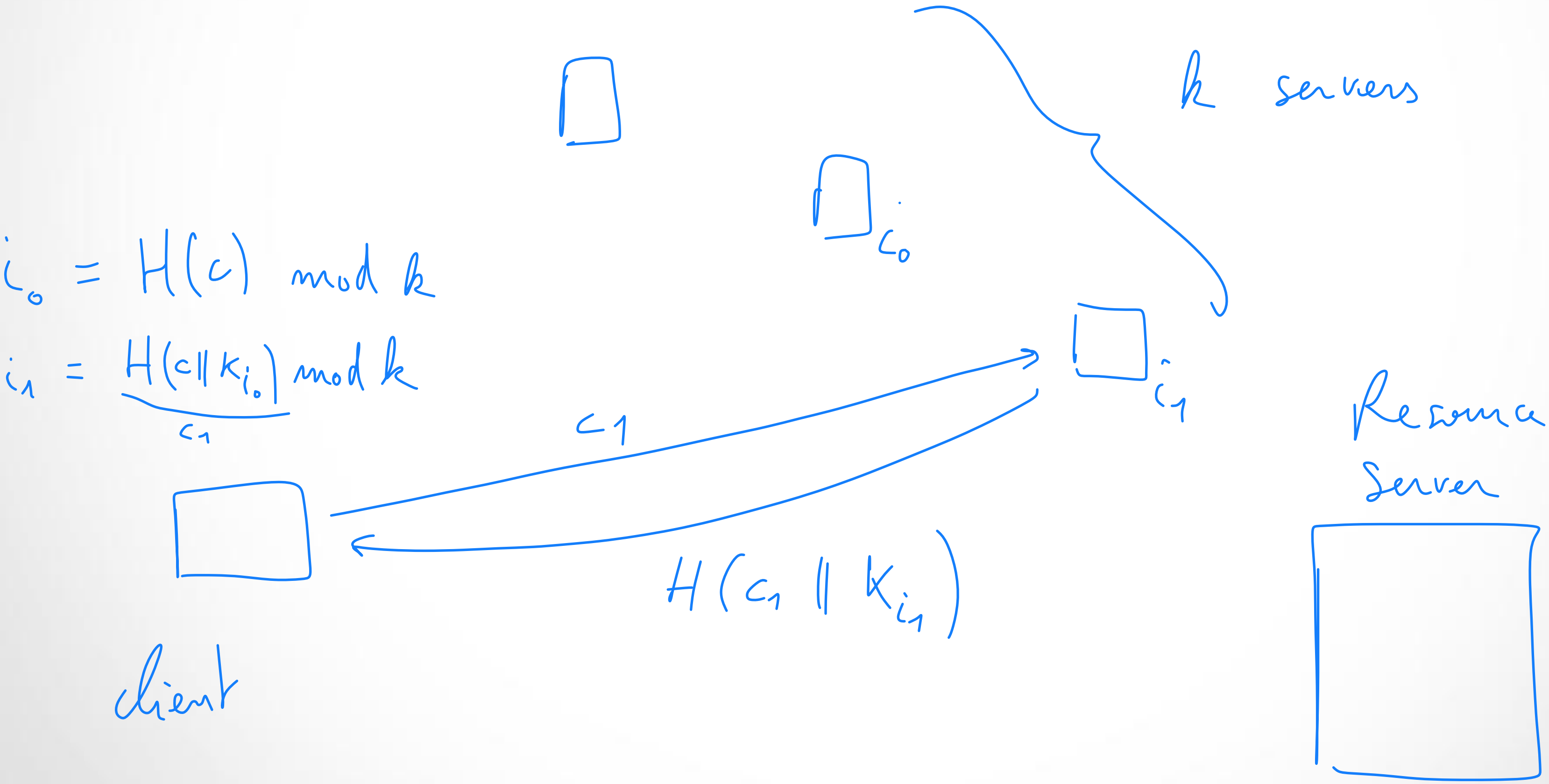
The guided tour puzzle



$i_0 = H(c) \bmod k$

$i_1 = \underbrace{H(c \| k_{i_0})}_{c_1} \bmod k$

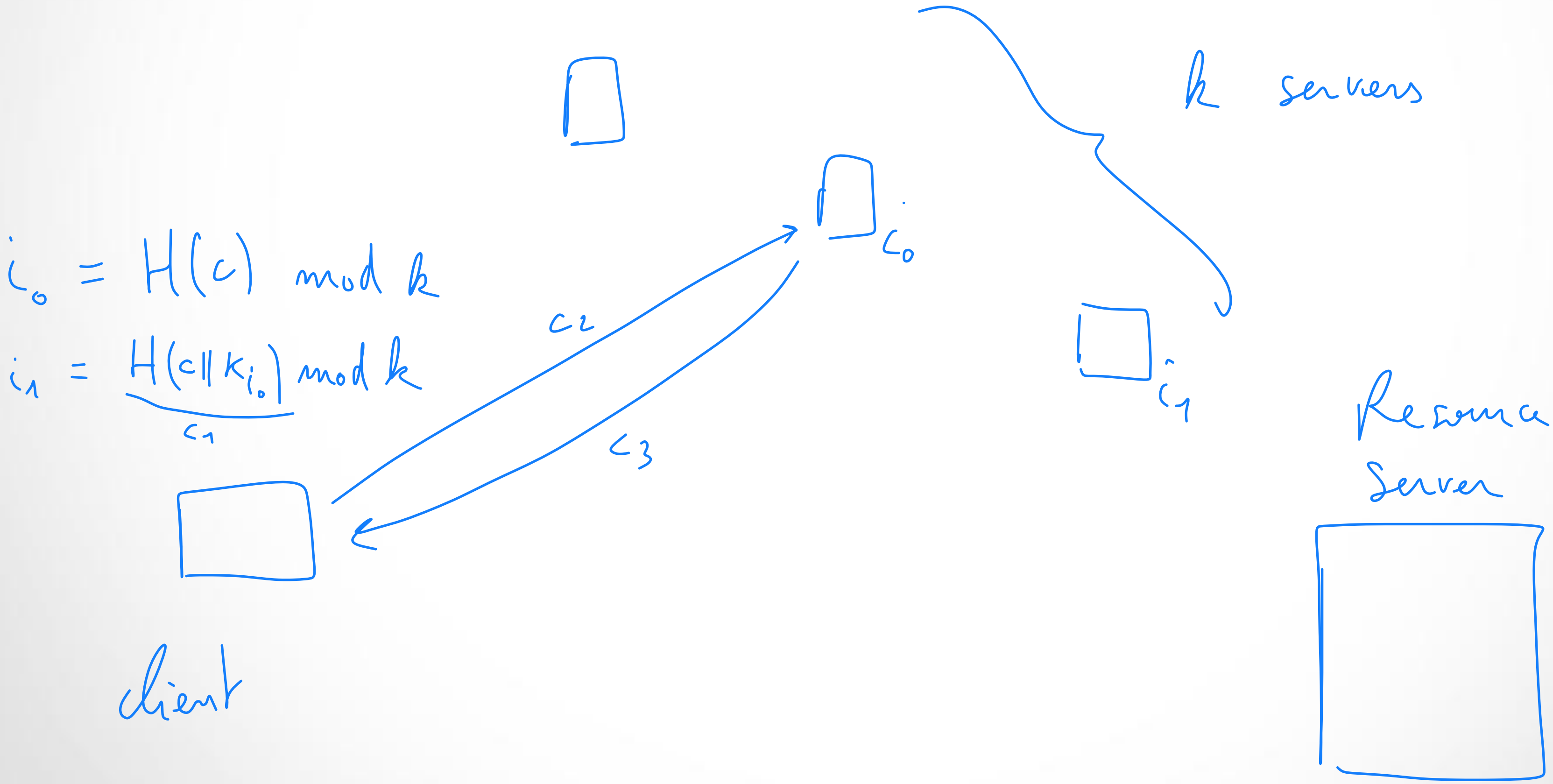
The guided tour puzzle



$i_0 = H(c) \bmod k$

$i_1 = \underbrace{H(c \| K_{i_0})}_{c_1} \bmod k$

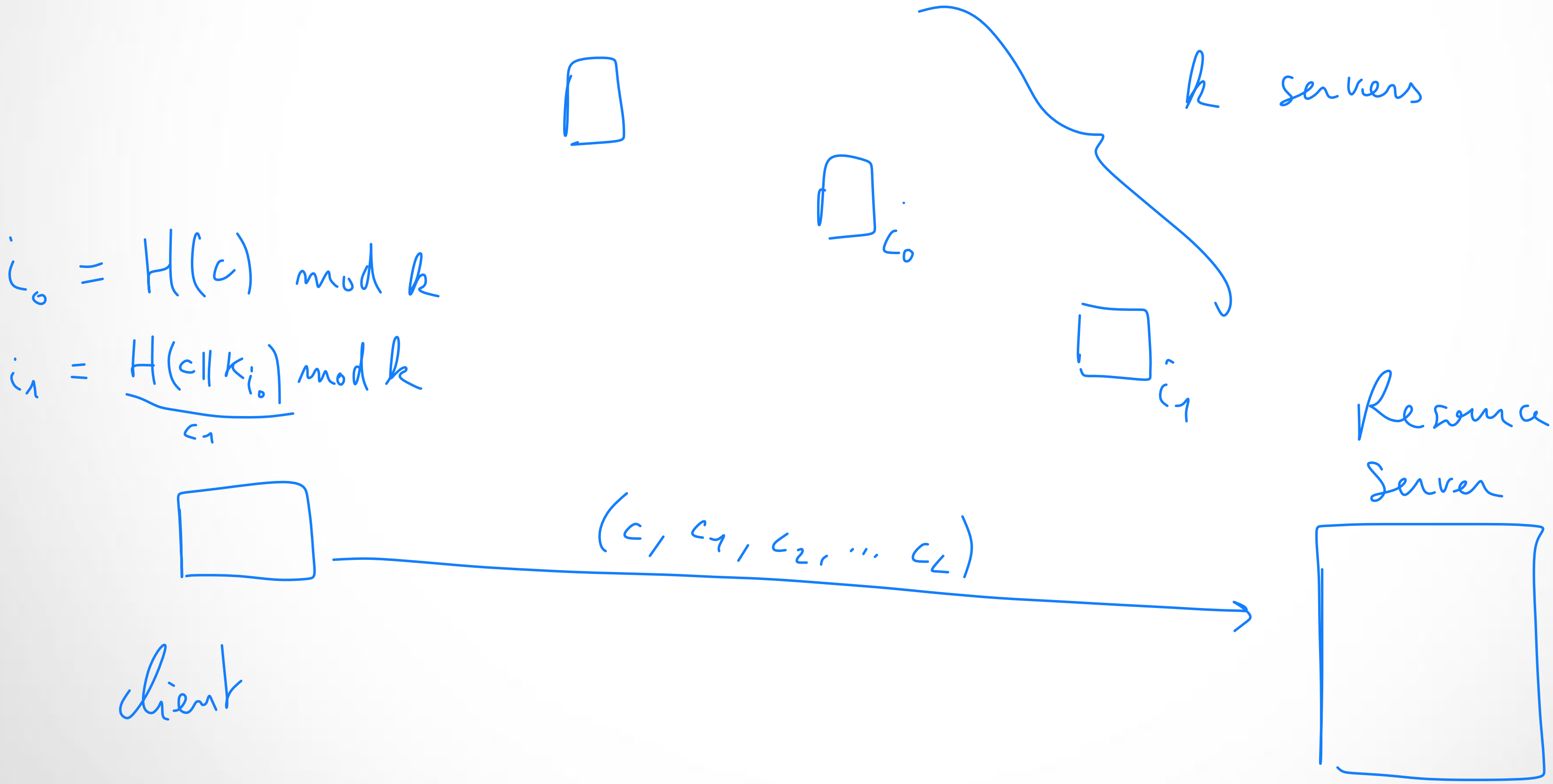
The guided tour puzzle



$$i_0 = H(c) \bmod k$$

$$i_1 = \underbrace{H(c \| k_{i_0})}_{c_1} \bmod k$$

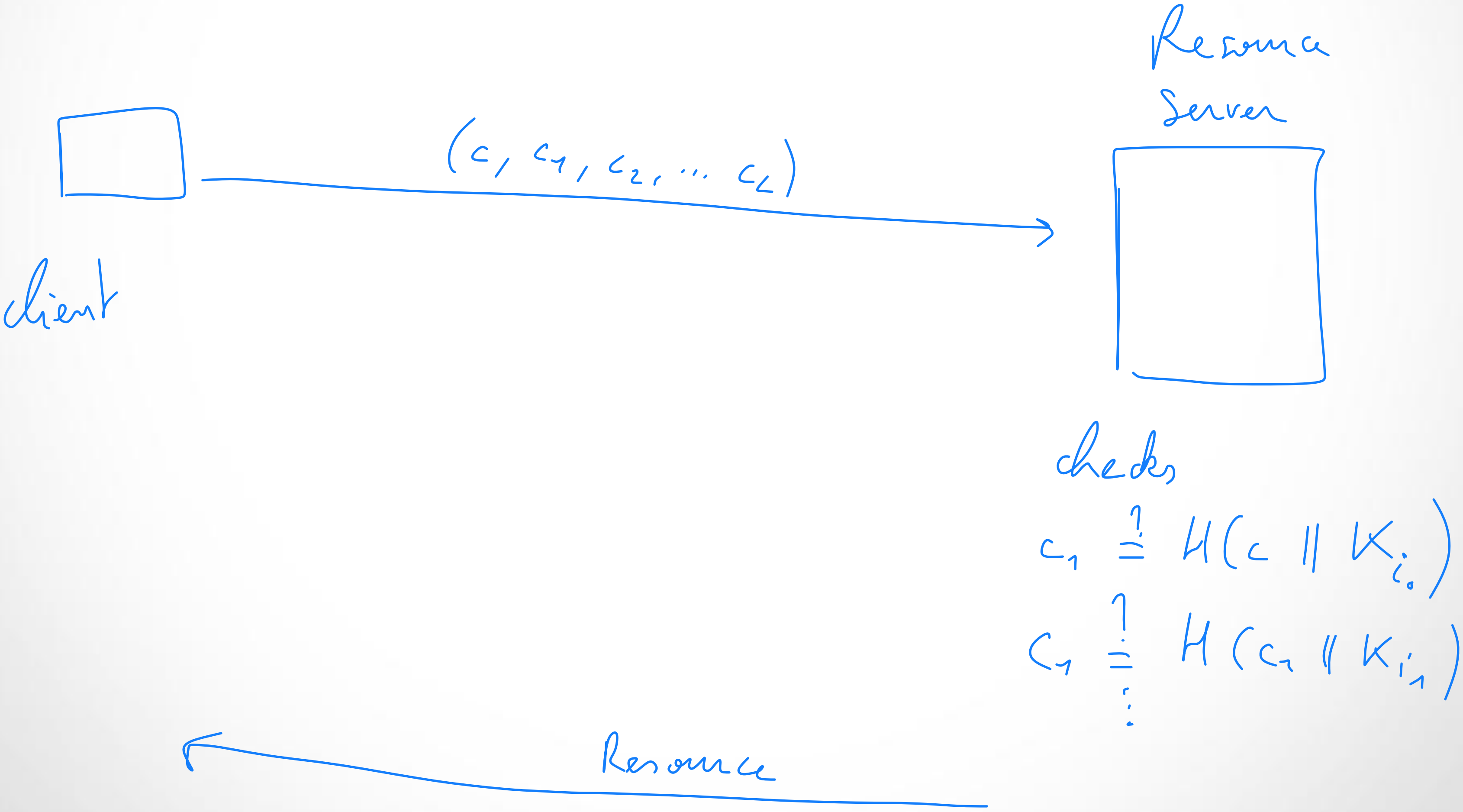
The guided tour puzzle



$$i_0 = H(c) \bmod k$$

