Safe in the Keyhive

🤝 Secure collaboration with E2EE & capabilities ⛓️‍💥

Safe in the Keyhive

Brooklyn Zelenka — @expede

Safe in the Keyhive

Brooklyn Zelenka — @expede

github.com/expede
Vancouver 🇨🇦

Safe in the Keyhive

Brooklyn Zelenka — @expede

- Lead the ***Keyhive*** project at ***Ink & Switch*** 🐝
  - Shout out to ***John Mumm*** & ***Alex Good*** 🥳
  - …and many others in the design loop
- Spec editor for ***UCAN*** distributed auth system
- Wrote some auth EIPs in my misspent youth
- PLs and DSys are my jam 🤘

github.com/expede
Vancouver 🇨🇦

Safe in the Keyhive

Brooklyn Zelenka — @expede

- Lead the ***Keyhive*** project at ***Ink & Switch*** 🐝
    - Shout out to ***John Mumm*** & ***Alex Good*** 🥳
    - …and many others in the design loop
- Spec editor for ***UCAN*** distributed auth system
- Wrote some auth EIPs in my misspent youth
- PLs and DSys are my jam 🤘

Safe in the Keyhive

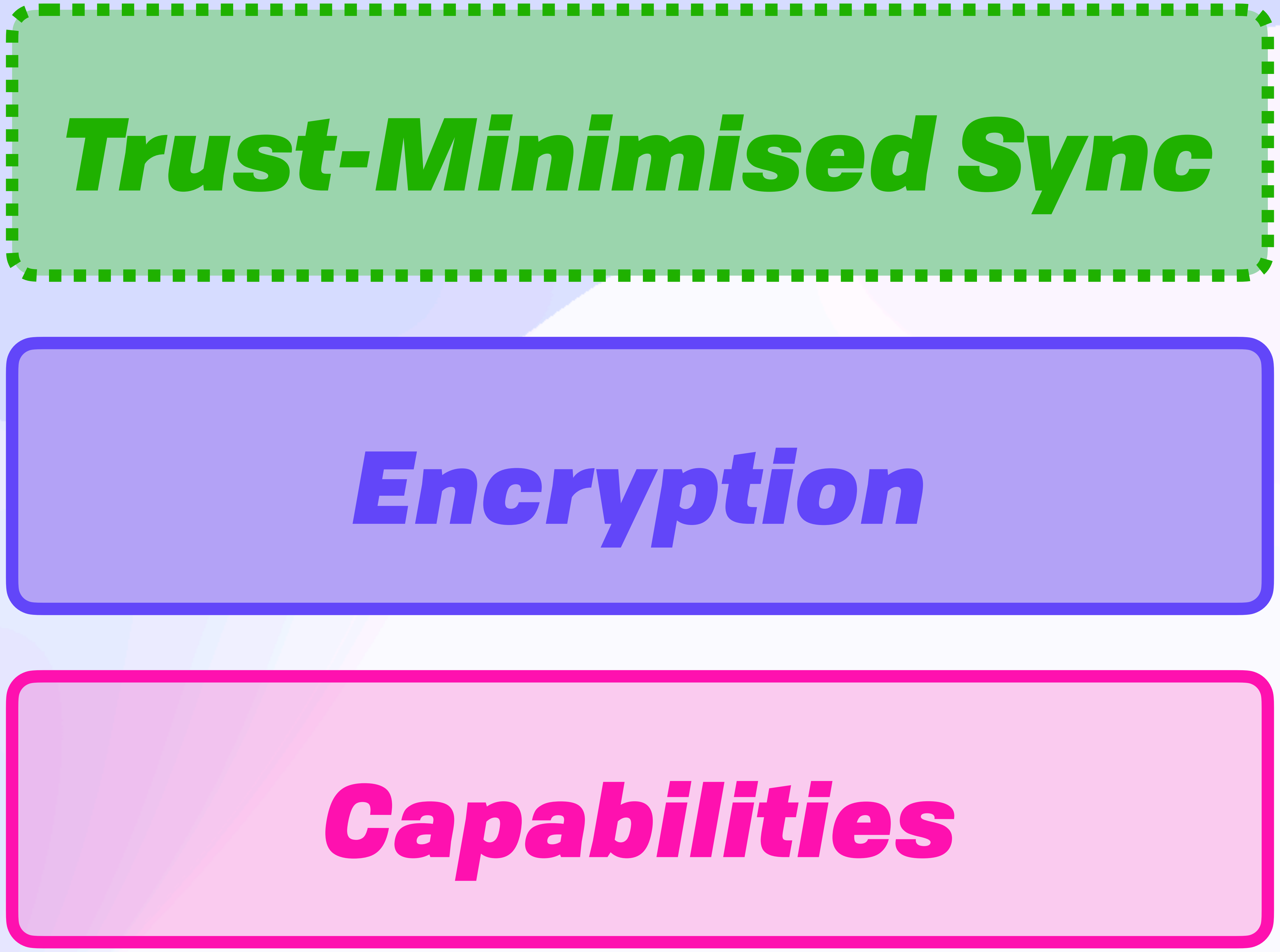
Good Things™ from LFC'24

Photo Credit: Nik Graf

Safe in the Keyhive

Topics & Depth

Topics & Depth



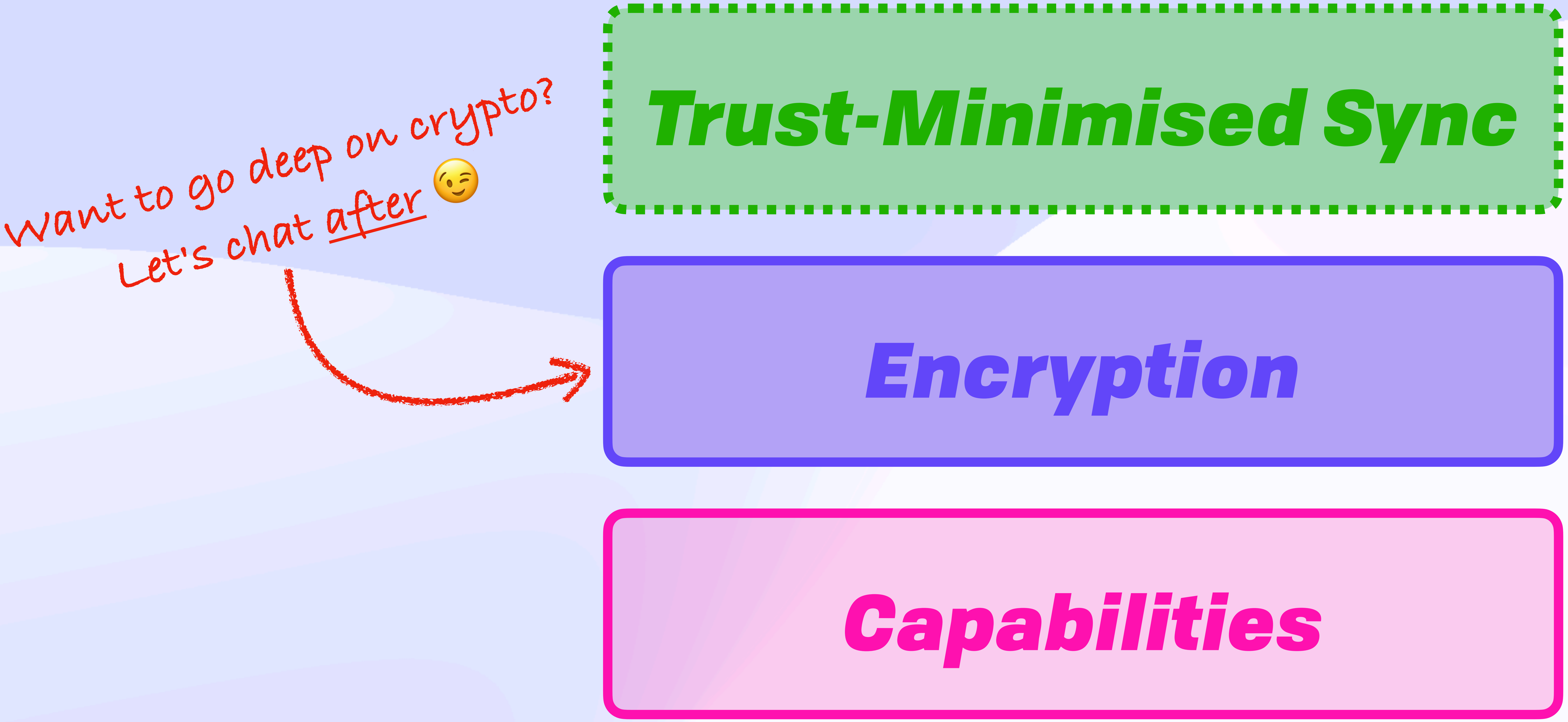
Trust-Minimised Sync

Encryption

Capabilities

Safe in the Keyhive

Topics & Depth



Want to go deep on crypto?
Let's chat after 😉

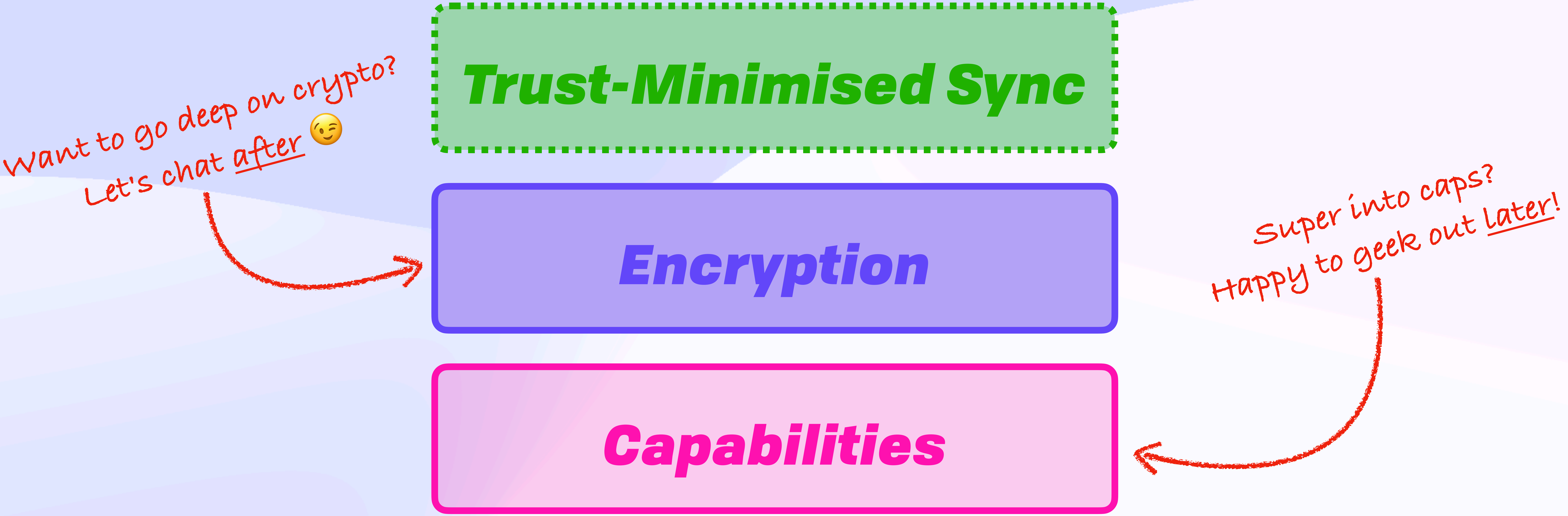
Trust-Minimised Sync

Encryption

Capabilities

Safe in the Keyhive

Topics & Depth



Trust-Minimised Sync

Encryption

Capabilities

Want to go deep on crypto?
Let's chat after 😉

Super into caps?
Happy to geek out later!

Safe in the Keyhive

Topics & Depth

Want to go deep on crypto?
Let's chat after 😉

Trust-Minimised Sync

Encryption

Capabilities

Super into caps?
Happy to geek out later!

Why an Auth Layer?

Motivation

💡

Motivation

Motivation

What if Signal ...

Motivation

What if Signal ...
but for ***everything else***

Motivation

Human Factors

Motivation

Human Factors

Familiar user experience 😌

Live collaboration speed 🏎️

Interchangeable sync servers 🔀

Automatic (no manual merges) 🤖

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) 🤖

Motivation

How Close to Wikipedia Scale?

Motivation

How Close to Wikipedia Scale?

100,000s interlinked docs 📚

10,000s readers 👀

1000s writers ✍️

100s admins 🦸

Motivation

~~Paranoia Level~~ "Informal Threat Model"

Motivation

~~Paranoia Level~~ "Informal Threat Model"

Secure against the ***FBI*** 🕵️

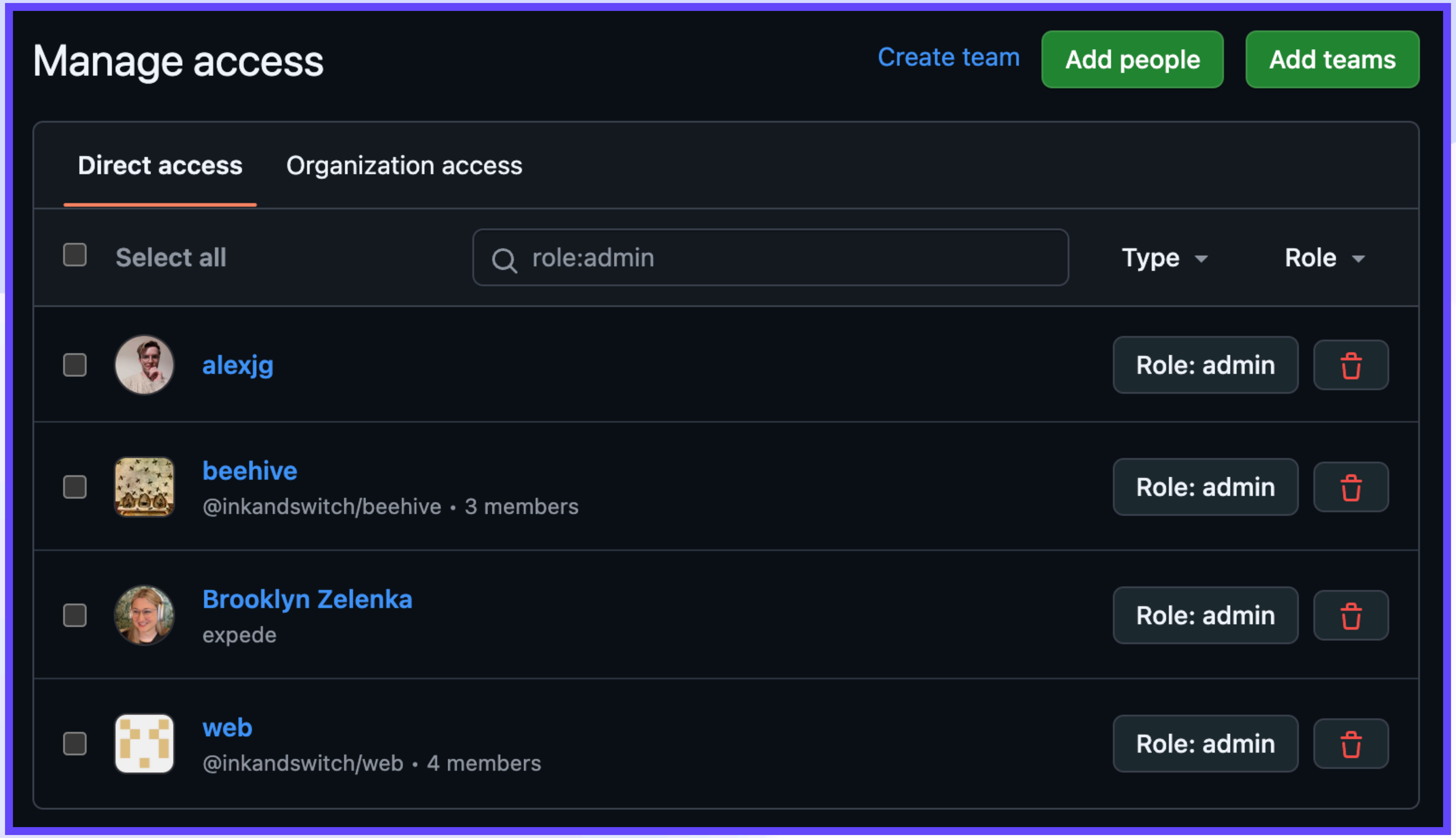
...but not the ***NSA*** 🪖 🕴️

Motivation

"Boring is Good, Actually"

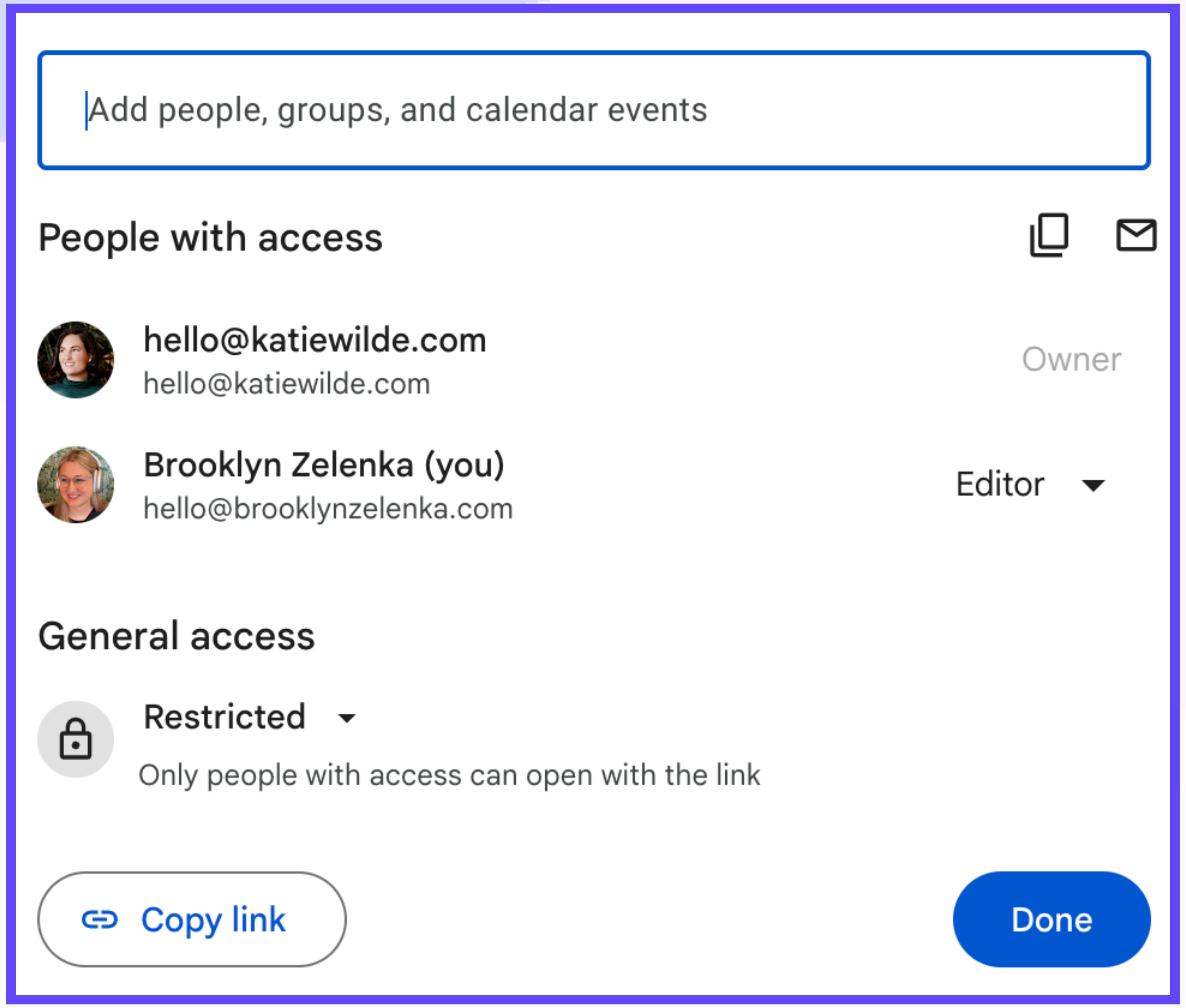
Motivation

"Boring is Good, Actually"



role:admin

- alexjg — Role: admin
- beehive — @inkandswitch/beehive • 3 members — Role: admin
- Brooklyn Zelenka — expede — Role: admin
- web — @inkandswitch/web • 4 members — Role: admin

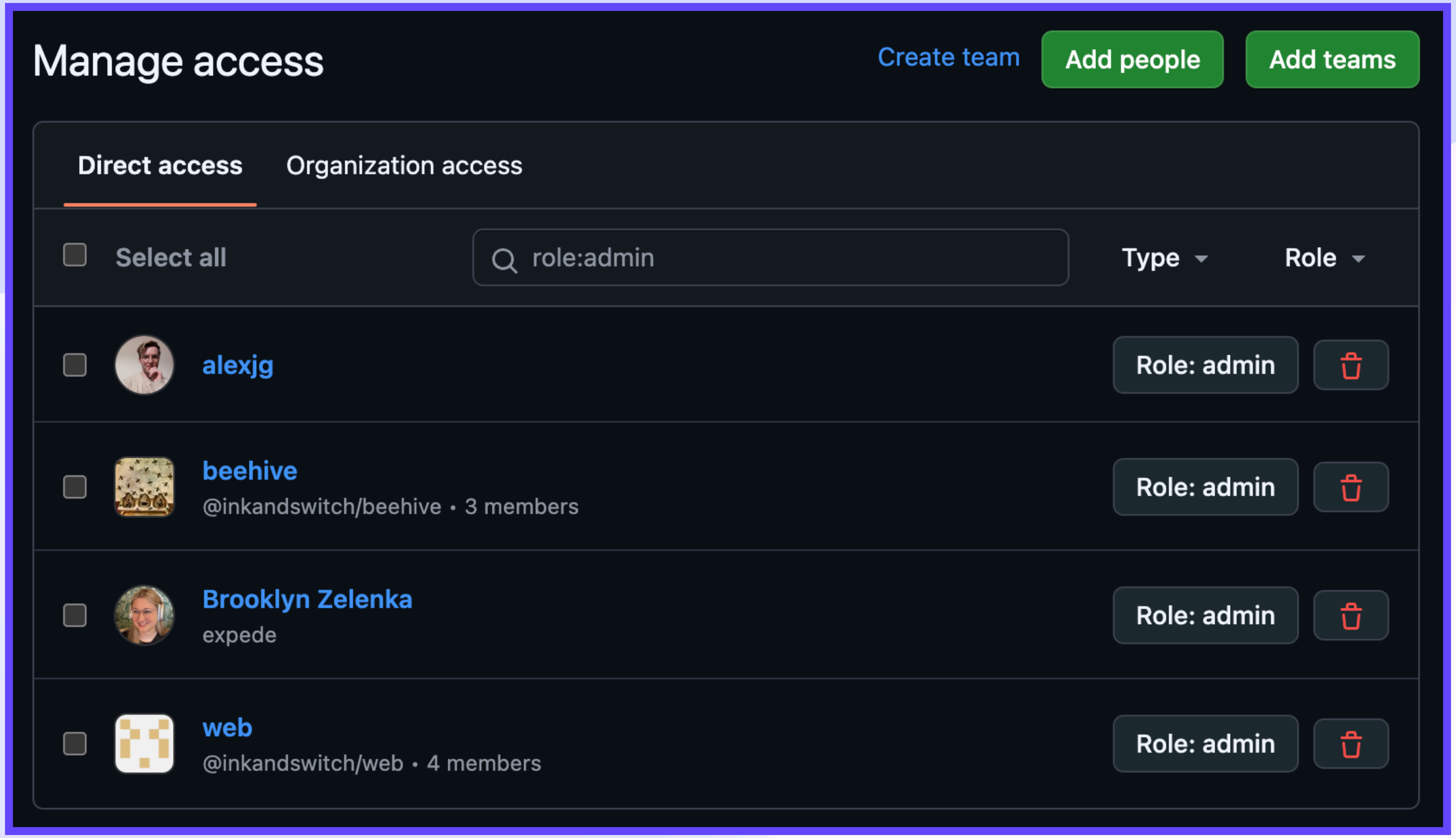


- hello@katiewilde.com — hello@katiewilde.com — Owner
- Brooklyn Zelenka (you) — hello@brooklynzelenka.com — Editor

Restricted
Only people with access can open with the link

Motivation

"Boring is Good, Actually"



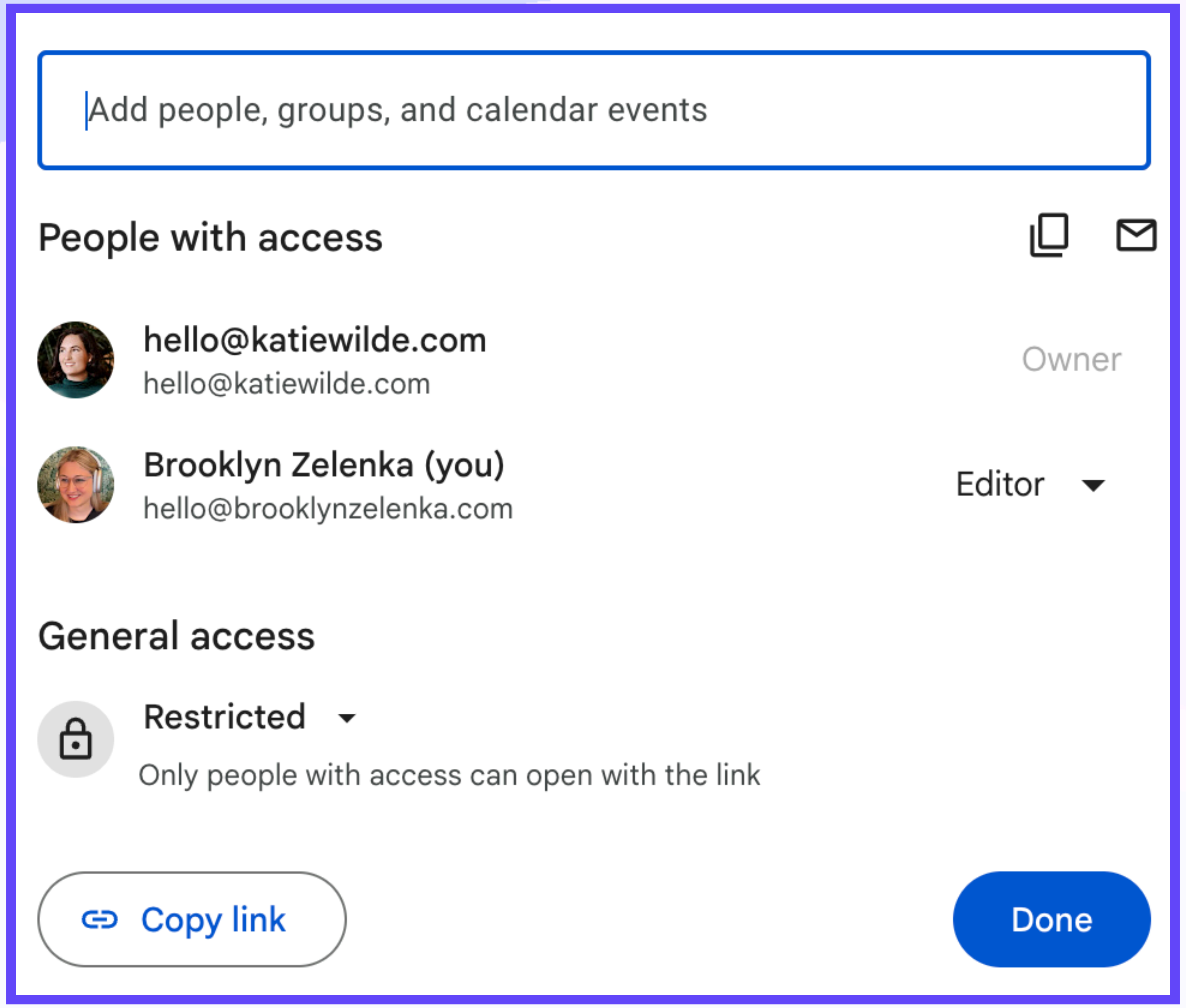
Manage access

Create team | Add people | Add teams

Direct access | Organization 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 hello@katiewilde.com	Owner
Brooklyn Zelenka (you) hello@brooklynzelenka.com	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"

Motivation

Unix Philosophy

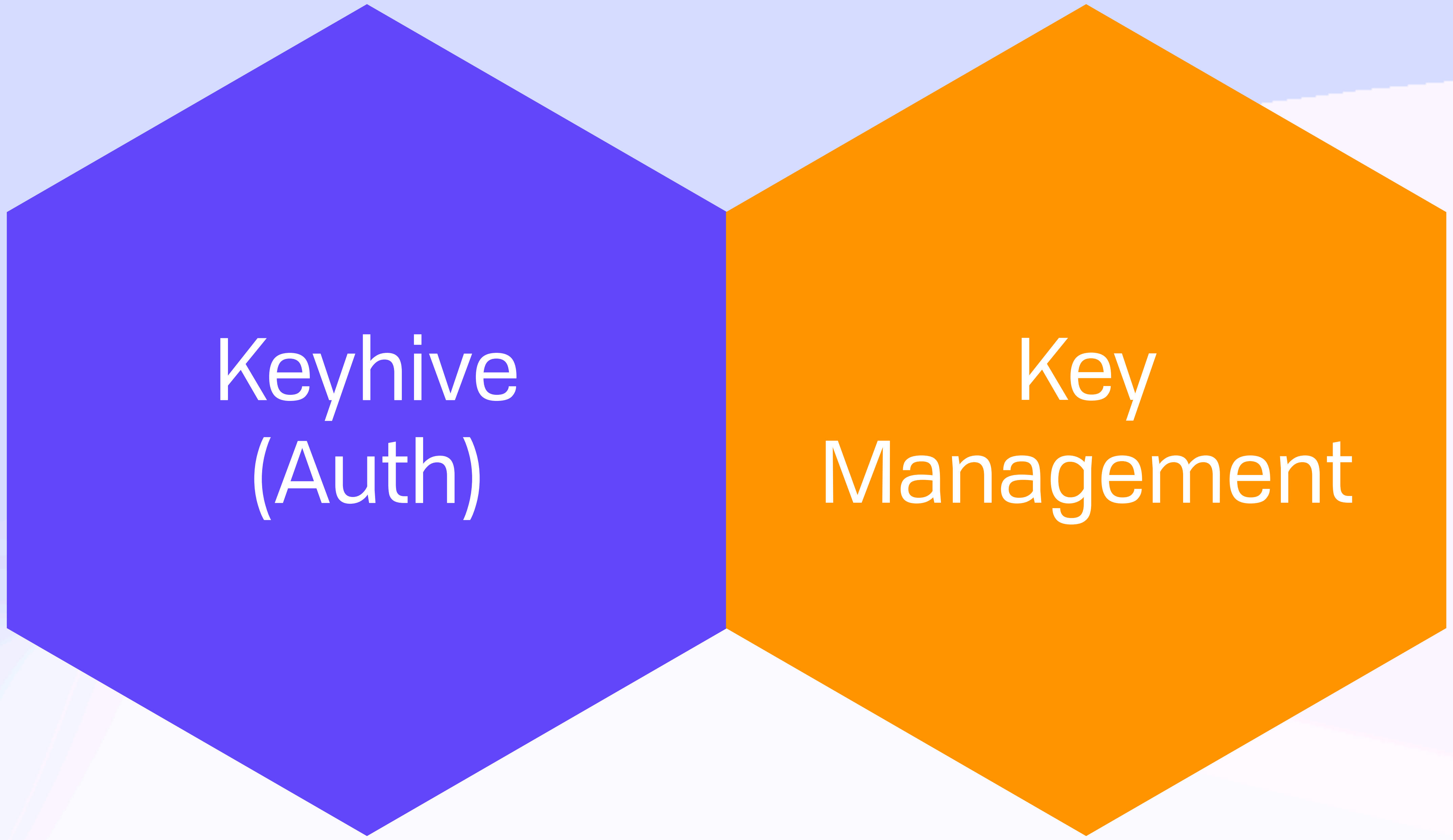
Motivation

Unix Philosophy

Keyhive
(Auth)

Motivation

Unix Philosophy

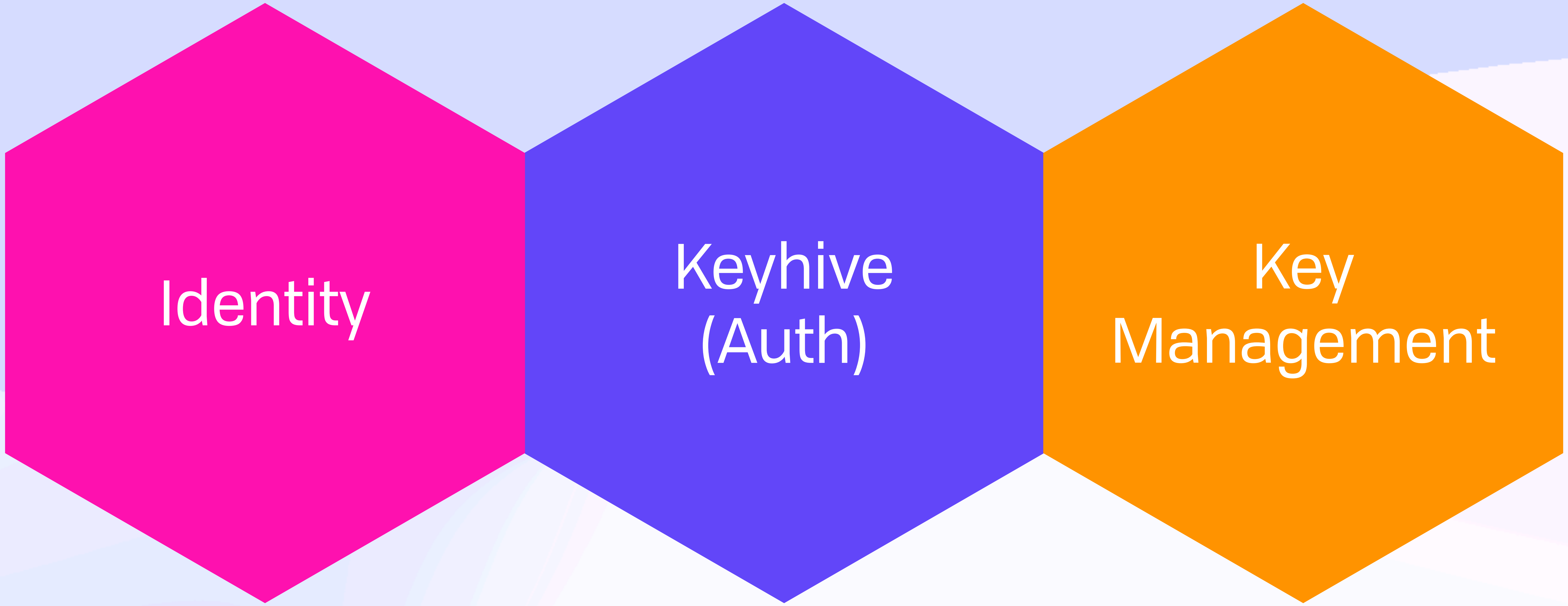


Keyhive (Auth)

Key Management

Motivation

Unix Philosophy



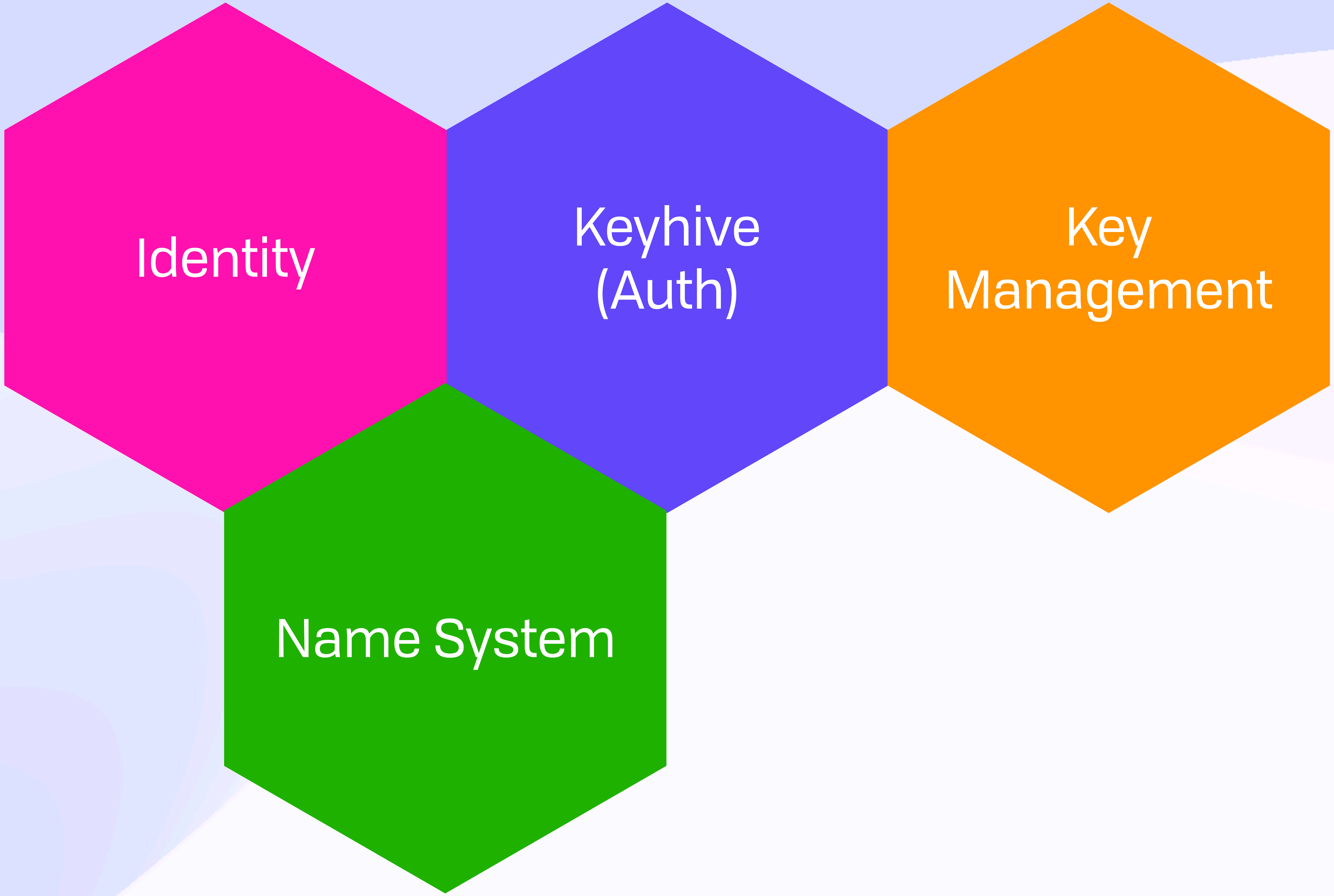
Identity

Keyhive (Auth)

Key Management

Motivation

Unix Philosophy



Identity

Keyhive (Auth)

