

Keyhive

 Coordination-Free Access Control for Local-First Apps 

Keyhive

 Coordination-Free Access Control for Local-First Apps 

Keyhive

Brooklyn Zelenka — @expede

Keyhive

Brooklyn Zelenka — @expede

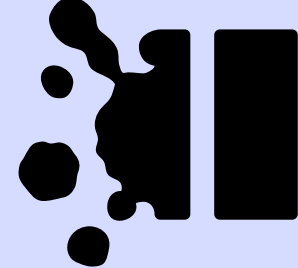


github.com/expede
Vancouver 🇨🇦

Keyhive

Brooklyn Zelenka — @expede

- ◆ Senior researcher at **Ink & Switch**



- ◆ Lead the **Keyhive** project 

- ◆ Team included **John Mumm** & **Alex Good** 

- ◆ Feedback with Martin Kleppmann, DXOS, Serenity, Matrix, & others

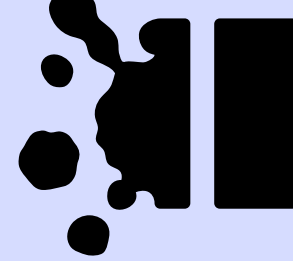


github.com/expede
Vancouver 

Keyhive

Brooklyn Zelenka — @expede



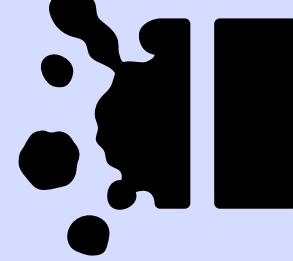
- ◆ Senior researcher at **Ink & Switch** 
- ◆ Lead the **Keyhive** project 
- ◆ Team included **John Mumm** & **Alex Good** 
- ◆ Feedback with Martin Kleppmann, DXOS, Serenity, Matrix, & others
- ◆ Spec editor for **UCAN** P2P auth & RPC system

github.com/expede
Vancouver 

Keyhive

Brooklyn Zelenka — @expede



- ◆ Senior researcher at **Ink & Switch** 
- ◆ Lead the **Keyhive** project 
- ◆ Team included **John Mumm** & **Alex Good** 
- ◆ Feedback with Martin Kleppmann, DXOS, Serenity, Matrix, & others
- ◆ Spec editor for **UCAN** P2P auth & RPC system
- ◆ Originated **WNFS**, an E2EE distributed file system

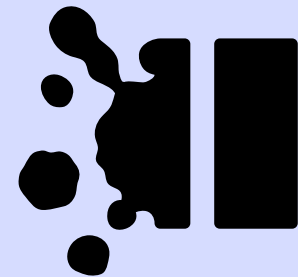
github.com/expede
Vancouver 

Keyhive

Brooklyn Zelenka — @expede



- ◆ Senior researcher at **Ink & Switch**



- ◆ Lead the **Keyhive** project 

- ◆ Team included **John Mumm** & **Alex Good** 

- ◆ Feedback with Martin Kleppmann, DXOS, Serenity, Matrix, & others

- ◆ Spec editor for **UCAN** P2P auth & RPC system

- ◆ Originated **WNFS**, an E2EE distributed file system

- ◆ Wrote some auth **EIPs** in my misspent crypto youth

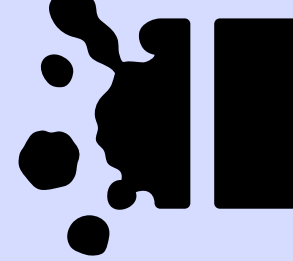
github.com/expede
Vancouver 

Keyhive

Brooklyn Zelenka — @expede



github.com/expede
Vancouver 🇨🇦

- ◆ Senior researcher at **Ink & Switch** 
- ◆ Lead the **Keyhive** project 
- ◆ Team included **John Mumm** & **Alex Good** 🥳
- ◆ Feedback with Martin Kleppmann, DXOS, Serenity, Matrix, & others
- ◆ Spec editor for **UCAN** P2P auth & RPC system
- ◆ Originated **WNFS**, an E2EE distributed file system
- ◆ Wrote some auth **EIPs** in my misspent crypto youth
- ◆ 30 minutes, *let's gooooo*

Keyhive *Topics*



What is local-first?

Motivate our authz approach

Describe Keyhive's design

Keyhive

Core Components

Keyhive

Core Components

ConCap

Convergent Capabilities / Auth CRDT

Keyhive

Core Components

BeeKEM

Decentralised Continuous Group Key Agreement Protocol

ConCap

Convergent Capabilities / Auth CRDT

Keyhive

Core Components

Causal Encryption

Key Distribution Scheme

BeeKEM

Decentralised Continuous Group Key Agreement Protocol

ConCap

Convergent Capabilities / Auth CRDT

Keyhive

Core Components

Beelay

E2EE Linked-Document Sync System

Causal Encryption

Key Distribution Scheme

BeeKEM

Decentralised Continuous Group Key Agreement Protocol

ConCap

Convergent Capabilities / Auth CRDT

Keyhive

Core Components

Beelay

E2EE Linked-Document Sync System

Causal Encryption

Key Distribution Scheme

BeeKEM

Decentralised Continuous Group Key Agreement Protocol

ConCap

Convergent Capabilities / Auth CRDT

A Local-First Primer

Beyond "Offline-Capable"



A Local-First Primer

Local-First, Not Local-Only

A Local-First Primer

Local-First, Not Local-Only



A Local-First Primer

Local-First, Not Local-Only



A Local-First Primer

Orienting Philosophy

Seven ideals for local-first software

1. No spinners: your work at your fingertips
2. Your work is not trapped on one device
3. The network is optional
4. Seamless collaboration with your colleagues
5. The Long Now
6. Security and privacy by default
7. You retain ultimate ownership and control

A Local-First Primer

Orienting Philosophy

Seven ideals for local-first software

1. No spinners: your work at your fingertips
2. Your work is not trapped on one device
3. The network is optional
4. Seamless collaboration with your colleagues
5. The Long Now
6. Security and privacy by default
7. You retain ultimate ownership and control

A Local-First Primer

Orienting Philosophy

Seven ideals for local-first software

1. No spinners: your work at your fingertips
2. Your work is not trapped on one device
3. The network is optional

4. Seamless collaboration with your colleagues

5. The Long Now

6. Security and privacy by default

7. You retain ultimate ownership and control

A Local-First Primer

Orienting Philosophy

Seven ideals for local-first software

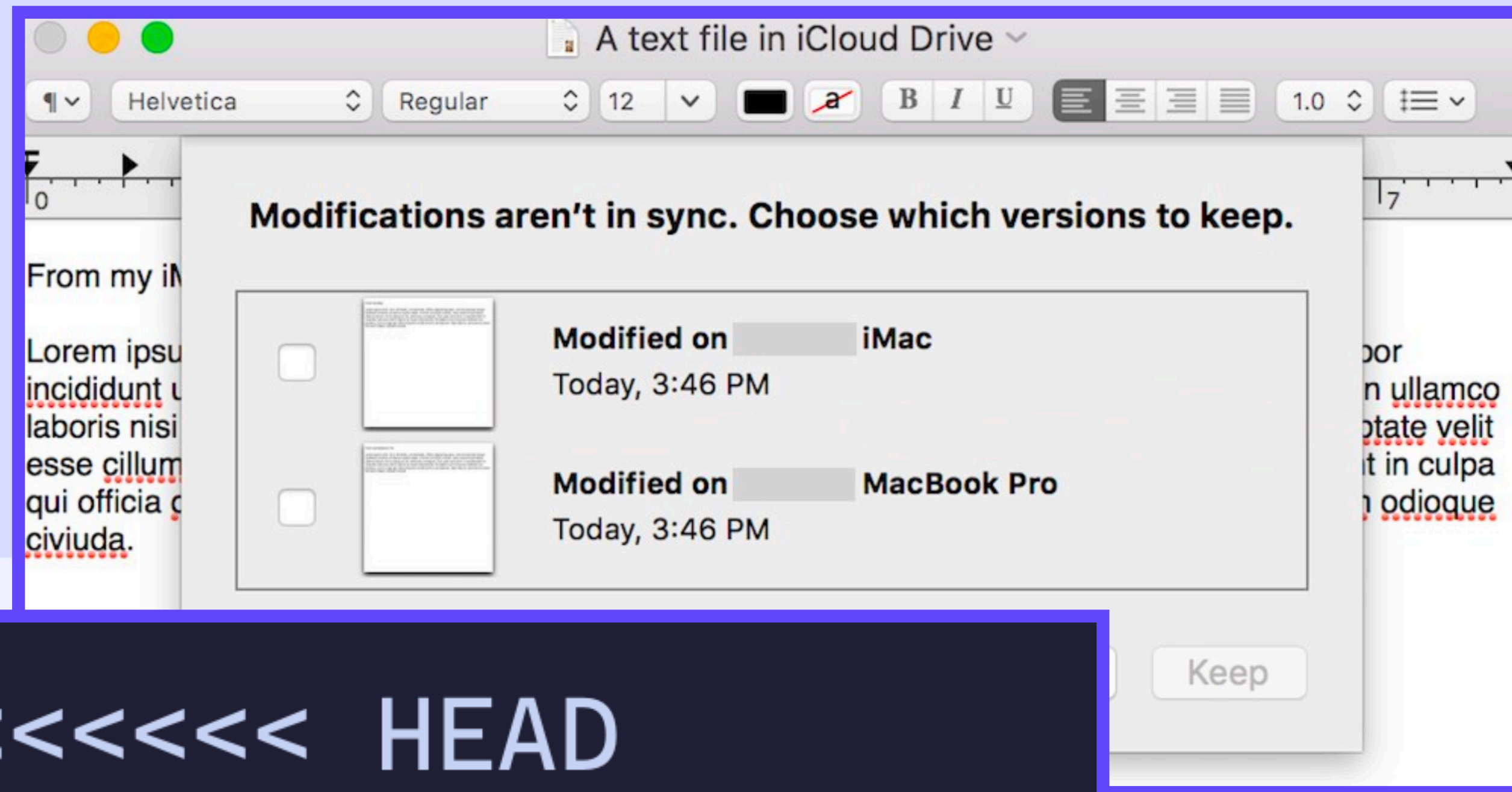
1. No spinners: your work at your fingertips
2. Your work is not trapped on one device
3. The network is optional
4. Seamless collaboration with your colleagues
5. The Long Now
6. Security and privacy by default
7. You retain ultimate ownership and control

A Local-First Primer

Automatic Merges

A Local-First Primer

Automatic Merges



```
<<<<<<< HEAD
```

```
Option A
```

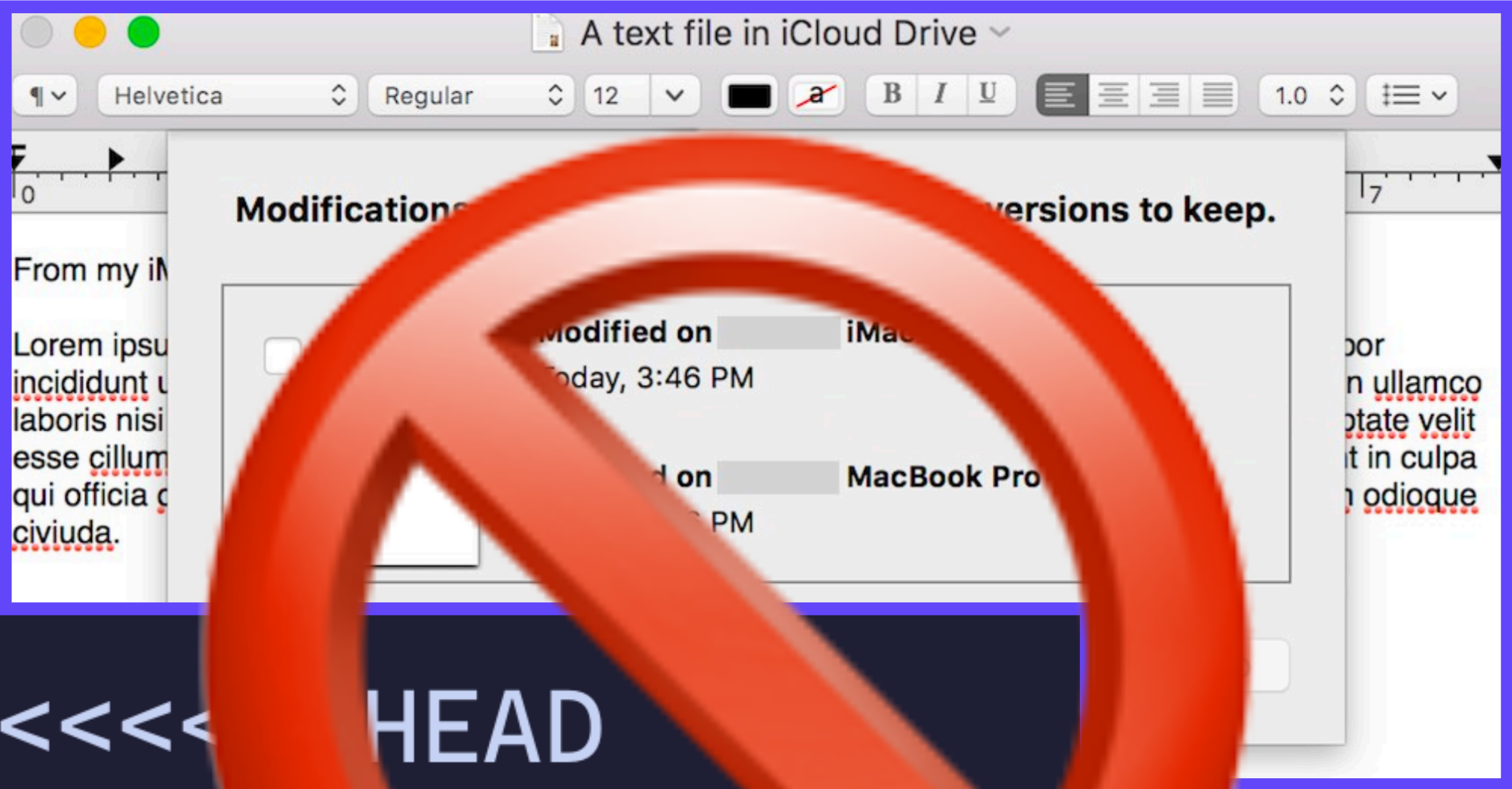
```
=====
```

```
Option B
```

```
>>>>>>> some-branch
```

A Local-First Primer

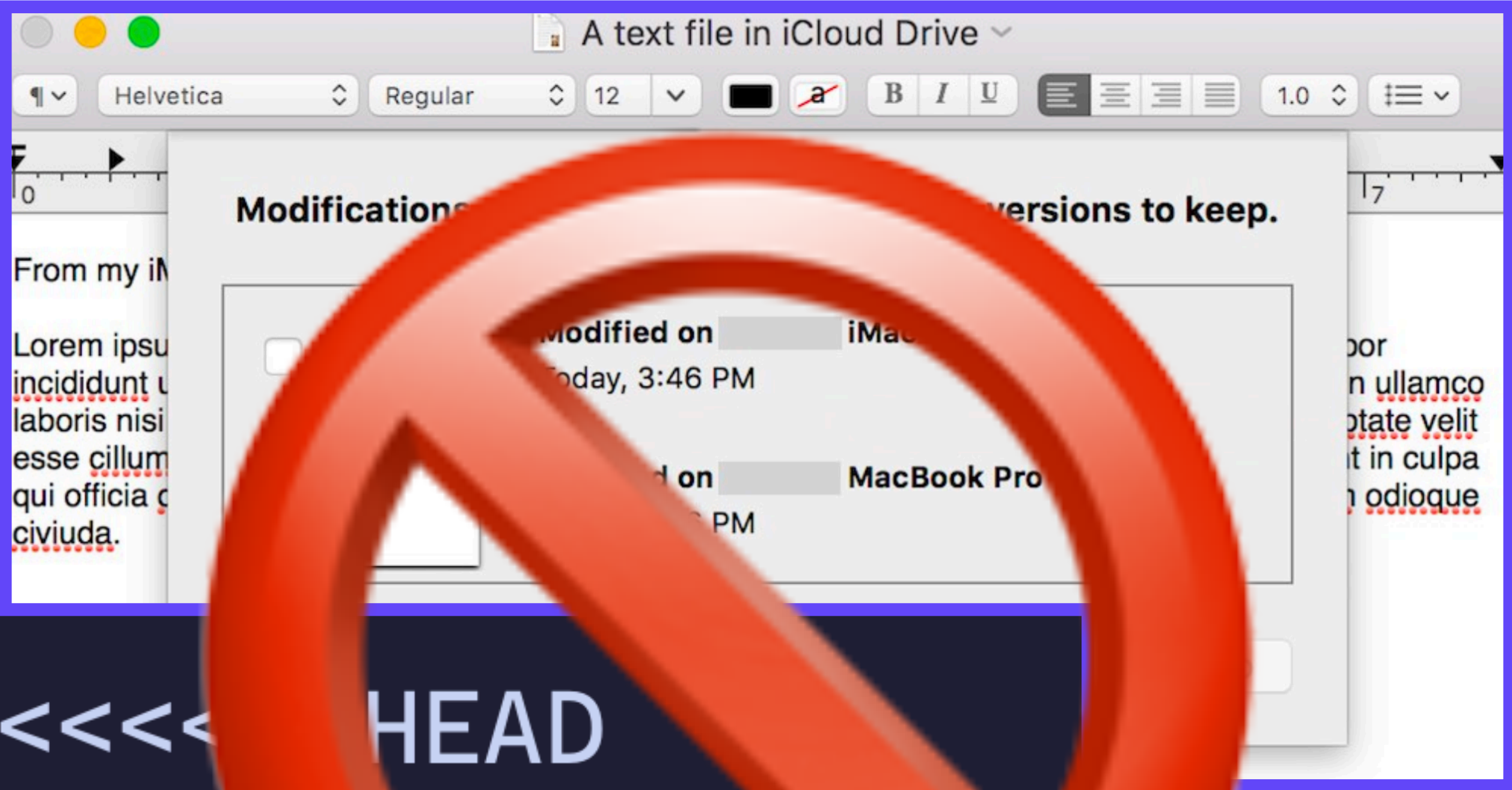
Automatic Merges



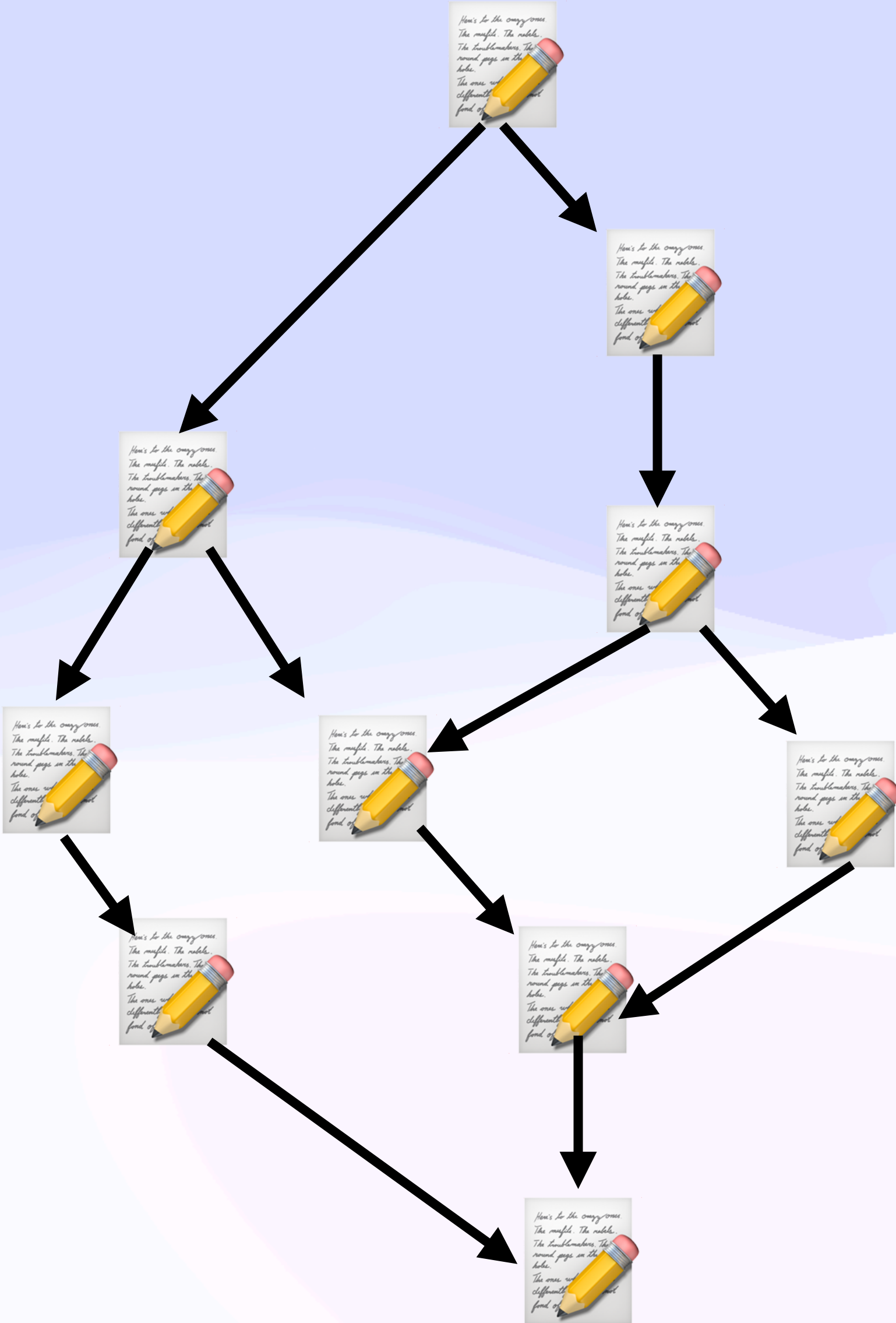
```
<<<<<< HEAD
Option
=====
Option B
>>>>>> some-branch
```


A Local-First Primer

Automatic Merges

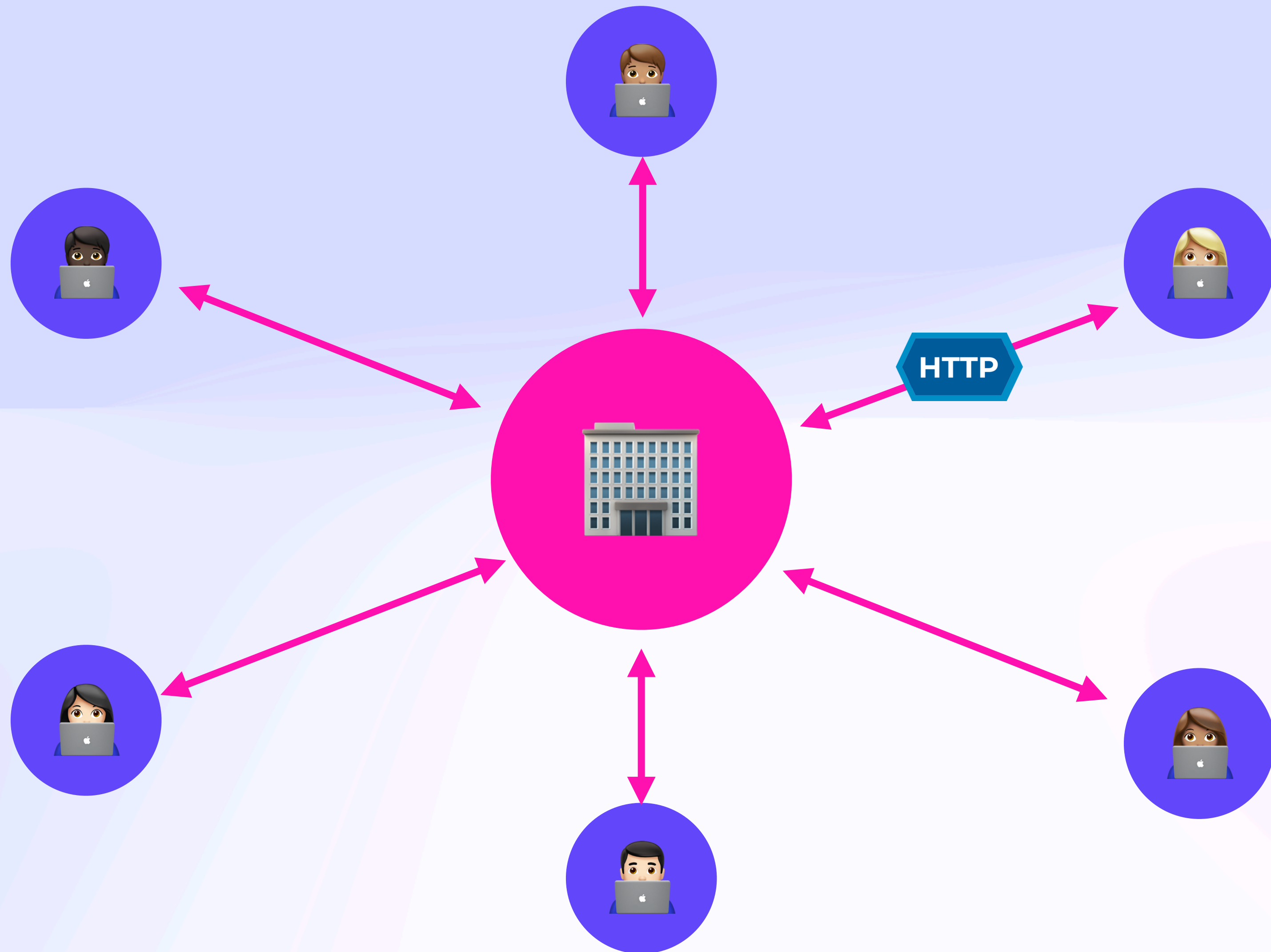


<<<<<<< HEAD
Option
=====
Option B
>>>>>>> some-branch



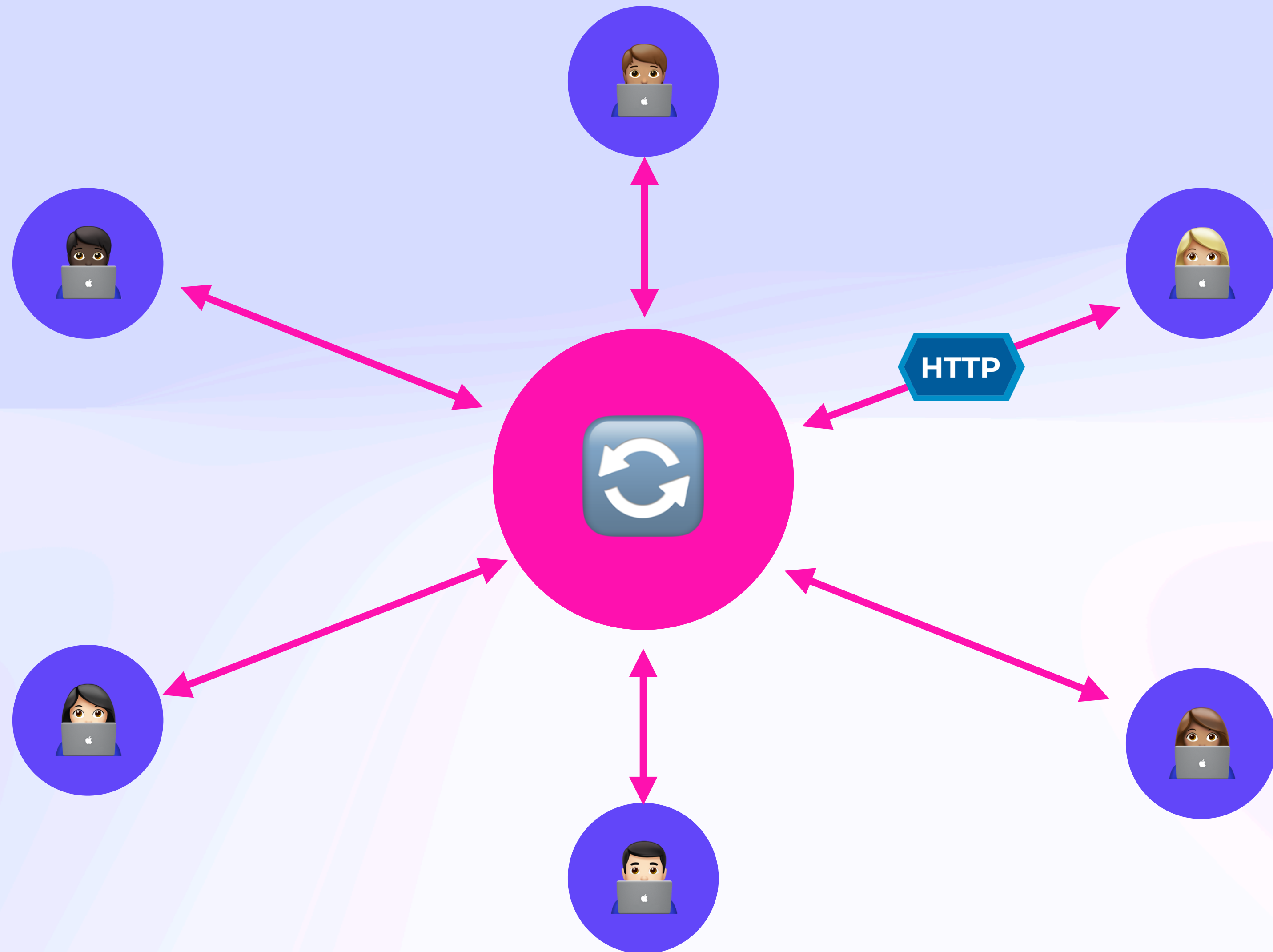
A Local-First Primer

What If Hosting Wasn't A Problem?



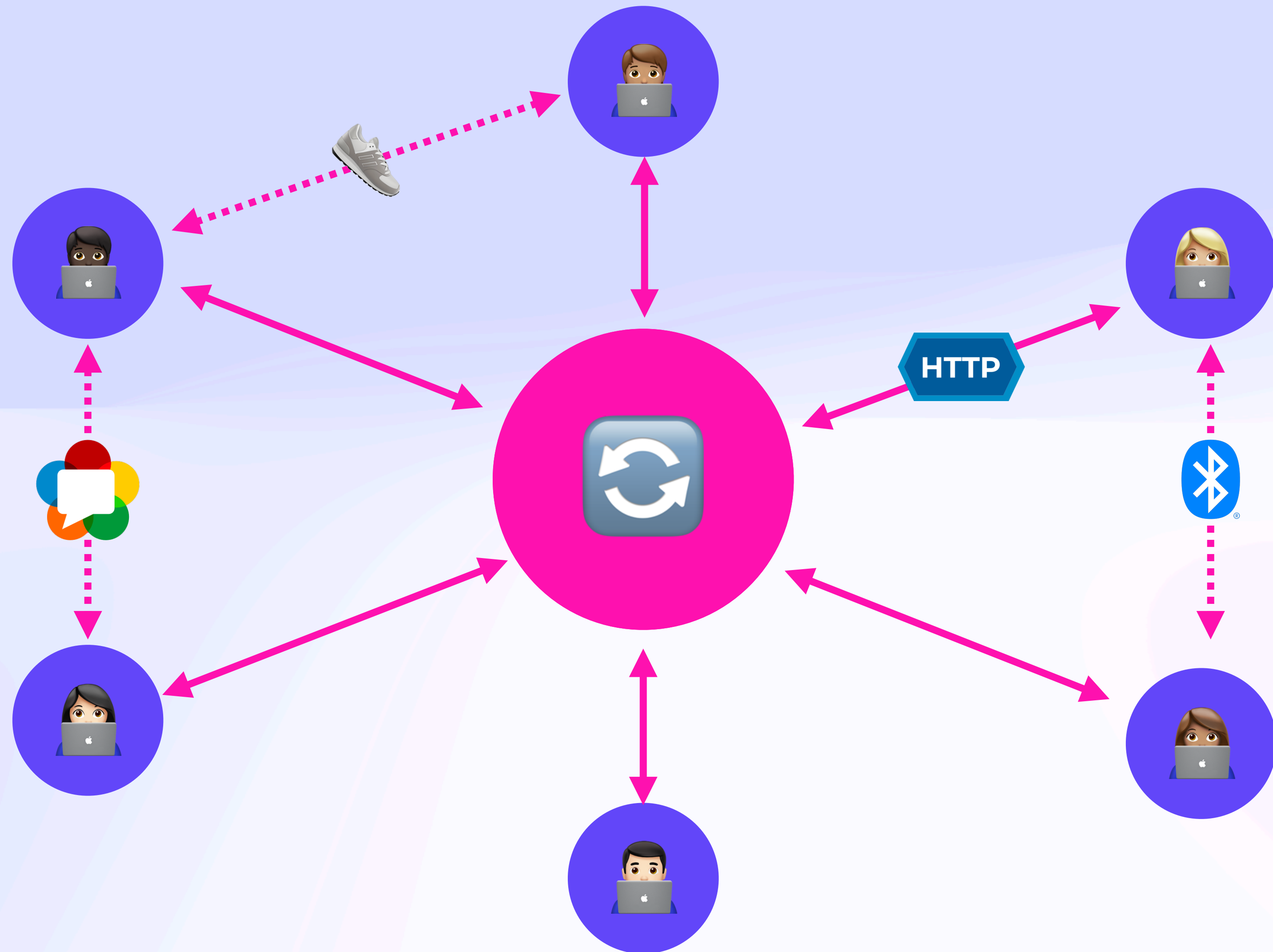
A Local-First Primer

What If Hosting Wasn't A Problem?



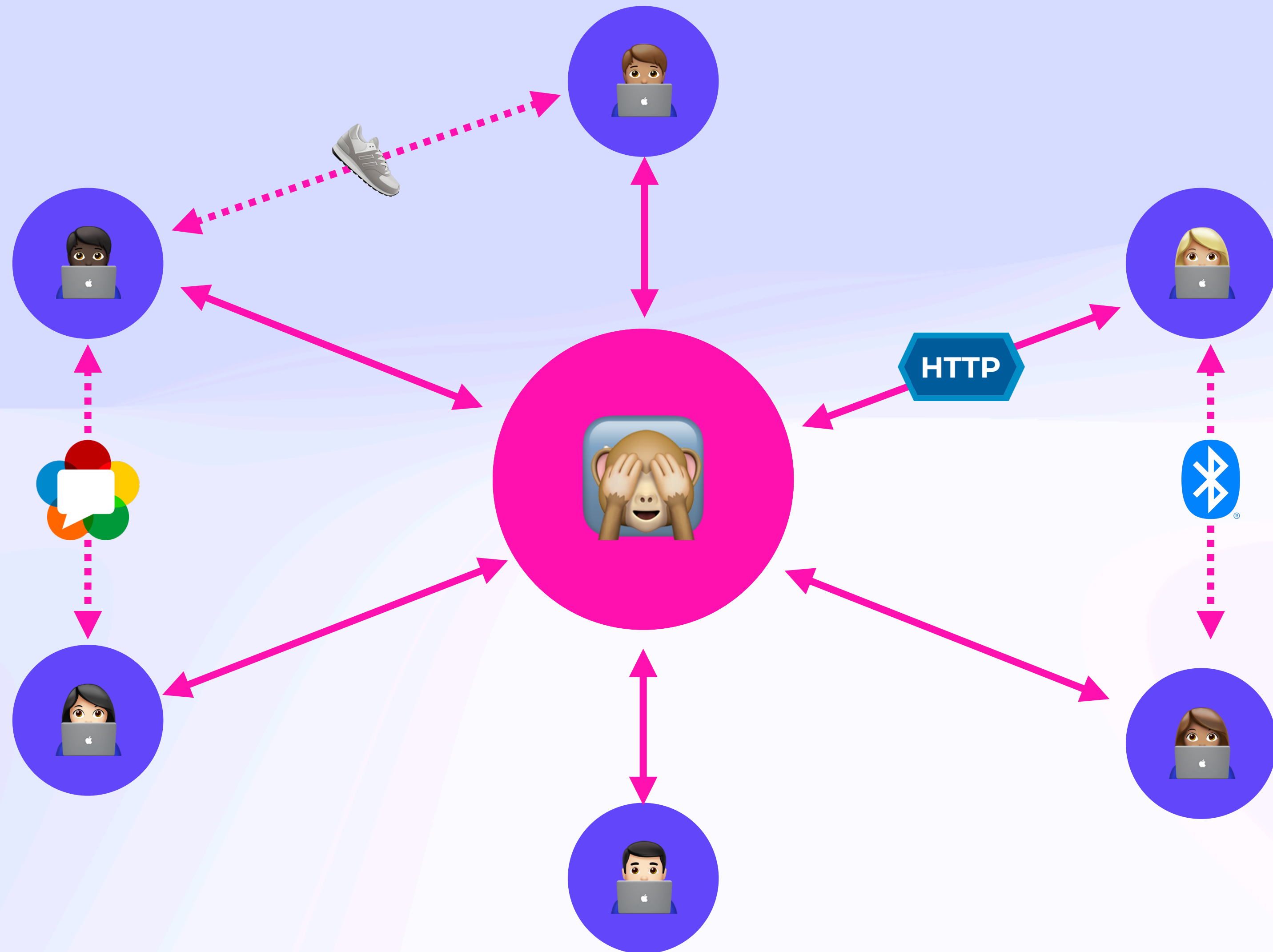
A Local-First Primer

What If Hosting Wasn't A Problem?

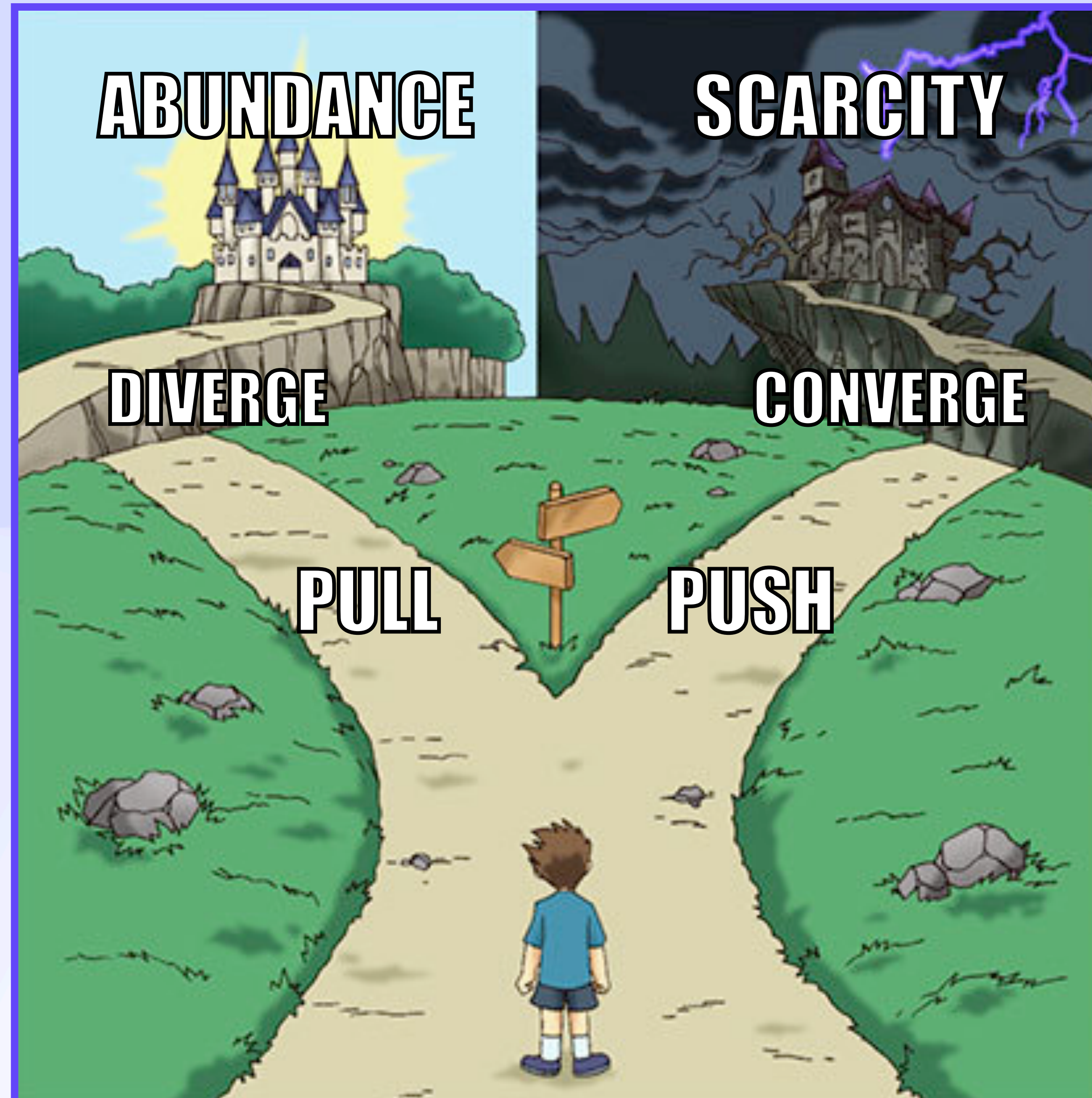


A Local-First Primer

What If Hosting Wasn't A Problem?



A Local-First Primer



Why an Auth Layer?

"Key" Motivation



"Key" Motivation

The background of the slide features a series of smooth, flowing, wavy lines that create a sense of movement and depth. The colors are soft and pastel, ranging from light blues and purples to pale pinks and whites. The lines appear to flow from the left side towards the right, with some areas being more saturated than others, creating a layered, ethereal effect.

"Key" Motivation

What if  Signal ...

"Key" Motivation

What if  Signal ...
but for ***collaboration?***

"Key" Motivation ***Human Factors***



"Key" Motivation

Human Factors

Familiar user experience 🤗

Live collaboration speed 🏎️

Interchangeable sync servers 🔁

Automatic (no manual merges) 🤖

"Key" Motivation

Human Factors

How much can you trust
a random sync server?

Familiar user experience 🤗

Live collaboration speed 🏎️

Interchangeable sync servers 🔀

Automatic (no manual merges) 🤖

"Key" Motivation

How Close to Wikipedia Scale?

"Key" Motivation

How Close to Wikipedia Scale?

100,000s interlinked docs 

10,000s readers 

1,000s writers 

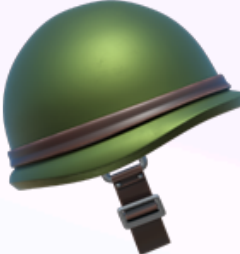
100s admins 

"Key" Motivation

~~**Paranoia Level**~~ **"Informal Threat Model"**

"Key" Motivation

~~Paranoia Level~~ **"Informal Threat Model"**

Secure against the **FBI** 
...but not the **NSA**  

Confidential journalistic sources
Corporate documents / secrets
Personal planning / family finances
Because of CALM, we can have PCS, but only weak FS

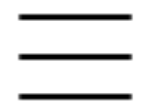
"Key" Motivation

Encryption is Not Enough

"Key" Motivation

Encryption is Not Enough

A



The Atlantic

Sign In

Subscribe

The Trump Administration Accidentally Texted Me Its War Plans

U.S. national-security leaders included me in a group chat about upcoming military strikes in Yemen. I didn't think it could be real. Then the bombs started falling.