$$i_1 = \underbrace{H(c \| k_{i_0})}_{c_1} \bmod k$$

The guided tour puzzle


Resource Server
client
$(c, c_1, c_2, \dots c_L)$
checks
$c_1 \overset{?}{=} H(c \,||\, K_{i_0})$
$c_1 \overset{?}{=} H(c_1 \,||\, K_{i_1})$
$\vdots$
Resource

First Work: Proof-of-Interaction

We consider a fixed set of participants $P_0, P_1, \dots P_n$

A participant P_i can perform a guided tour, with a seed derived from **its public key**

First Work: Proof-of-Interaction

We consider a fixed set of participants $P_0, P_1, \dots P_n$

A participant P_i can perform a guided tour, with a seed derived from **its public key**

$$c = H(P_i), \quad i_0 = c \bmod n$$

First Work: Proof-of-Interaction

We consider a fixed set of participants $P_0, P_1, \ldots P_n$

A participant P_i can perform a guided tour, with a seed derived from **its public key**

$$c = H(P_i), \quad i_0 = c \bmod n$$

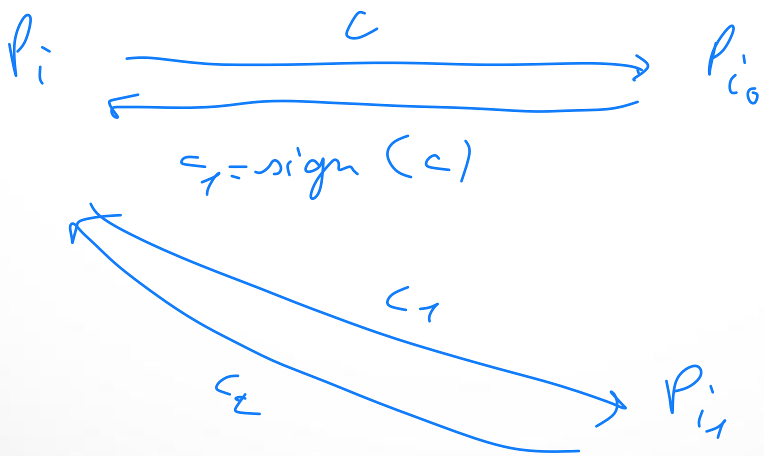
$$\begin{tikzcd}
P_i \arrow[r, "c"] & P_{i_0} \arrow[l, bend left, "s_1 = sign(c)"]
\end{tikzcd}$$