Key Management

Name System

Auth-as-Place

Cloud Auth

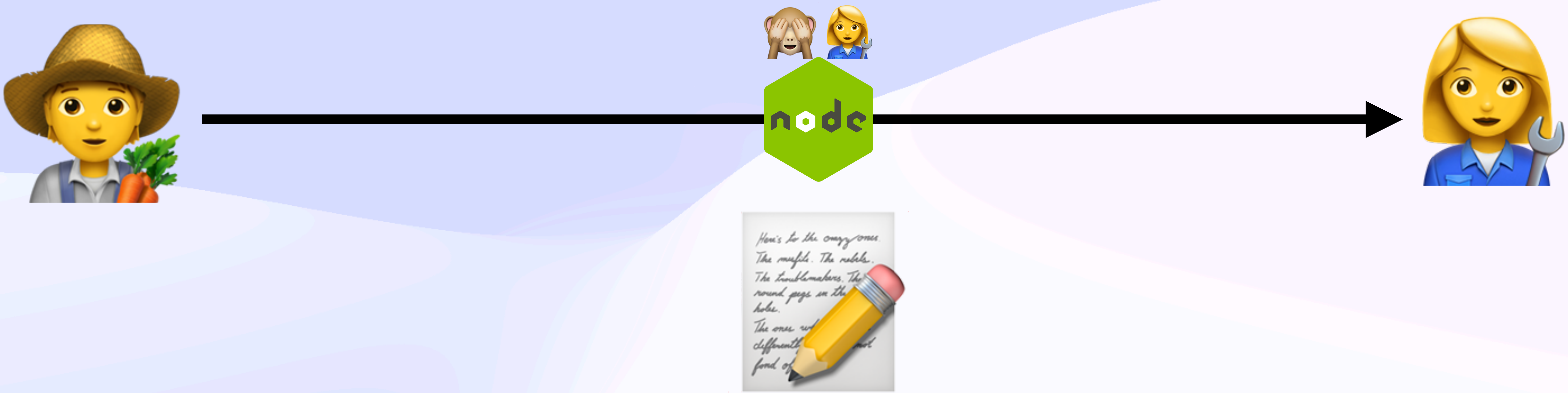
🗺️

Auth-as-Place

Cloud Auth Flow ☁️

Auth-as-Place

Cloud Auth Flow ☁️



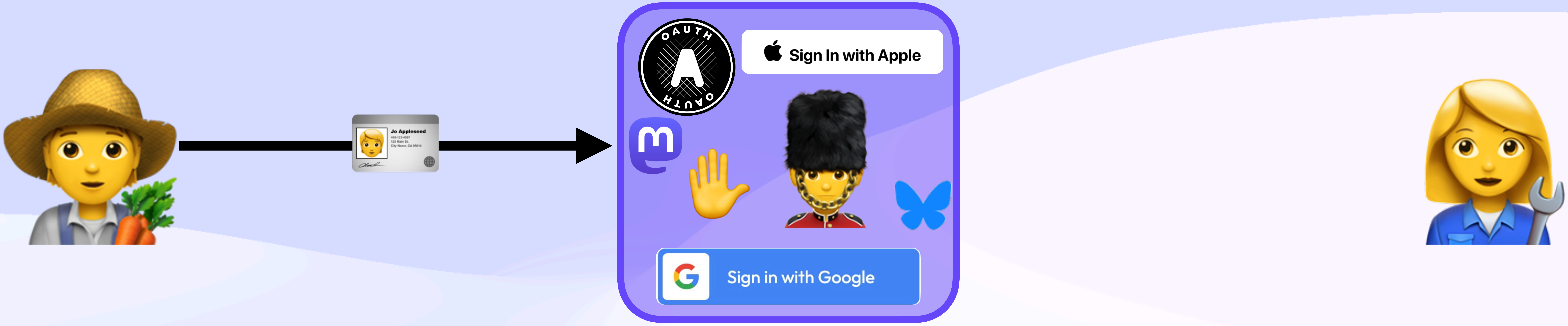
Auth-as-Place

Cloud Auth Flow ☁️

🧑‍🌾 👩‍🔧

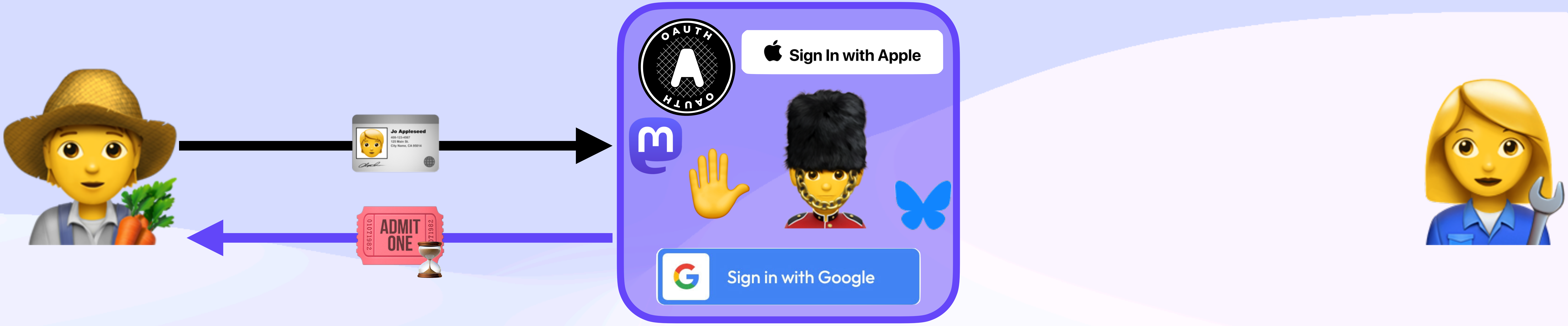
Auth-as-Place

Cloud Auth Flow ☁️



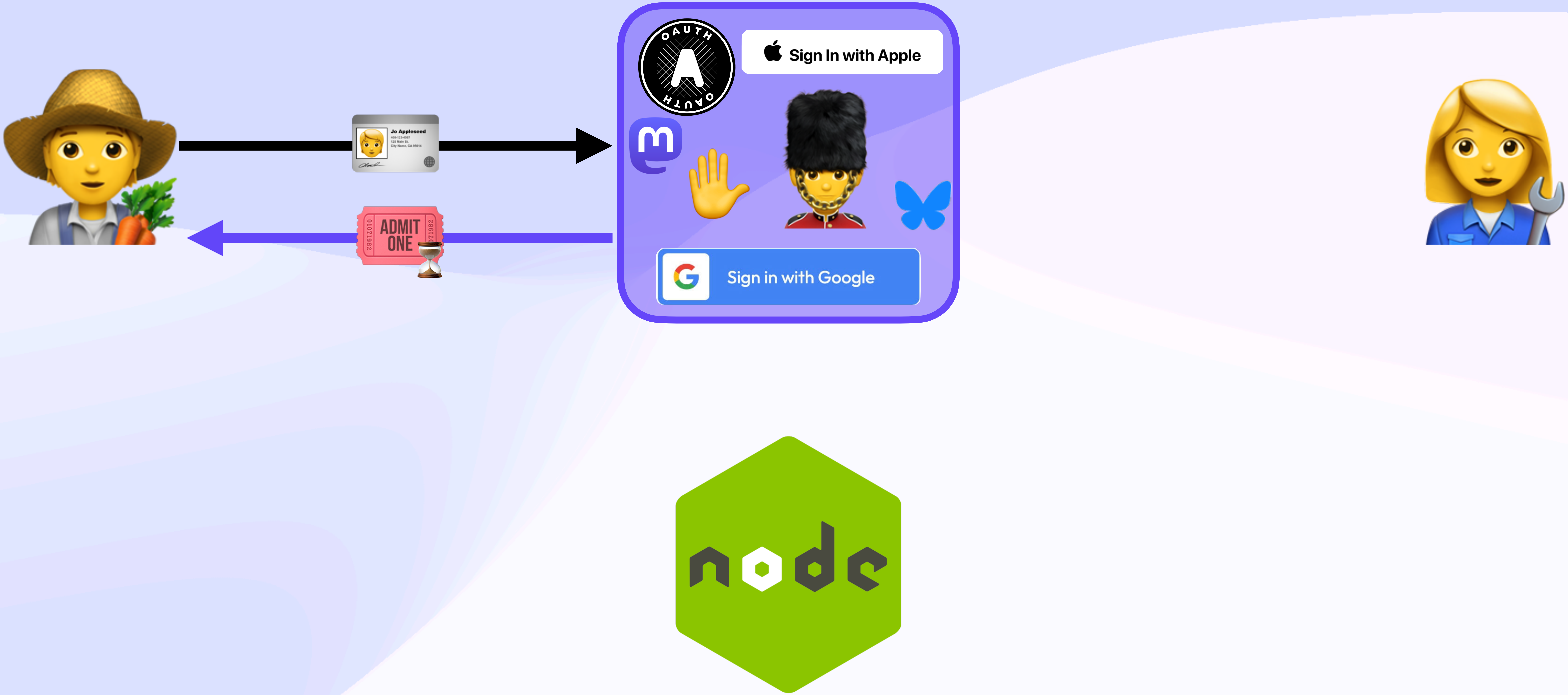
Auth-as-Place

Cloud Auth Flow ☁️



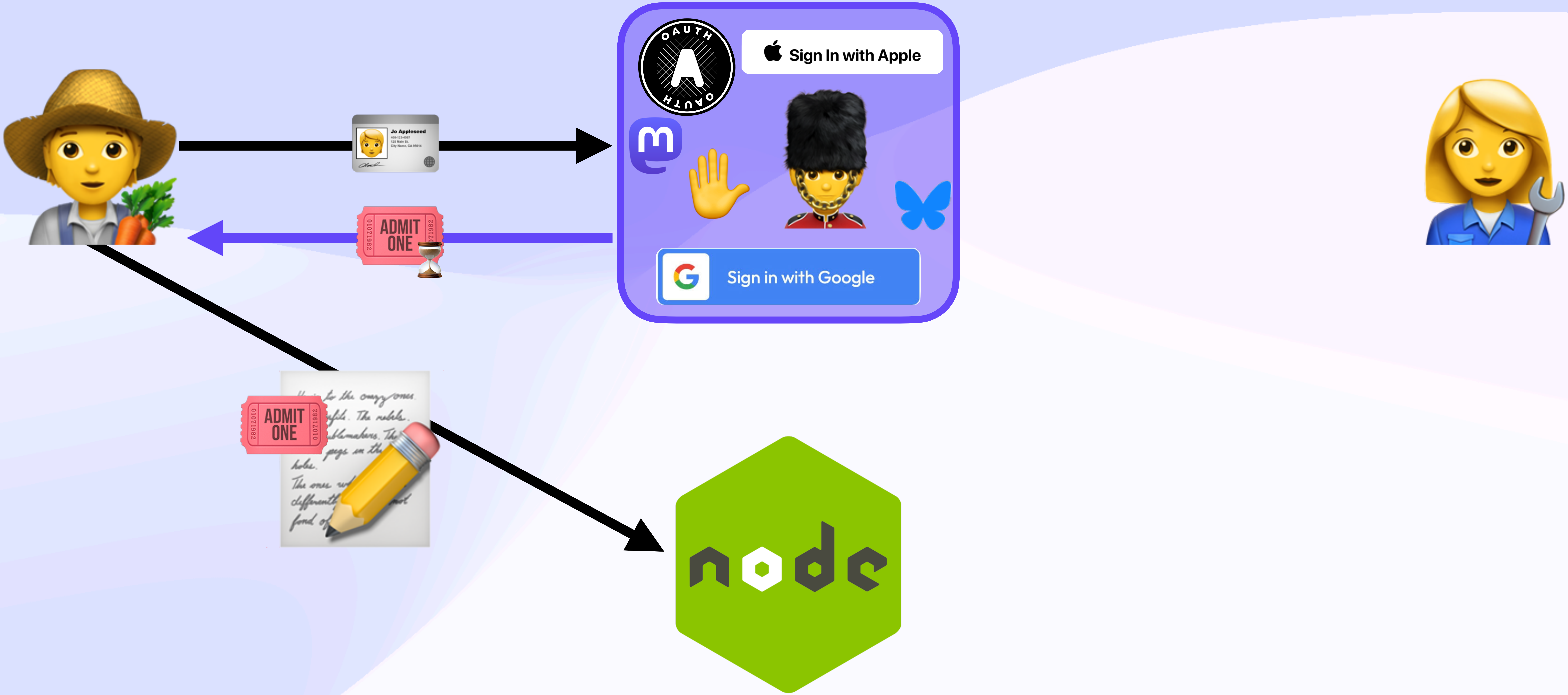
Auth-as-Place

Cloud Auth Flow ☁️



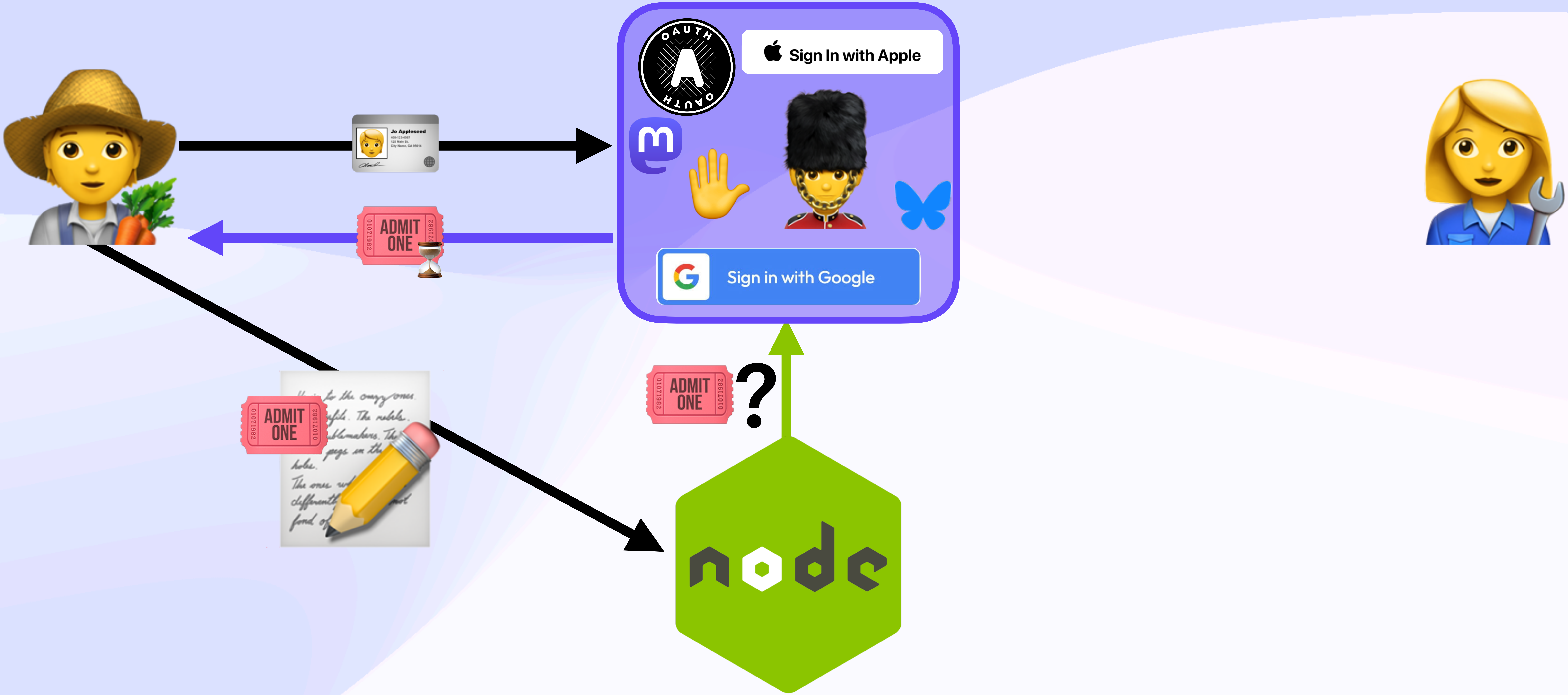
Auth-as-Place

Cloud Auth Flow ☁️



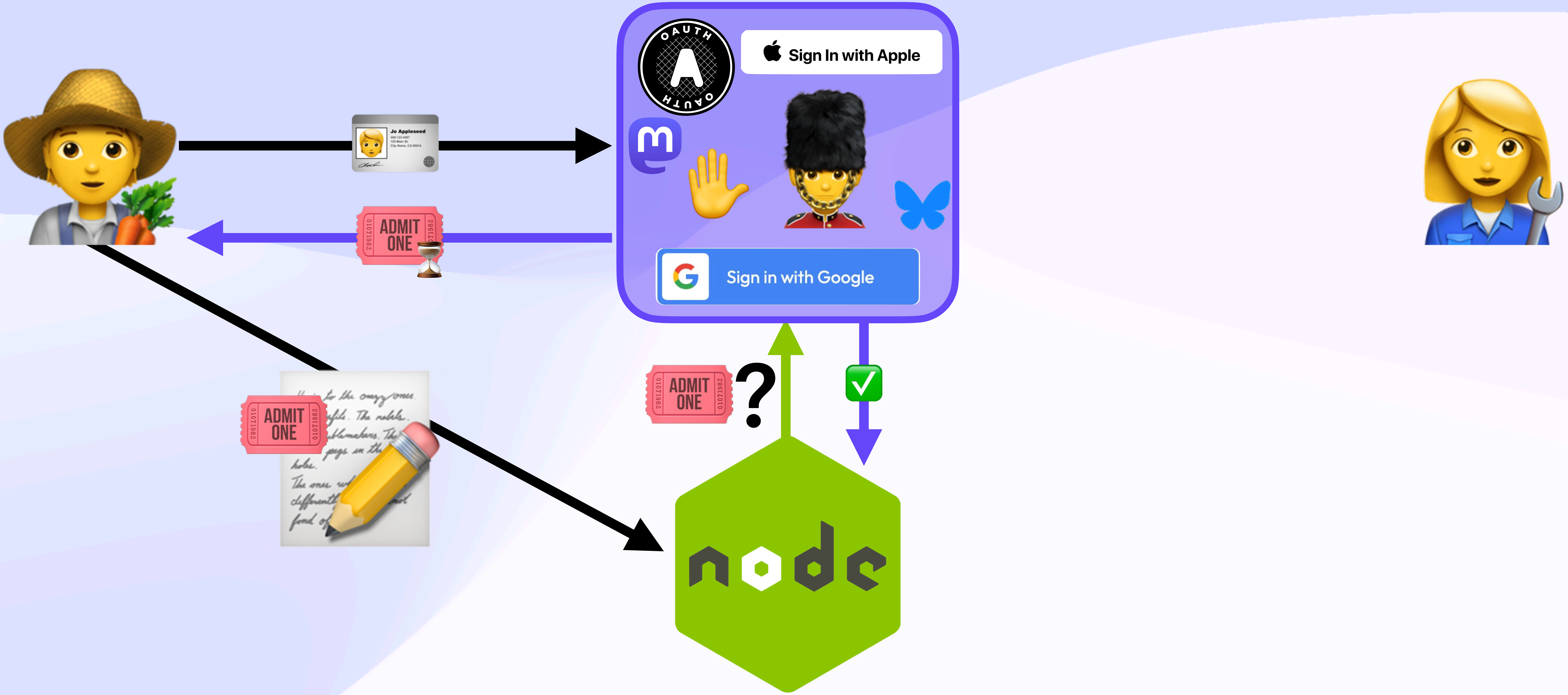
Auth-as-Place

Cloud Auth Flow ☁️



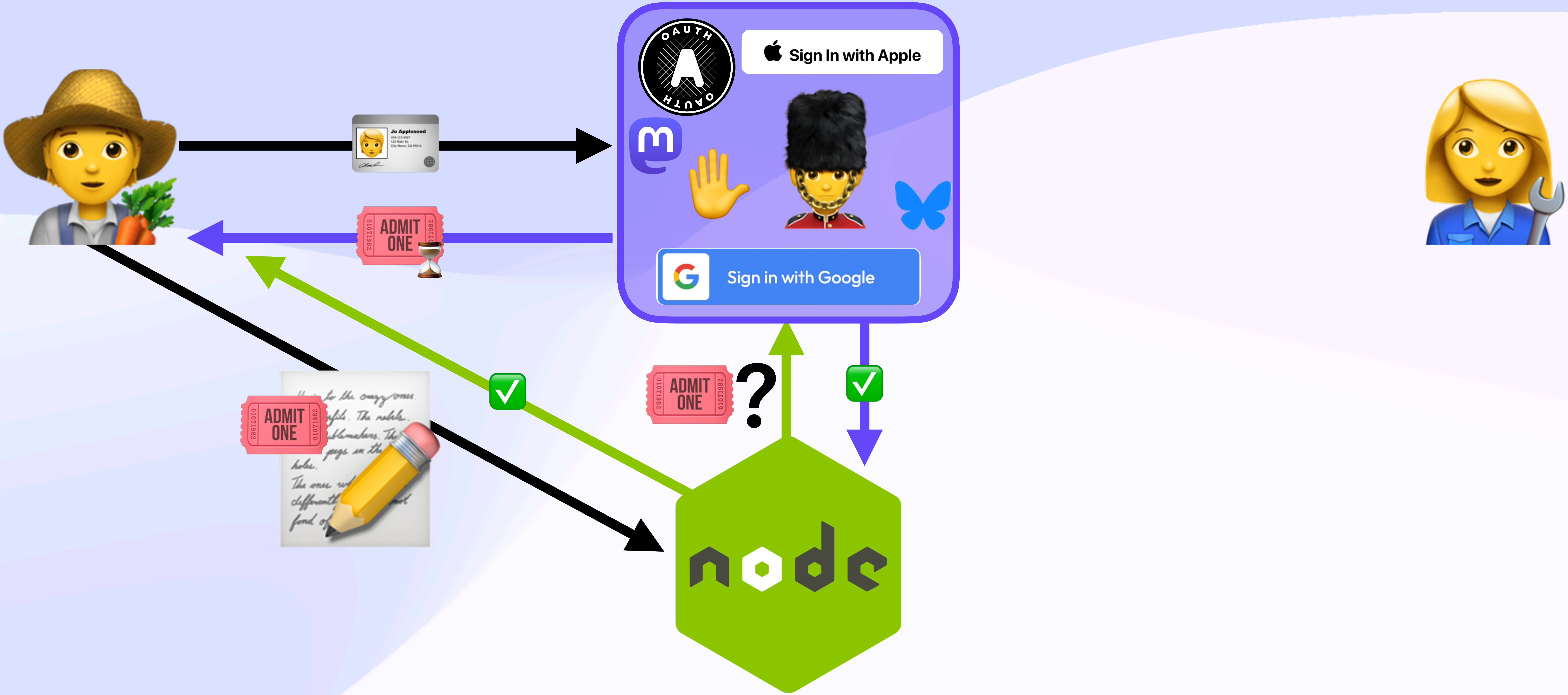
Auth-as-Place

Cloud Auth Flow ☁️



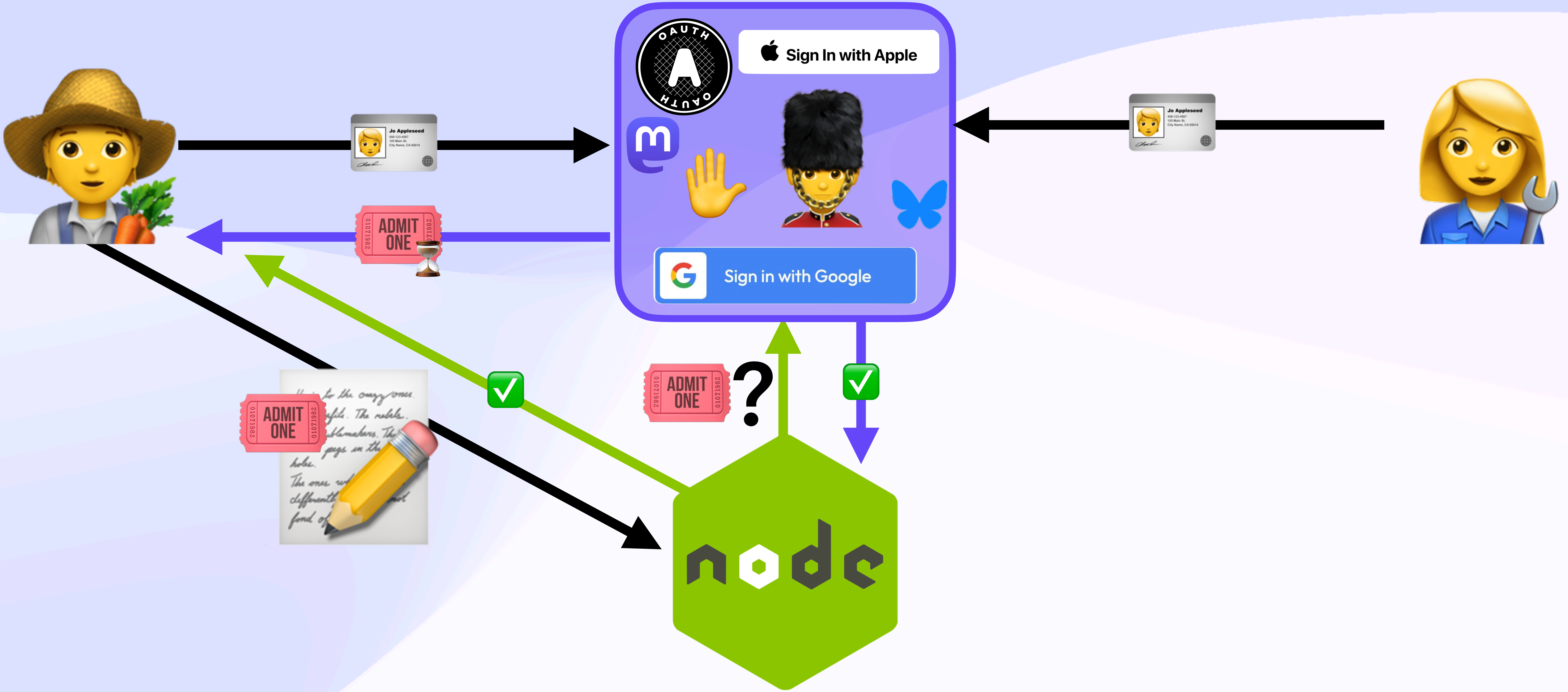
Auth-as-Place

Cloud Auth Flow ☁️



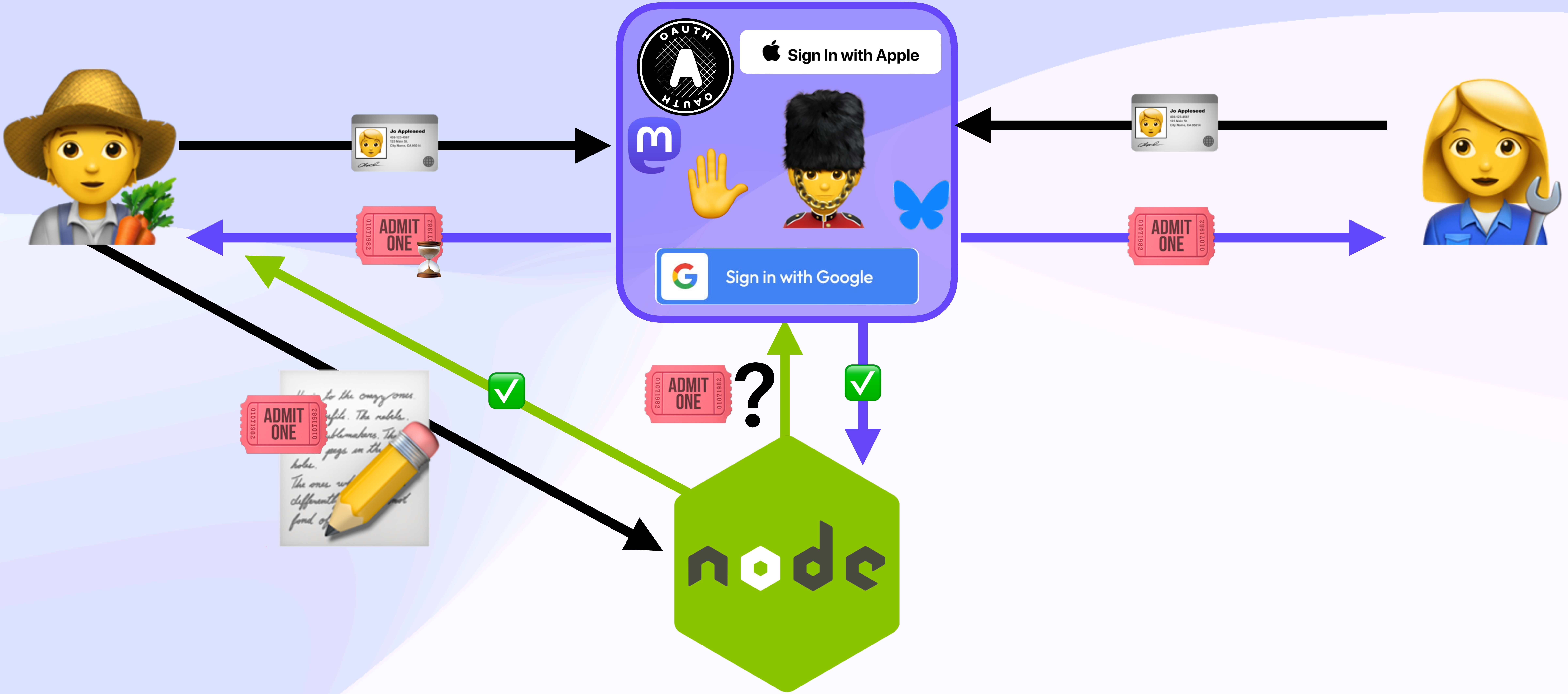
Auth-as-Place

Cloud Auth Flow ☁️



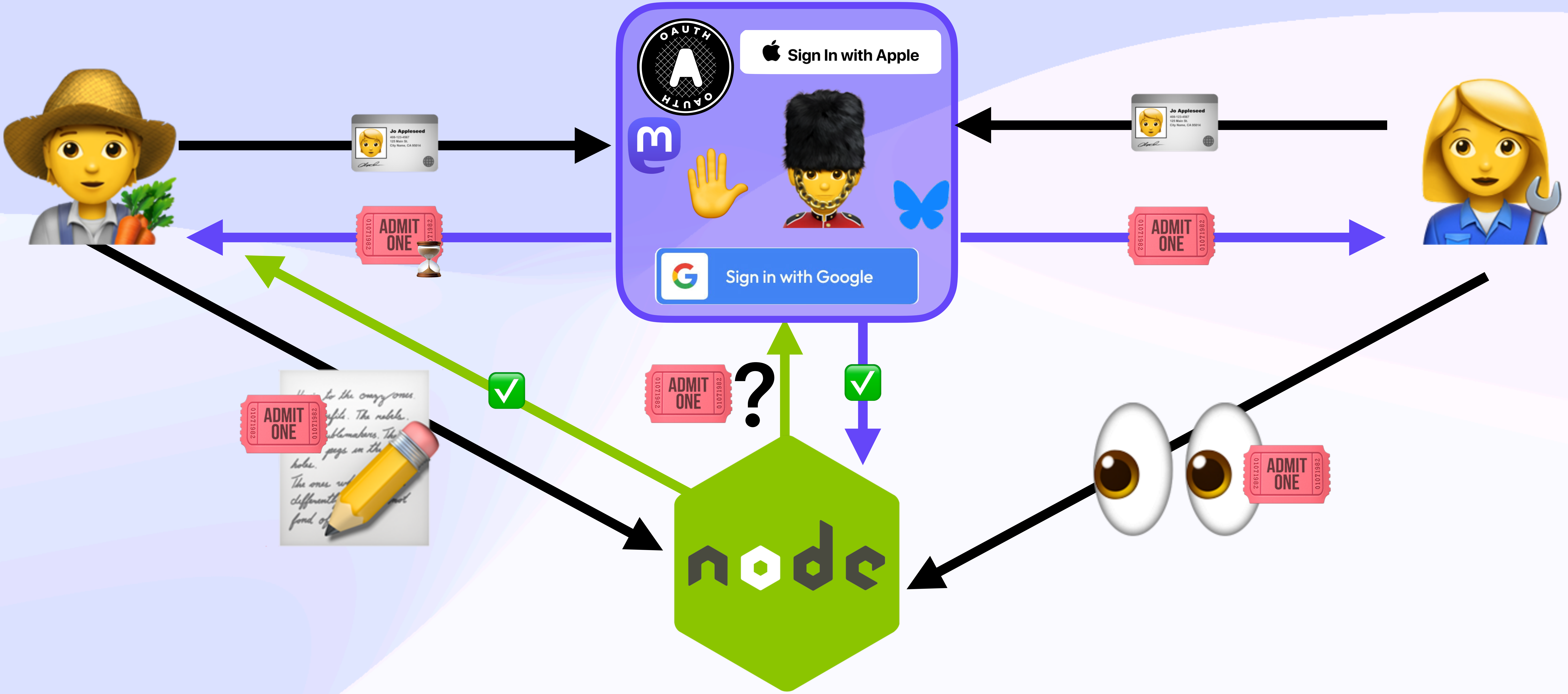
Auth-as-Place

Cloud Auth Flow ☁️



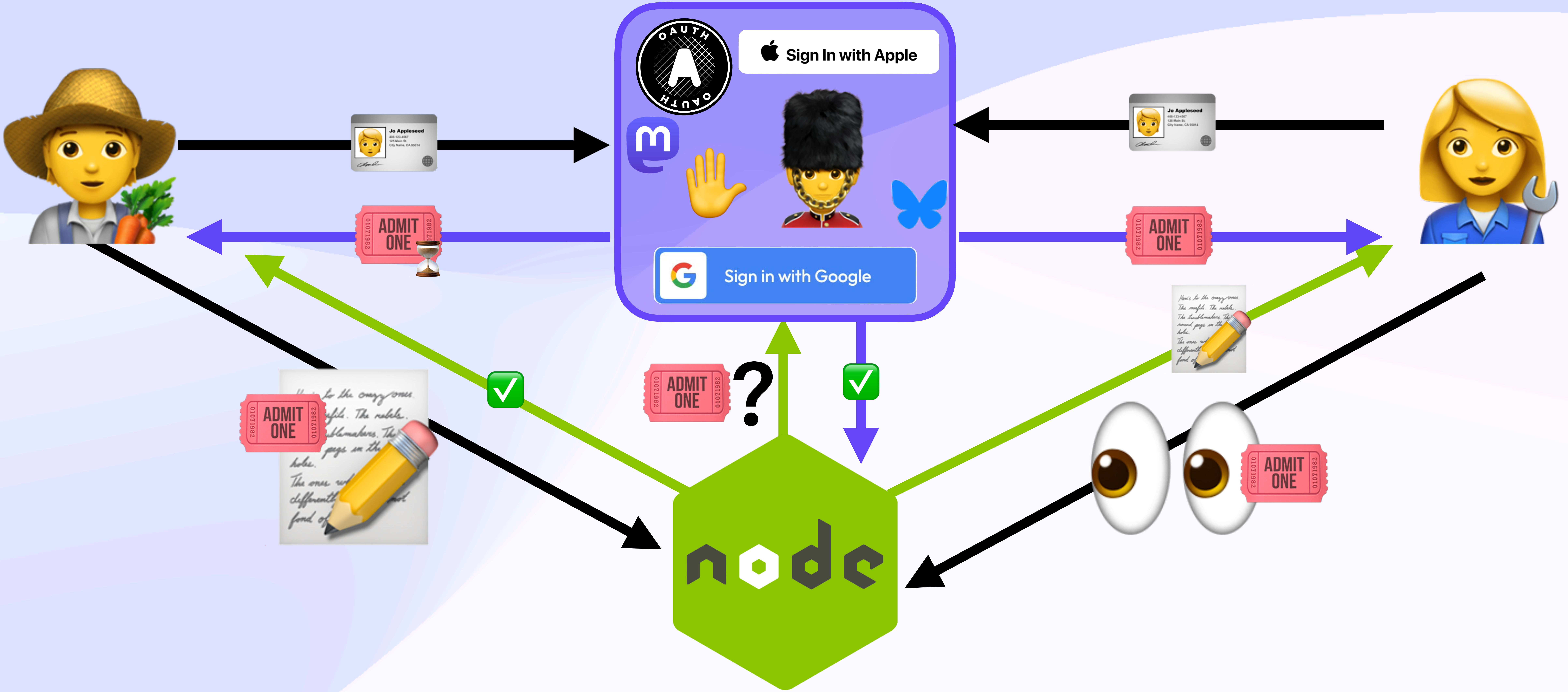
Auth-as-Place

Cloud Auth Flow ☁️



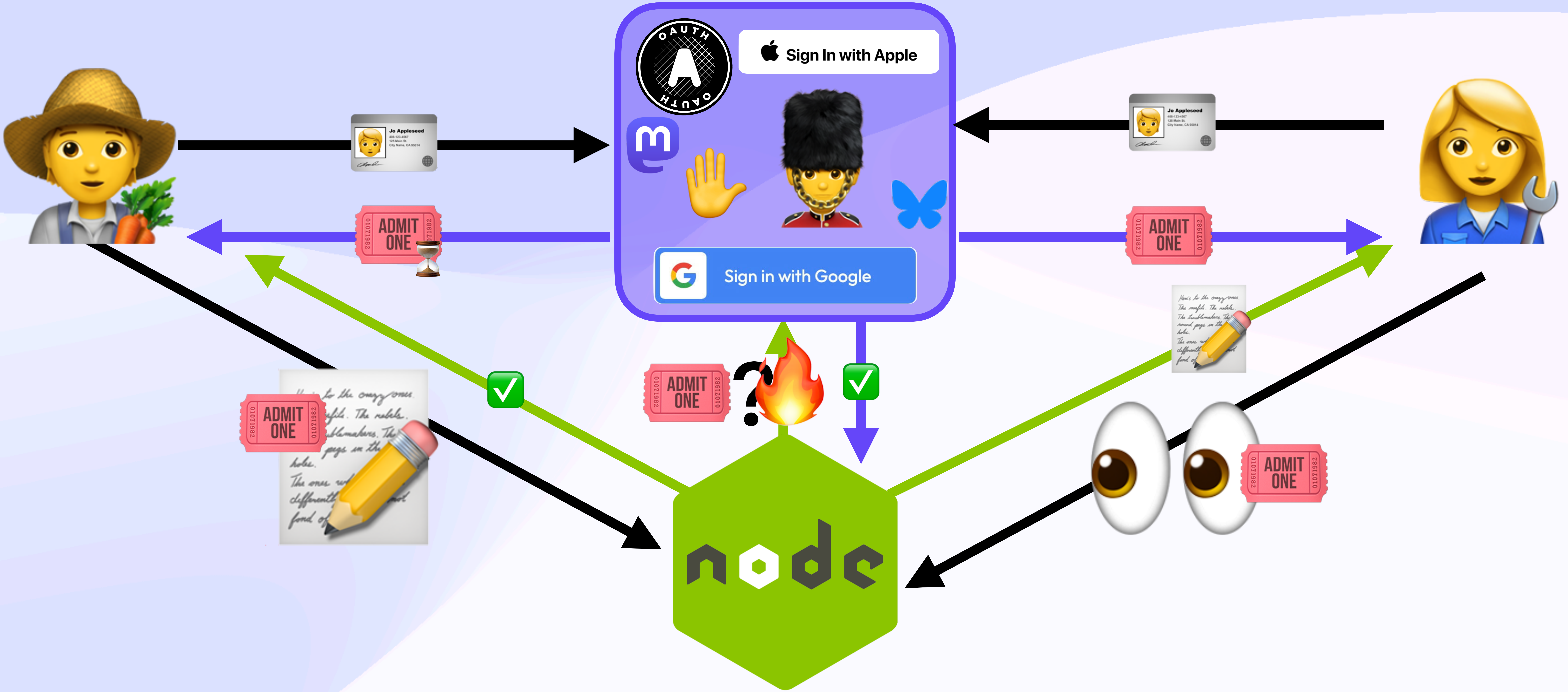
Auth-as-Place

Cloud Auth Flow ☁️



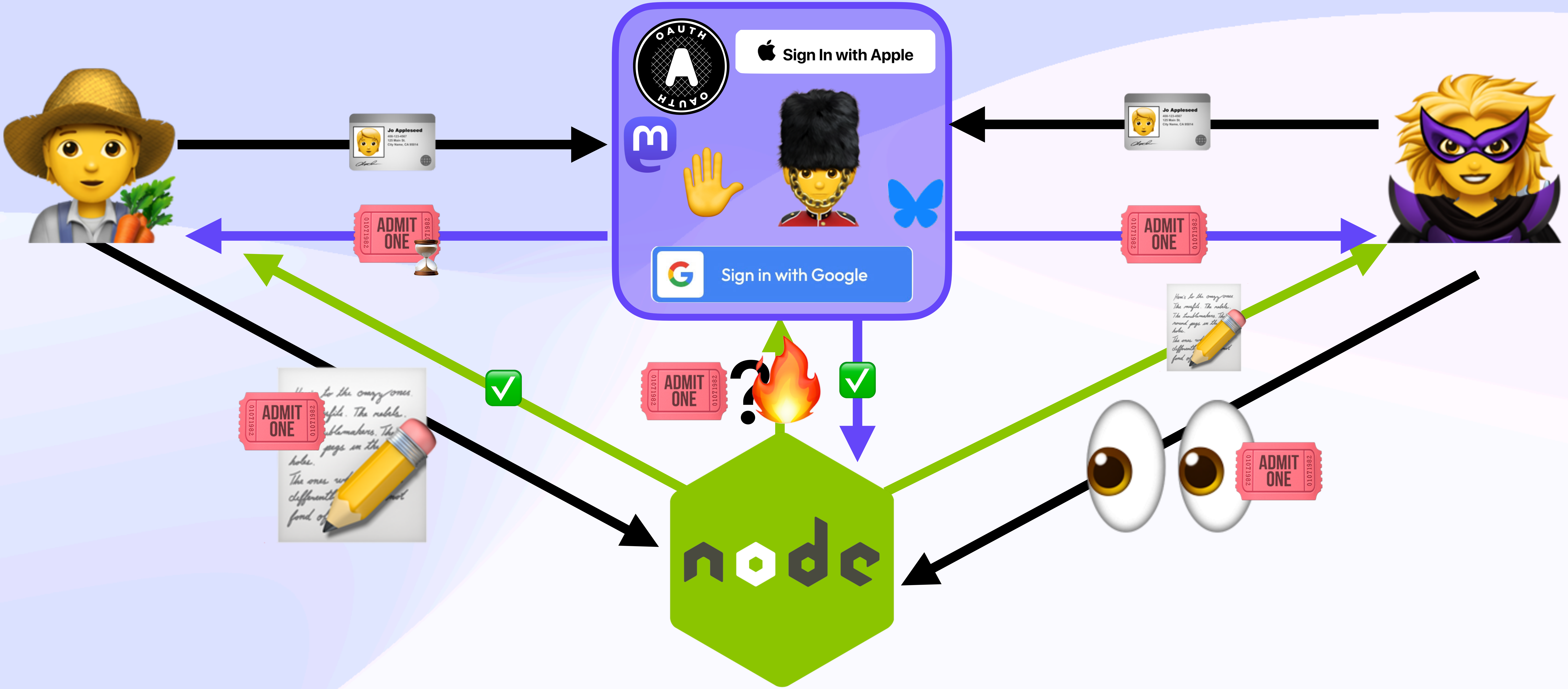
Auth-as-Place

Cloud Auth Flow ☁️



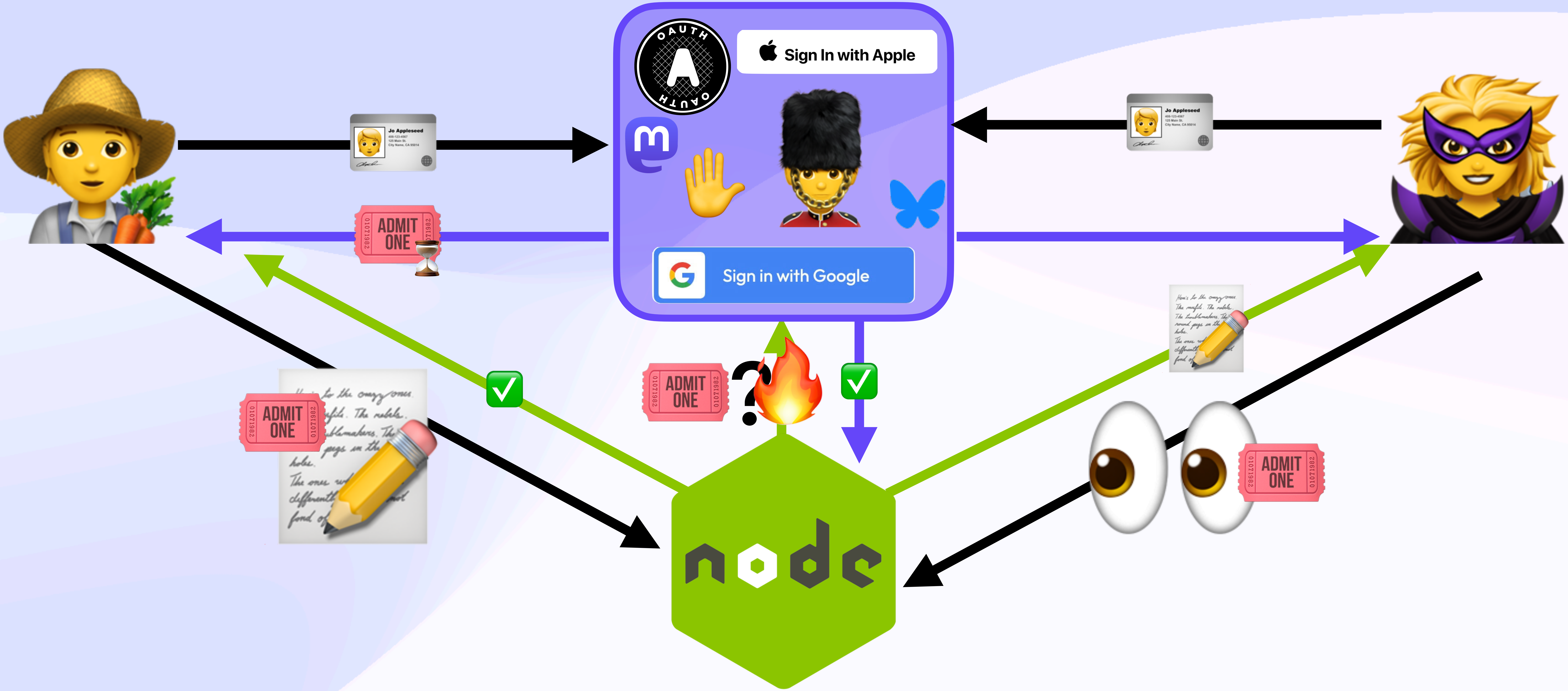
Auth-as-Place

Cloud Auth Flow ☁️



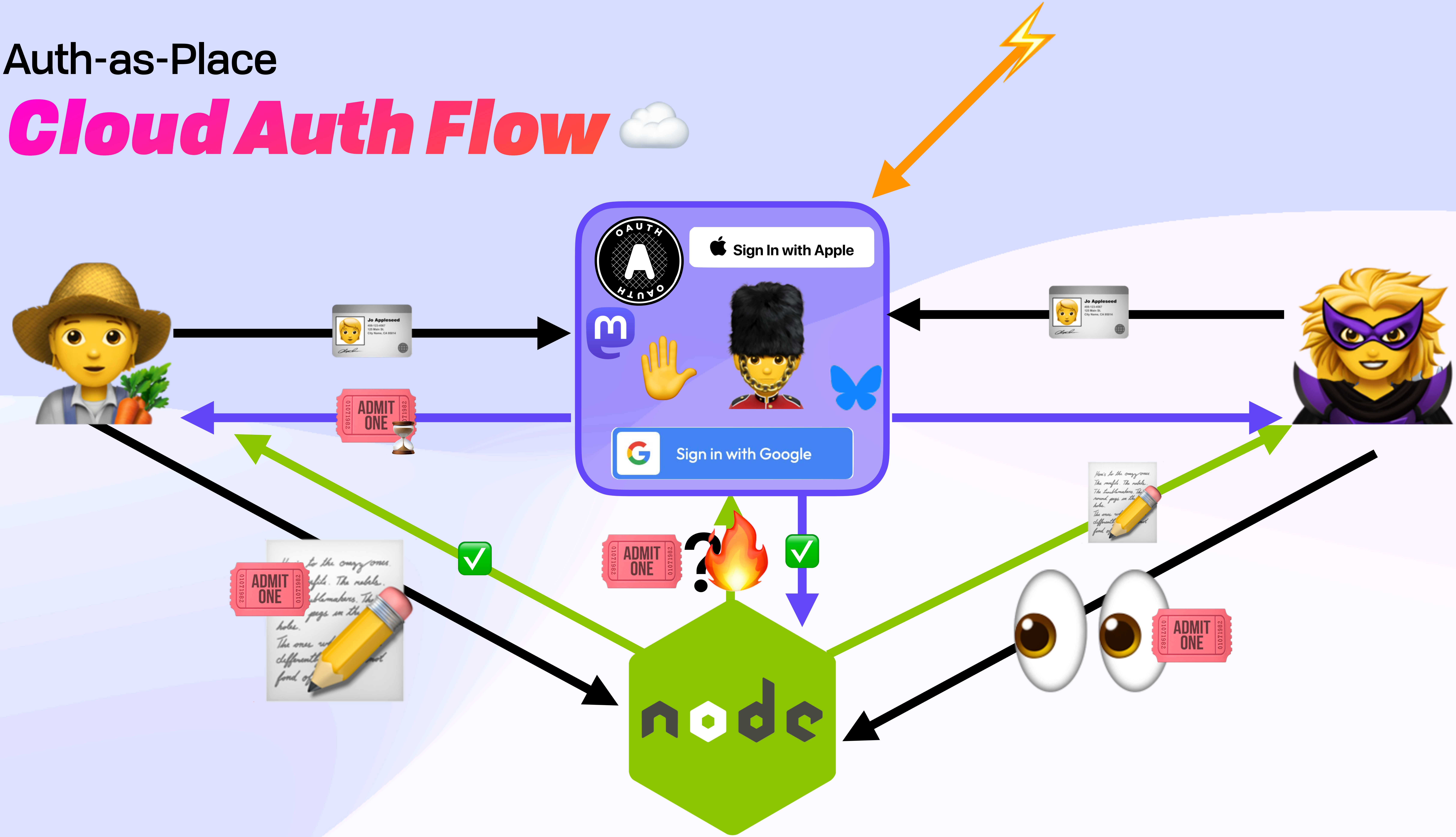
Auth-as-Place

Cloud Auth Flow ☁️



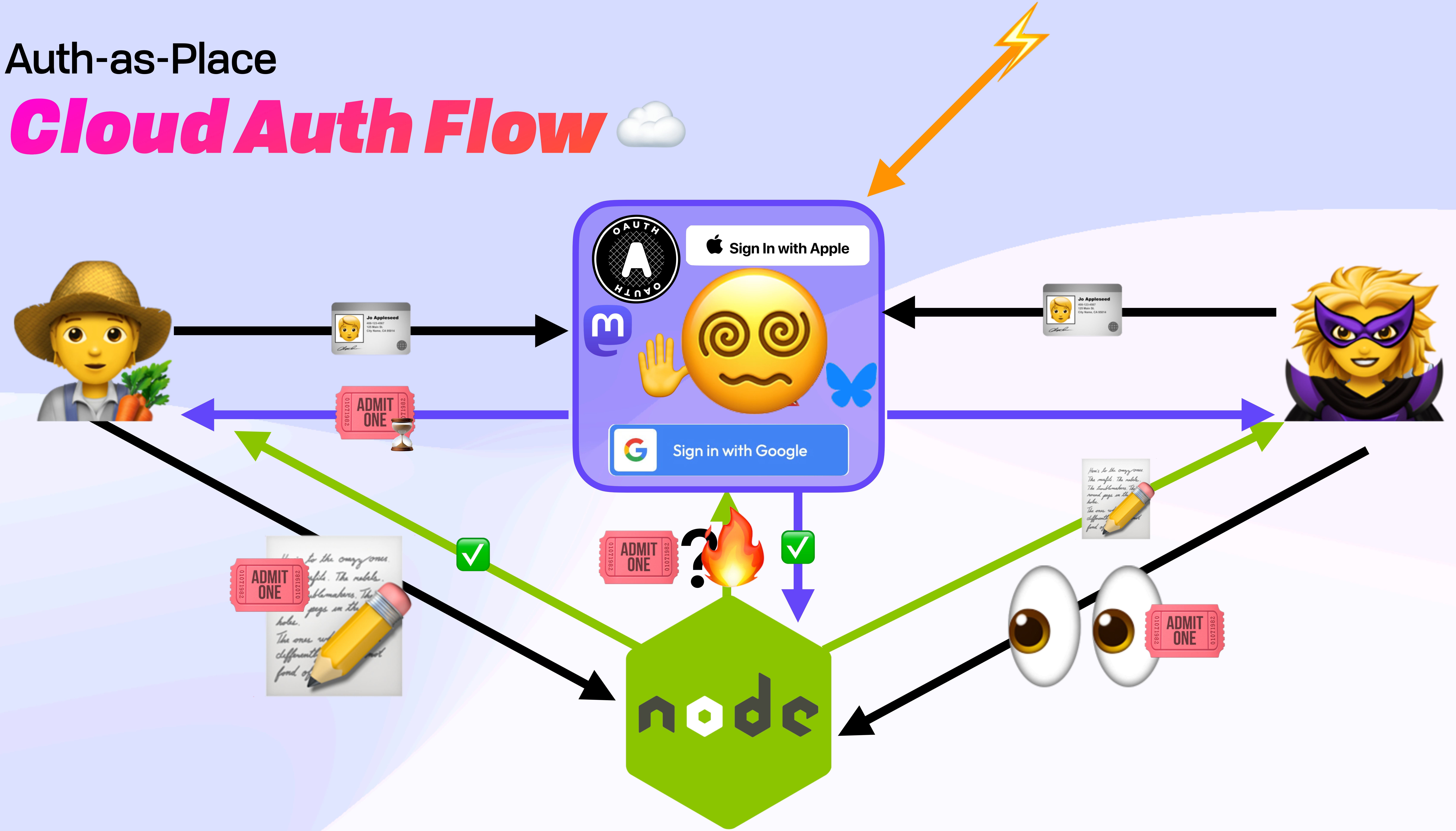
