Meridian

Starlight

A Layer 2 Payment Channel Protocol for the Stellar Network

Leigh McCulloch
Alec Charbonneau

Welcome

MEET LEIGH

Leigh McCulloch is a Principal Software Engineer at the Stellar Development Foundation (SDF), a non-profit organization that supports the development and growth of Stellar, an open-source network that connects the world's financial infrastructure. He leads forward-looking cross-functional engineering projects for Stellar.

Meridian

Welcome

MEET ALEC

Alec is a Software Engineer on the SDF Product Engineering team. Alec has been working on products for SDF for over a year, and has contributed to projects such as Laboratory, Vibrant, and Data. Currently Alec is focused on Stellar's Starlight project.

Meridian

Agenda

Meridian

1. Why Layer 2

2. What are Payment Channels?

3. Demo a Starlight Payment Channel on Stellar

WHY LAYER 2?

Meridian

The Stellar Network

Why Configure With An Artificial Limit?

Meridian

Configured Limit

1,000
operations
per ledger

- Voted on by network validators
- Promotes financial inclusion
- Promotes decentralization
- Preserves cost predictability
- Broadens who can run the network

The Stellar Network

Current Configuration

Meridian

Configured Limit

1,000
operations
per ledger

~5-10
seconds
per ledger

The Stellar Network

Current Configuration

Meridian

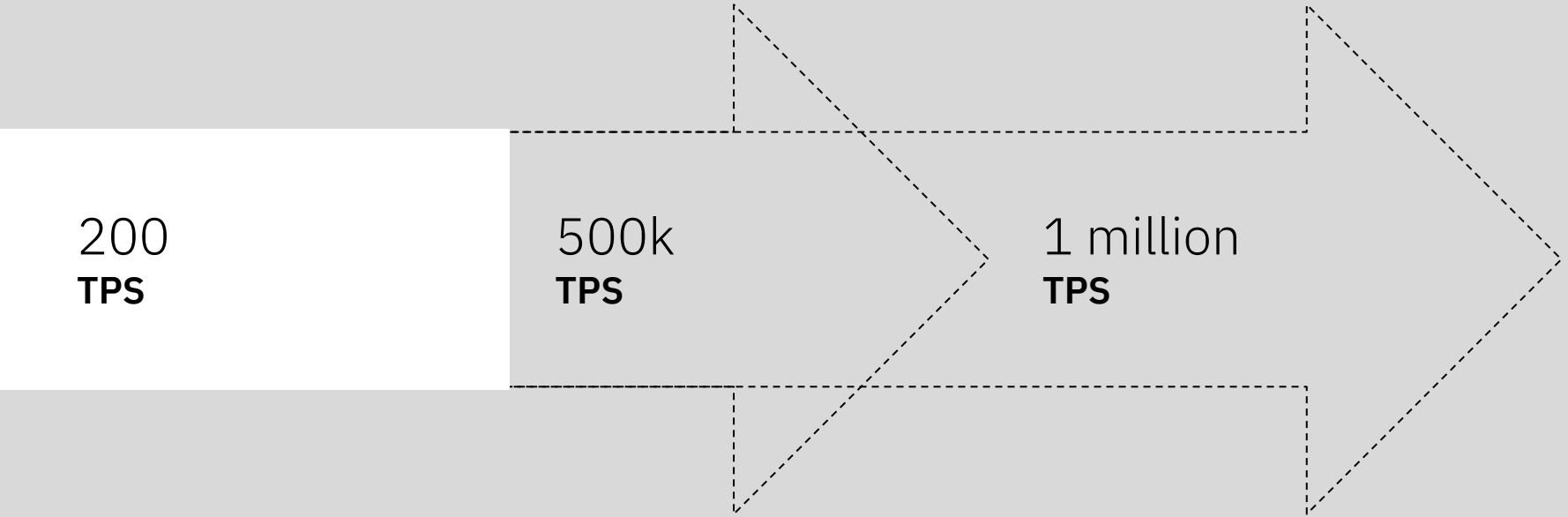
Configured Limit

1,000
operations
per ledger

~5-10
seconds
per ledger

≈ 200
transactions per
second (TPS)

Meridian



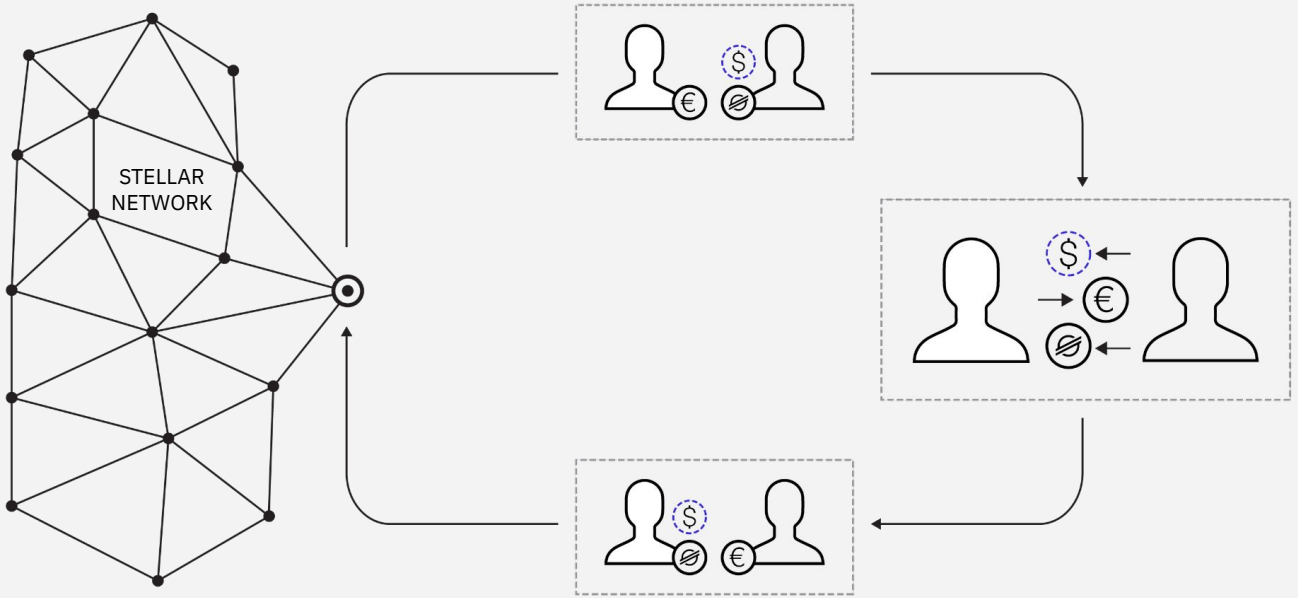
PAYMENT CHANNELS

A Layer 2 Technology

Meridian

Payment Channels

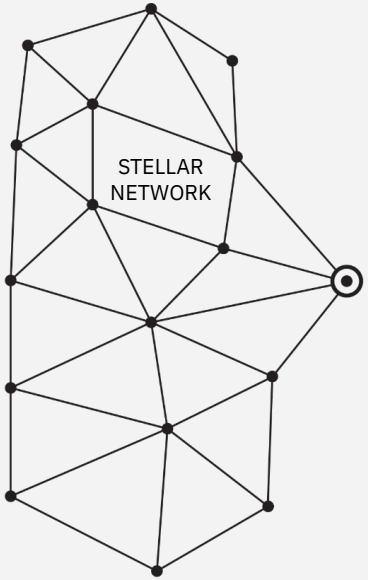
Enable Fast Payments Between Two Parties



Meridian

Payment Channels

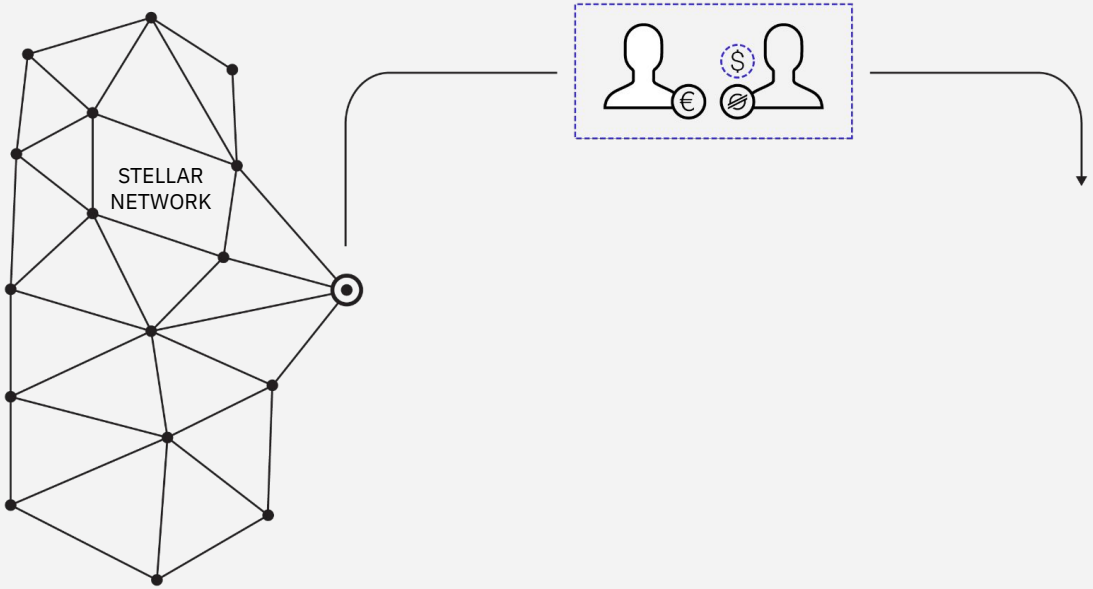
Enable Fast Payments Between Two Parties