By Jeffrey Goldberg

"Key" Motivation

"Boring is Good, Actually"

"Key" Motivation

"Boring is Good, Actually"

Manage access

Create teamAdd peopleAdd teams

Direct accessOrganization access

Select all

role:admin

Type

Role

alexjg

Role: admin

beehive

@inkandswitch/beehive • 3 members

Role: admin

Brooklyn Zelenka

expede

Role: admin

web

@inkandswitch/web • 4 members

Role: admin

Add people, groups, and calendar events

People with access

hello@katiewilde.com

Owner

Brooklyn Zelenka (you)

Editor

General access

Restricted

Only people with access can open with the link

Copy link

Done

"Key" Motivation

"Boring is Good, Actually"

Manage access

Create teamAdd peopleAdd teams

Direct accessOrganization access

Select all

role:admin

TypeRole

alexjg

Role: admin

beehive

@inkandswitch/beehive • 3 members

Role: admin

Brooklyn Zelenka

expede

Role: admin

web

@inkandswitch/web • 4 members

Role: admin

Add people, groups, and calendar events

People with access

hello@katiewilde.com

Owner

Brooklyn Zelenka (you)

Editor

General access

Restricted

Only people with access can open with the link

Copy link

Done

If we do our job well, it'll seem "familiar" and "boring"

"Key" Motivation

Unix Philosophy

"Key" Motivation

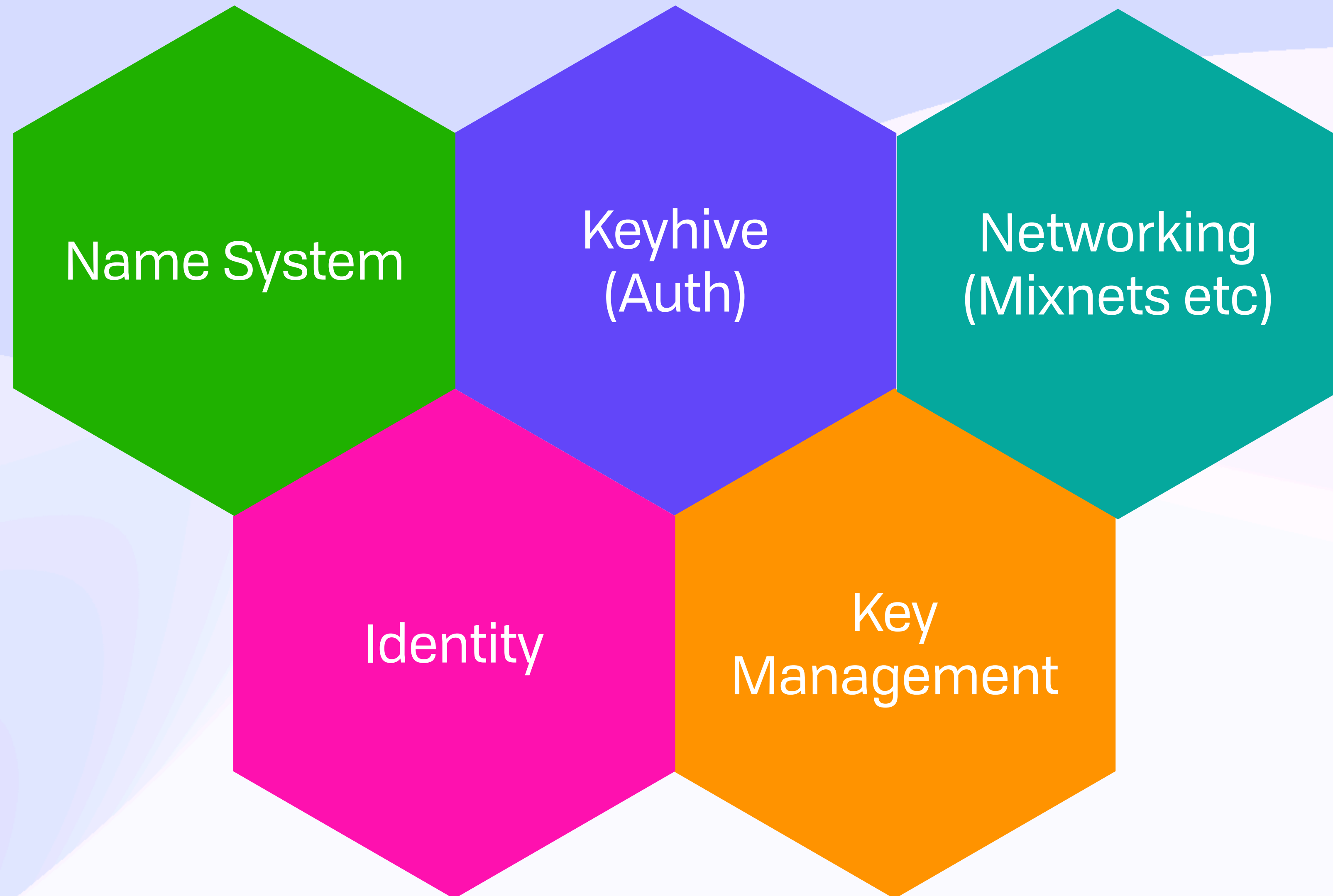
Unix Philosophy



Keyhive
(Auth)

"Key" Motivation

Unix Philosophy



Auth-as-Place

Cloud Auth

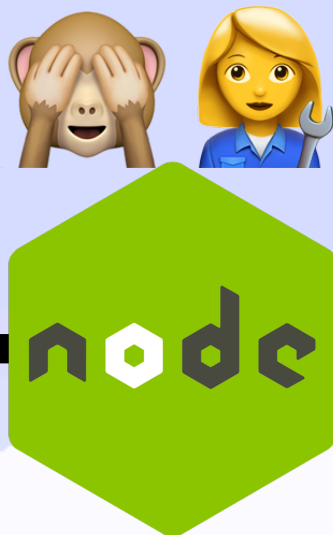


Auth-as-Place

Cloud Auth Flow ☁️

Auth-as-Place

Cloud Auth Flow ☁



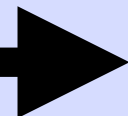
Auth-as-Place

Cloud Auth Flow ☁️



Auth-as-Place

Cloud Auth Flow ☁️



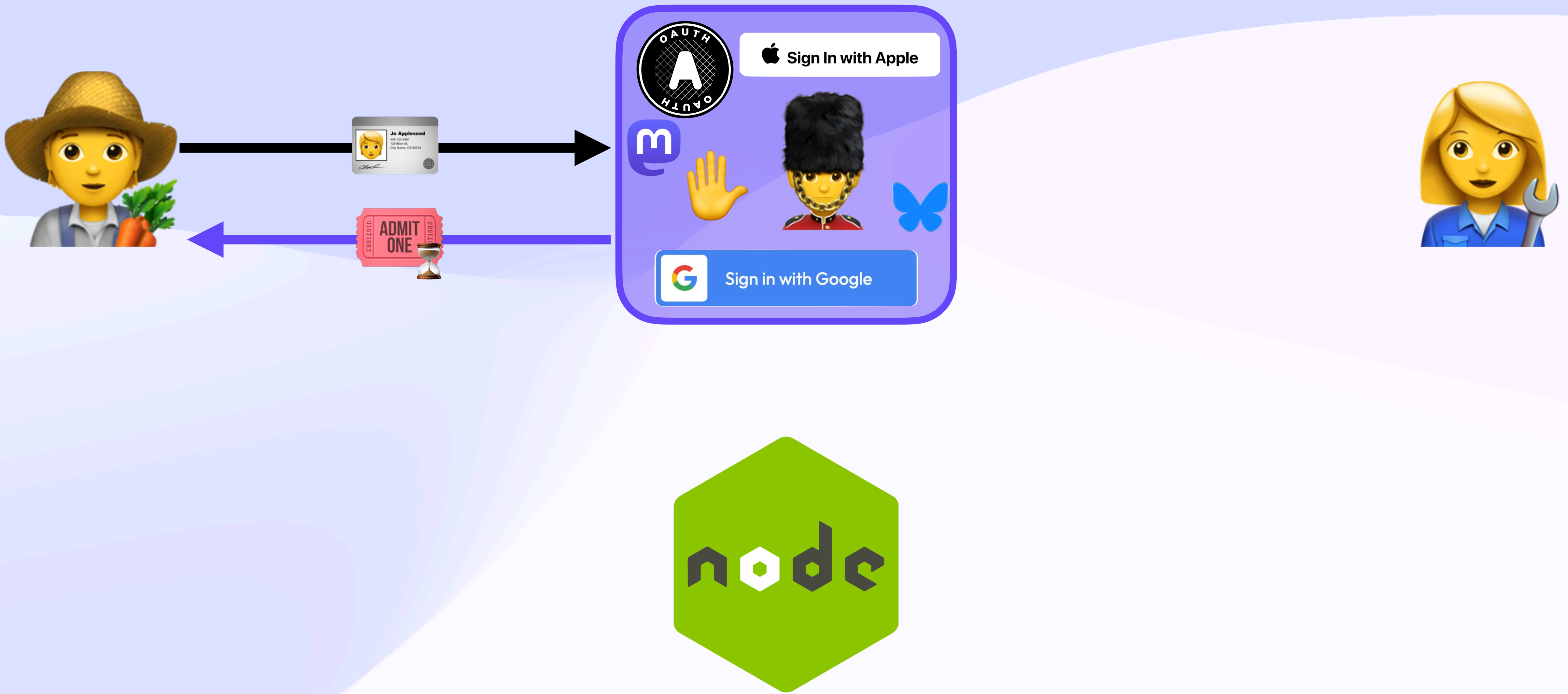
Auth-as-Place

Cloud Auth Flow ☁️



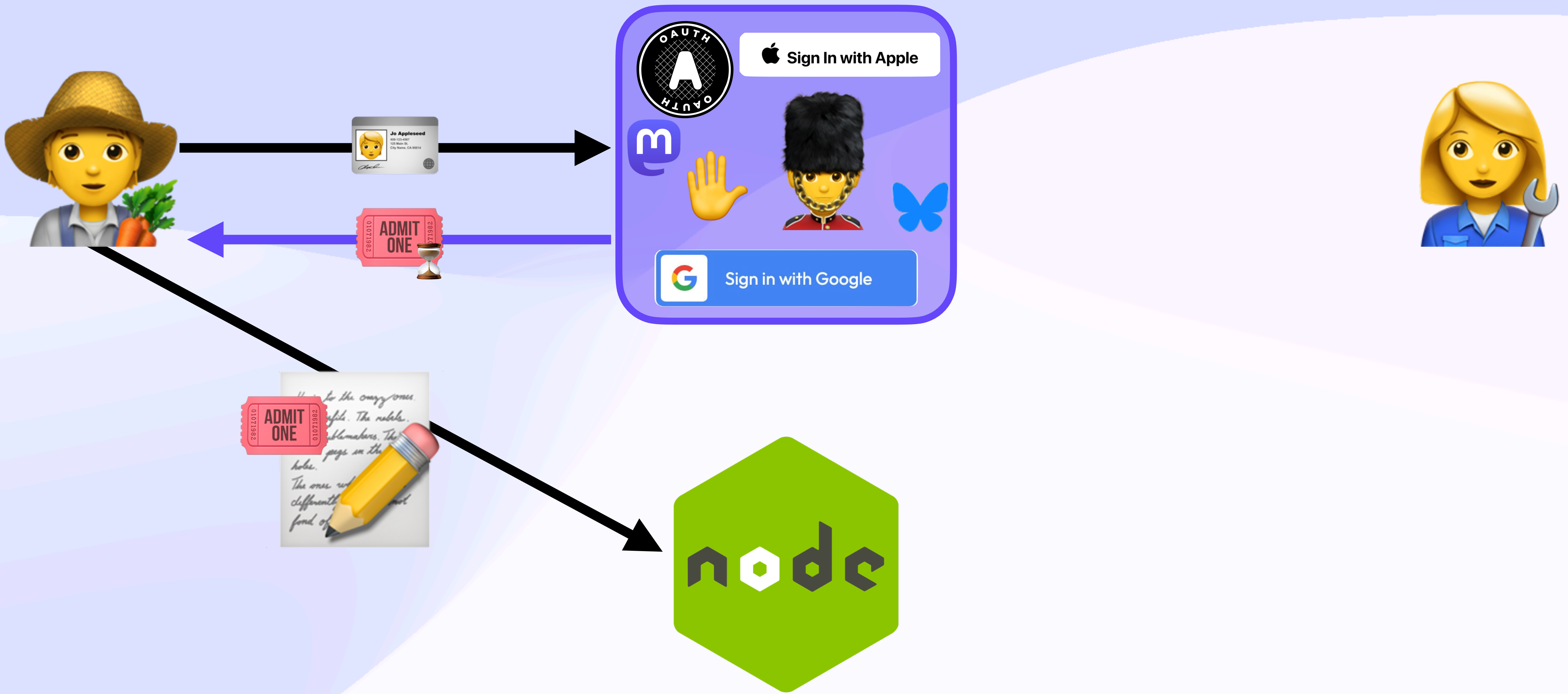
Auth-as-Place

Cloud Auth Flow ☁️



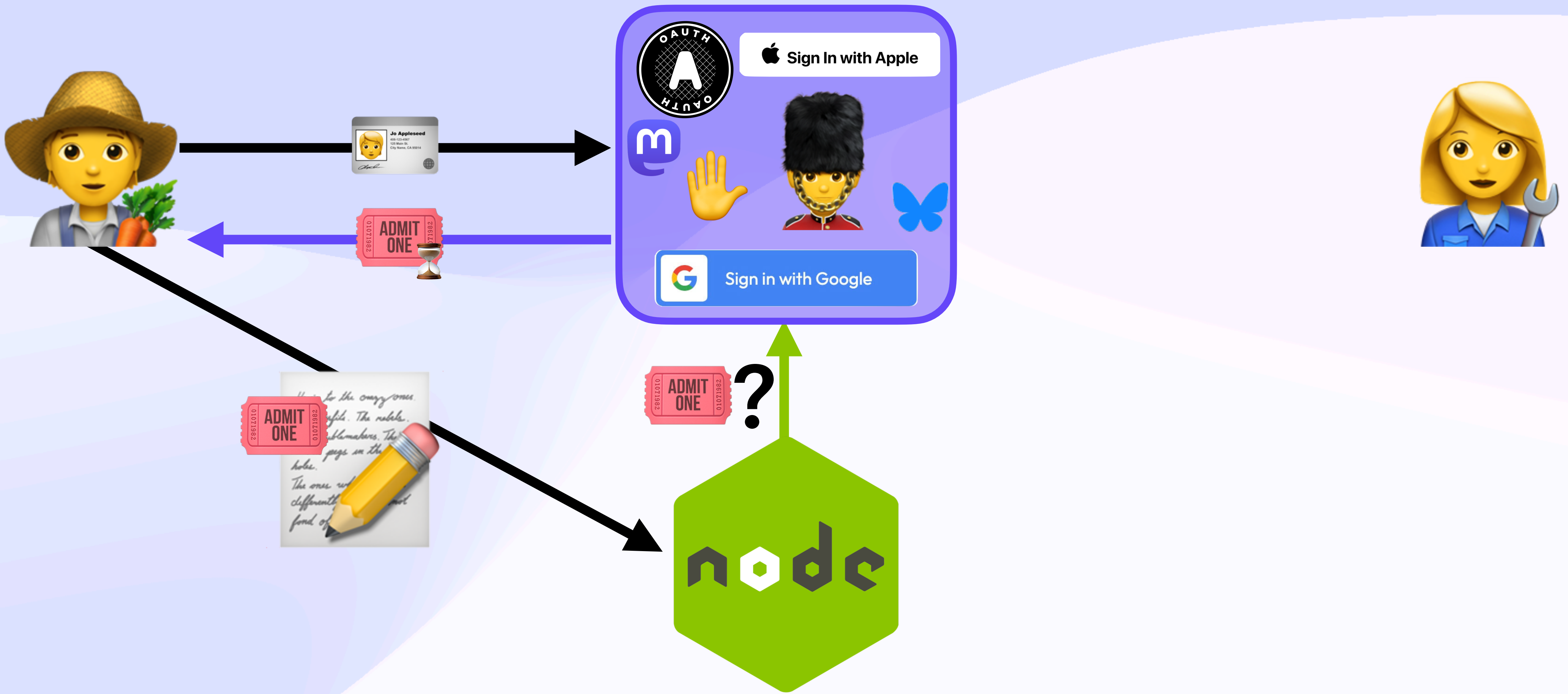
Auth-as-Place

Cloud Auth Flow ☁️



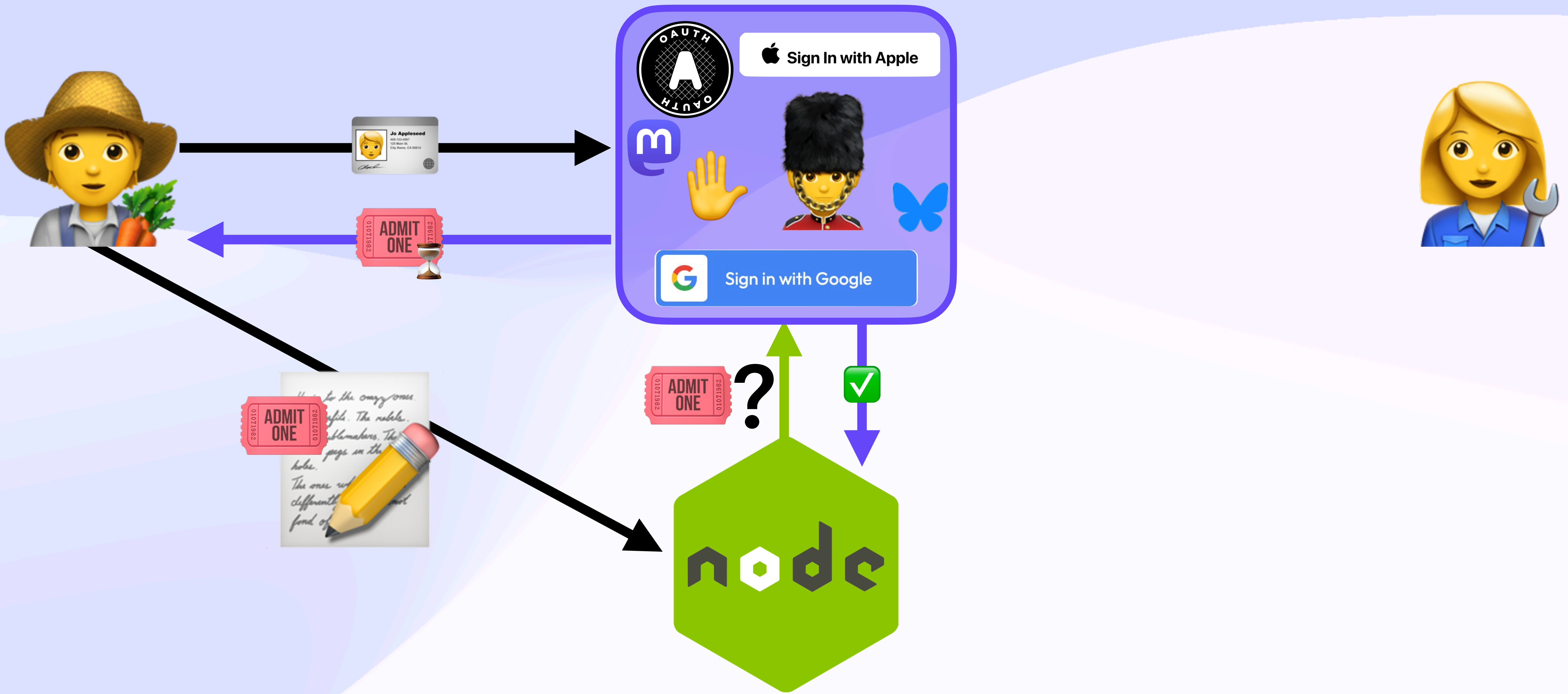
Auth-as-Place

Cloud Auth Flow ☁️



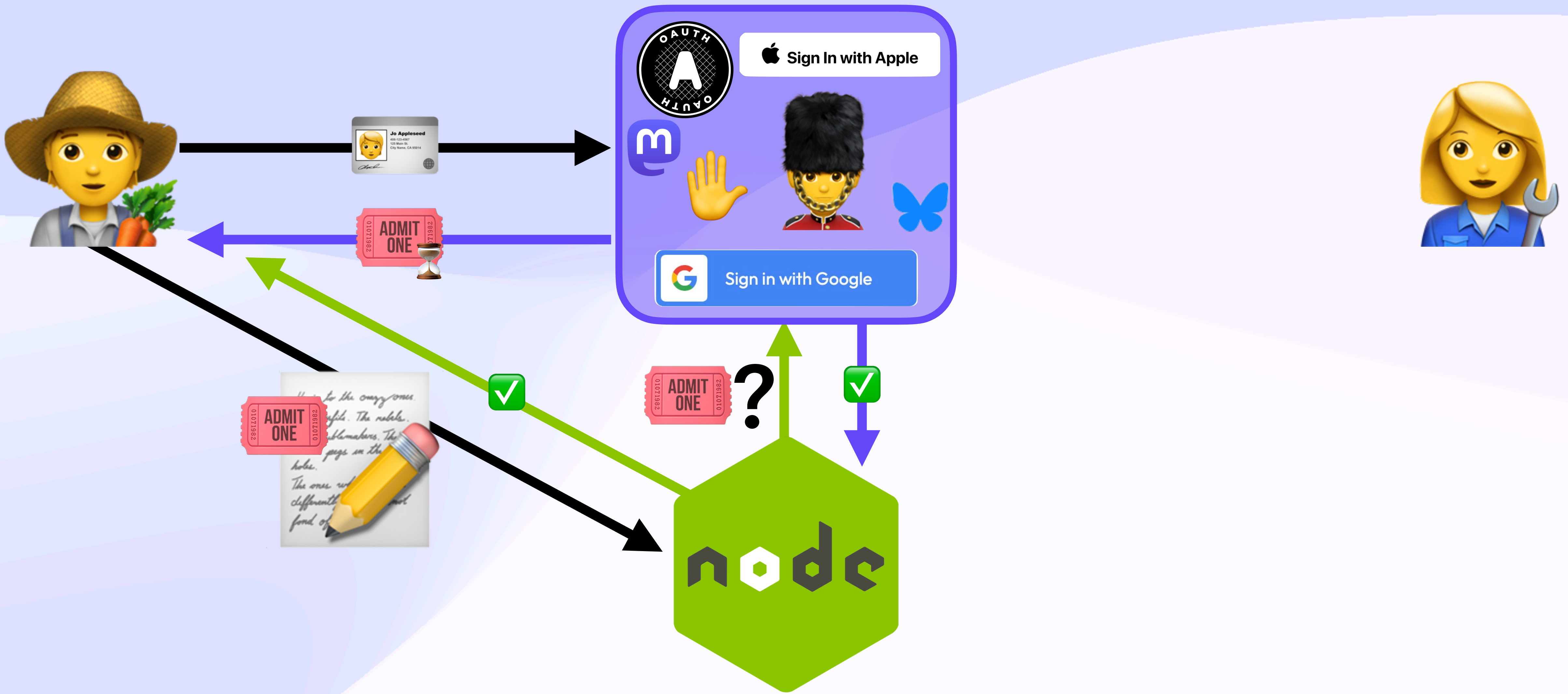
Auth-as-Place

Cloud Auth Flow ☁️



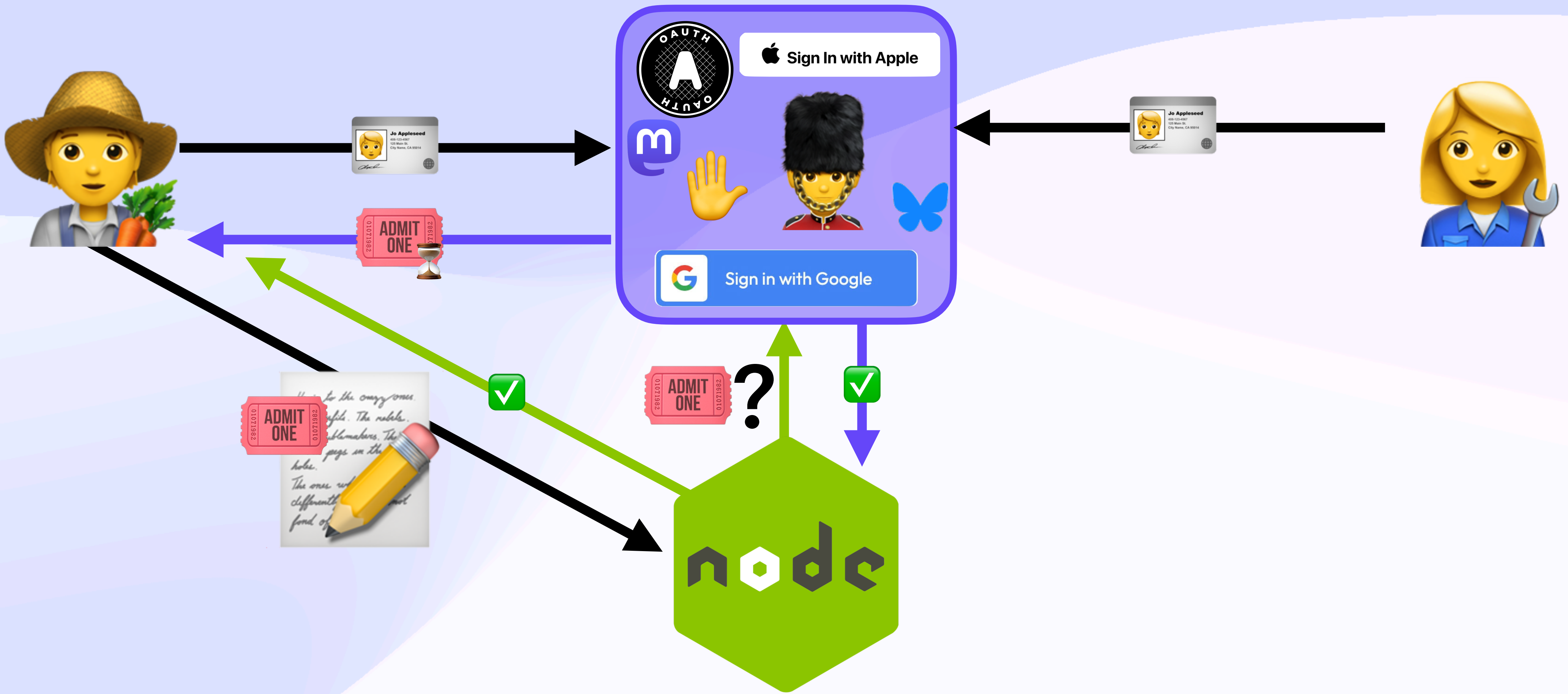
Auth-as-Place

Cloud Auth Flow ☁️



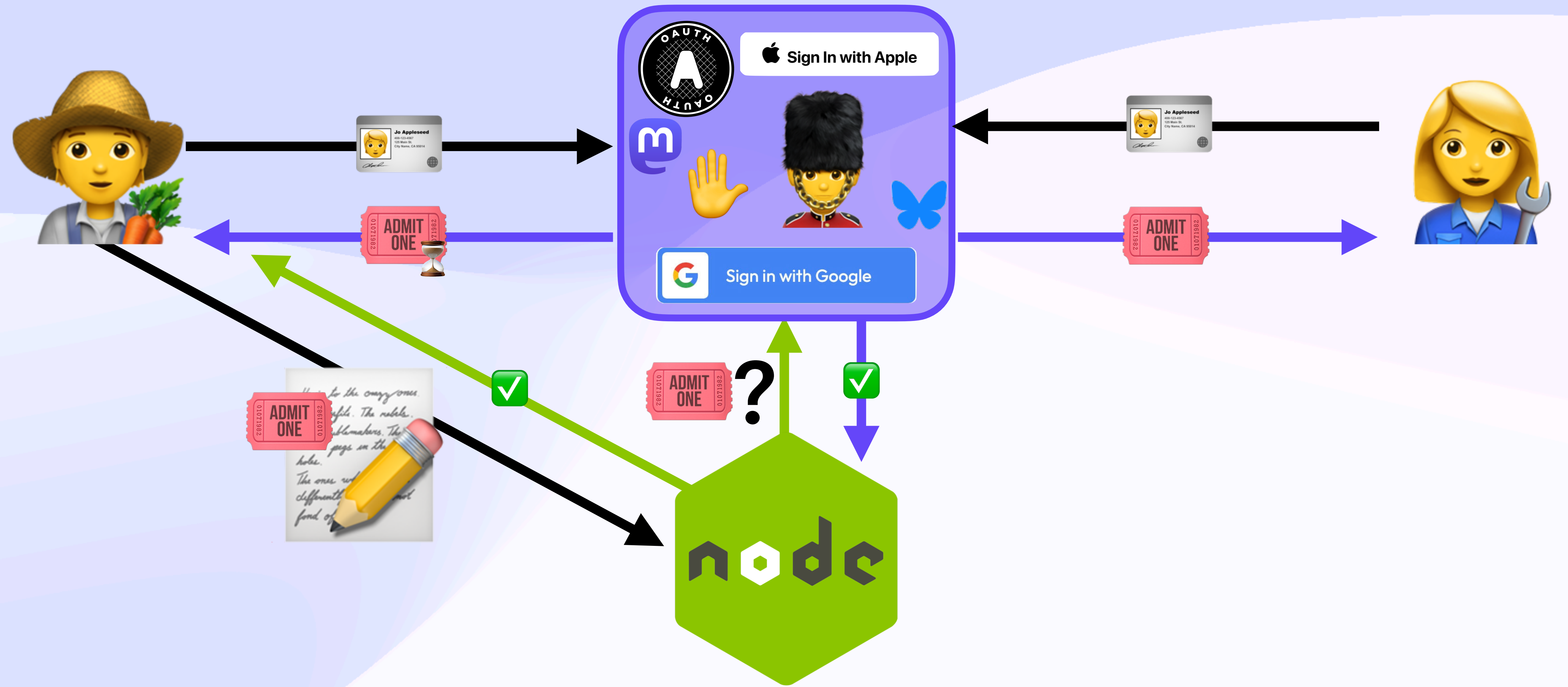
Auth-as-Place

Cloud Auth Flow ☁️



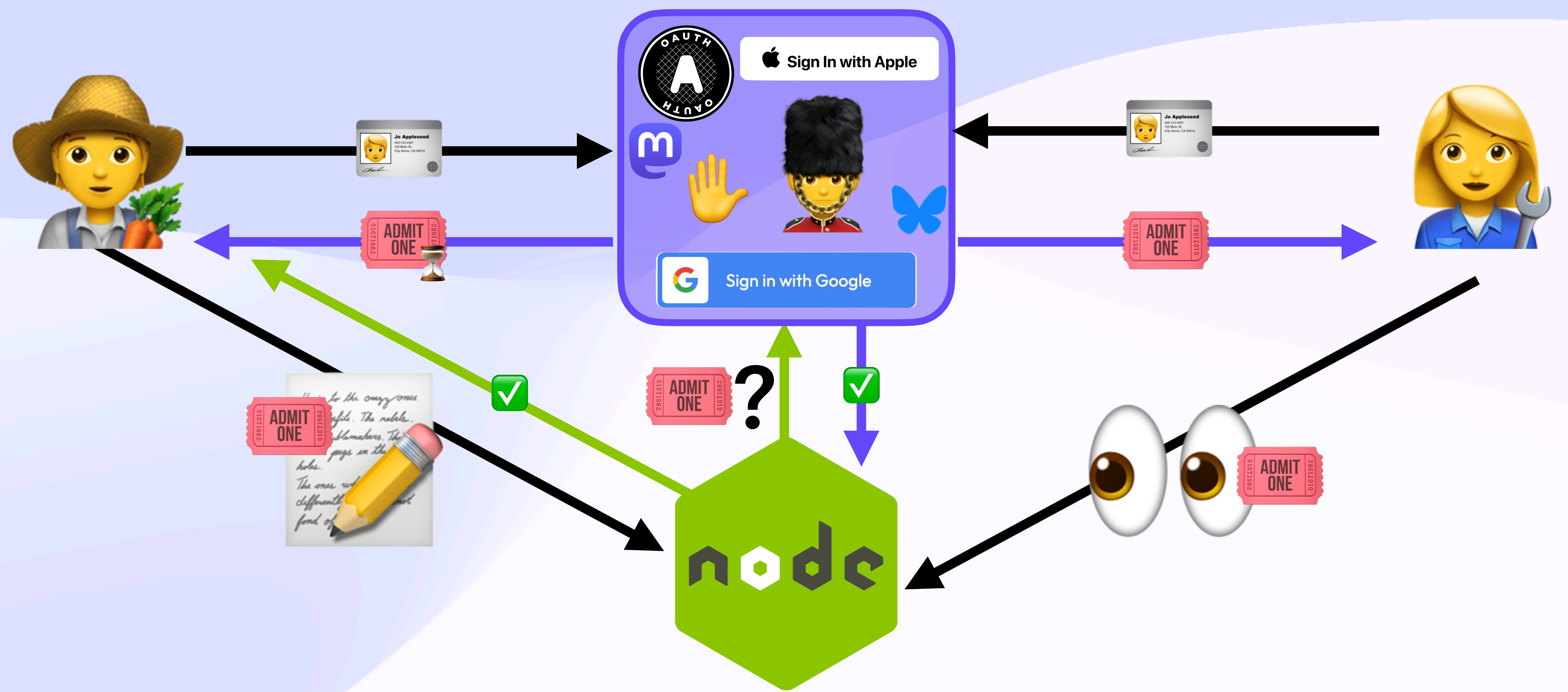
Auth-as-Place

Cloud Auth Flow ☁️



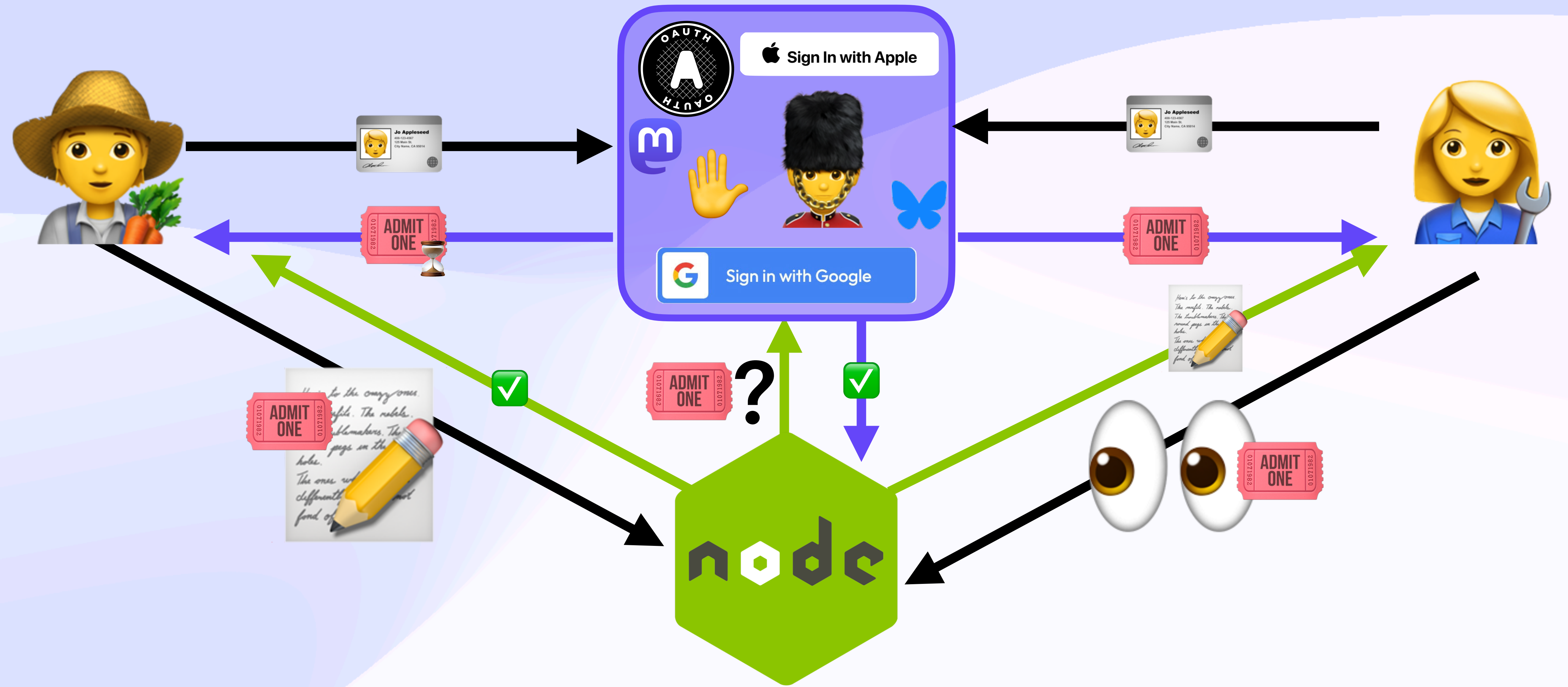
Auth-as-Place

Cloud Auth Flow ☁️



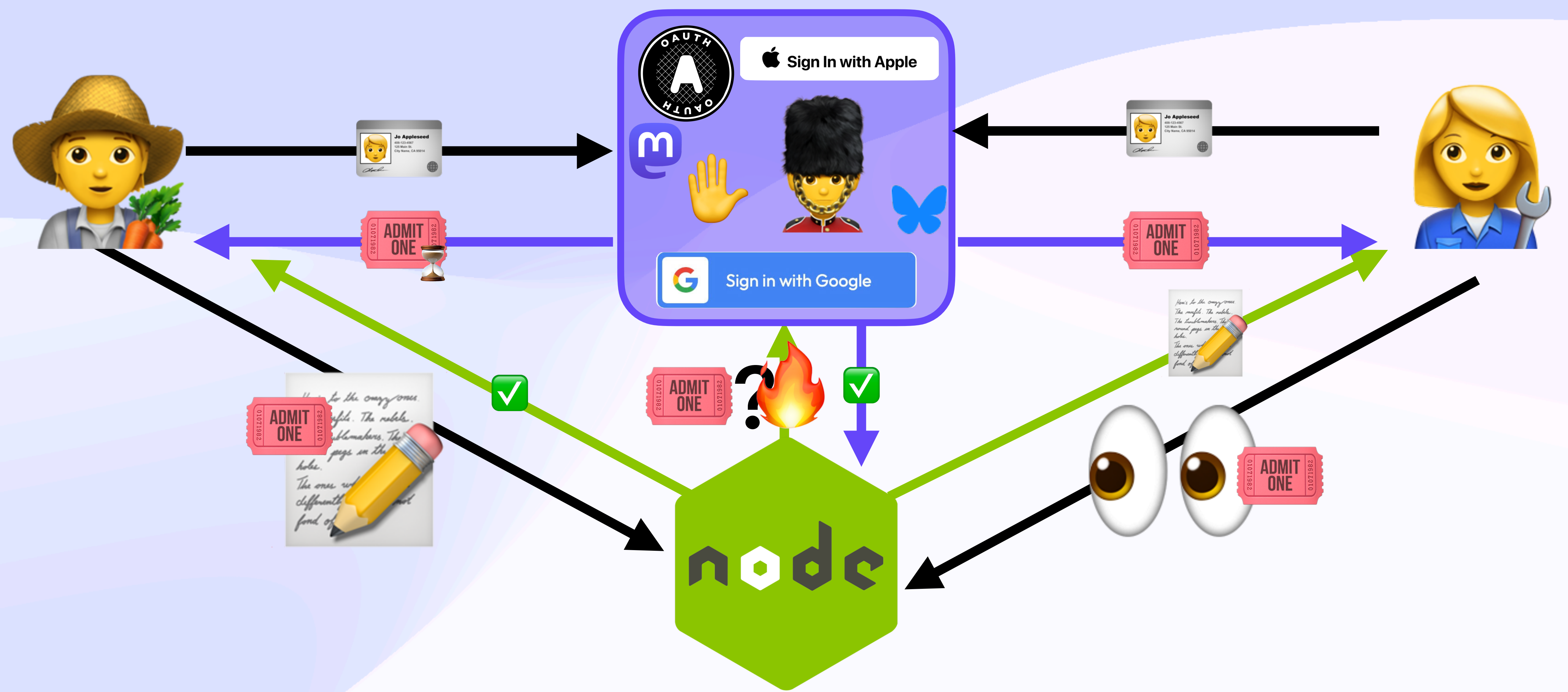
Auth-as-Place

Cloud Auth Flow



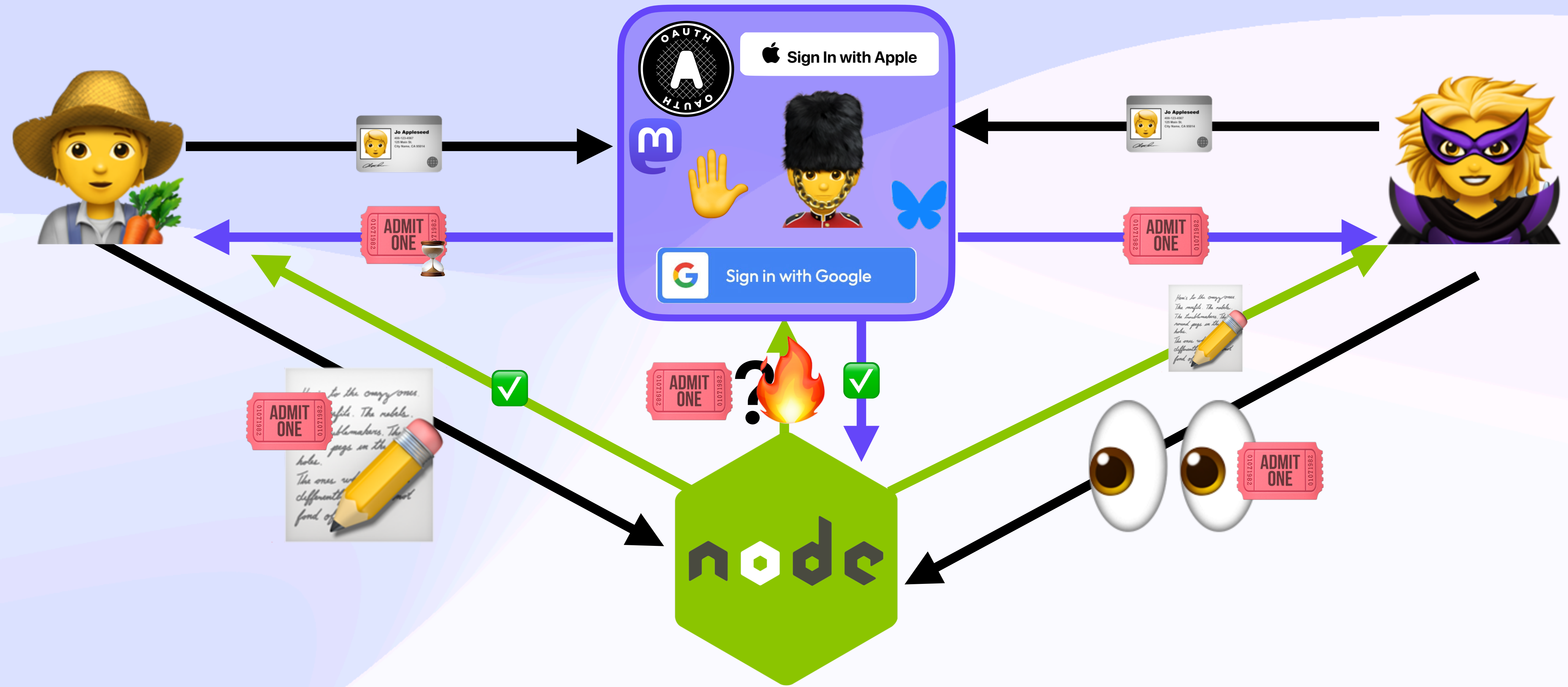
Auth-as-Place

Cloud Auth Flow ☁



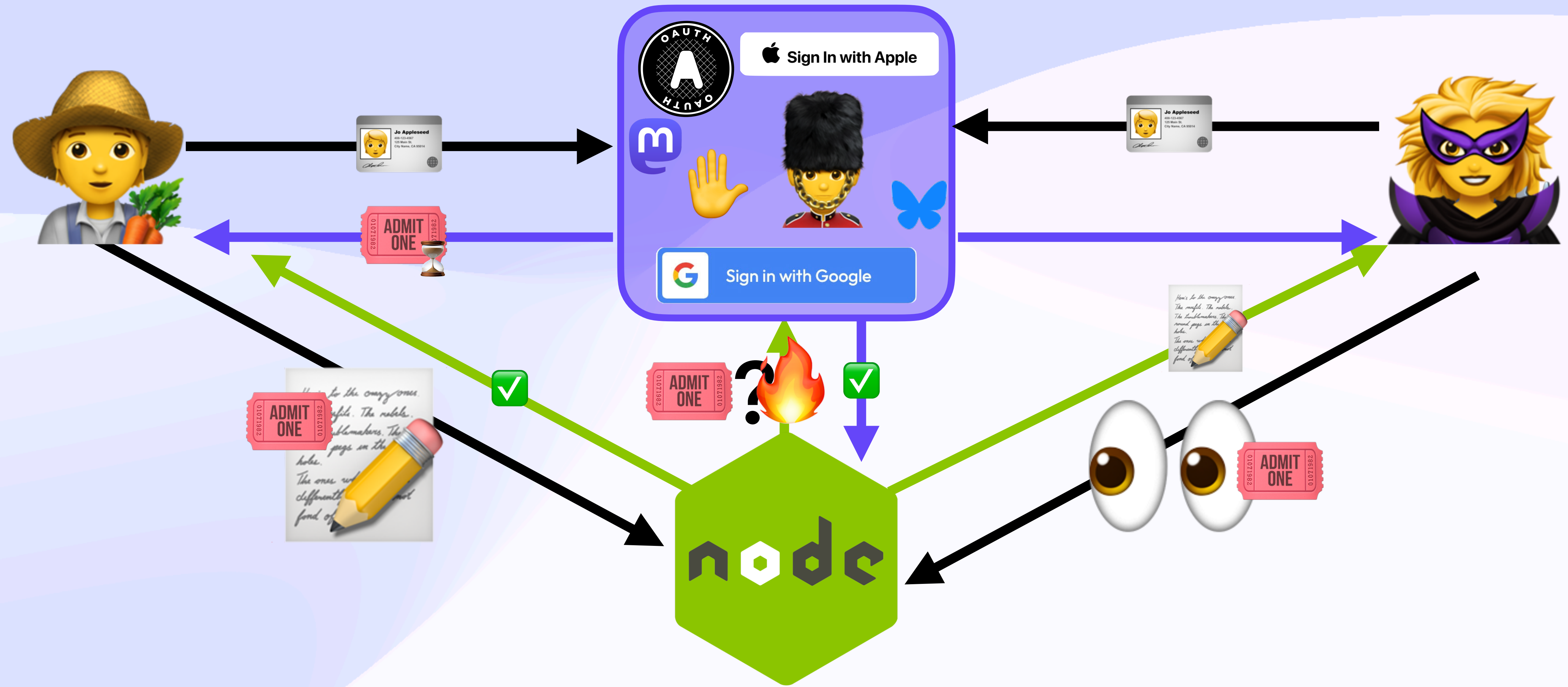
Auth-as-Place

Cloud Auth Flow



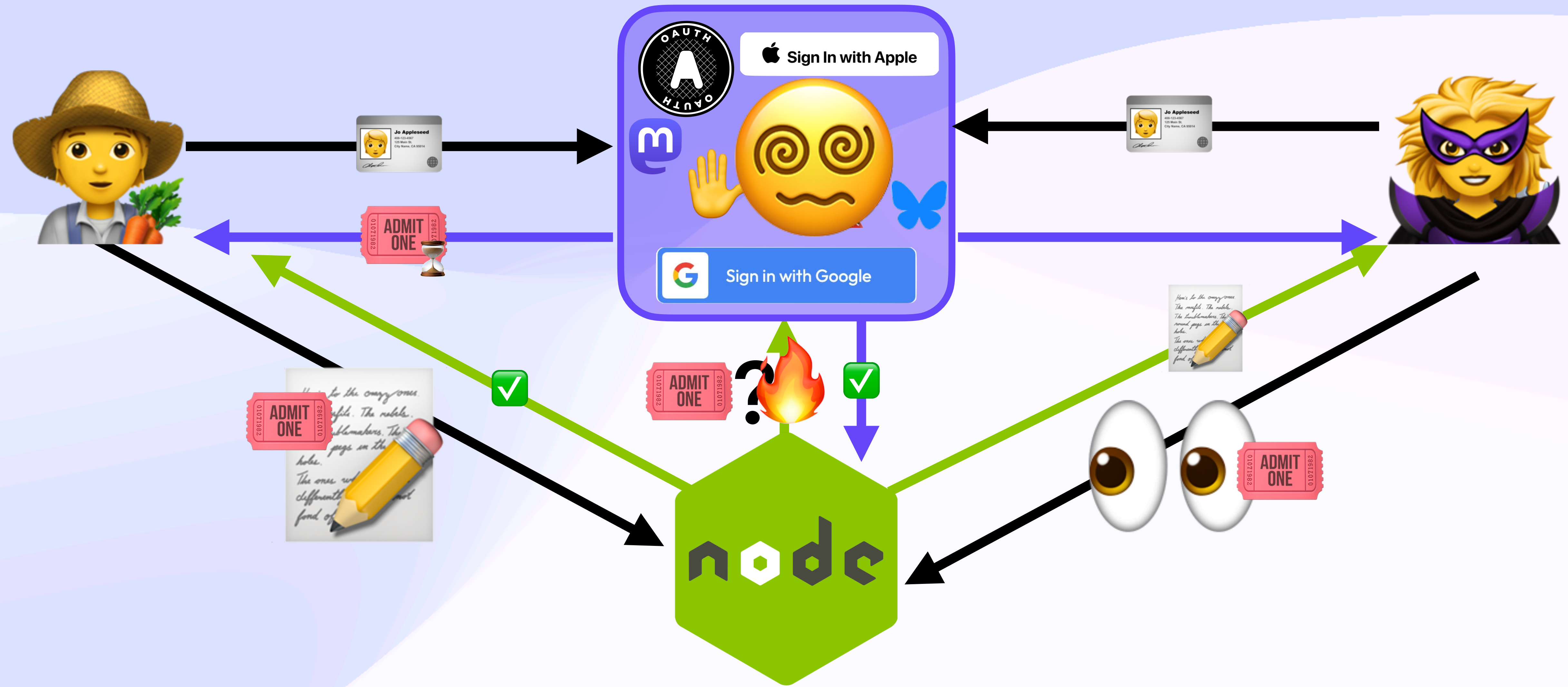
Auth-as-Place

Cloud Auth Flow



Auth-as-Place

Cloud Auth Flow ☁️



Auth-as-Place

Cloud: Auth-as-Place ☁️

Auth-as-Place

Cloud: Auth-as-Place ☁️



Auth-as-Place

Cloud: Auth-as-Place ☁️

"Over Here"