Auth-as-Place

Cloud Auth Flow ☁️



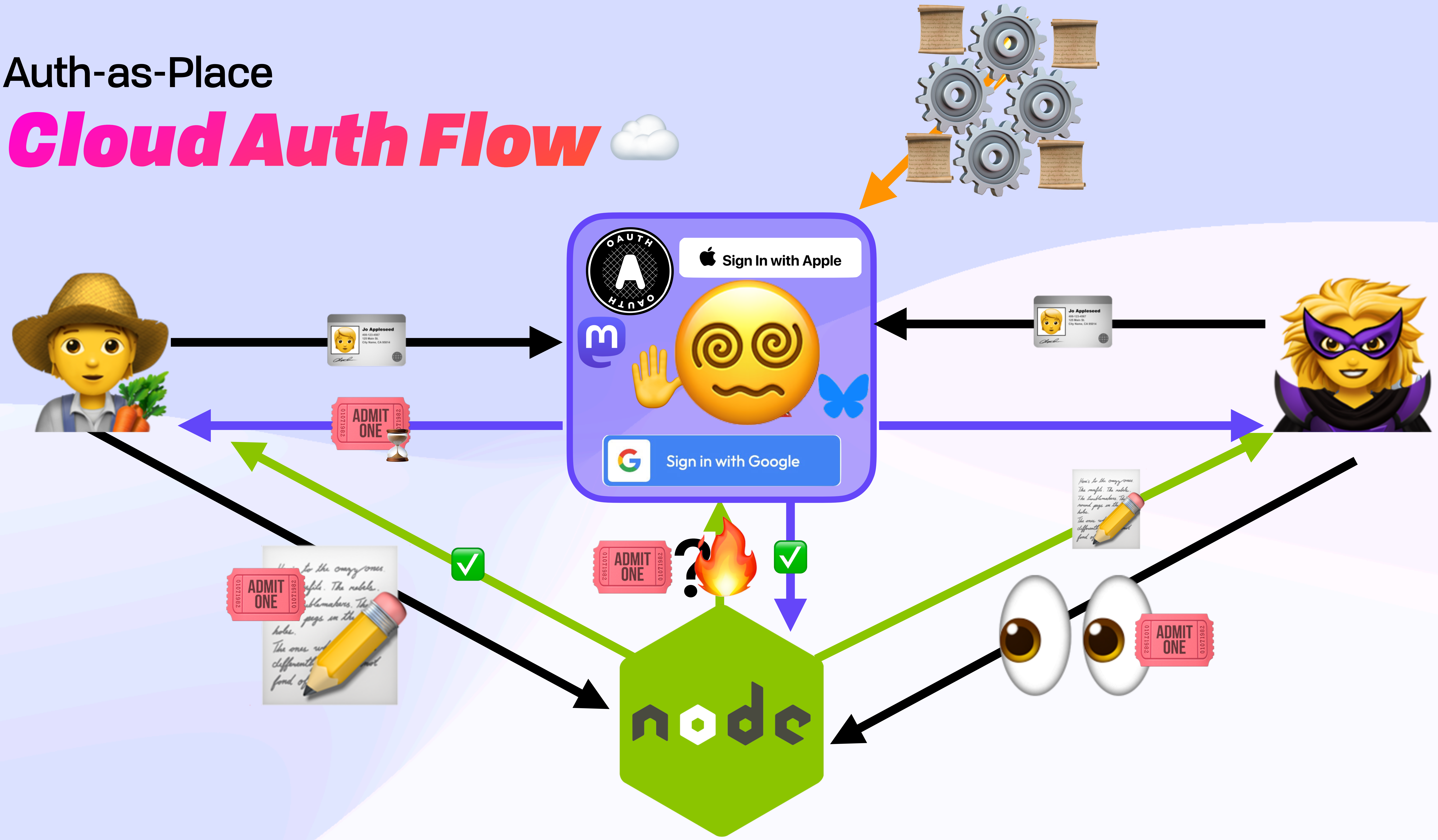
Auth-as-Place

Cloud Auth Flow ☁️



Auth-as-Place

Cloud Auth Flow ☁️



Cloud: Auth-as-Place ☁️

Cloud: Auth-as-Place ☁️

OAUTH
Sign In with Apple
Sign in with Google

Auth-as-Place

Cloud: Auth-as-Place ☁️

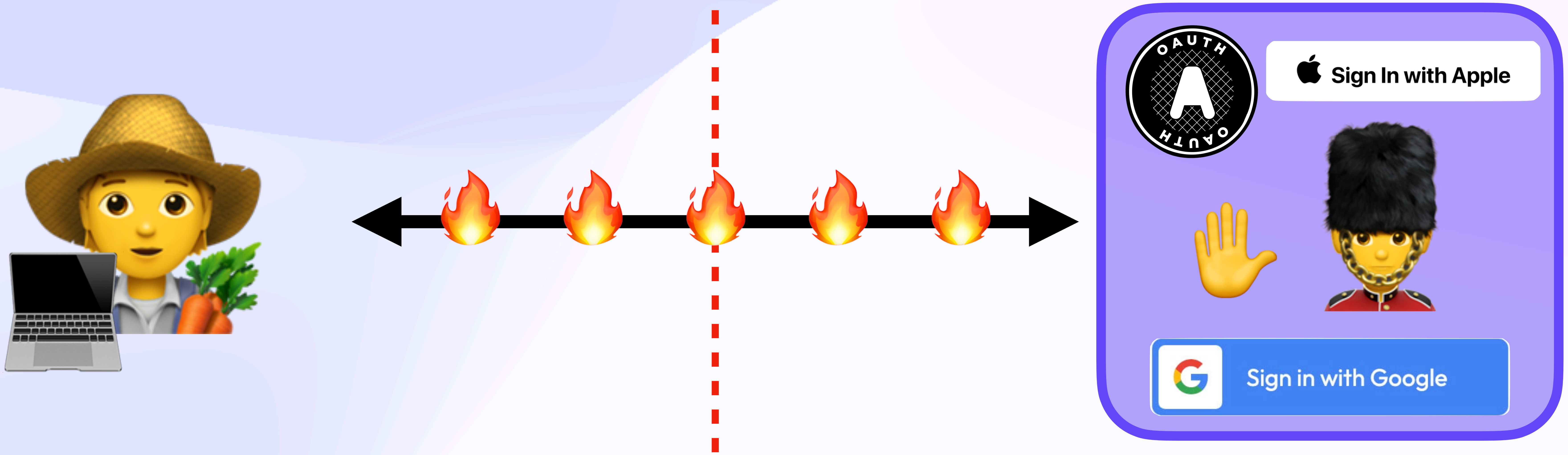
"Over Here"

"Over There"

Cloud: Auth-as-Place ☁️

"Over Here"

"Over There"



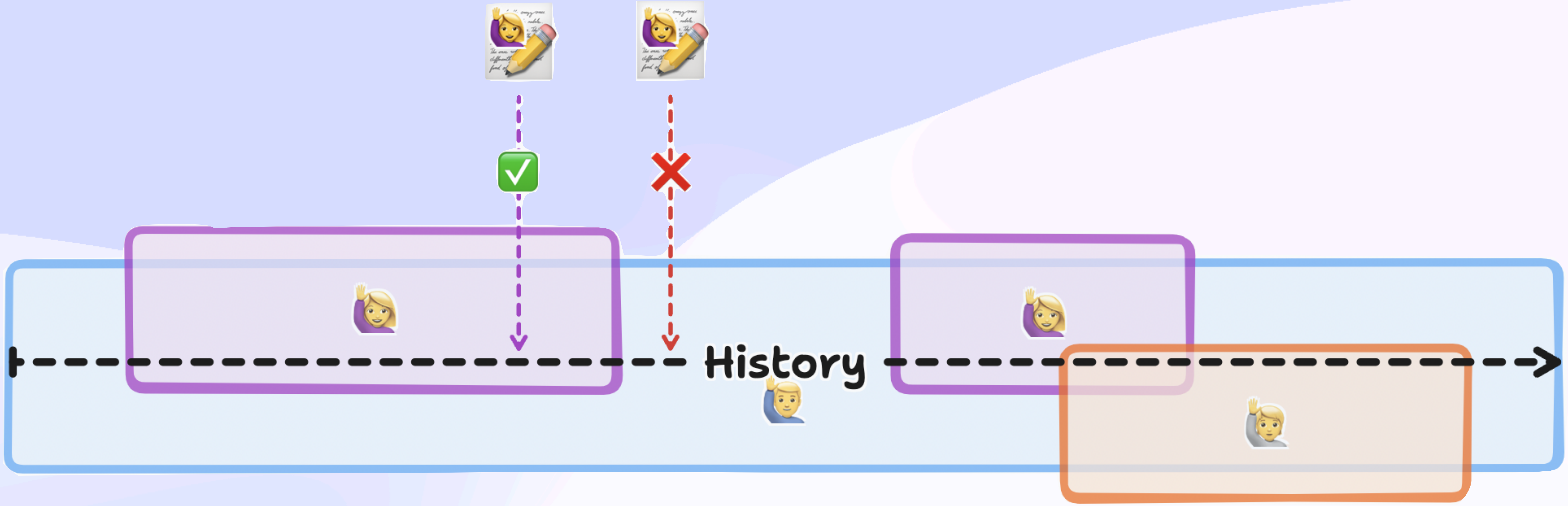
"Over there" is a bottleneck / hard to scale

Playing By New Rules 🎯

Local Context

Local Context

Adds & Removals Over Time



Local Context

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

Local Context

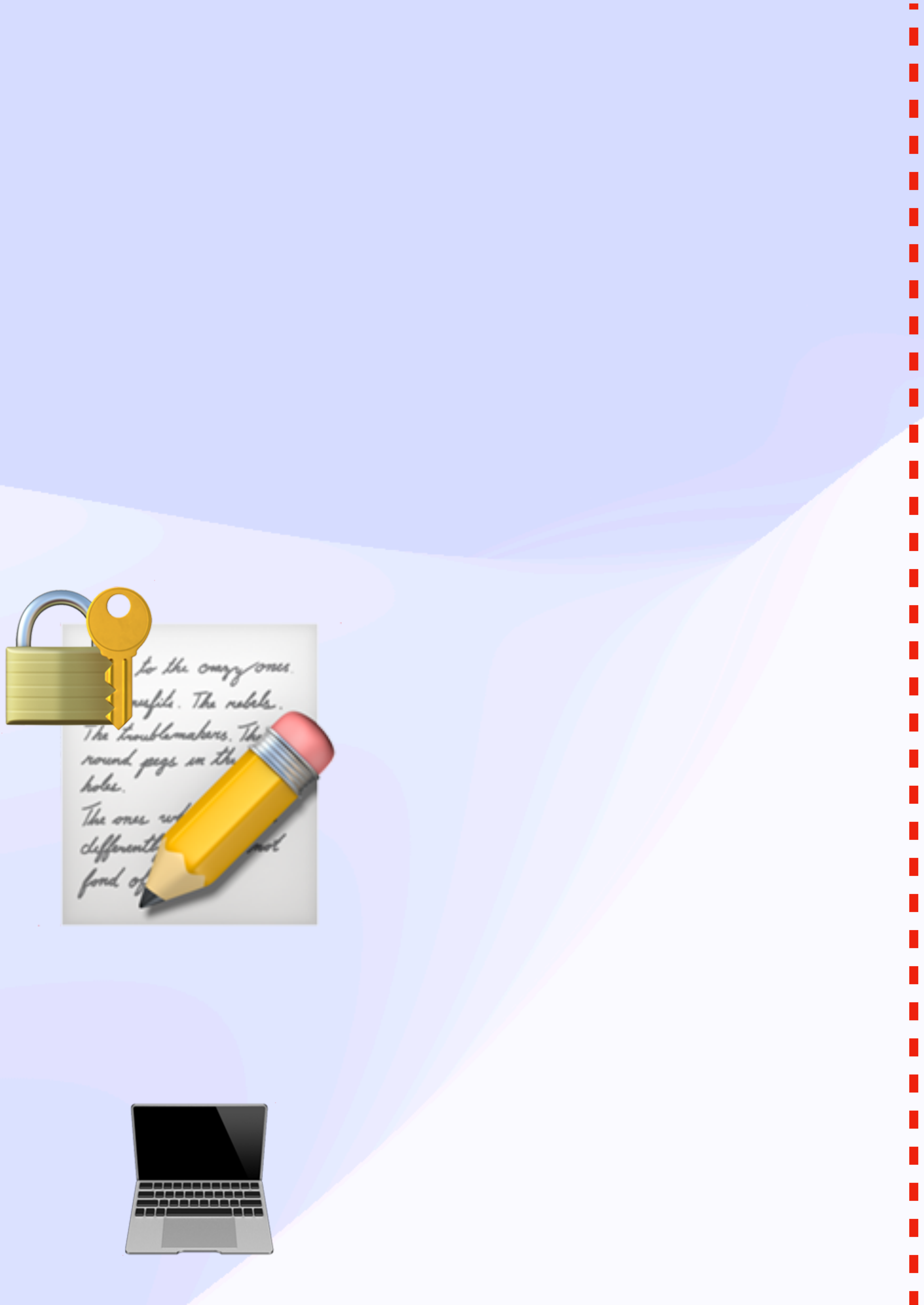
Auth-as-Data: "Auth Must Travel with Data" 🧳

📝

💻

Local Context

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

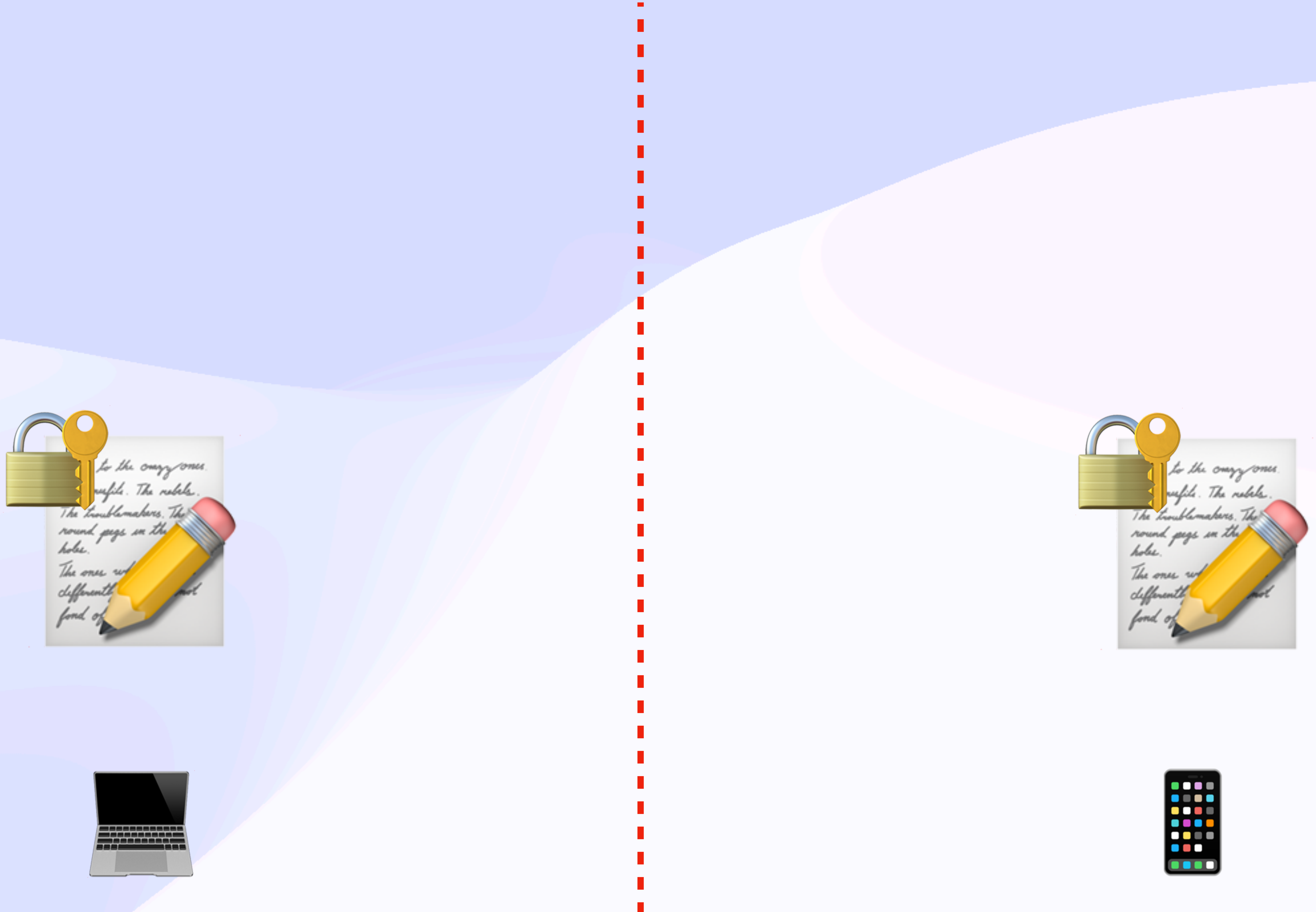


Local Context

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

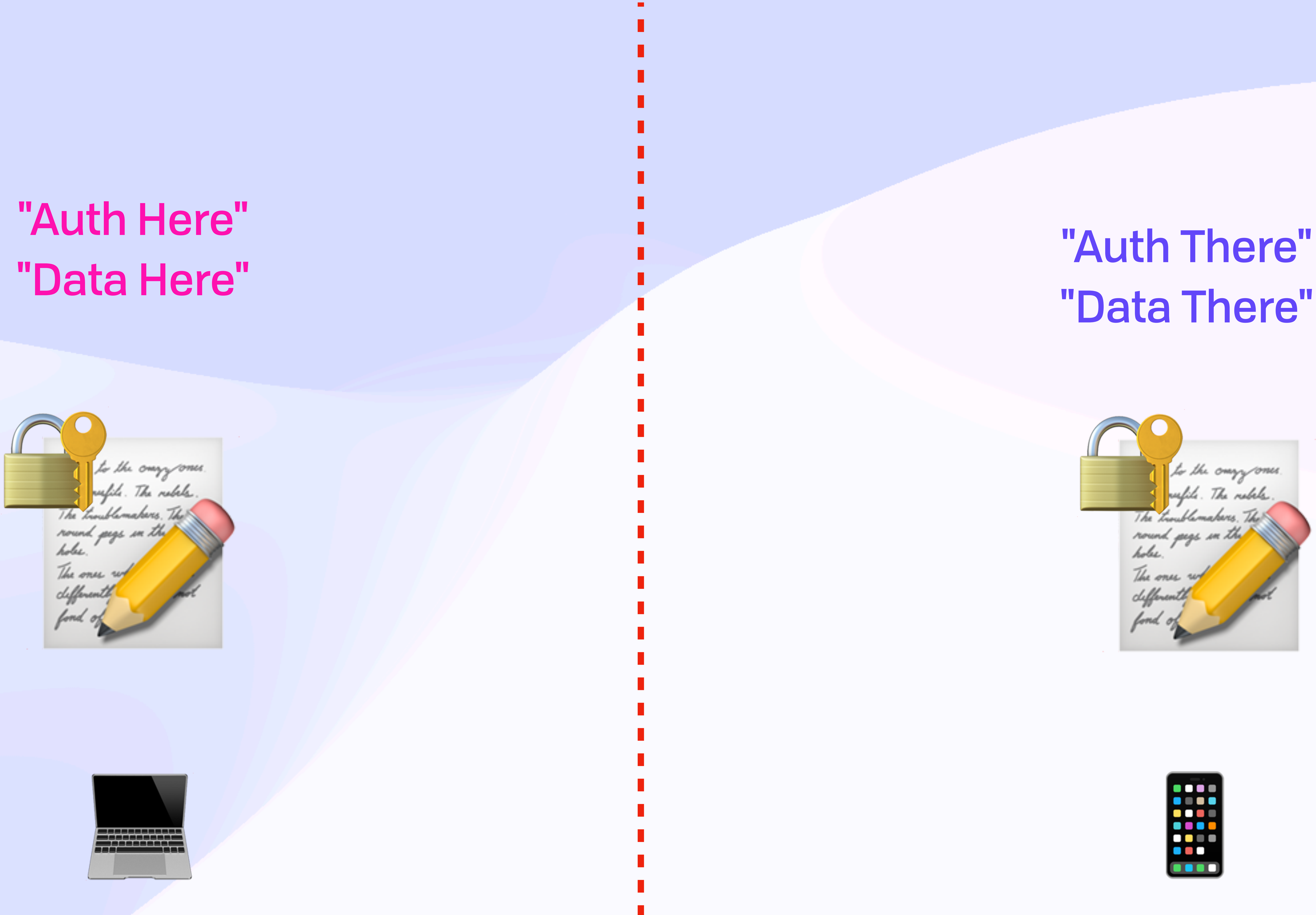
Local Context

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



Local Context

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

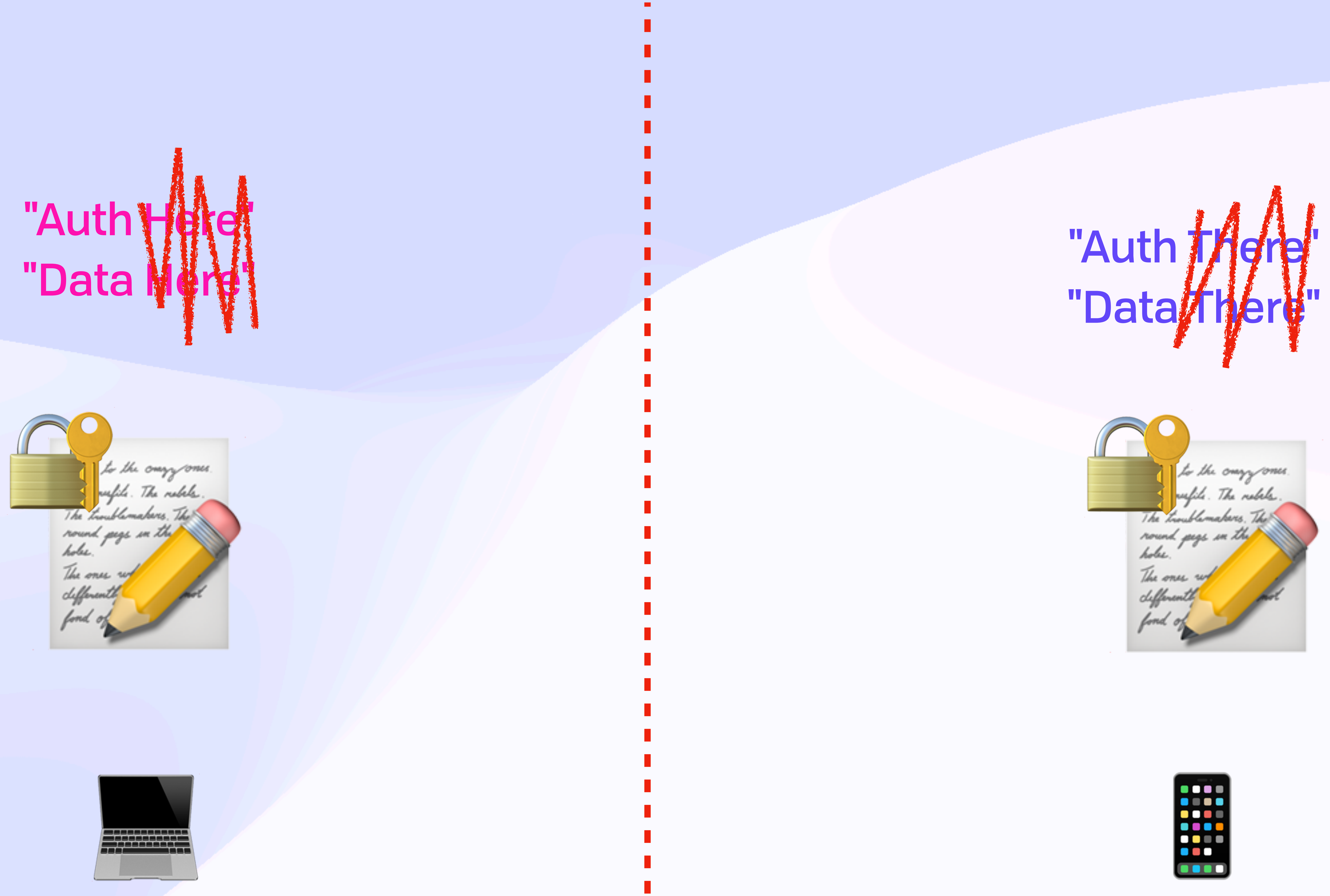


"Auth Here"
"Data Here"

"Auth There"
"Data There"

Local Context

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

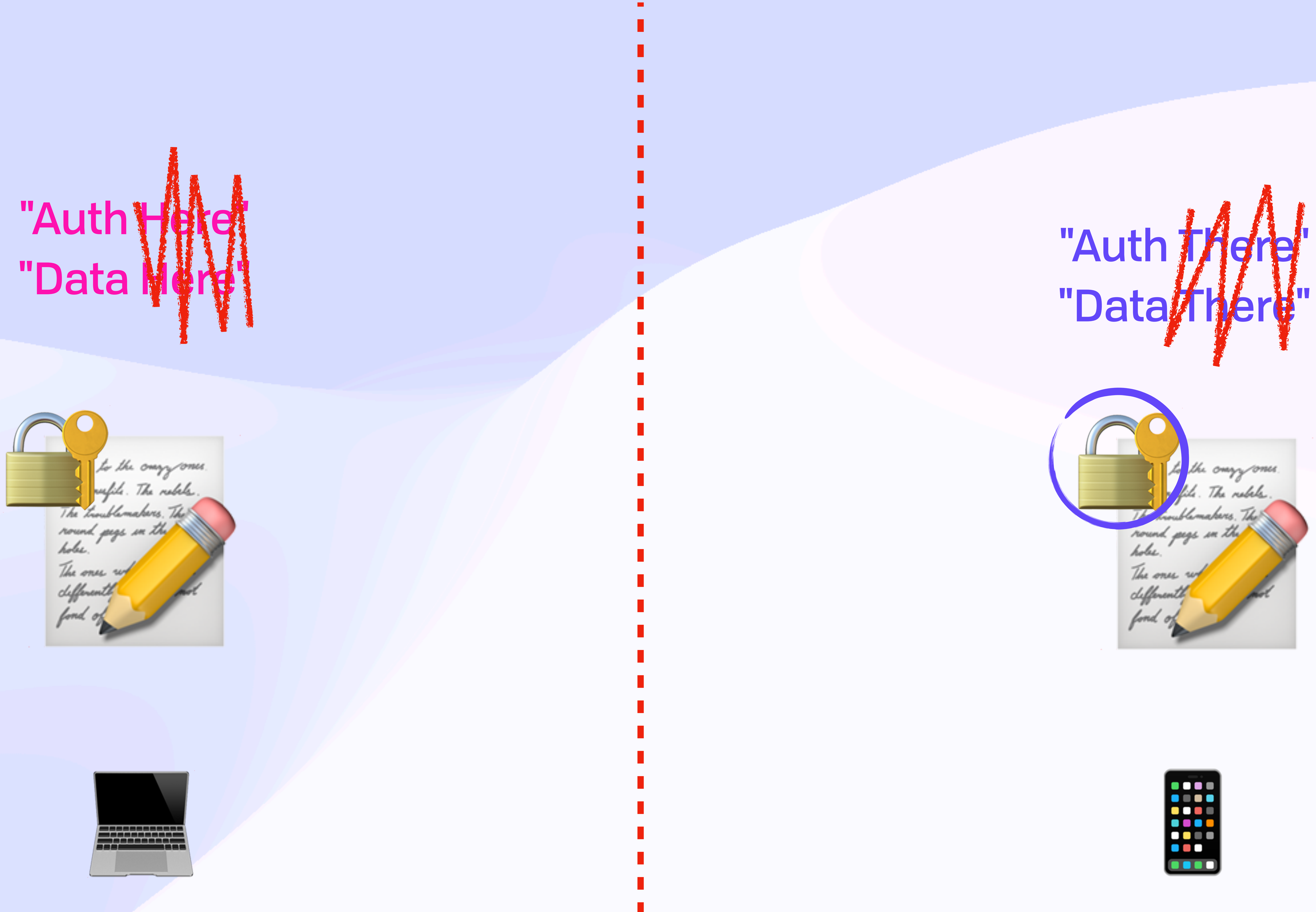


"Auth ~~Here~~"
"Data ~~Here~~"