Meridian

Payment Channels

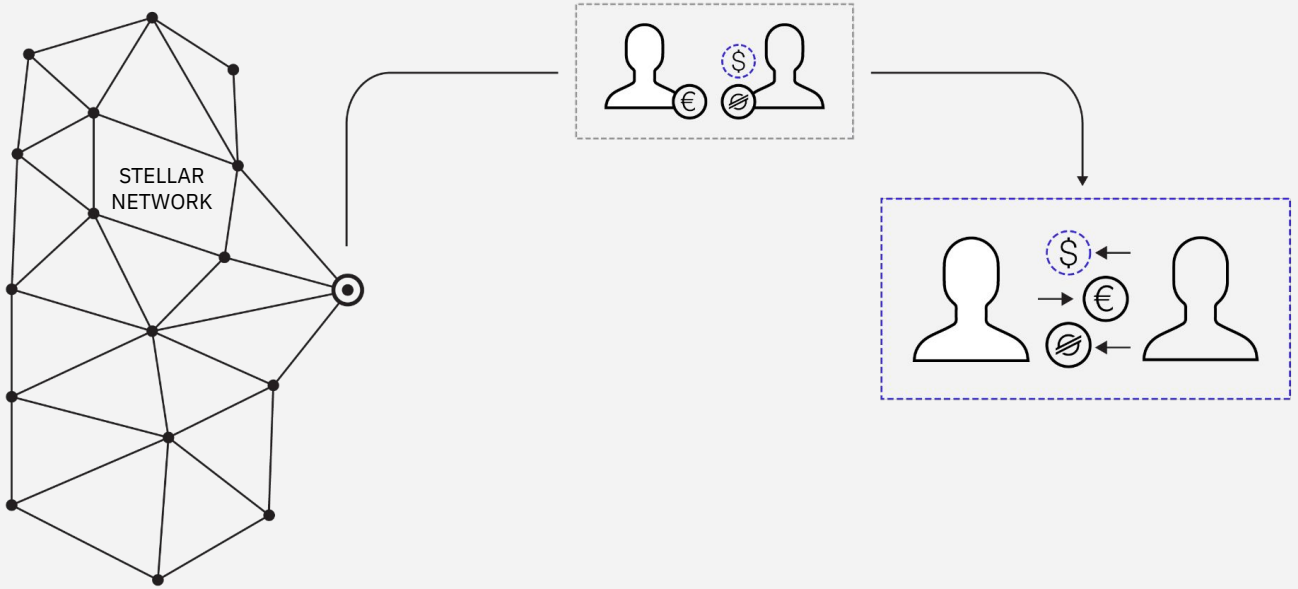
Enable Fast Payments Between Two Parties



Meridian

Payment Channels

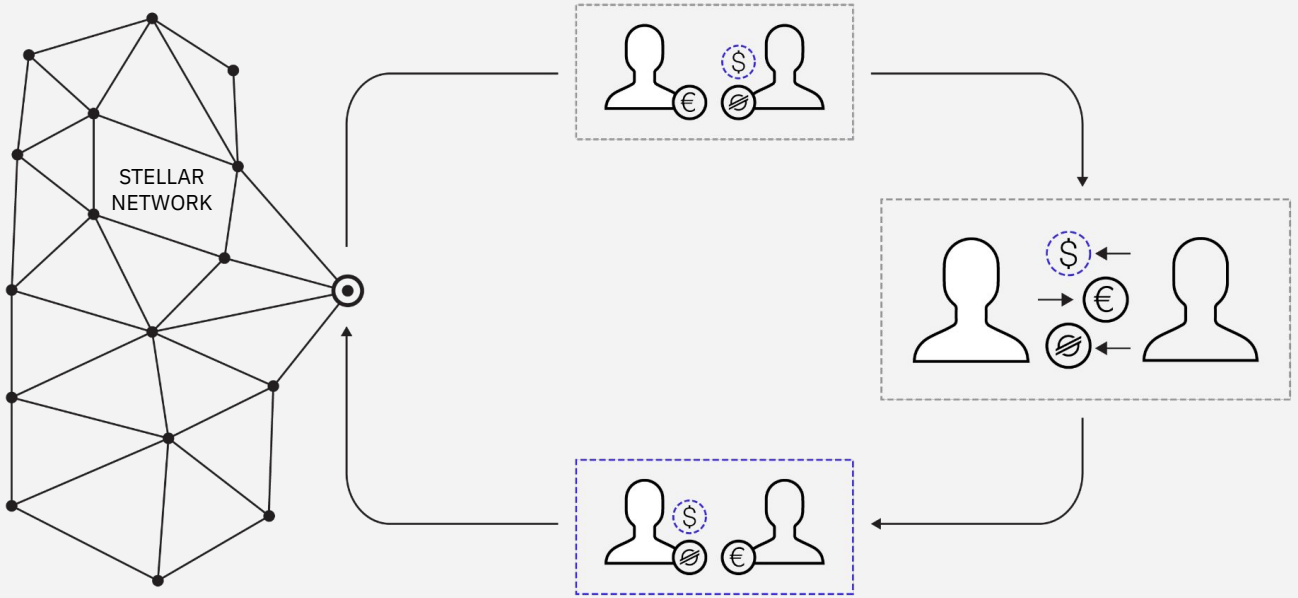
Enable Fast Payments Between Two Parties



Meridian

Payment Channels

Enable Fast Payments Between Two Parties



Meridian

Demo

PROTOTYPE OF A STARLIGHT PAYMENT CHANNEL

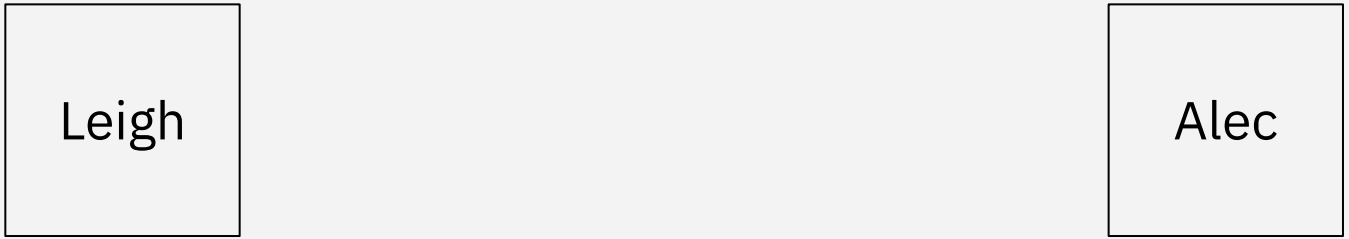
Meridian

OPENING A PAYMENT CHANNEL

Meridian

Opening a Payment Channel

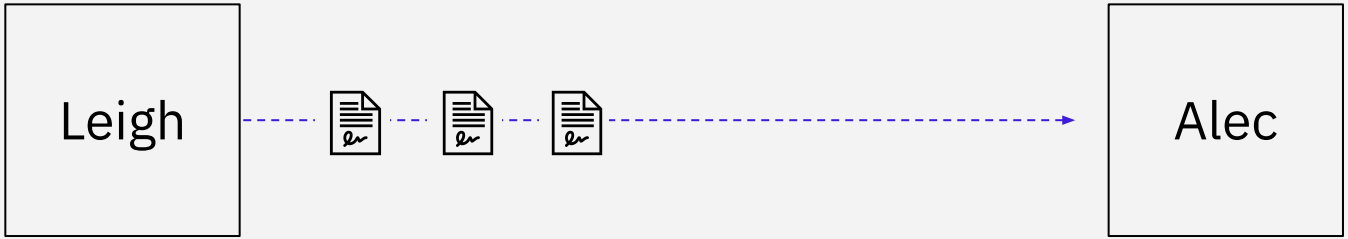
Involves Signing Three Transactions



Meridian

Opening a Payment Channel

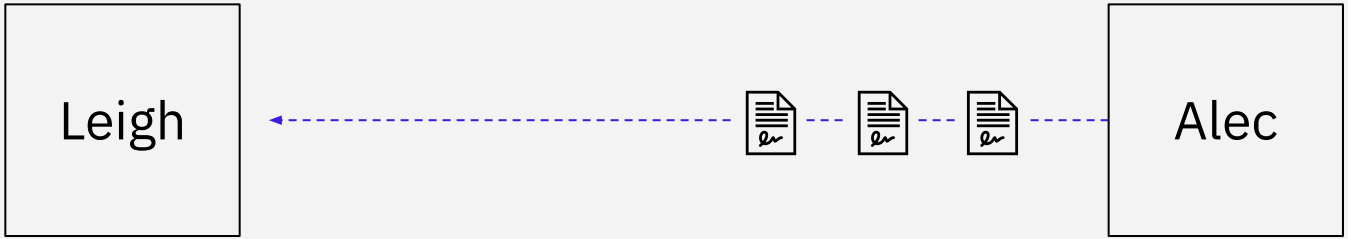
Both Parties Sign Each Transaction to Authorize the Agreement



Meridian

Opening a Payment Channel

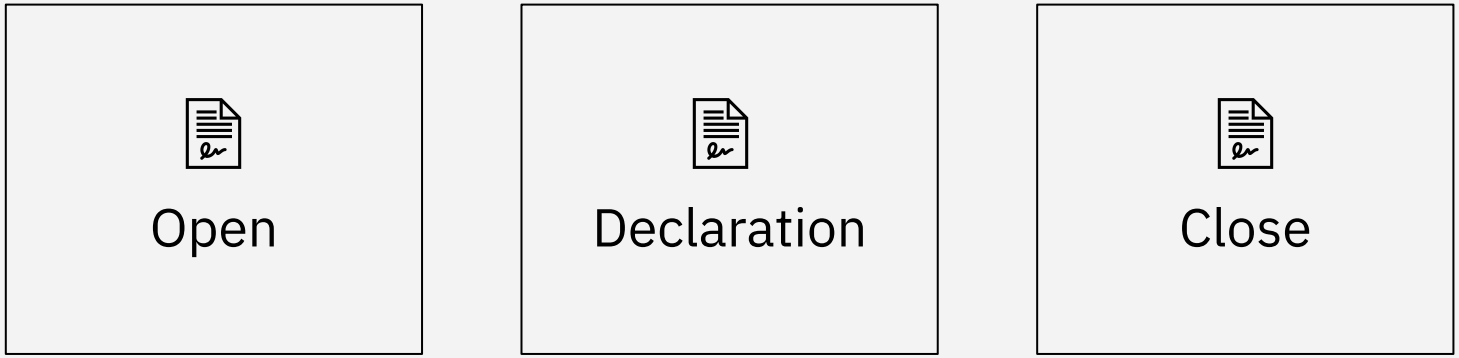
Both Parties Sign Each Transaction to Authorize the Agreement