"Over There"



Auth-as-Place

Cloud: Auth-as-Place ☁️

"Over Here"



"Over There"



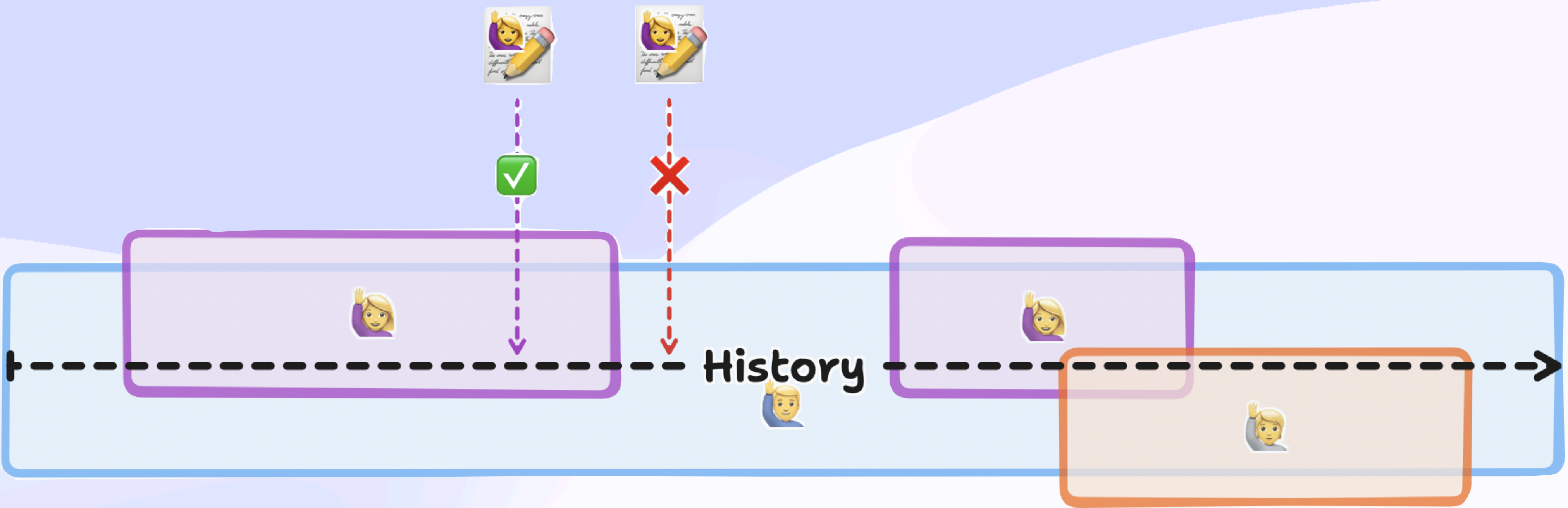
"Over there" is a bottleneck / hard to scale

Playing By New Rules 🎯

Local Context

Local Context

Adds & Removals Over Time



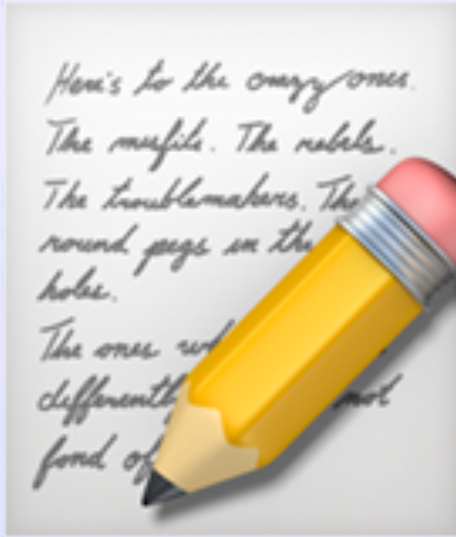
Local Context

Auth-as-Data: "Auth Must Travel with Data"



Local Context

Auth-as-Data: "Auth Must Travel with Data"



Local Context

Auth-as-Data: "Auth Must Travel with Data"



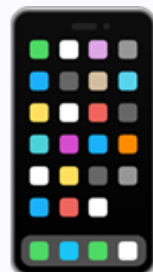
Local Context

Auth-as-Data: "Auth Must Travel with Data"



Local Context

Auth-as-Data: "Auth Must Travel with Data"



Local Context

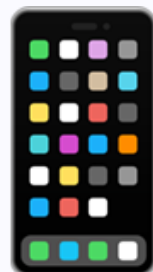
Auth-as-Data: "Auth Must Travel with Data"



"Auth Here"
"Data Here"



"Auth There"
"Data There"



Local Context

Auth-as-Data: "Auth Must Travel with Data"



"Auth Here"
"Data Here"



"Auth There"
"Data There"



Local Context

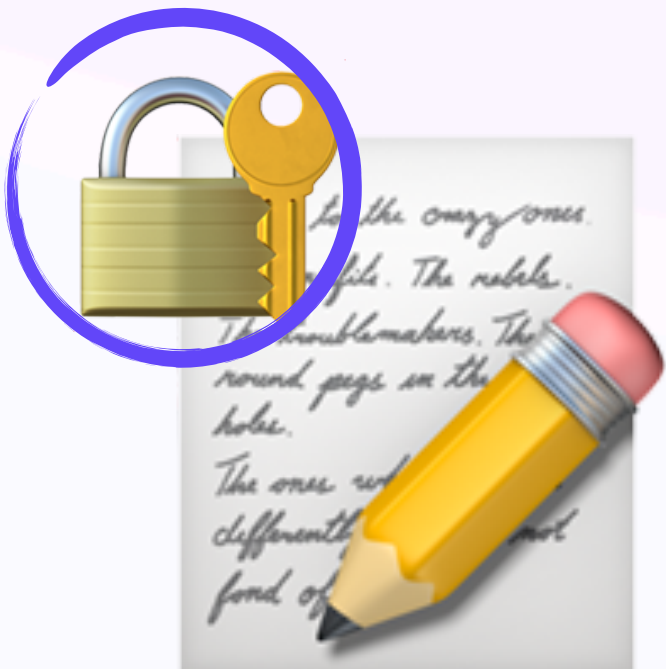
Auth-as-Data: "Auth Must Travel with Data"



"Auth Here"
"Data Here"



"Auth There"
"Data There"



Local Context



Local Context

Cloud

Local-First

Local Context

Cloud

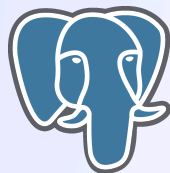
Auth 



Compute 



Data 



Local-First

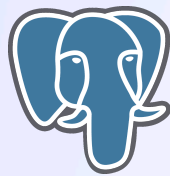
Local Context

Cloud

Auth 

Compute 

Data 



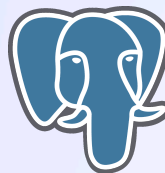
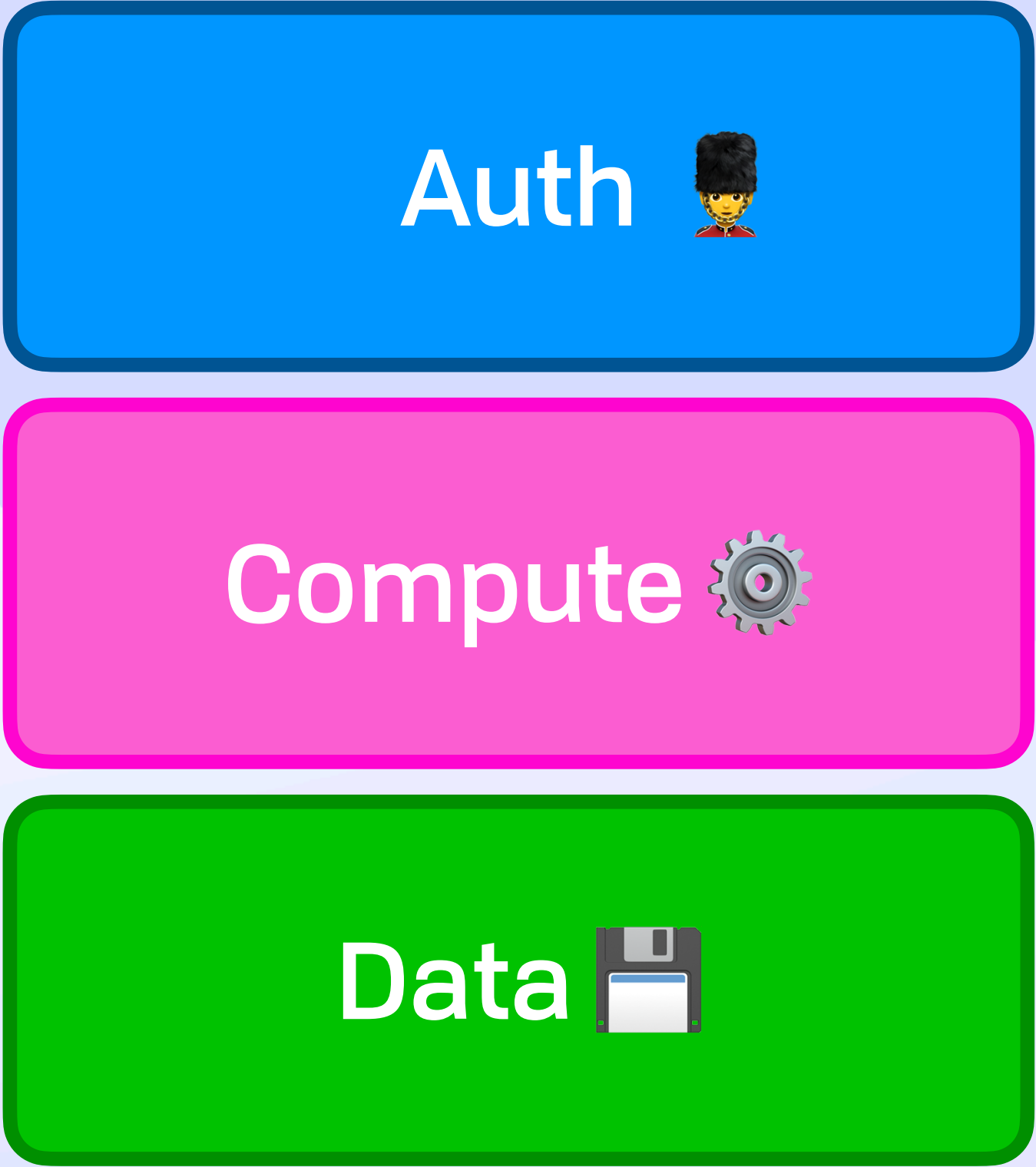
Local-First

Compute 

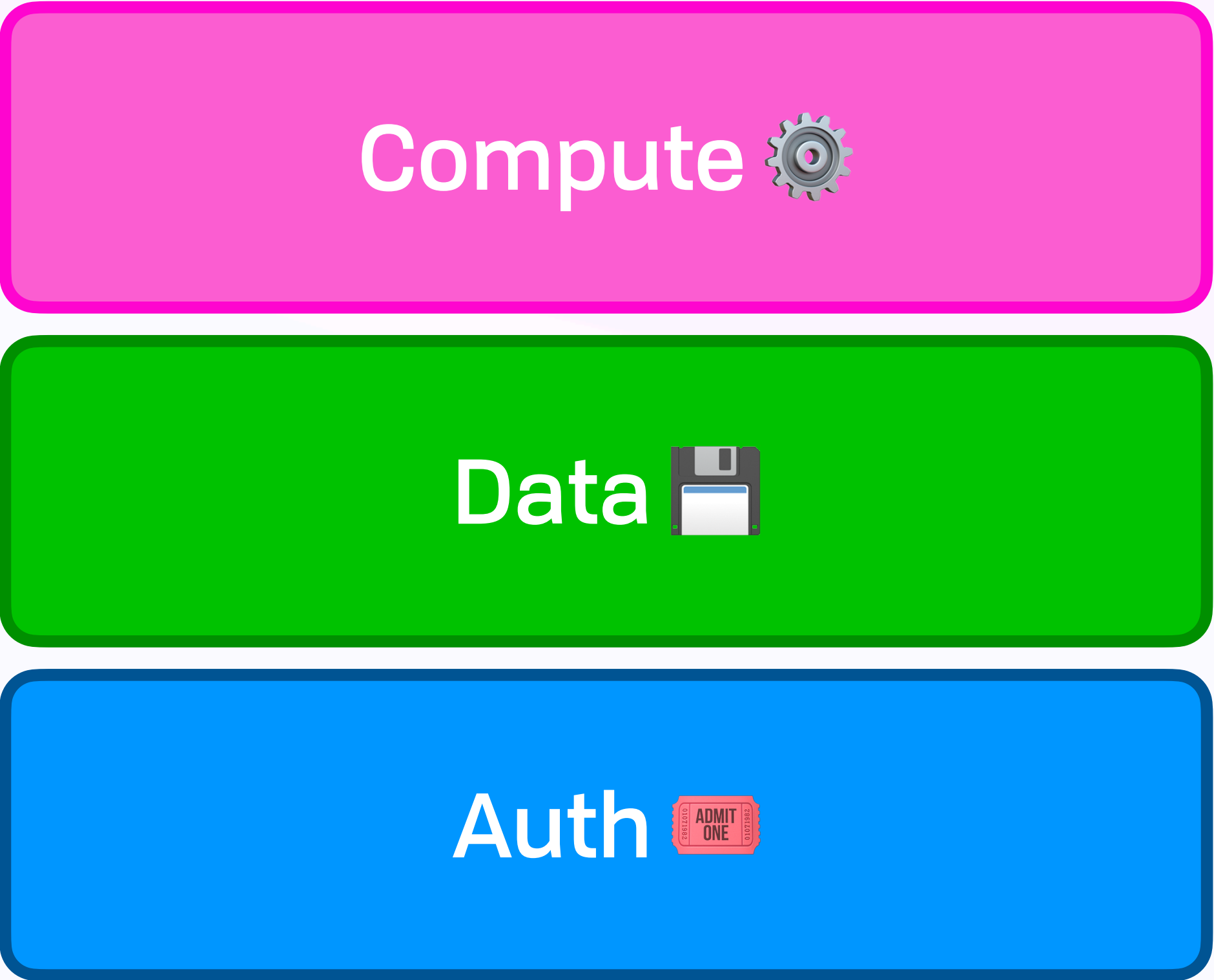
Data 

Local Context

Cloud



Local-First

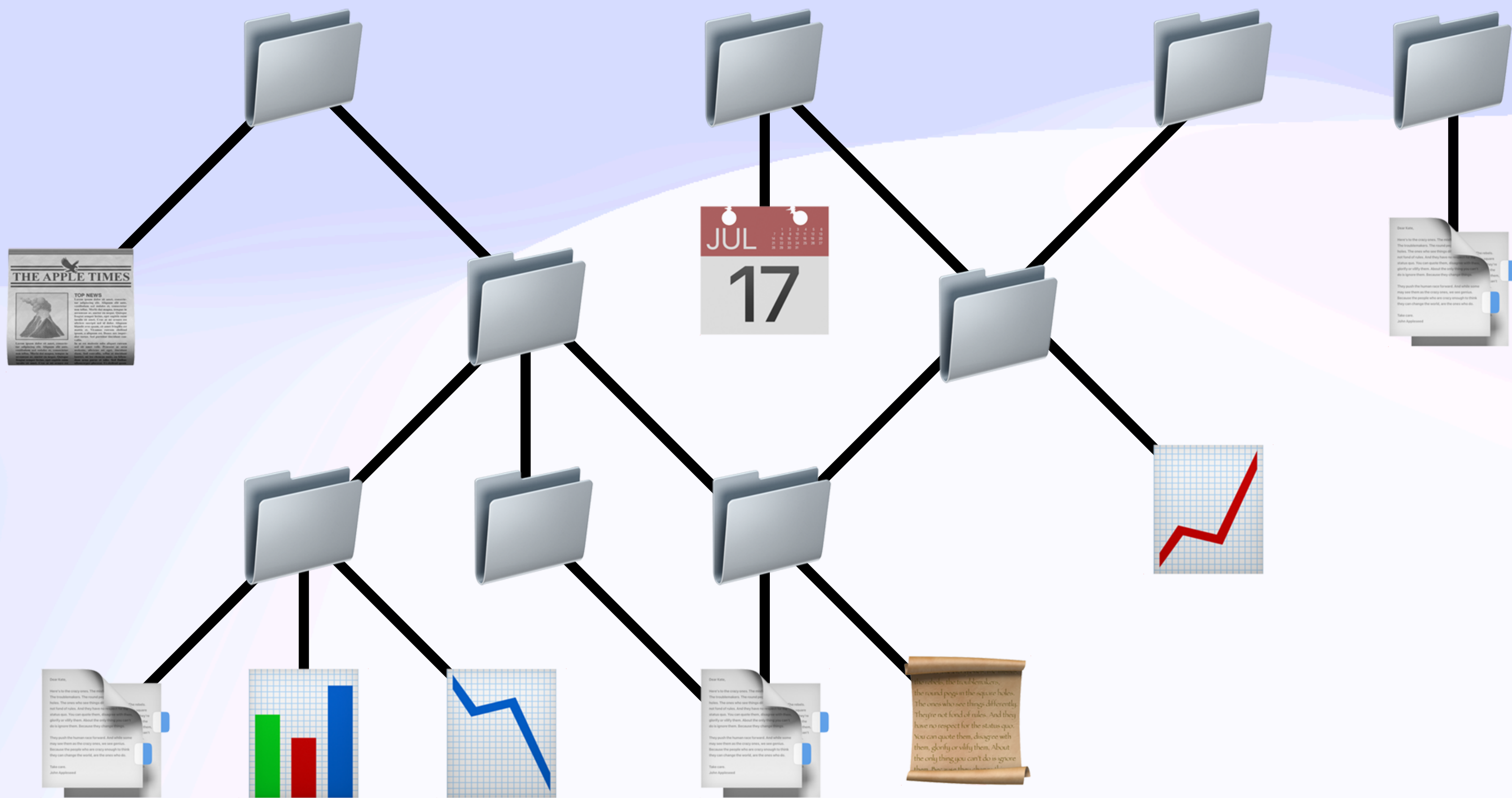


Local Context

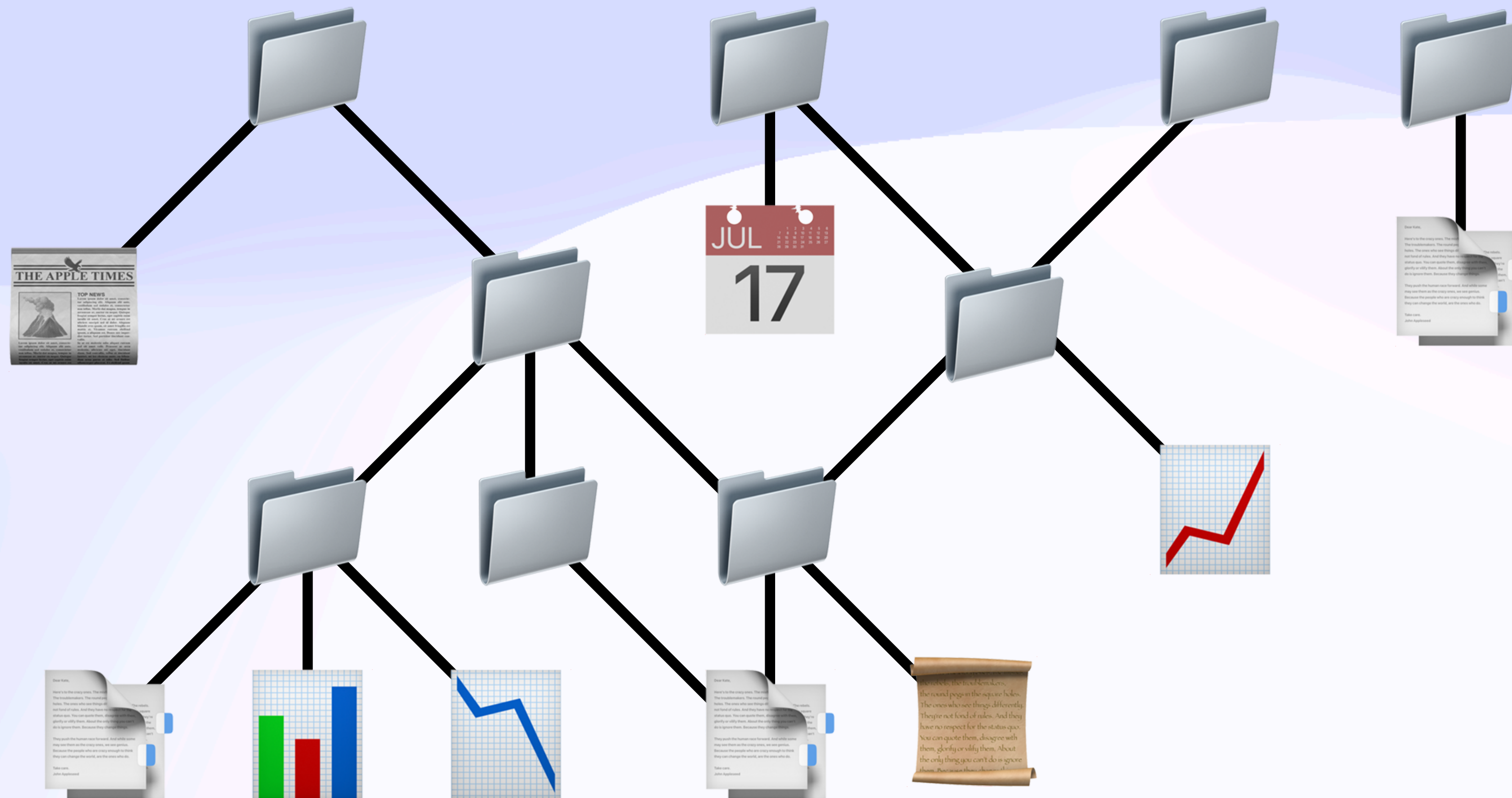
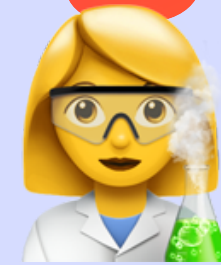
Beyond All-Or-Nothing

Local Context

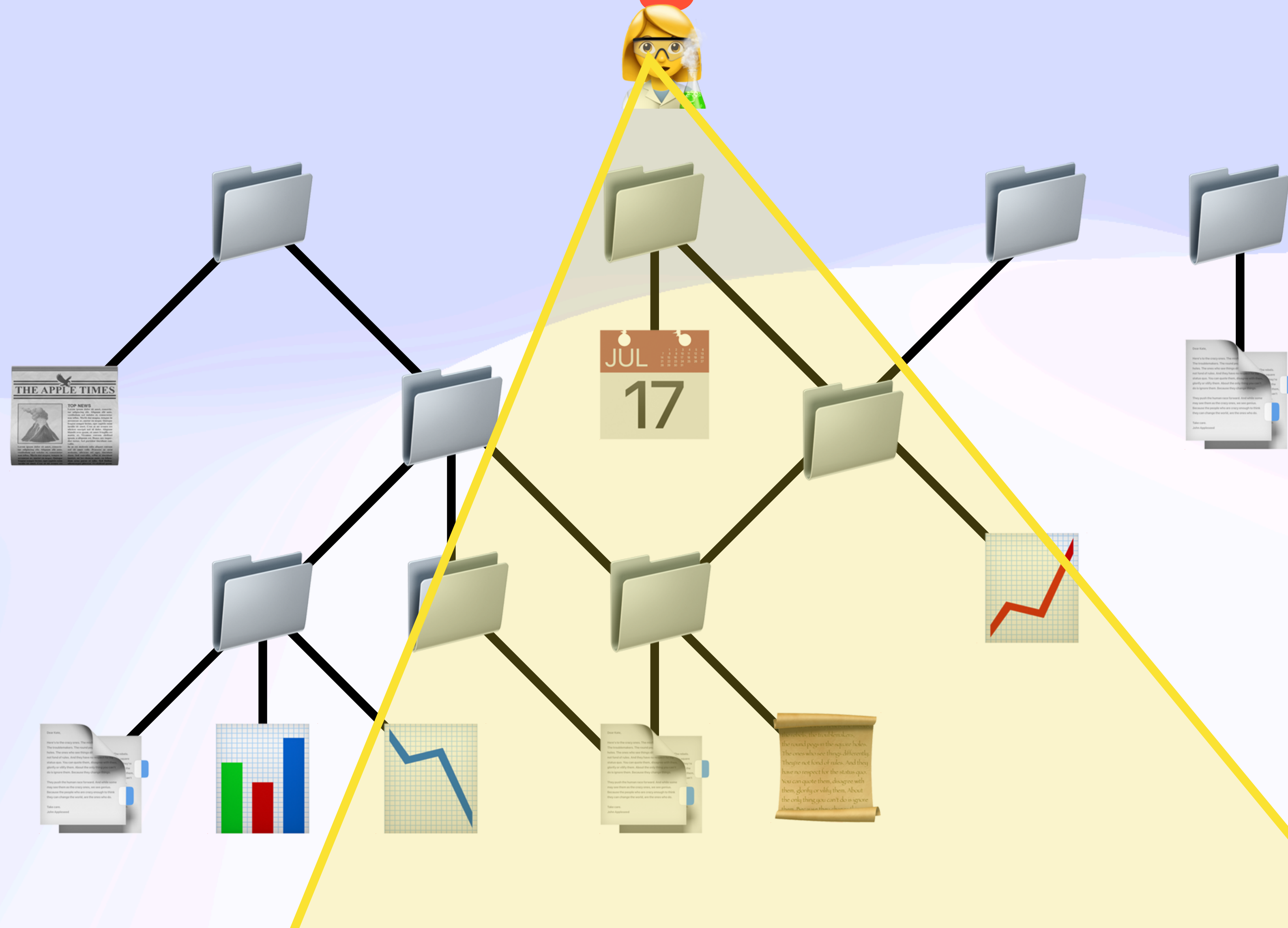
Beyond All-Or-Nothing



Beyond All-Or-Nothing

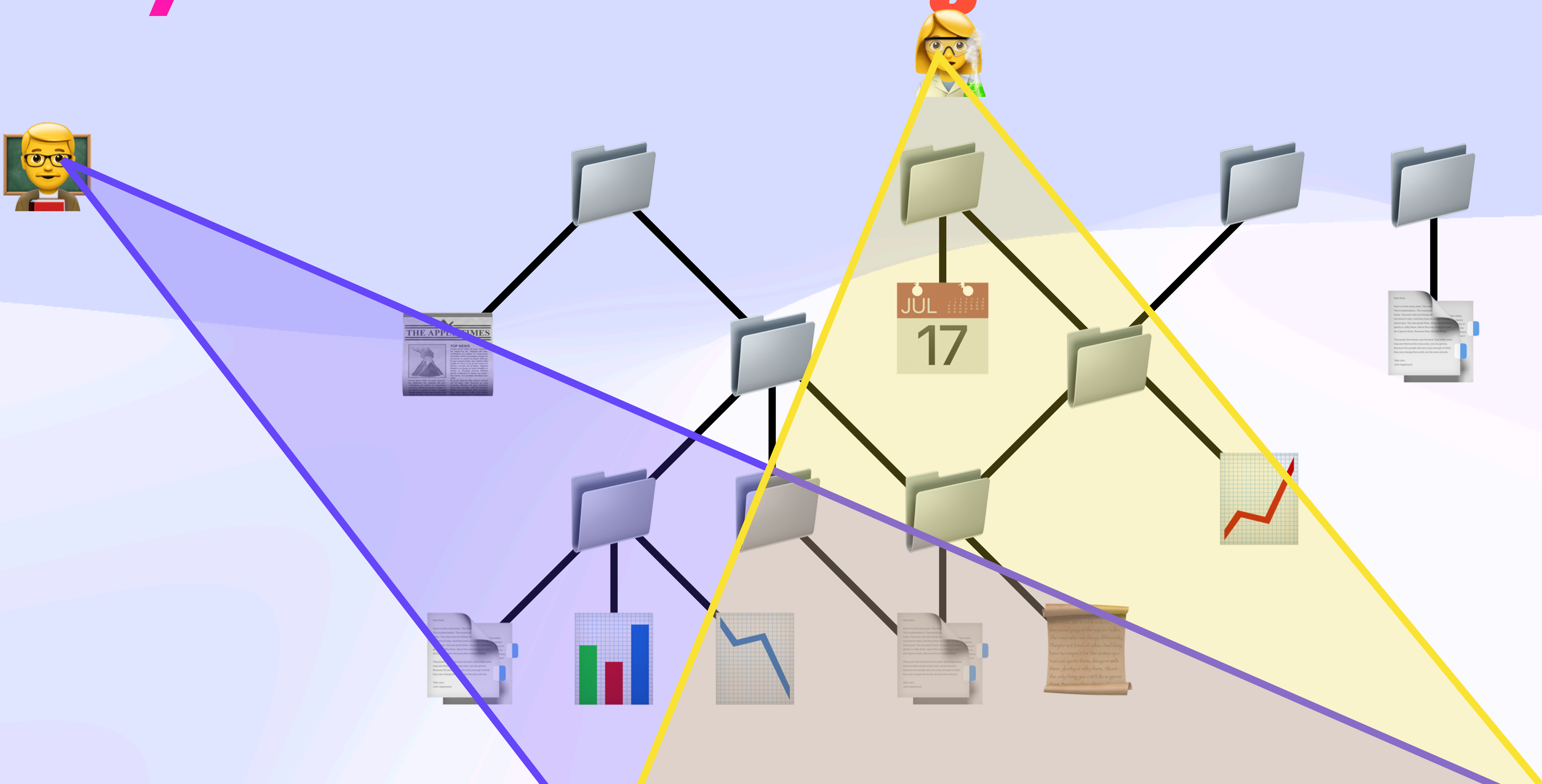
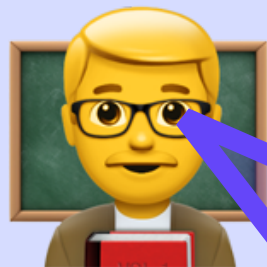


Beyond All-Or-Nothing



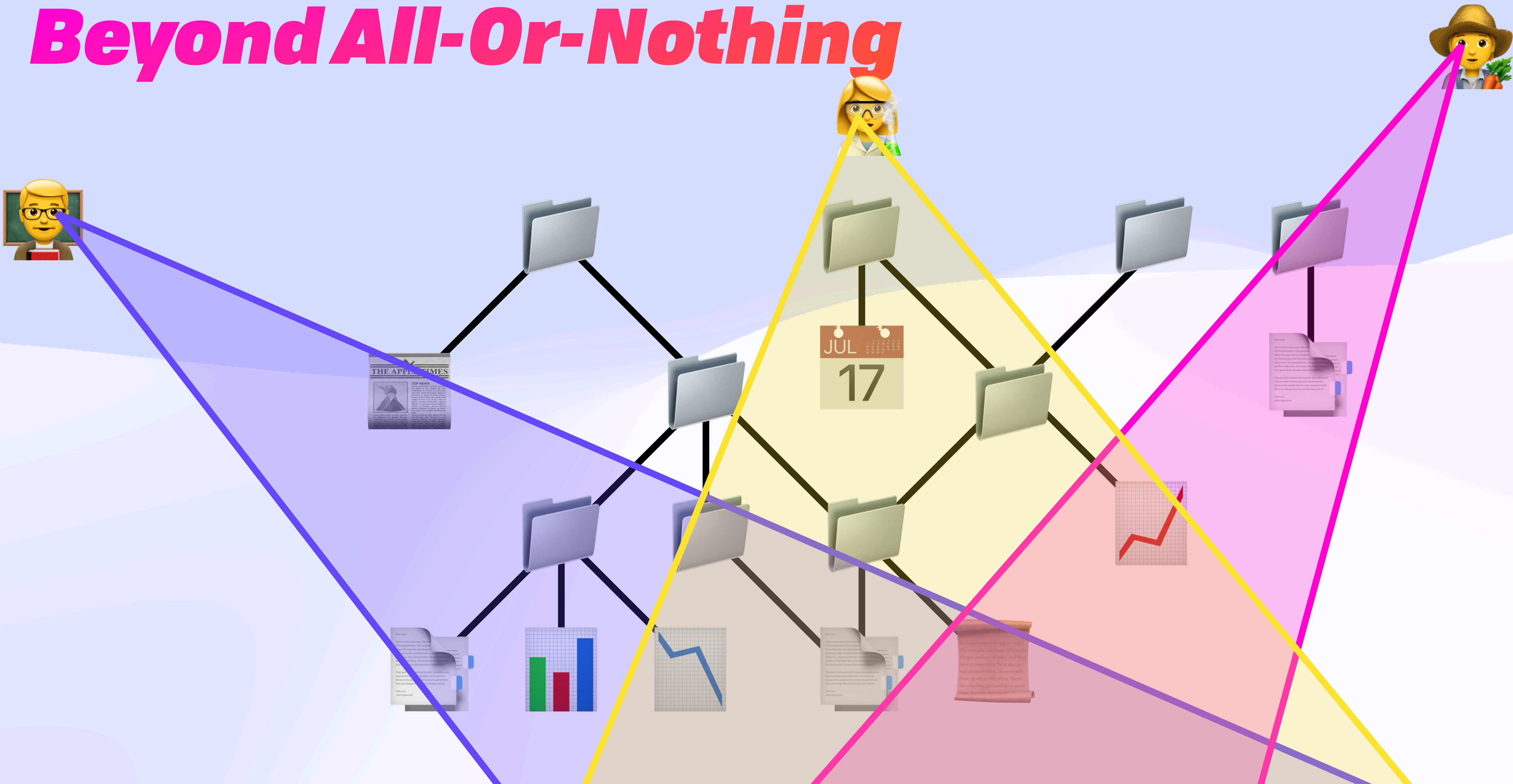
Local Context

Beyond All-Or-Nothing



Local Context

Beyond All-Or-Nothing



Protecting Writes & Agreeing on Membership

Convergent Capabilities



Convergent Capabilities



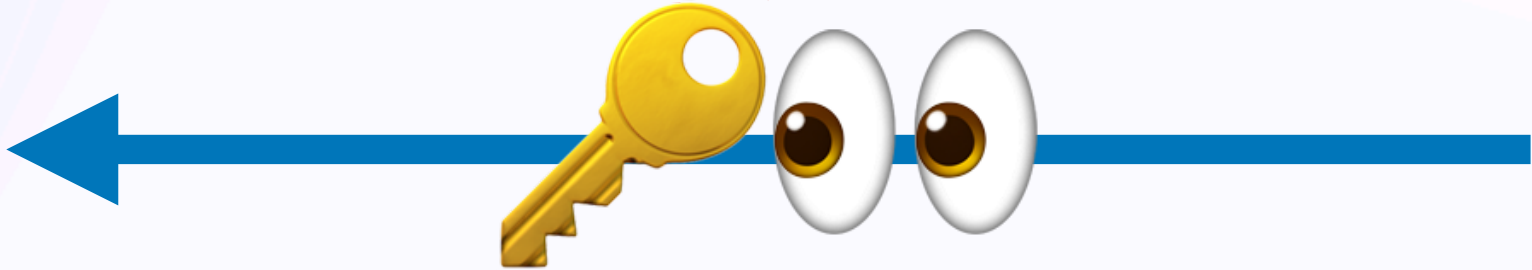
Convergent Capabilities

Pull
(Distribute)

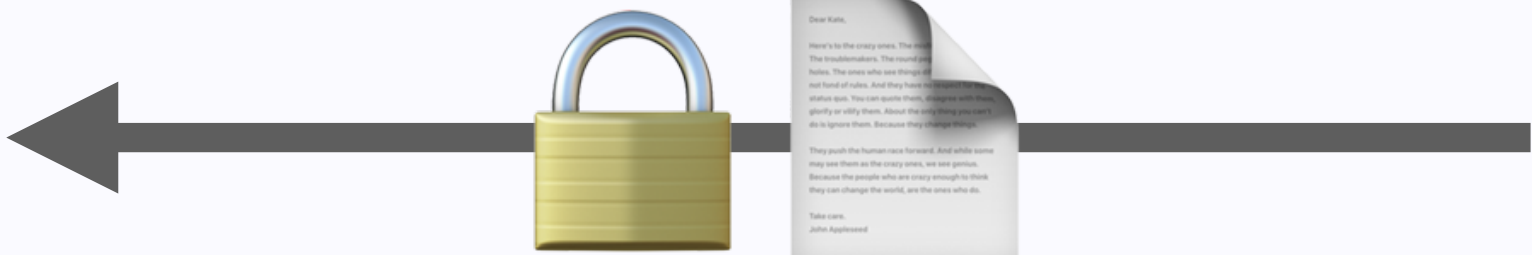


Convergent Capabilities

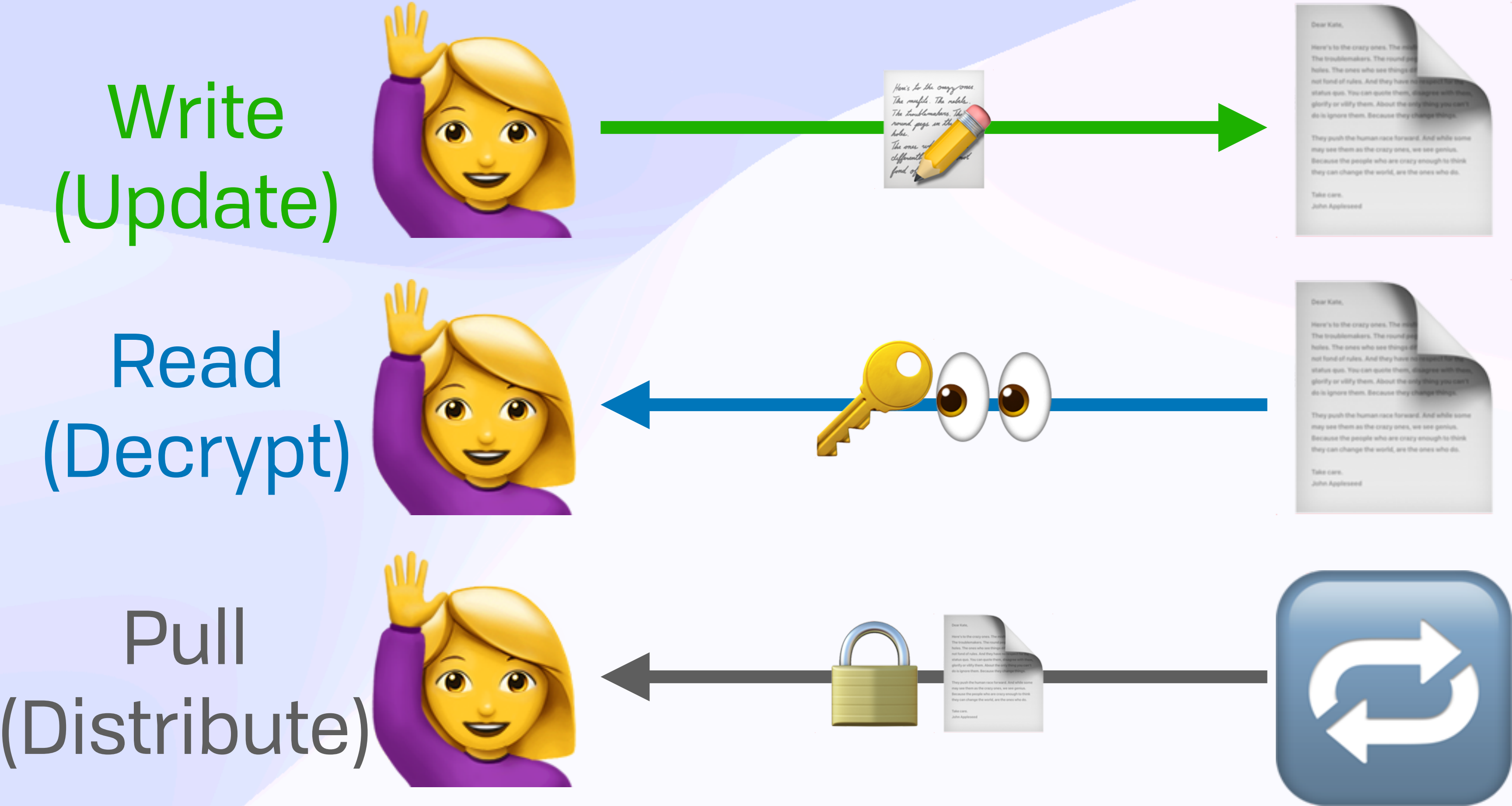
Read
(Decrypt)



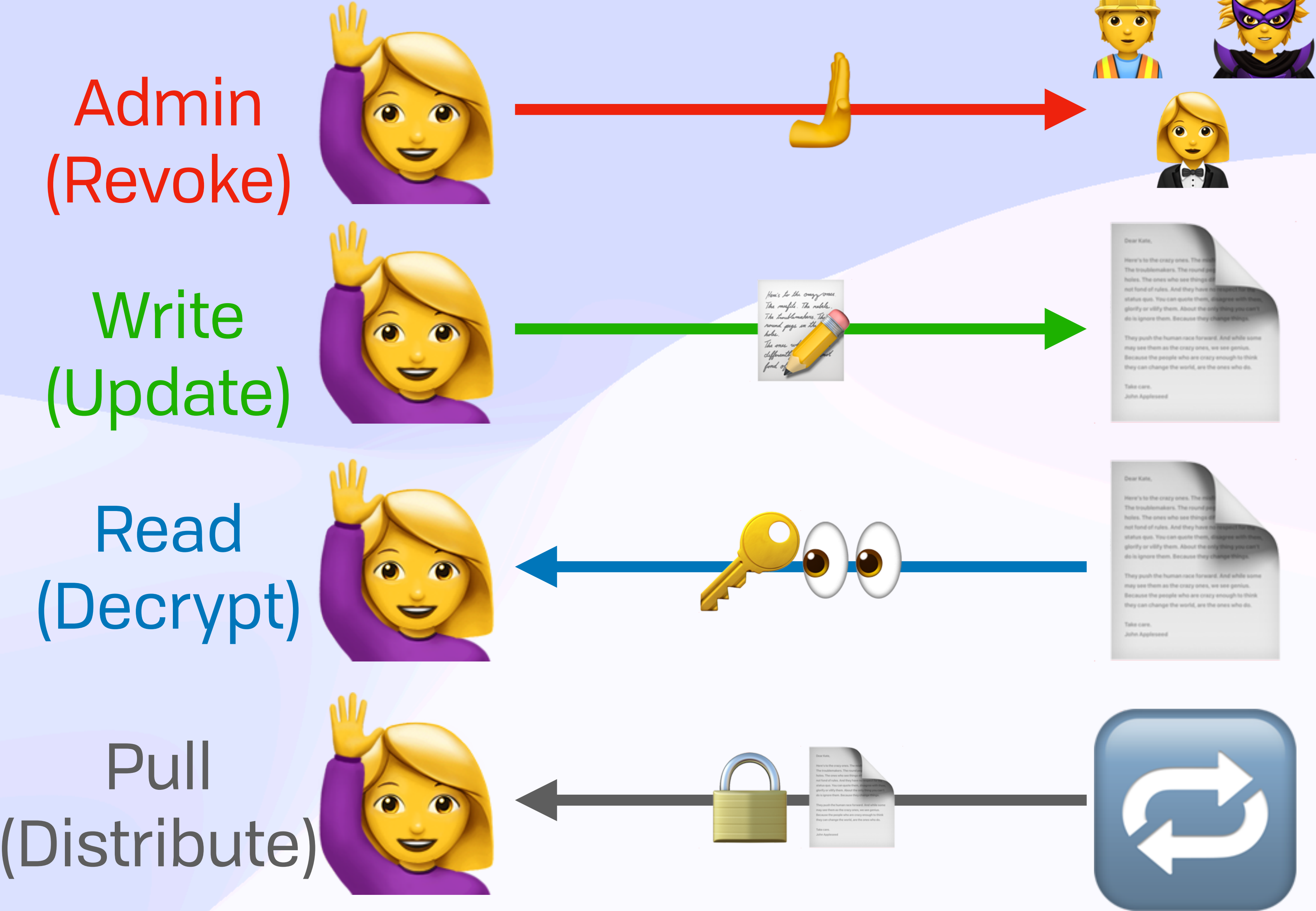
Pull
(Distribute)