First Work: Proof-of-Interaction

We consider a fixed set of participants $P_0, P_1, .. P_n$

A participant P_i can perform a guided tour, with a seed derived from **its public key**

$c = H(P_i)$, $i_0 = c \bmod n$

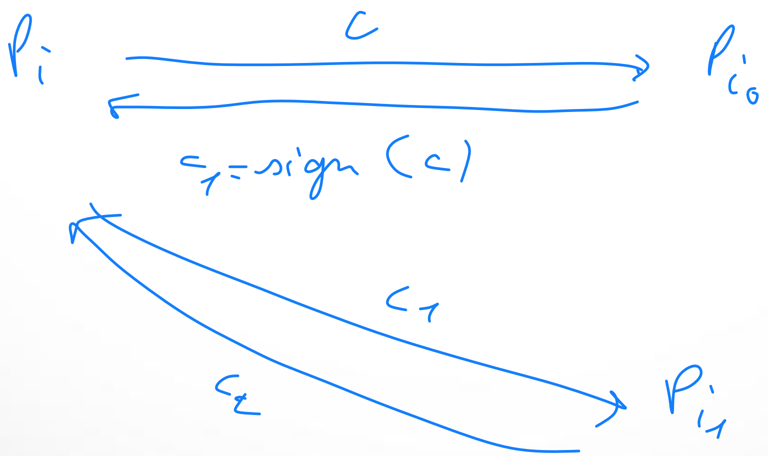


First Work: Proof-of-Interaction

We consider a fixed set of participants $P_0, P_1, \ldots P_n$

A participant P_i can perform a guided tour, with a seed derived from **its public key**

$$c = H(P_i), \quad i_0 = c \bmod n$$



$$(c, c_1, c_2 \ldots, c_l)$$

First Work: Proof-of-Interactions

We consider a fixed set of participants $P_0, P_1, \dots P_n$

A participant P_i can perform a guided tour, with a seed derived from its public key and the Merkel tree root **and the hash of the previous block.**

$$c = sign_i (P_i \parallel M \parallel B_{prev})$$

First Work: Proof-of-Interactions

We consider a fixed set of participants $P_0, P_1, \dots P_n$

How long is the tour?

$$L = rand(sign_i(B_{prev}))$$

First Work: Proof-of-Interactions

We consider a fixed set of participants $P_0, P_1, \ldots P_n$

What data do we ask participant to sign ?

$$\begin{tikzcd}
P_i \arrow[rr, shift left, "{c, B_{prev}, M}"] & & P_{i_0} \arrow[ll, shift left, "{sign_{i_0}(c \| B_{prev} \| M)}"]
\end{tikzcd}$$

First Work: Proof-of-Interactions

We consider a fixed set of participants $P_0, P_1, .. P_n$

How to tolerate crashes?

Make a tour around a subset

S = select 20 random nodes

Make a tour among S.

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against
Selfish-mining

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against Selfish-mining

$$c := sign_i(B_{prev} \| P_i \| M)$$

$$\xrightarrow{c,\ B_{prev},\ M} P_{i_0}$$

First Work: Proof-of-Interactions

Properties:

Not parallelizable

$$c := sign_i(B_{prev} \| P_i \| M)$$

$$\xrightarrow{c,\, B_{prev},\, M} P_{i_0}$$

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

$$c' := sign_i(B_{prev} \| P_i \| M')$$

$$\xrightarrow{c',\, B_{prev},\, M'} P_{i_0}'$$

Protected against
Selfish-mining

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against
Selfish-mining

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against
Selfish-mining

$$L = \underset{\substack{\uparrow \\ \text{adjustable.}}}{\mathrm{rand}}\left(\mathrm{sign}_i\left(B_{prev}\right)\right)$$

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against
Selfish-mining

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against
Selfish-mining

Proba ($\exists i$ P_i has a
tour with correct nodes)

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against
Selfish-mining

Proba ($\exists i$ P_i has a tour with correct nodes)

$\xrightarrow{n} 1$

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against
Selfish-mining

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against
Selfish-mining

Proba (not all node in a tour are Byzantine)

$\xrightarrow{n} 1$

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against Selfish-mining

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against Selfish-mining

to create a block, P_i must send the previous Block

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against Selfish-mining

Small message complexity

First Work: Proof-of-Interactions

Properties:

Not parallelizable

Difficulty is adjustable

Crash-tolerant

Byzantine-tolerant

Protected against Selfish-mining

Small message complexity

Each participant is part of ≈ 20 tours but contribute $\frac{1}{20}$ of the time.

total ≈ 2 continuous ⇄

2nd Work: Application Scalability

2nd Work: Application Scalability

Motivation: how to guarantee data transmissions between IoT devices using blockchain?

2nd Work: Application Scalability

Motivation: how to guarantee data transmissions between IoT devices using blockchain?