Meridian

Opening a Payment Channel

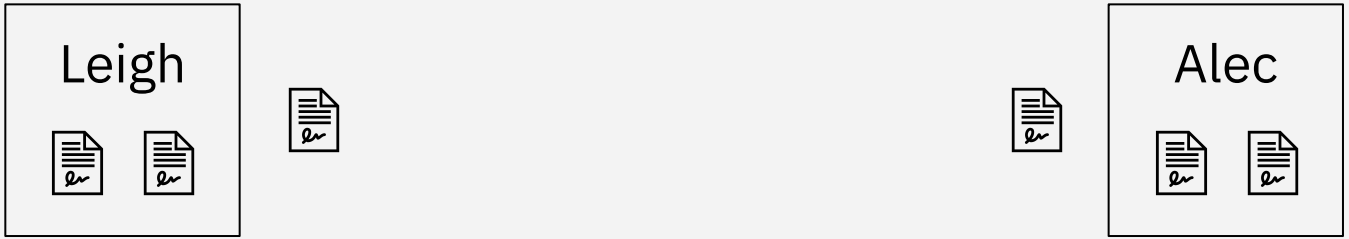
Defining the Three Transactions



Meridian

Opening a Payment Channel

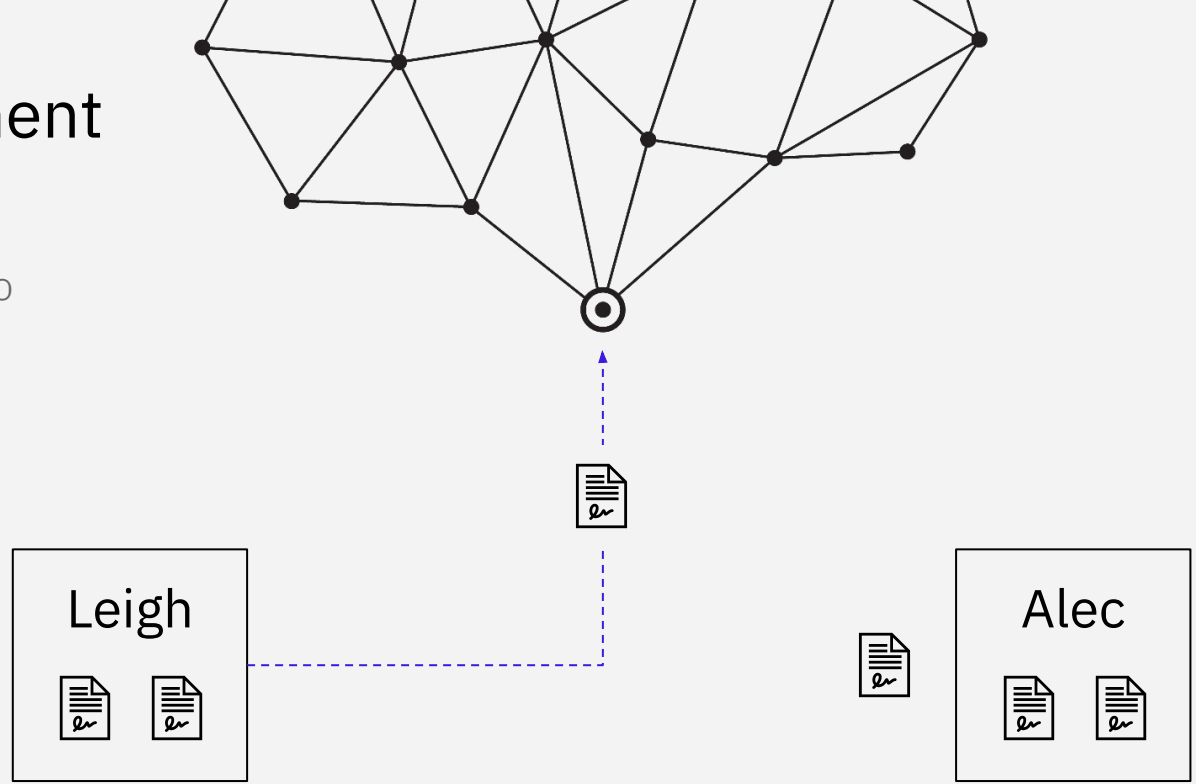
Submit Open Transaction to the Network



Meridian

Opening a Payment Channel

Submit Open Transaction to the Network



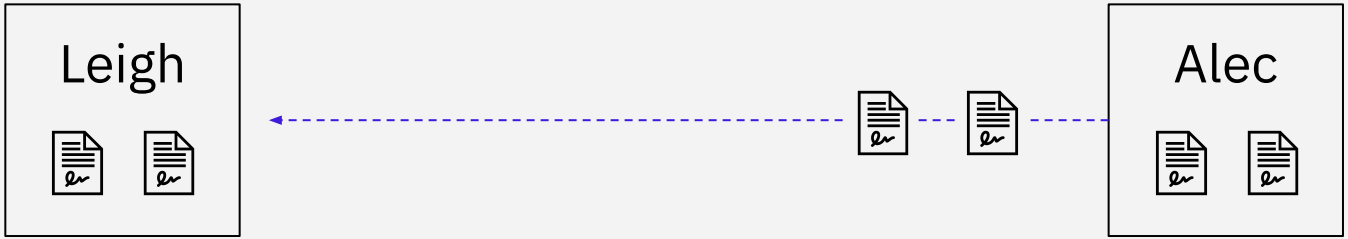
Meridian

MAKING A PAYMENT

Meridian

Making a Payment

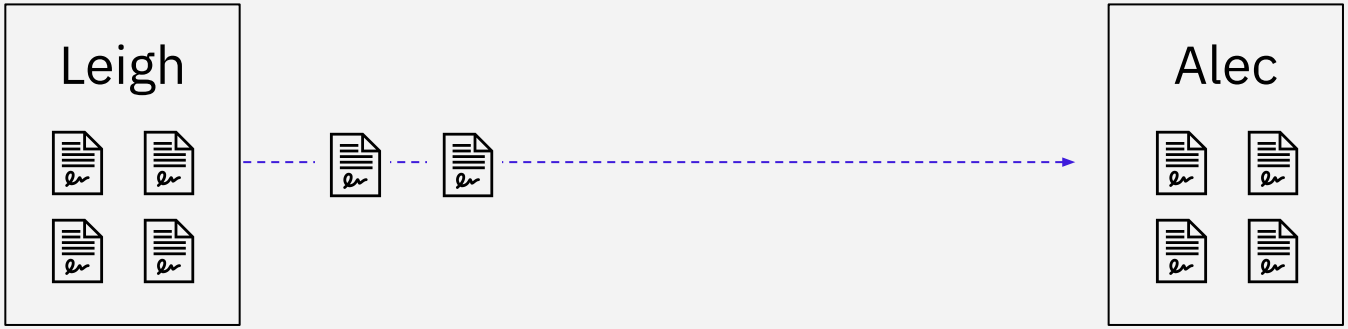
Proposes a New Close Agreement



Meridian

Making a Payment

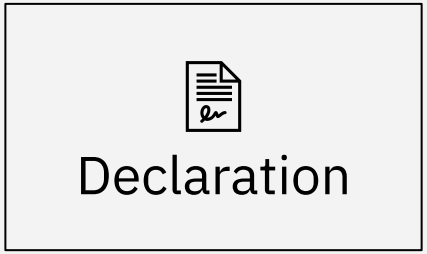
Confirms the New Agreement

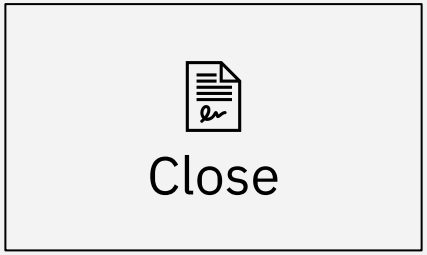


Meridian

Making a Payment

A Close Agreement Is Two Transactions

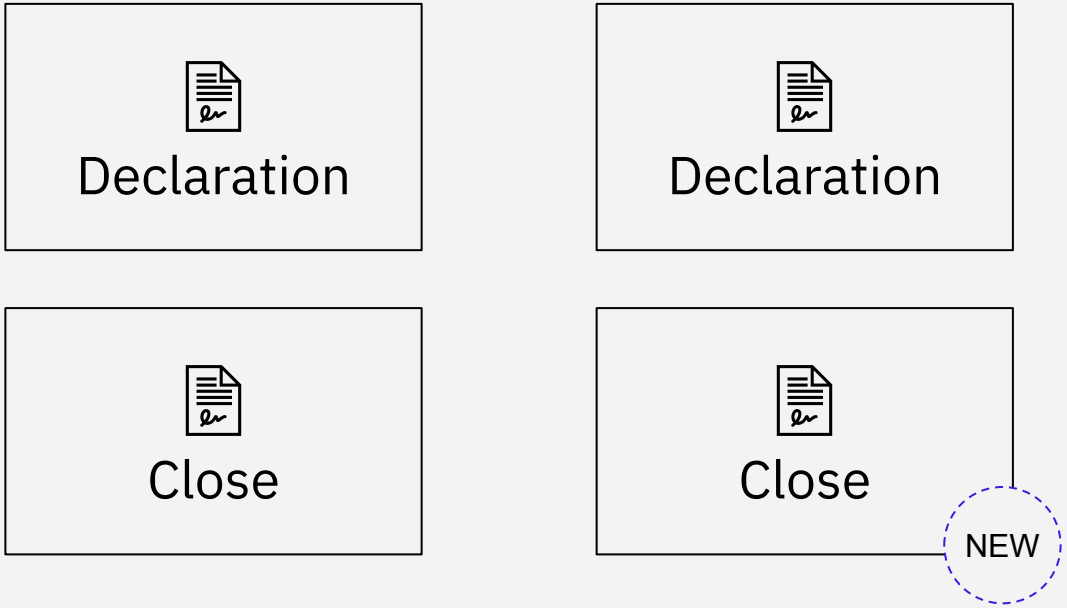




Meridian

Making a Payment

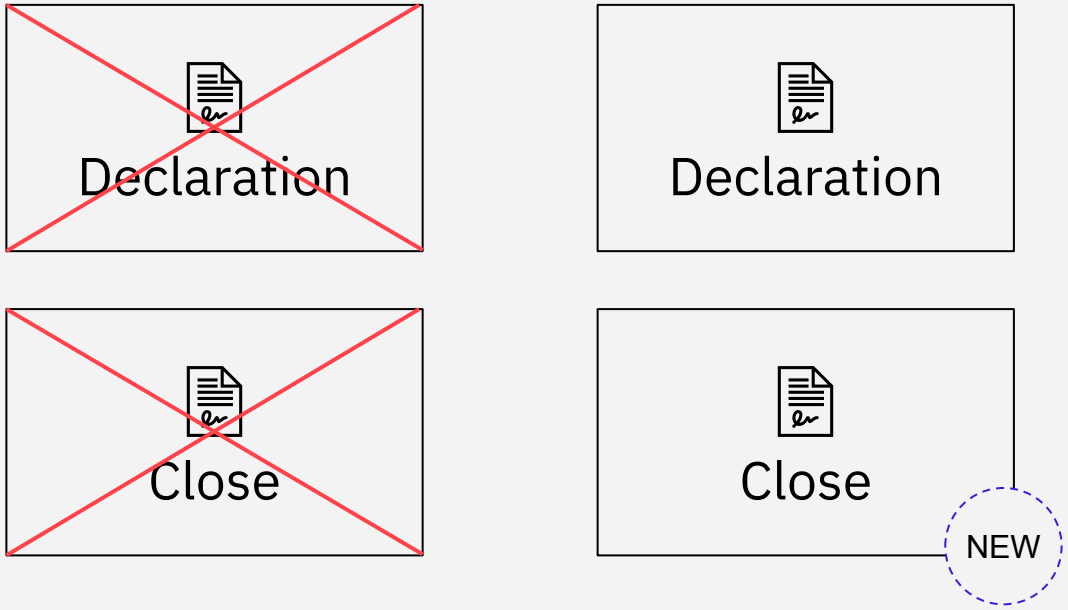
A Close Agreement Is Two Transactions



Meridian

Making a Payment

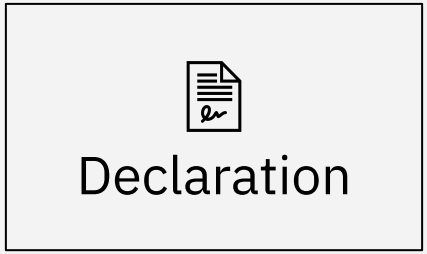
A Close Agreement Is Two Transactions



Meridian

The Declaration Transaction

Understanding the Role of the Declaration