Convergent Capabilities



Convergent Capabilities

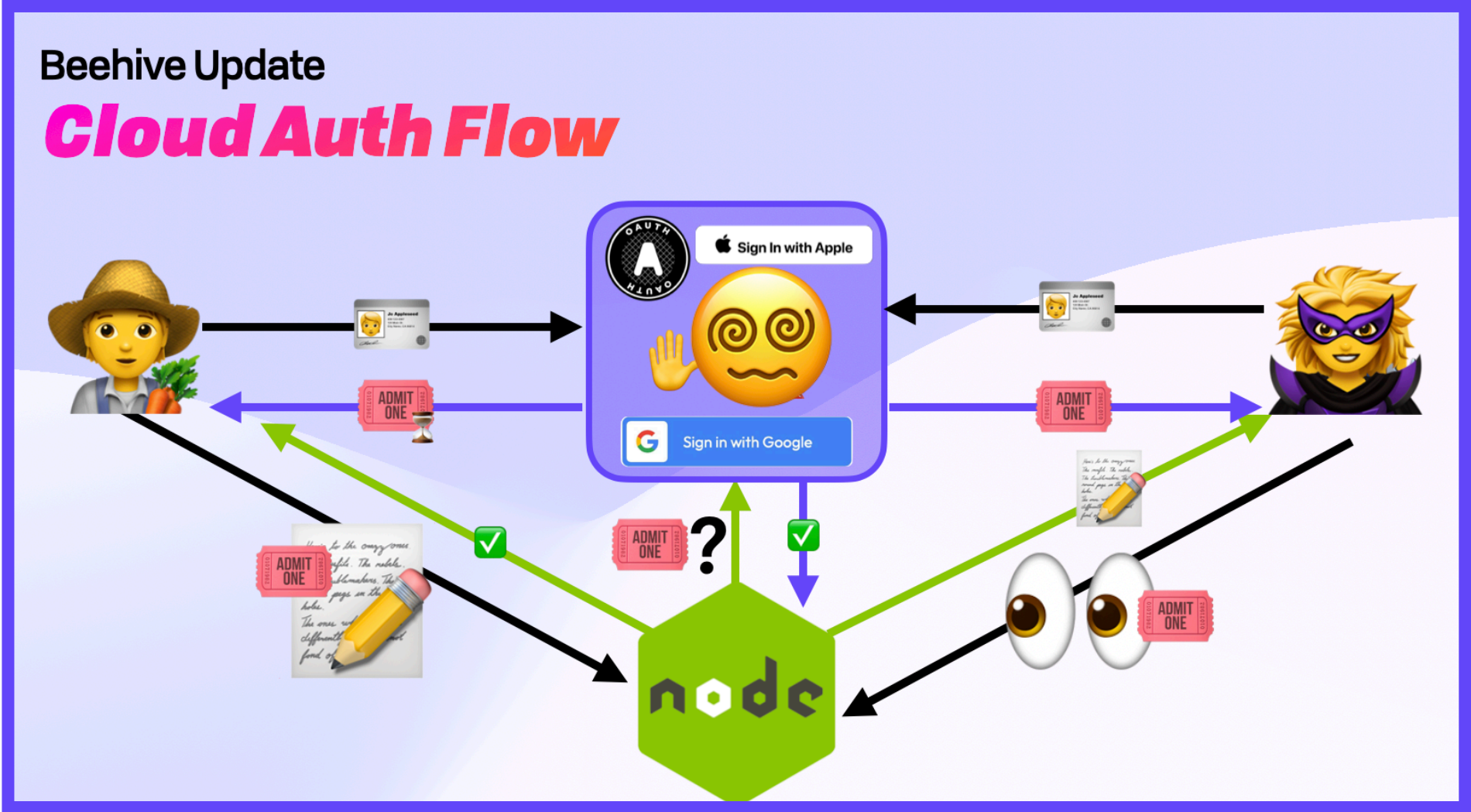


Convergent Capabilities

Self-Authenticating Changes

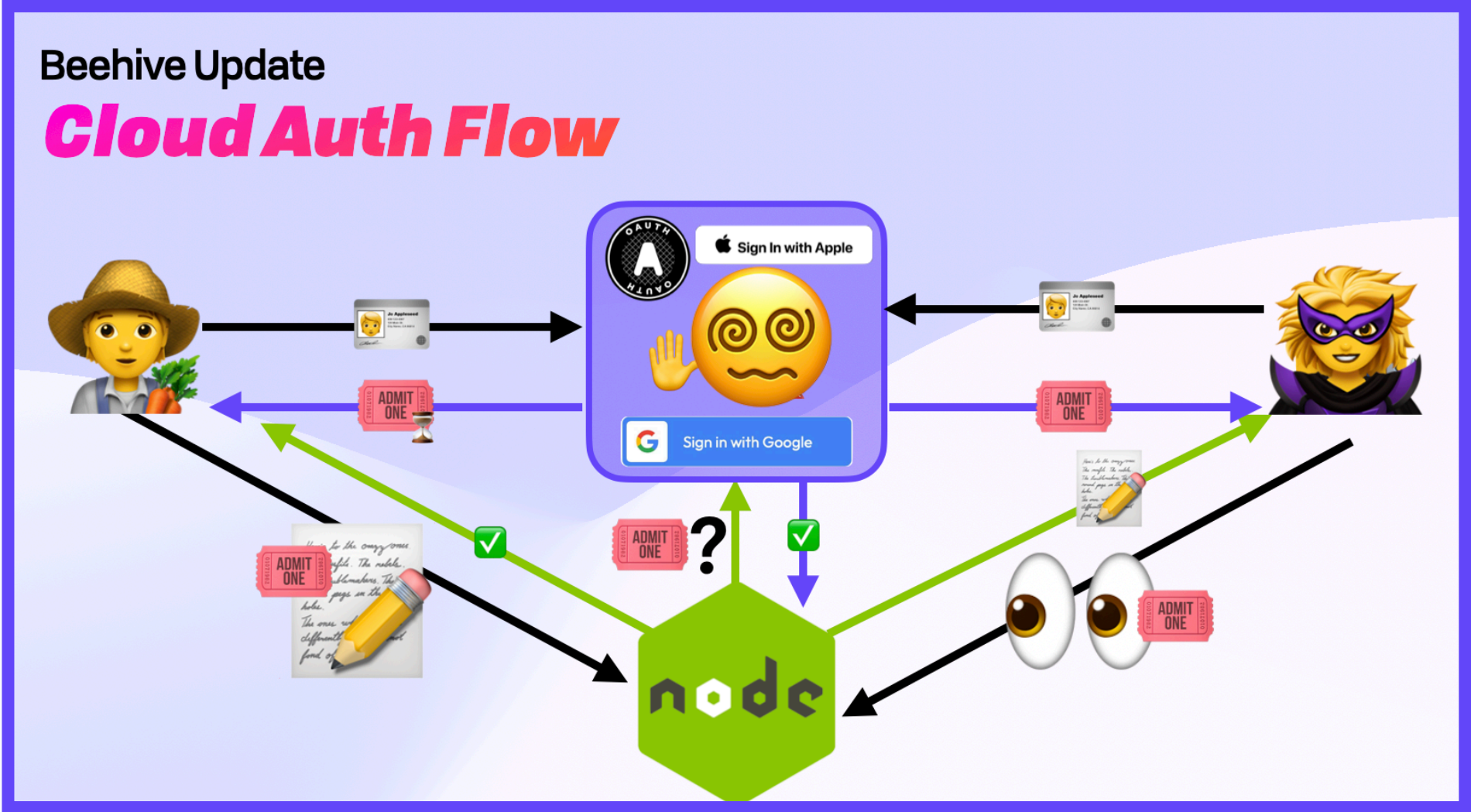
Convergent Capabilities

Self-Authenticating Changes



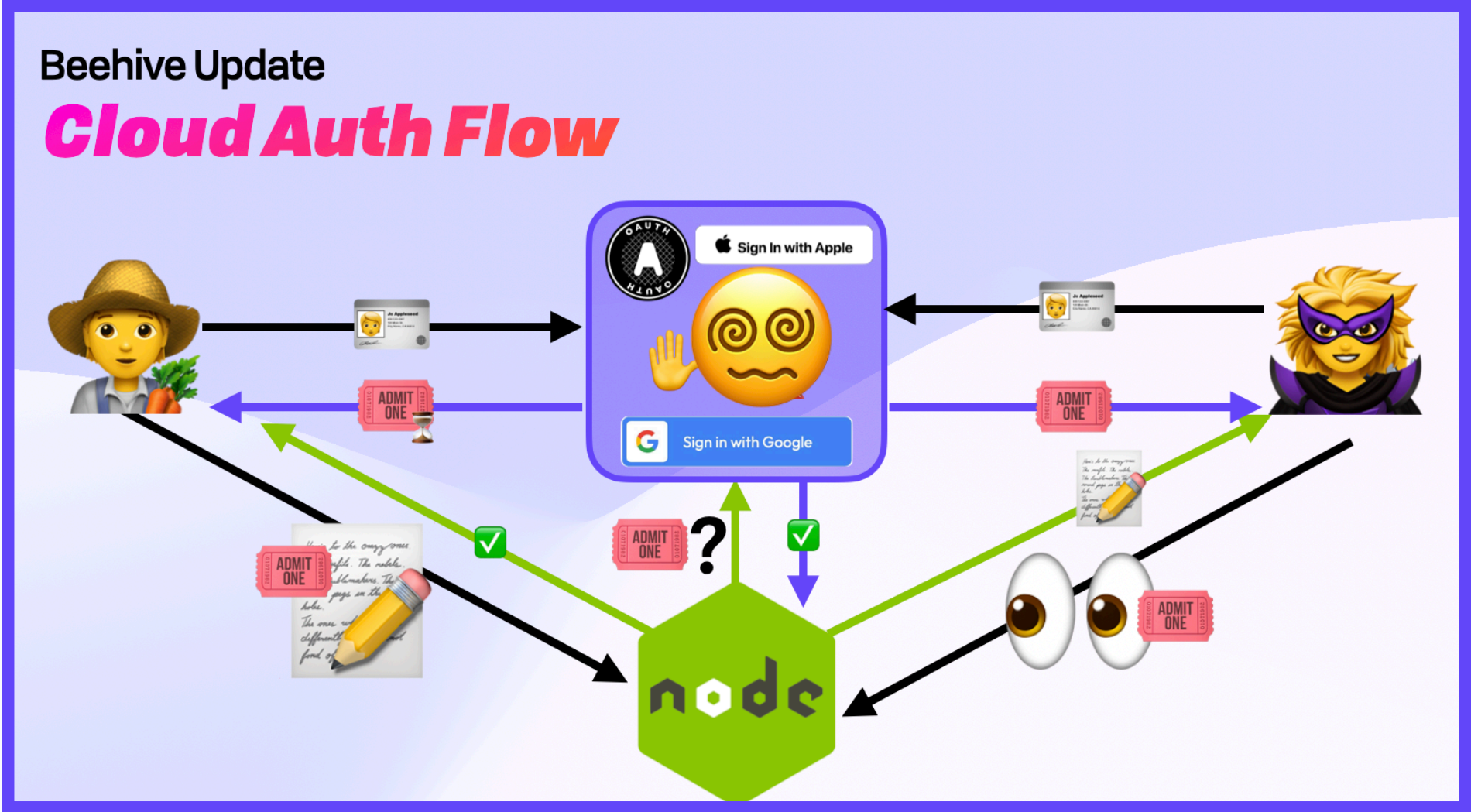
Convergent Capabilities

Self-Authenticating Changes



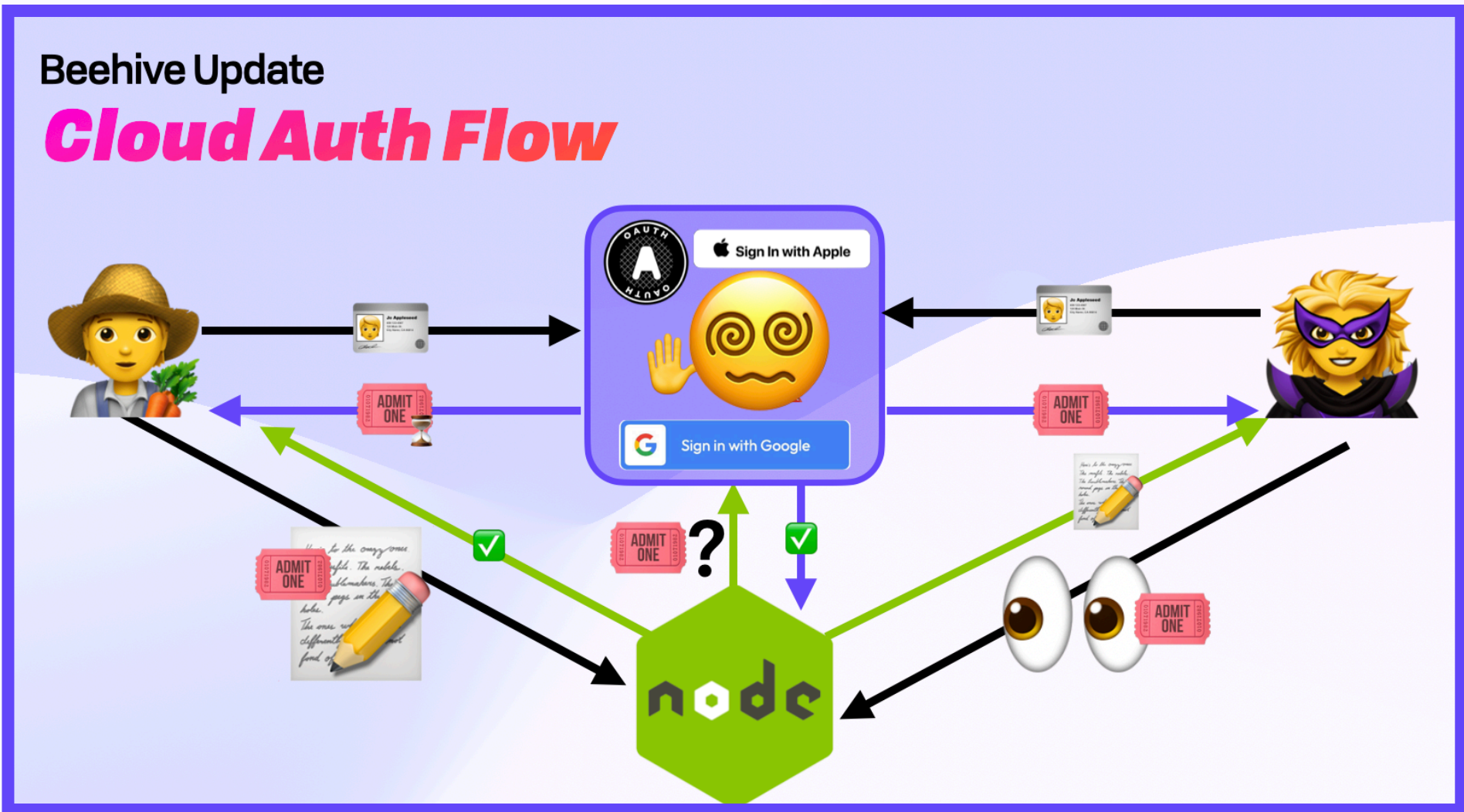
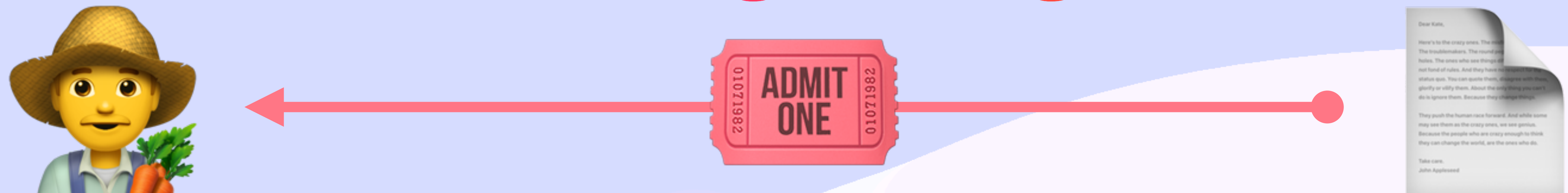
Convergent Capabilities

Self-Authenticating Changes

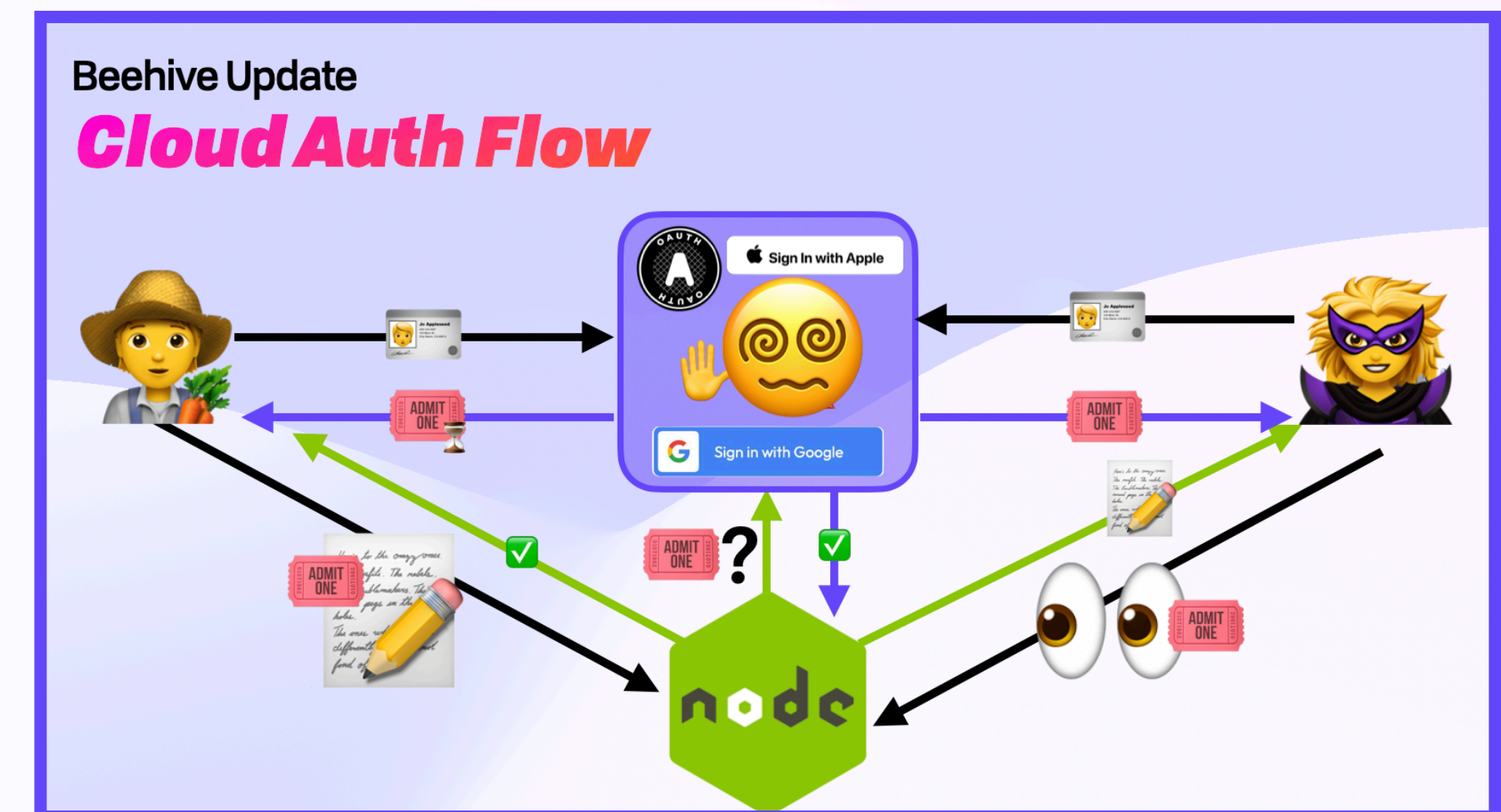


Convergent Capabilities

Self-Authenticating Changes

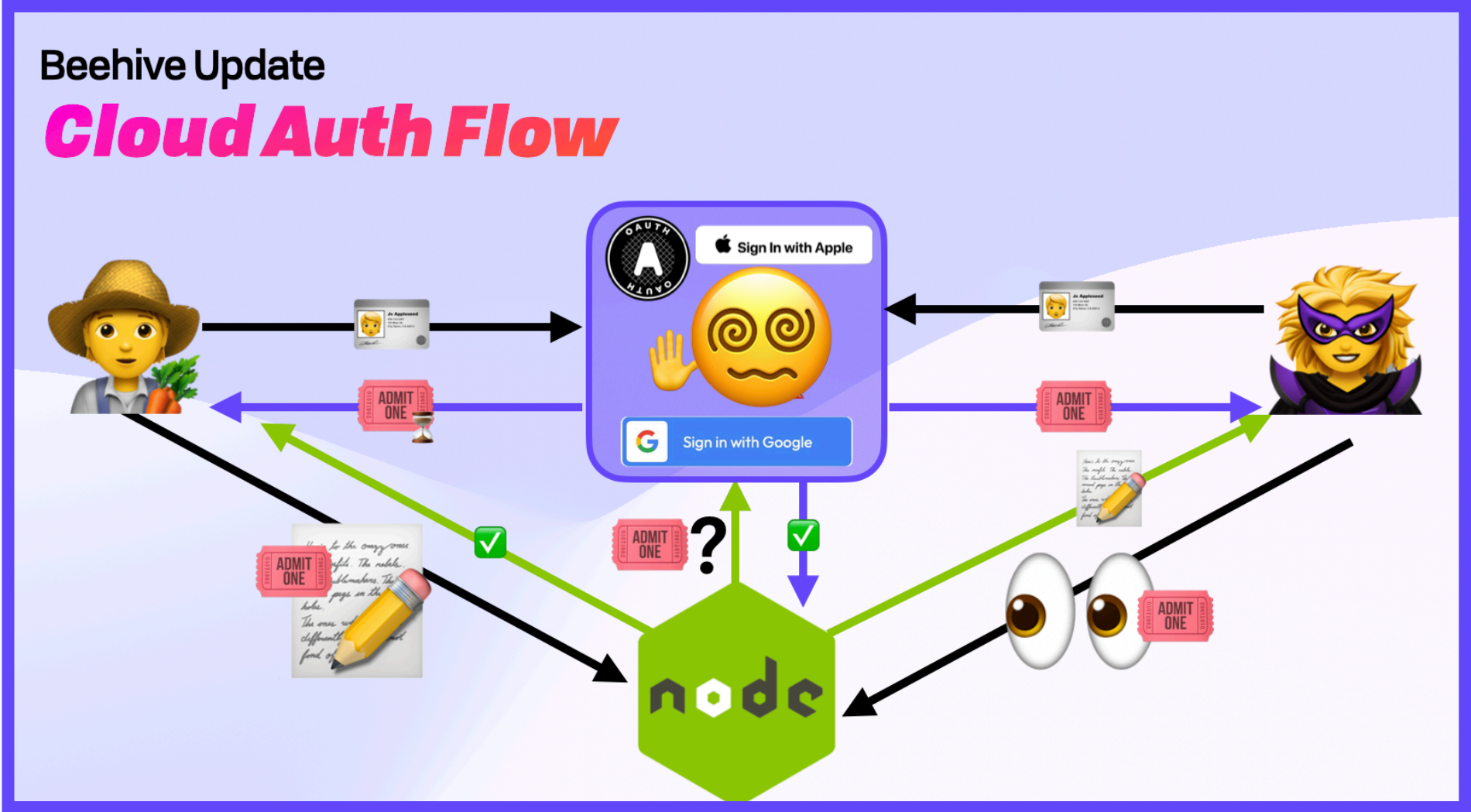


Self-Authenticating Changes



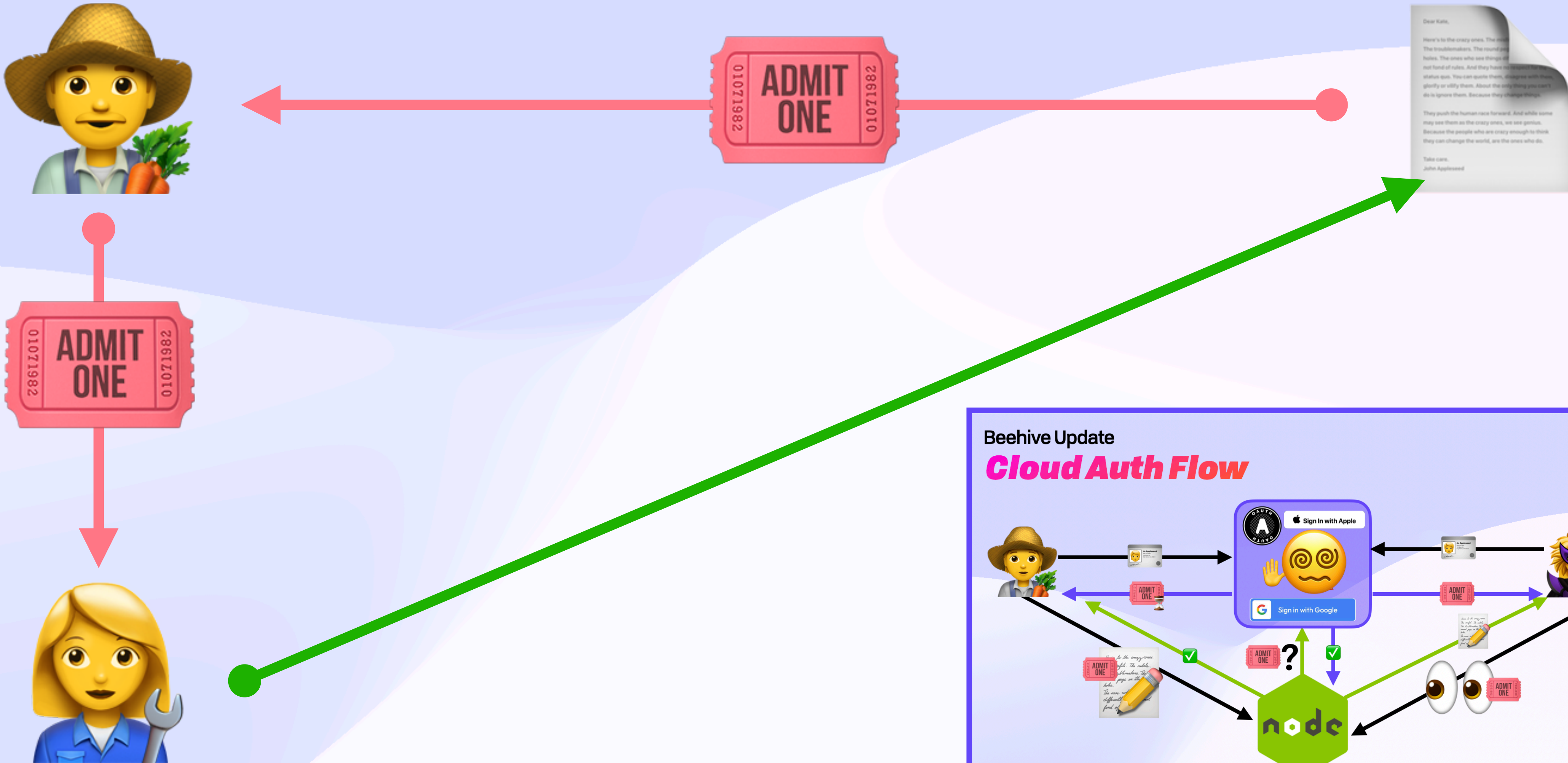
Convergent Capabilities

Self-Authenticating Changes



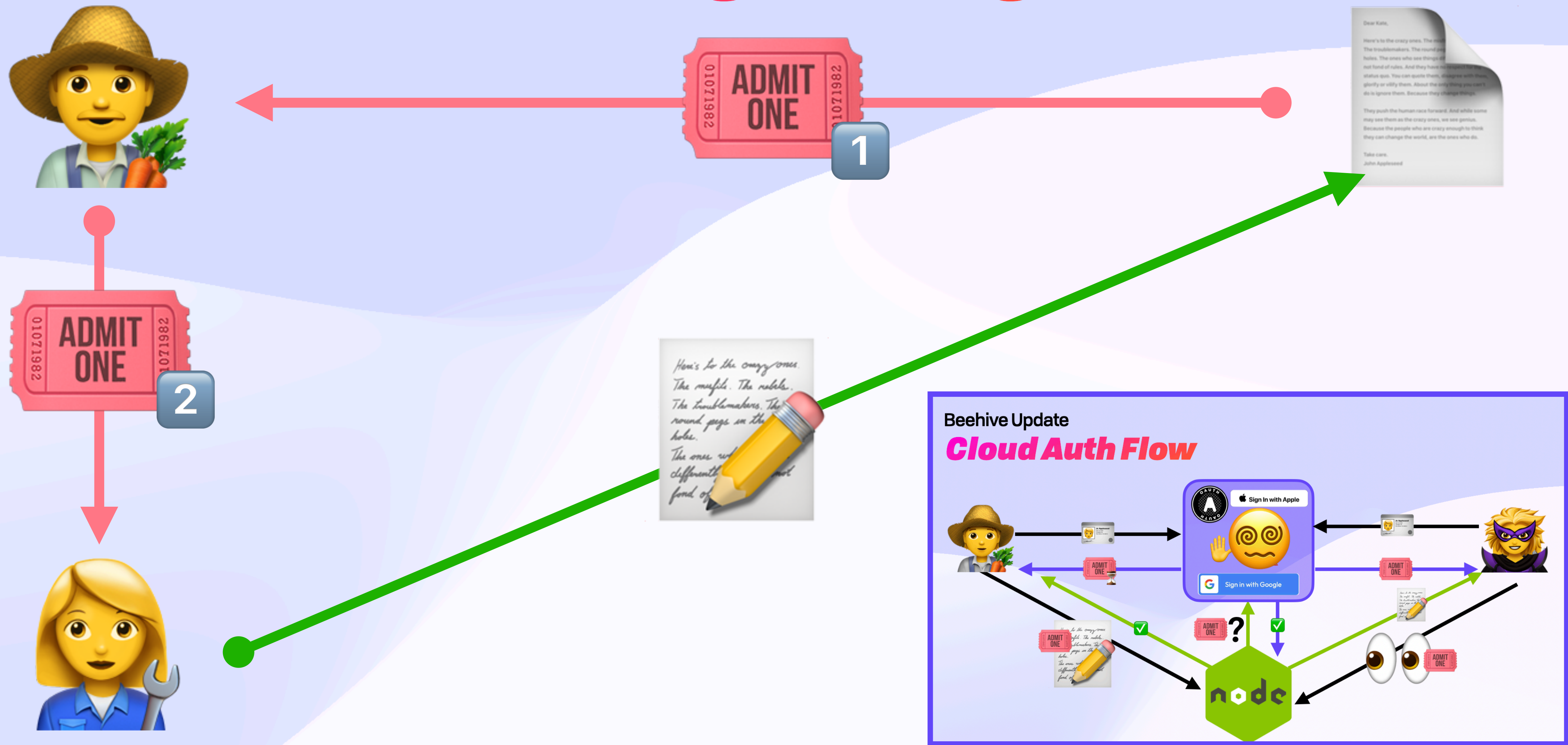
Convergent Capabilities

Self-Authenticating Changes



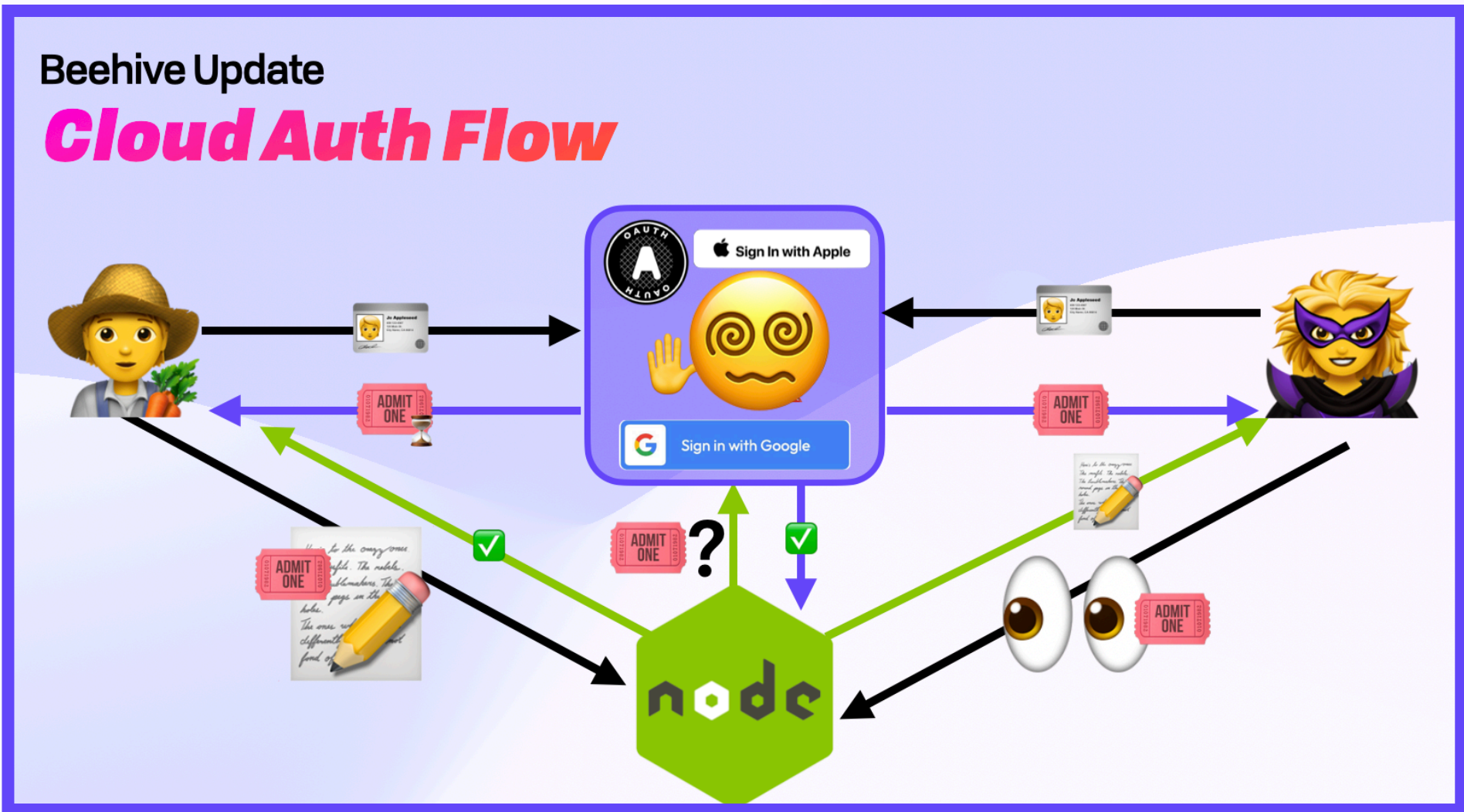
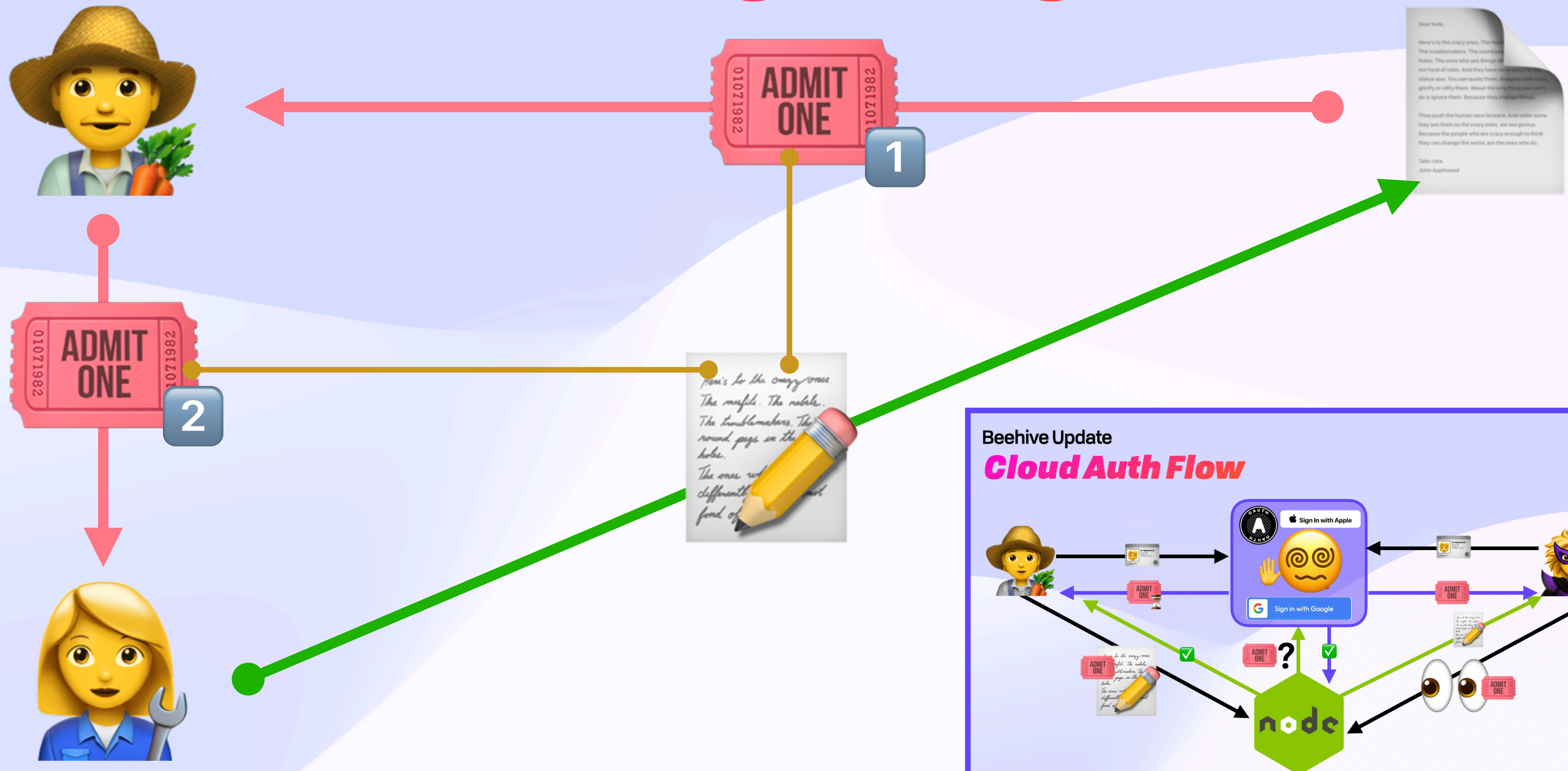
Convergent Capabilities