Challenge: IoT devices generate a lot of data

2nd Work: Application Scalability

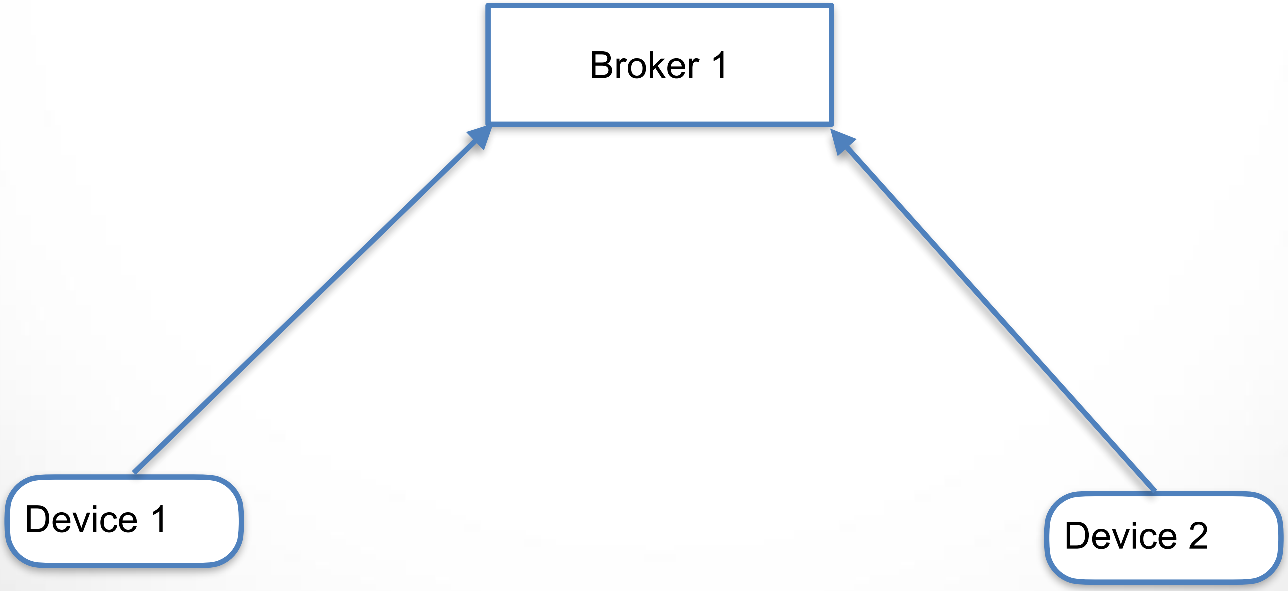
Motivation: how to guarantee data transmissions between IoT devices using blockchain?

Challenge: IoT devices generate a lot of data

Idea: use off-chain transmission if possible

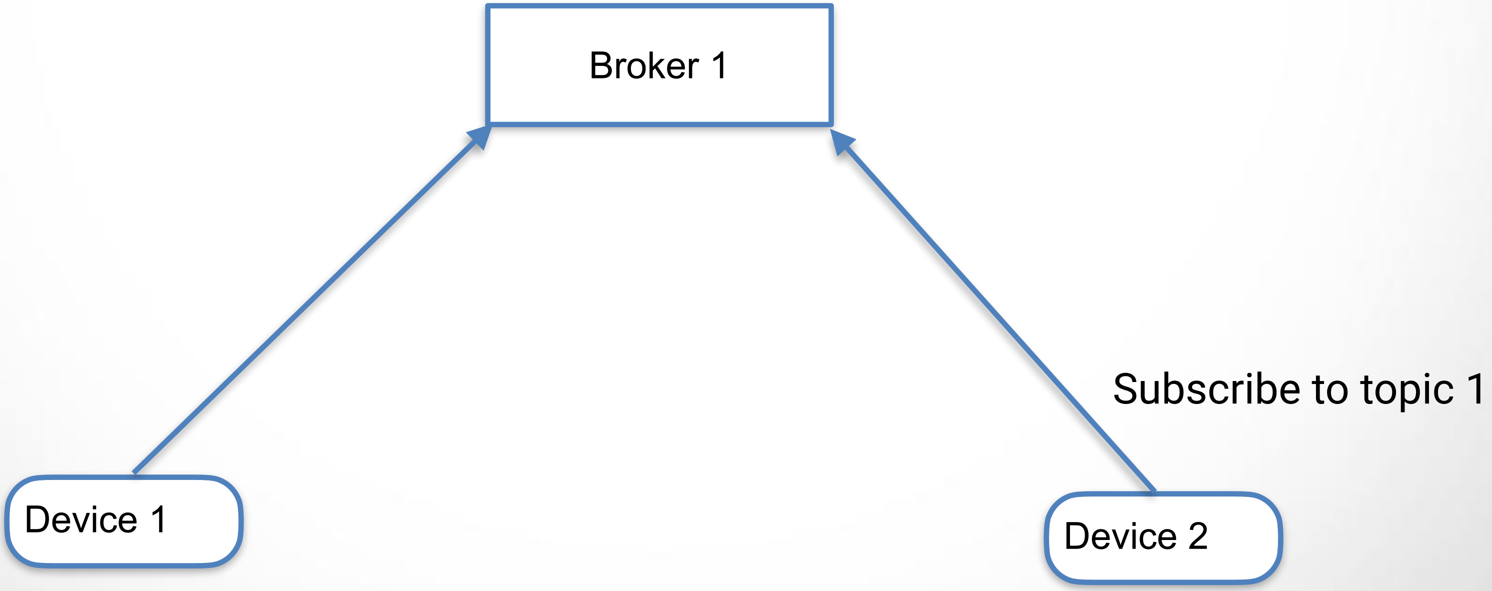
2nd Work: a pub-sub protocol

A centralized pub-sub protocol:



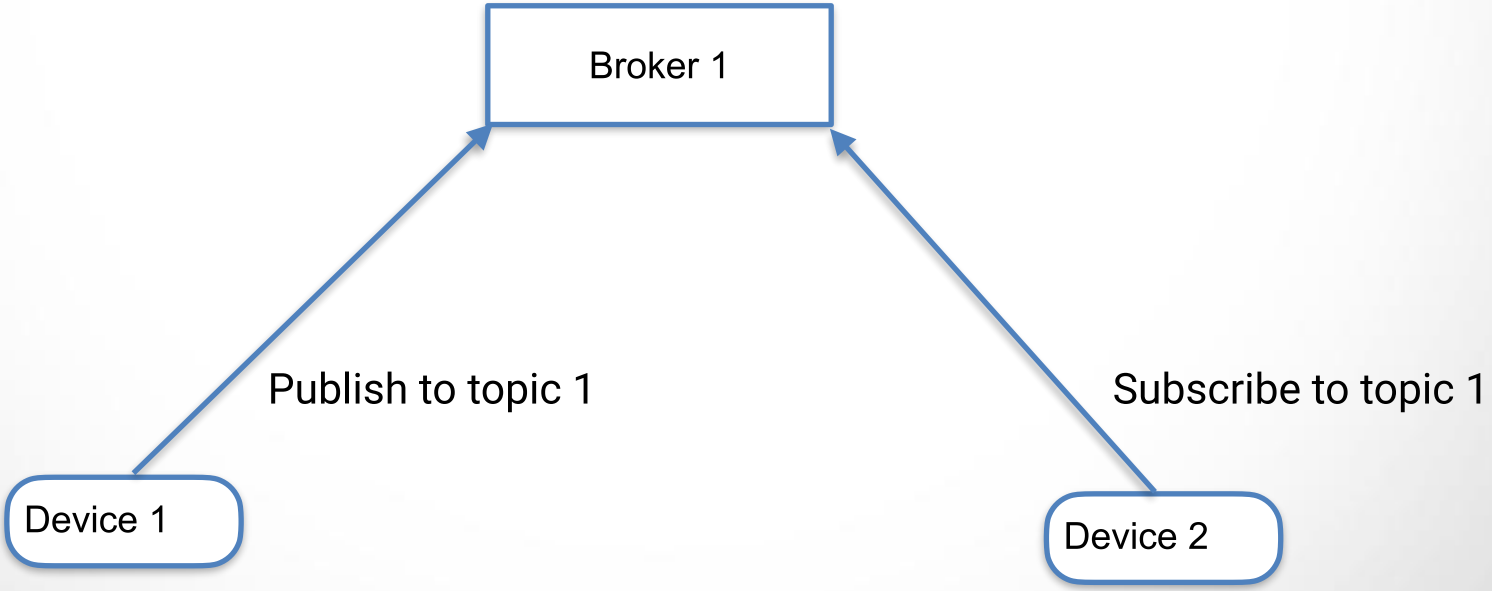
2nd Work: a pub-sub protocol

A centralized pub-sub protocol:



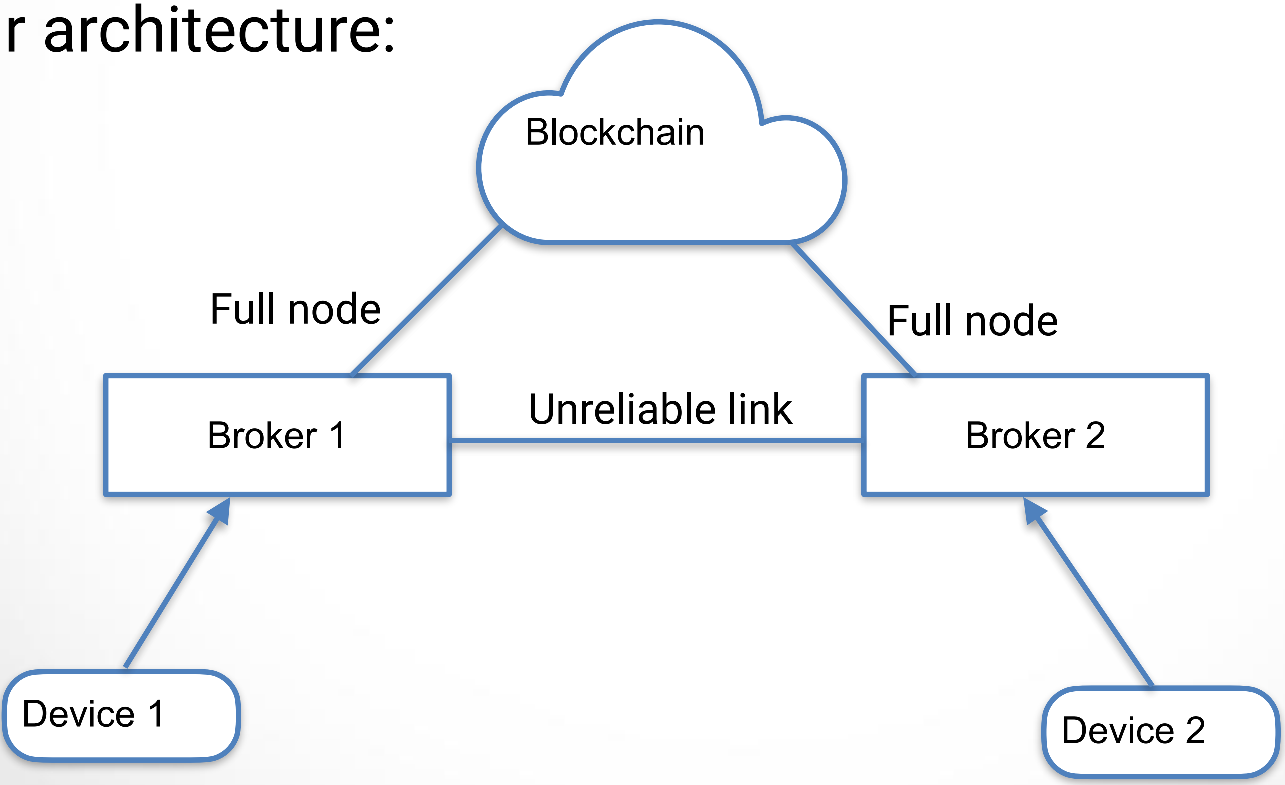
2nd Work: a pub-sub protocol

A centralized pub-sub protocol:



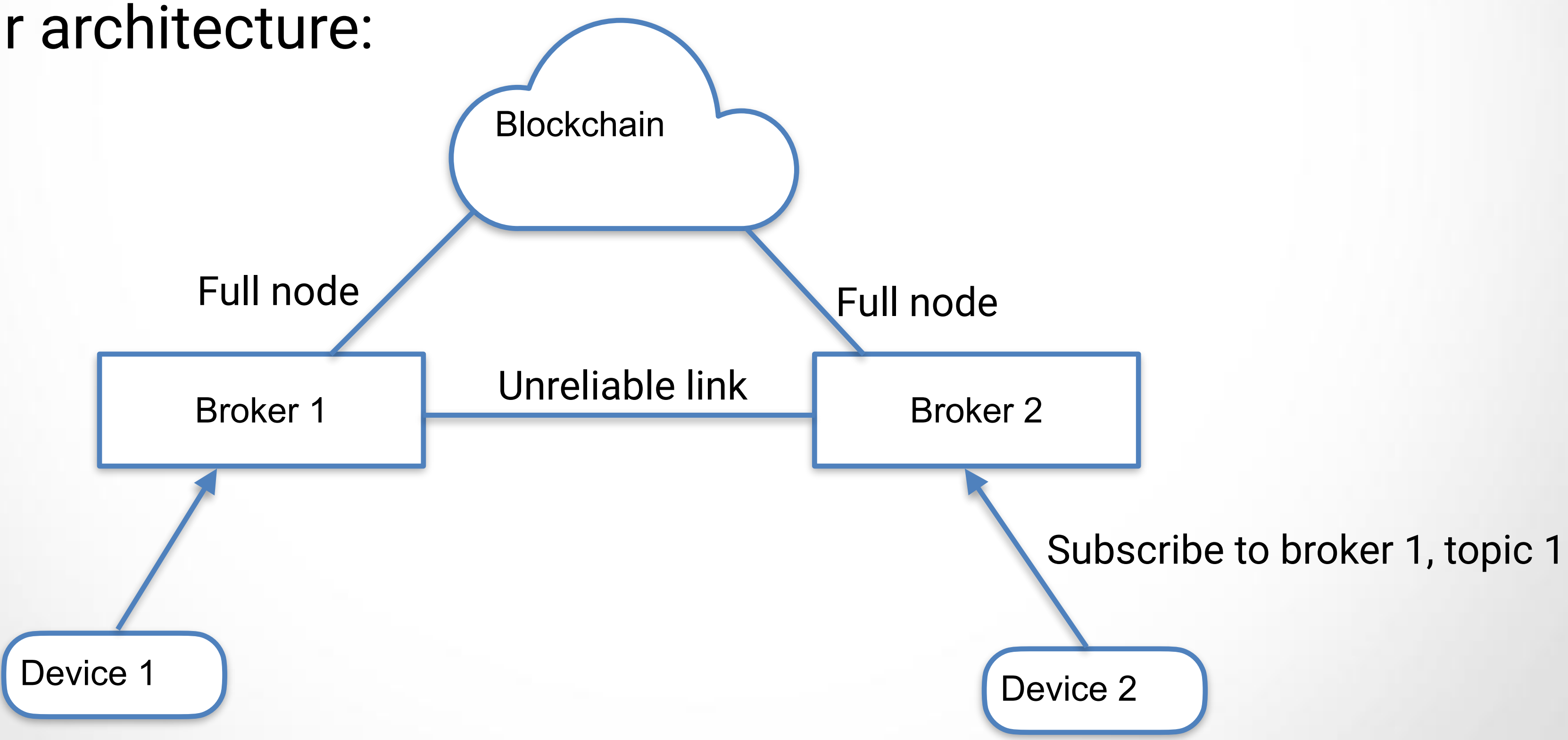
2nd Work: a pub-sub protocol

Our architecture:



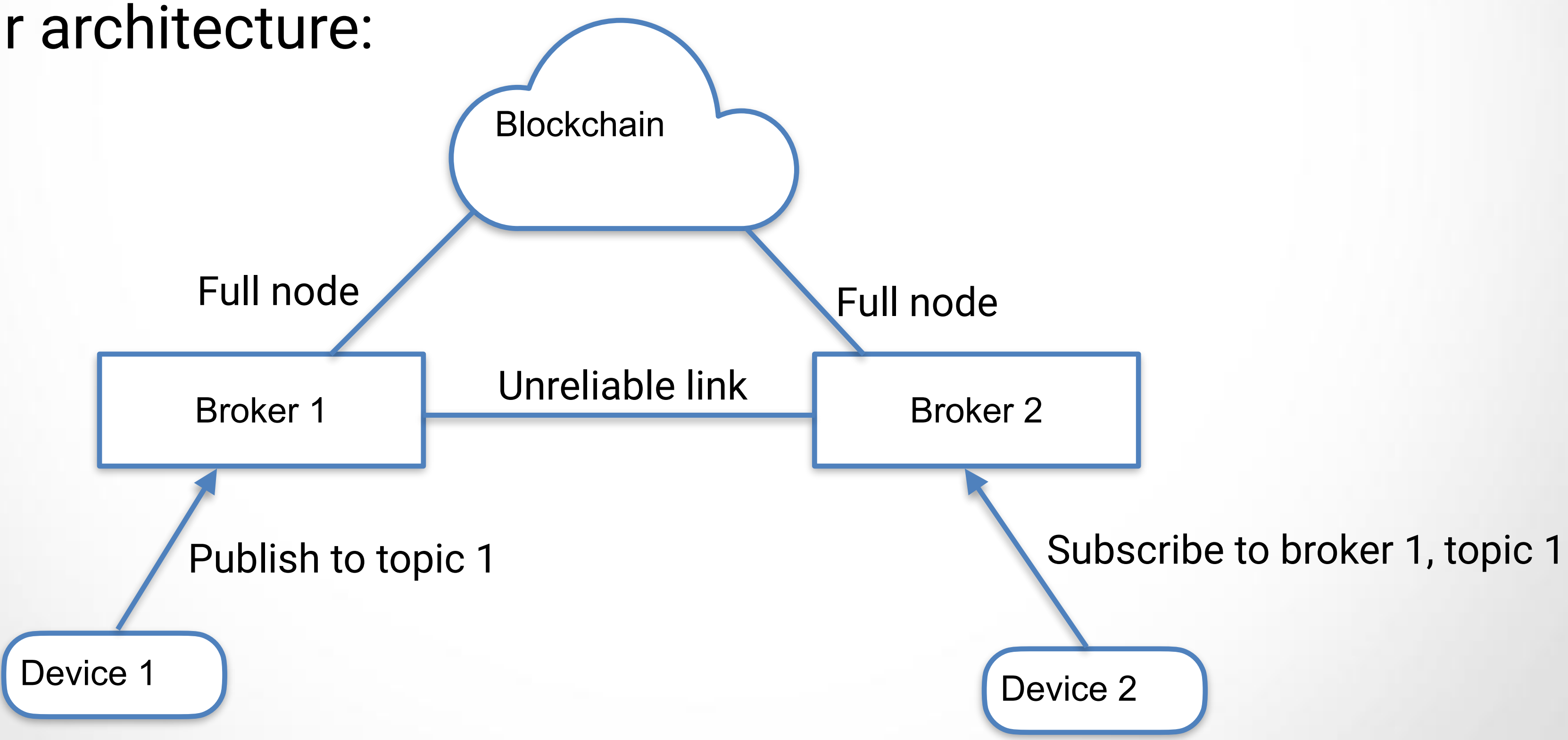
2nd Work: a pub-sub protocol

Our architecture:



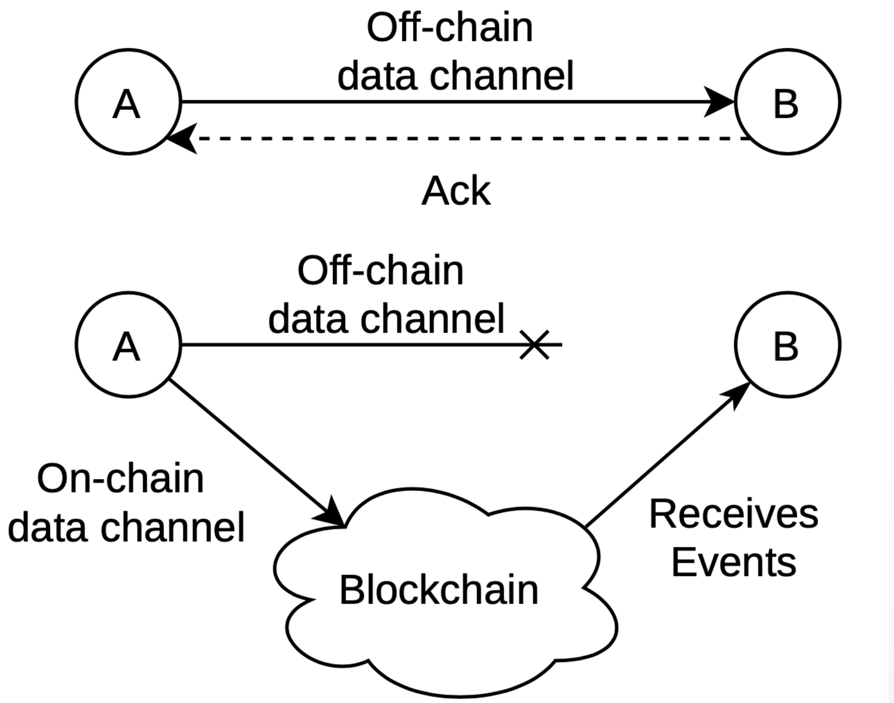
2nd Work: a pub-sub protocol

Our architecture:



2nd Work: a pub-sub protocol

Unidirectional off-chain data channel



2nd Work: a pub-sub protocol

2^{nd} Work: a pub-sub protocol

- The receiver has a proof of the origin of the data

2nd Work: a pub-sub protocol

- The receiver has a proof of the origin of the data
- The sender has a proof that the data is received

2nd Work: a pub-sub protocol

- The receiver has a proof of the origin of the data
- The sender has a proof that the data is received
- The sender can sell his data and be sure to be paid (In this case the buyer is sure to receive its data)

2nd Work: a pub-sub protocol

- The receiver has a proof of the origin of the data
- The sender has a proof that the data is received
- The sender can sell his data and be sure to be paid (In this case the buyer is sure to receive its data)
- Messages are sent off-chain, unless there is a problem (link failure or malicious behavior)

Conclusion

Conclusion

2 examples to improve scalability in Blockchains

- Proof-of-interactions

Jean-Philippe Abegg, Quentin Bramas and Thomas Noël.
Blockchain Using Proof-of-Interaction, Netys 2021

- Off-chain pub-sub protocol

Jean-Philippe Abegg, Quentin Bramas, Timothée Goubault de Brugière and Thomas Noël.
Distributed Publish/Subscribe Protocol with Minimum Number of Encryption, ICDCN 2022

Conclusion

2 examples to improve scalability in Blockchains

- Proof-of-interactions

Jean-Philippe Abegg, Quentin Bramas and Thomas Noël.
Blockchain Using Proof-of-Interaction, Netys 2021

- Off-chain pub-sub protocol

Jean-Philippe Abegg, Quentin Bramas, Timothée Goubault de Brugière and Thomas Noël.
Distributed Publish/Subscribe Protocol with Minimum Number of Encryption, ICDCN 2022

Thank you