Meridian

The Declaration Transaction

Using and Extending Sequence Numbers

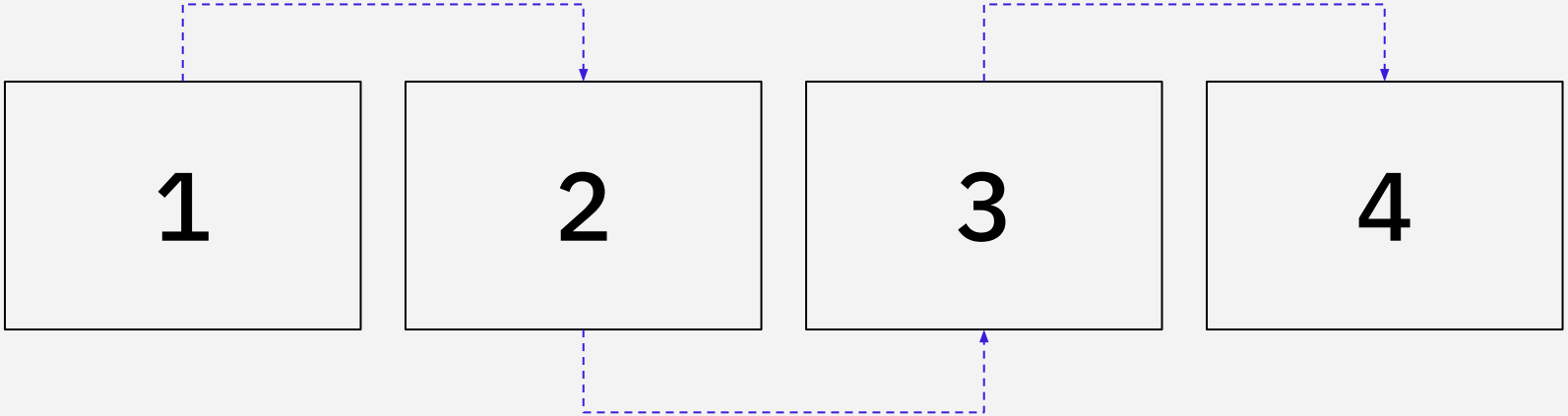
Meridian

Sequence Numbers

- Feature of the Stellar Network today
- Provides an order for how transactions must be executed on the network
- Stored in transactions
- Increases by one for every transaction
- Extension proposed in CAP-21

Sequence Numbers

Traditional Sequence Numbers Require a Series of Transactions to Execute in Order



Meridian

Sequence Numbers

CAP-21 Allows for Sequence Numbers to Be Skipped

Meridian

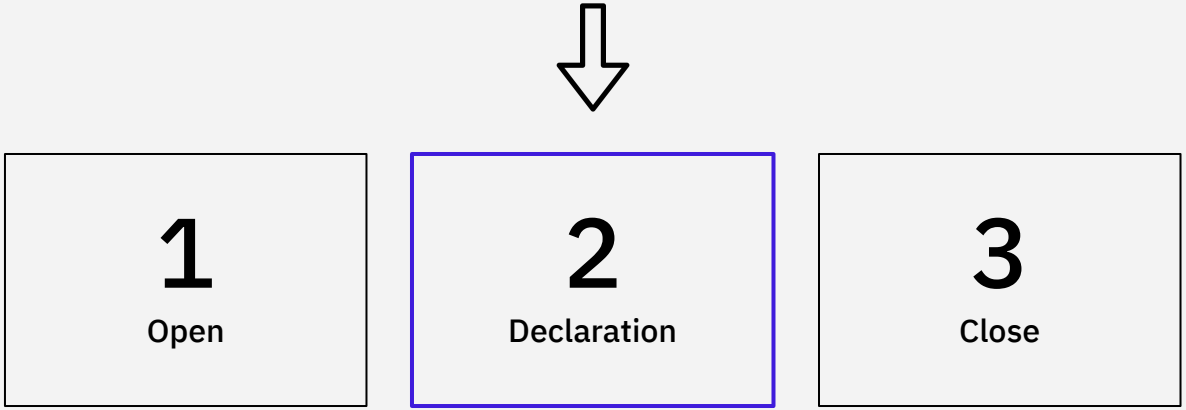
Sequence Numbers

Opening a Payment Channel Created Three Transactions

Meridian

Sequence Numbers

Opening a Payment Channel Created Three Transactions



Meridian

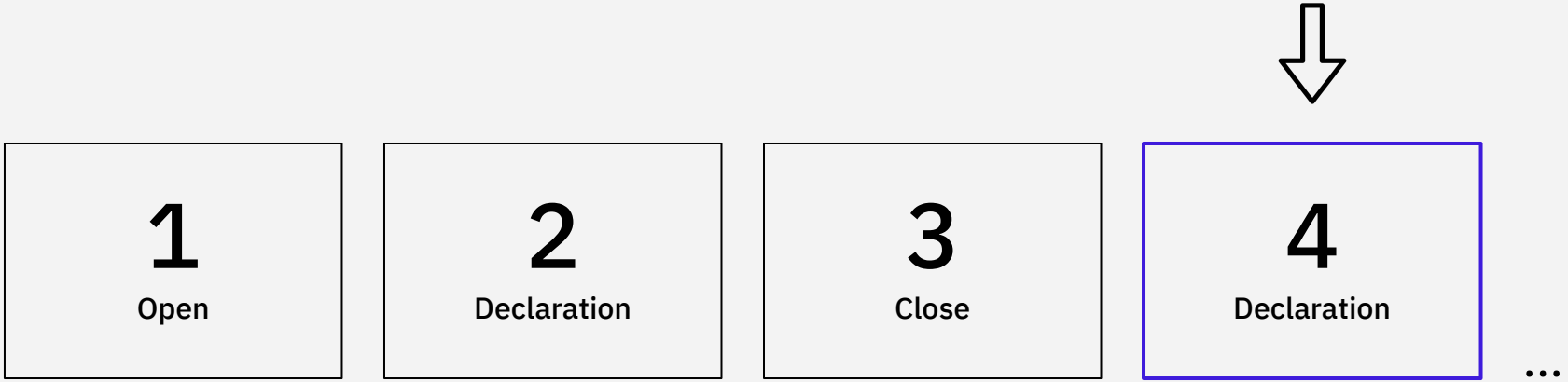
Sequence Numbers

Opening a Payment Channel Created Three Transactions

Meridian

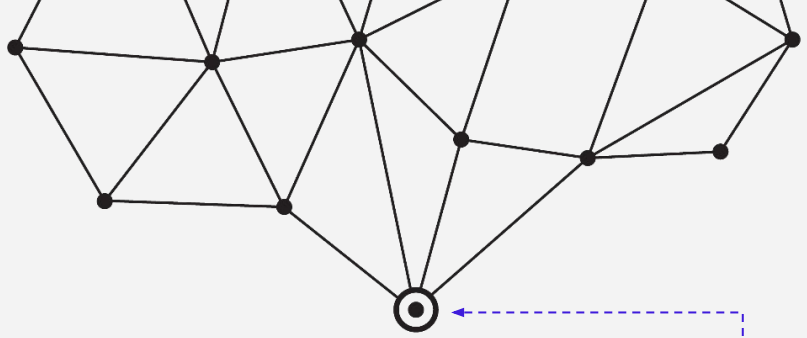
Sequence Numbers

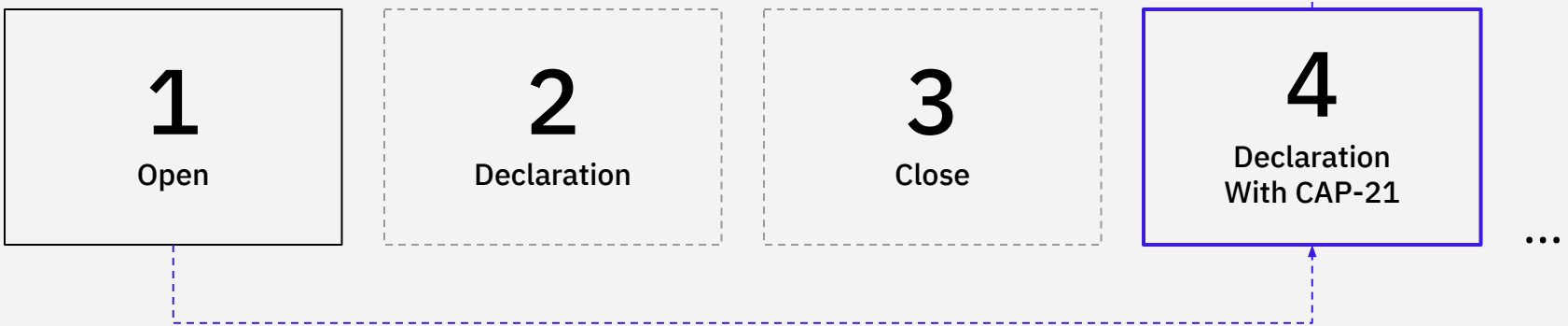
Making a Payment Creates a New Declaration and Close