Self-Authenticating Changes



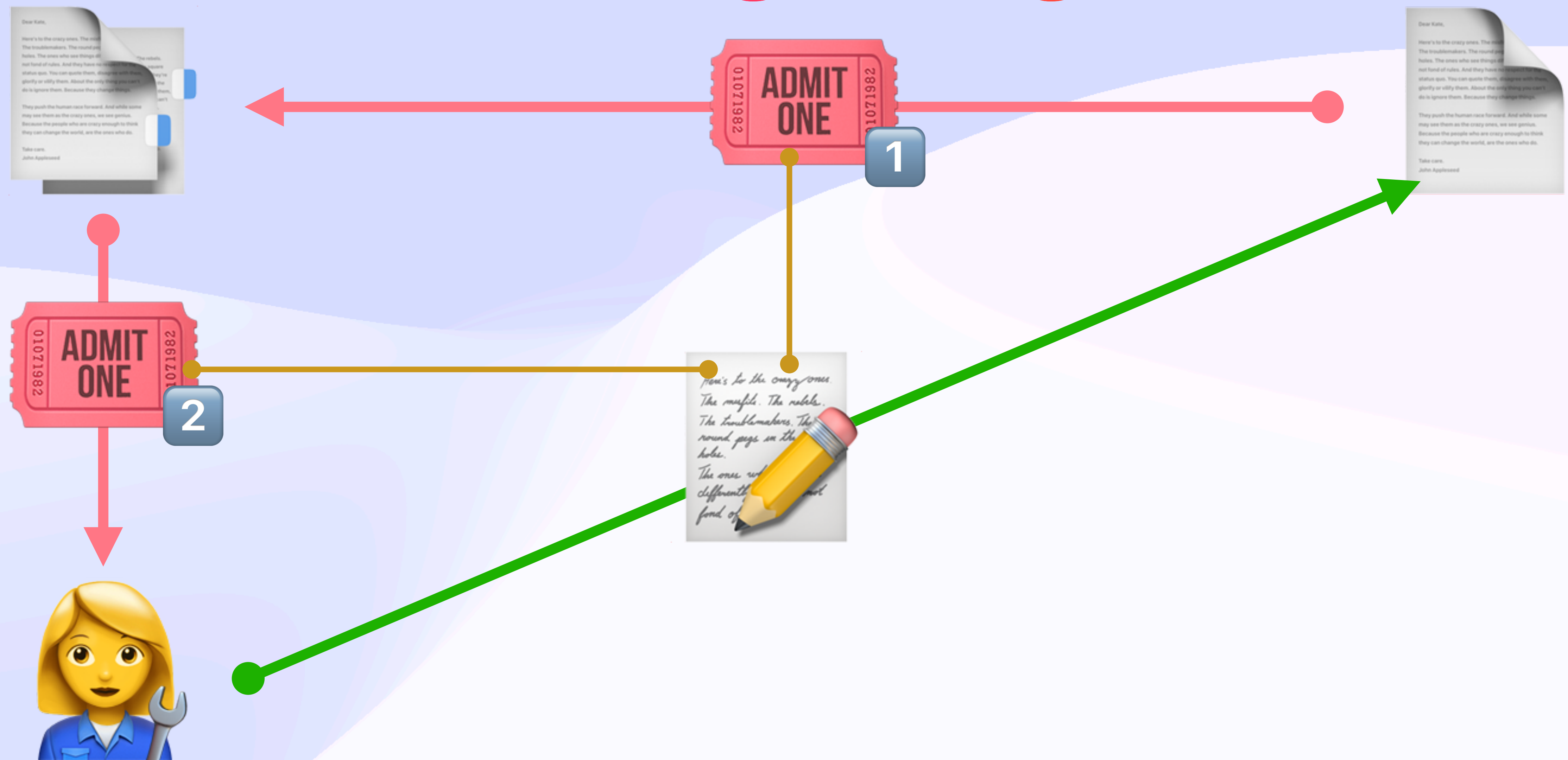
Convergent Capabilities

Self-Authenticating Changes



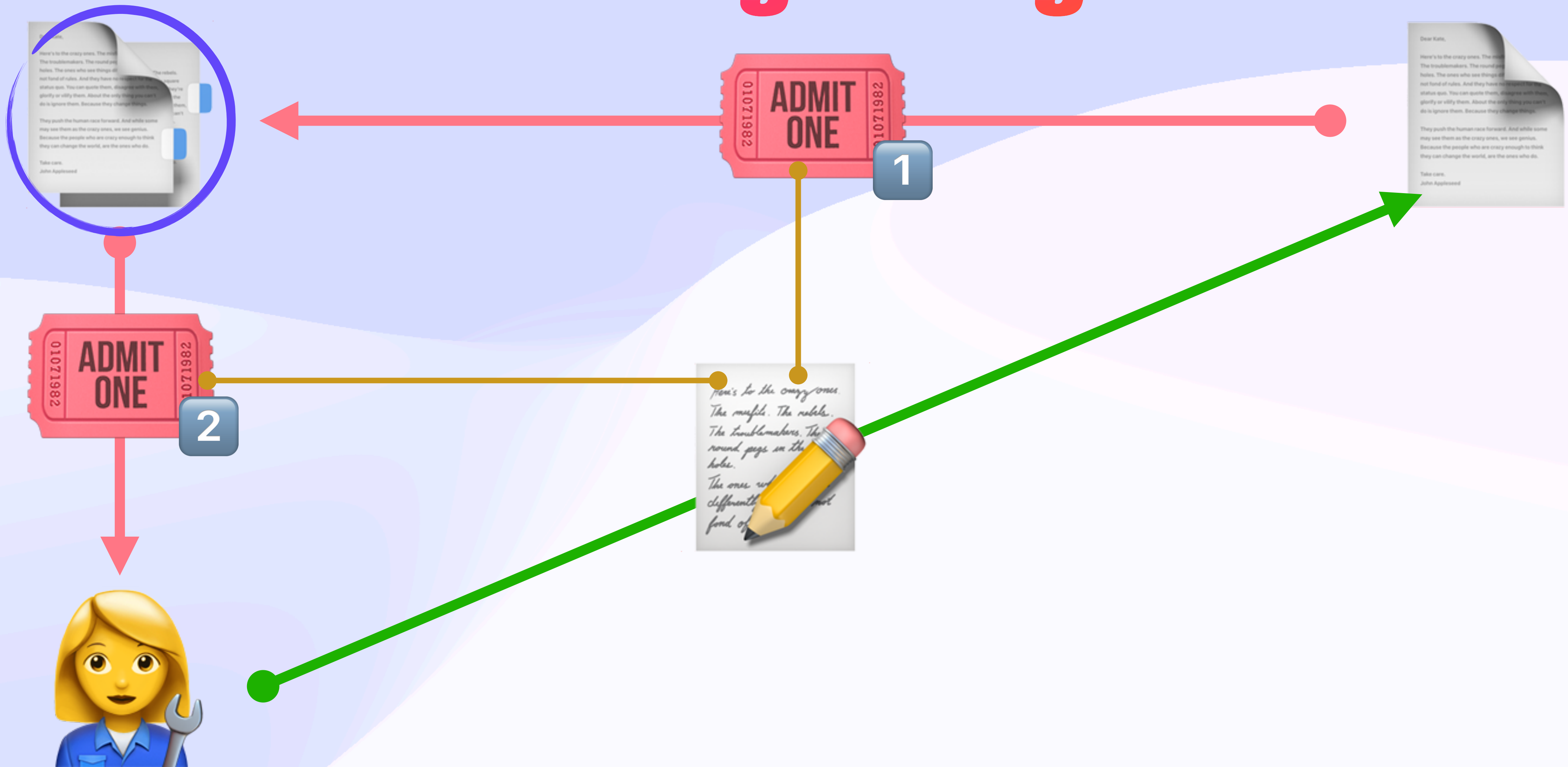
Convergent Capabilities

Self-Authenticating Changes



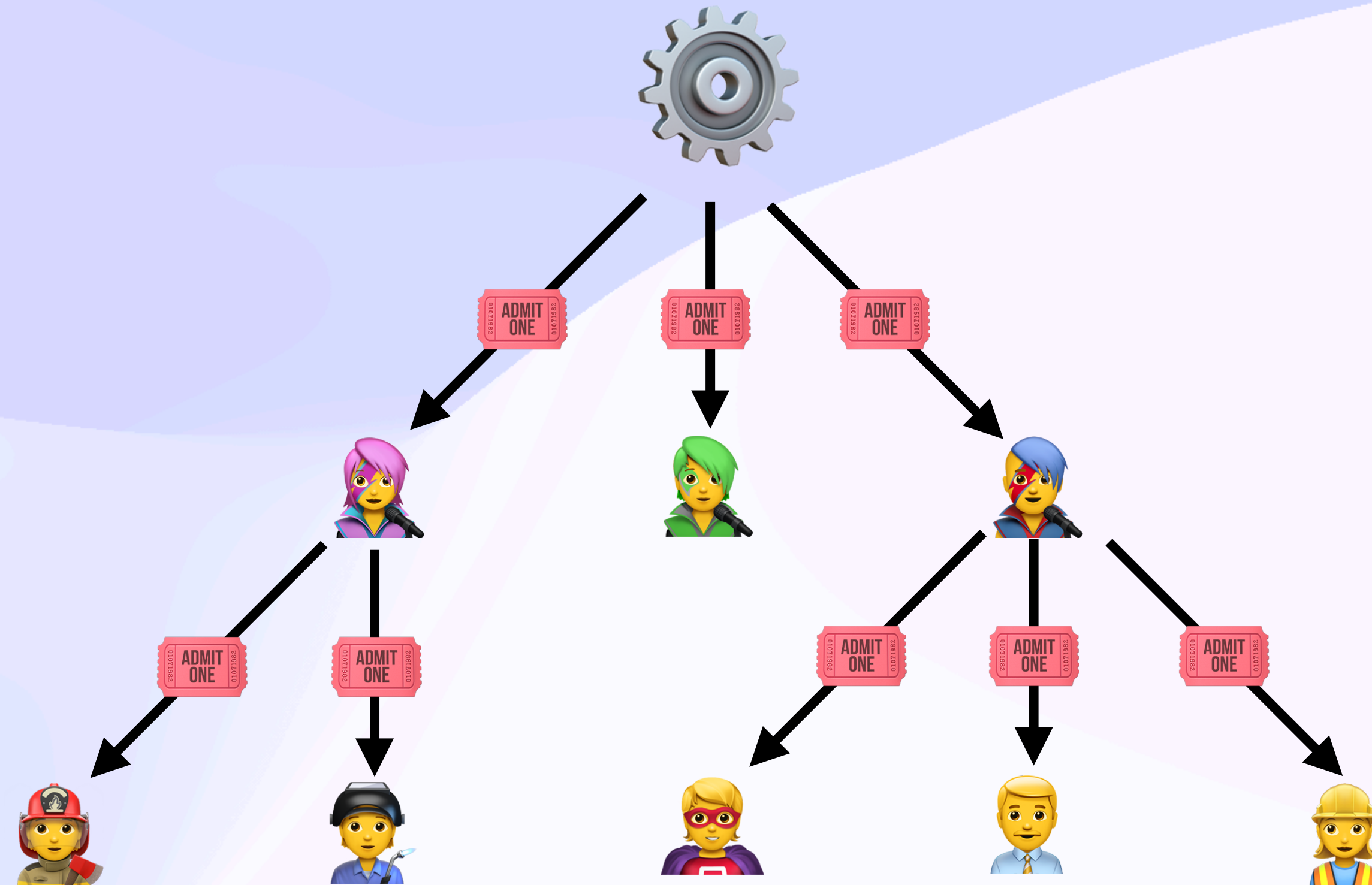
Convergent Capabilities

Self-Authenticating Changes



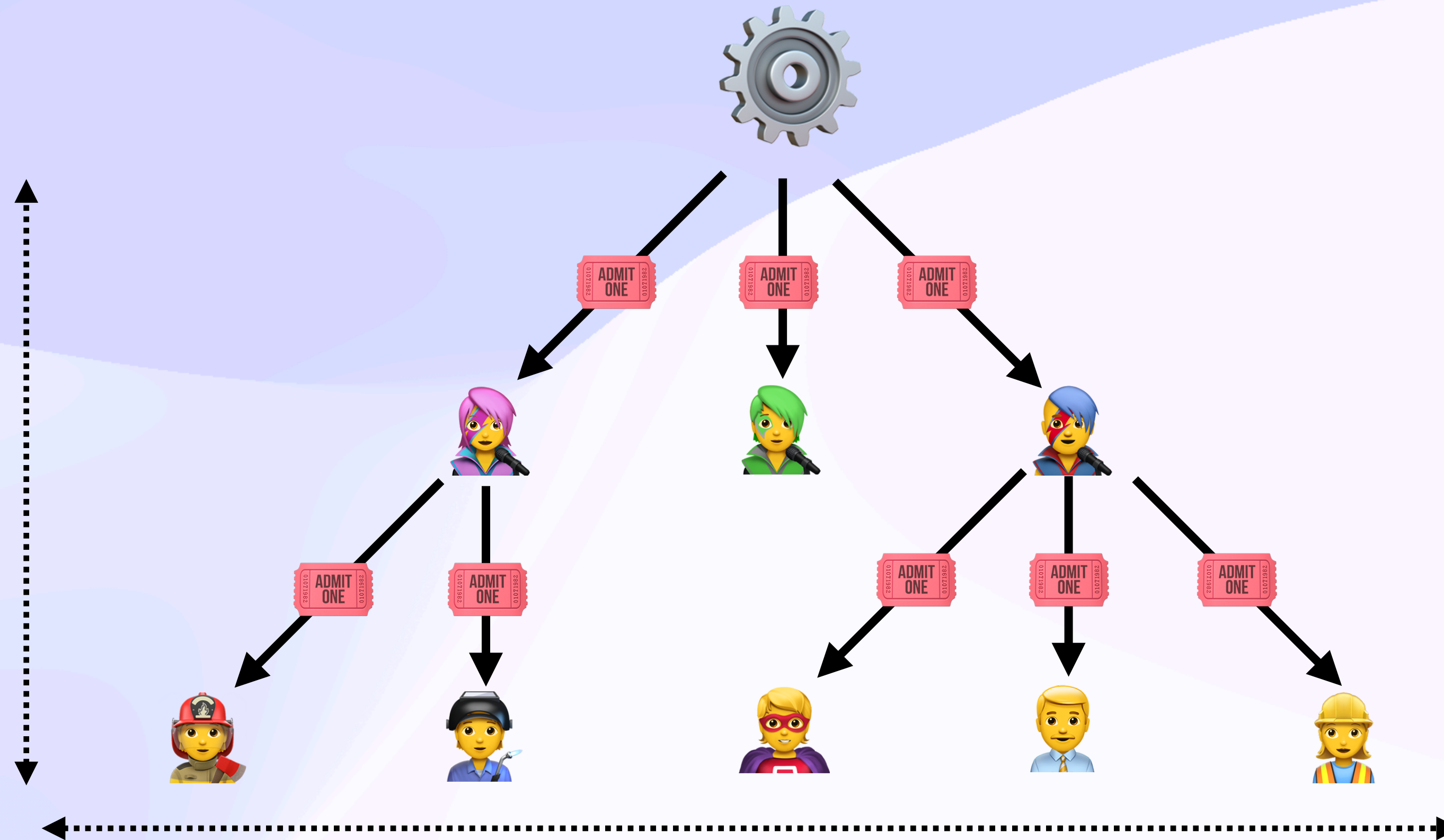
Keyhive

On a Need to Know Basis



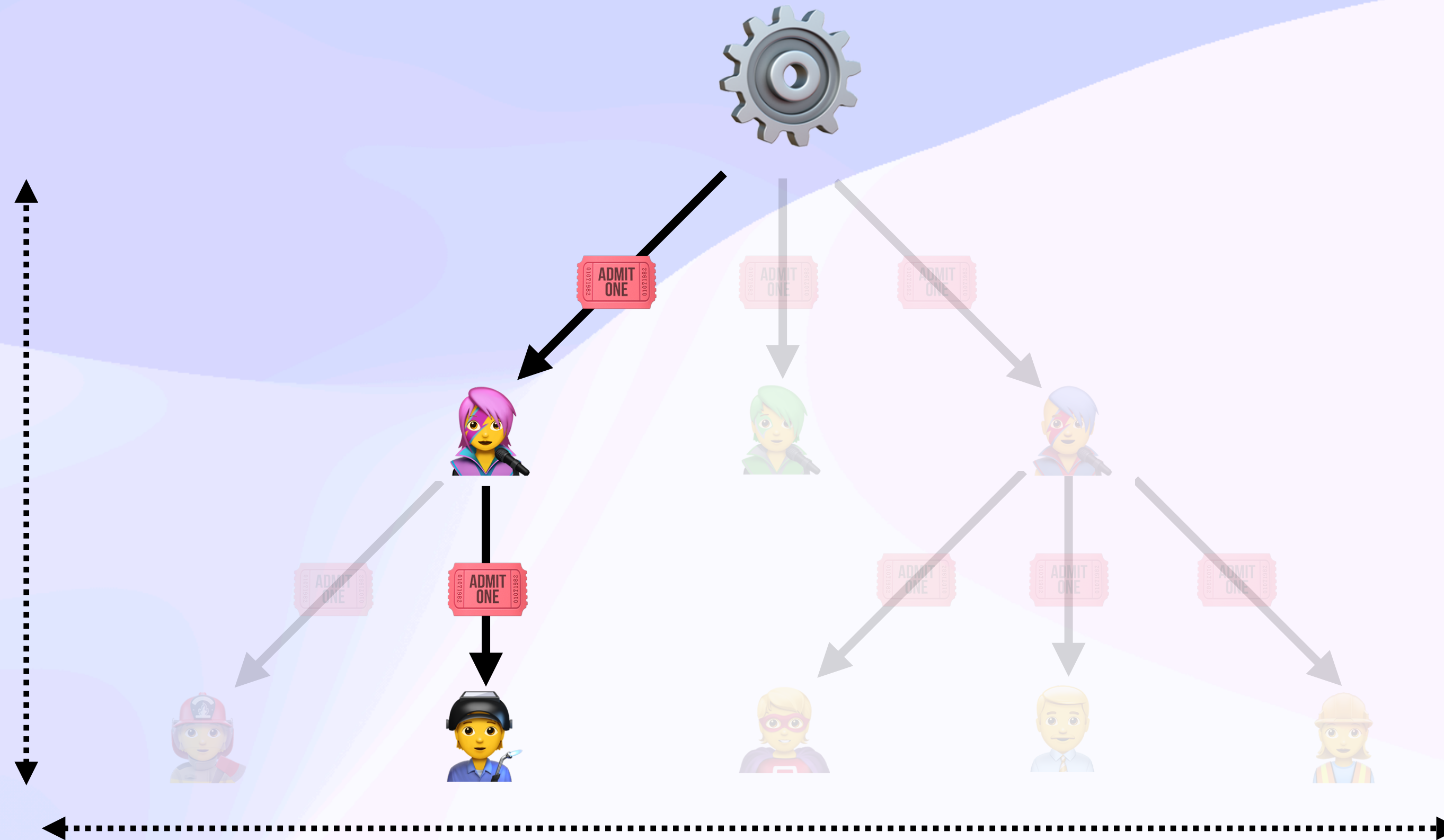
Keyhive

On a Need to Know Basis



Keyhive

On a Need to Know Basis



Convergent Capabilities

Example High Level API

Convergent Capabilities

Example High Level API

```
authedDocHandle.change(doc ⇒ {  
  doc.event = "ReCAP"  
  doc.city = "NYC"  
})
```

Convergent Capabilities

Example High Level API

```
authedDocHandle.change(doc ⇒ {  
  doc.event = "ReCAP"  
  doc.city = "NYC"  
})
```

```
authedDocHandle.addMember(alice, ADMIN)
```

Convergent Capabilities

Example High Level API

```
authedDocHandle.change(doc ⇒ {  
    doc.event = "ReCAP"  
    doc.city = "NYC"  
})
```

```
authedDocHandle.addMember(alice, ADMIN)  
authedDocHandle.removeMember(bob)
```

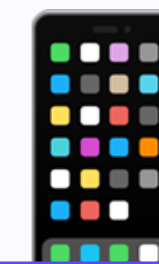

Convergent Capabilities

Groups



Convergent Capabilities

Groups



Alice's
Phone

Convergent Capabilities

Groups



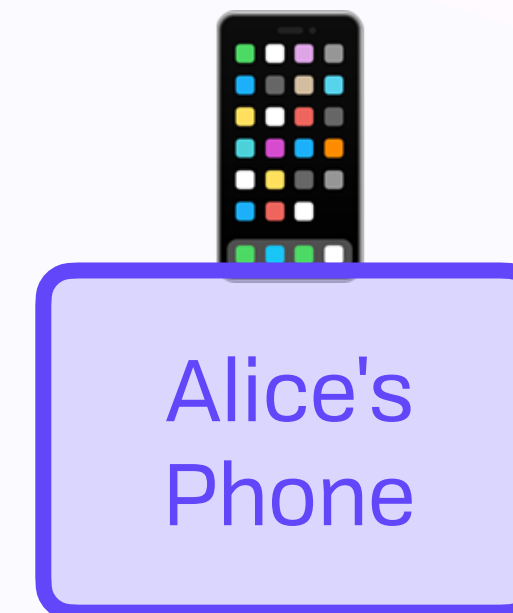
Alice's
Laptop



Alice's
Phone

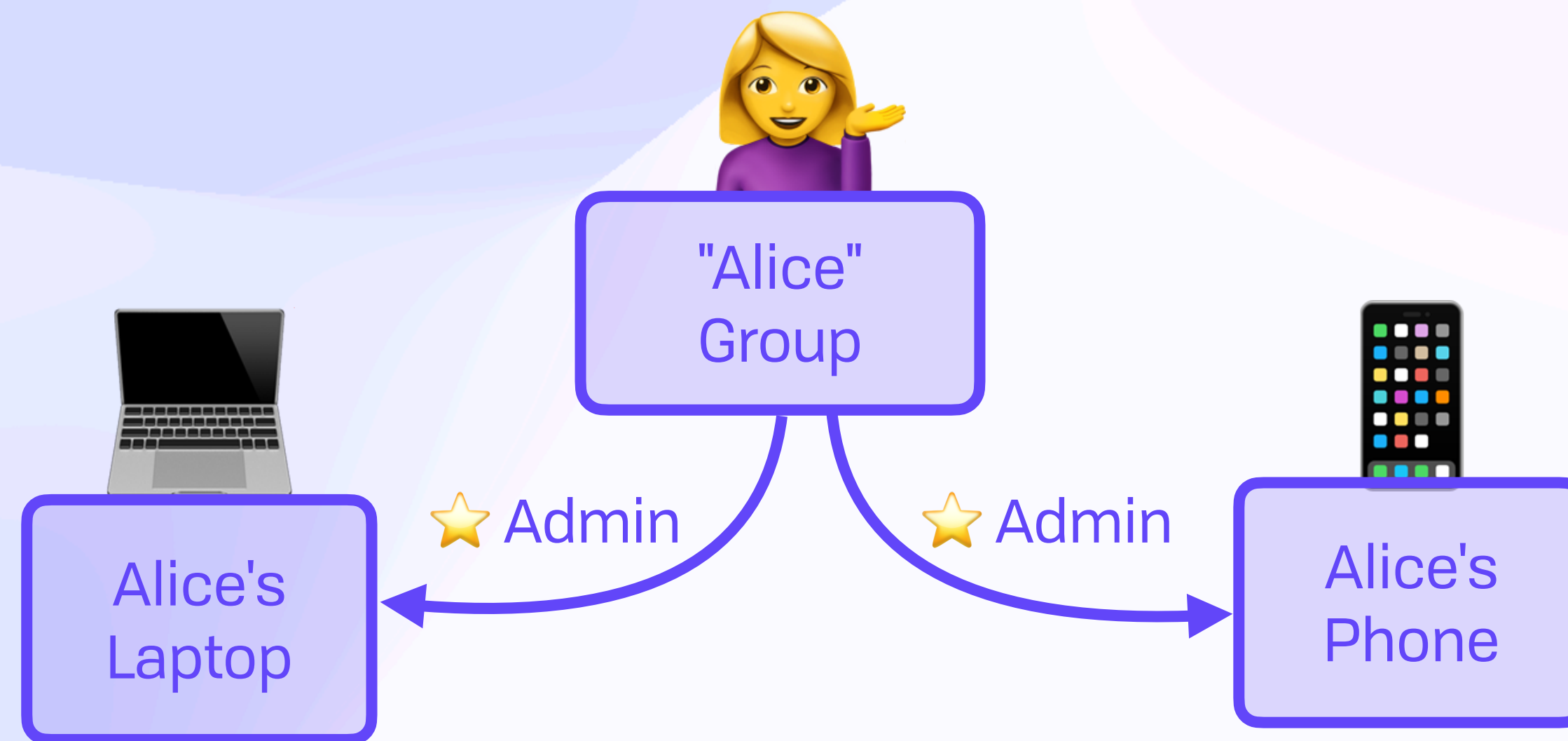
Convergent Capabilities

Groups



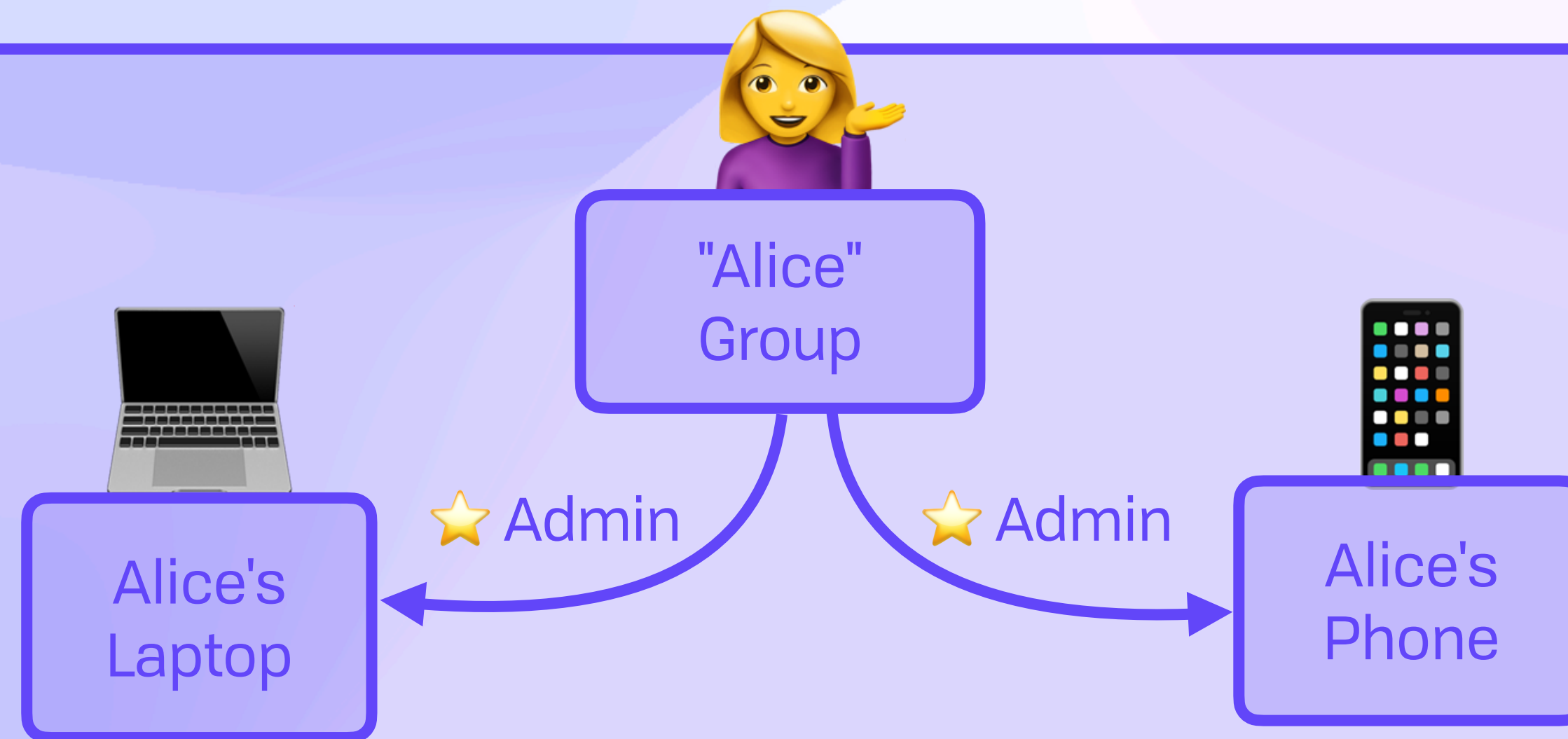
Convergent Capabilities

Groups



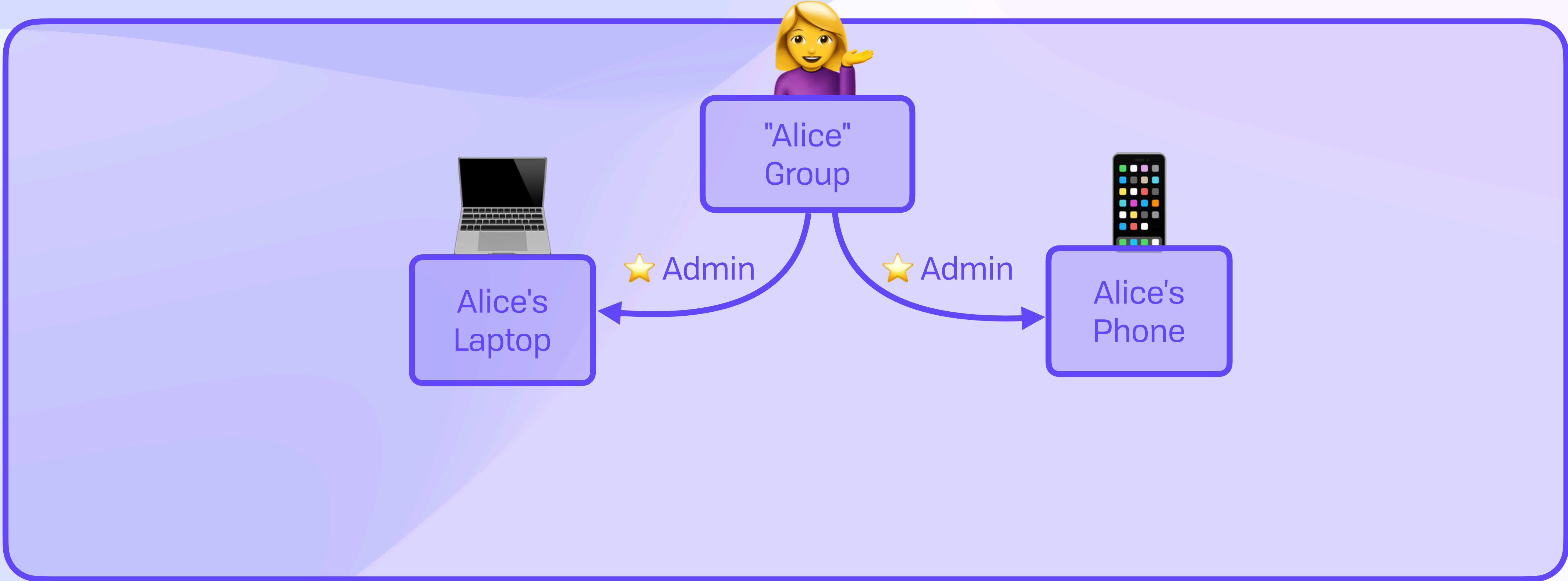
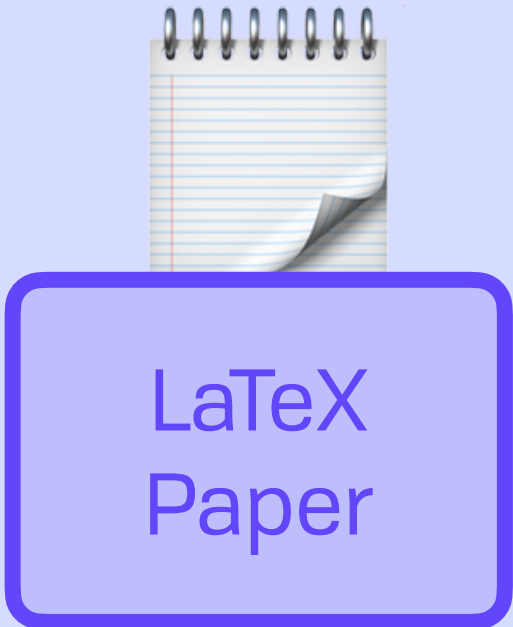
Convergent Capabilities

Groups



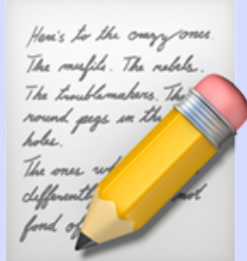
Convergent Capabilities

Groups

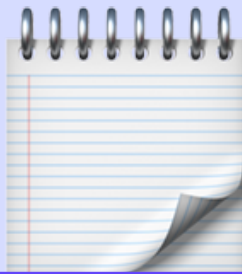


Convergent Capabilities

Groups



Meeting
Notes



LaTeX
Paper



"Alice"
Group



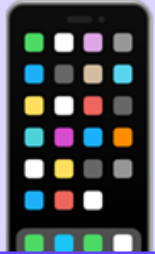
Alice's
Laptop



Admin



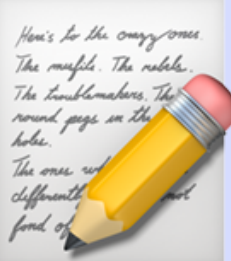
Admin



Alice's
Phone

Convergent Capabilities

Groups



Meeting Notes



LaTeX Paper



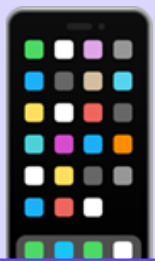
Ink & Switch Group



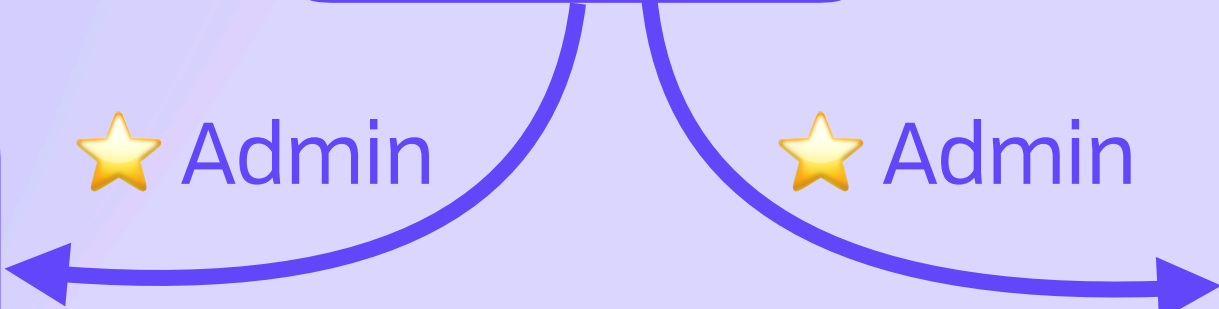
"Alice" Group



Alice's Laptop

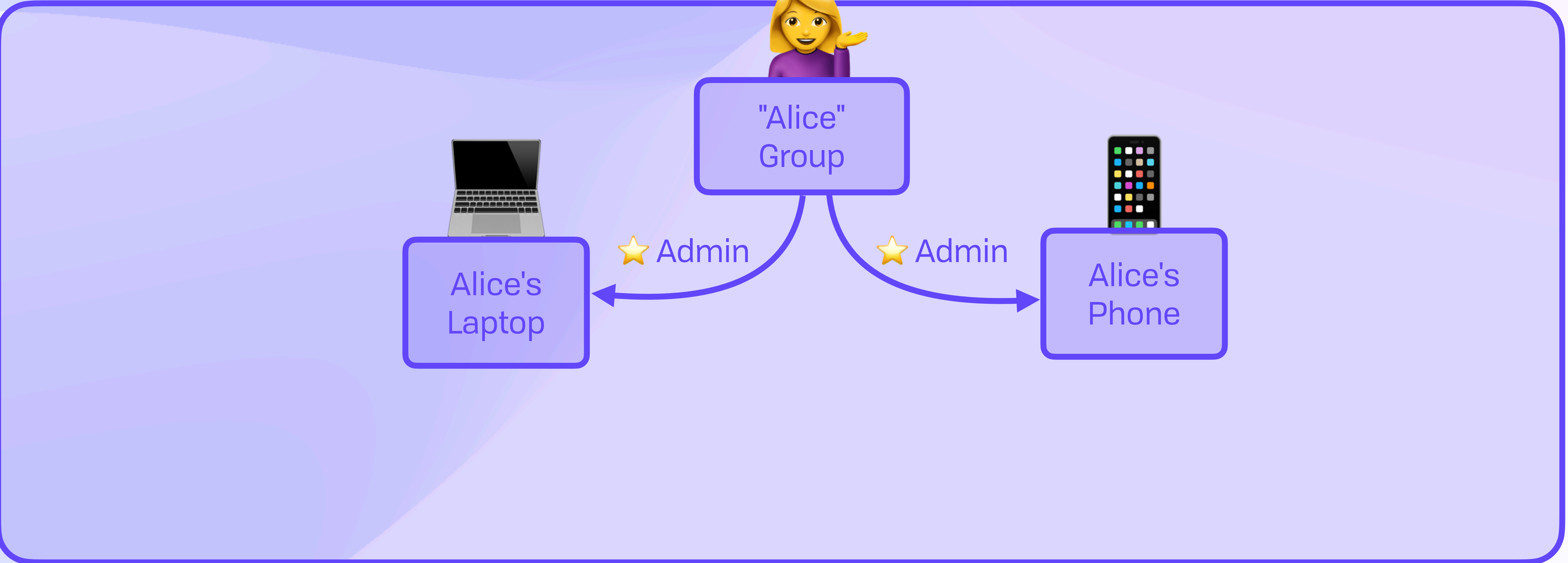
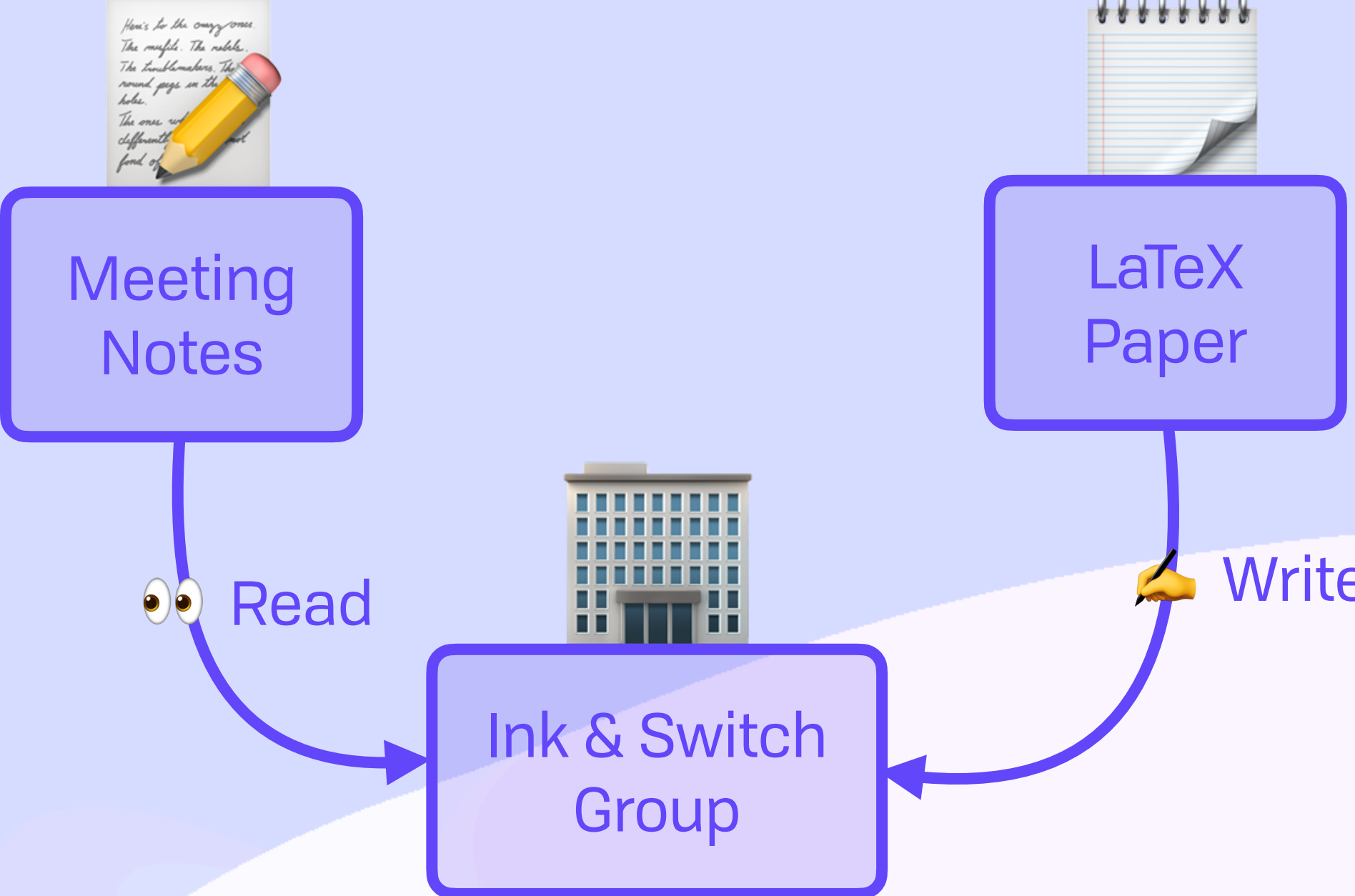


Alice's Phone



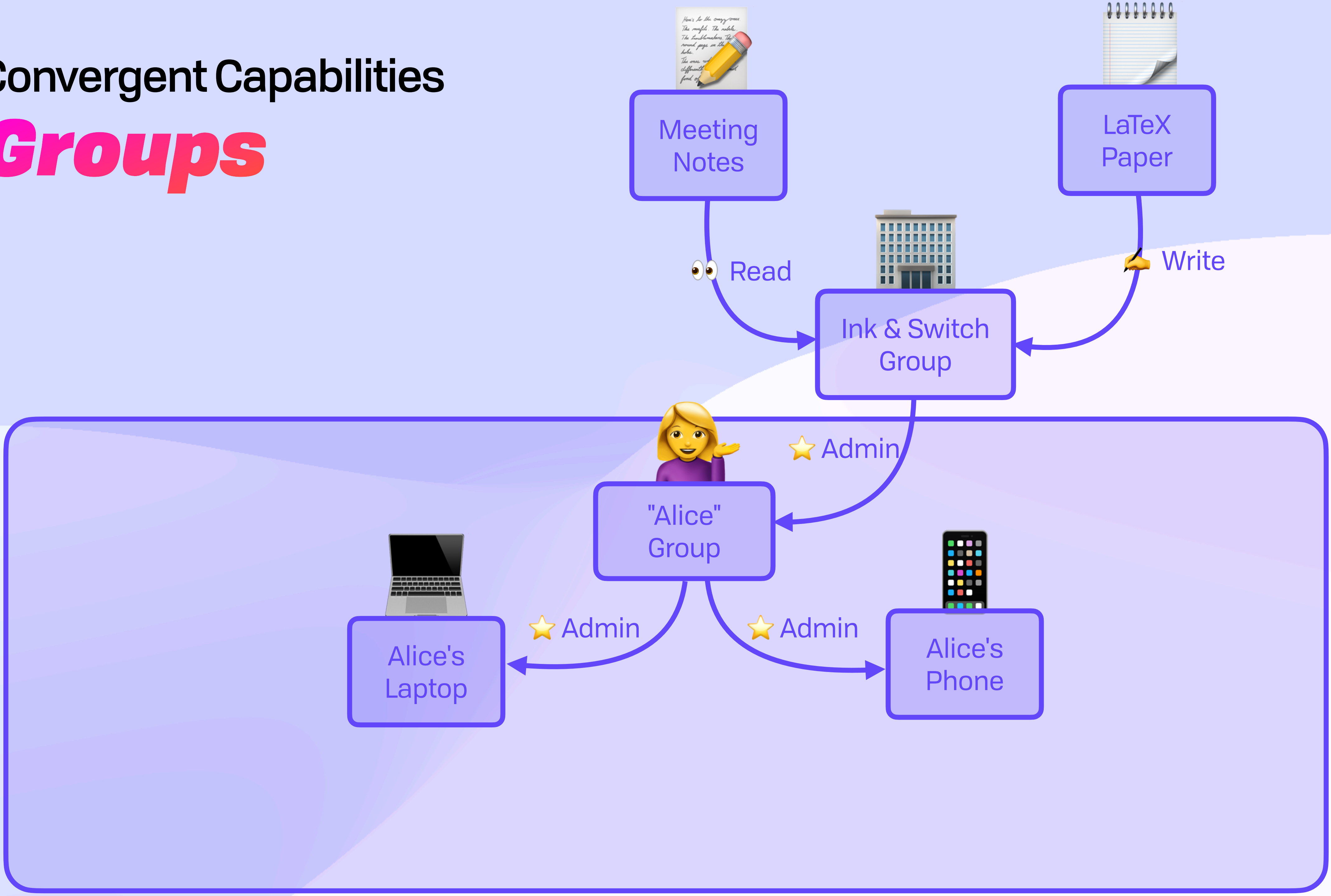
Convergent Capabilities

Groups



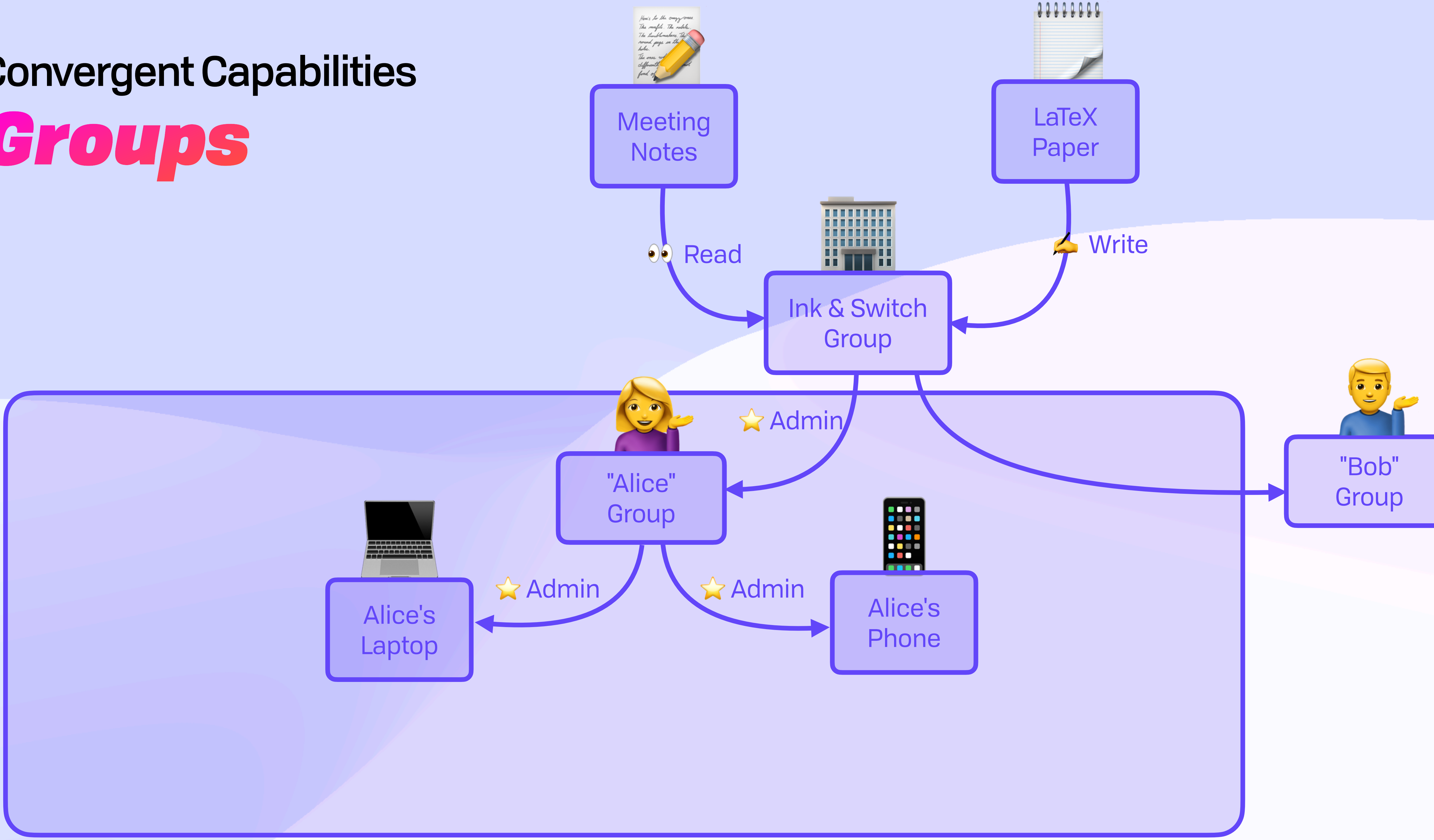
Convergent Capabilities

Groups



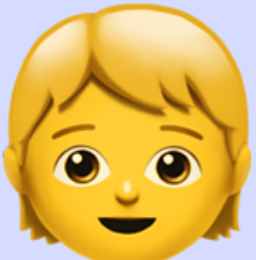
Convergent Capabilities

Groups

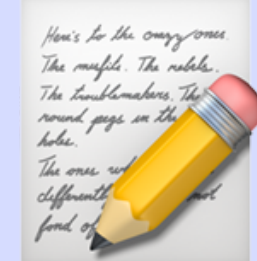


Convergent Capabilities

Groups



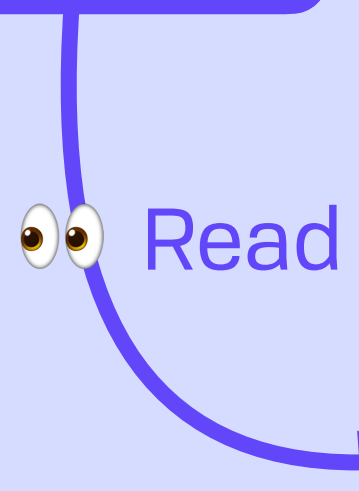
Kid's Homework
(Patchwork)