"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

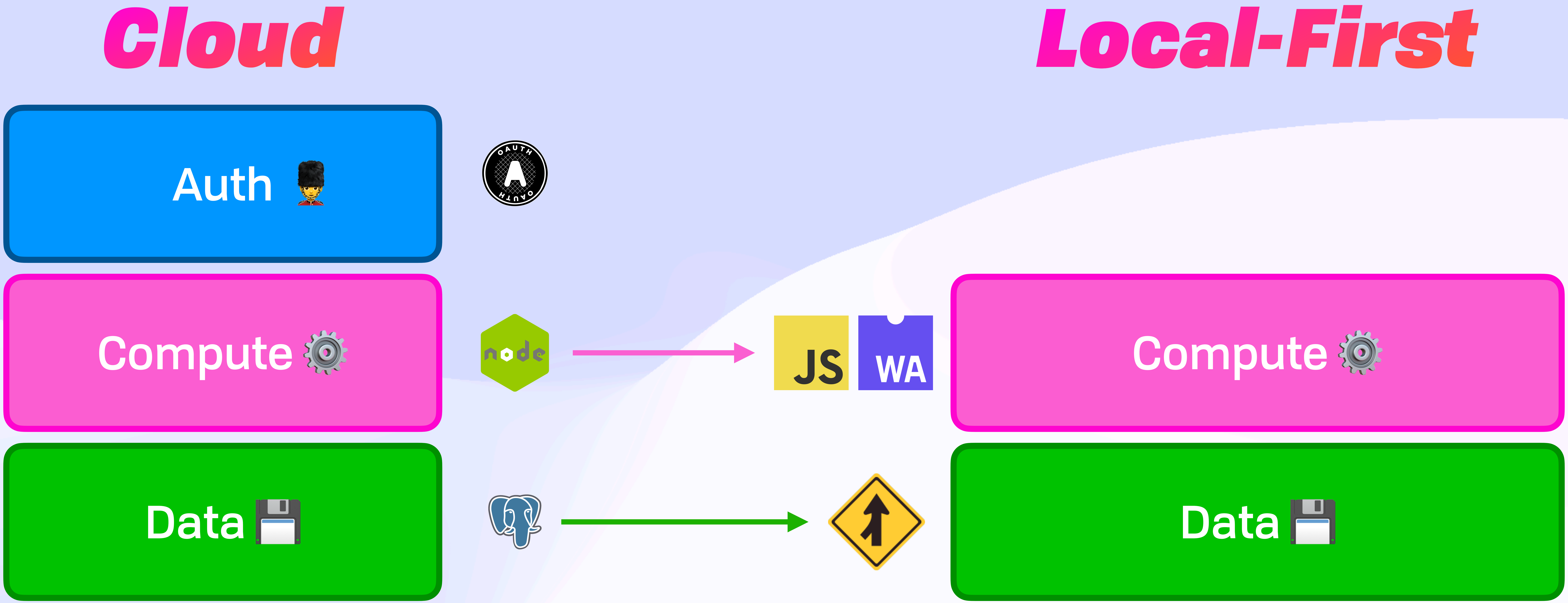
Local-First

Auth 💂

Compute ⚙️

Data 💾

Local Context



Cloud

Auth 💂

Compute ⚙️

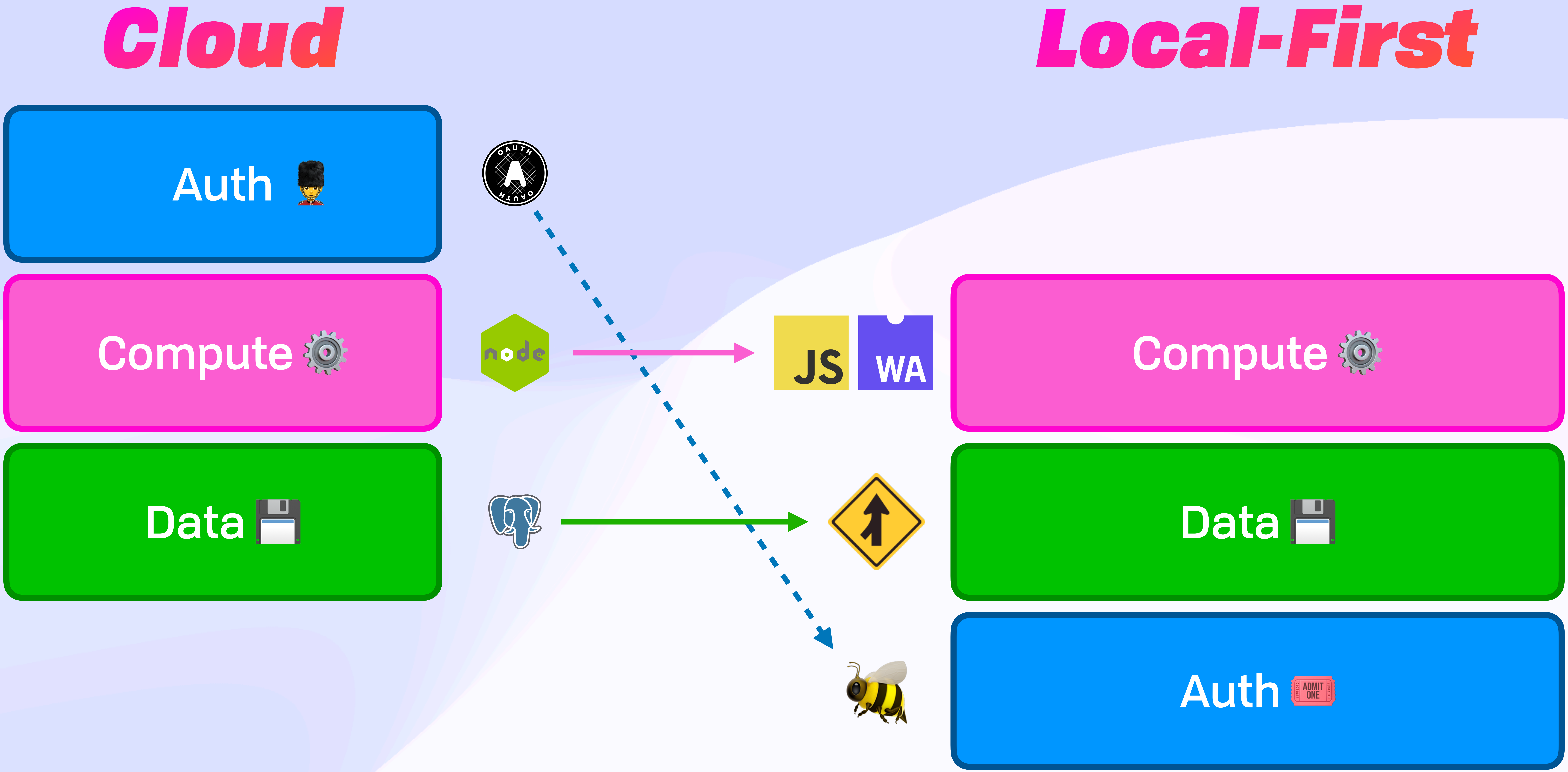
Data 💾

Local-First

Compute ⚙️

Data 💾

Local Context



Cloud

Auth 💂

Compute ⚙️

Data 💾

Local-First

Compute ⚙️

Data 💾

Auth 🎟️

Securing Data *Wherever It Happens To Be*

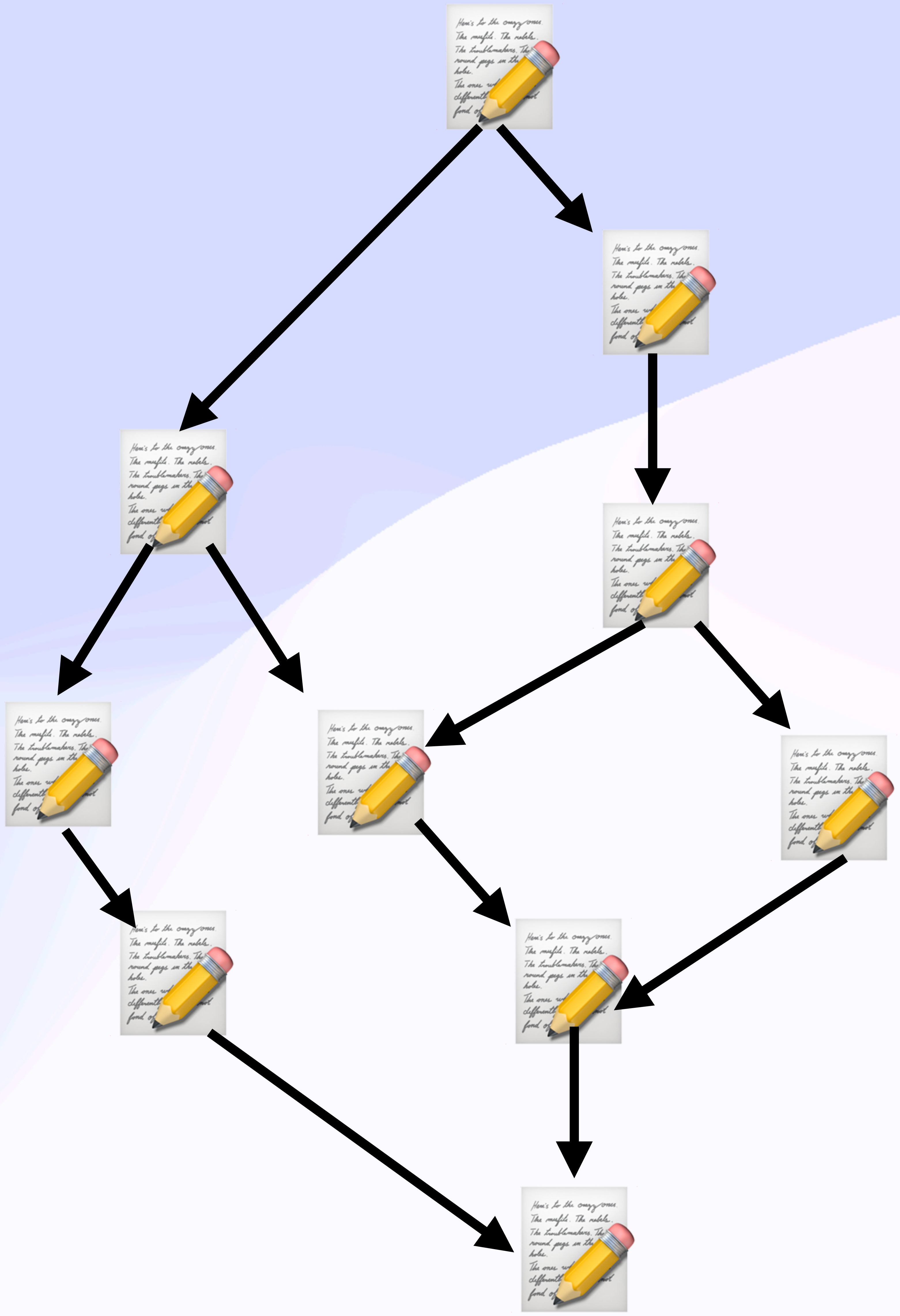
End-to-End Encryption

End-to-End Encryption

Tradeoffs

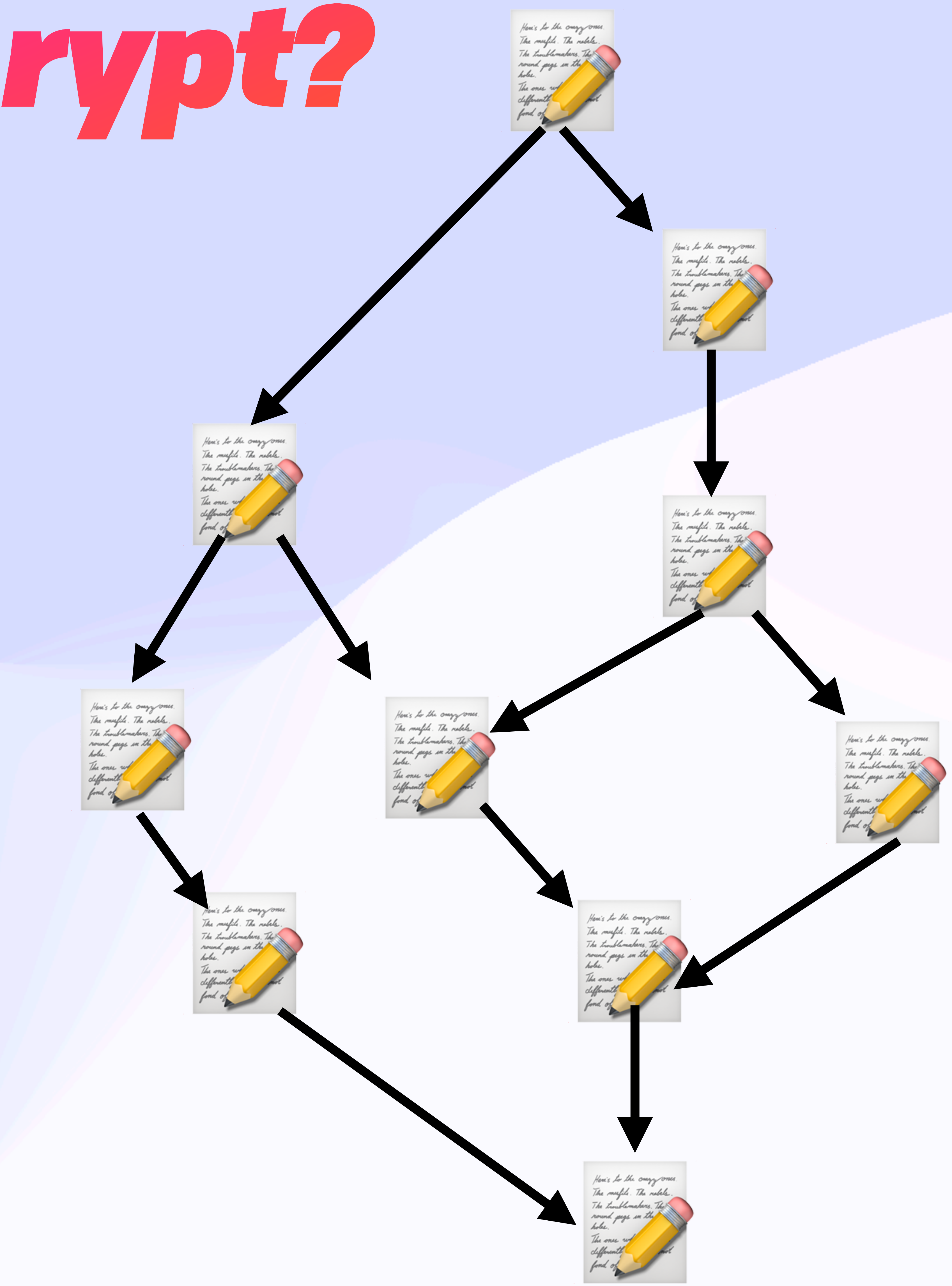
End-to-End Encryption

Tradeoffs



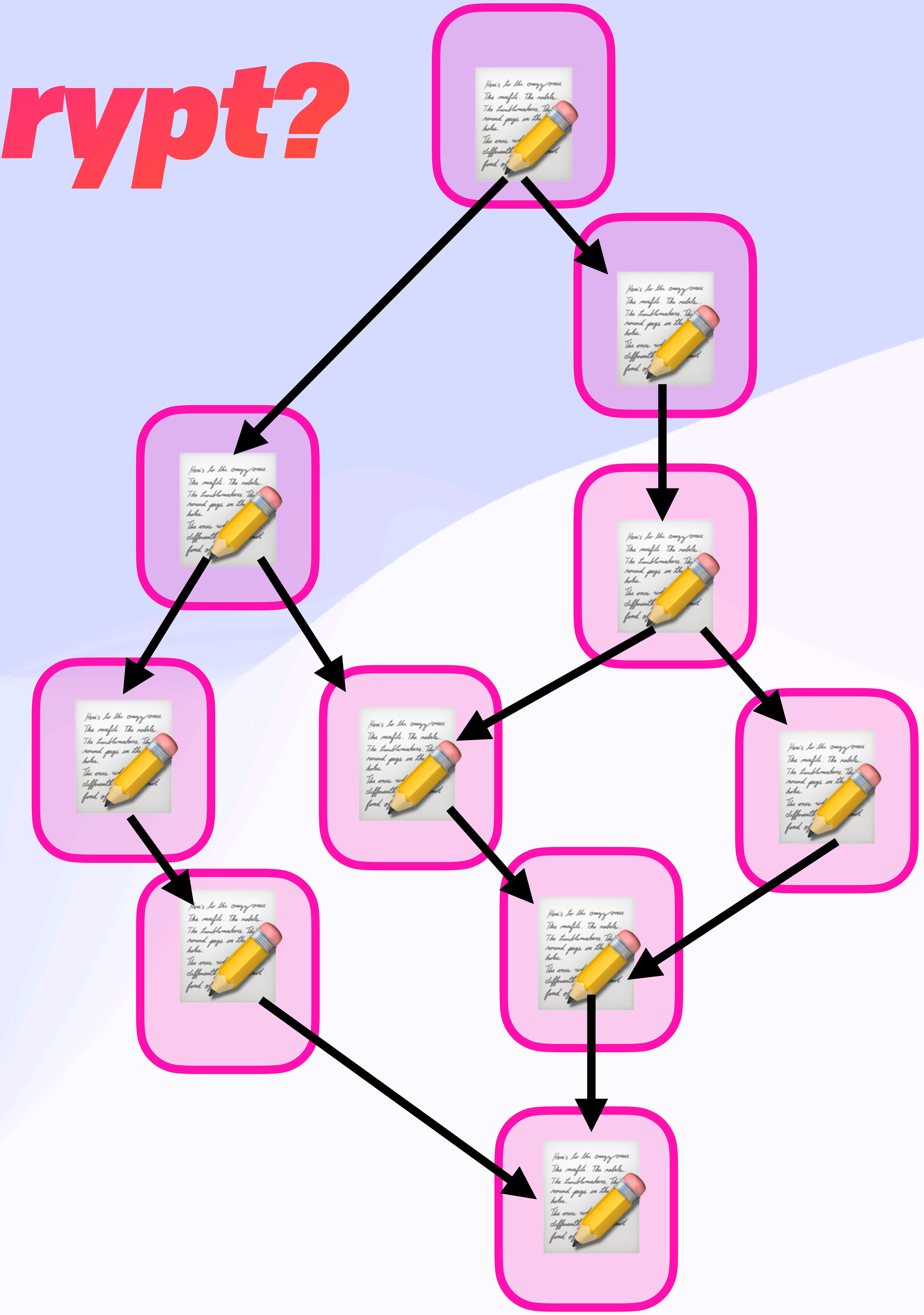
End-to-End Encryption

What To Encrypt?



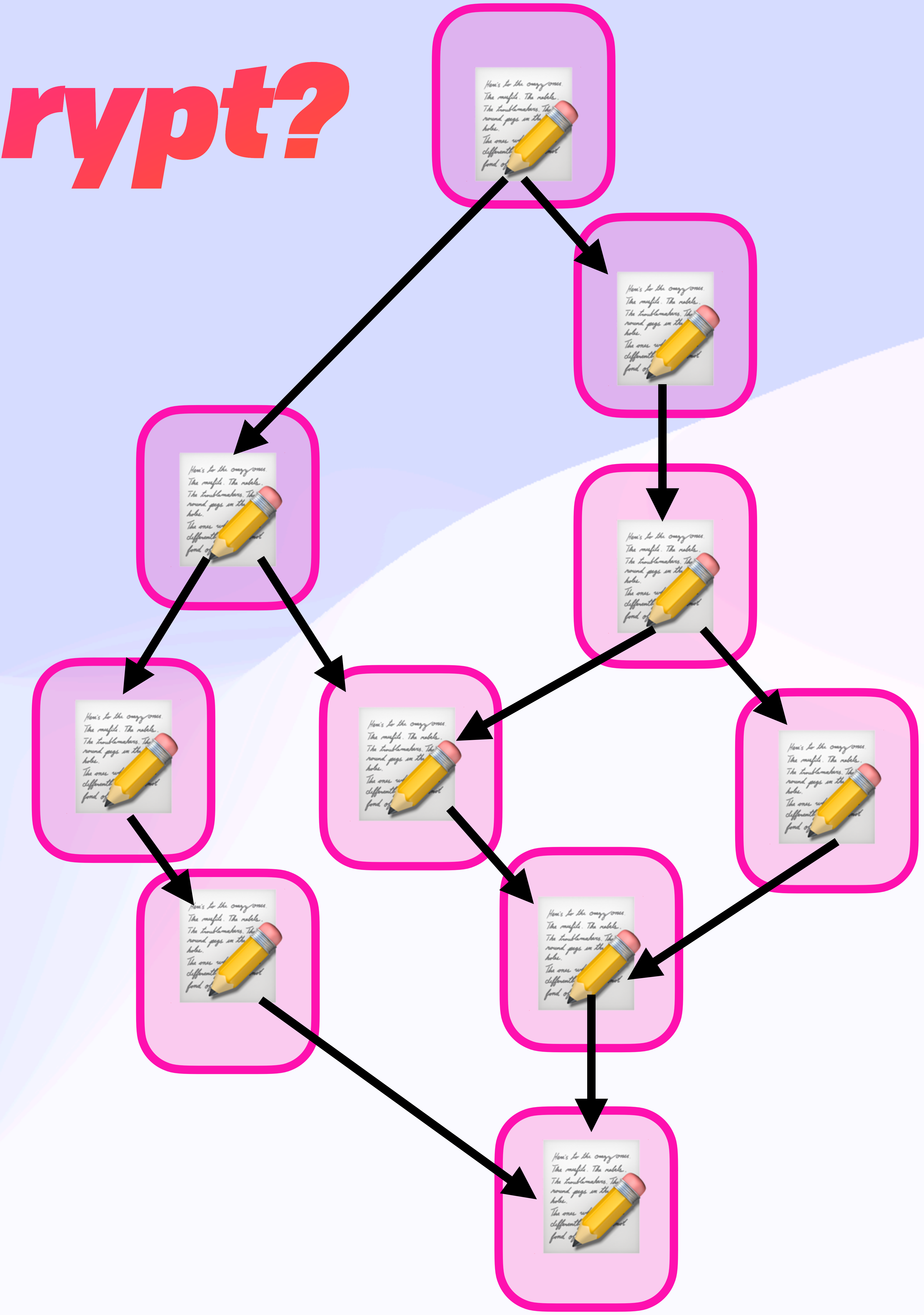
End-to-End Encryption

What To Encrypt?



End-to-End Encryption

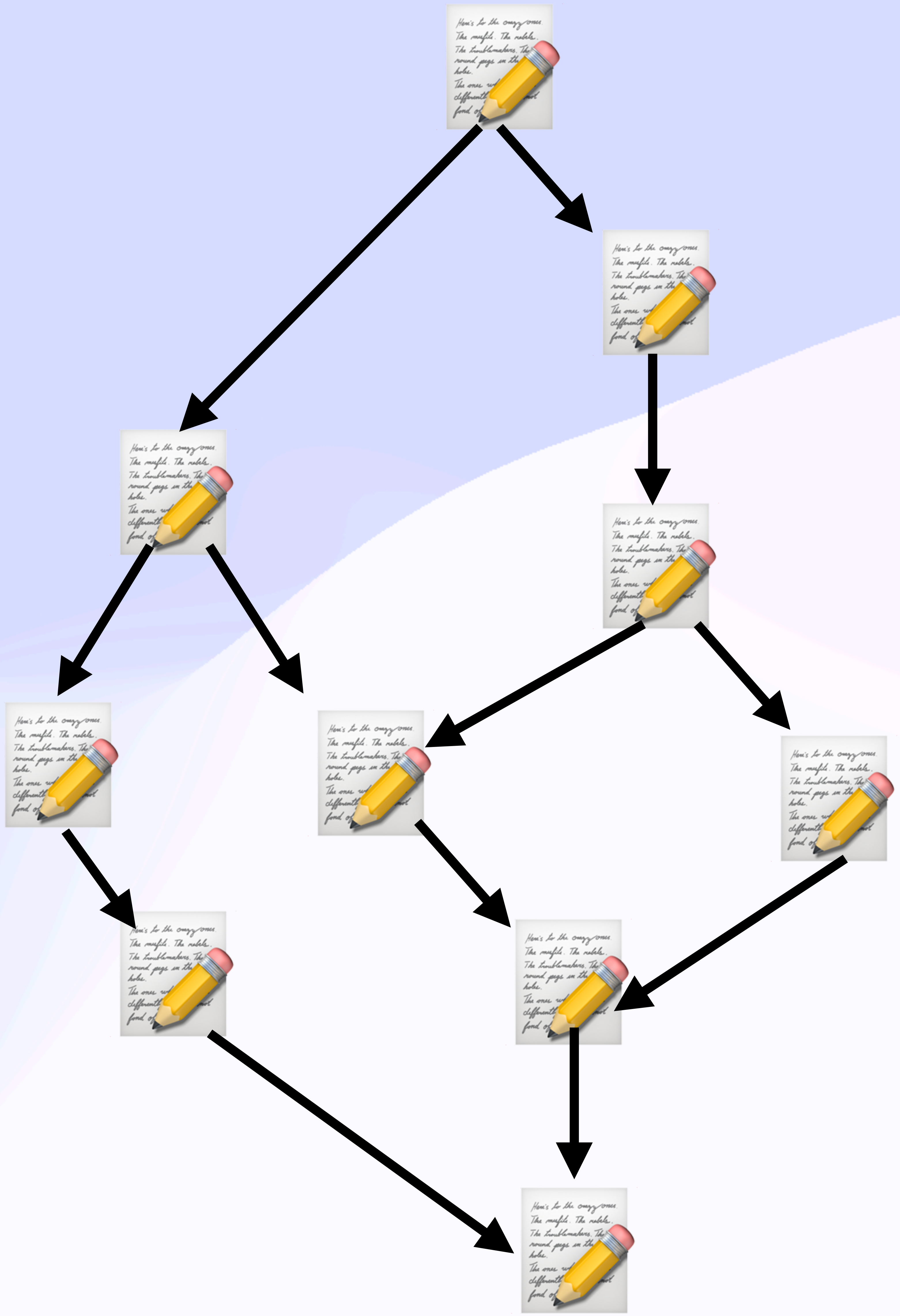
What To Encrypt?



🤔🗜️😭

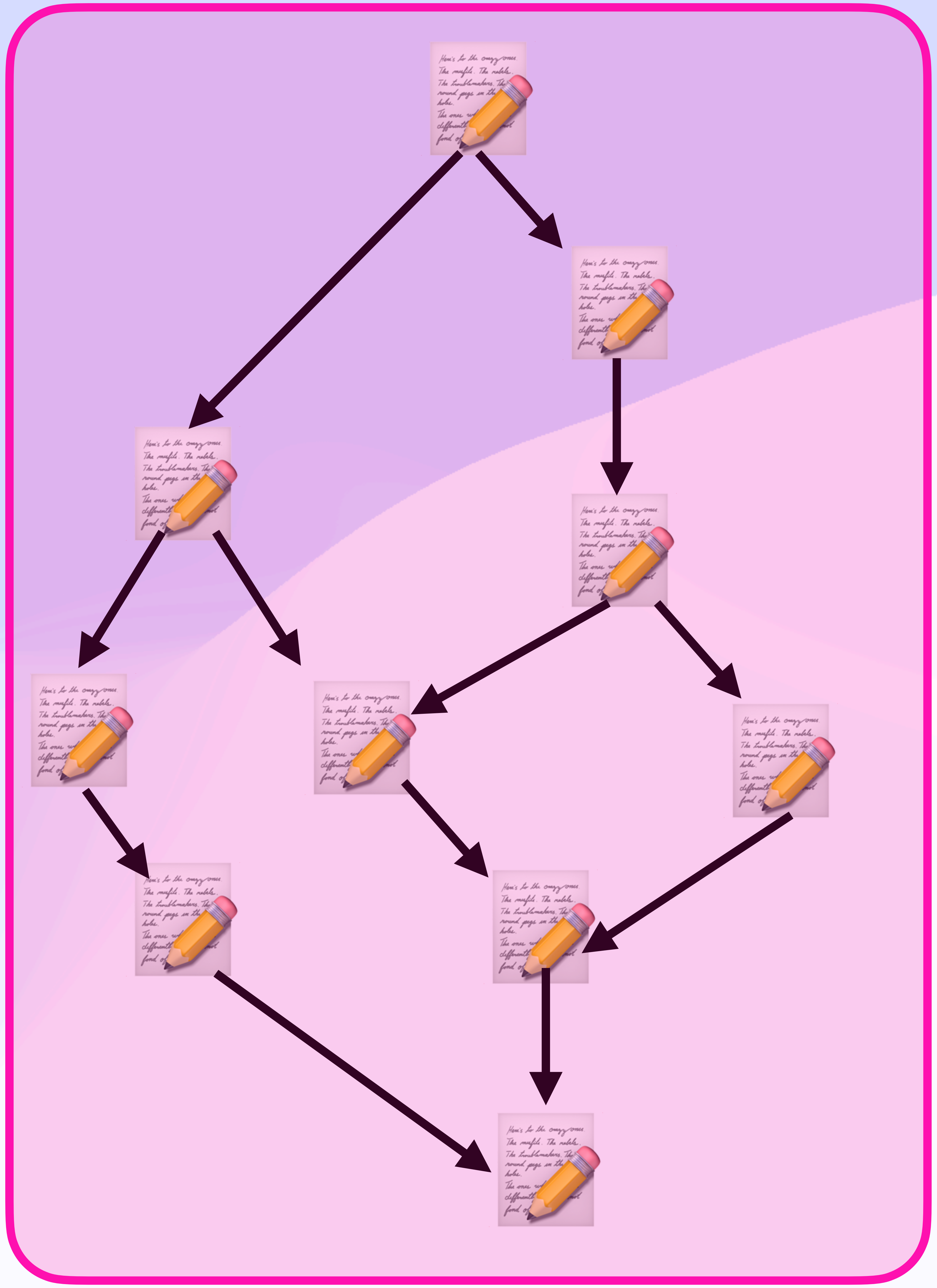
End-to-End Encryption

Everything?



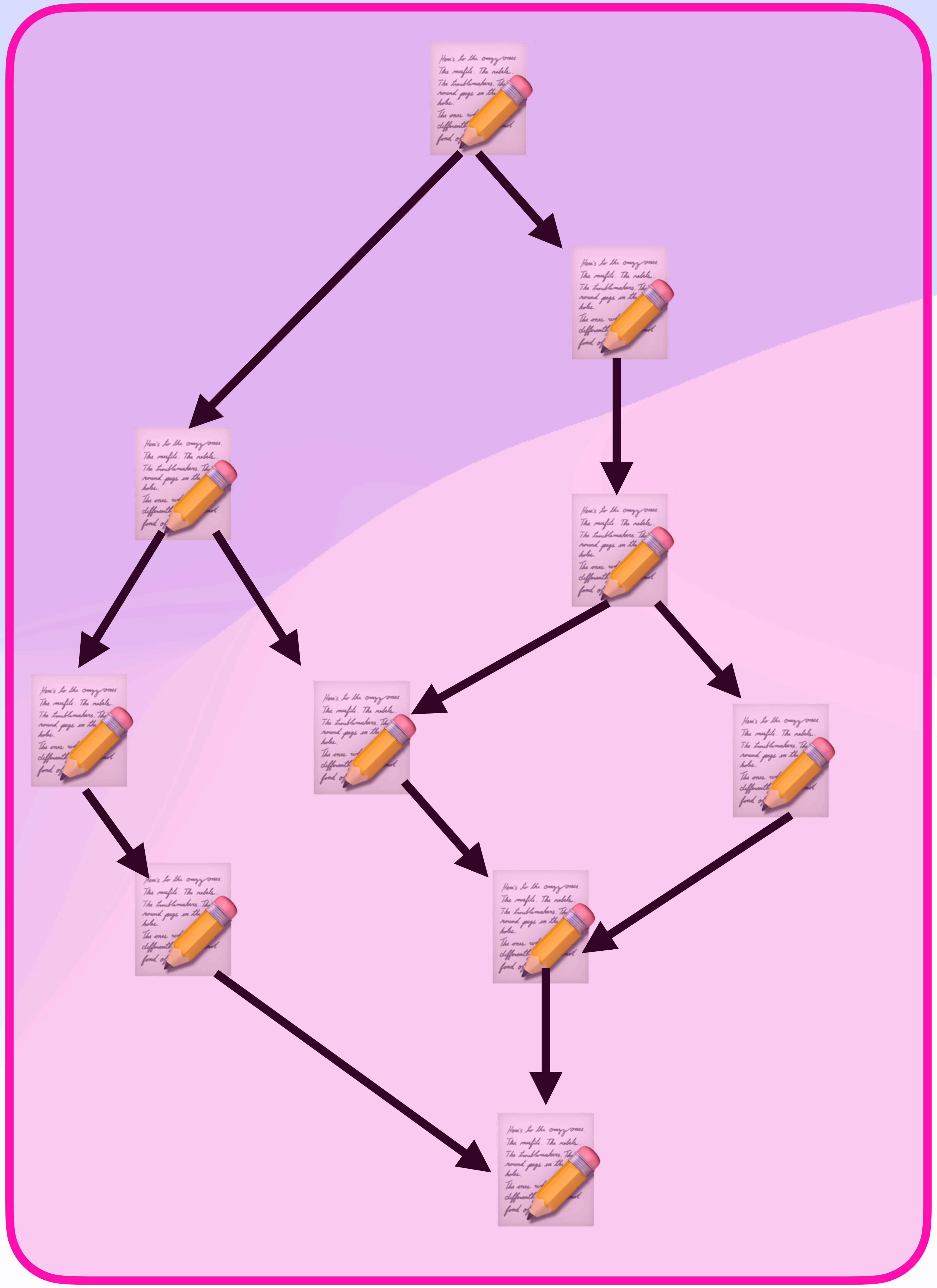
End-to-End Encryption

Everything?



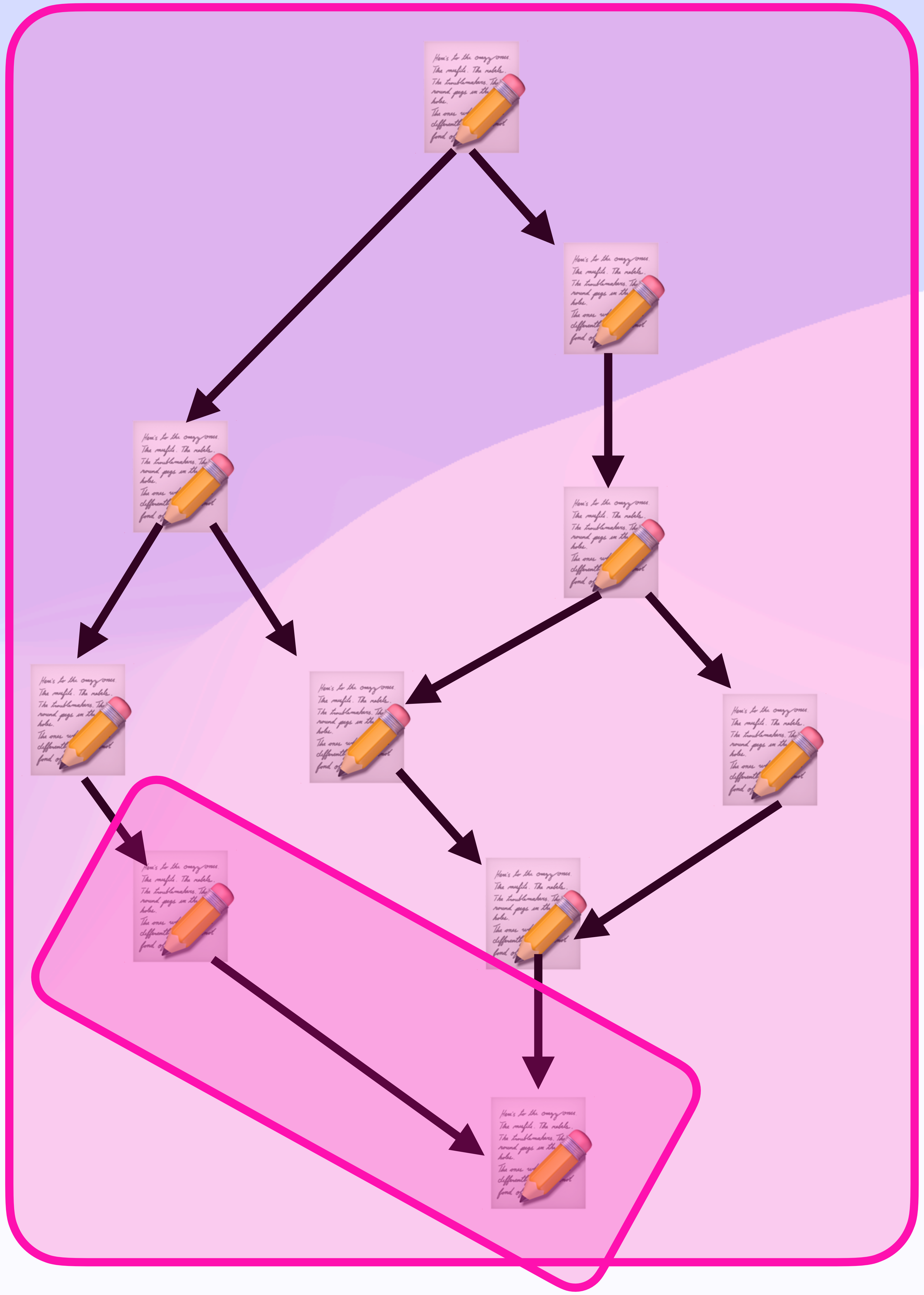
End-to-End Encryption

Everything?



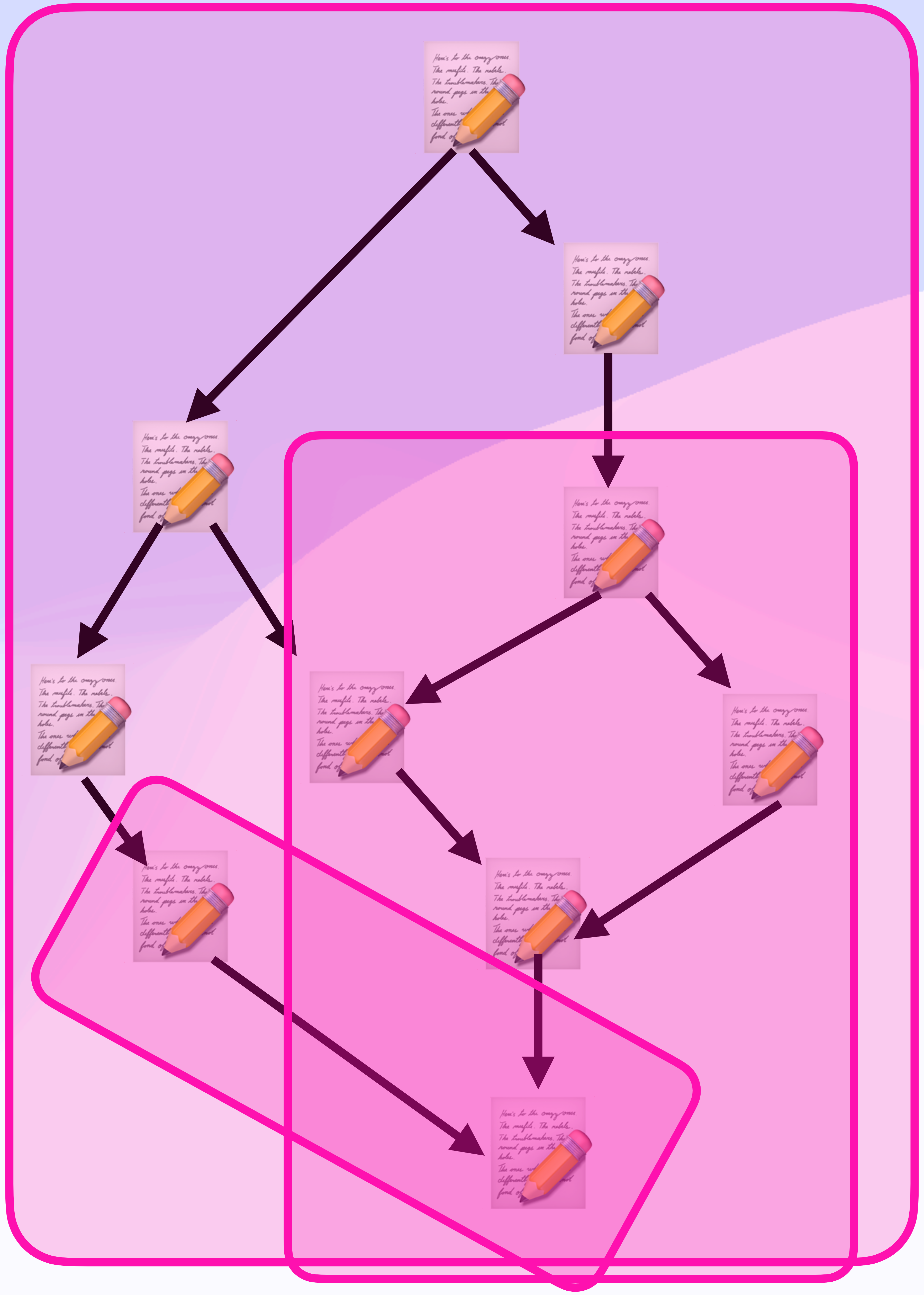
End-to-End Encryption

Everything?



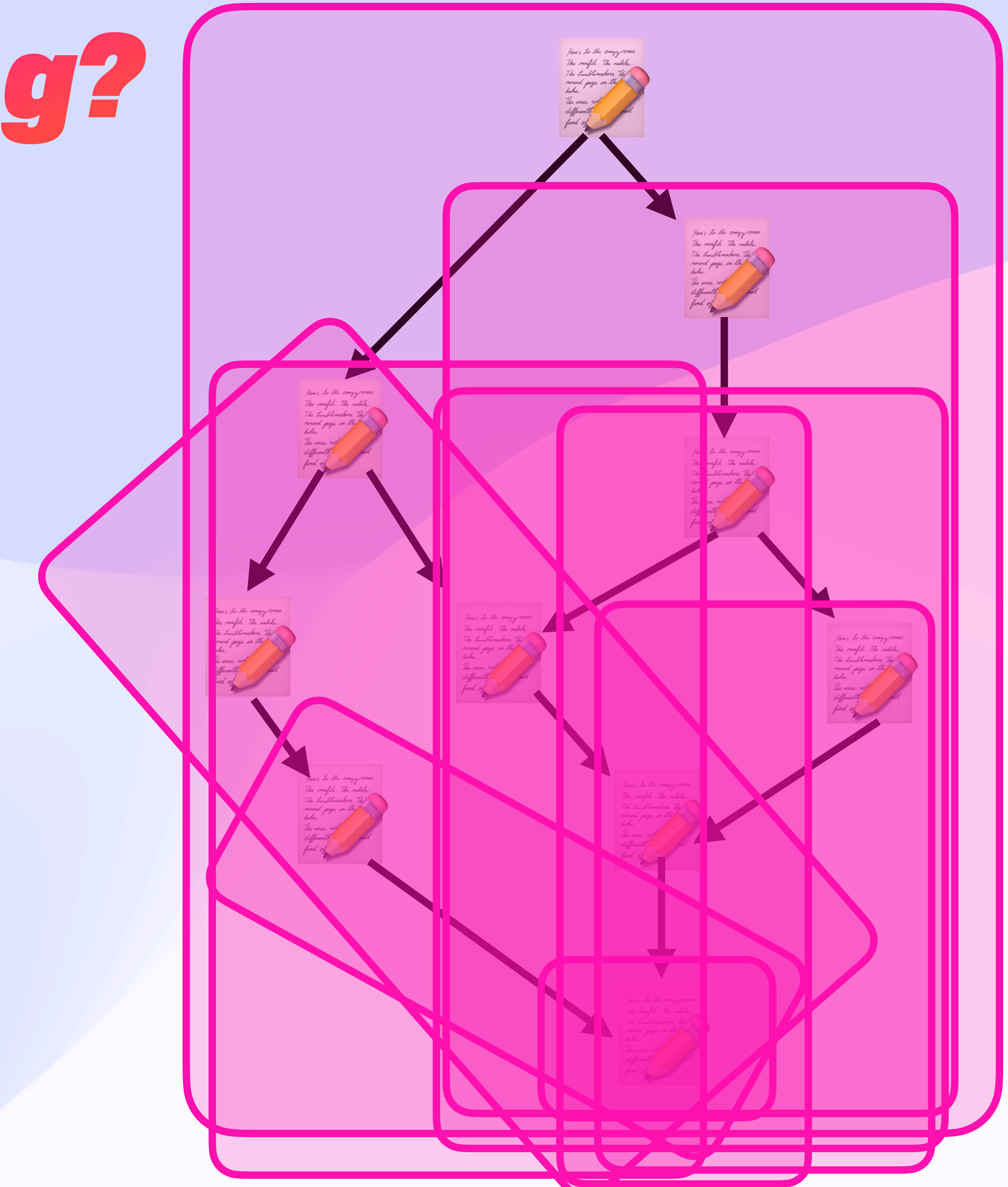
End-to-End Encryption

Everything?



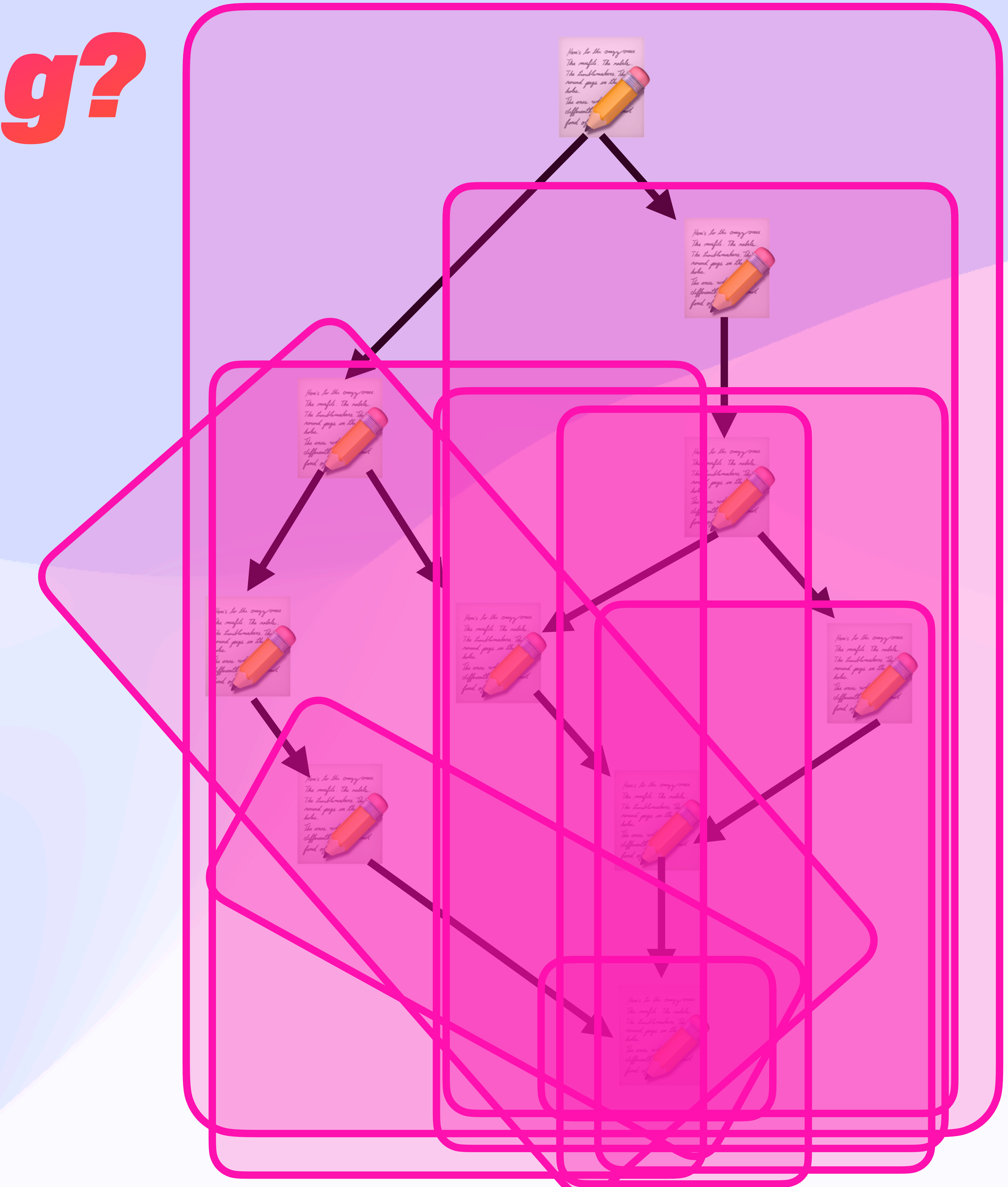
End-to-End Encryption

Everything?



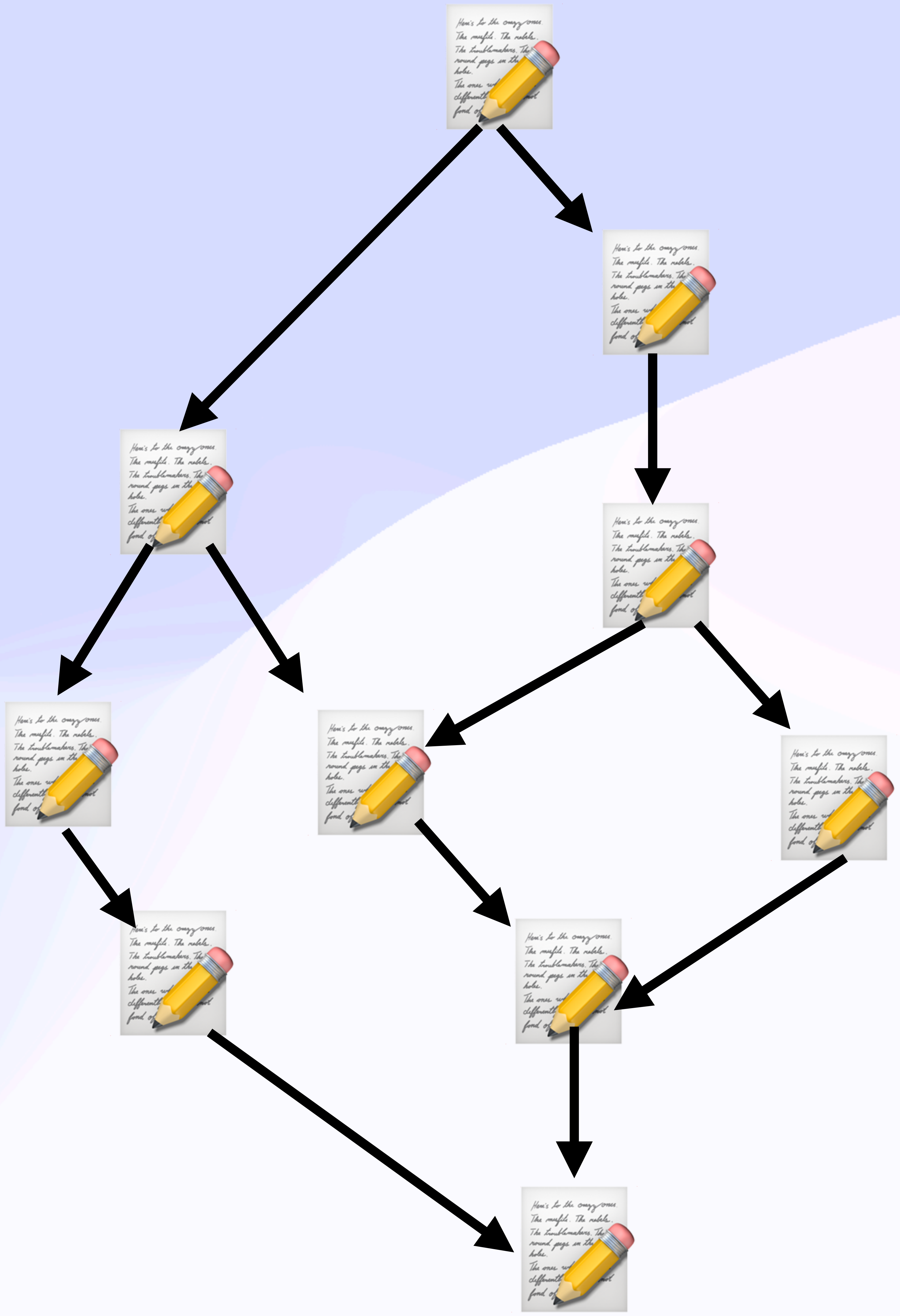
End-to-End Encryption

Everything?