Sequence Numbers

CAP-21 Permits the Close Process to Skip Ahead to the Most Recent Declaration

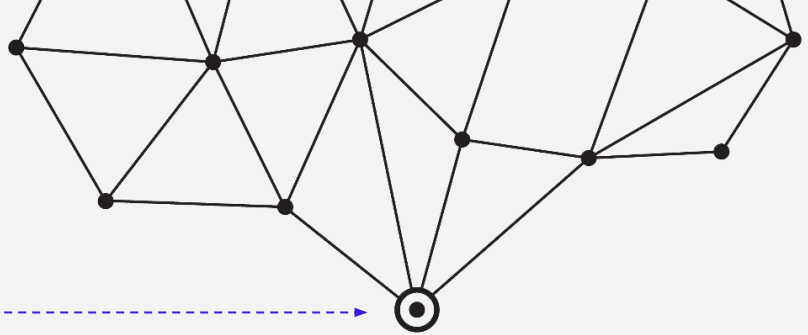




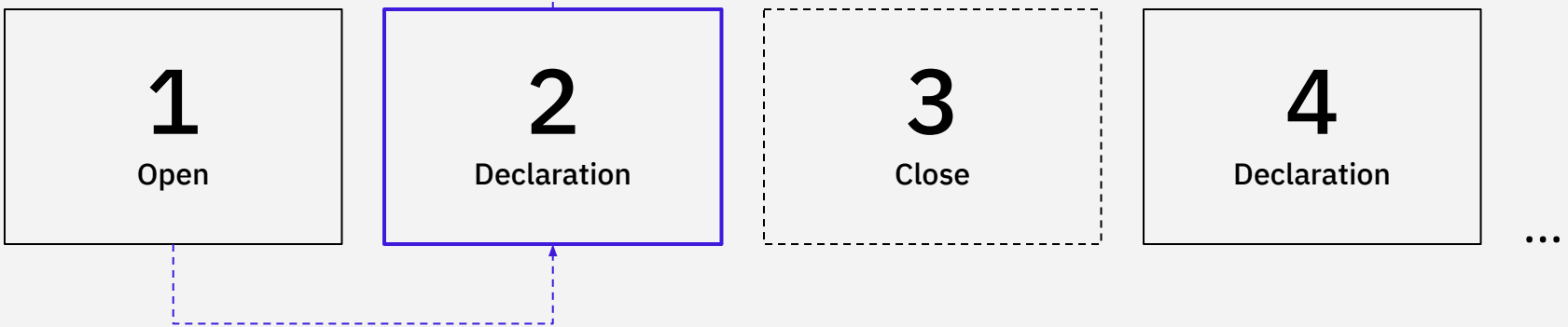
Meridian

Sequence Numbers

CAP-21 Allows Participants to Dispute Fraudulent Behavior

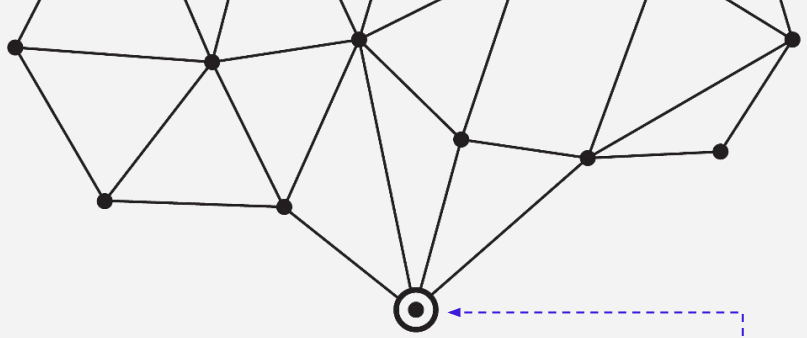


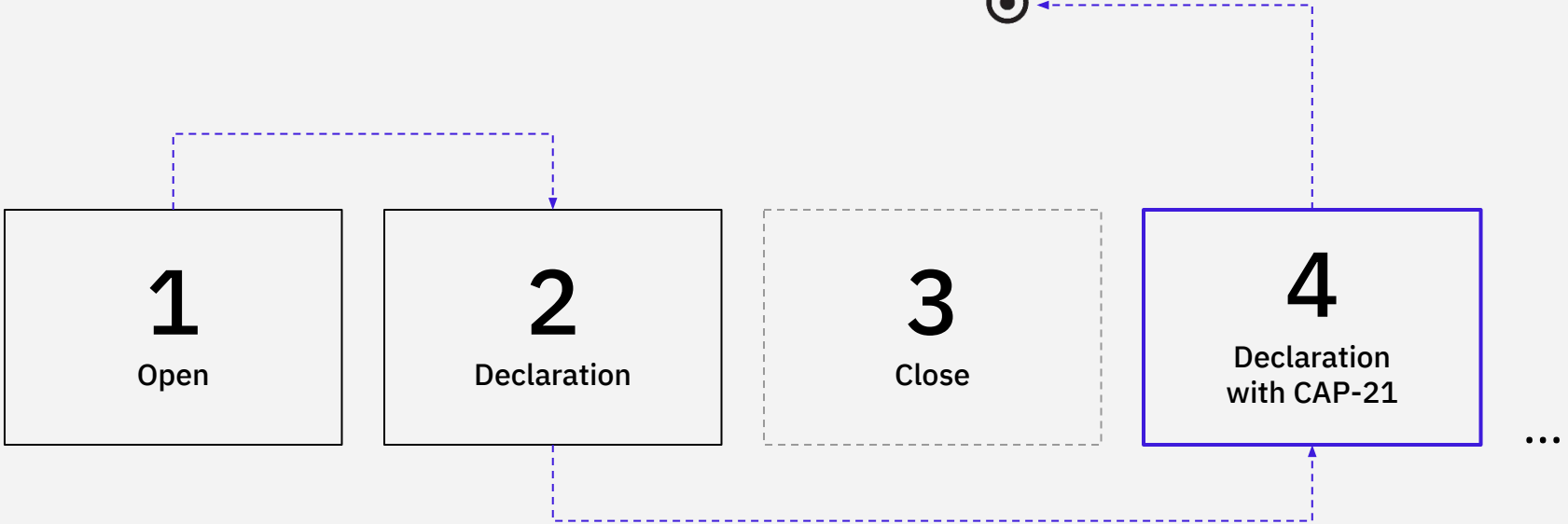
Meridian



Sequence Numbers

CAP-21 Allows Participants to Dispute Fraudulent Behavior

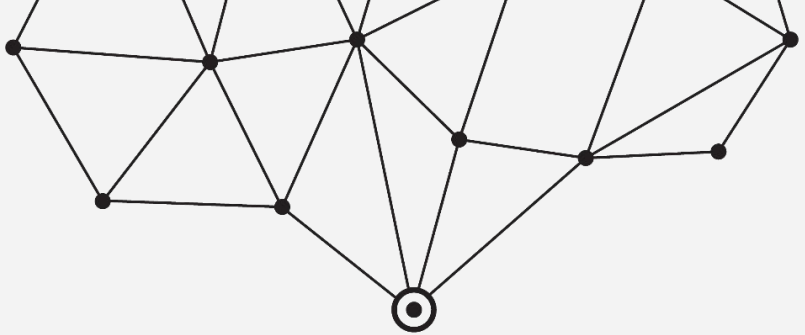




Meridian

Sequence Numbers

Cap-21 Makes Channels Lightweight



Meridian

~~1~~
~~Open~~

~~2~~
~~Declaration~~

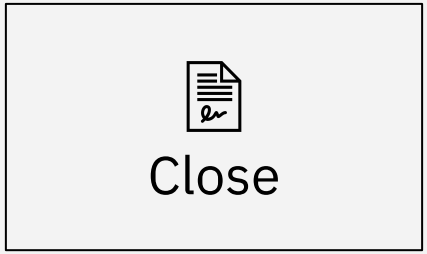
~~3~~
~~Close~~

4
Declaration
with CAP-21

...

The Close Transaction

Understanding the Role of the Close



Meridian

The Close Transaction

Contains a few operations

Meridian

Operations

- Payment – Distributes the net-settlement
- 2x Set Options – Modifies the signers of the accounts

The Close Transaction

Introducing a Transaction Time Delay

Meridian

Relative Time Lock

- New capability proposed in CAP-21
- Introduces a configurable delay between two transactions
- Delay is relative to when first transaction executes

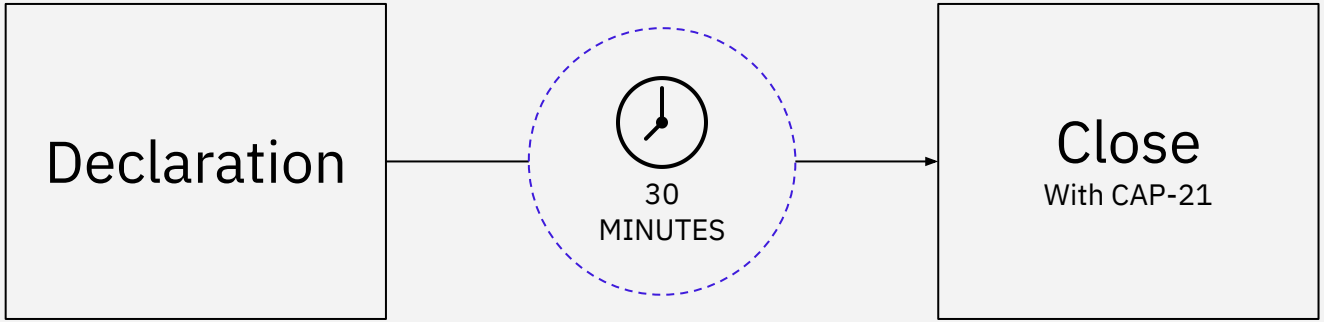
Relative Time Lock

How It Works

Meridian

Relative Time Lock

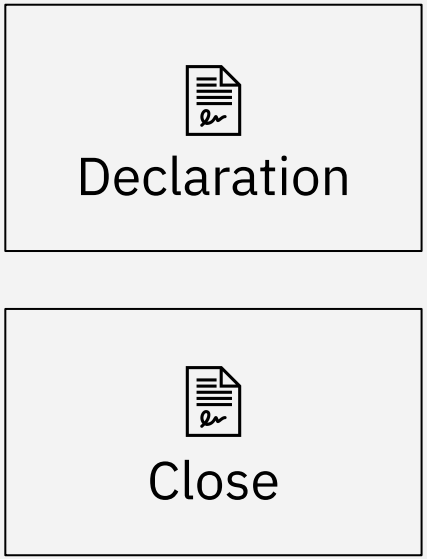
How It Works



Meridian

Making a Payment

A Close Agreement Is Two Transactions



Meridian

Atomic Signature Disclosure

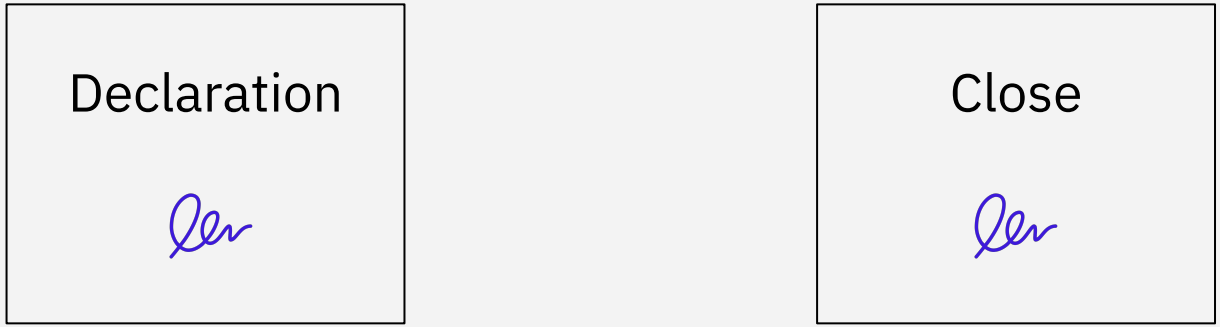
Meridian

A capability in CAP-40 to safely share signatures for multiple transactions in a single message.