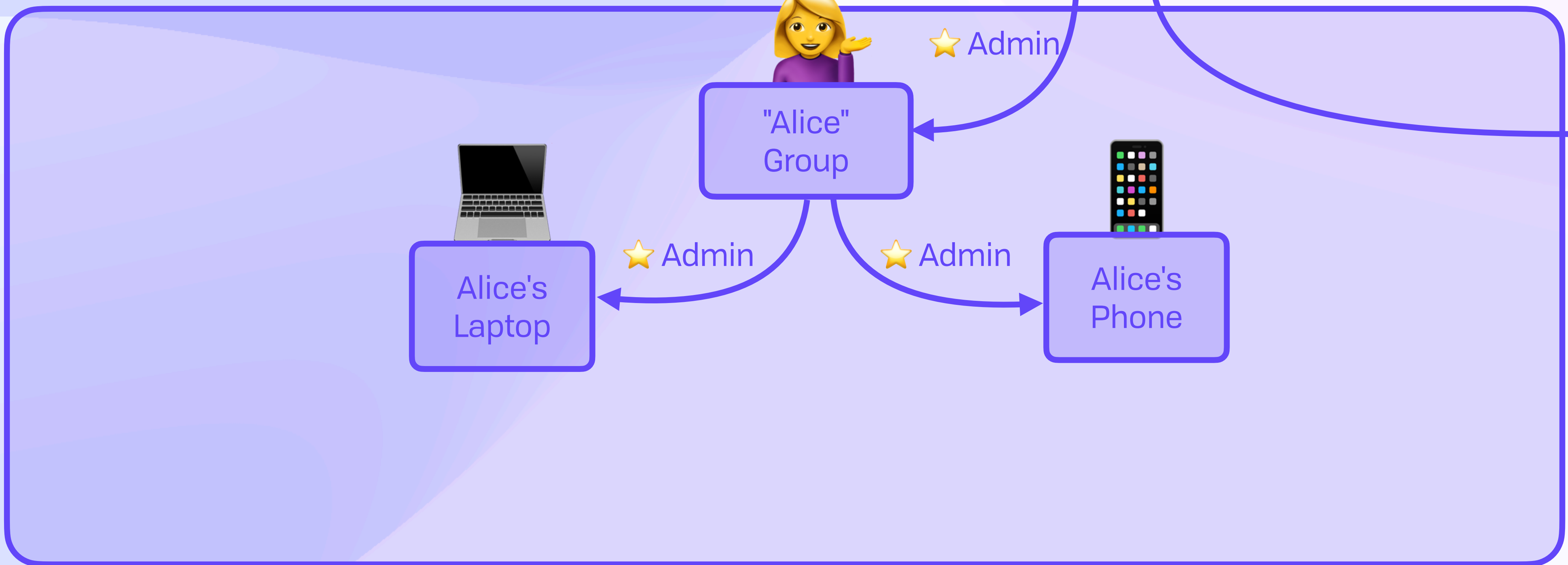
Meeting Notes



LaTeX Paper



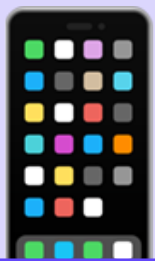
Ink & Switch
Group



"Alice"
Group



Alice's
Laptop



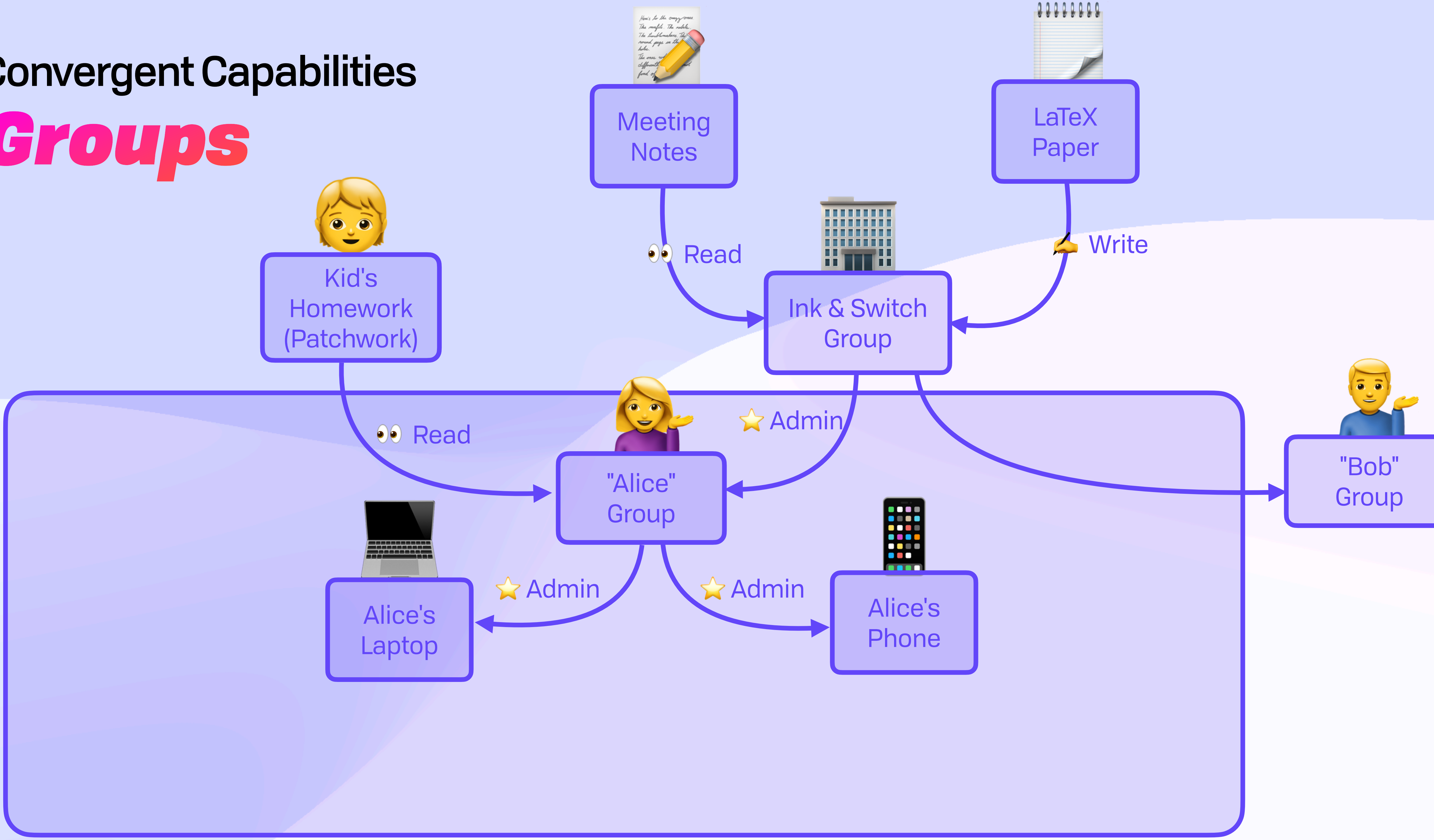
Alice's
Phone



"Bob"
Group

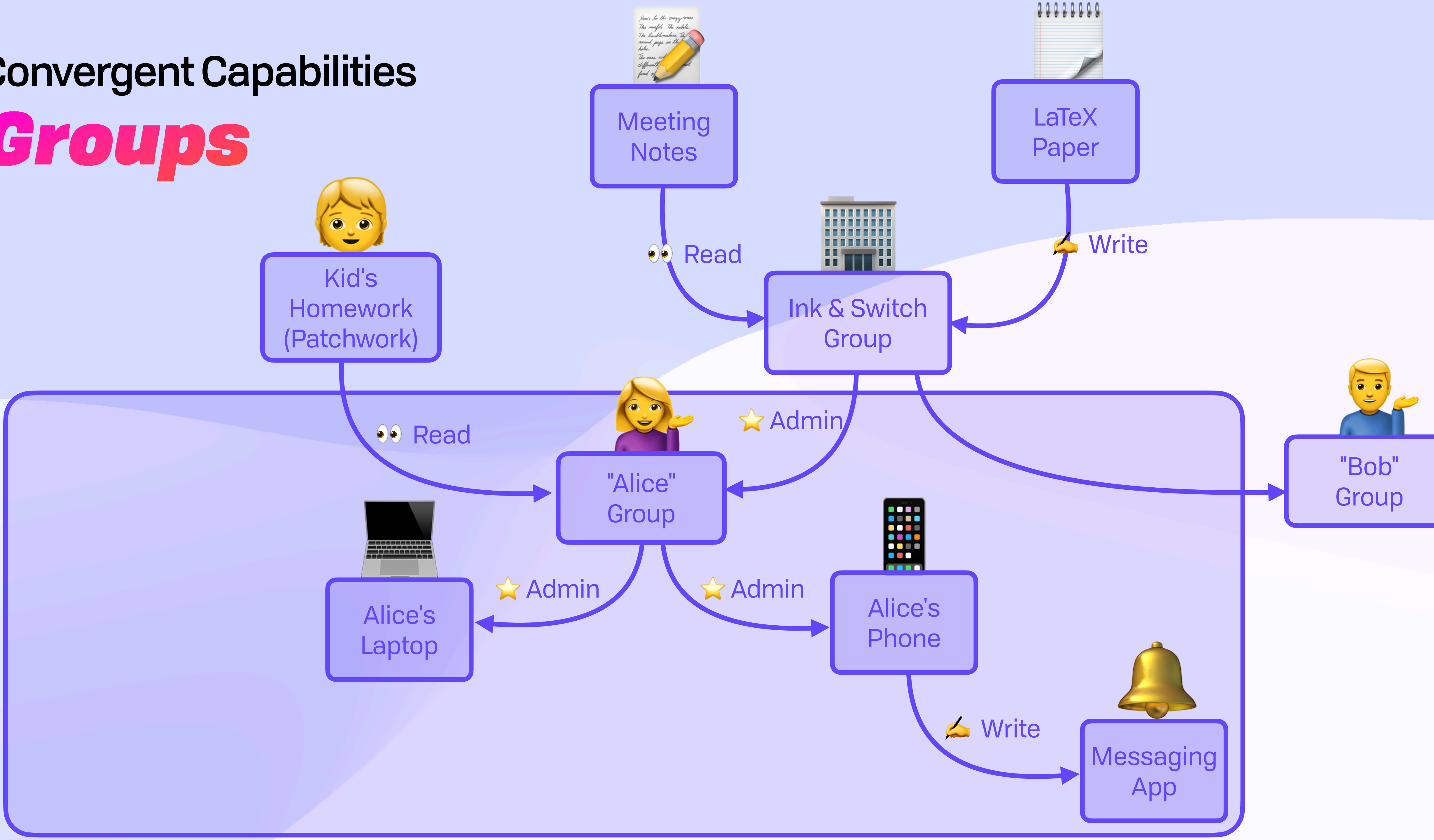
Convergent Capabilities

Groups



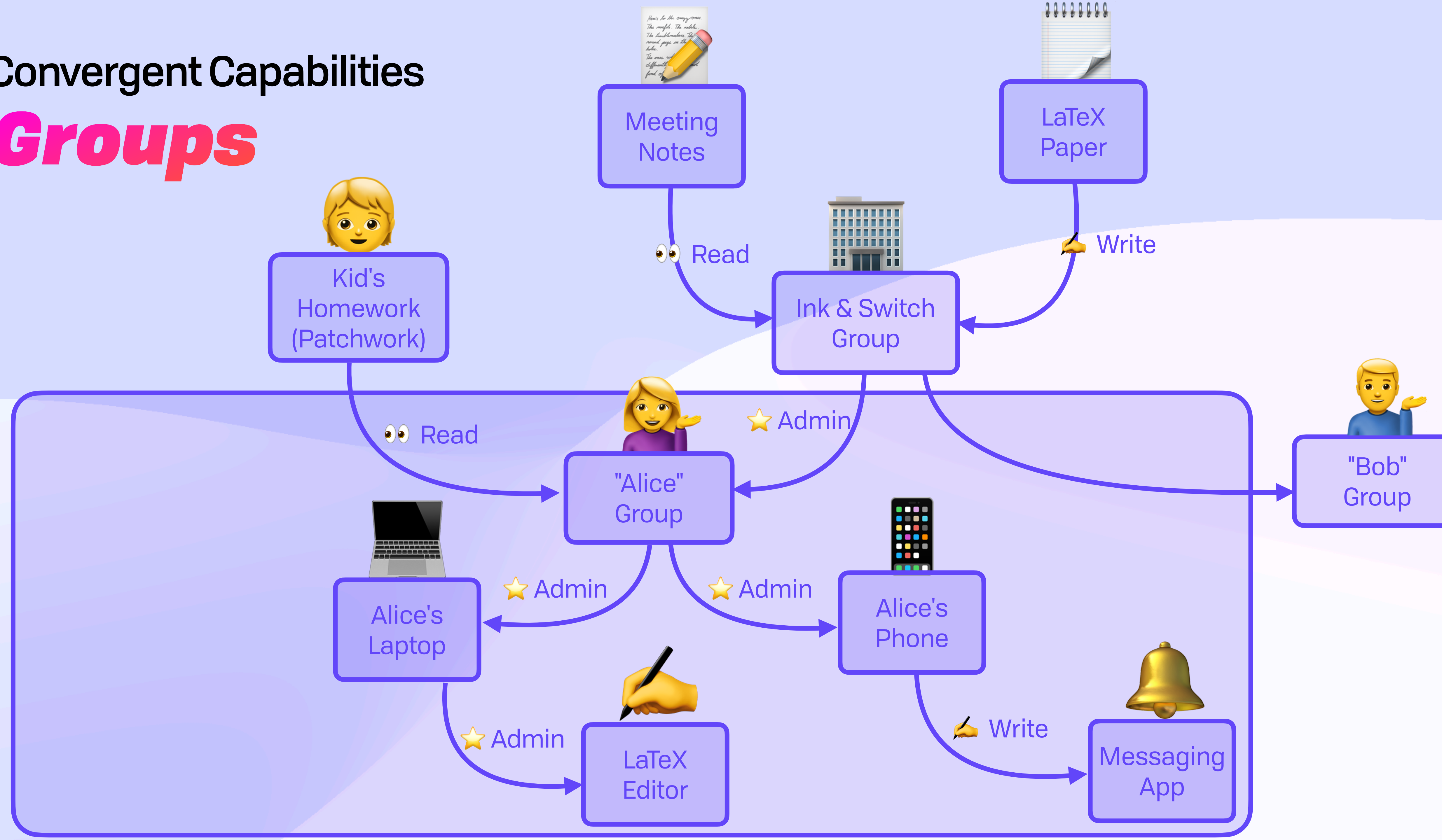
Convergent Capabilities

Groups



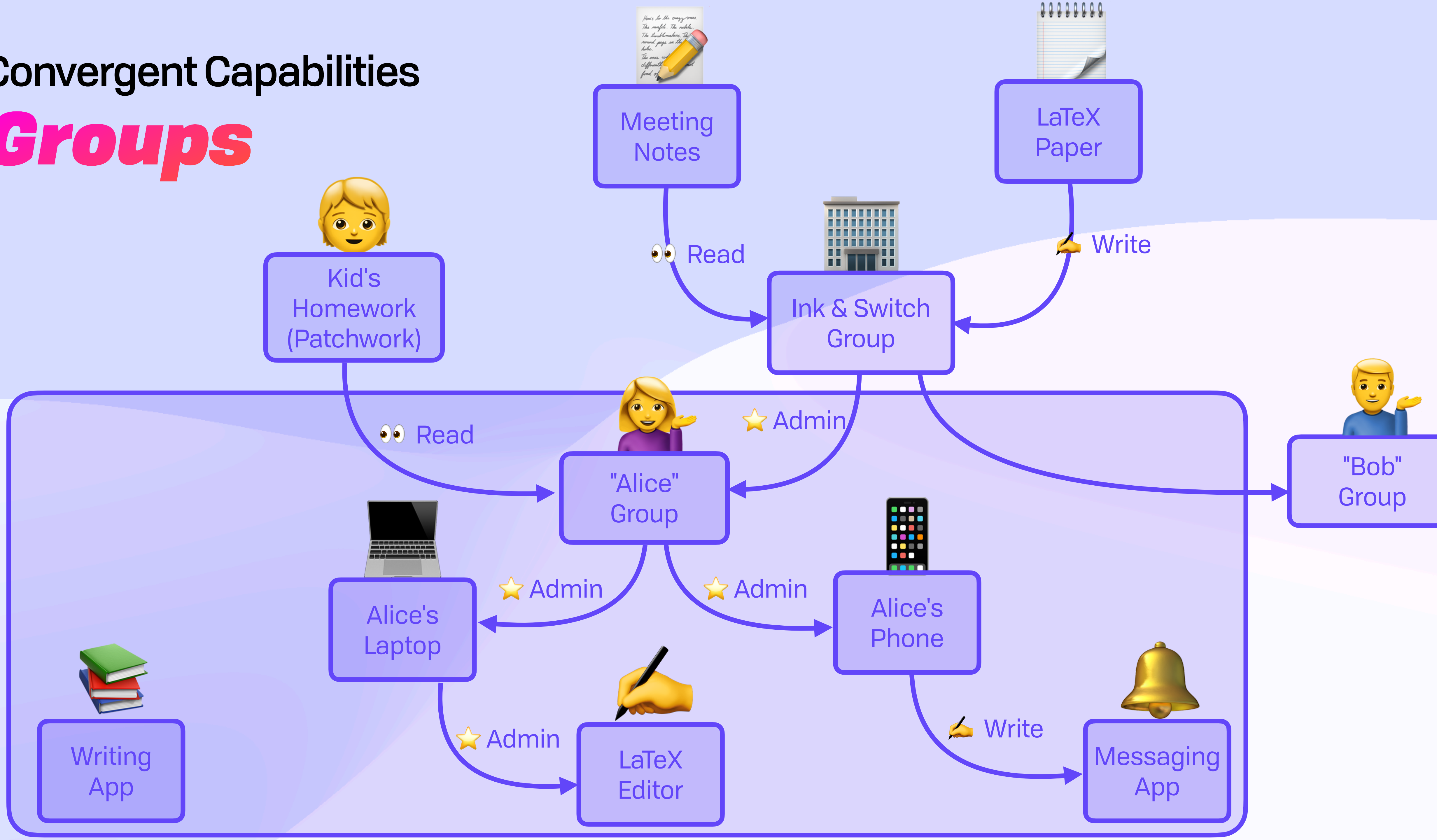
Convergent Capabilities

Groups



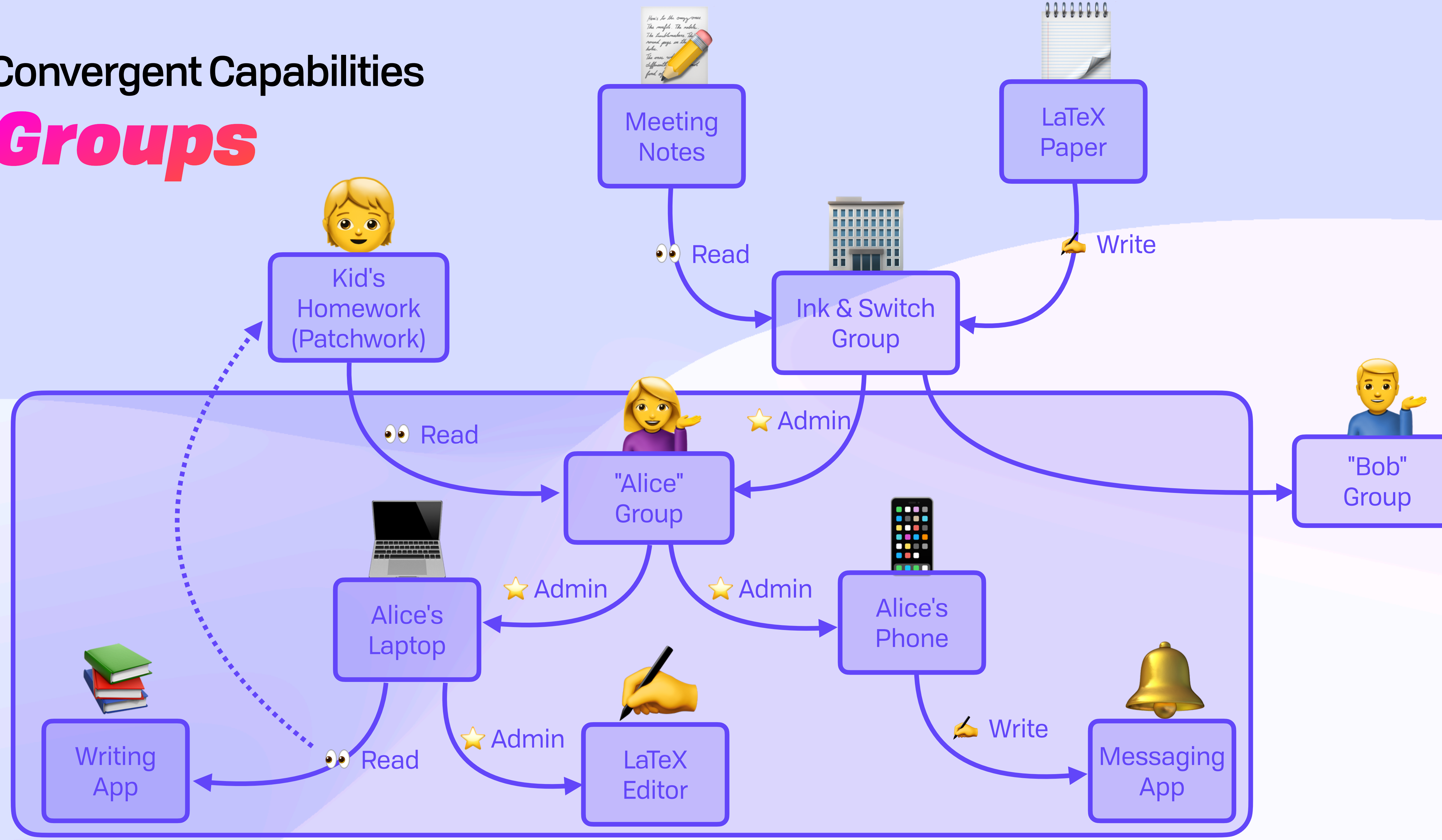
Convergent Capabilities

Groups



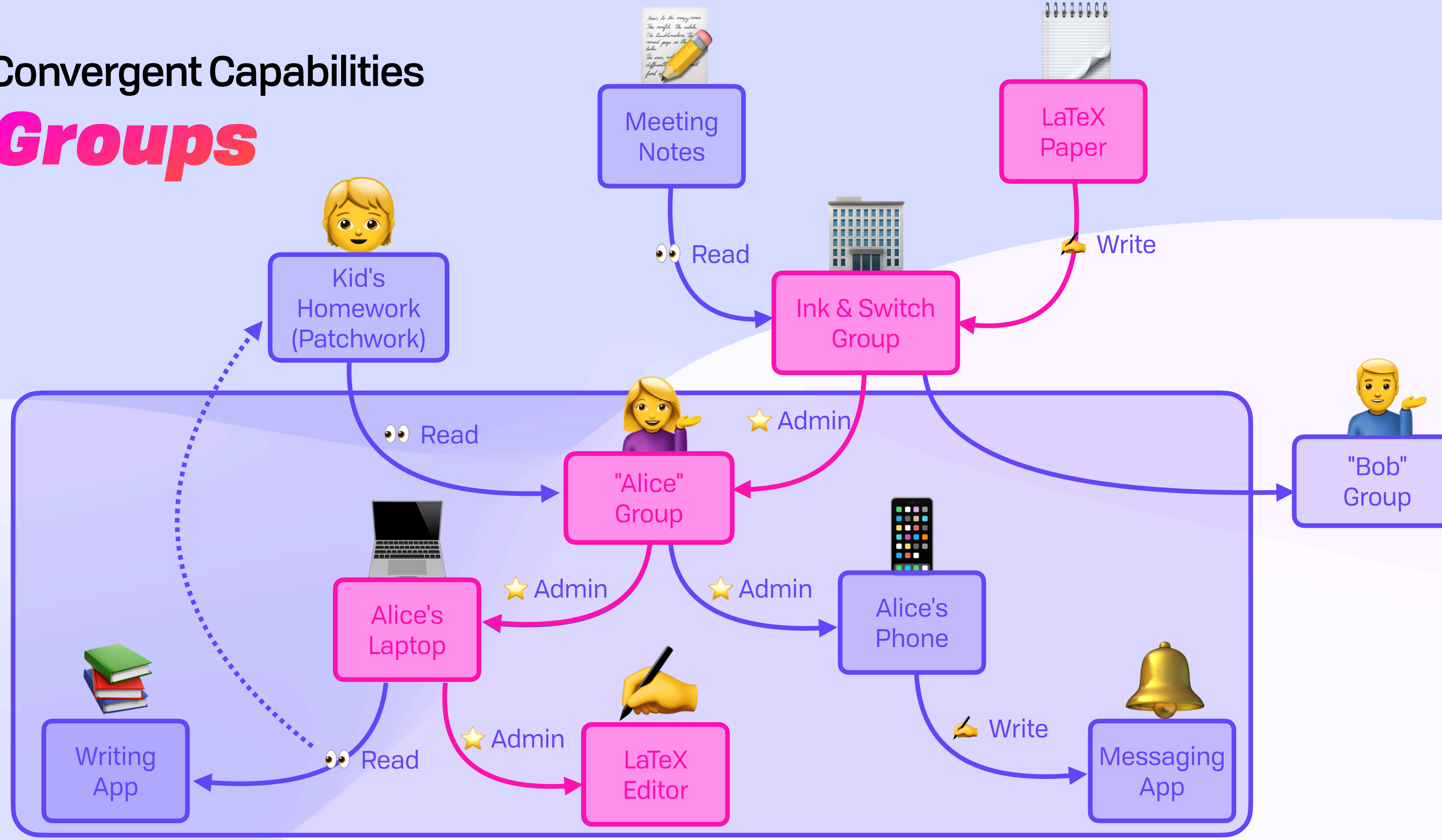
Convergent Capabilities

Groups



Convergent Capabilities

Groups



Convergent Capabilities

Causal Encryption

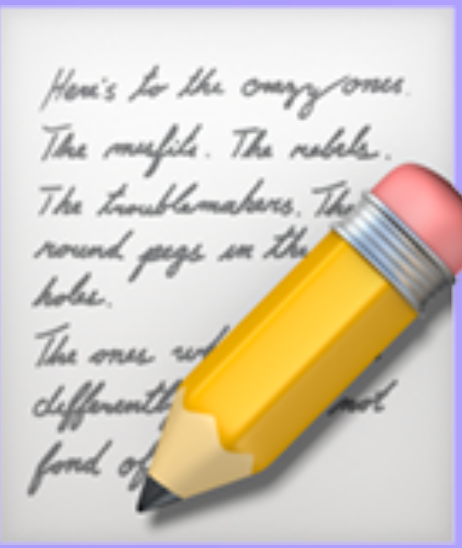
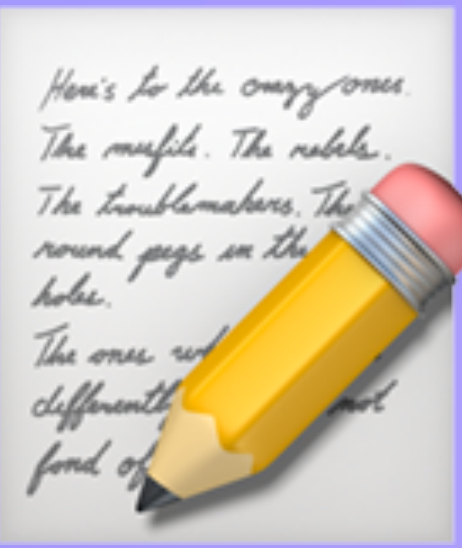
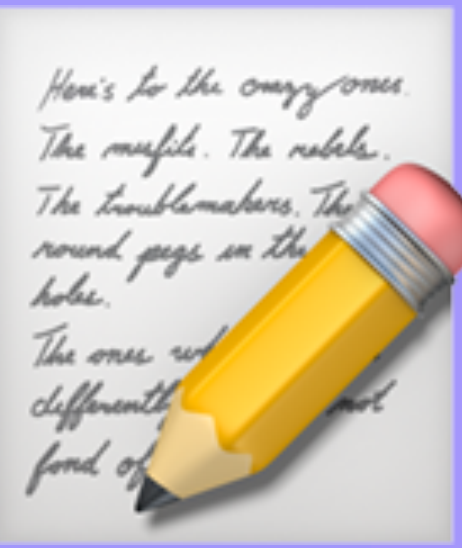
Convergent Capabilities

Causal Encryption



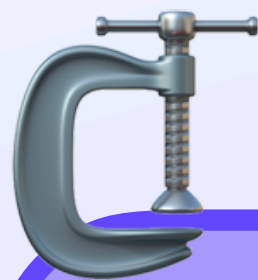
Convergent Capabilities

Causal Encryption



Convergent Capabilities

Causal Encryption



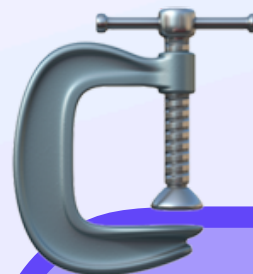
Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of

Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of

Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of

Convergent Capabilities

Causal Encryption



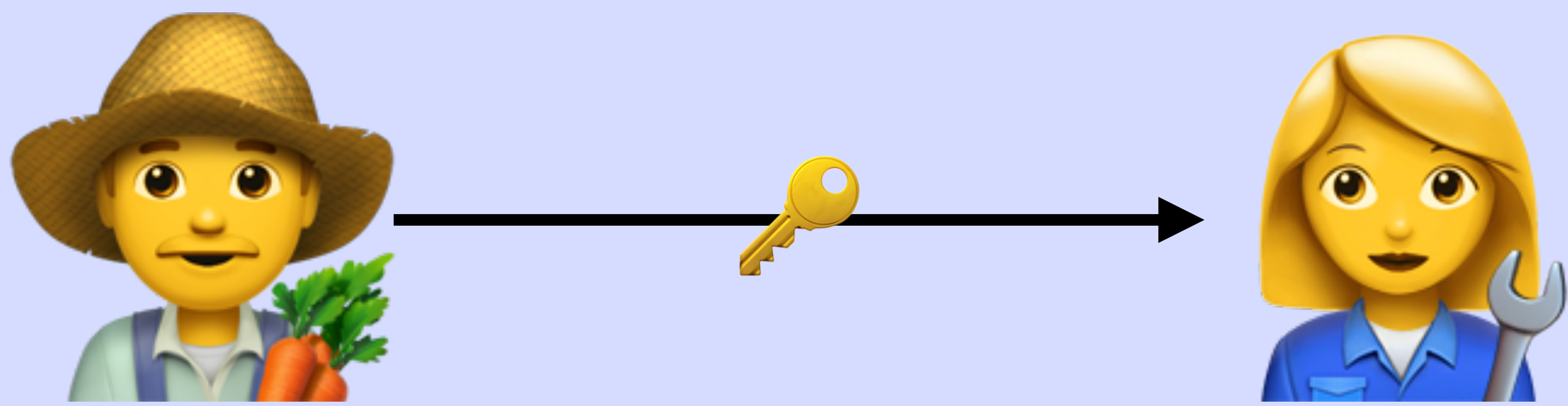
Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of

Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of

Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of

Convergent Capabilities

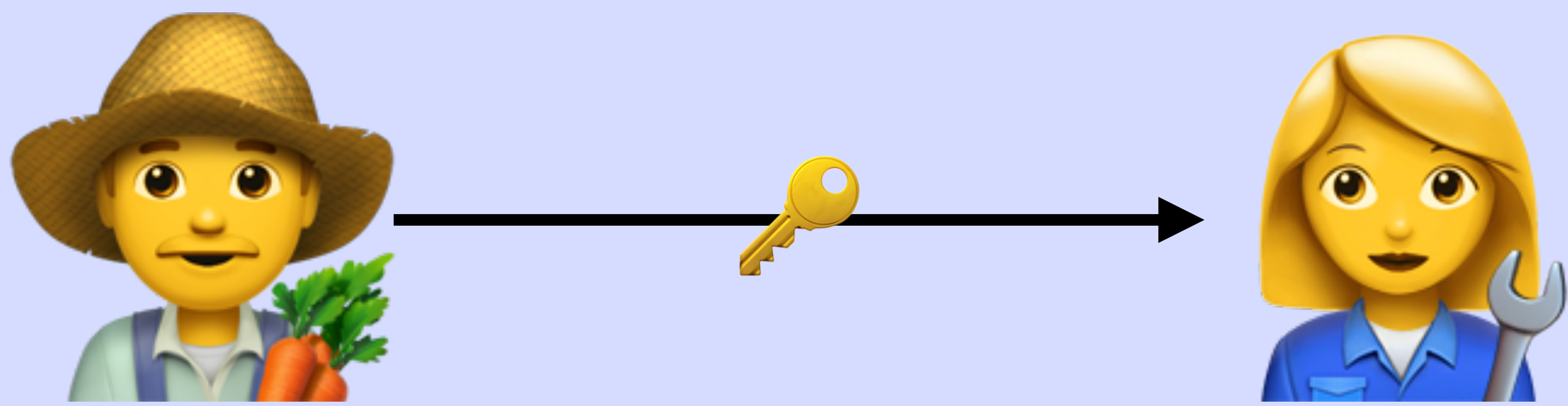
Causal Encryption

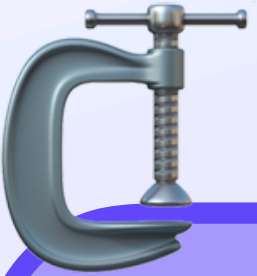
A purple rounded rectangle containing several icons. At the top center is a metal padlock with a yellow key inserted. To the left of the padlock is a metal clamp. Below the padlock are three identical notepad icons, each with a yellow pencil resting on it. The notepads contain handwritten text in cursive script.

Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of

Convergent Capabilities

Causal Encryption







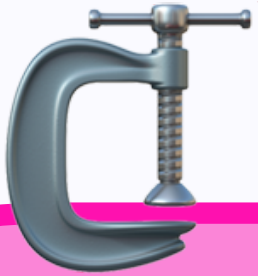
Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of



Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of

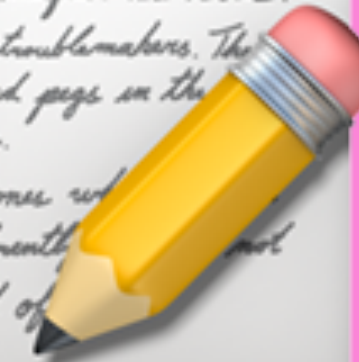


Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of





Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of



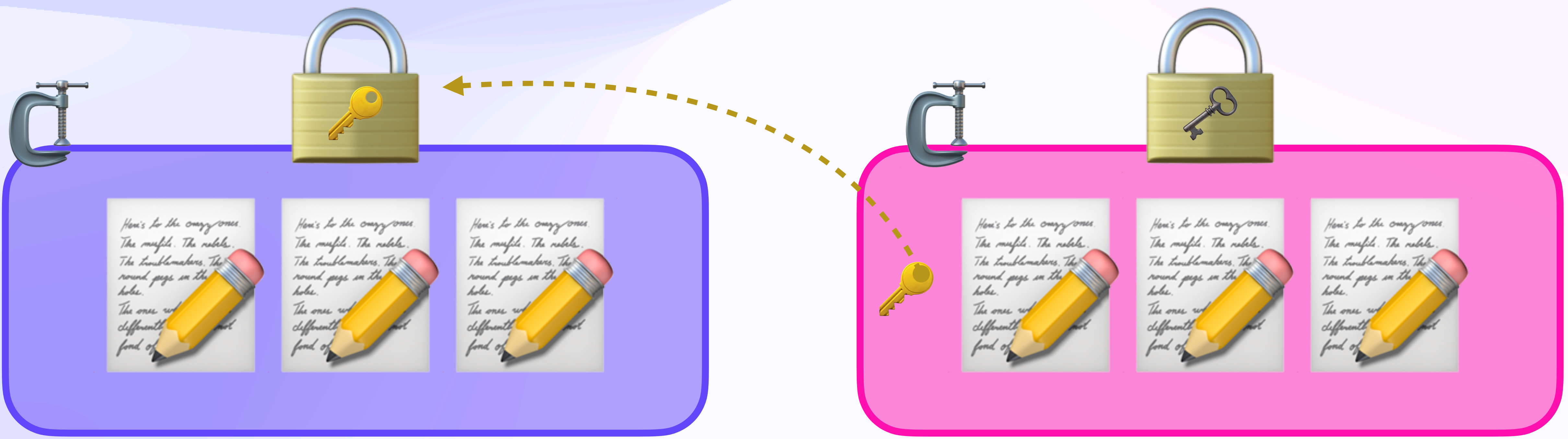
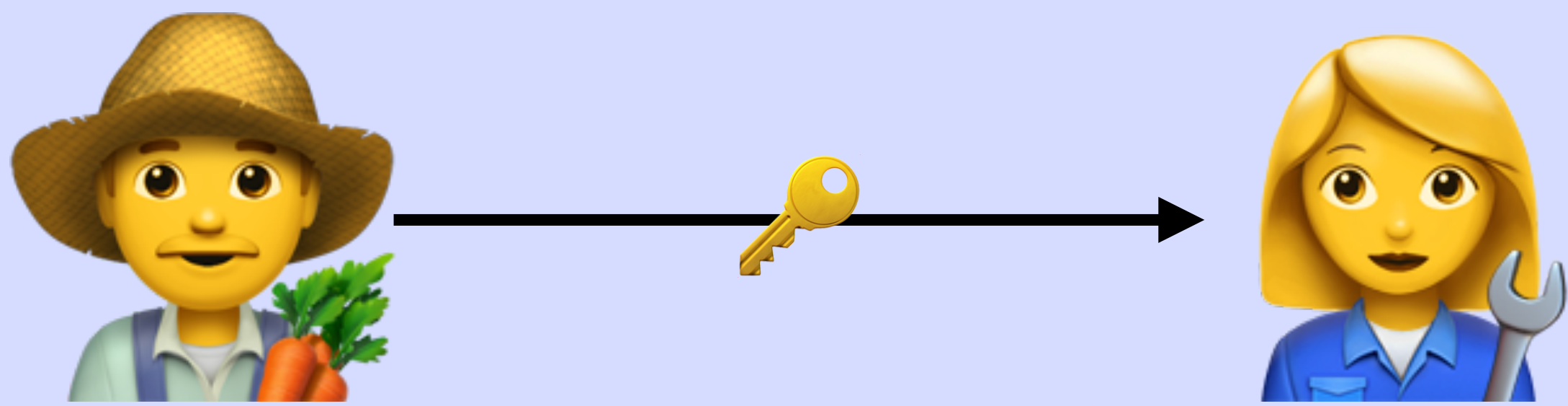
Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of



Here's to the crazy ones.
The mavericks. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones who
different. They're not
fond of

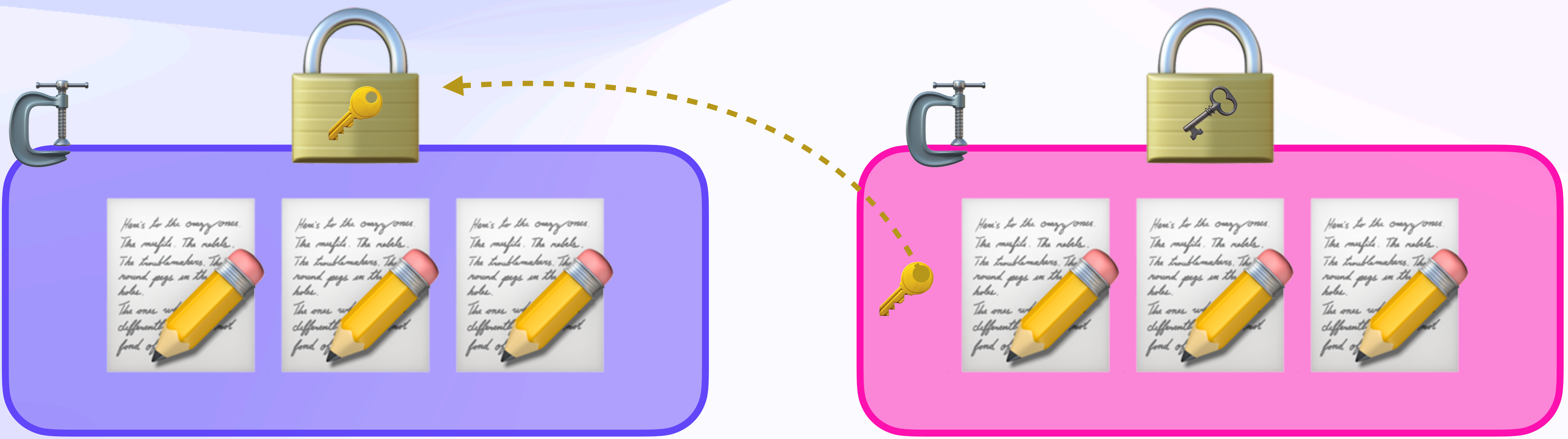
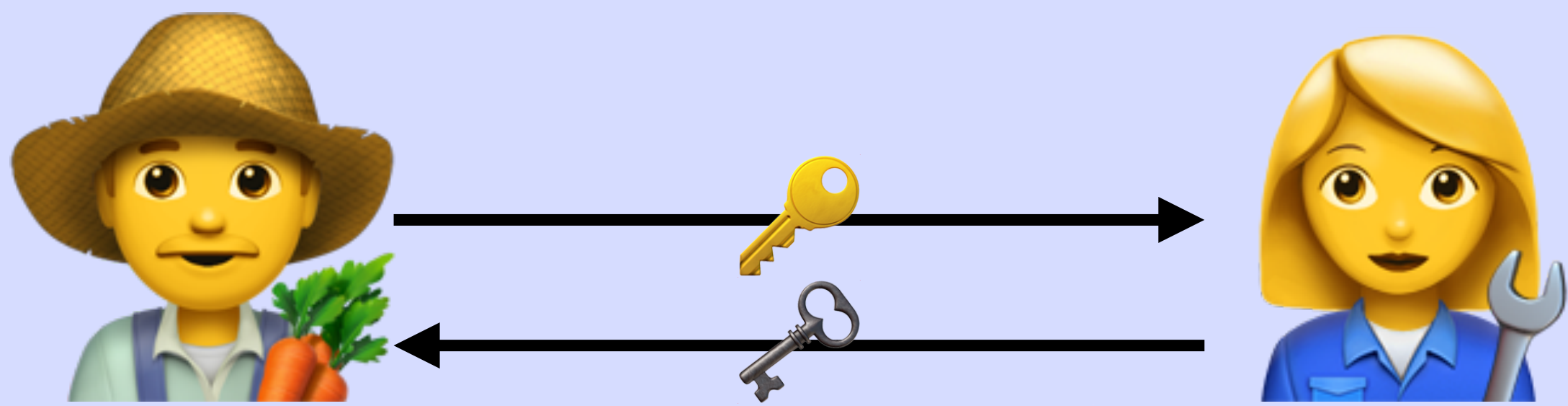
Convergent Capabilities

Causal Encryption



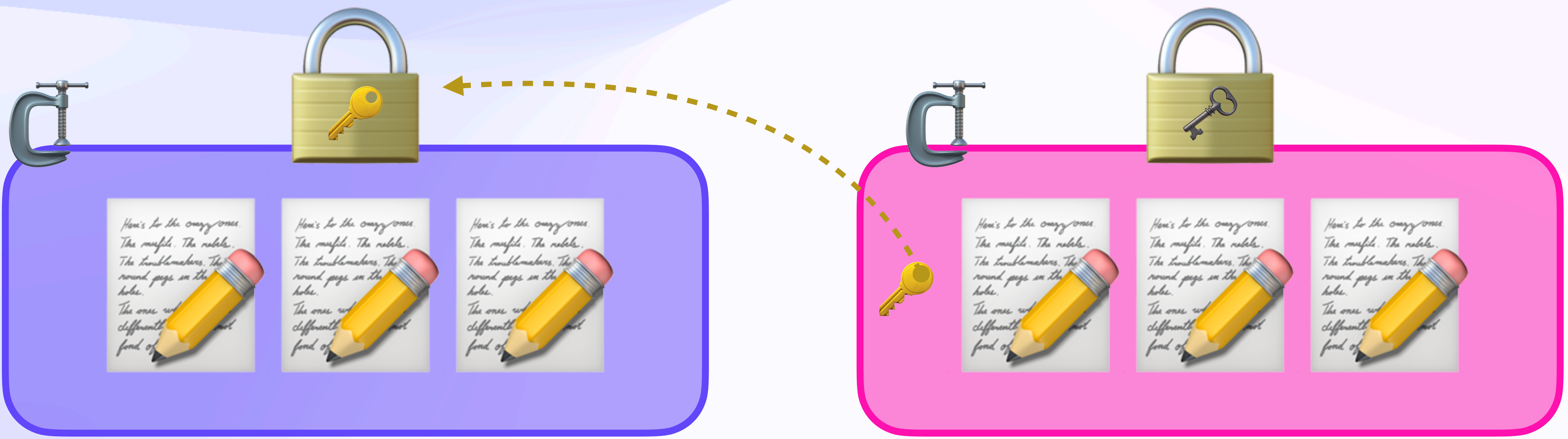
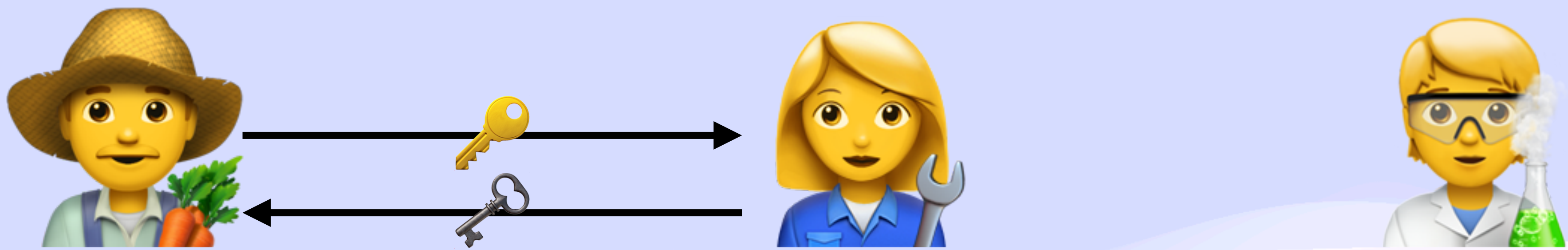
Convergent Capabilities

Causal Encryption



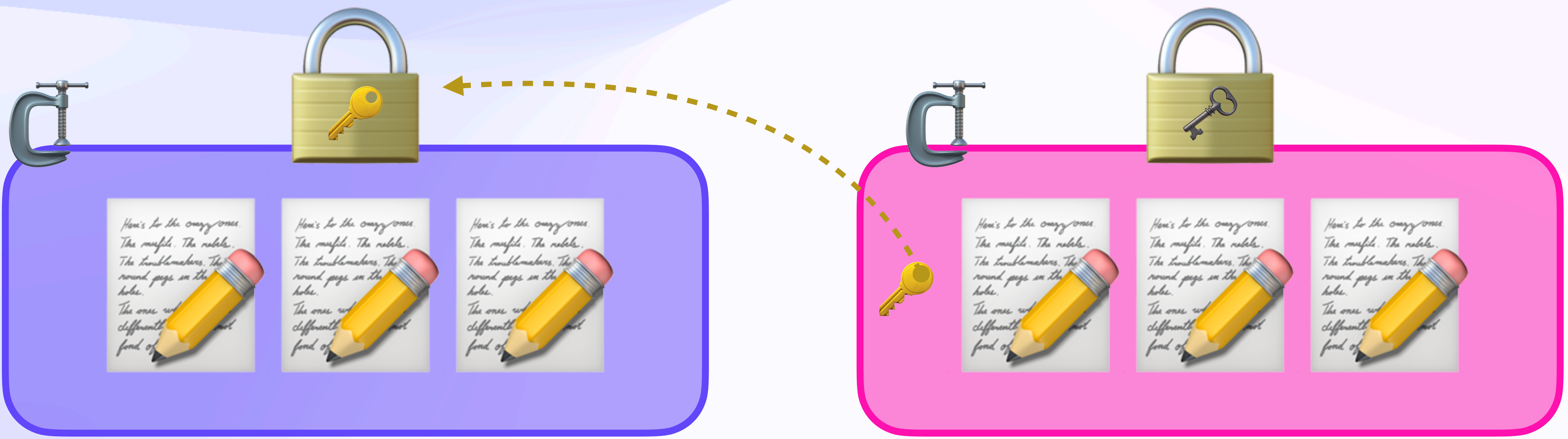
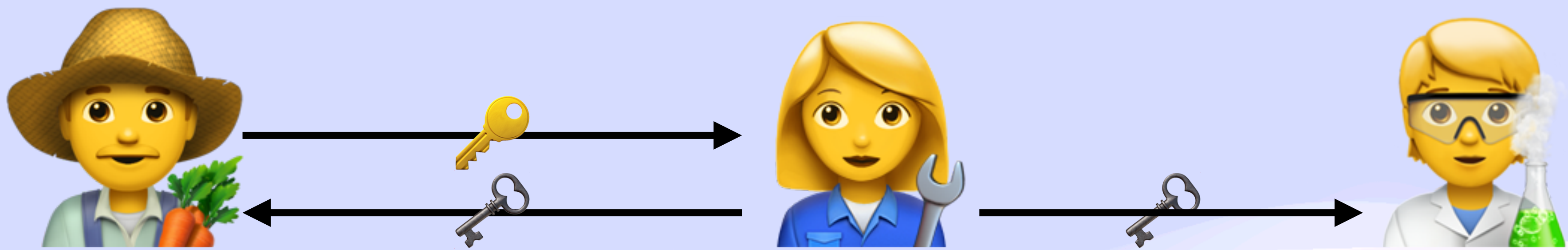
Convergent Capabilities