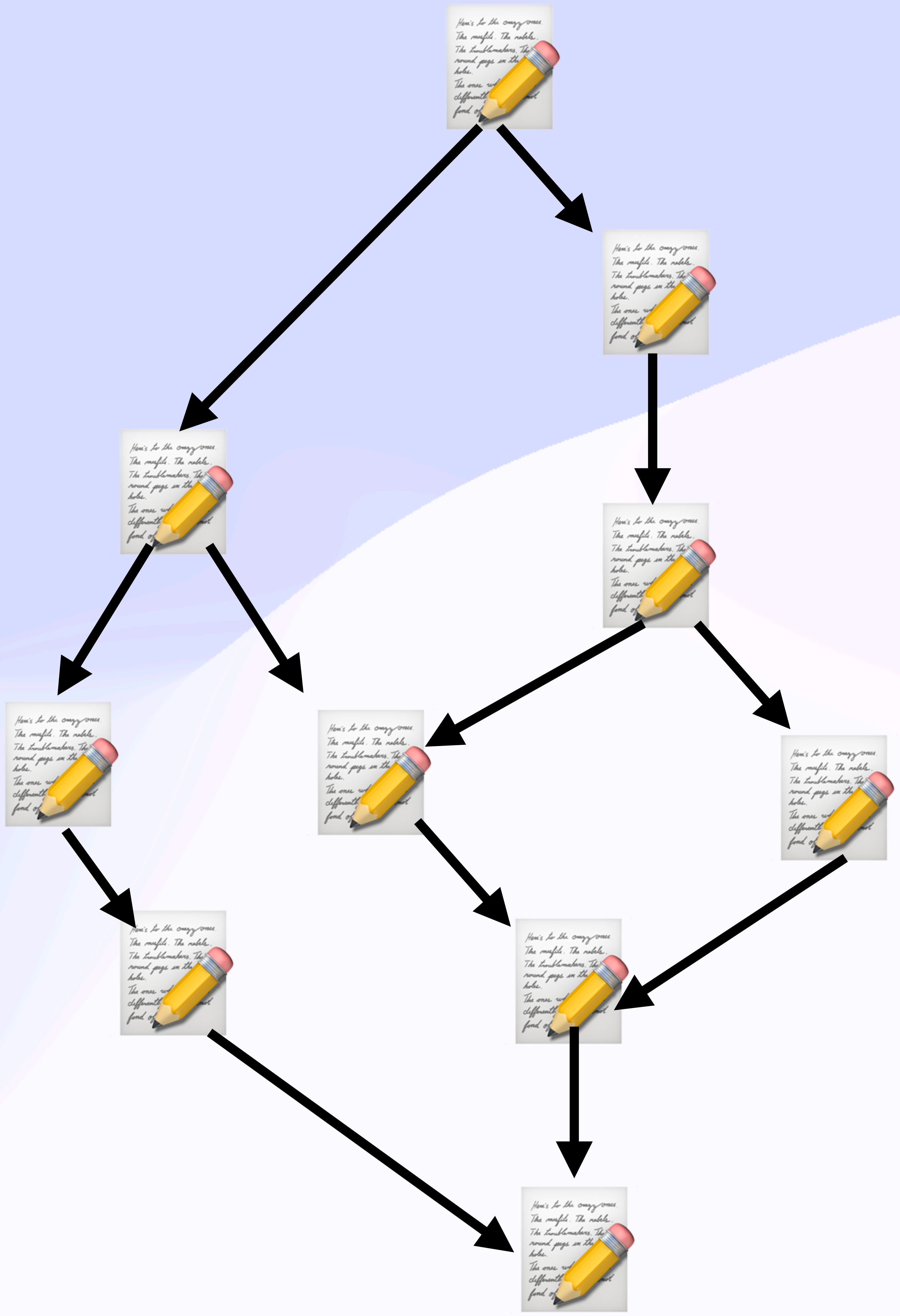
End-to-End Encryption

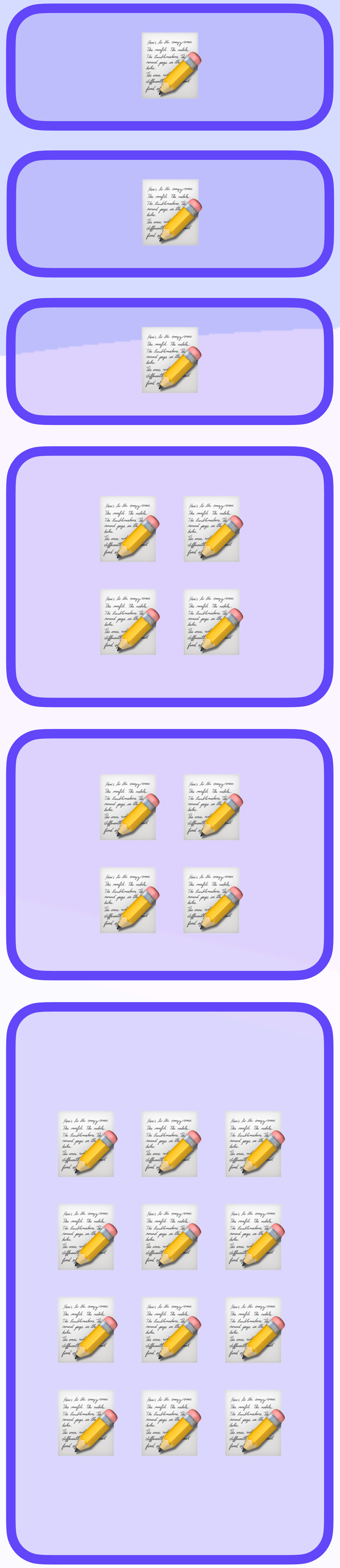
Everything?



End-to-End Encryption

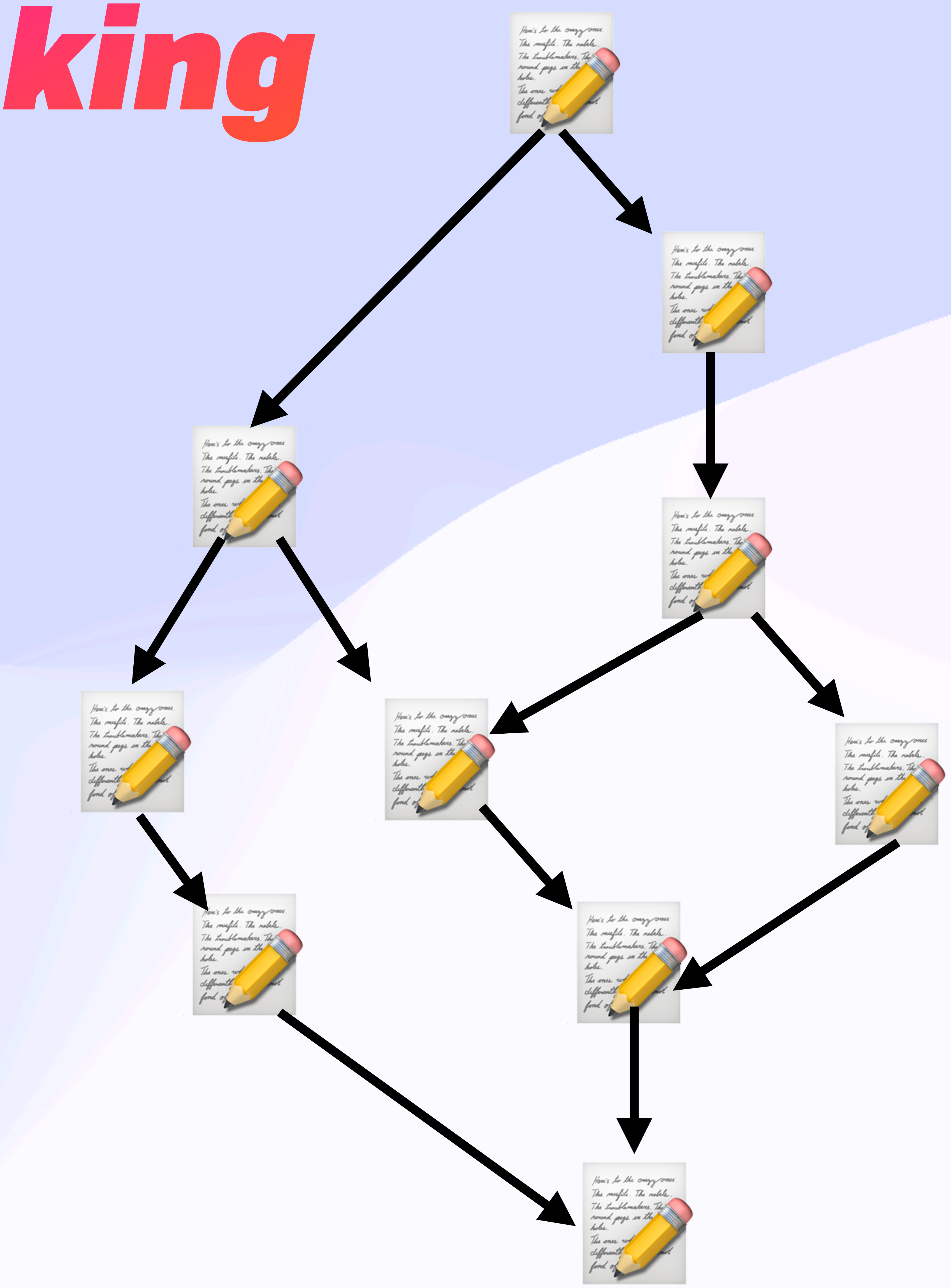
Everything?