Atomic Signature Disclosure

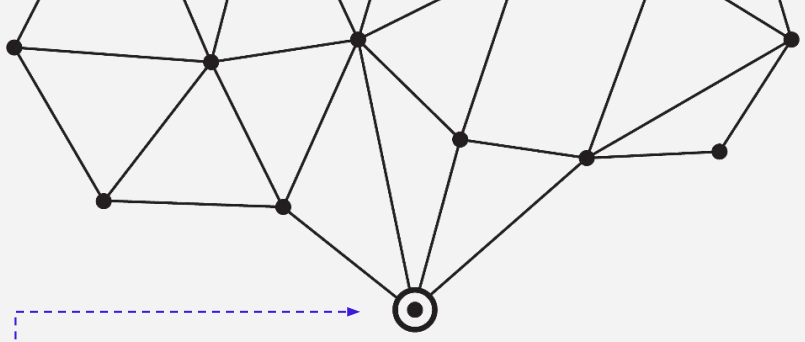
The Problem This Solves

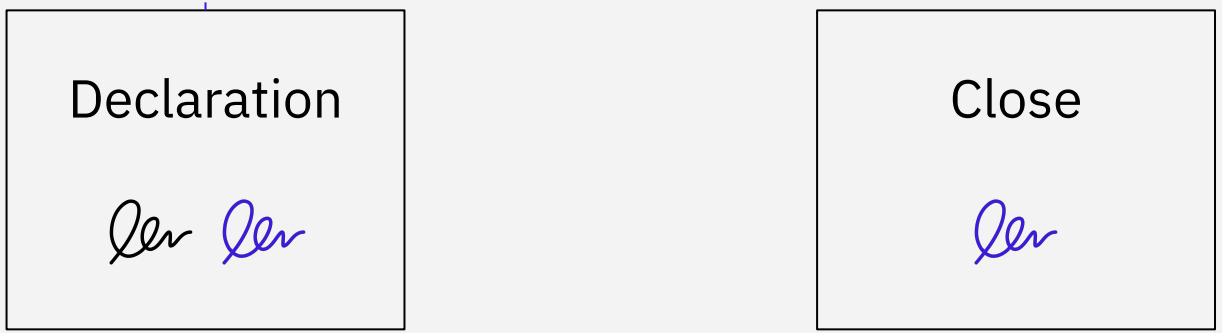
Meridian



Atomic Signature Disclosure

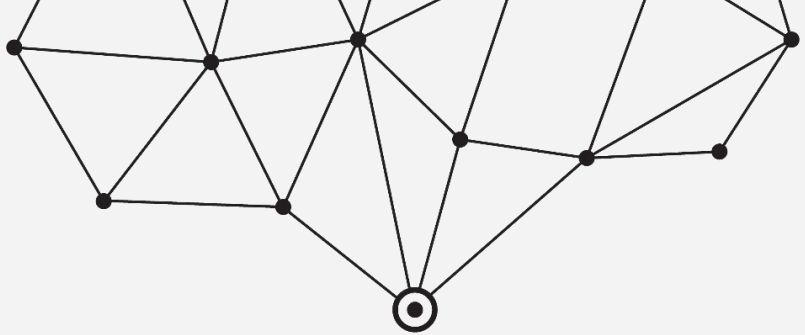
The Problem This Solves



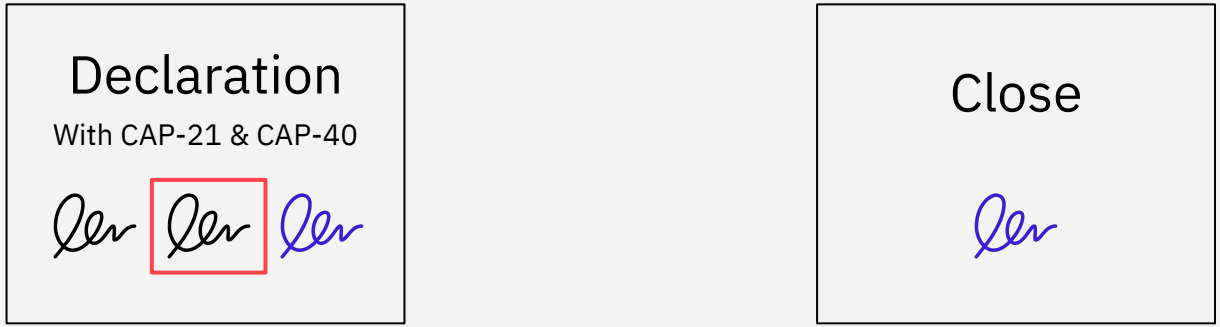


Meridian

Atomic Signature Disclosure



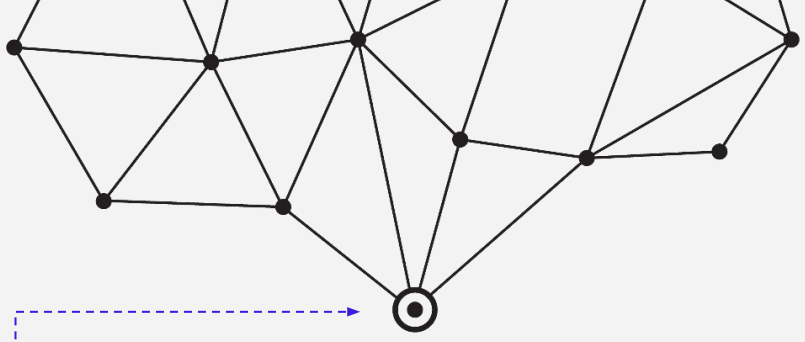
The Solution: CAP-40 and CAP-21 Require the Signature of the Close Within the Declaration



Meridian

Atomic Signature Disclosure

The Solution: CAP-40 and CAP-21 Require the Signature of the Close Within the Declaration



Declaration

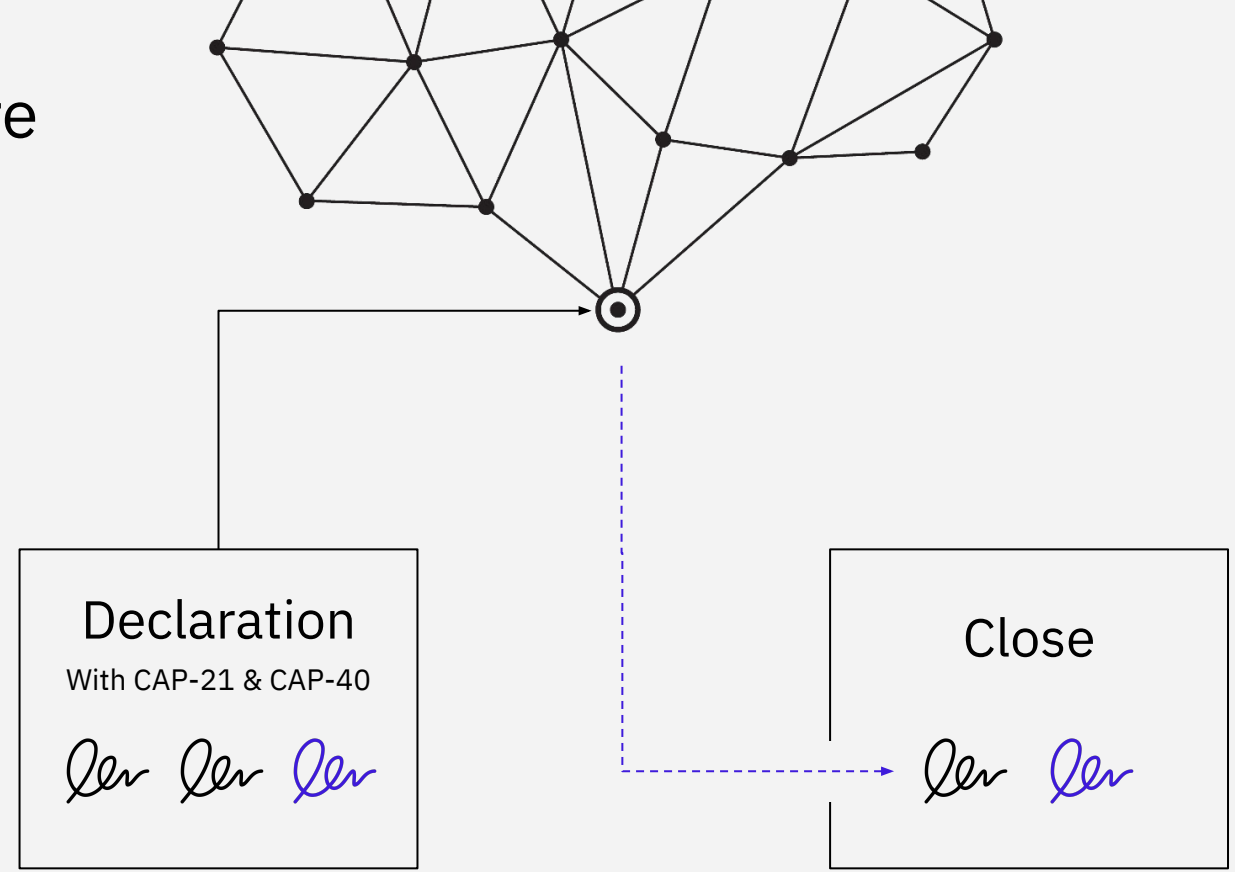
With CAP-21 & CAP-40

Close

Meridian

Atomic Signature Disclosure

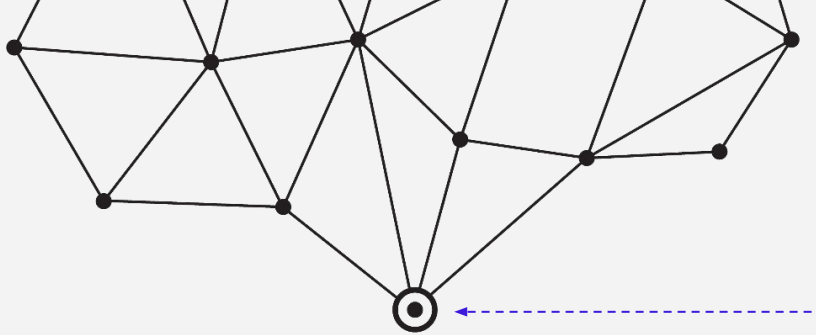
The Solution: CAP-40 and CAP-21 Require the Signature of the Close Within the Declaration



Meridian

Atomic Signature Disclosure

Allowing the Other Participant to Copy the Embedded Signature and Submit the Close