Causal Encryption



Convergent Capabilities

Causal Encryption



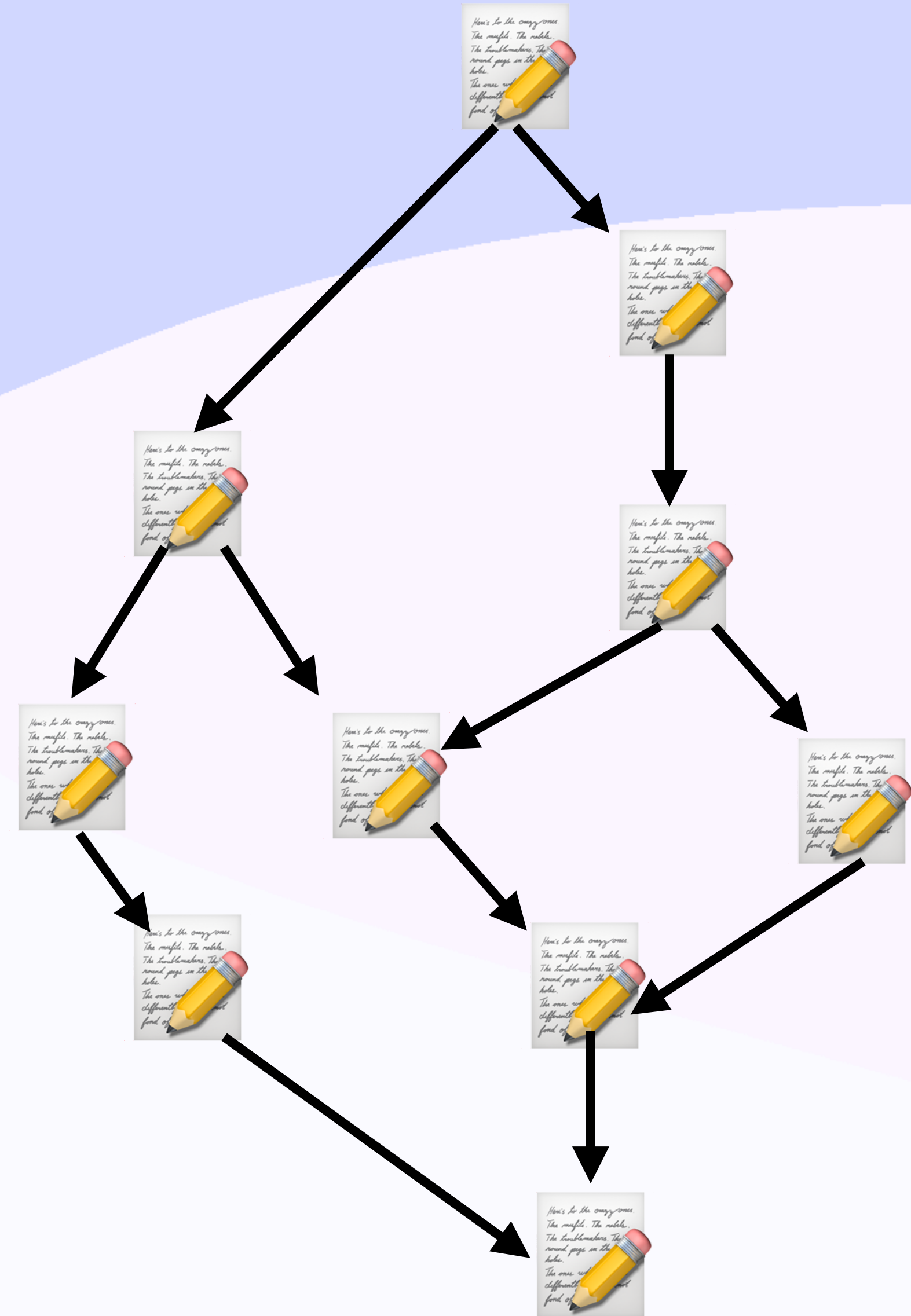
Rejection in the Face of Backdating

Revocation



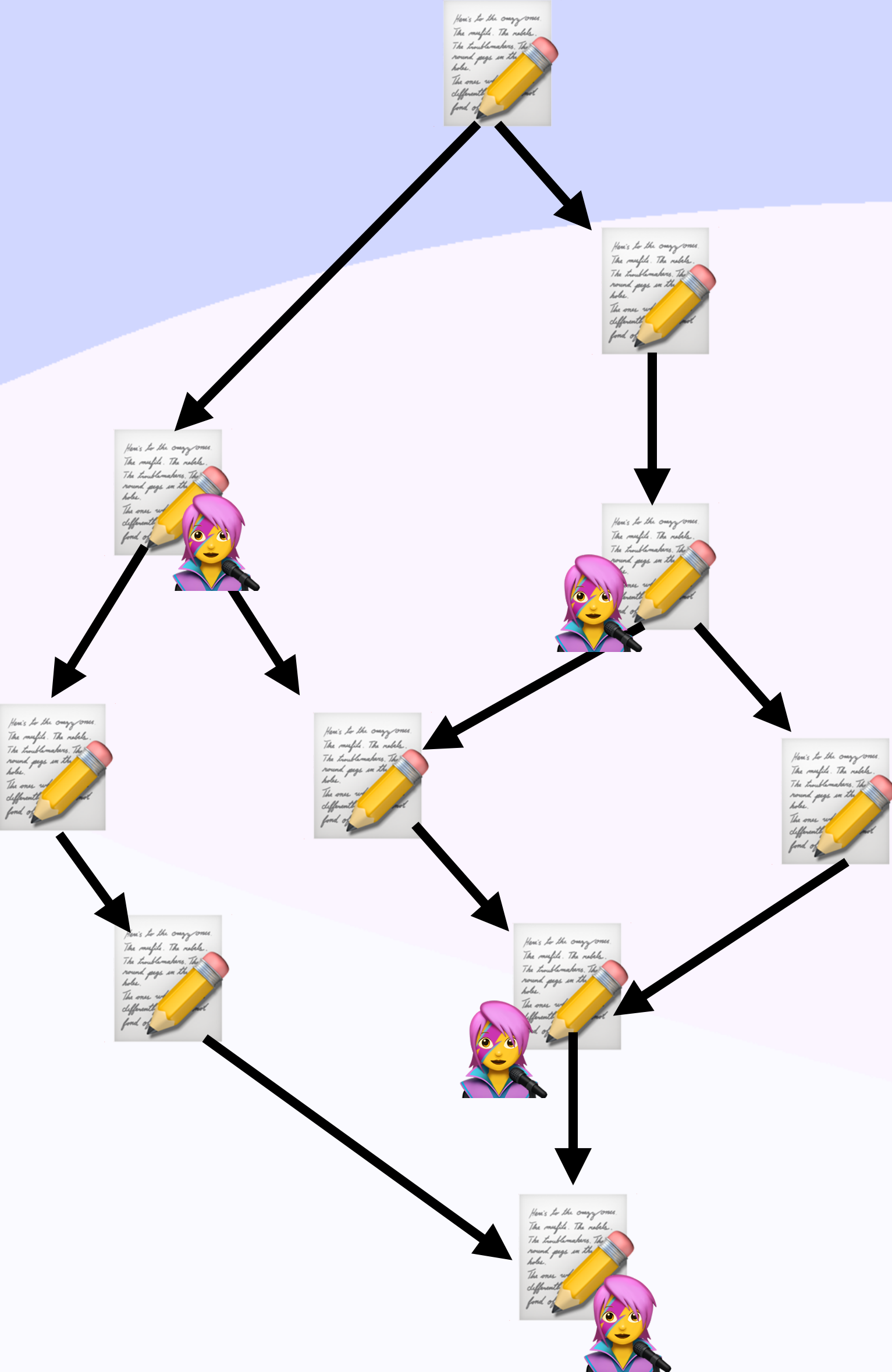
Revocation

Causal Operations



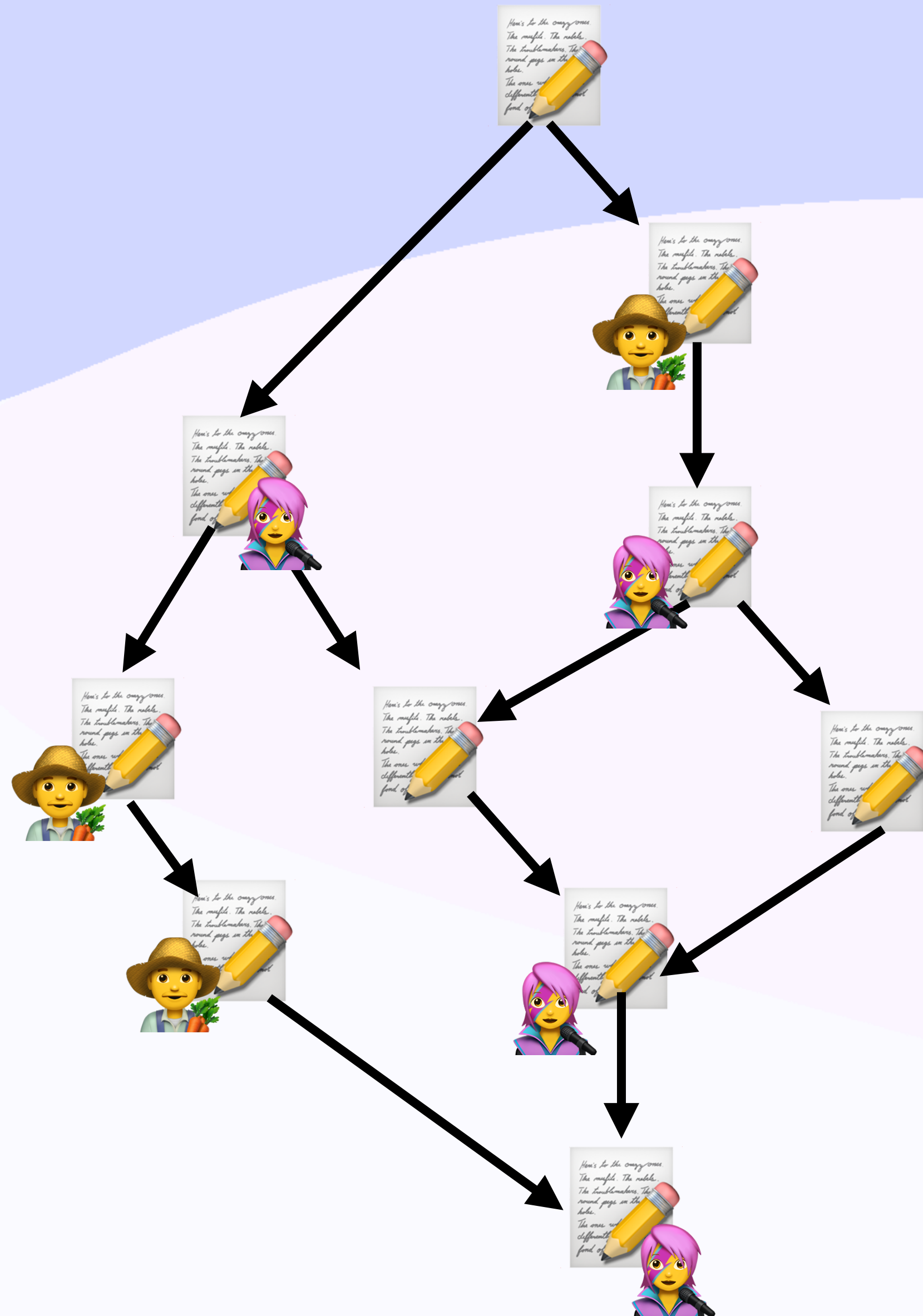
Revocation

Causal Operations



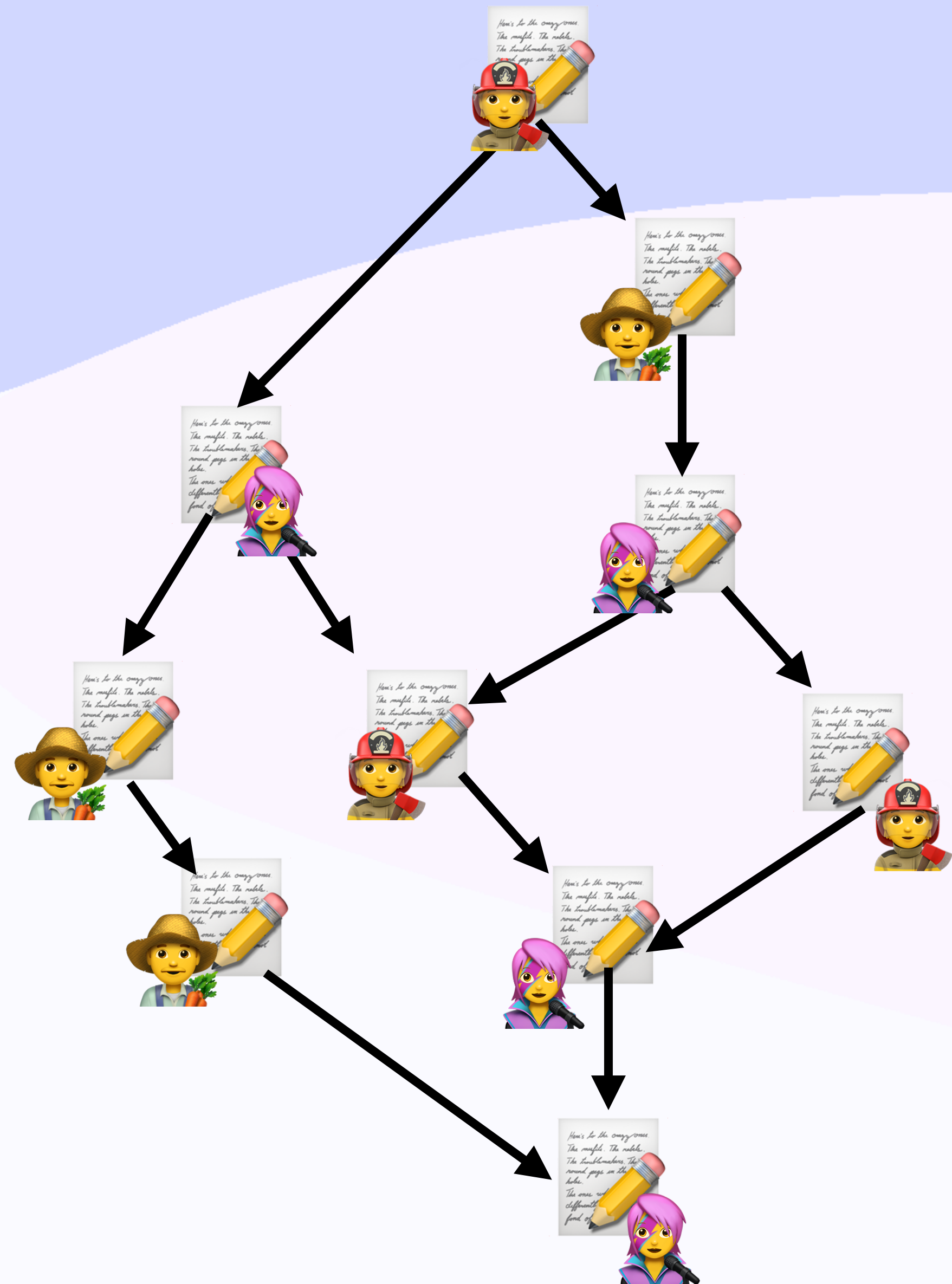
Revocation

Causal Operations

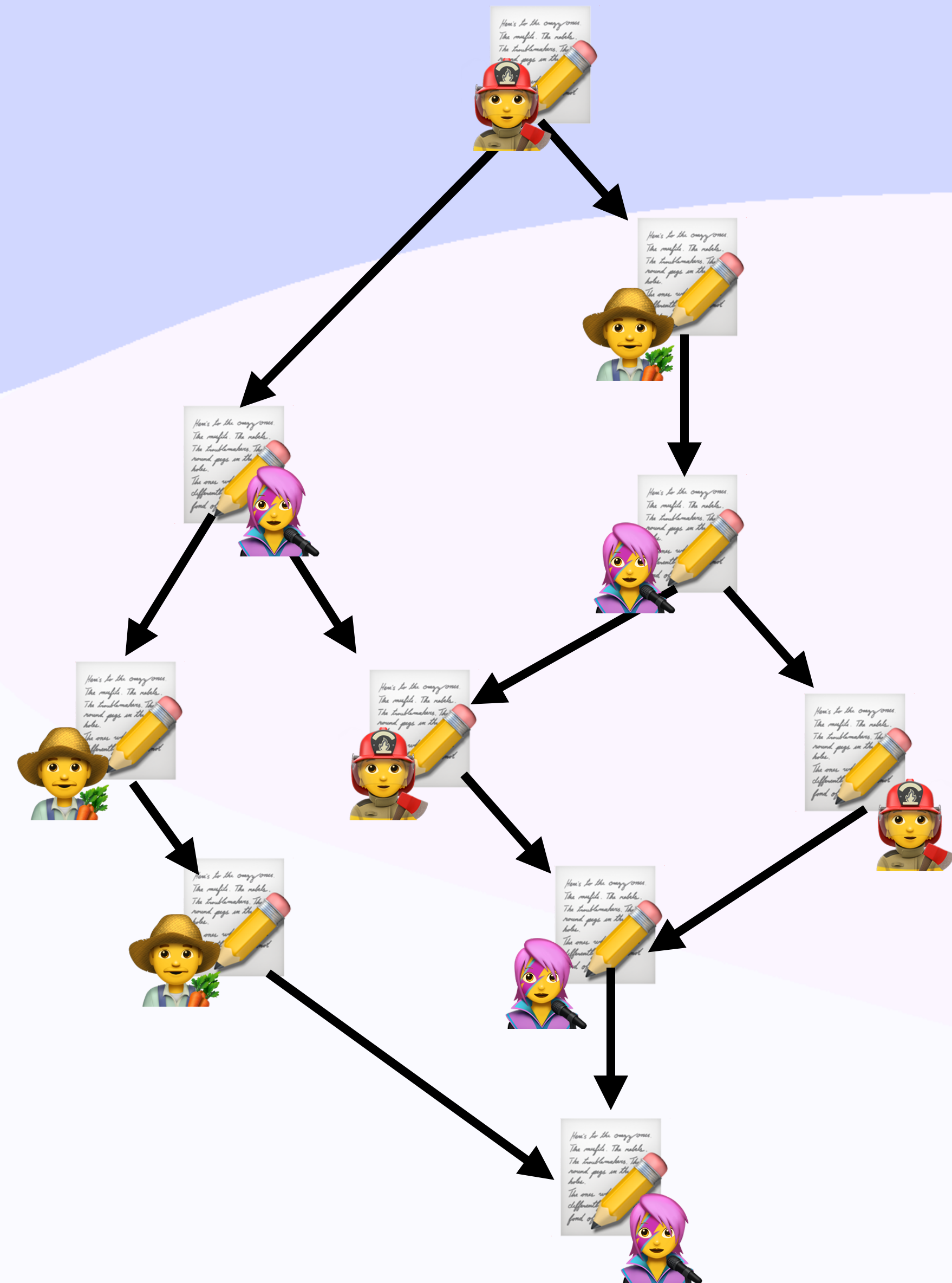


Revocation

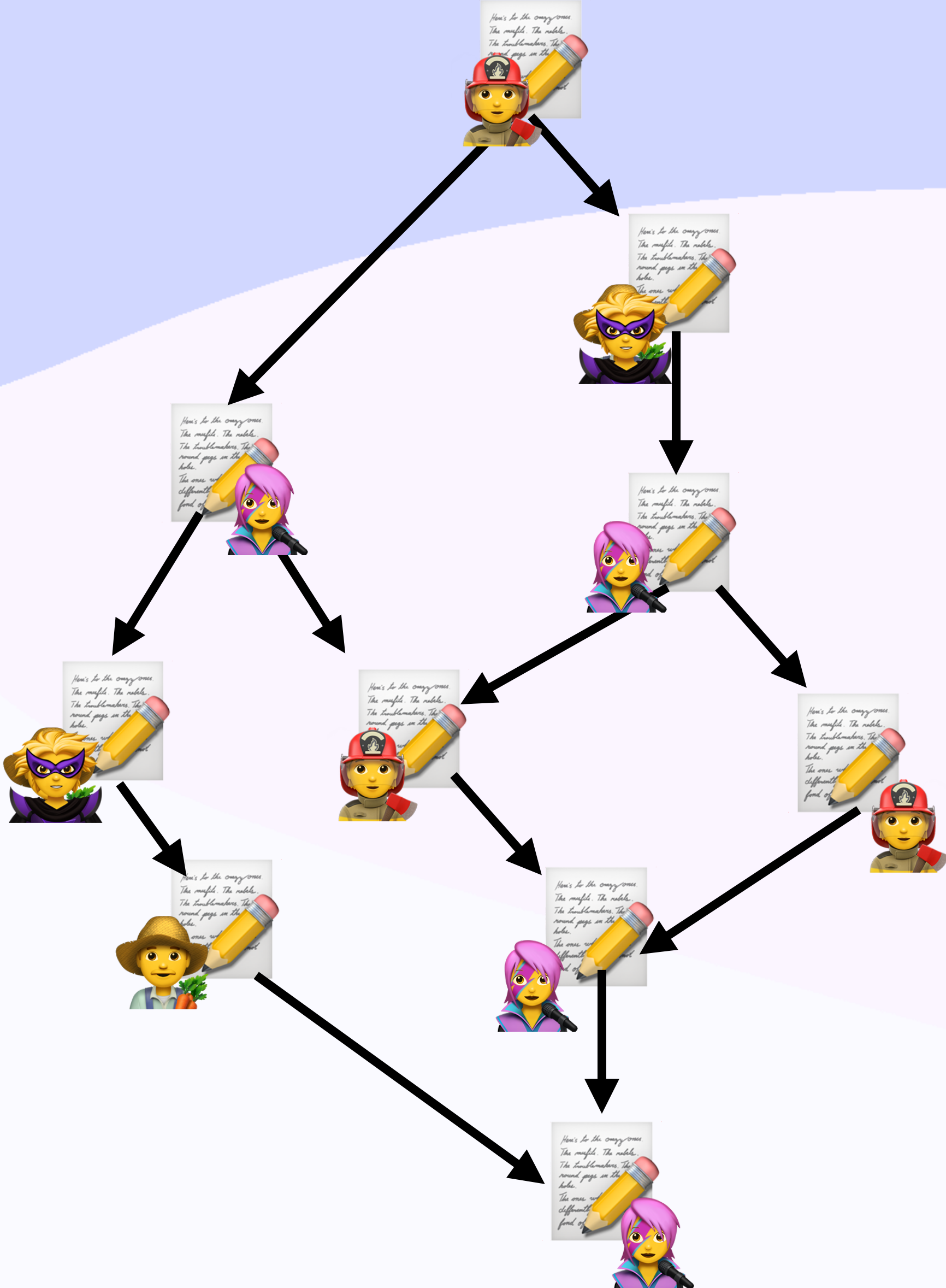
Causal Operations



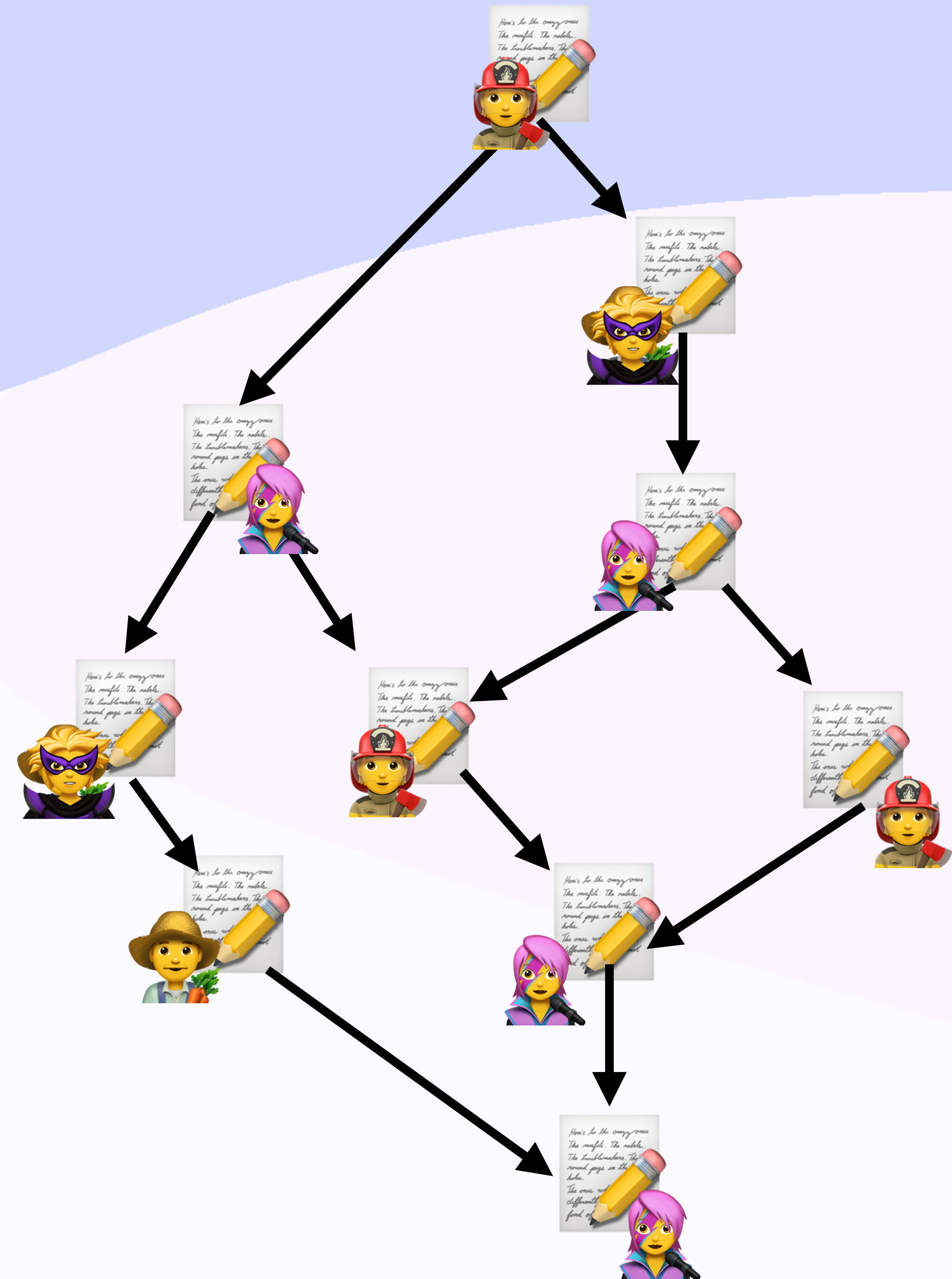
Causal Operations



Causal Operations

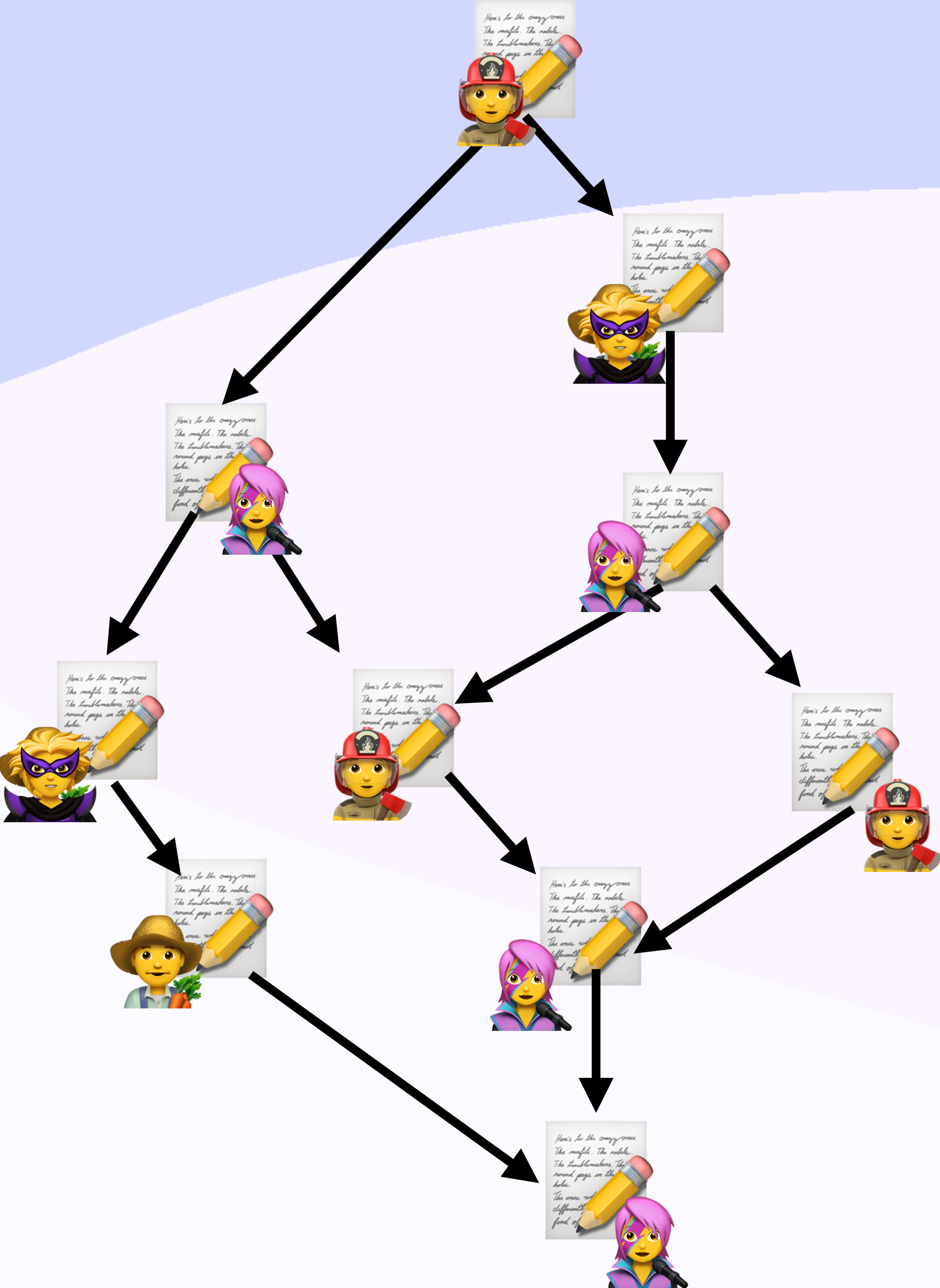


Causal Operations



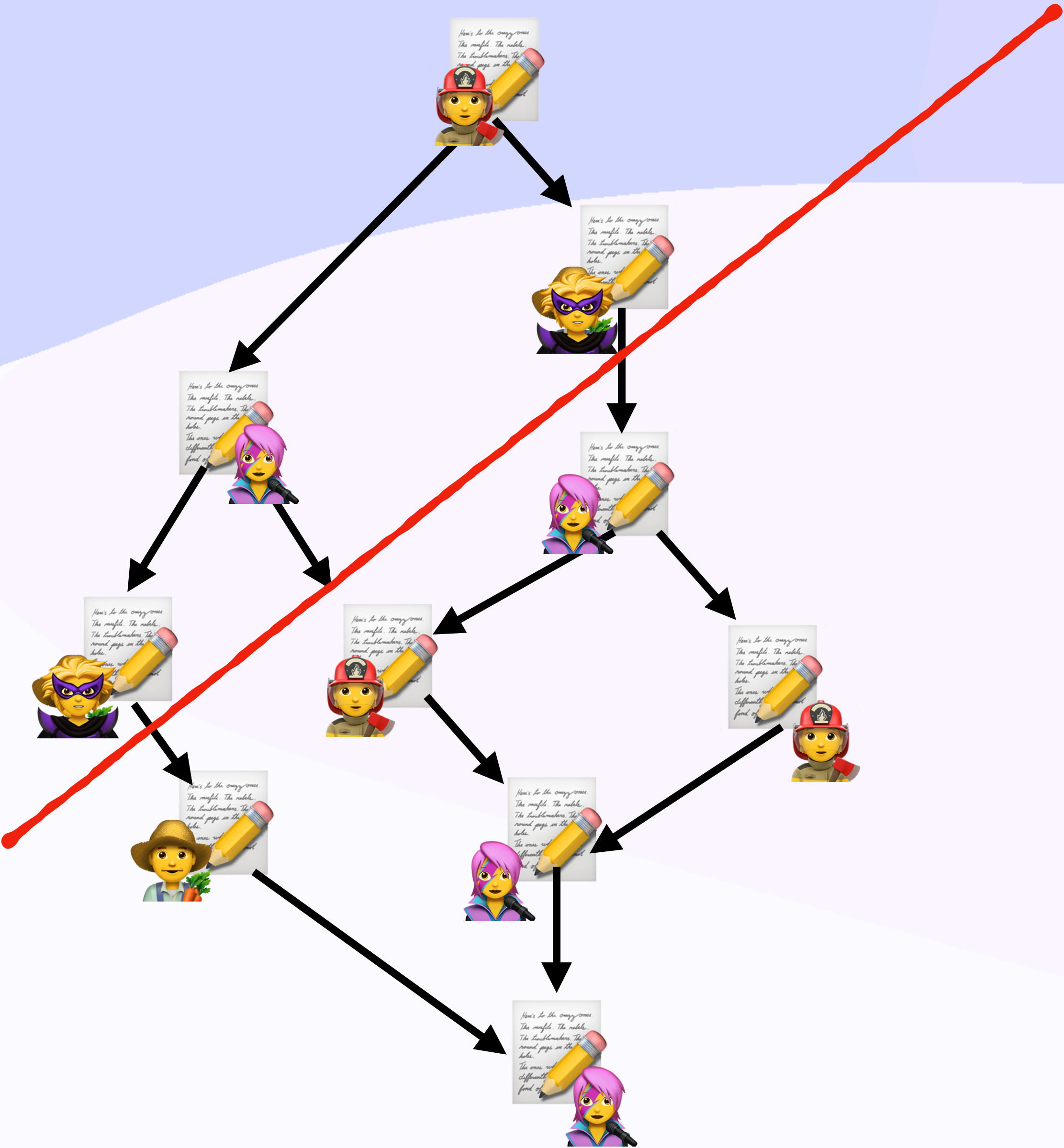
Revocation

Naïve Tombstoning



Revocation

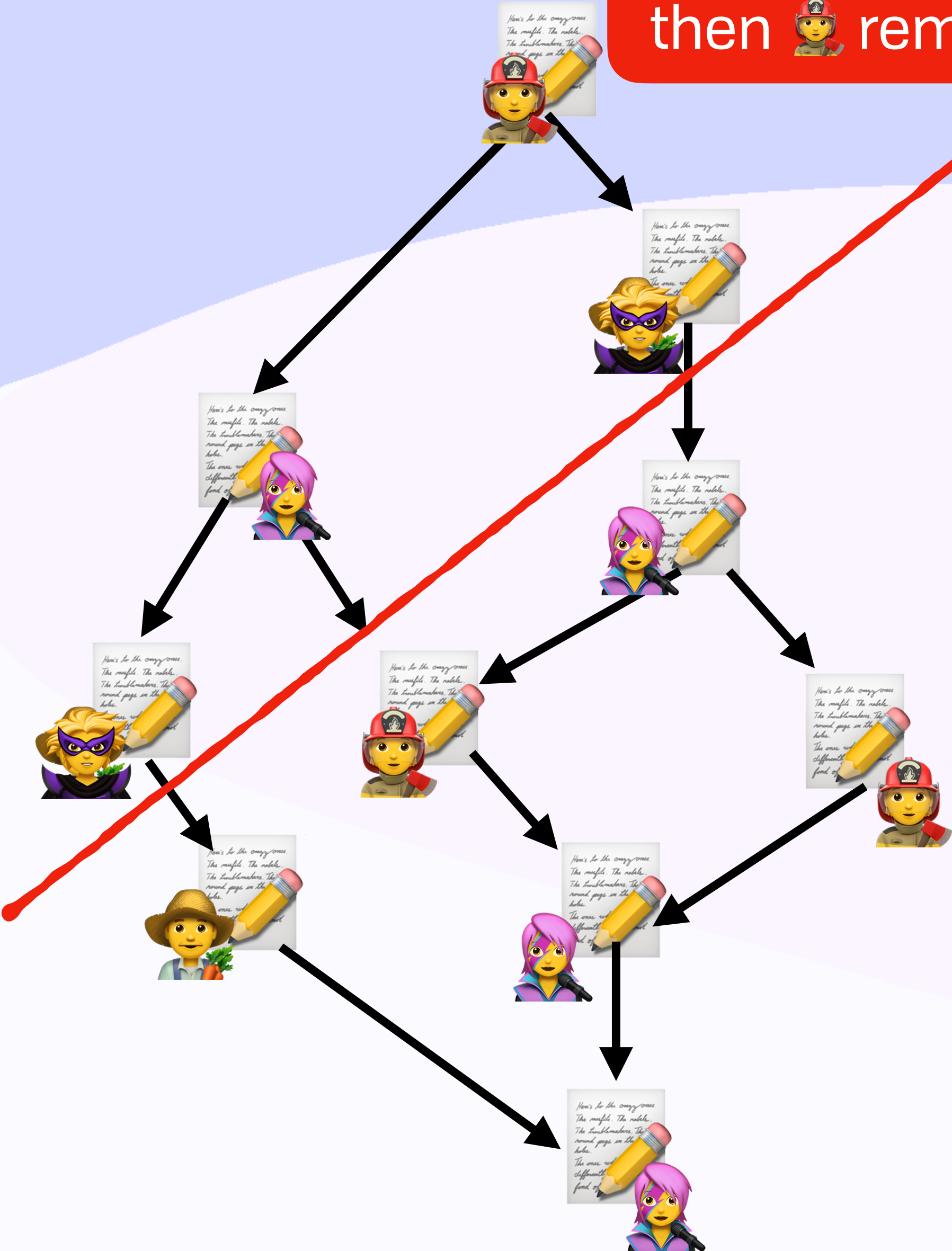
Naïve Tombstoning



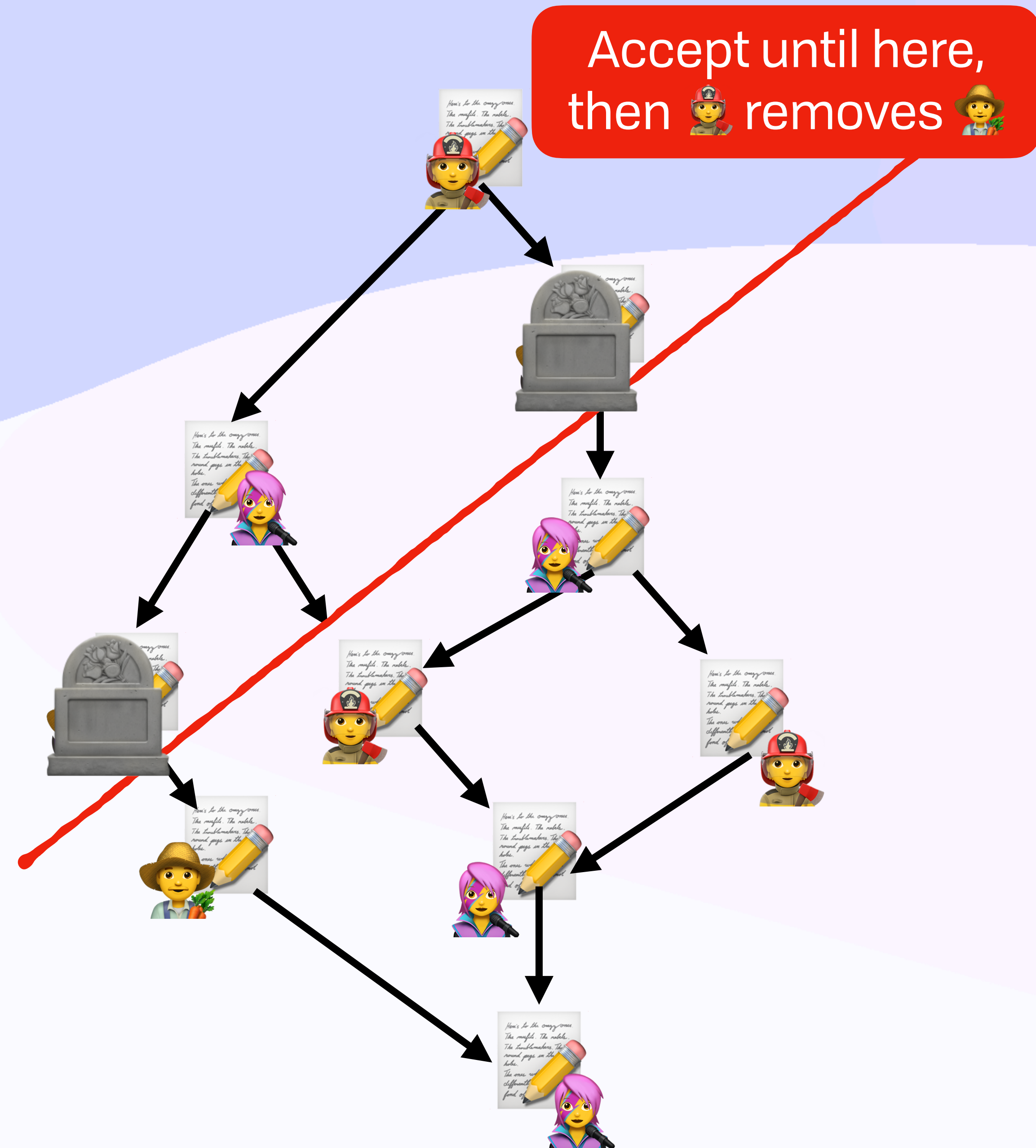
Revocation

Naïve Tombstoning

Accept until here,
then 🧑🚒 removes 🧑🌾

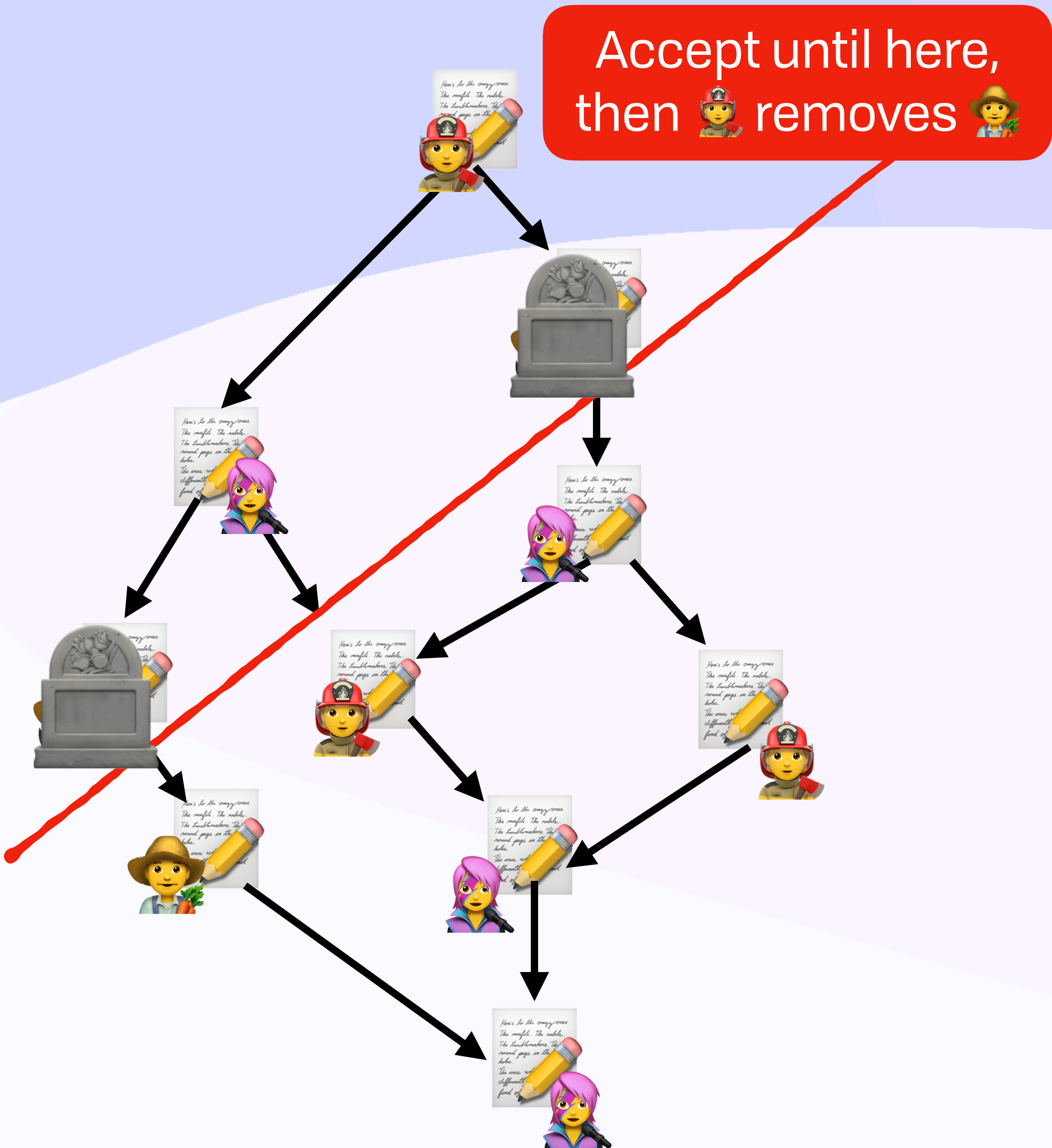
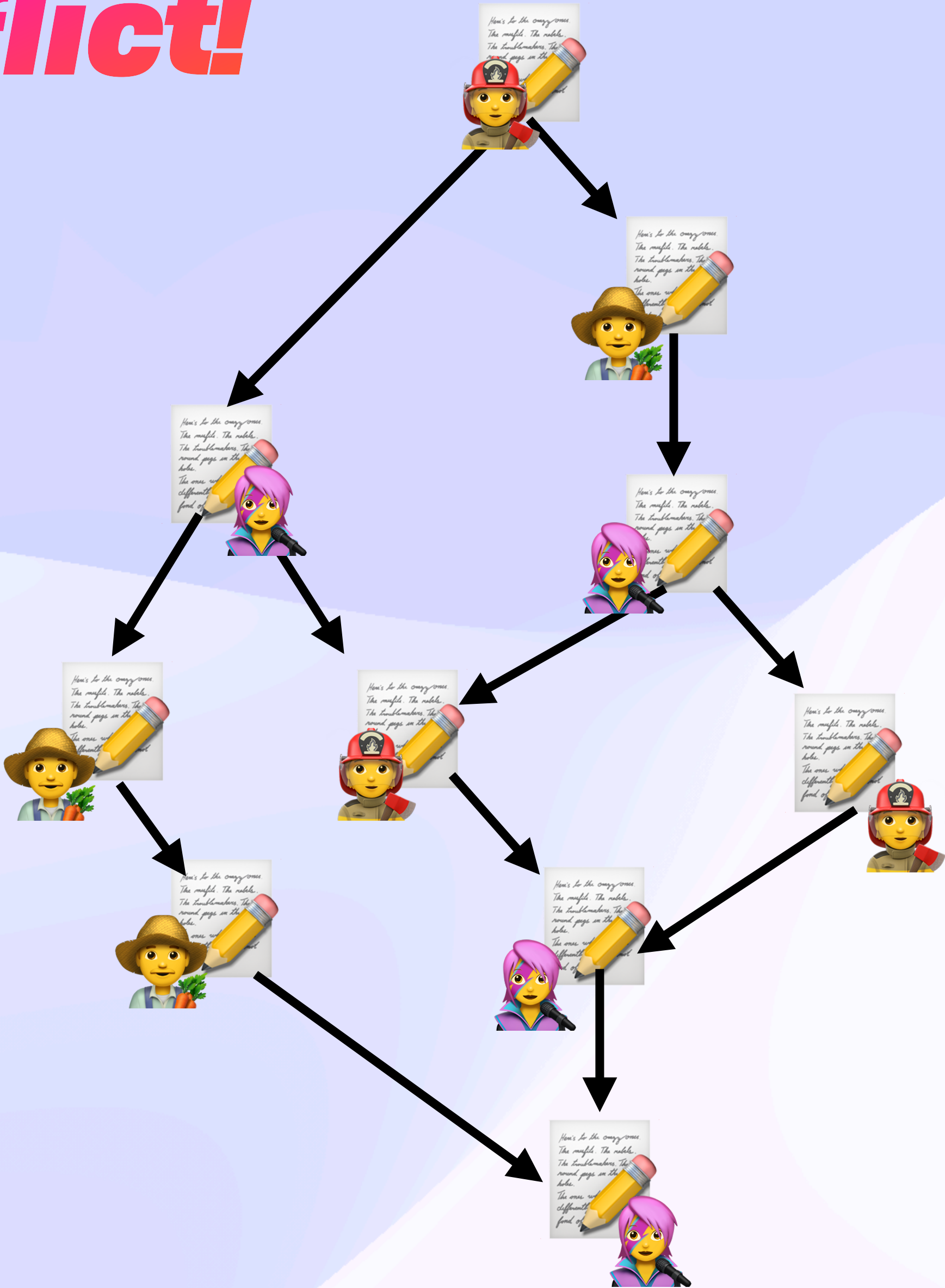


Naïve Tombstoning



Revocation

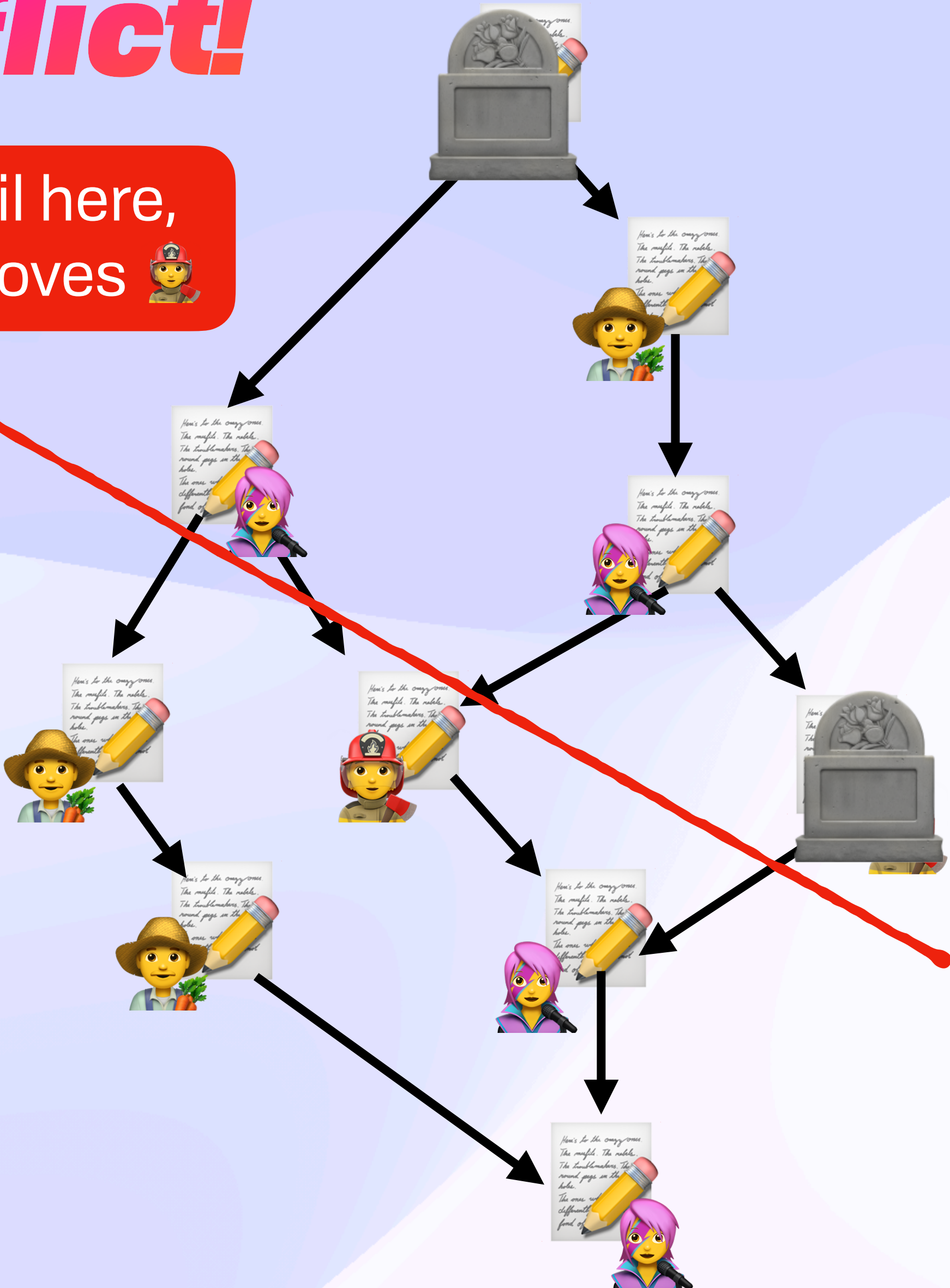
Conflict!