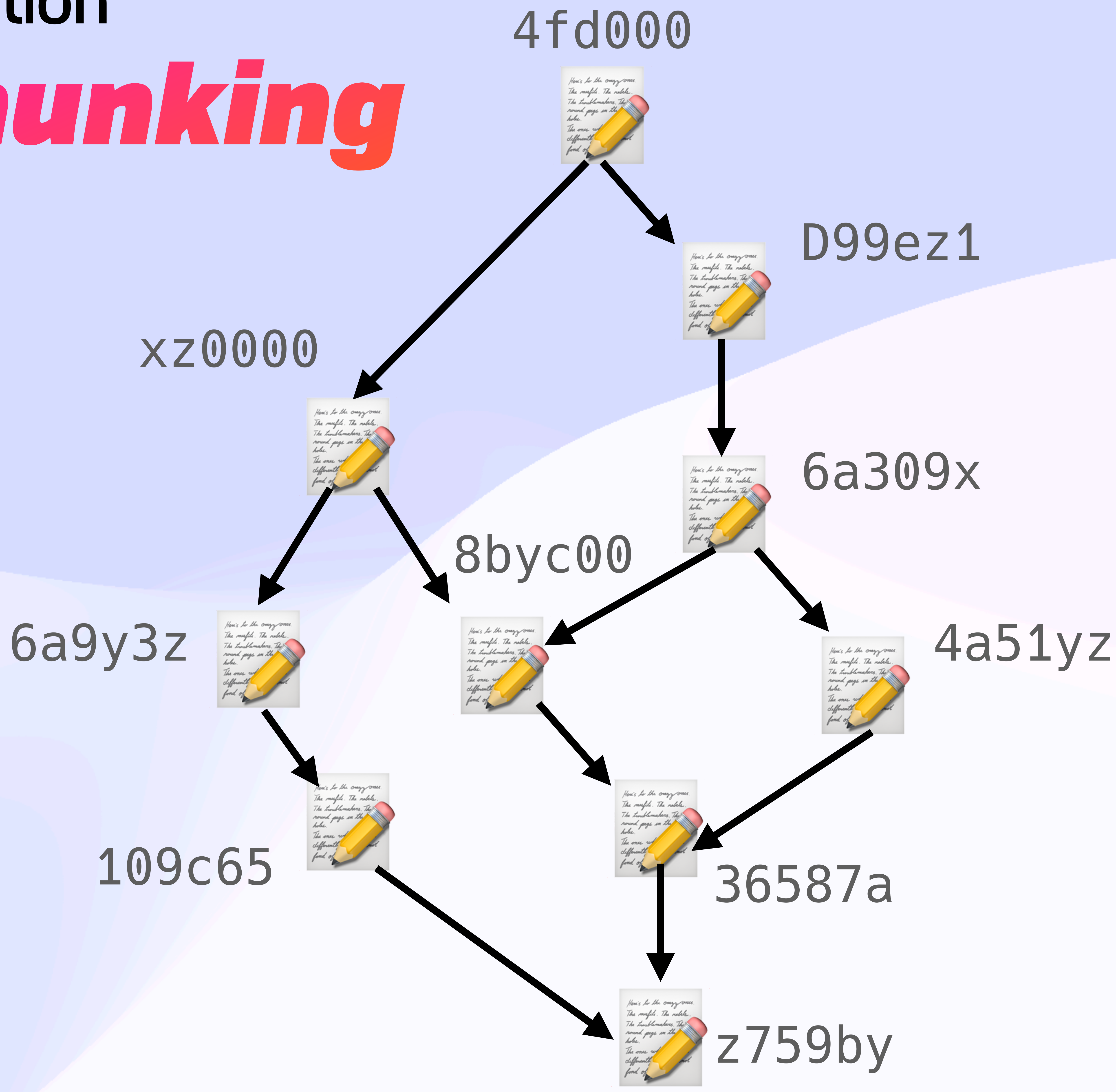
End-to-End Encryption

Stable Chunking



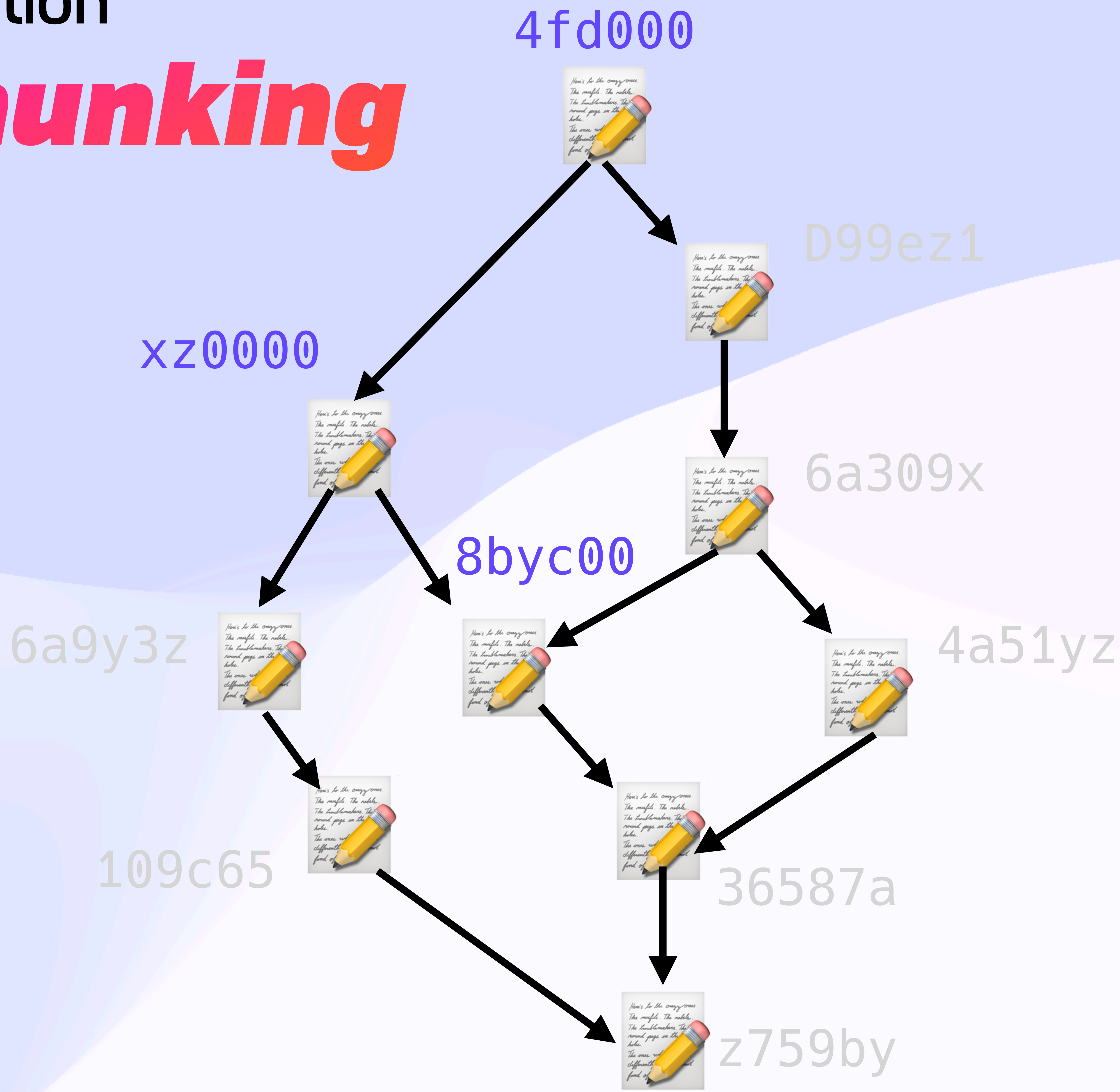
End-to-End Encryption

Stable Chunking



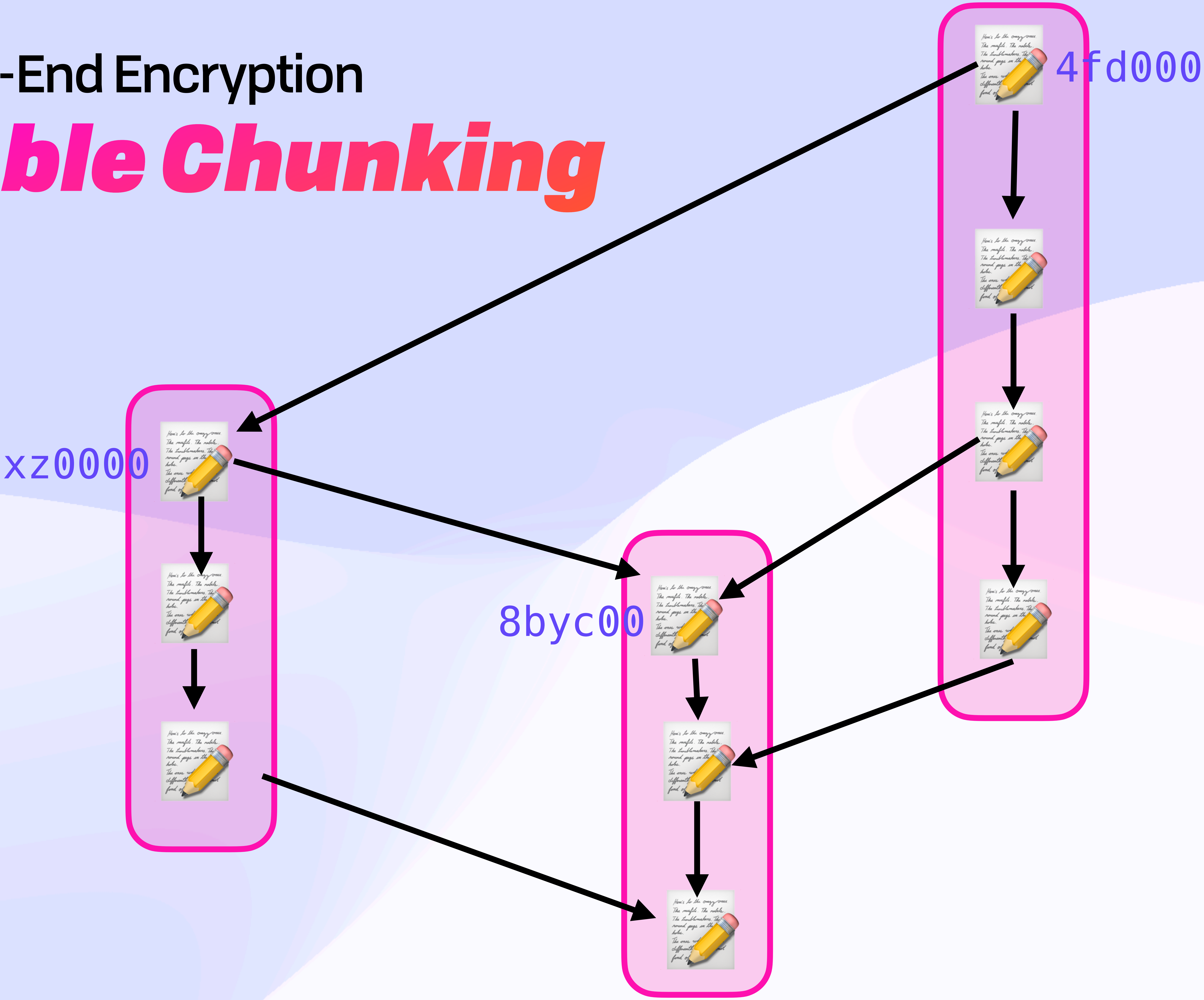
End-to-End Encryption

Stable Chunking



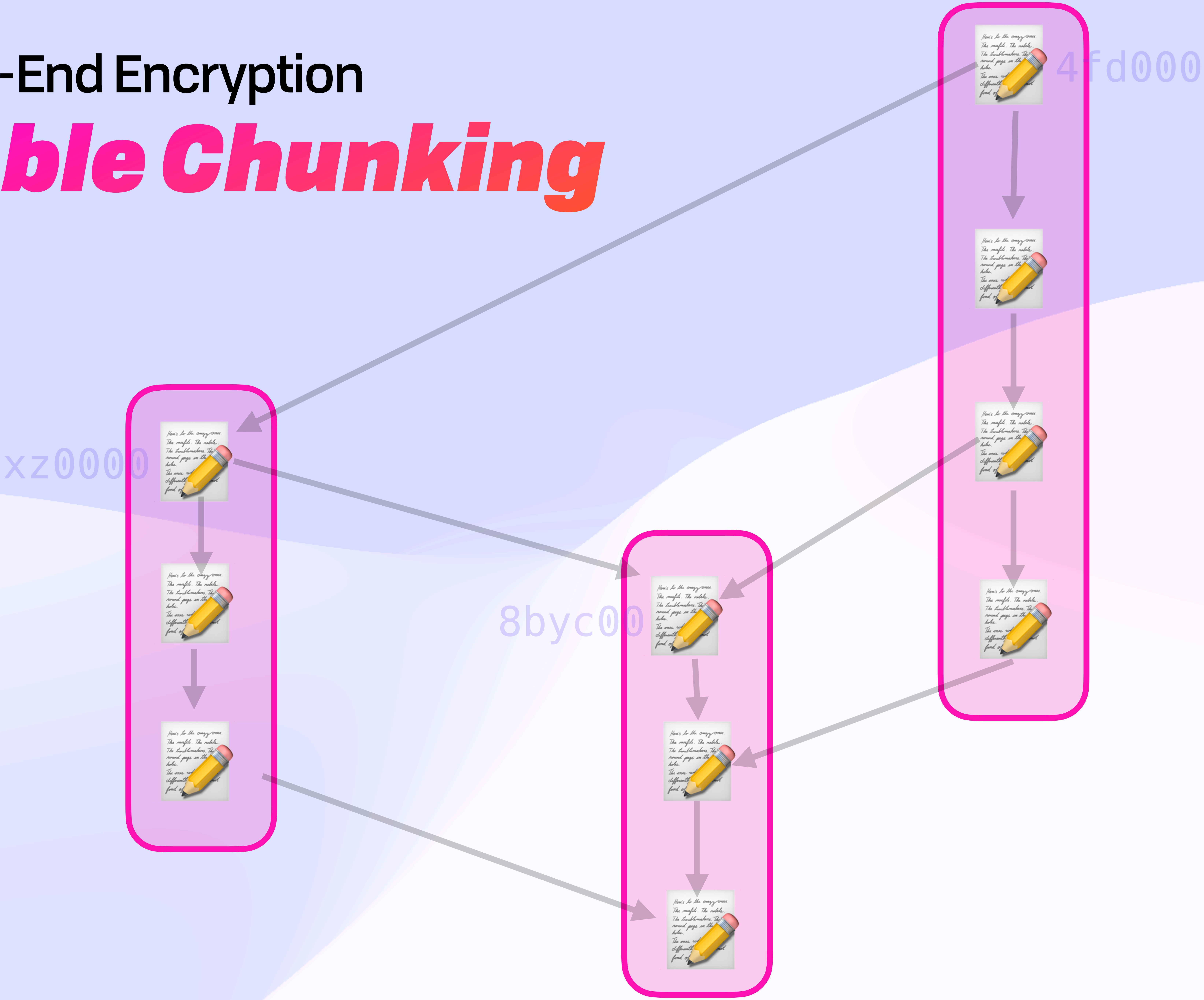
End-to-End Encryption

Stable Chunking



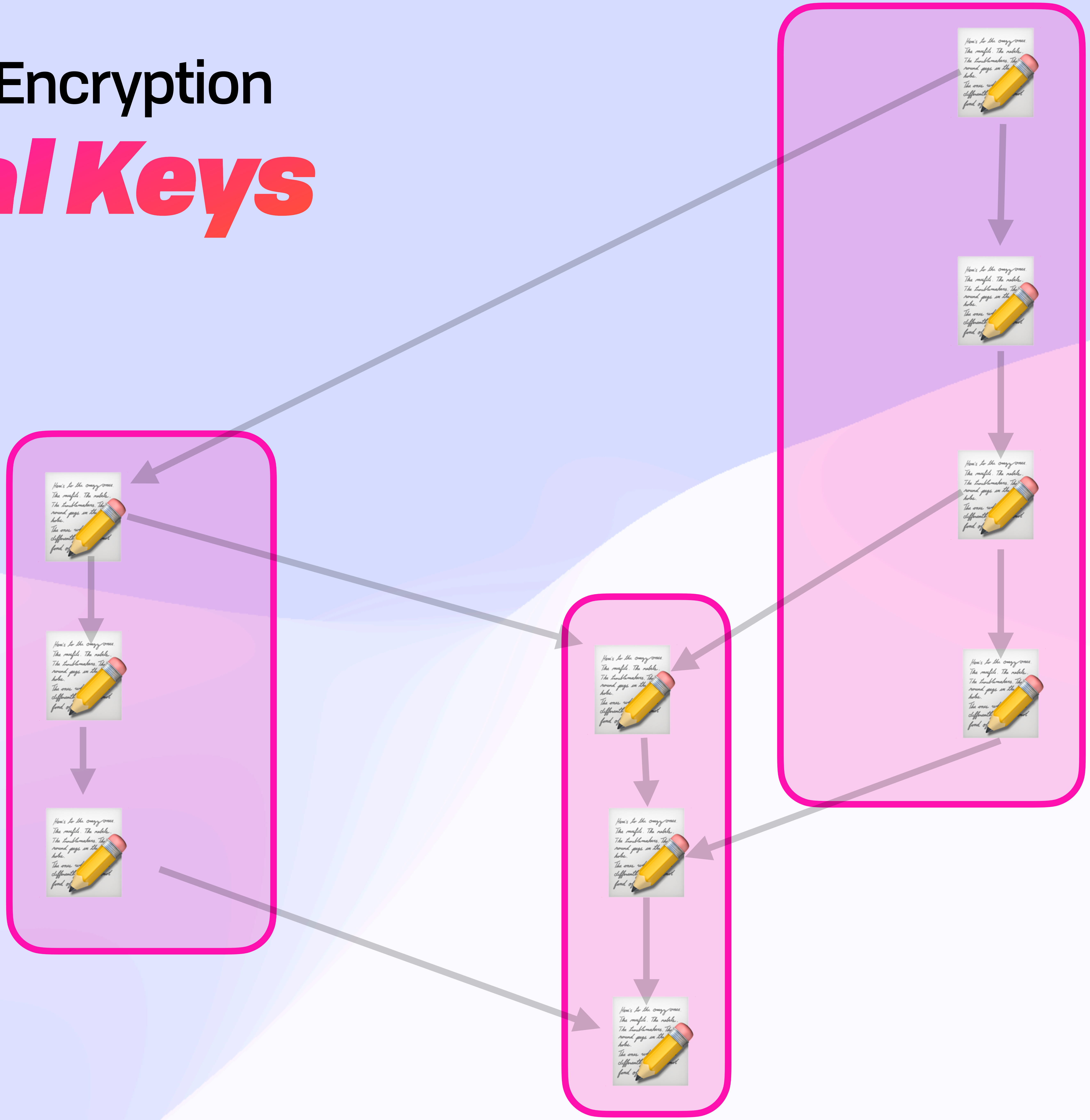
End-to-End Encryption

Stable Chunking



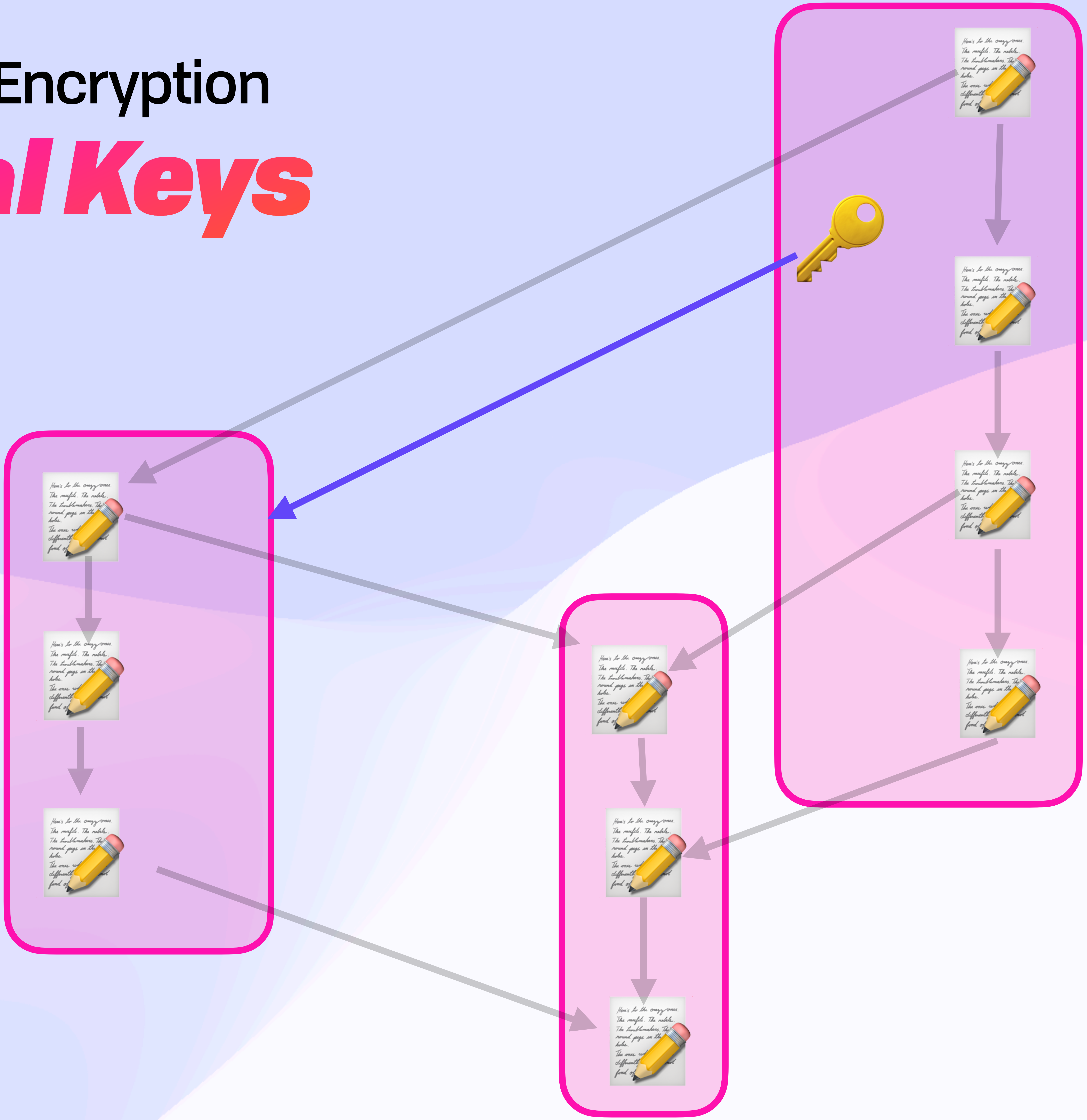
End-to-End Encryption

Causal Keys



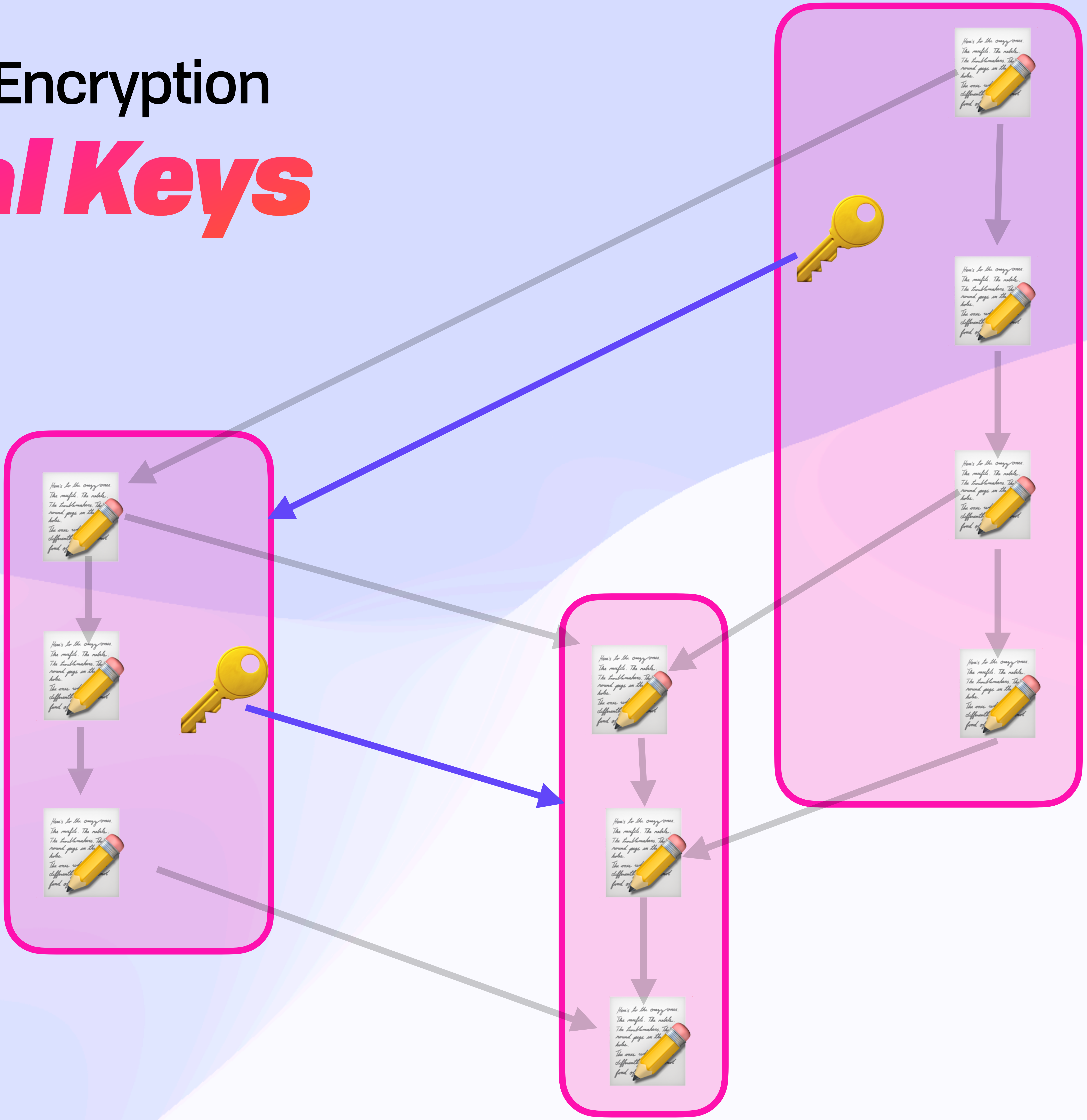
End-to-End Encryption

Causal Keys



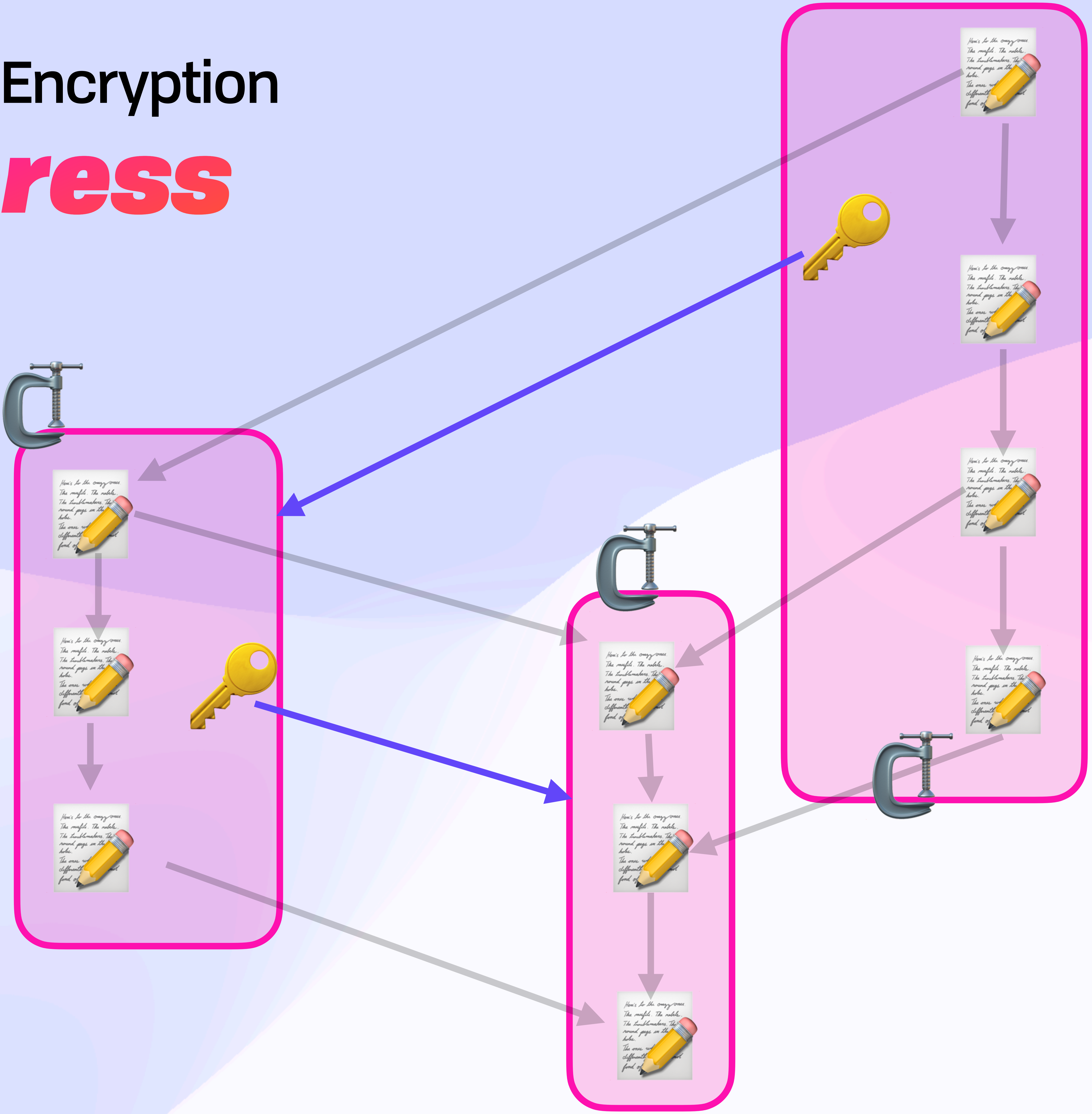
End-to-End Encryption

Causal Keys



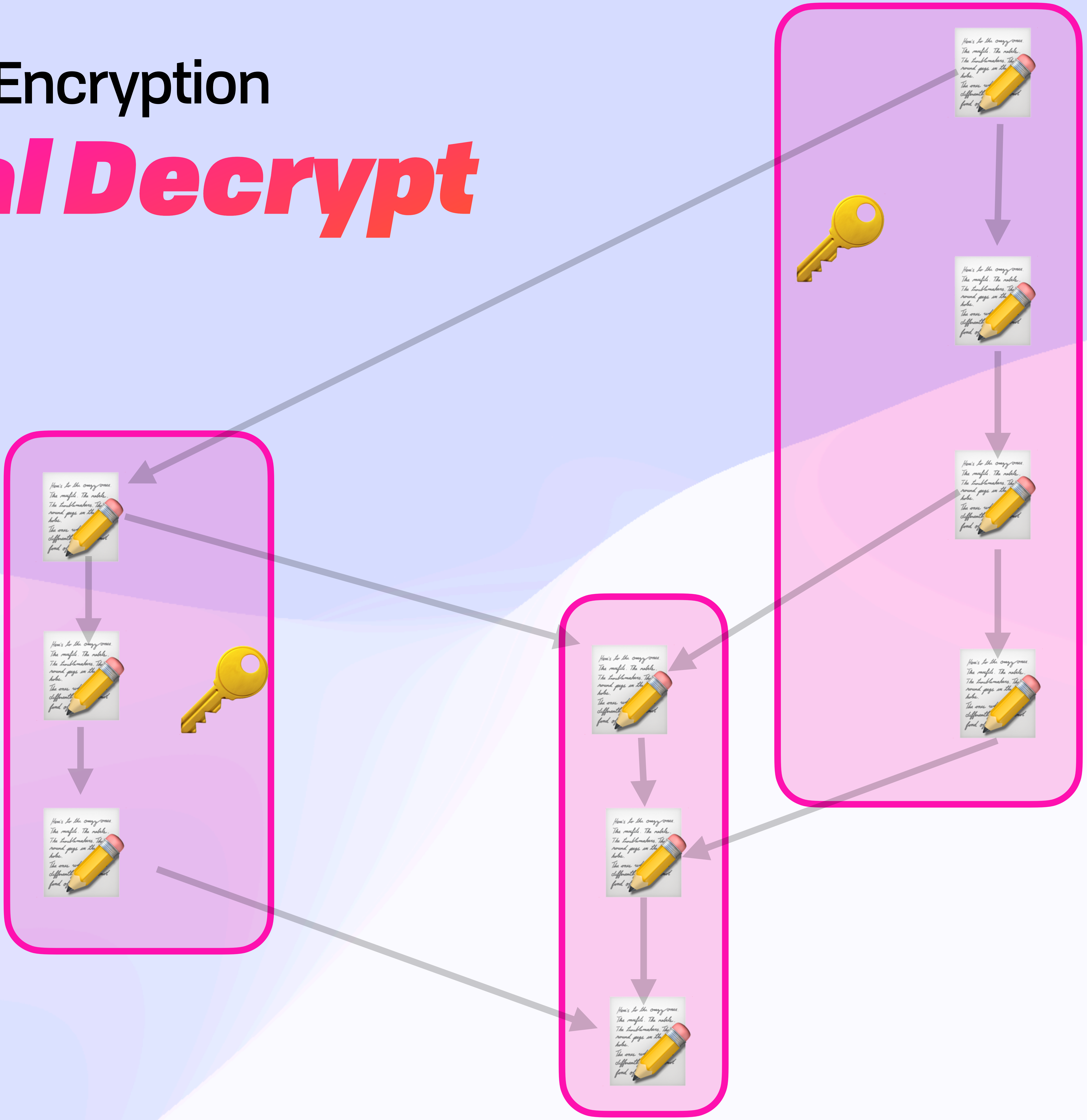
End-to-End Encryption

Compress



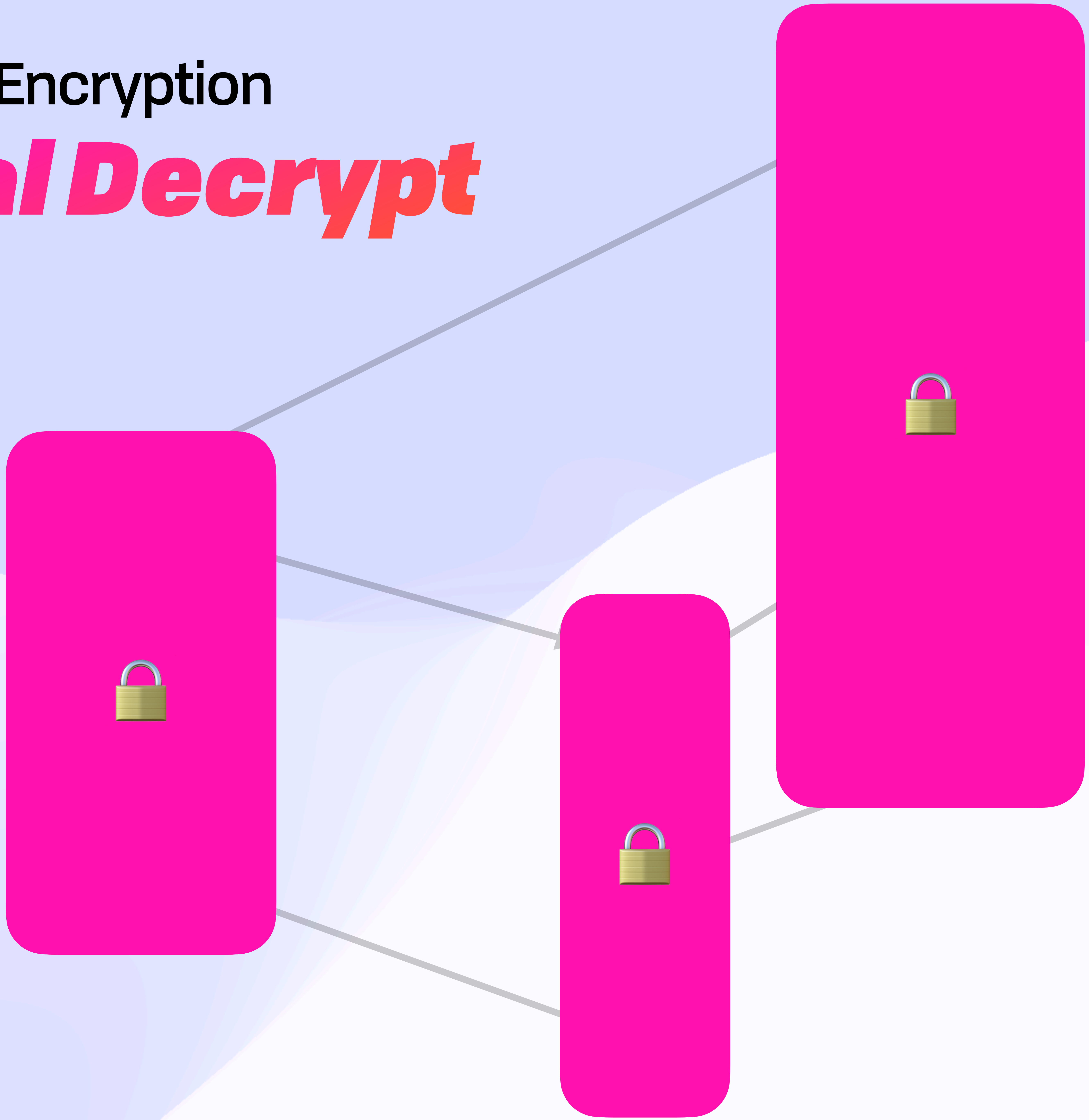
End-to-End Encryption

Causal Decrypt



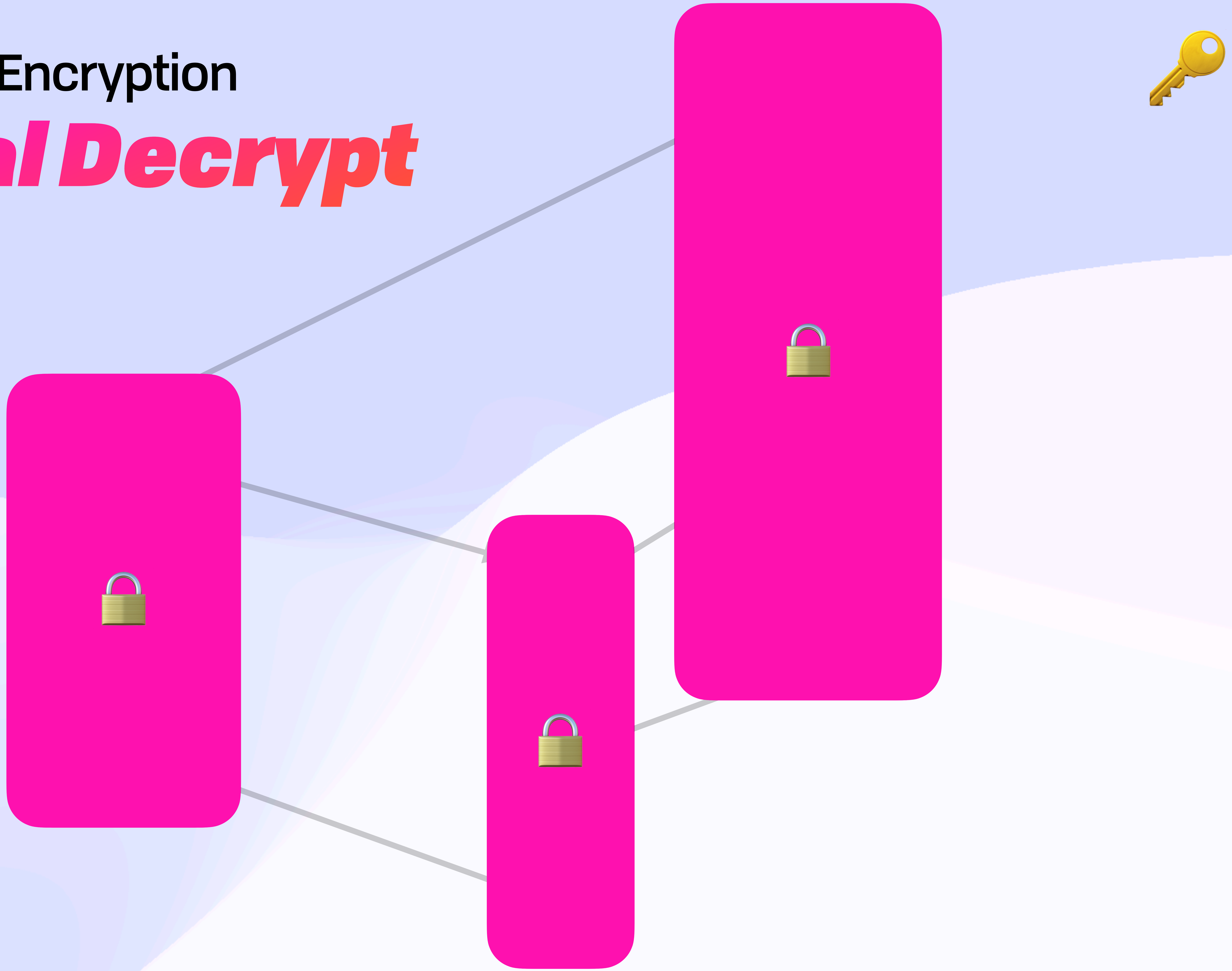
End-to-End Encryption

Causal Decrypt



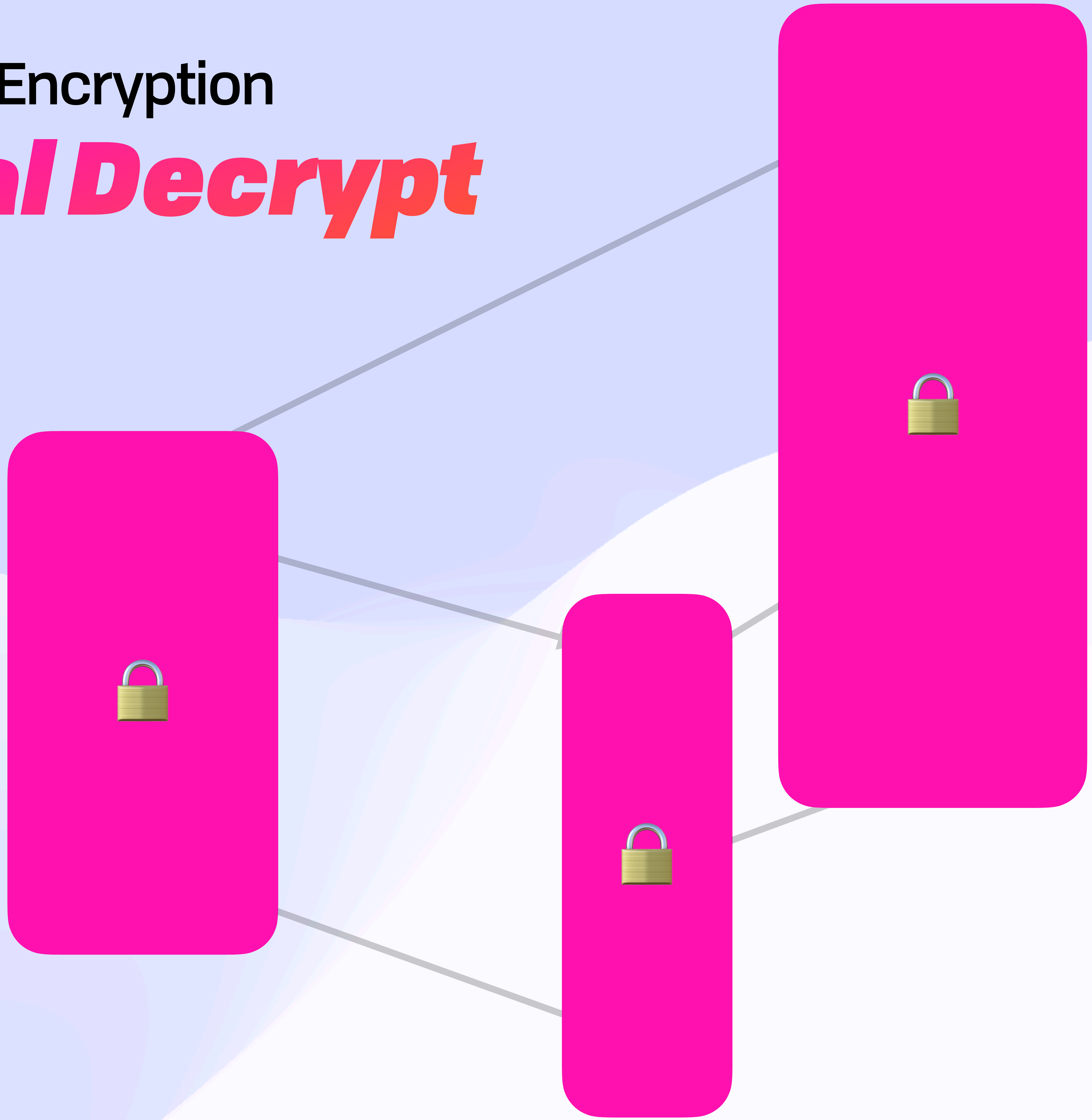
End-to-End Encryption

Causal Decrypt



End-to-End Encryption

Causal Decrypt



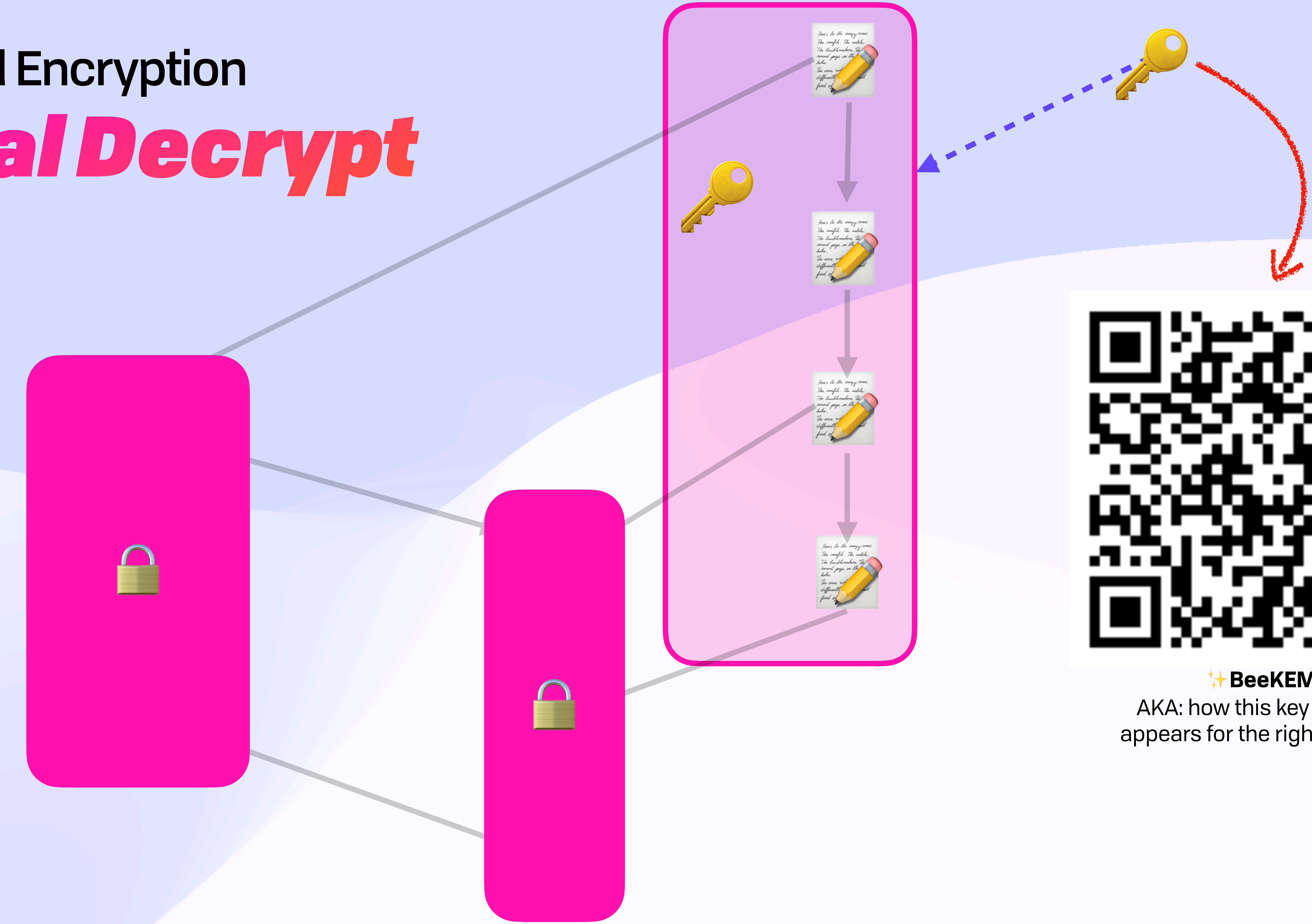
🔑

✨BeeKEM✨

AKA: how this key magically
appears for the right users only

End-to-End Encryption

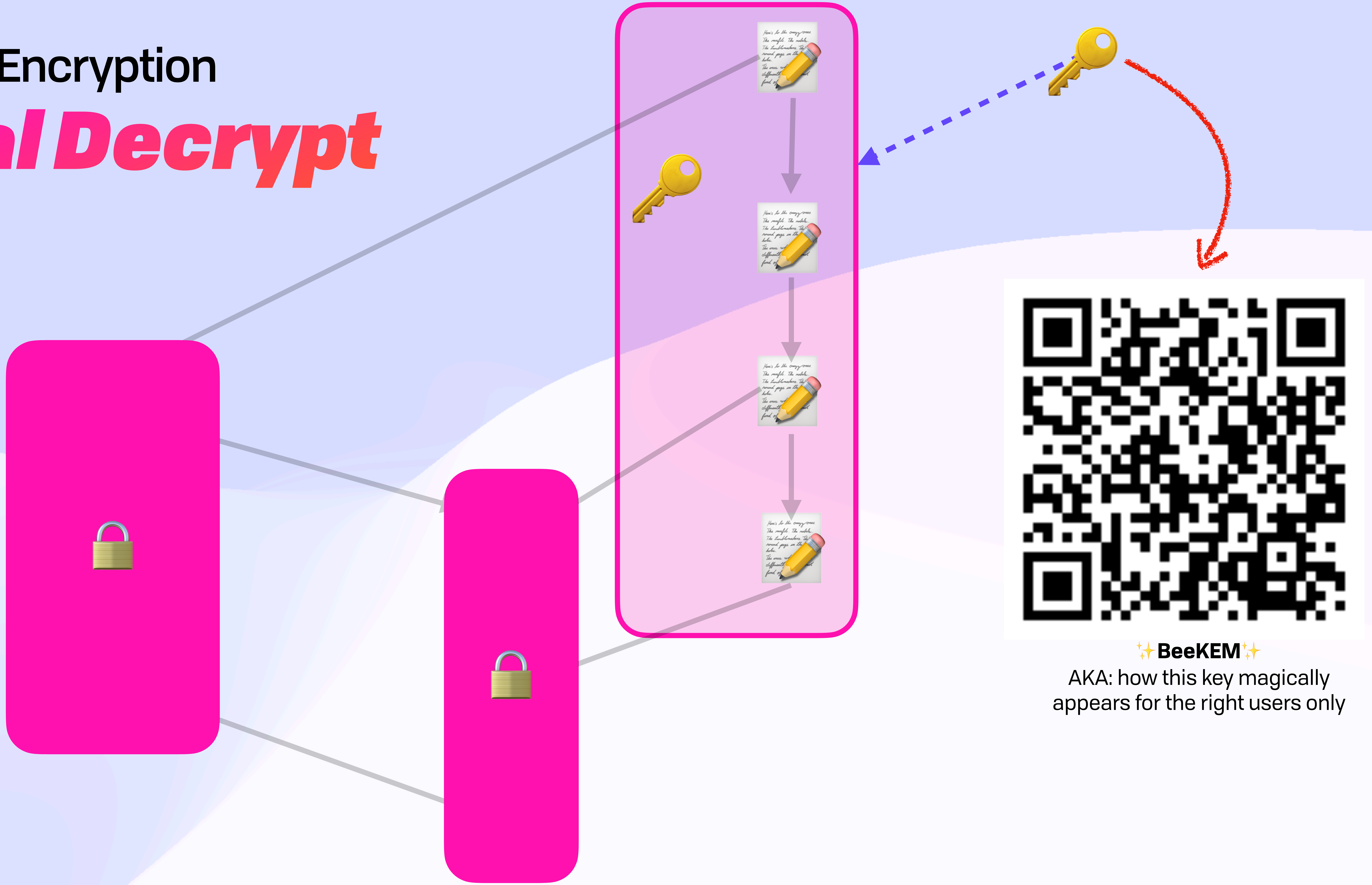
Causal Decrypt



✨**BeeKEM**✨
AKA: how this key magically
appears for the right users only

End-to-End Encryption

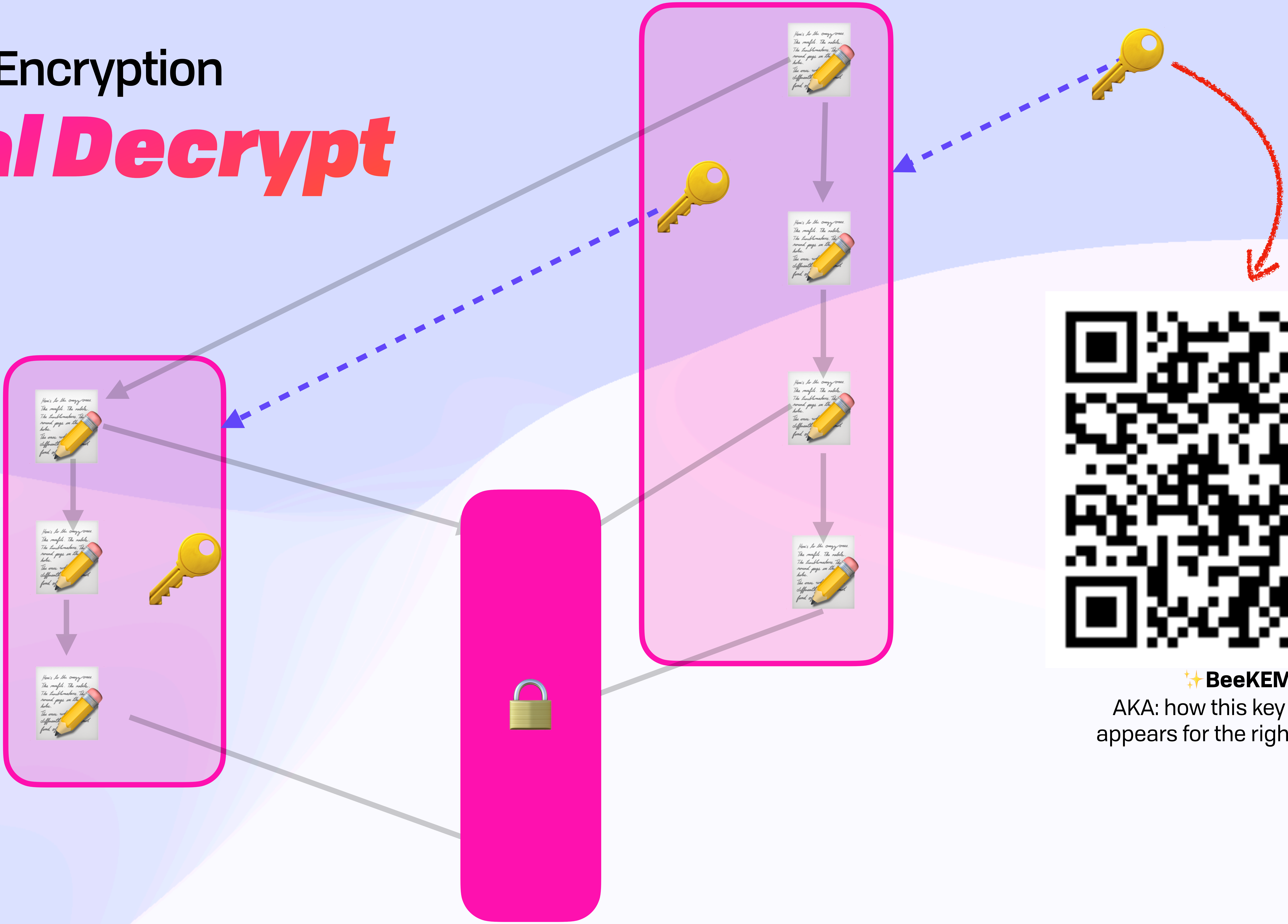
Causal Decrypt



✨**BeeKEM**✨
AKA: how this key magically
appears for the right users only

End-to-End Encryption

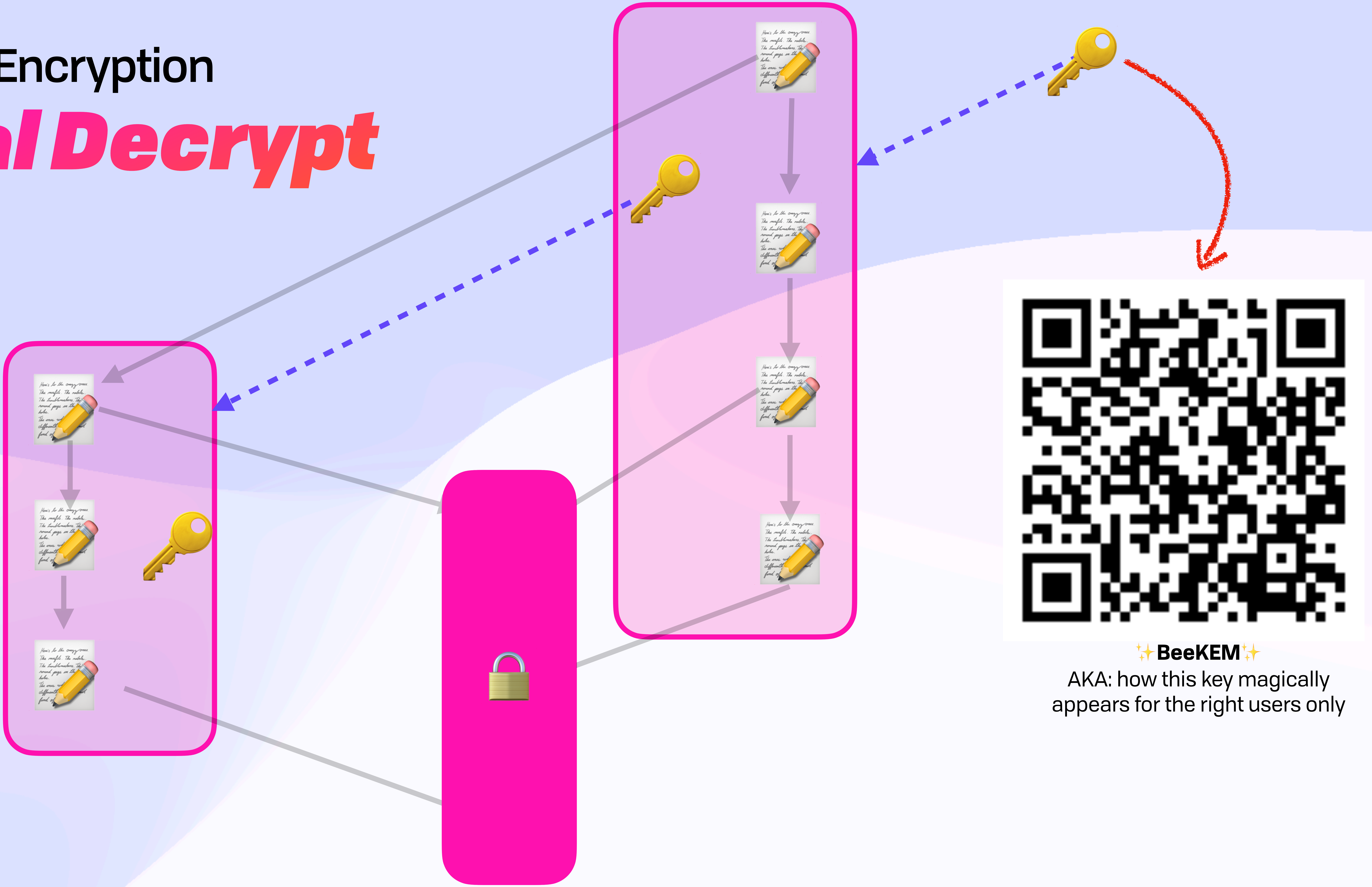
Causal Decrypt



✨**BeeKEM**✨
AKA: how this key magically
appears for the right users only

End-to-End Encryption

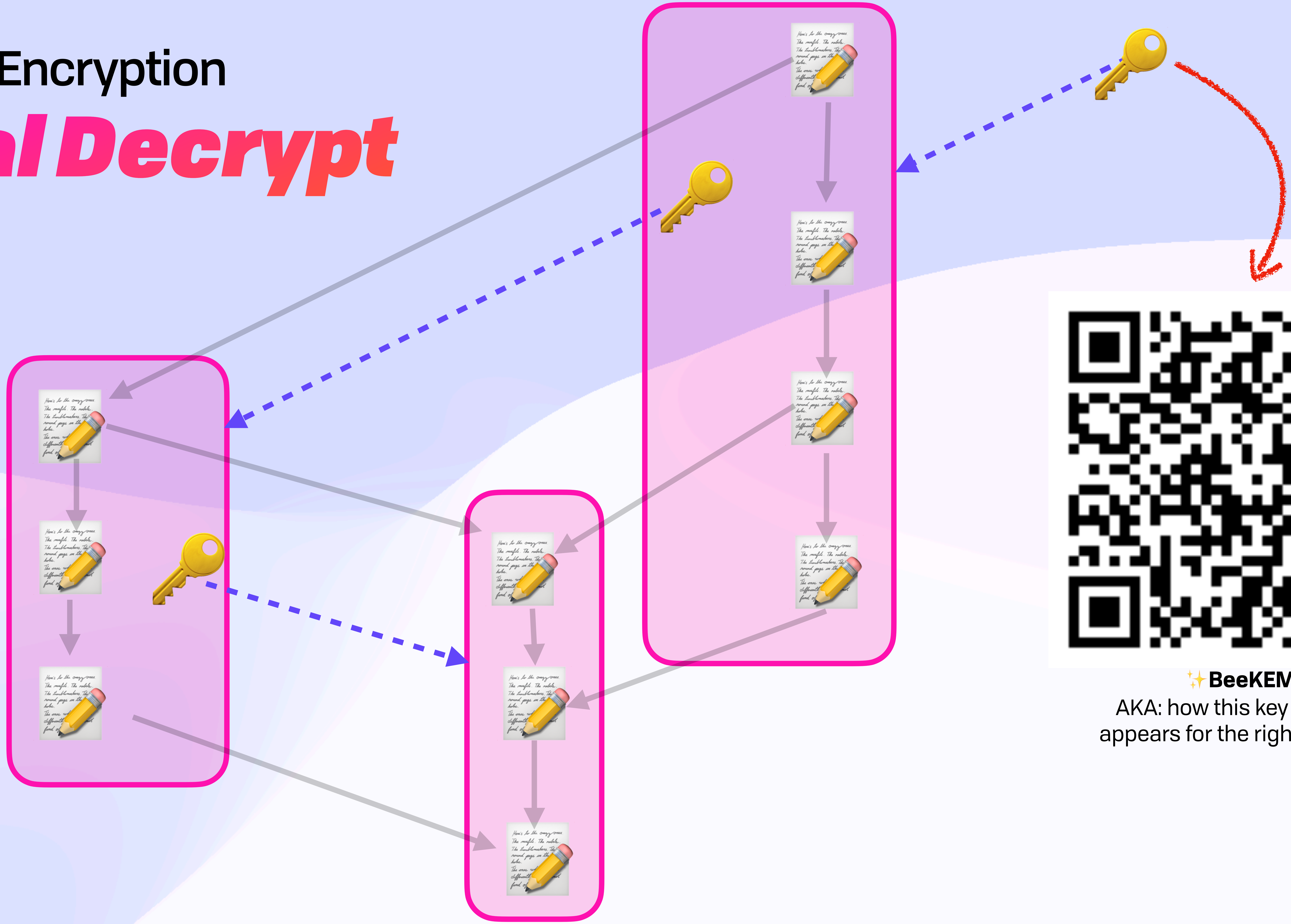
Causal Decrypt



✨**BeeKEM**✨
AKA: how this key magically appears for the right users only

End-to-End Encryption

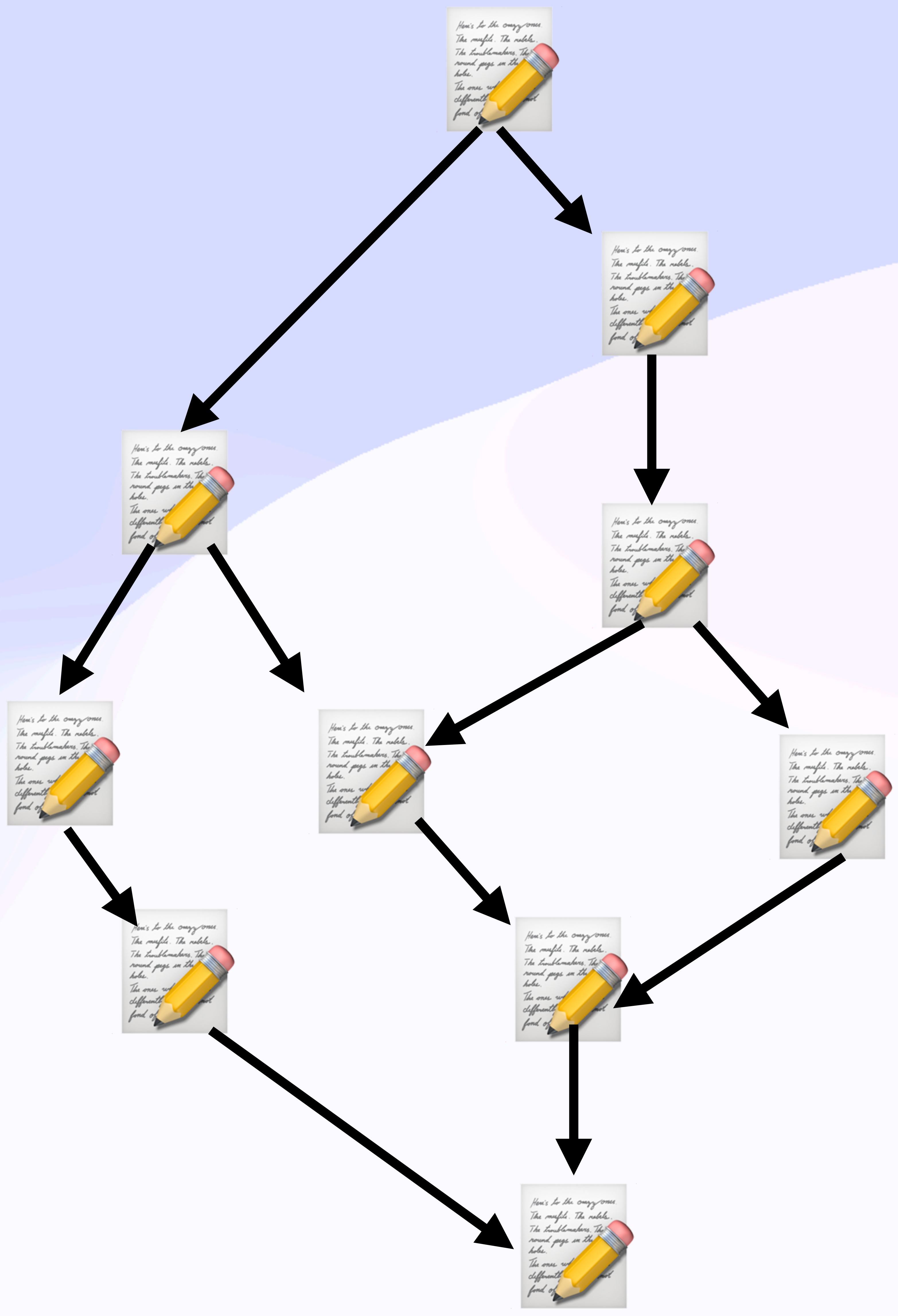
Causal Decrypt



✨**BeeKEM**✨
AKA: how this key magically
appears for the right users only

End-to-End Encryption

Reconstruct

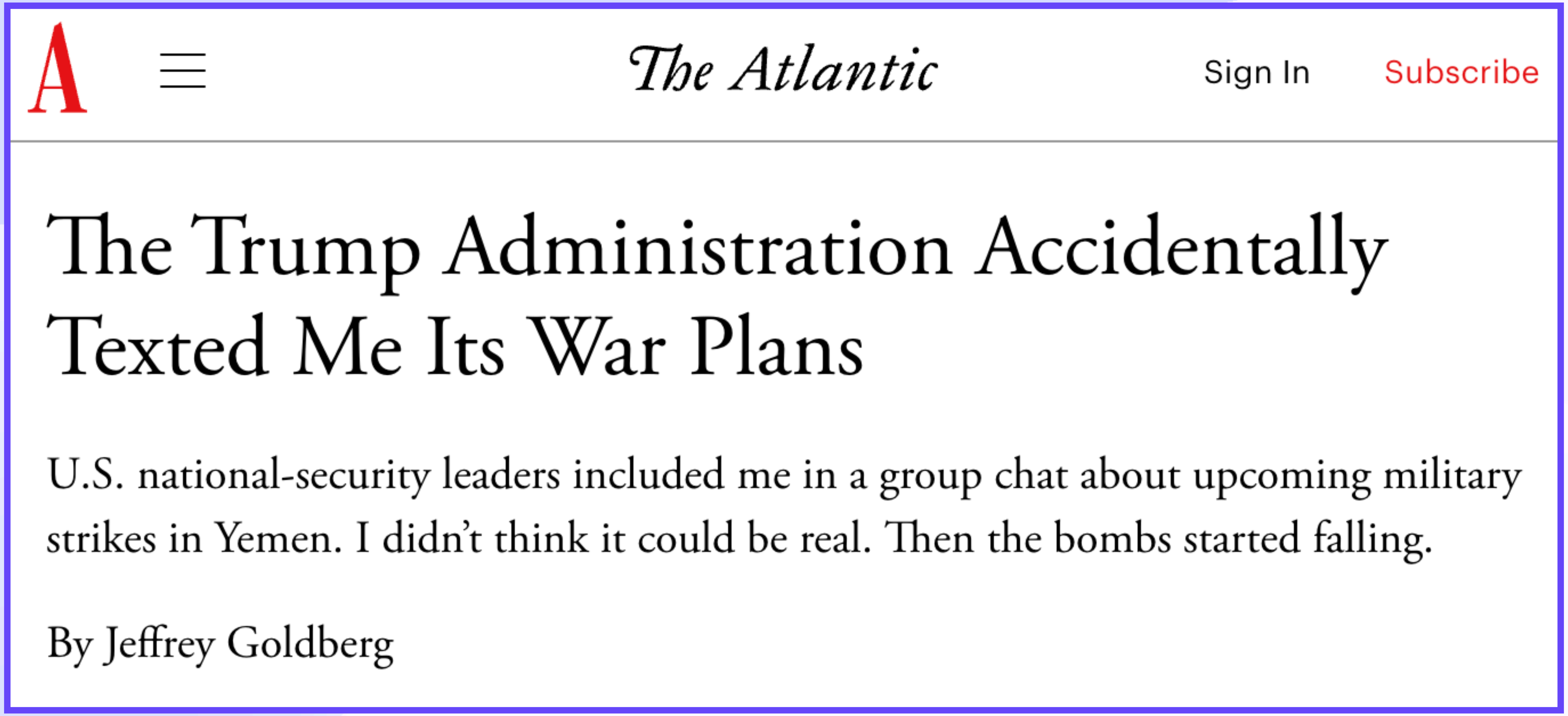


End-to-End Encryption

Encryption is Not Enough

End-to-End Encryption

Encryption is Not Enough



The Atlantic

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

End-to-End Encryption

The "IYKYK" Principal

End-to-End Encryption

The "IYKYK" Principal

Data wants to be free.
You can't claw back leaked bytes.
Once they know, they know.

End-to-End Encryption

The "IYKYK" Principal

Data wants to be free.
You can't claw back leaked bytes.
Once they know, they know.