Declaration

With CAP-21 & CAP-40

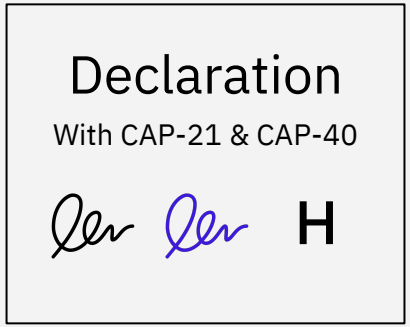
Close

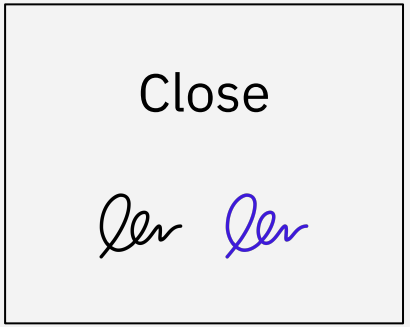
Meridian

Adding Hash Signers Directly to Transactions

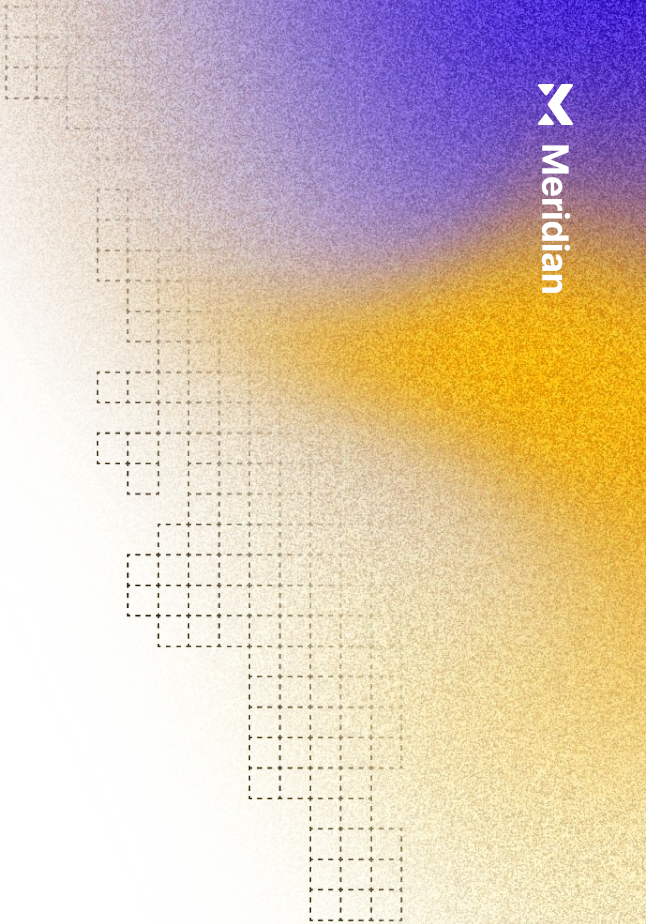
Another CAP-21 Capability: Stateless HTLCs