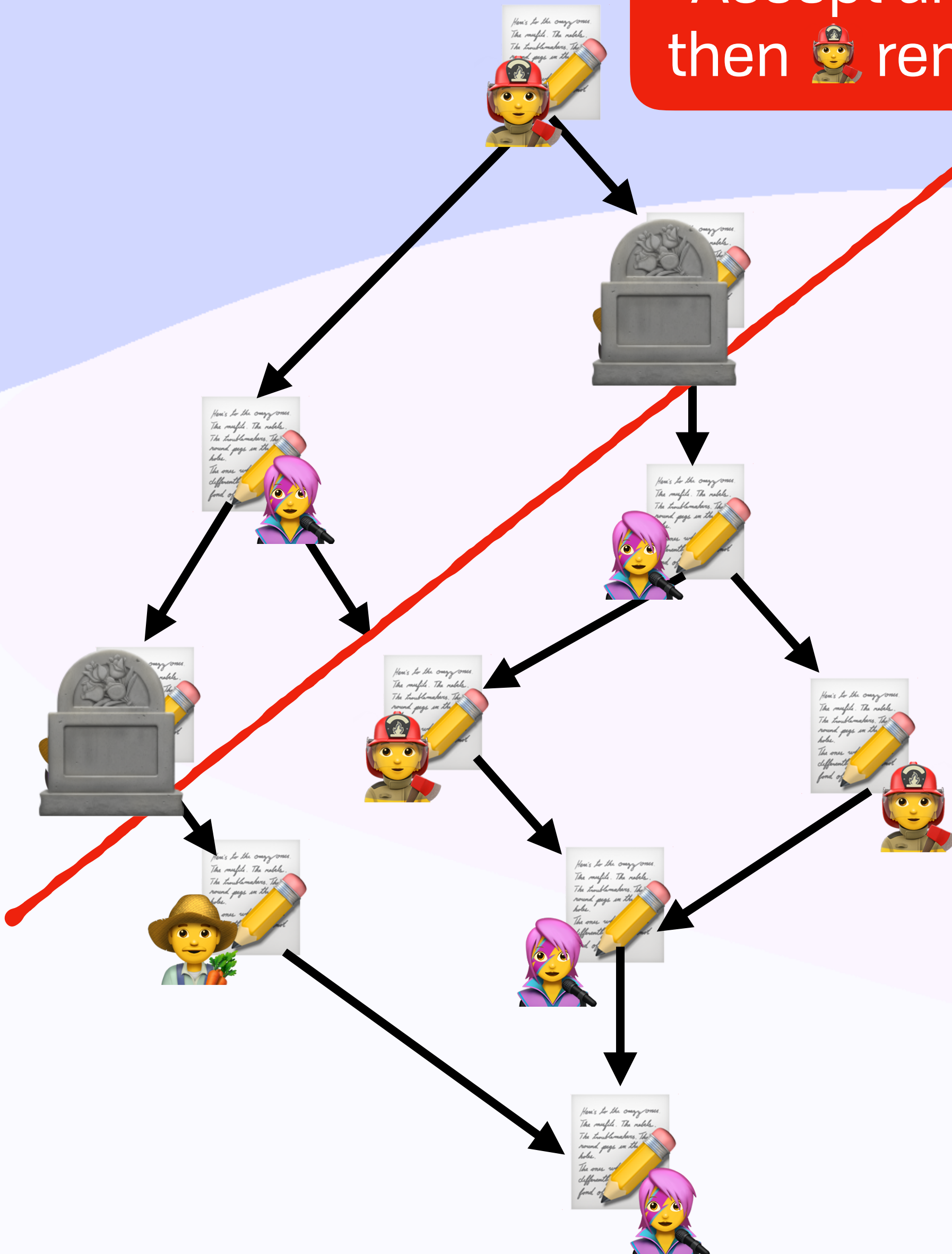
Revocation

Conflict!

Accept until here,
then 🧑 removes 🧑



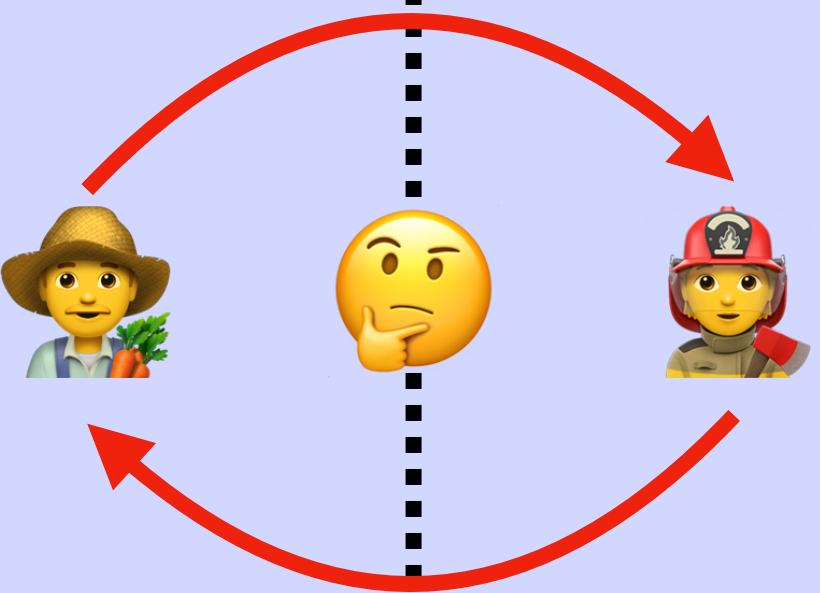
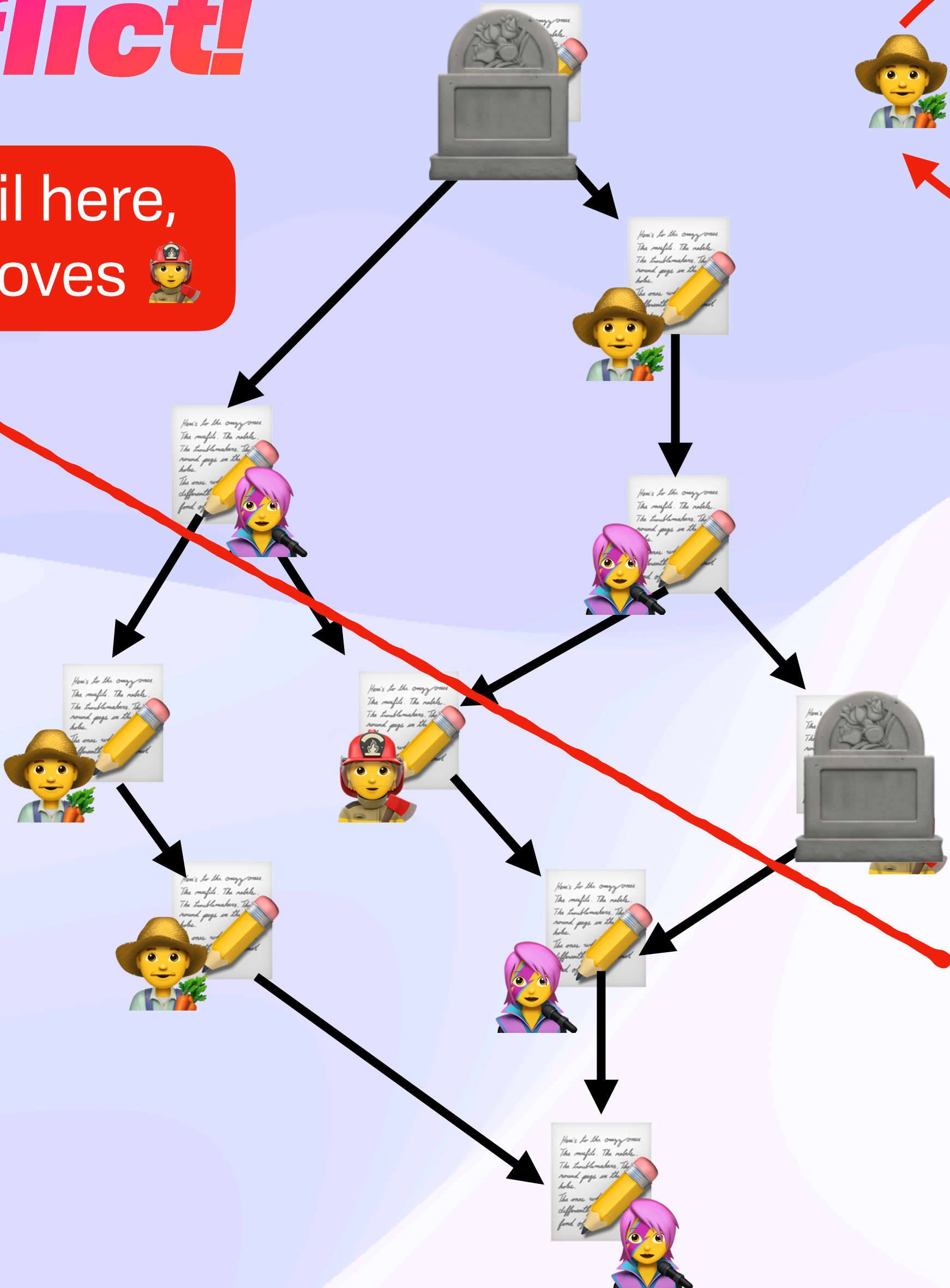
Accept until here,
then 🧑 removes 🧑



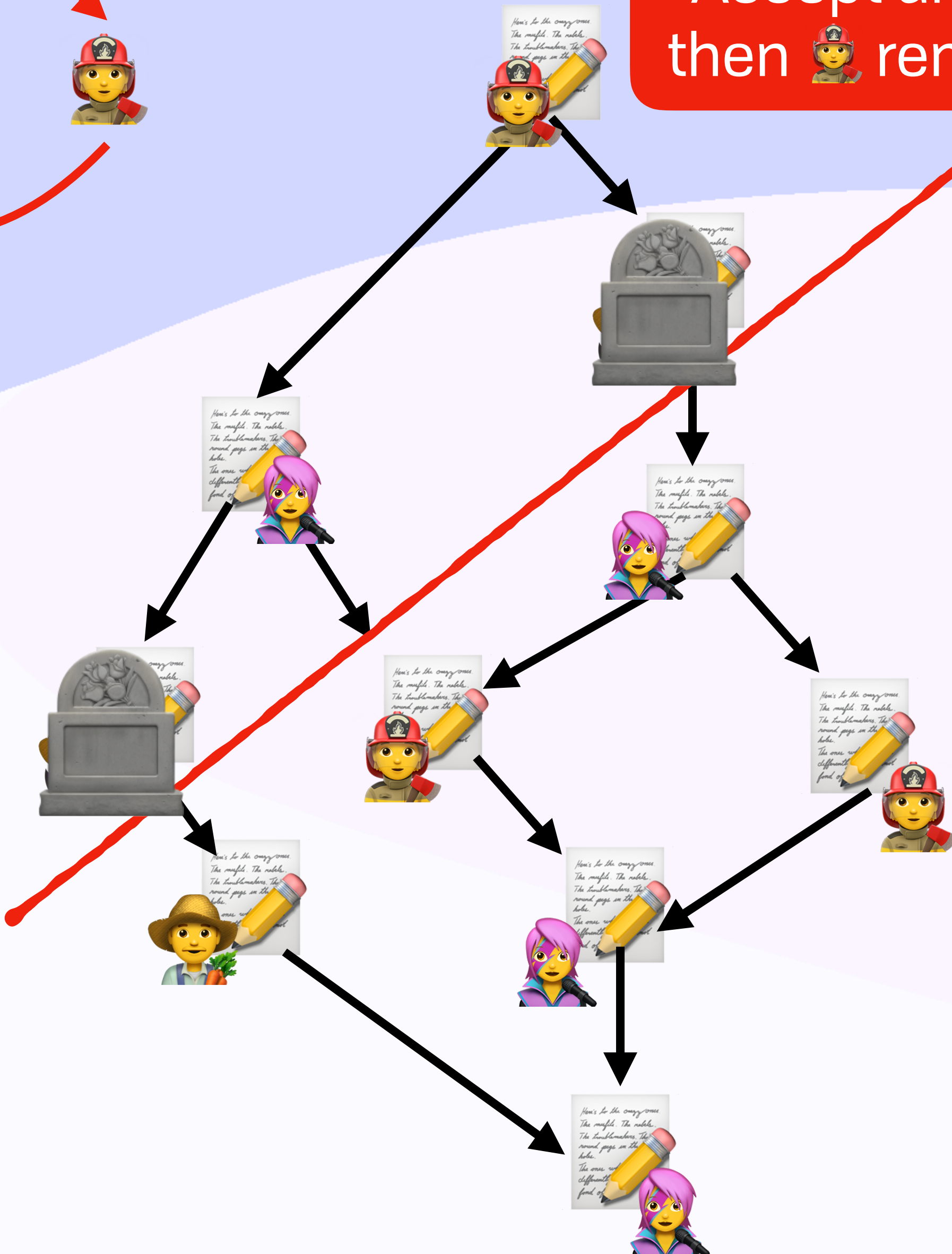
Revocation

Conflict!

Accept until here,
then 🧑 removes 🧑



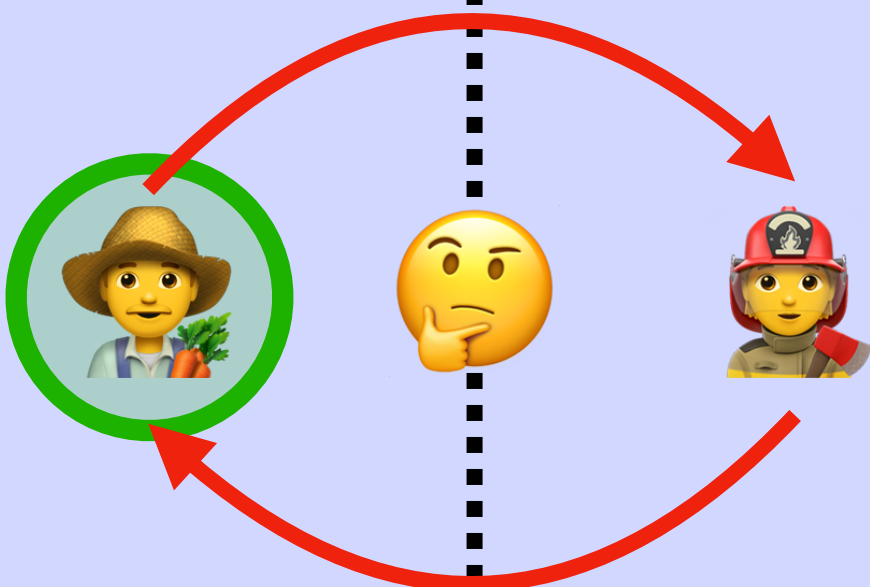
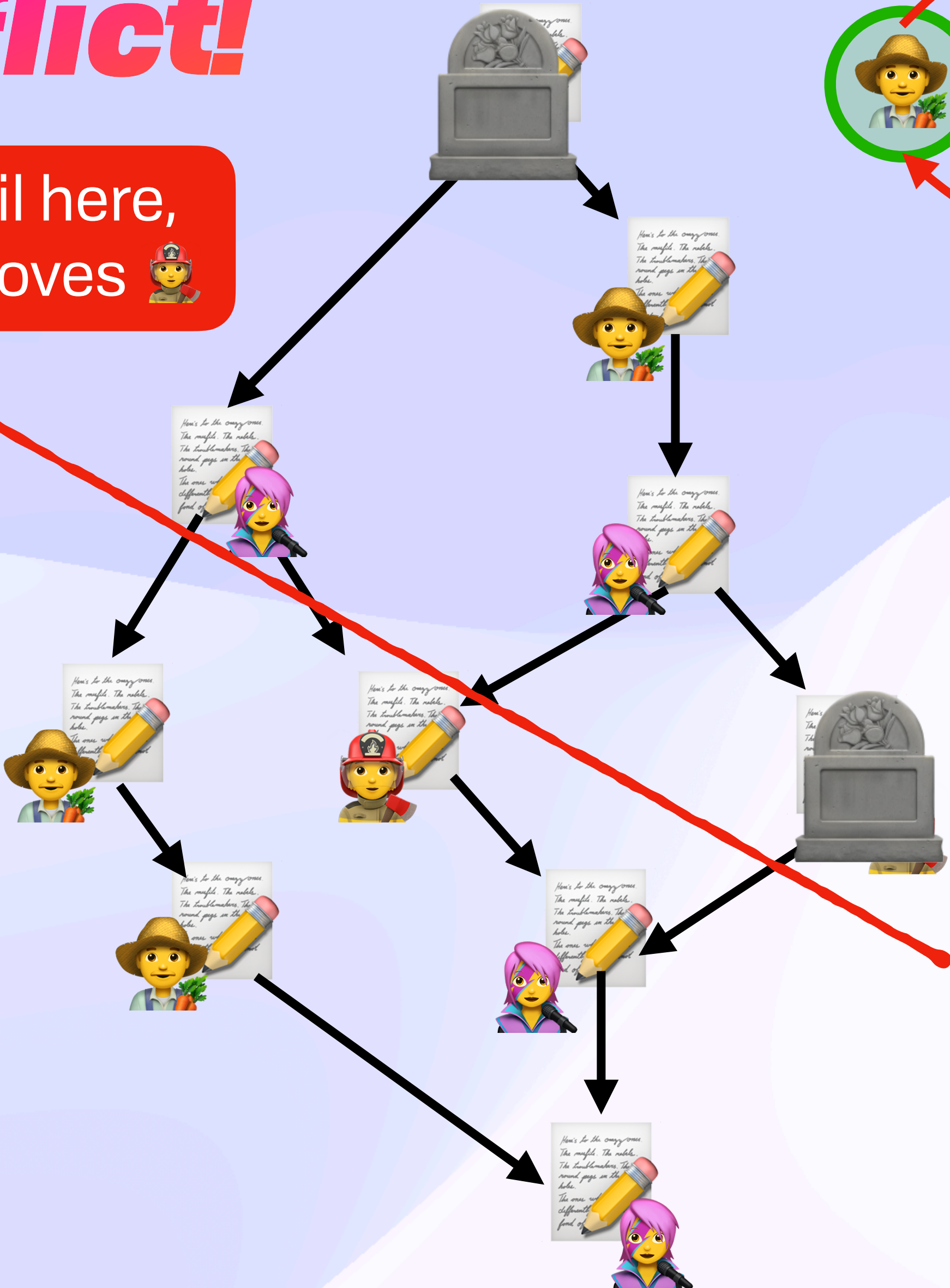
Accept until here,
then 🧑 removes 🧑



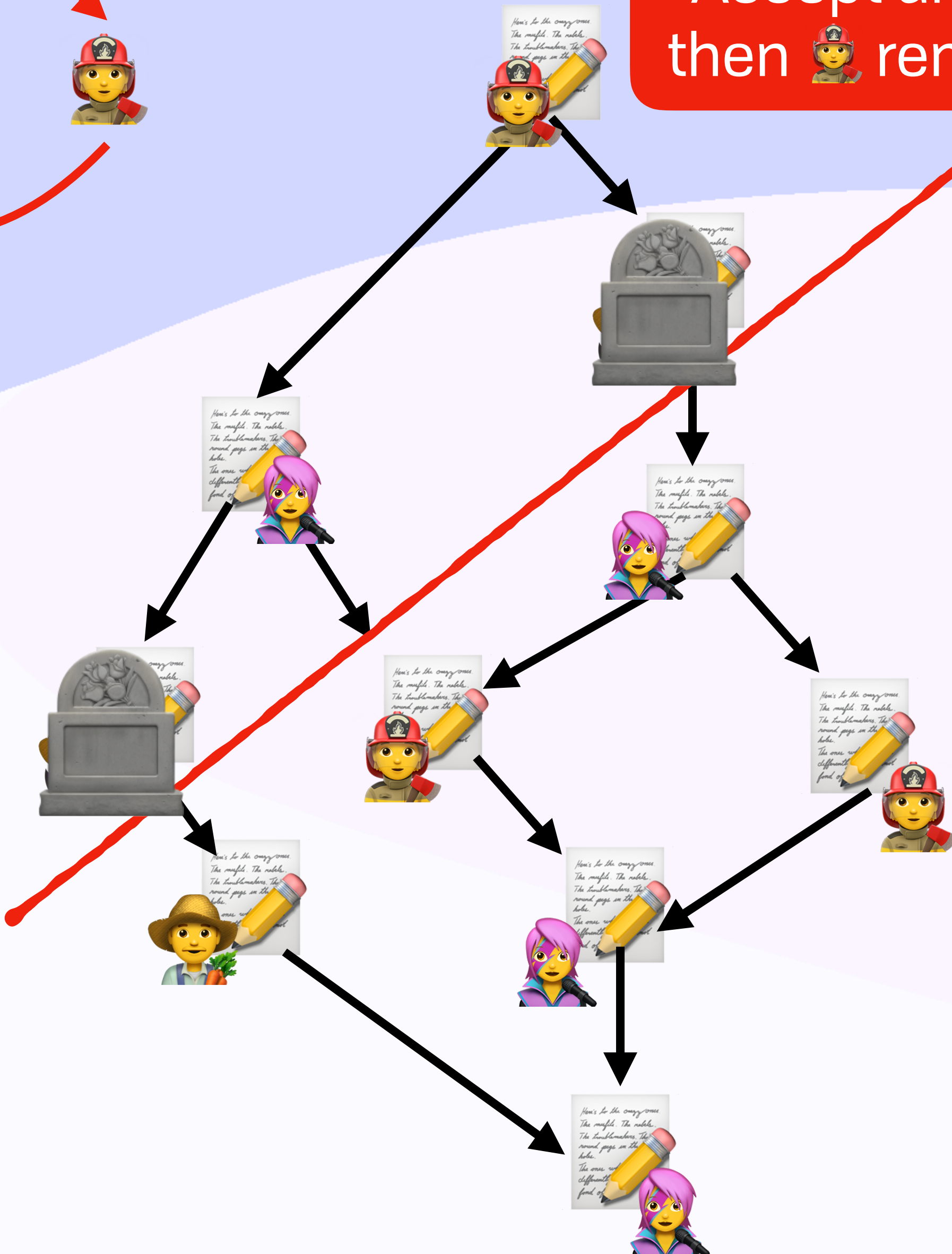
Revocation

Conflict!

Accept until here,
then 🧑 removes 🧑



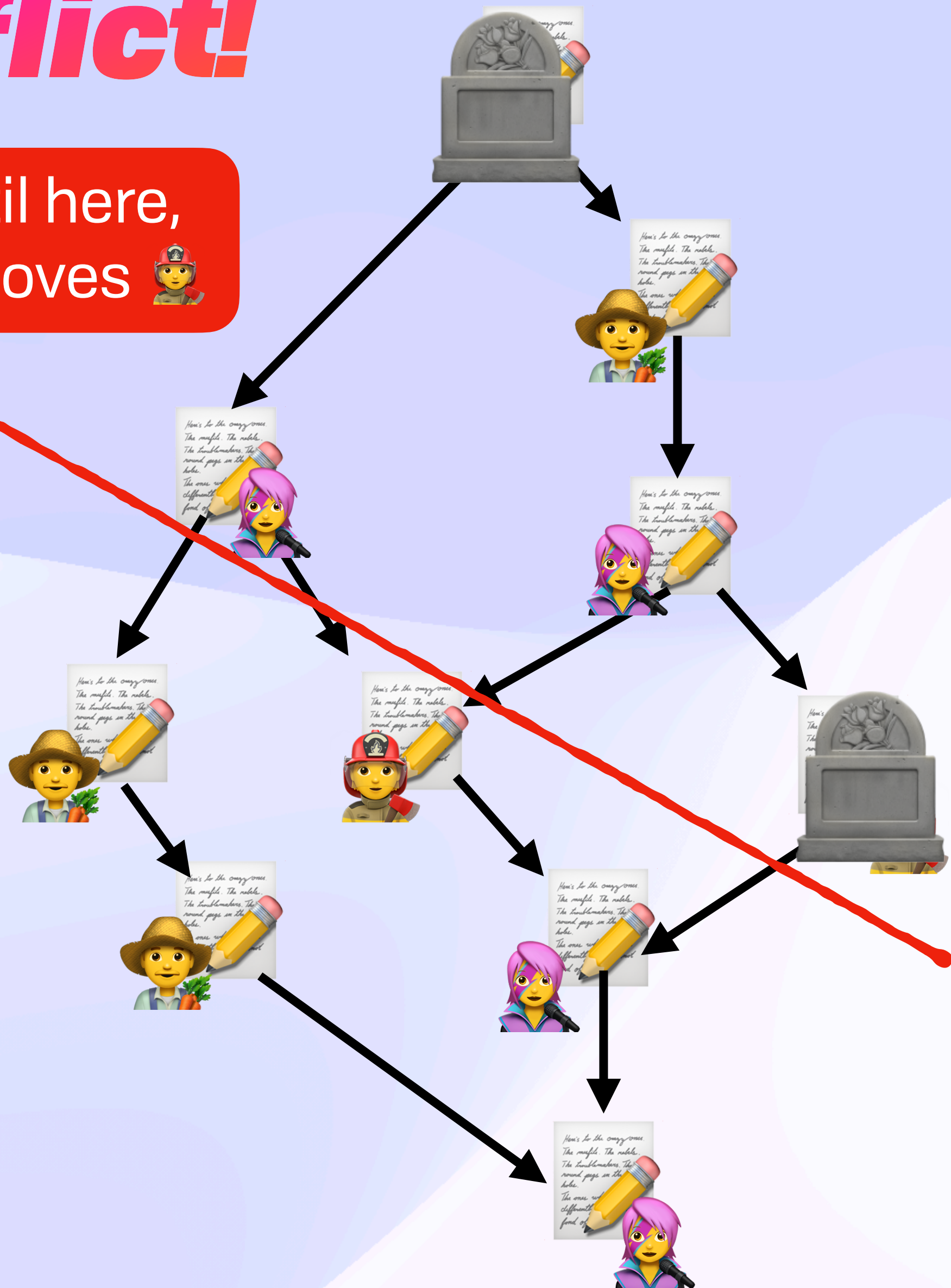
Accept until here,
then 🧑 removes 🧑



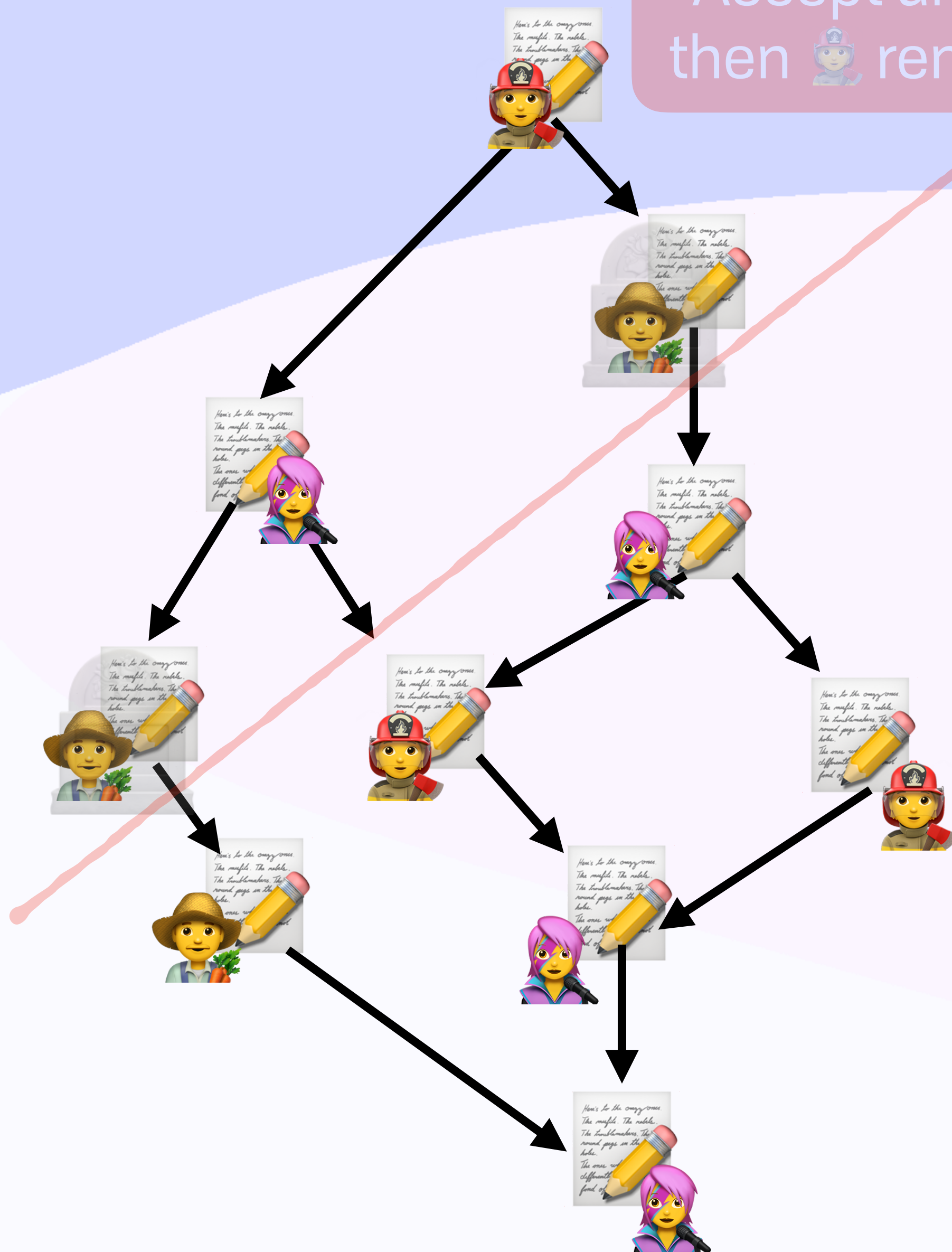
Revocation

Conflict!

Accept until here,
then 🧑 removes 🧑



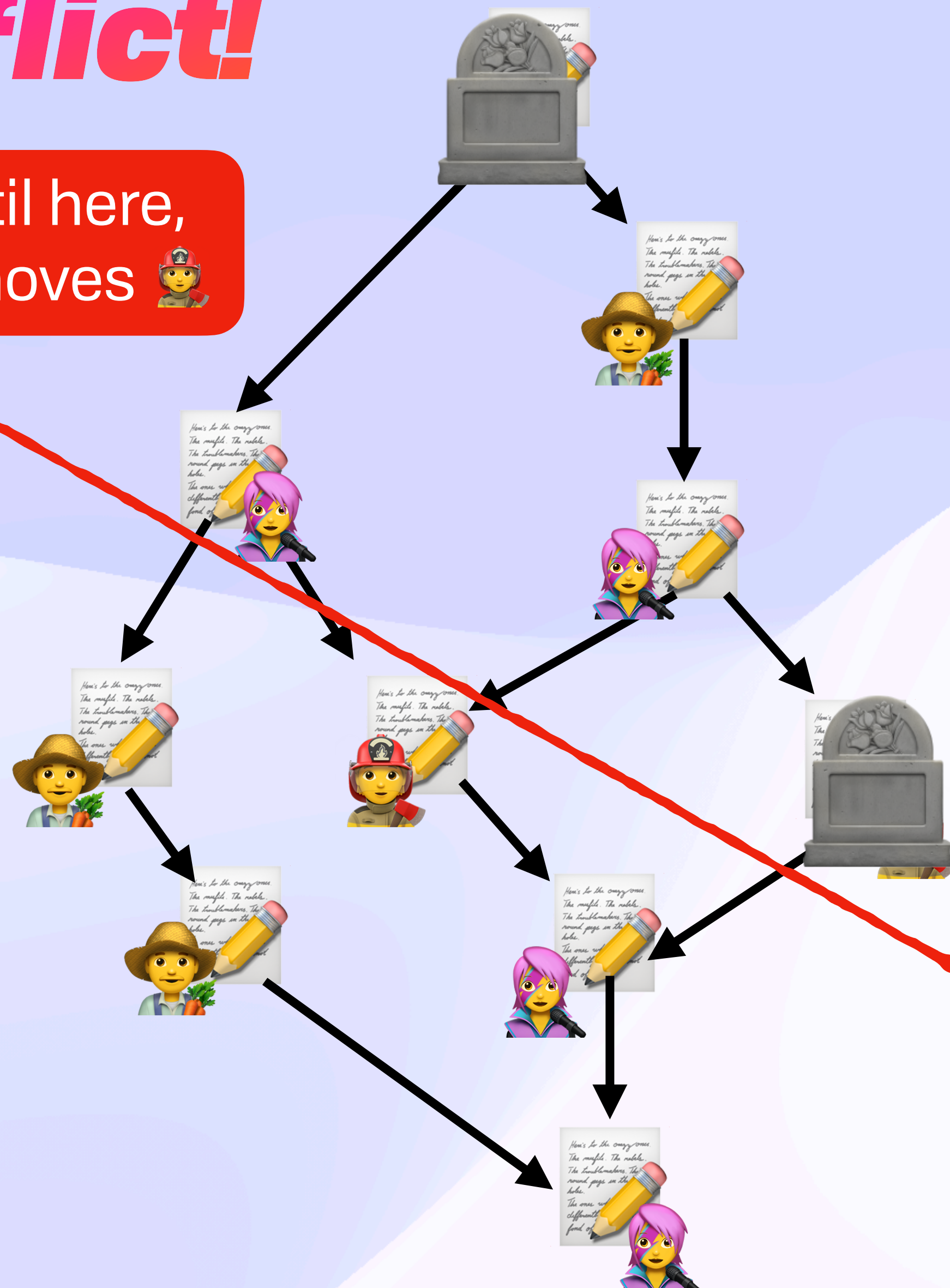
Accept until here,
then 🧑 removes 🧑



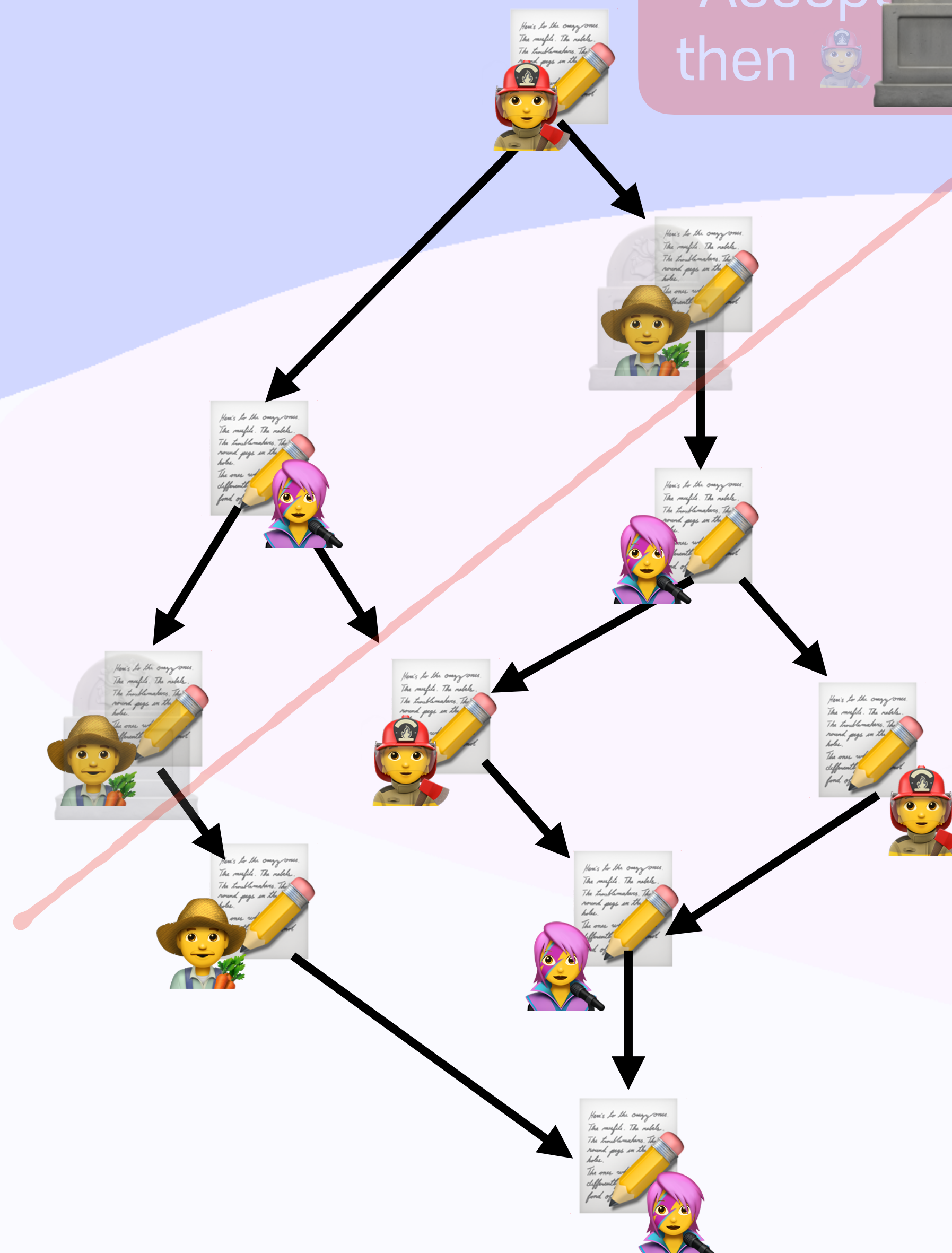
Revocation

Conflict!

Accept until here,
then  removes 



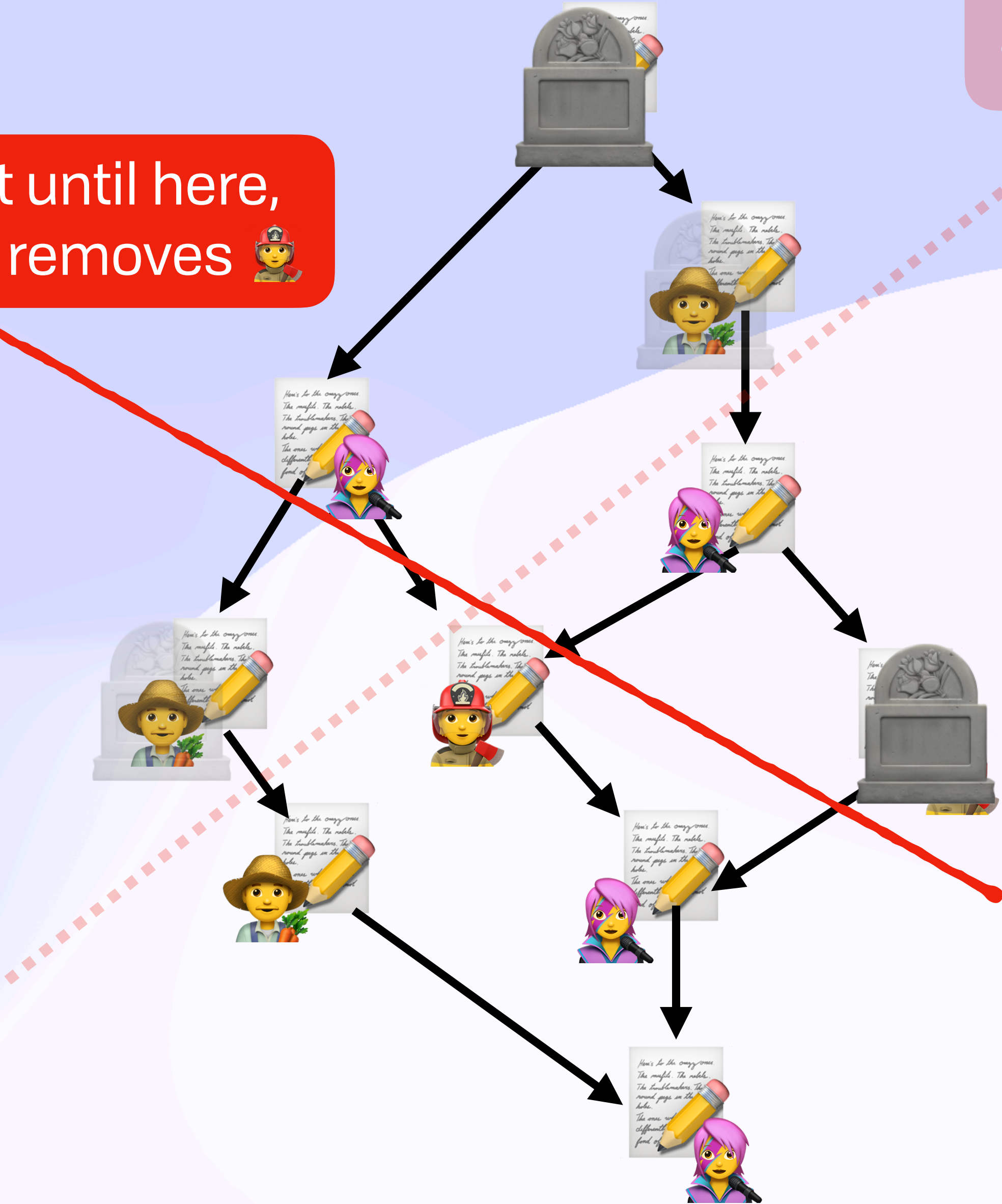
Accept until here,
then  removes 



Revocation *Resolved*

Accept until here,
then 🧑🌾 removes 🧑🚒

Accept until here,
then 🧑🚒 moves 🧑🌾



Wrap Up



Wrap Up

Covered at The Highest of Levels

Add people, groups, and calendar events

People with access

hello@katiwilde.com

Owner

Brooklyn Zelenka (you)

Editor

General access

Restricted

Only people with access can open with the link

Copy link

Done

Wrap Up

Covered at The Highest of Levels

- ♦ Mutation Control 🖋️
 - ♦ Convergent capabilities
 - ♦ Concurrent revocation
- ♦ Read Control 👁️
 - ♦ End-to-end encryption
 - ♦ Causal encryption
- ♦ Backdating-Aware Revocation

People with access

 hello@katiewilde.com Owner

 Brooklyn Zelenka (you) Editor ▼

General access

 Restricted ▼
Only people with access can open with the link

[Copy link](#) [Done](#)

 @expede.wtf

 @expede@types.pl

 notes.brooklynzelenka.com



Thank You, NYC



inkandswitch.com/keyhive