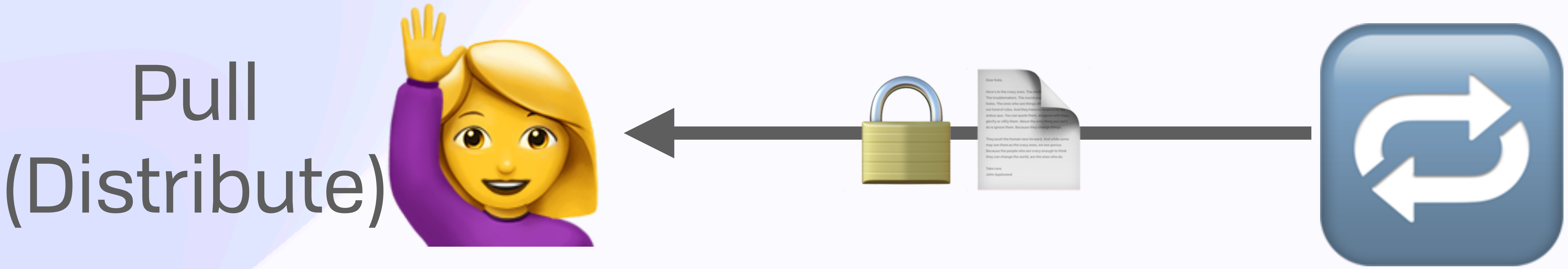
e.g. About your "surprise birthday party" 🥳😬

Protecting Writes & Agreeing on Membership

Convergent Capabilities

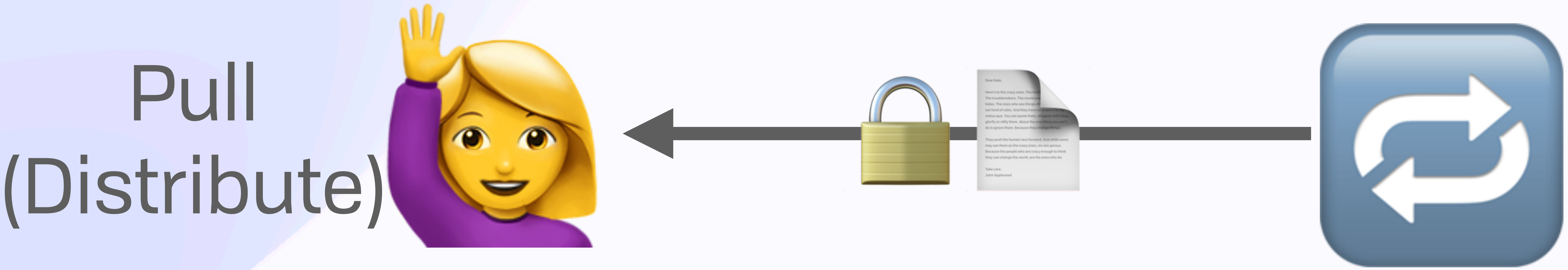
Convergent Capabilities

Convergent Capabilities



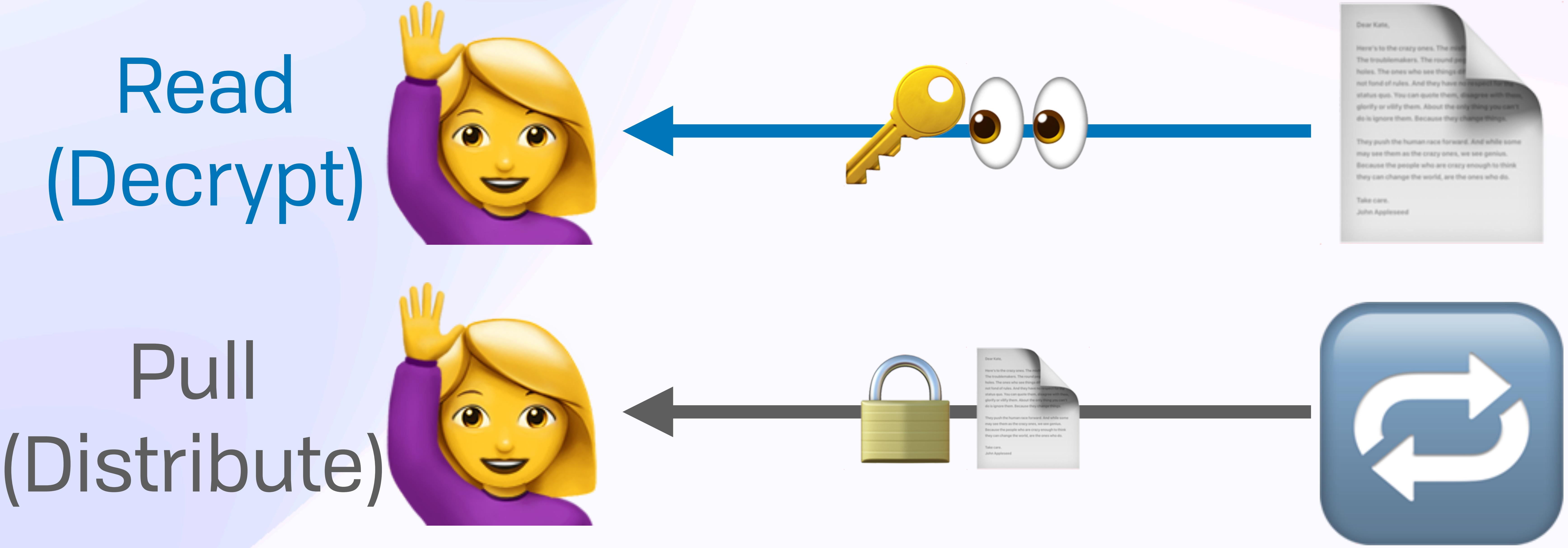
Pull
(Distribute)

Convergent Capabilities



Pull
(Distribute)

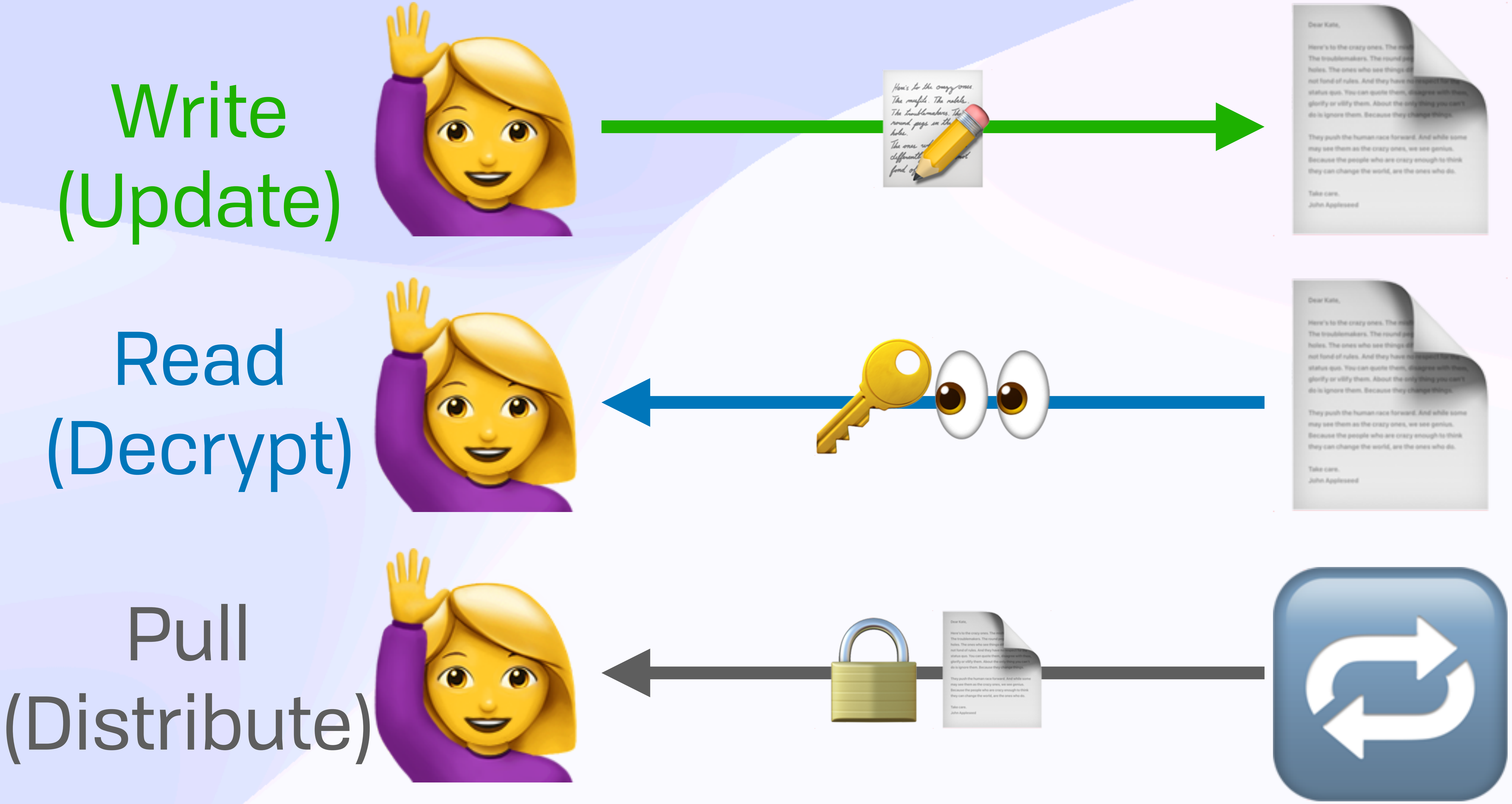
Convergent Capabilities



Read
(Decrypt)

Pull
(Distribute)

Convergent Capabilities

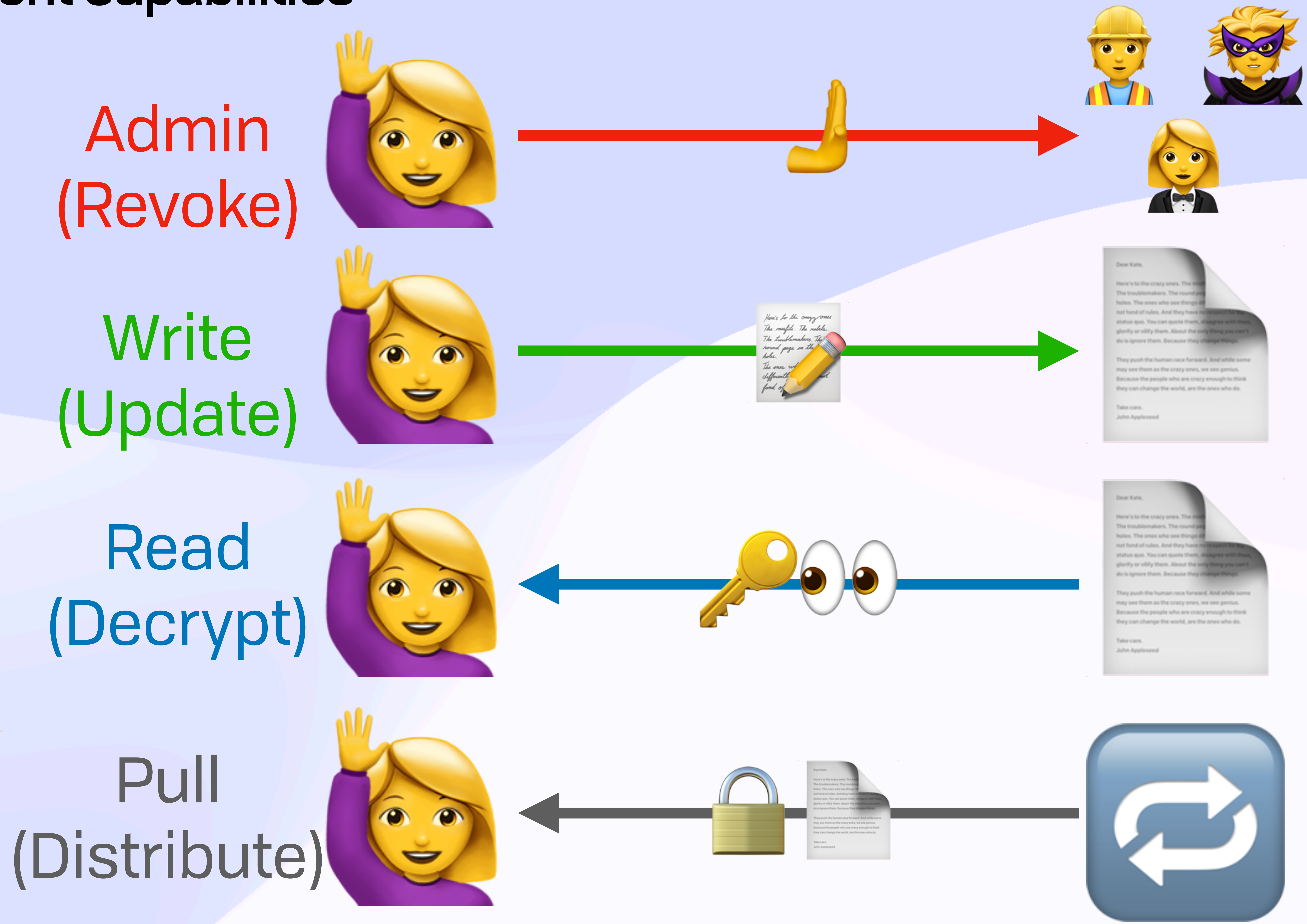


Write (Update)

Read (Decrypt)

Pull (Distribute)

Convergent Capabilities



Admin (Revoke)

Write (Update)

Read (Decrypt)

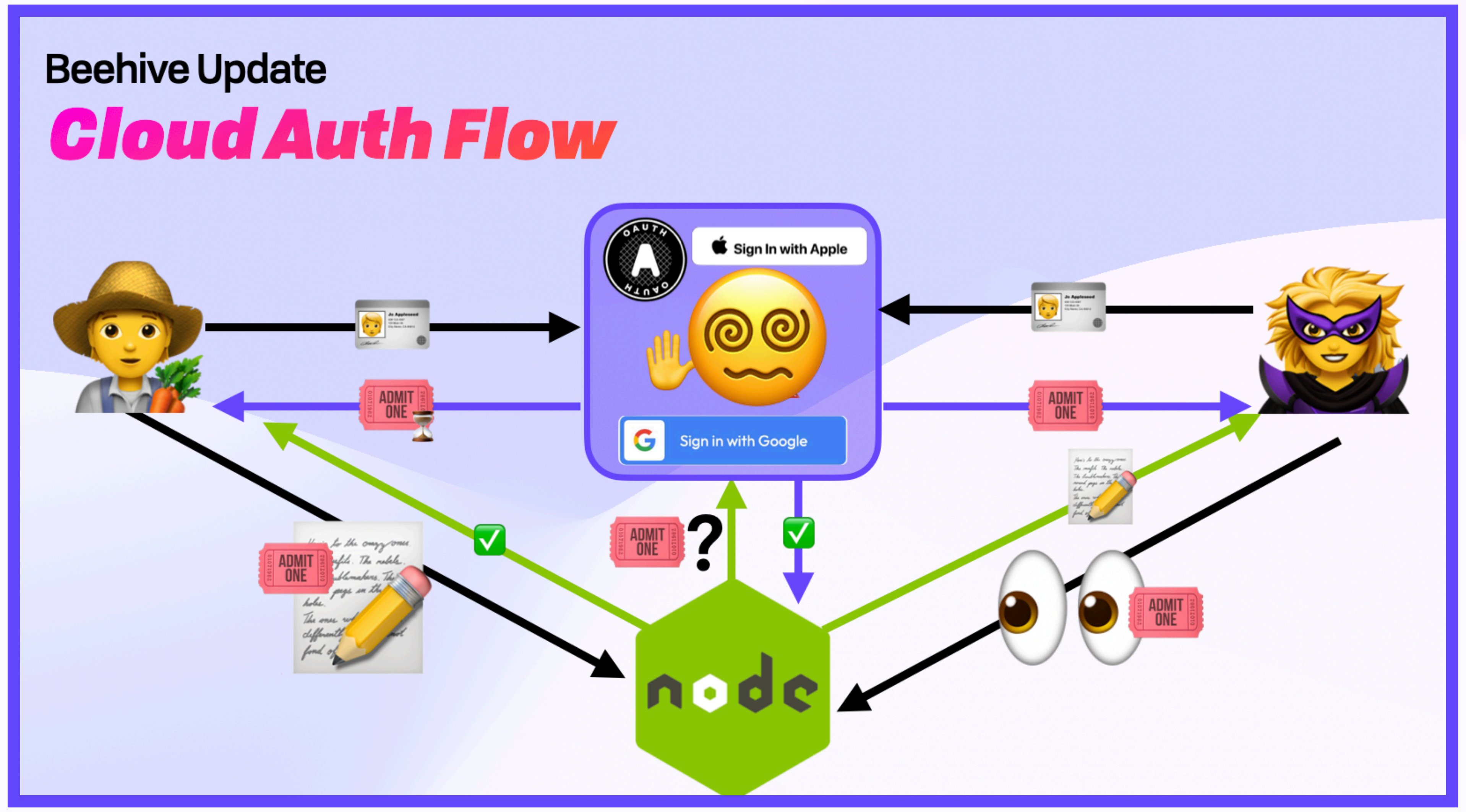
Pull (Distribute)

Convergent Capabilities

Self-Authenticating Changes

Convergent Capabilities

Self-Authenticating Changes

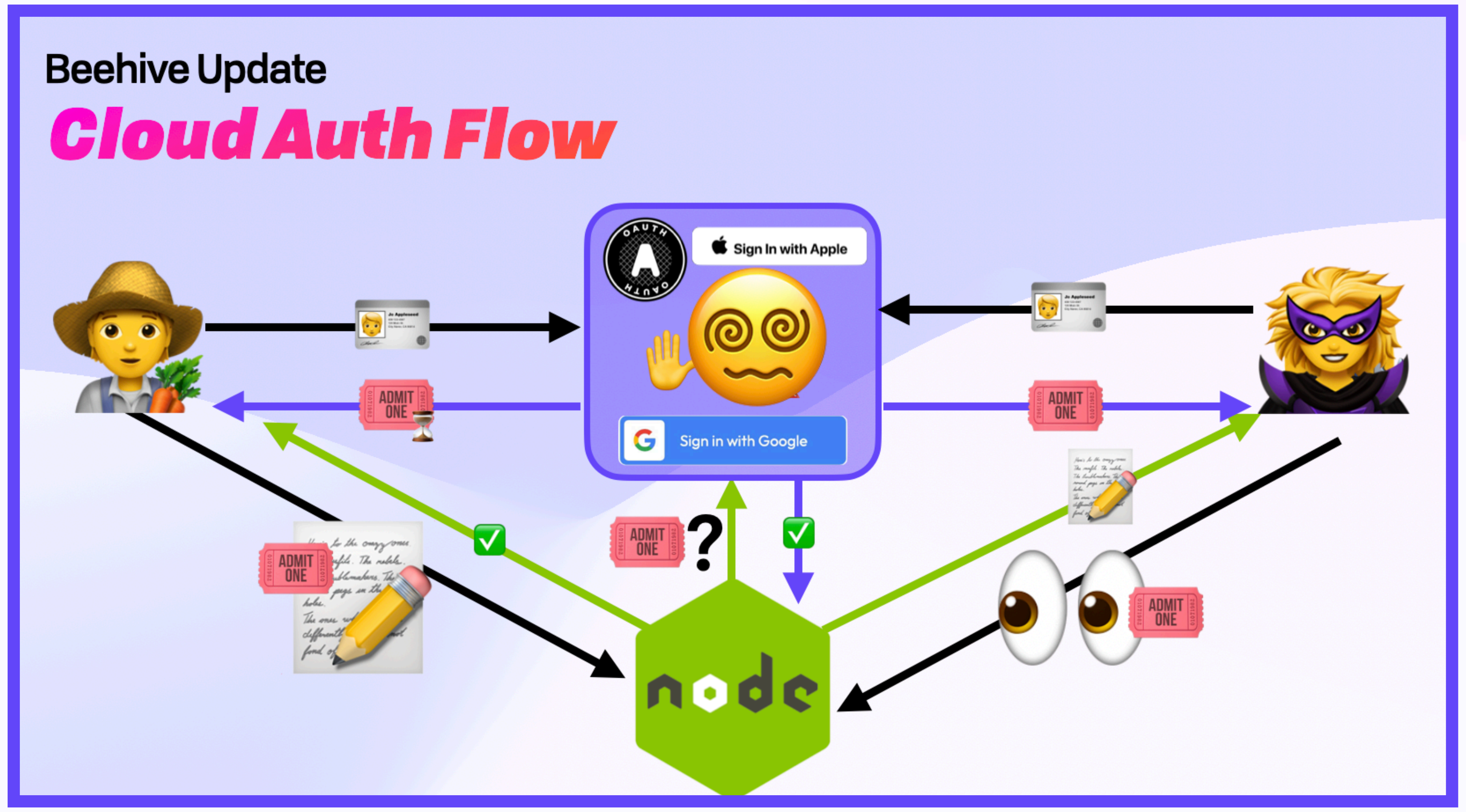


Beehive Update

Cloud Auth Flow

Convergent Capabilities

Self-Authenticating Changes

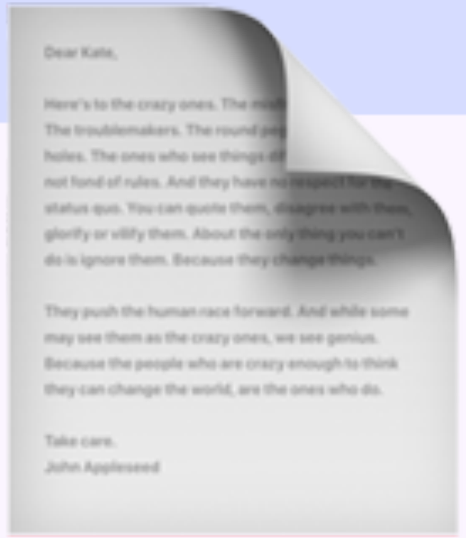


Beehive Update

Cloud Auth Flow

Convergent Capabilities

Self-Authenticating Changes

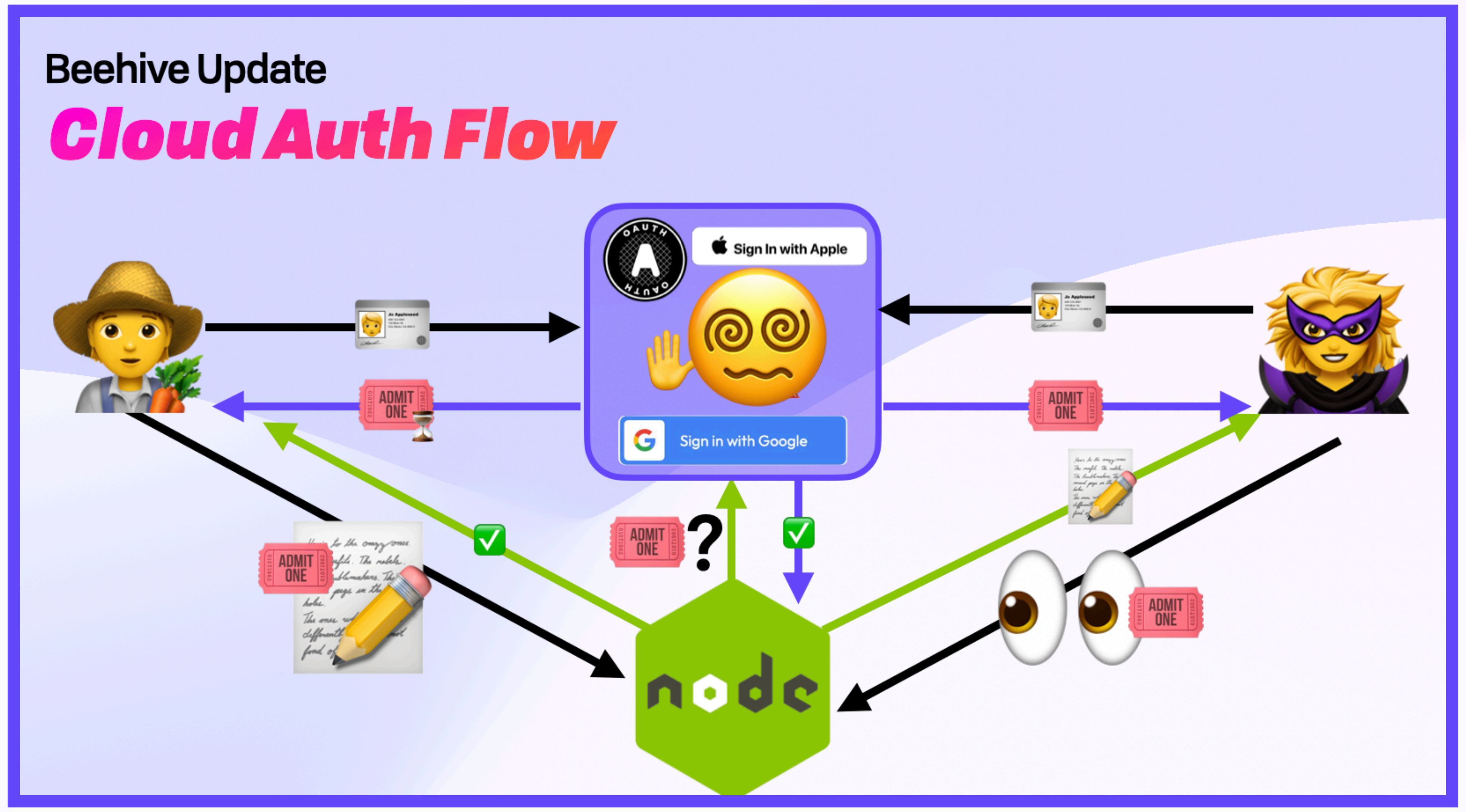


Dear Kate,

Here's to the crazy ones. The misf
The troublemakers. The round peg
holes. The ones who see things di
not fond of rules. And they have no respect for the
status quo. You can quote them, disagree with them,
glorify or vilify them. About the only thing you can't
do is ignore them. Because they change things.

They push the human race forward. And while some
may see them as the crazy ones, we see genius.
Because the people who are crazy enough to think
they can change the world, are the ones who do.

Take care.
John Appleseed

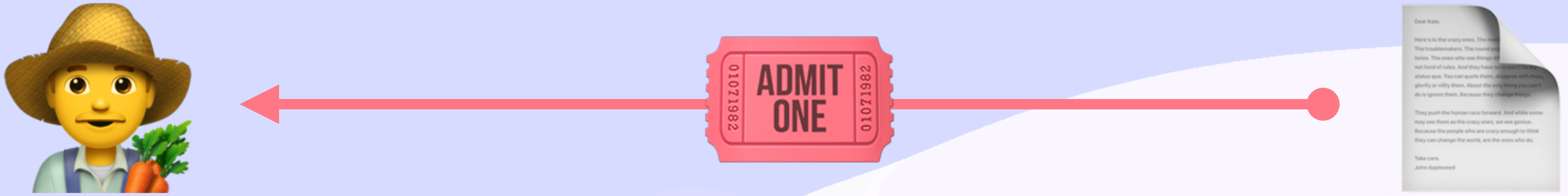


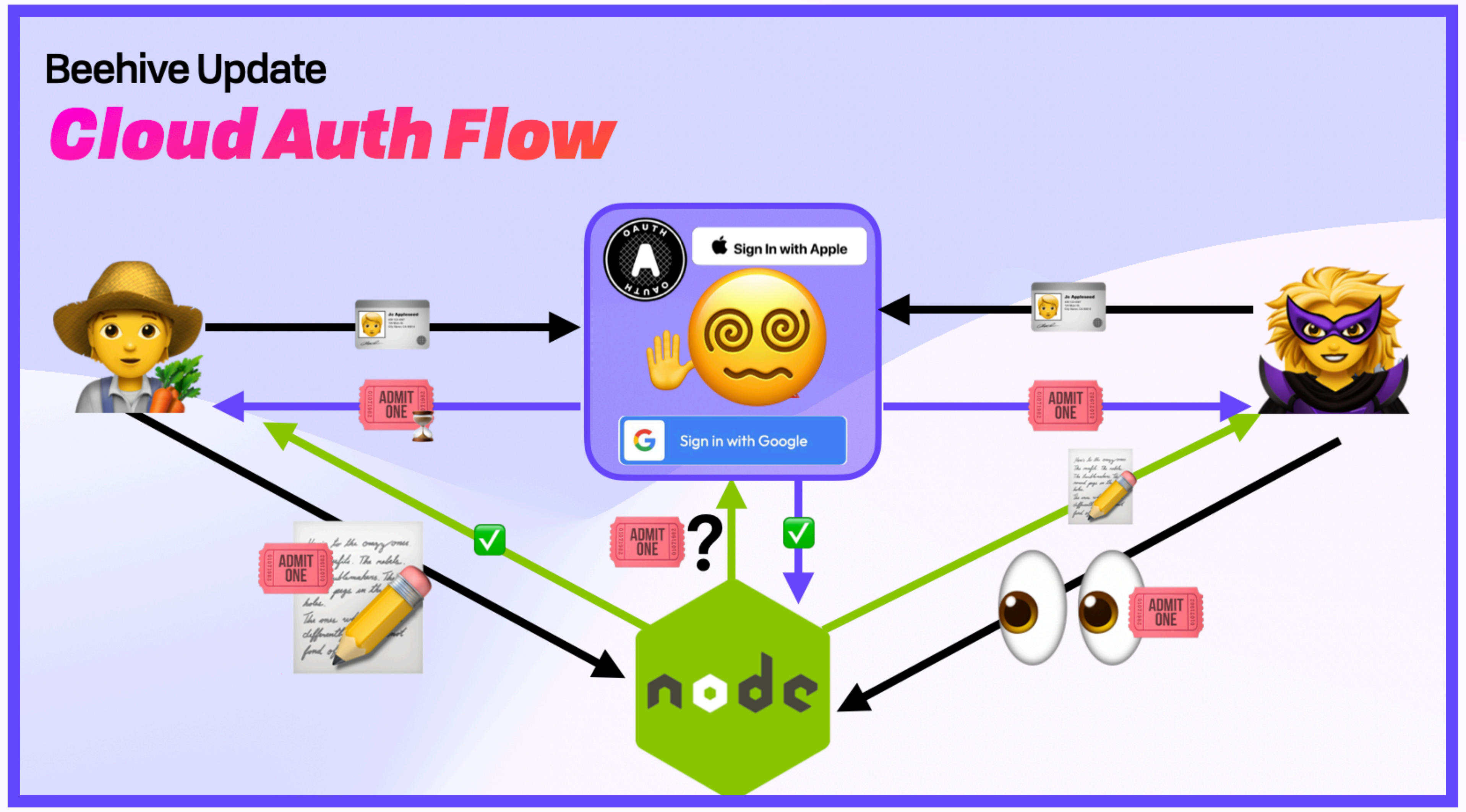
Beehive Update

Cloud Auth Flow

Convergent Capabilities

Self-Authenticating Changes


ADMIT ONE
01071982
01071982
Dear Kate,
Here's to the crazy ones. The
The troublemakers. The round peg
holes. The ones who see things di
not fond of rules. And they have no respect for the
status quo. You can quote them, disagree with them,
glorify or vilify them. About the only thing you can't
do is ignore them. Because they change things.
They push the human race forward. And while some
may see them as the crazy ones, we see genius.
Because the people who are crazy enough to think
they can change the world, are the ones who do.
Take care,
John Appleseed

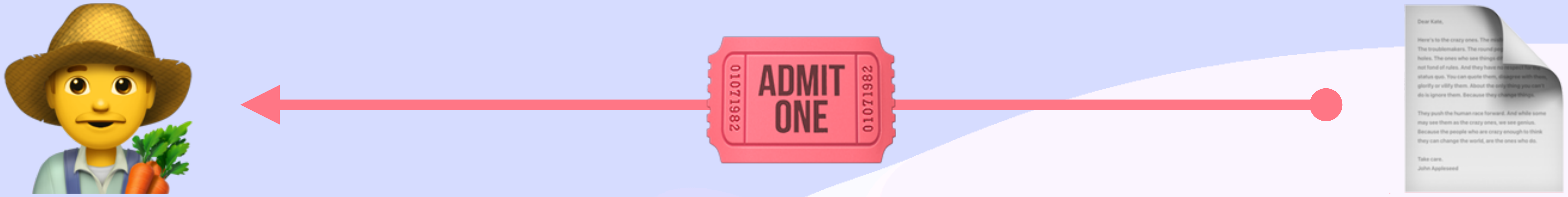


Beehive Update

Cloud Auth Flow

Convergent Capabilities

Self-Authenticating Changes

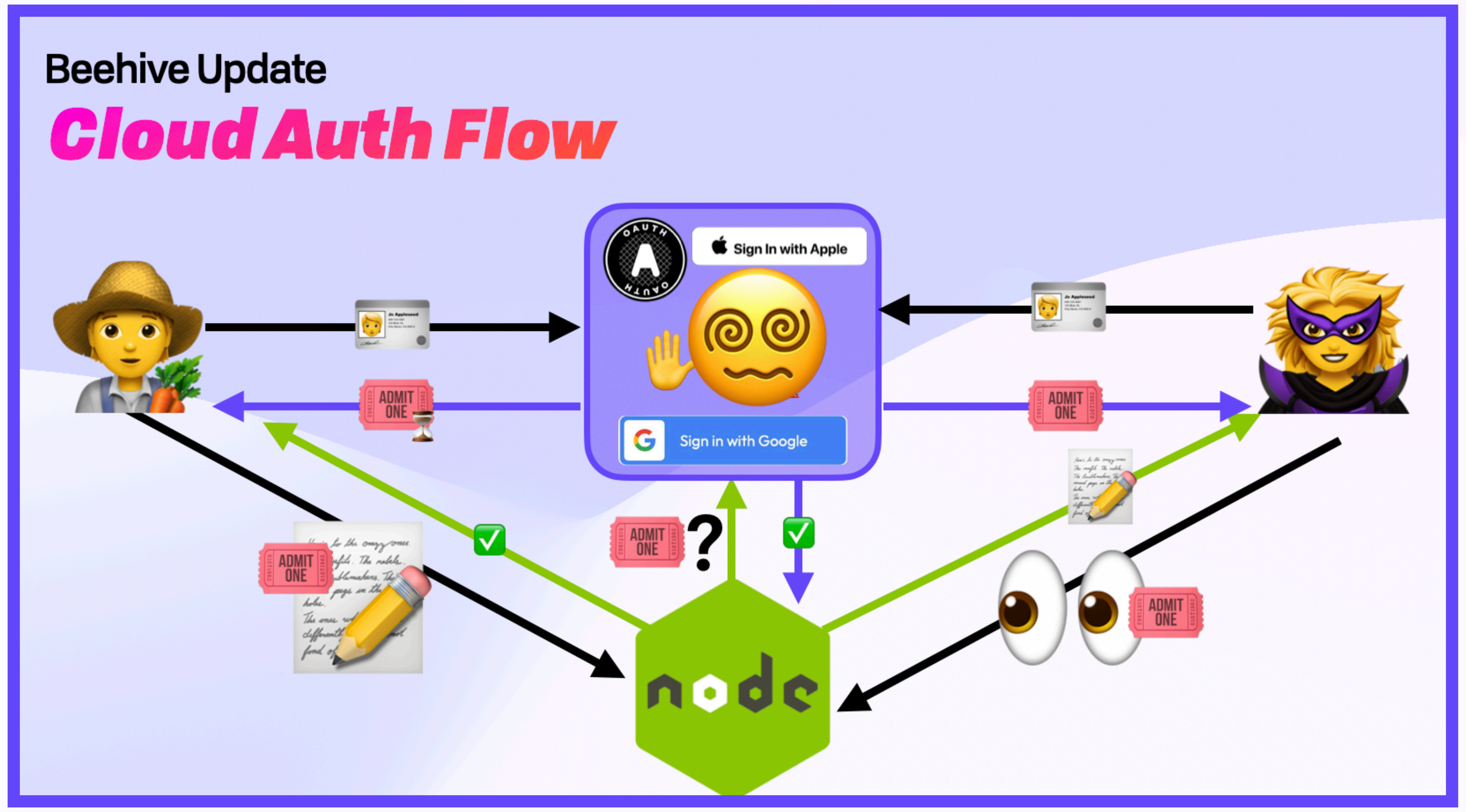


Dear Kate,

Here's to the crazy ones. The misfi
The troublemakers. The round peg
holes. The ones who see things dif
not fond of rules. And they have no respect for the
status quo. You can quote them, disagree with them,
glorify or vilify them. About the only thing you can't
do is ignore them. Because they change things.

They push the human race forward. And while some
may see them as the crazy ones, we see genius.
Because the people who are crazy enough to think
they can change the world, are the ones who do.

Take care.
John Appleseed



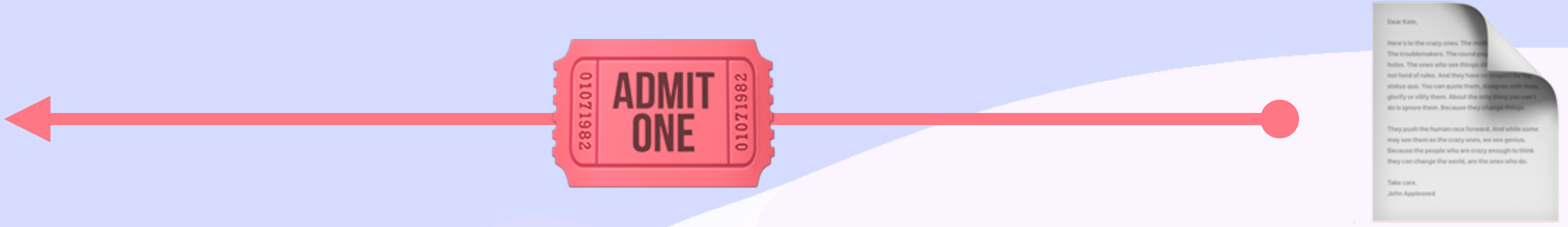
Beehive Update

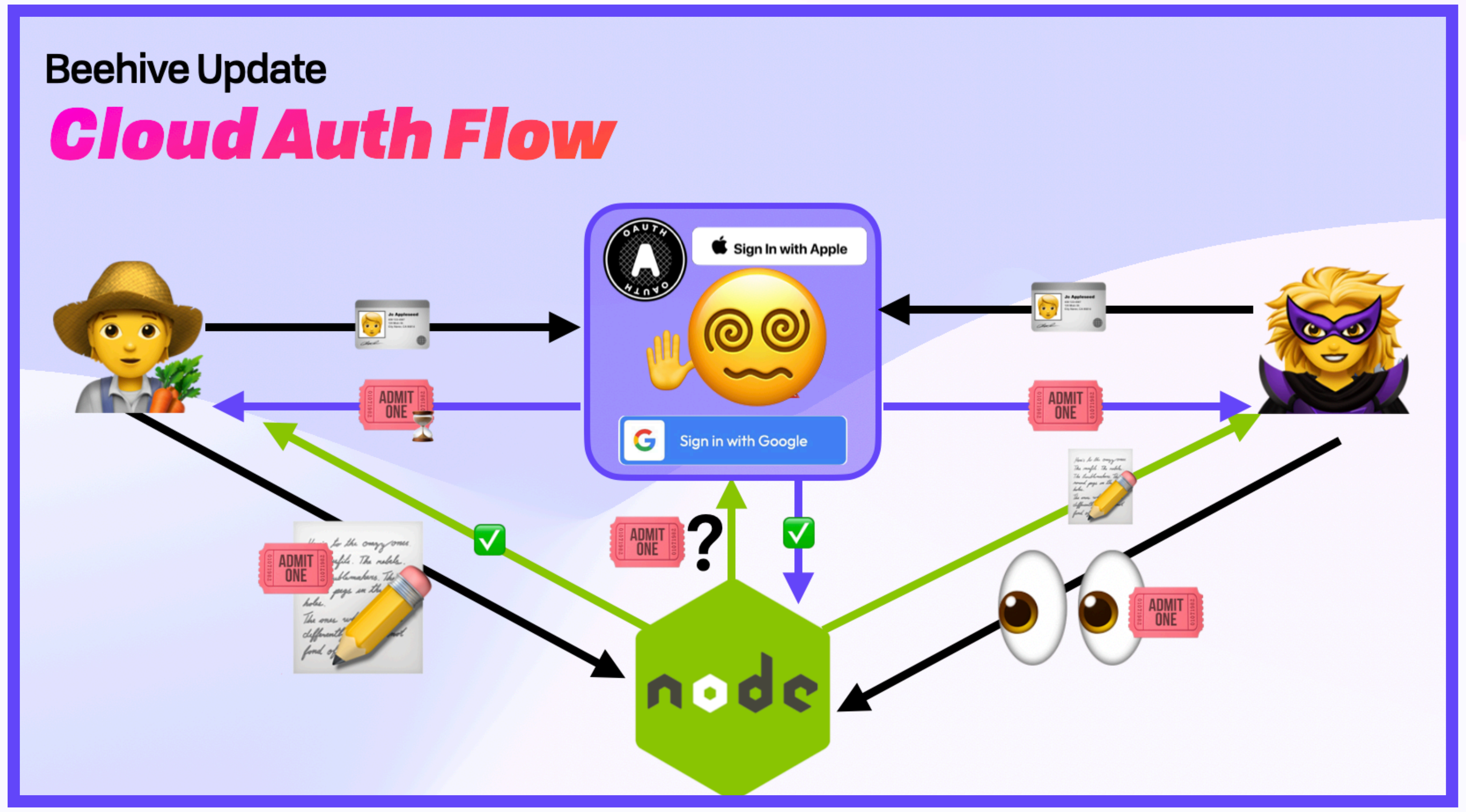
Cloud Auth Flow

Convergent Capabilities

Self-Authenticating Changes

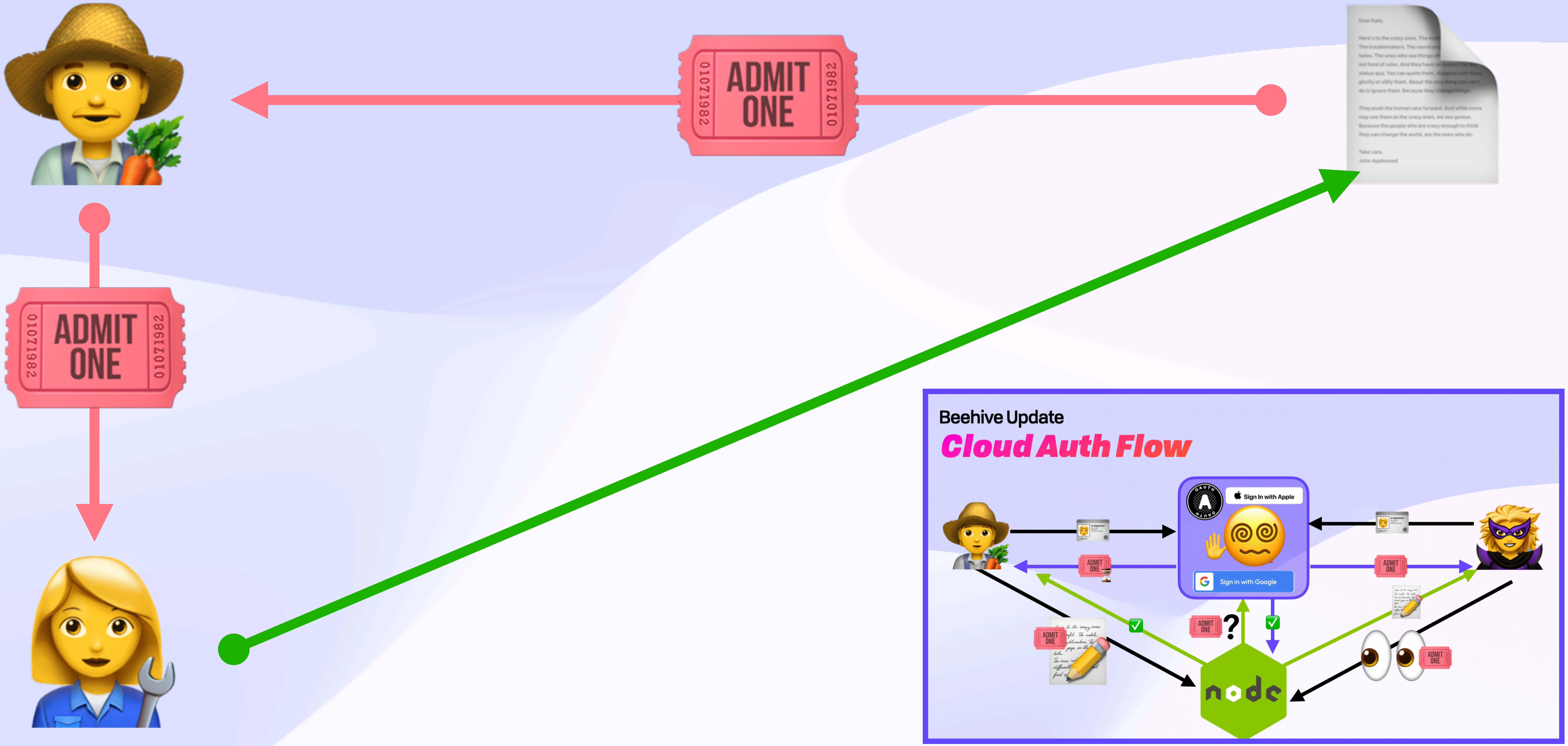
ADMIT ONE
01071982





Convergent Capabilities

Self-Authenticating Changes



Dear Kate,

Here's to the crazy ones. The mis
The troublemakers. The round pe
holes. The ones who see things di
not fond of rules. And they have no respect for the
status quo. You can quote them, disagree with them,
glorify or vilify them. About the only thing you can't
do is ignore them. Because they change things.

They push the human race forward. And while some
may see them as the crazy ones, we see genius.
Because the people who are crazy enough to think
they can change the world, are the ones who do.