Meridian





BUFFERING PAYMENTS

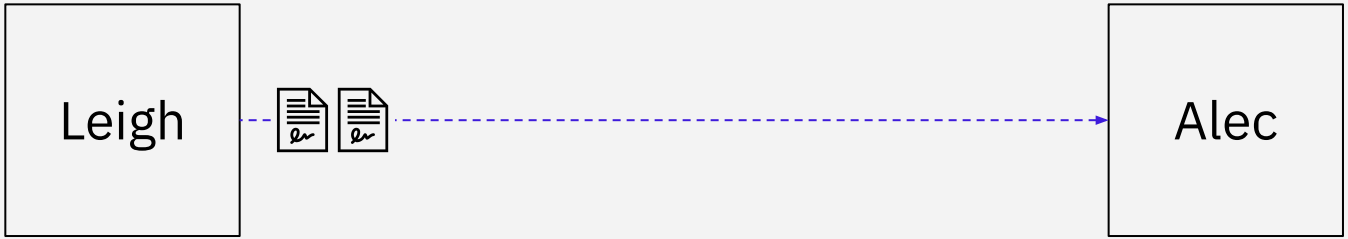


Buffering Payments

Collect Payments While an Agreement Is Being Authorized

Meridian

Buffer = 0 payments

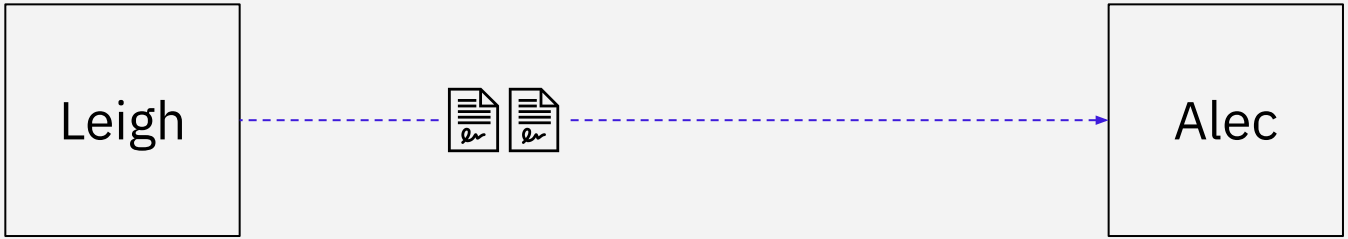


Buffering Payments

Collect Payments While an Agreement Is Being Authorized

Meridian

Buffer = 23 payments



Buffering Payments

Collect Payments While an Agreement Is Being Authorized

Meridian

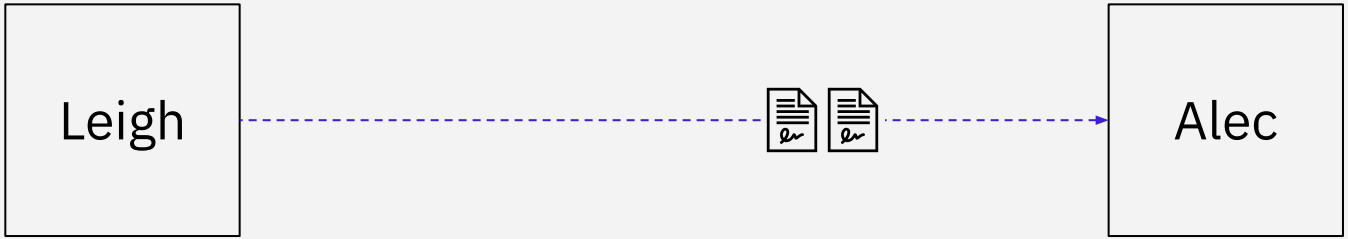
Buffer = 63 payments

Buffering Payments

Collect Payments While an Agreement Is Being Authorized

Meridian

Buffer = 407 payments

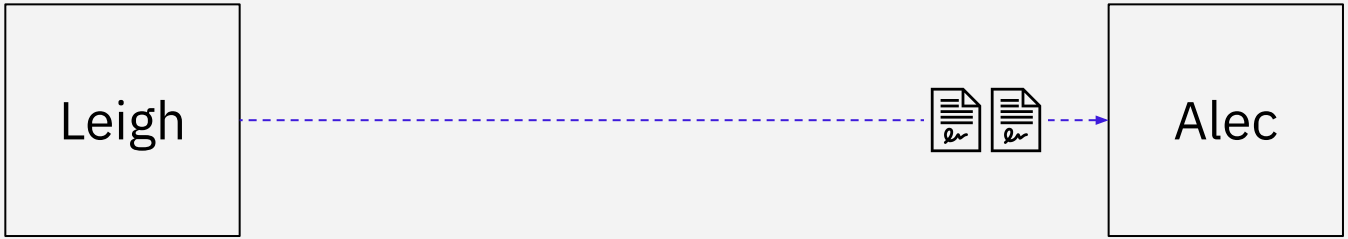


Buffering Payments

Collect Payments While an Agreement Is Being Authorized

Meridian

Buffer = 614 payments

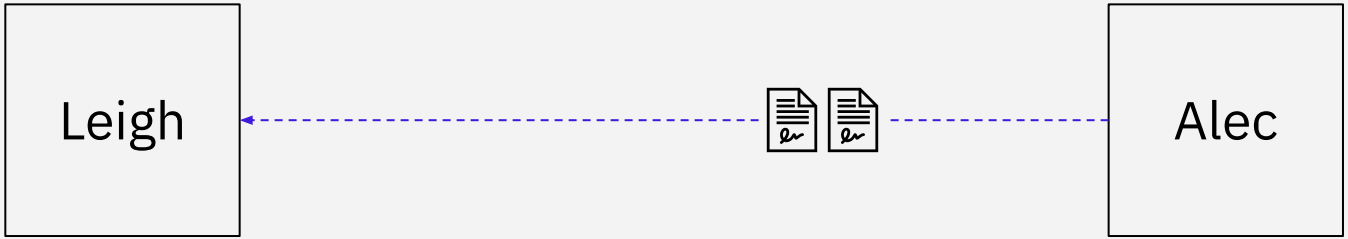


Buffering Payments

Collect Payments While an Agreement Is Being Authorized

Meridian

Buffer = 768 payments



Buffering Payments

Collect Payments While an Agreement Is Being Authorized

Meridian

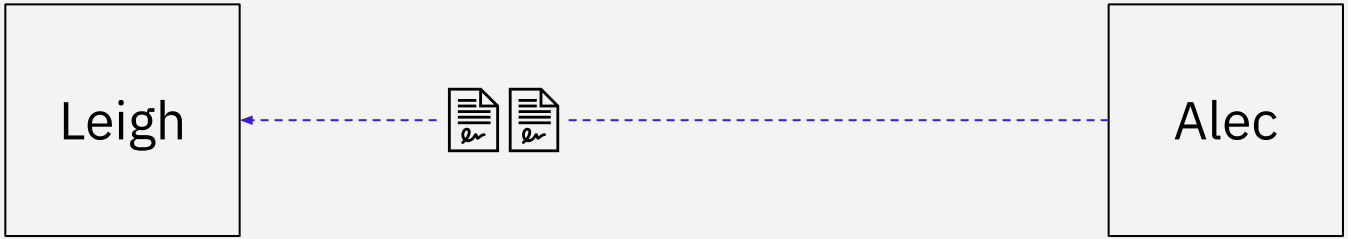
Buffer = 1092 payments

Buffering Payments

Collect Payments While an Agreement Is Being Authorized

Meridian

Buffer = 1250 payments

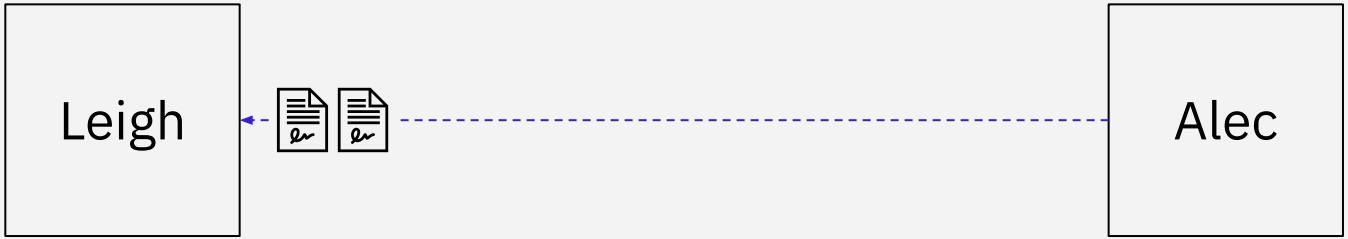


Buffering Payments

Collect Payments While an Agreement Is Being Authorized

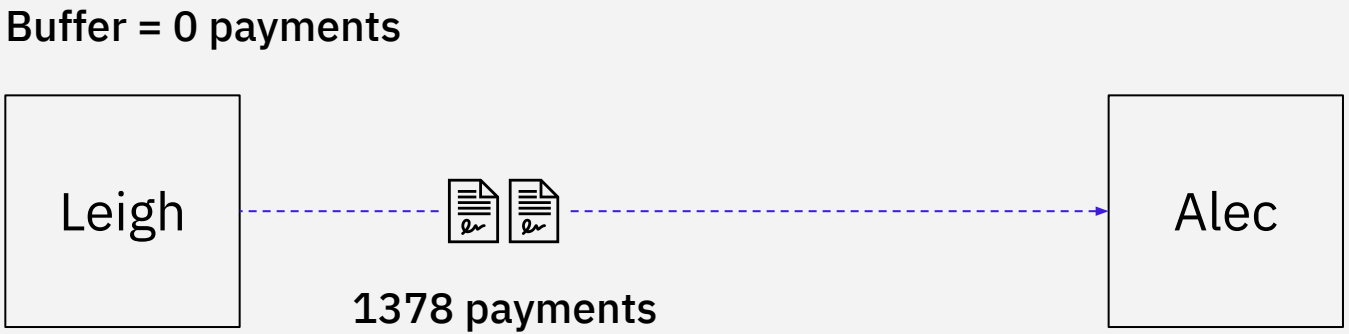
Meridian

Buffer = 1378 payments



Buffering Payments

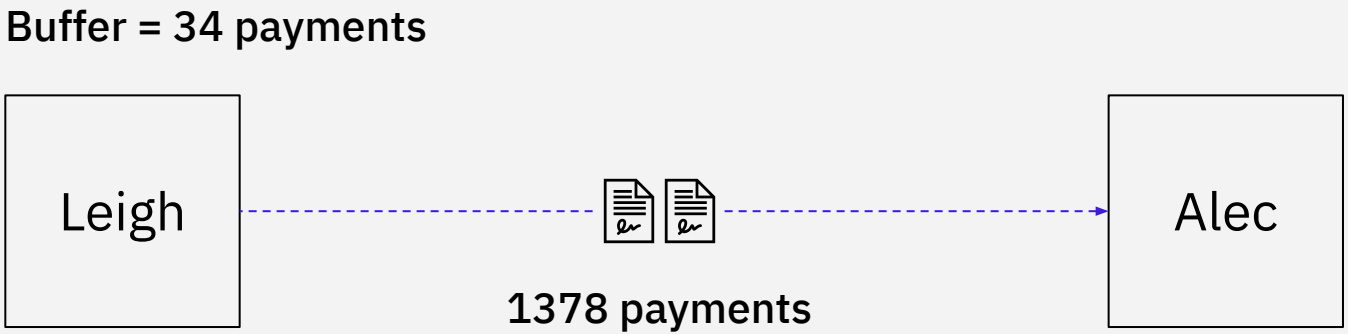
Propose a New Agreement With the Payments Previously Buffered



Buffering Payments

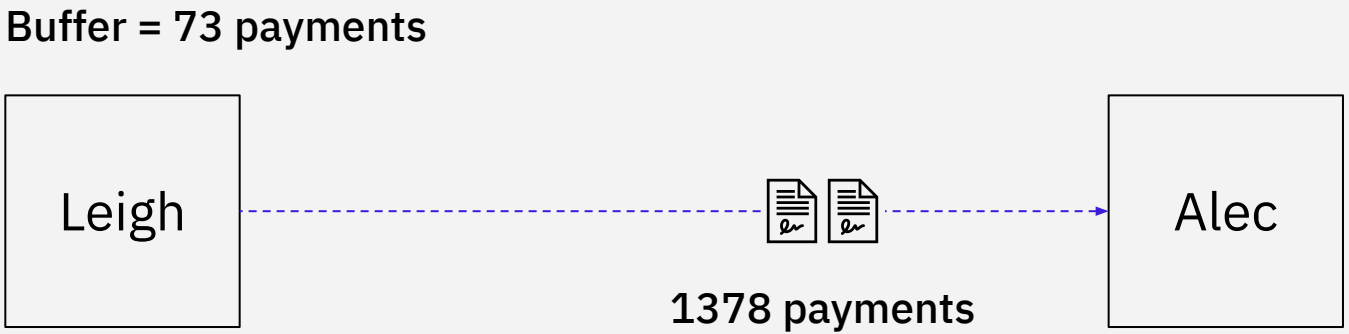
Propose a New Agreement With the Payments Previously Buffered

Meridian



Buffering Payments

Each Subsequent Agreement Will Contain All
Payments Buffered During the 30 Millisecond Wait

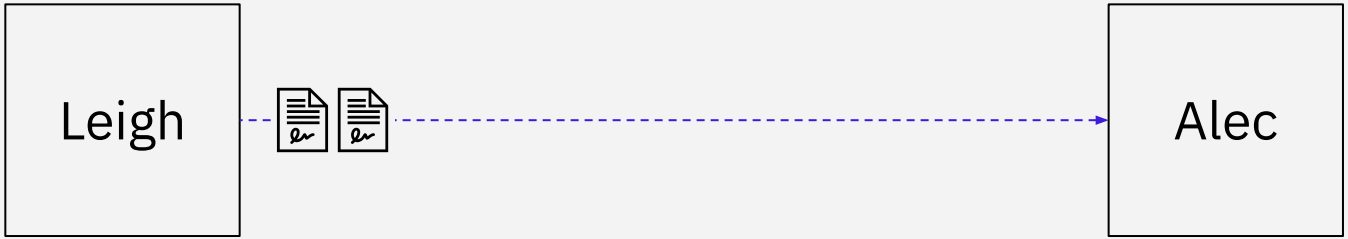


CLOSING THE PAYMENT CHANNEL

Meridian

Closing the Payment Channel

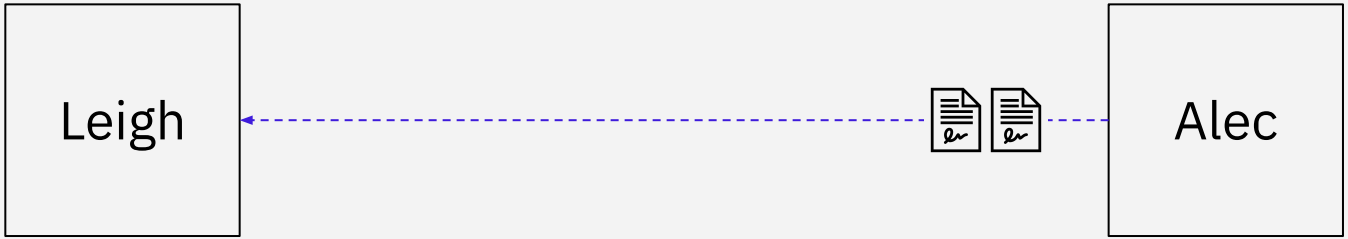
Both Parties Sign to Authorize the Agreement



Meridian

Closing the Payment Channel

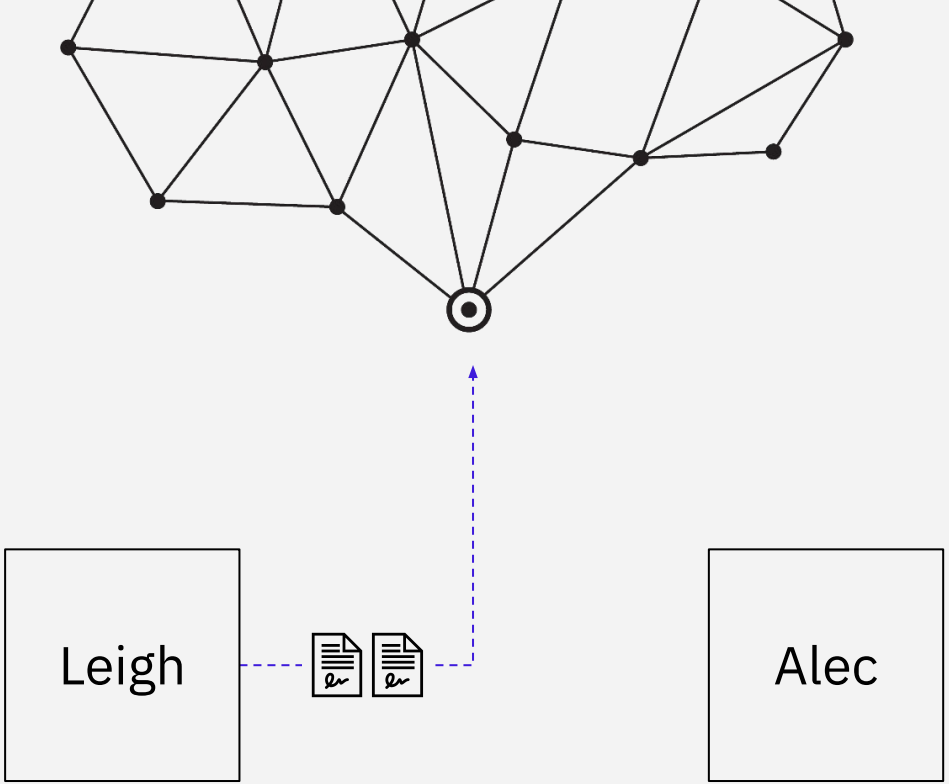
Both Parties Sign to Authorize the Agreement



Meridian

Closing the Payment Channel

Submit to the Network



Meridian

Starlight Demo

A Summary

Meridian

1

We Opened and Closed a Channel

- Performed millions of payments
- Closed the channel quickly because the Stellar network is fast

2

We Did It Efficiently

- Stored only the most recent agreement leveraging CAP-21
- Used single message in either direction to exchange signatures using CAP-40

3

We Can Recover

- Able to dispute fraudulent behavior using CAP-21
- Able to recover signatures not shared using CAP-40

WHAT’S NEXT?

Meridian

Check Out Starlight

Public and Open Source

Meridian

Open Source

github.com/stellar/starlight

- Docker image runs a network with prototypes of CAP-21 and CAP-40
- Starlight Go SDK
- Example code

THANK YOU

github.com/stellar/starlight

Meridian