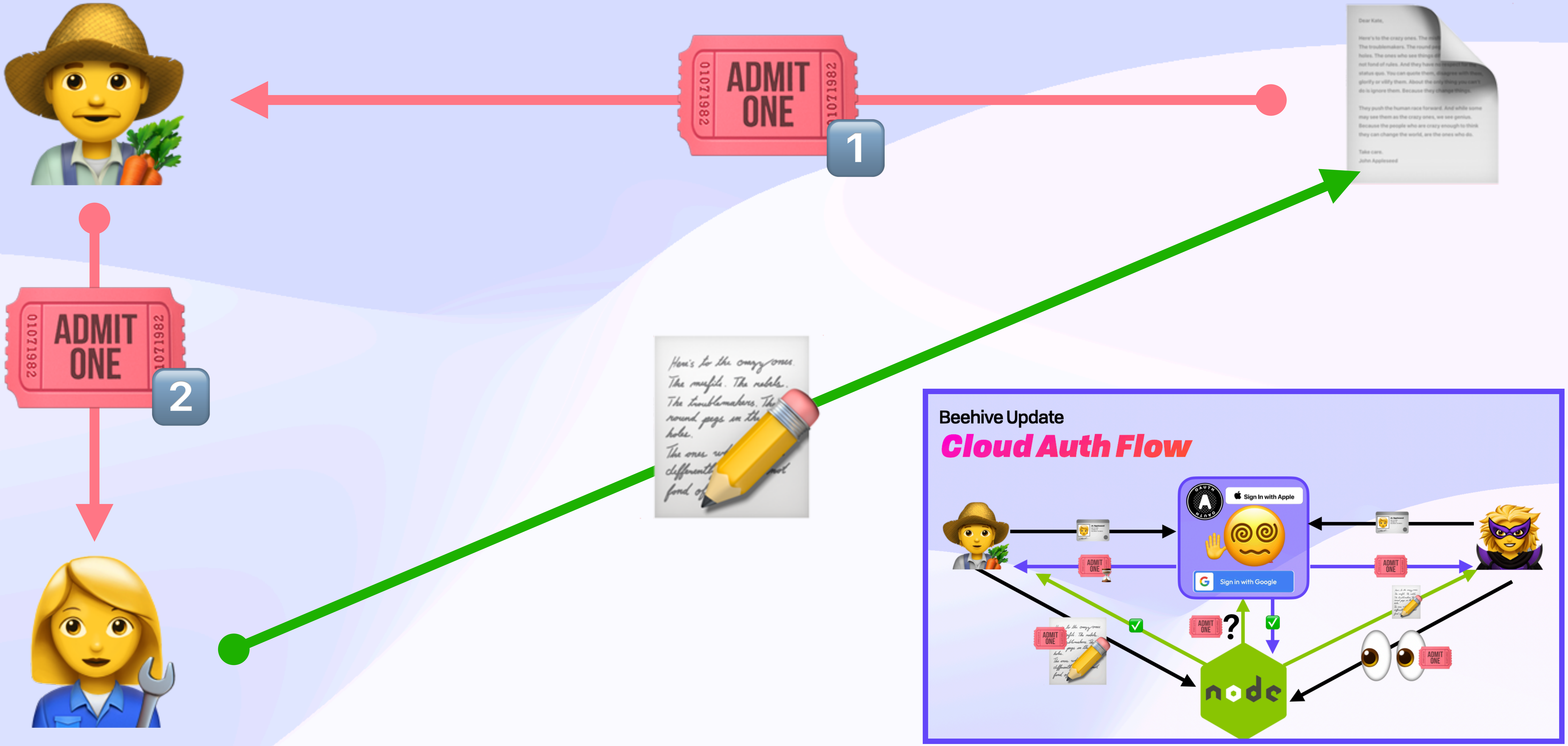
Take care,
John Appleseed

Beehive Update

Cloud Auth Flow

Convergent Capabilities

Self-Authenticating Changes

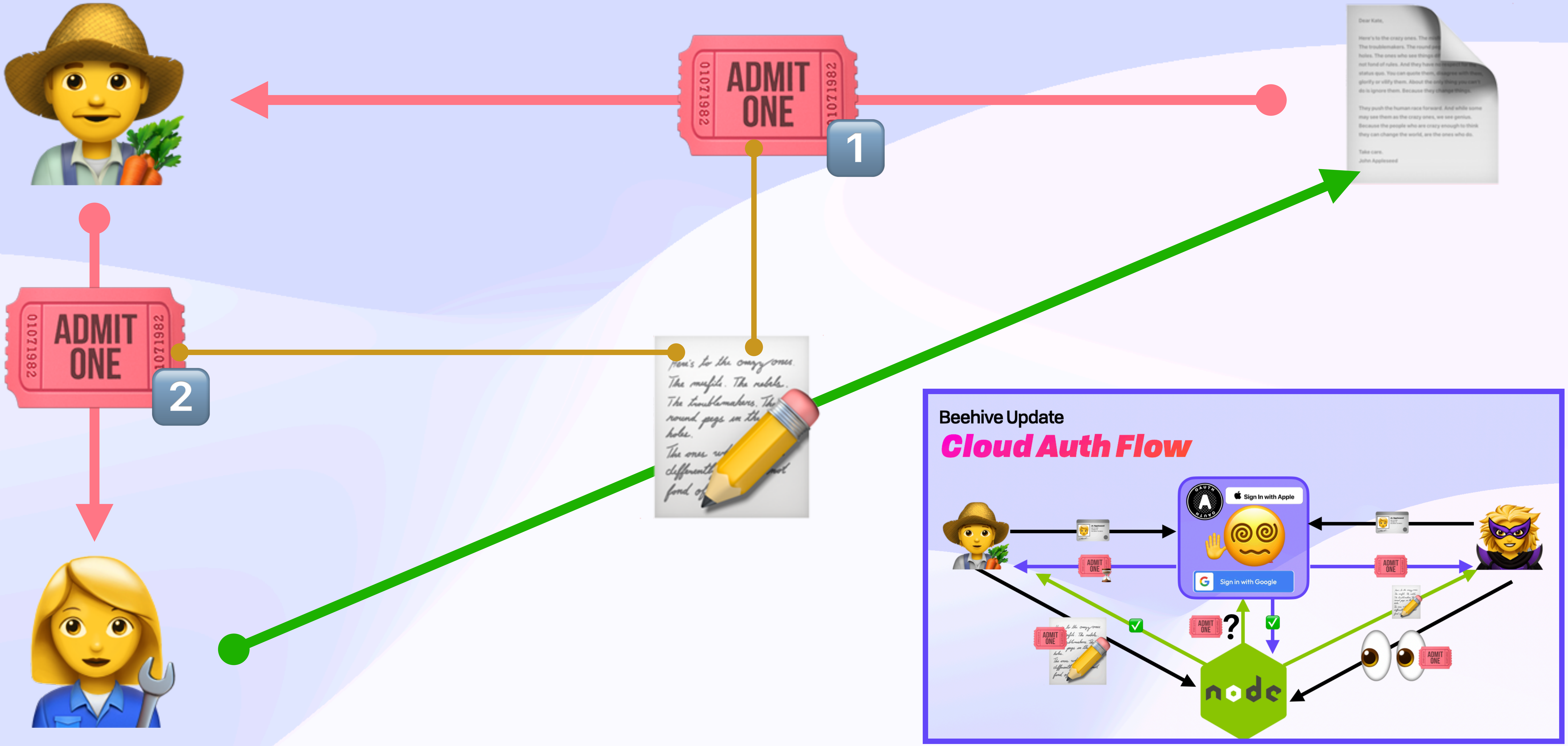

ADMIT ONE
01071982
1
ADMIT ONE
01071982
2
Here's to the crazy ones. The misfits. The rebels. The troublemakers. The round pegs in the holes.
Sign in with Apple
Sign in with Google
node

Beehive Update

Cloud Auth Flow

Convergent Capabilities

Self-Authenticating Changes



Dear Kate,

Here's to the crazy ones. The mis
The troublemakers. The round peg
holes. The ones who see things dif
not fond of rules. And they have no respect for the
status quo. You can quote them, disagree with them,
glorify or vilify them. About the only thing you can't
do is ignore them. Because they change things.

They push the human race forward. And while some
may see them as the crazy ones, we see genius.
Because the people who are crazy enough to think
they can change the world, are the ones who do.

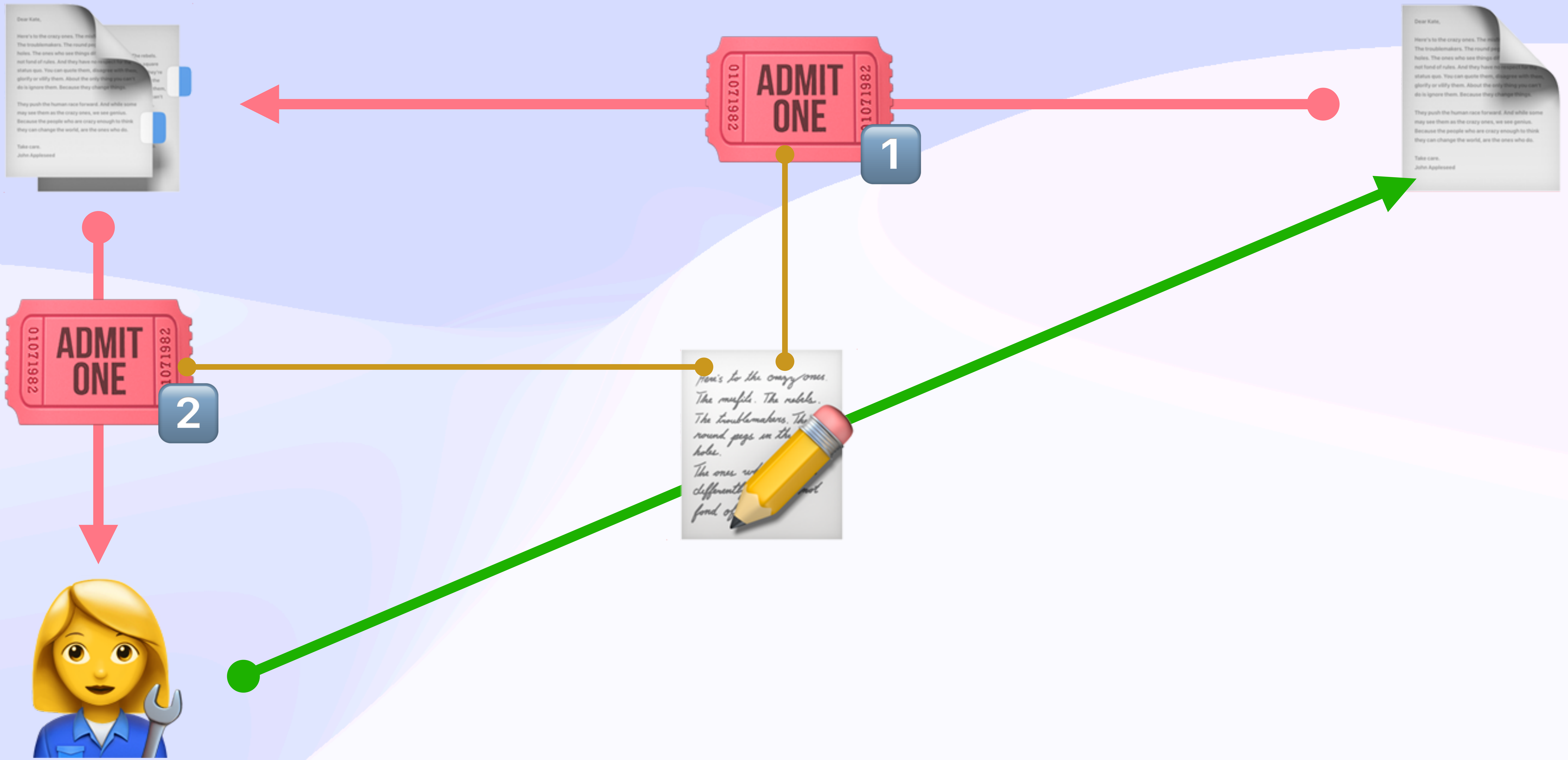
Take care,
John Appleseed

Beehive Update

Cloud Auth Flow

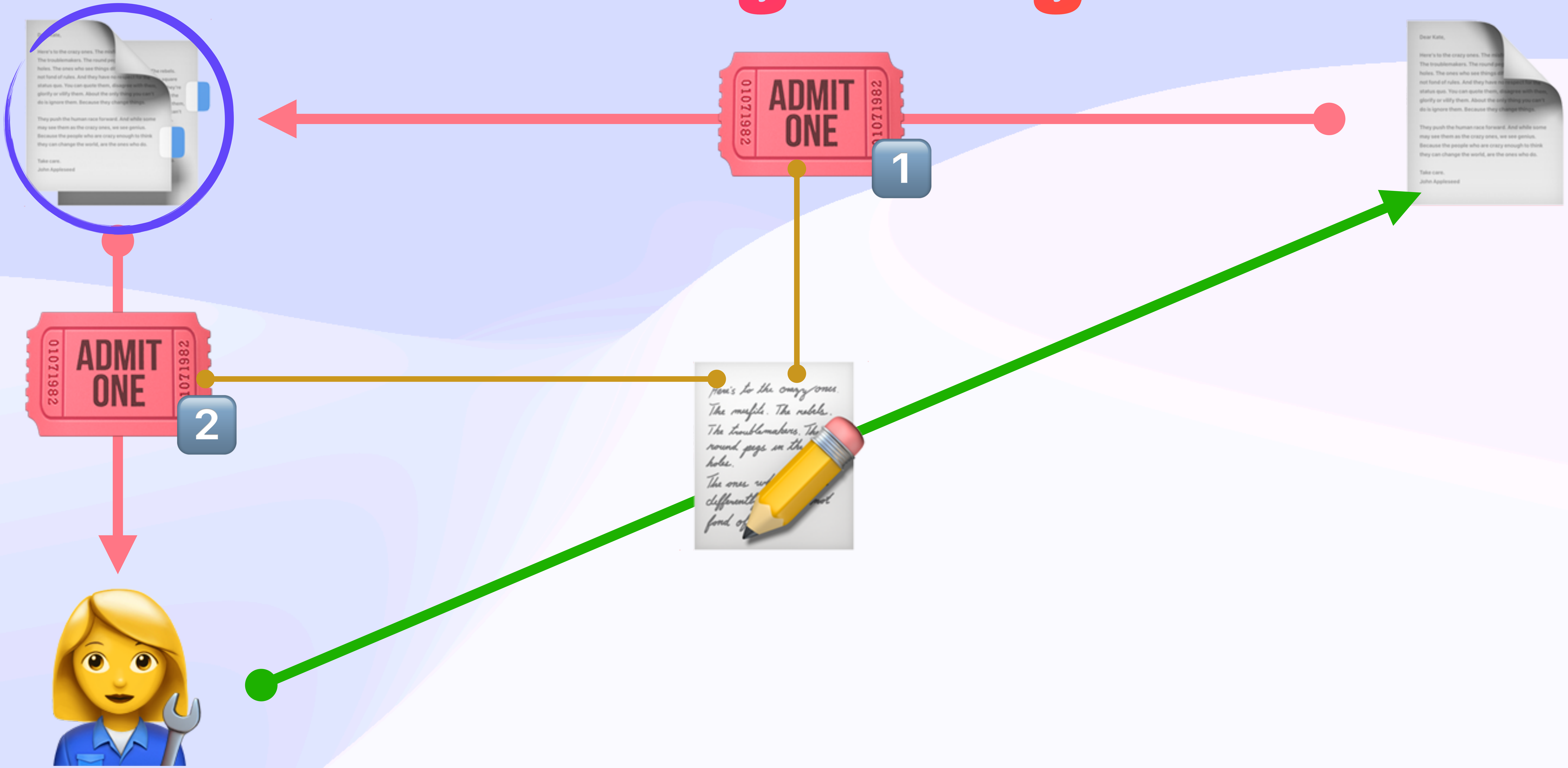
Convergent Capabilities

Self-Authenticating Changes



Convergent Capabilities

Self-Authenticating Changes



Convergent Capabilities

Example High Level API

Convergent Capabilities

Example High Level API

```
authedDocHandle.change(doc => {
  doc.event = "Local First Conf"
  doc.city ="Berlin"
})
```

Convergent Capabilities

Example High Level API

```
authedDocHandle.change(doc => {
  doc.event = "Local First Conf"
  doc.city ="Berlin"
})

authedDocHandle.addMember(alice, ADMIN)
```

Convergent Capabilities

Example High Level API

```
authedDocHandle.change(doc ⇒ {
  doc.event = "Local First Conf"
  doc.city ="Berlin"
})

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

Convergent Capabilities

Groups

Convergent Capabilities

Groups

Alice's Phone

Convergent Capabilities

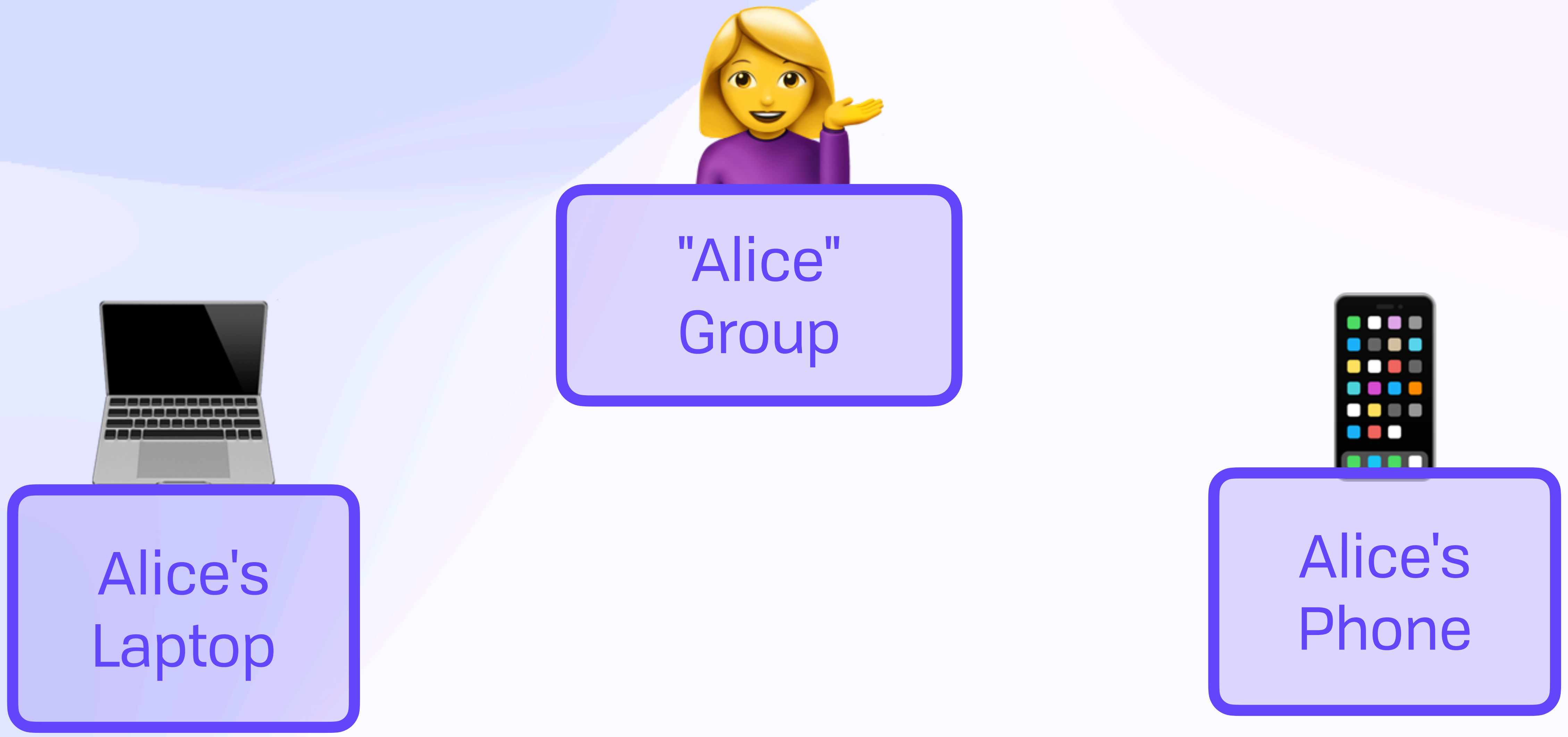
Groups

Alice's Laptop

Alice's Phone

Convergent Capabilities

Groups



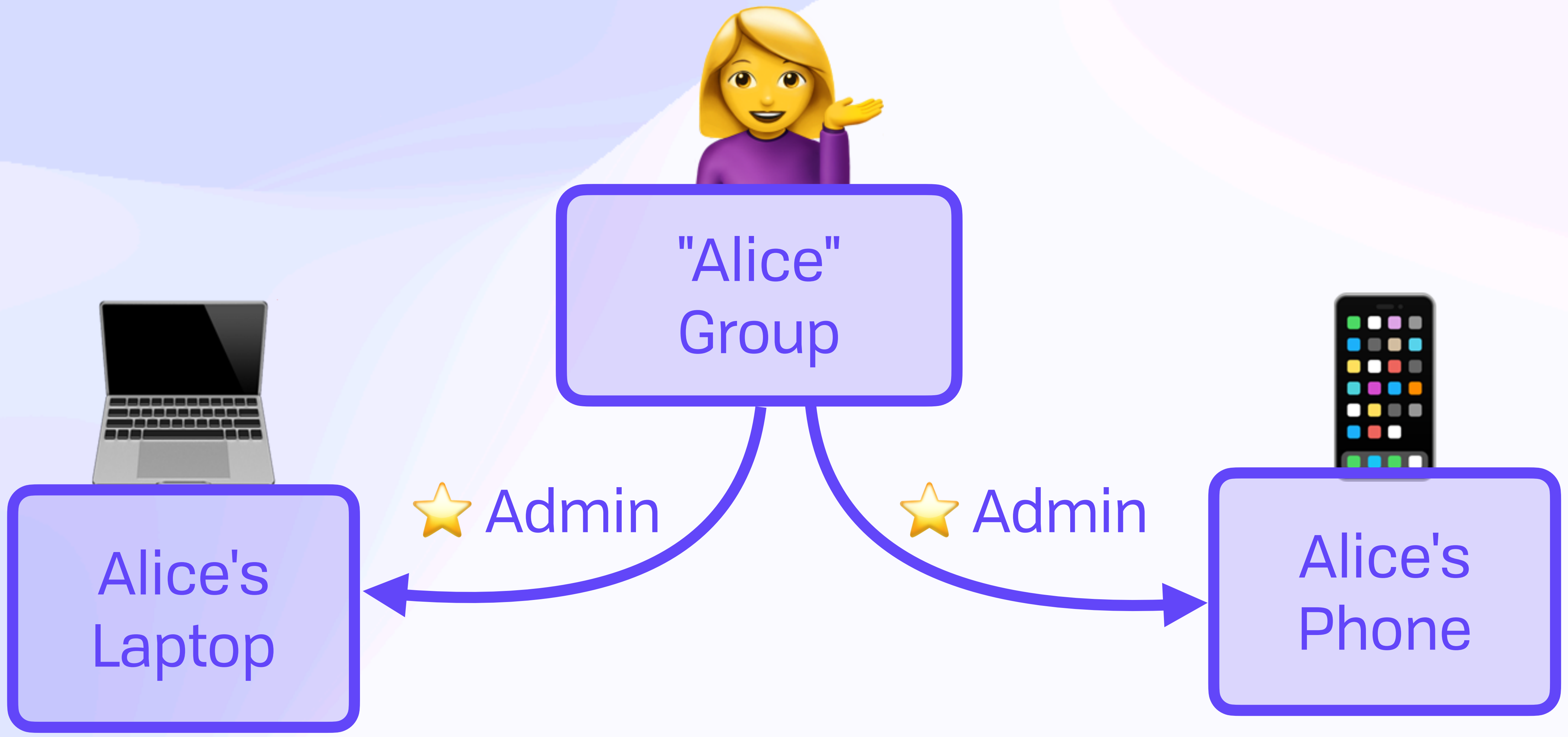
"Alice" Group

Alice's Laptop

Alice's Phone

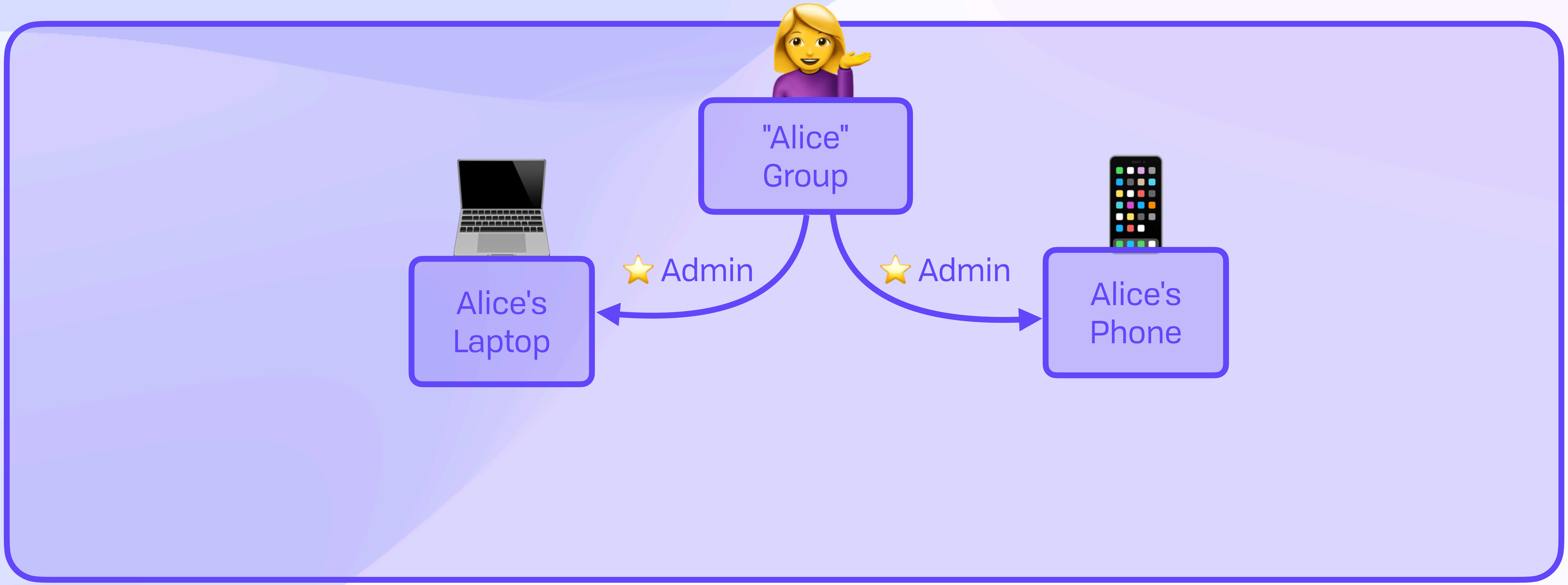
Convergent Capabilities

Groups



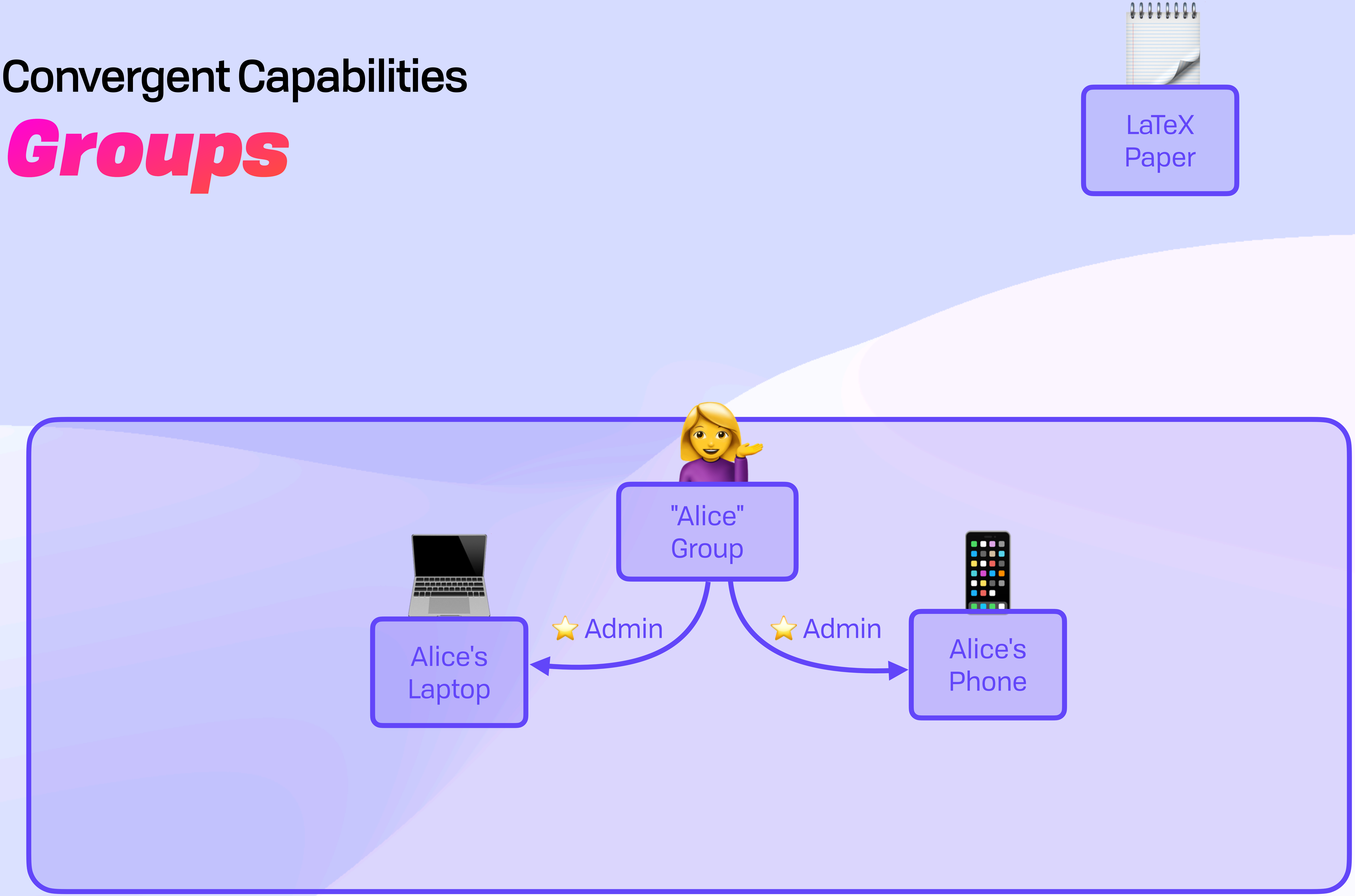
Convergent Capabilities

Groups



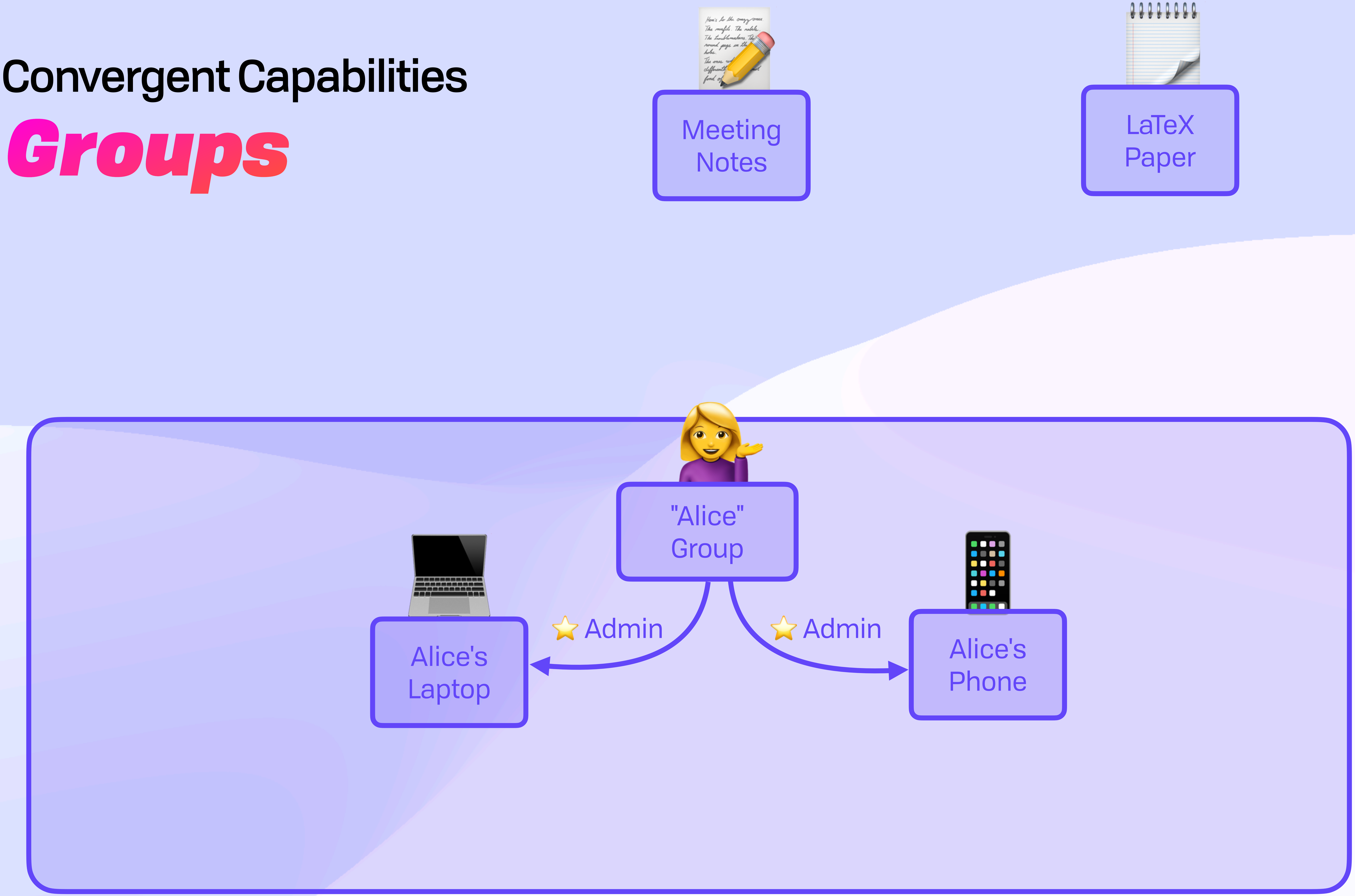
Convergent Capabilities

Groups



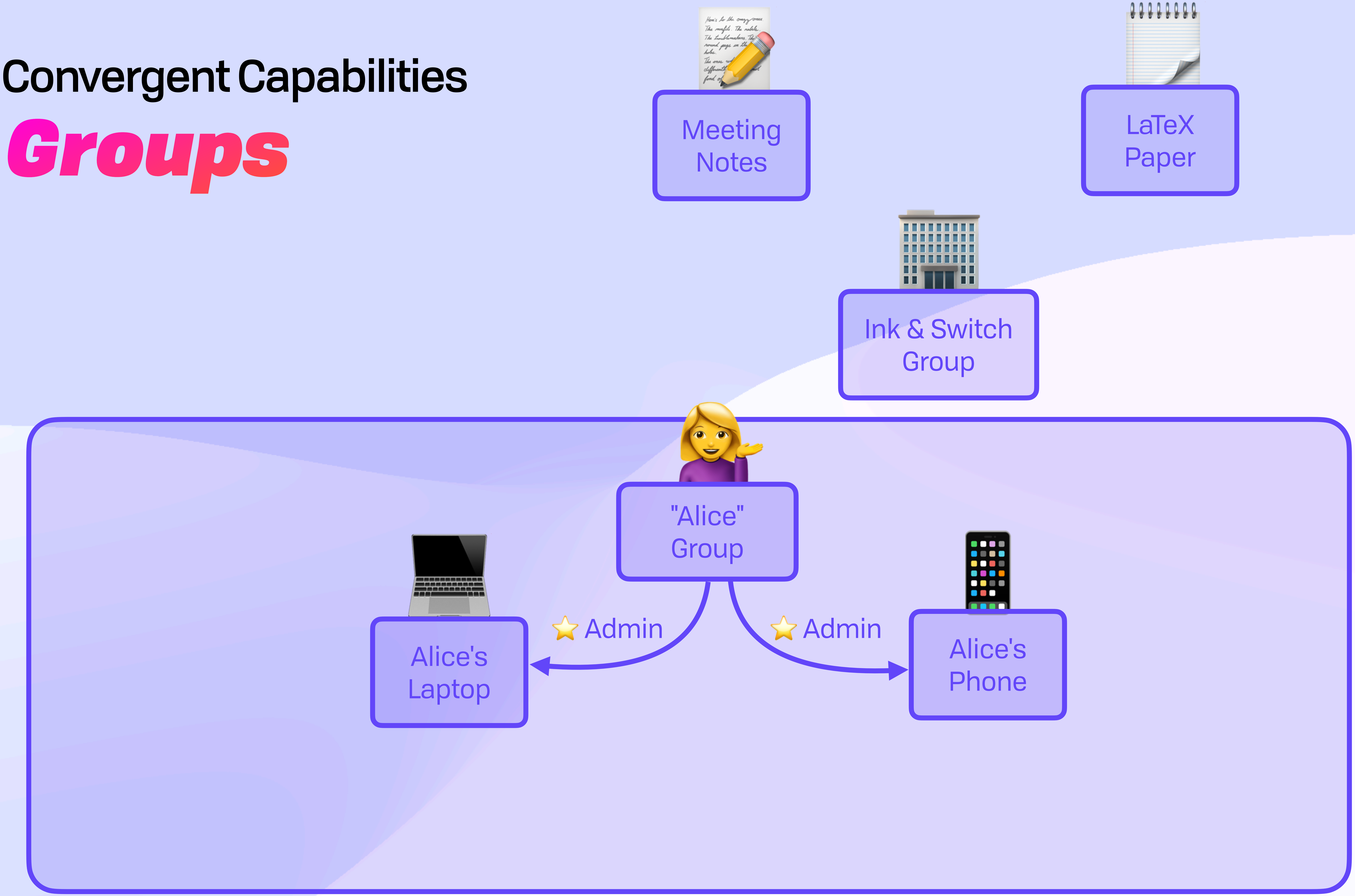
Convergent Capabilities

Groups



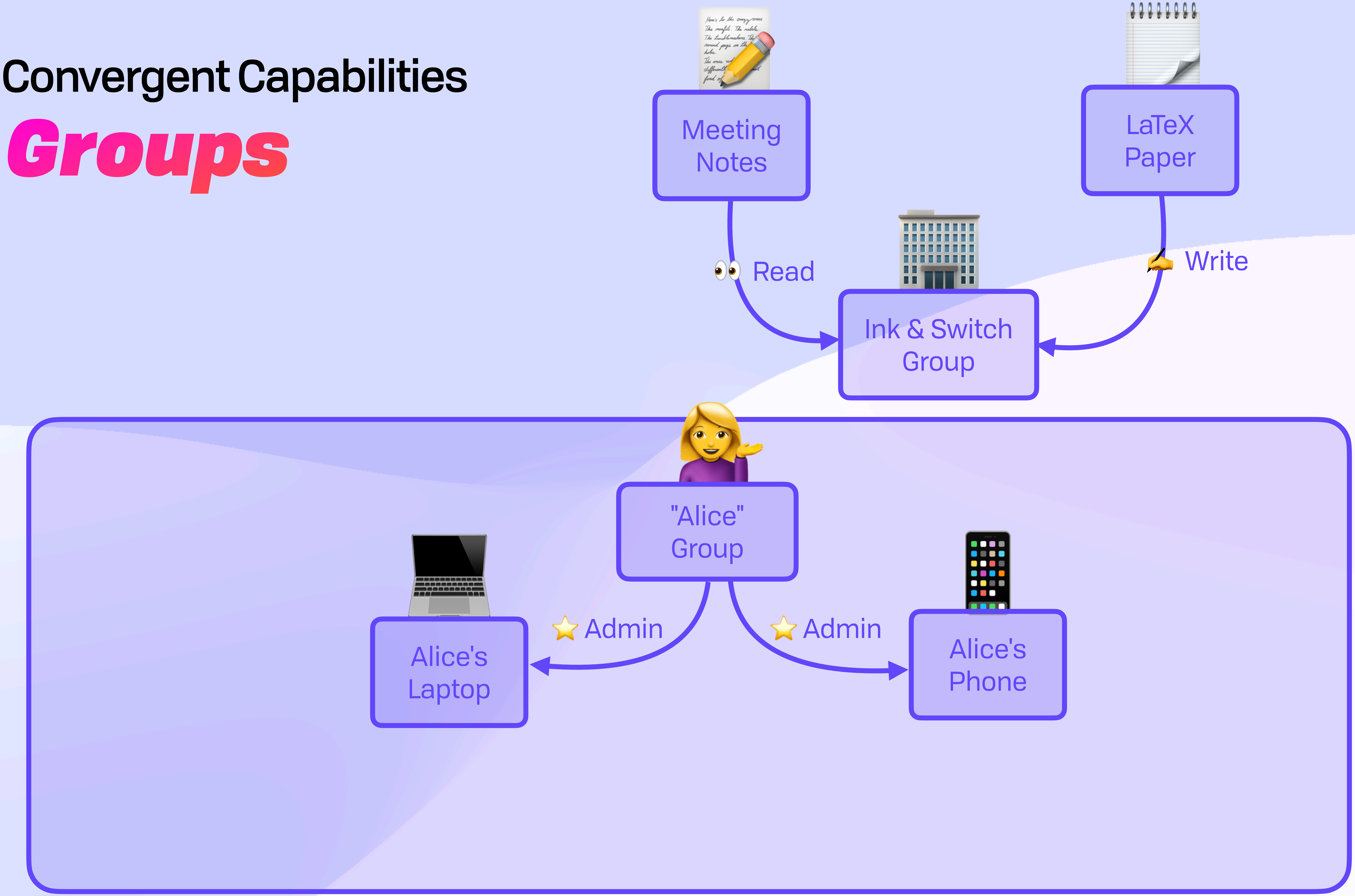
Convergent Capabilities

Groups



Convergent Capabilities

Groups



Meeting Notes

LaTeX Paper

👀 Read

✍️ Write

Ink & Switch Group

"Alice" Group

⭐ Admin

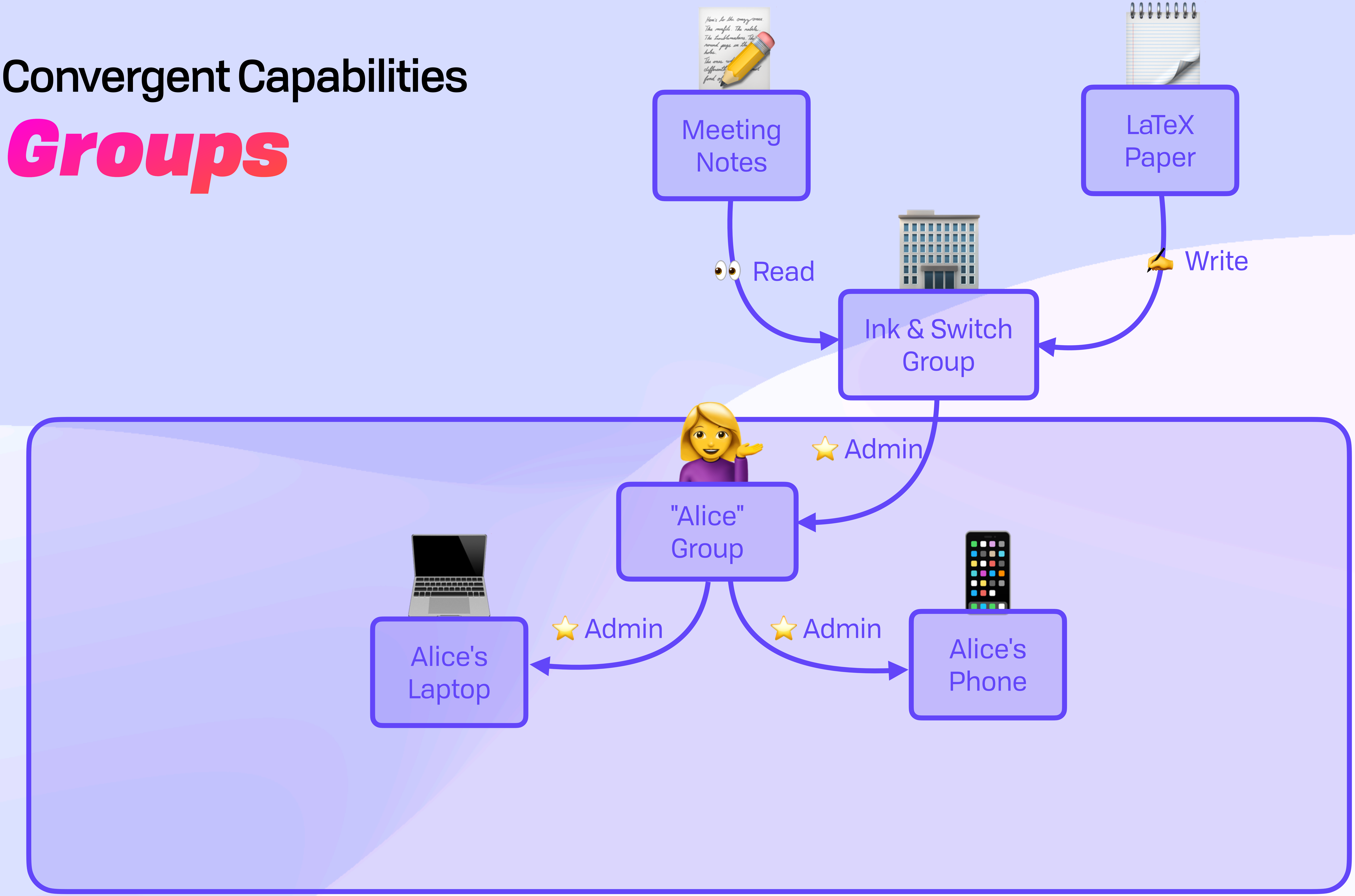
⭐ Admin

Alice's Laptop

Alice's Phone

Convergent Capabilities

Groups



Meeting Notes

LaTeX Paper

👀 Read

✍️ Write

Ink & Switch Group

⭐ Admin

"Alice" Group

⭐ Admin

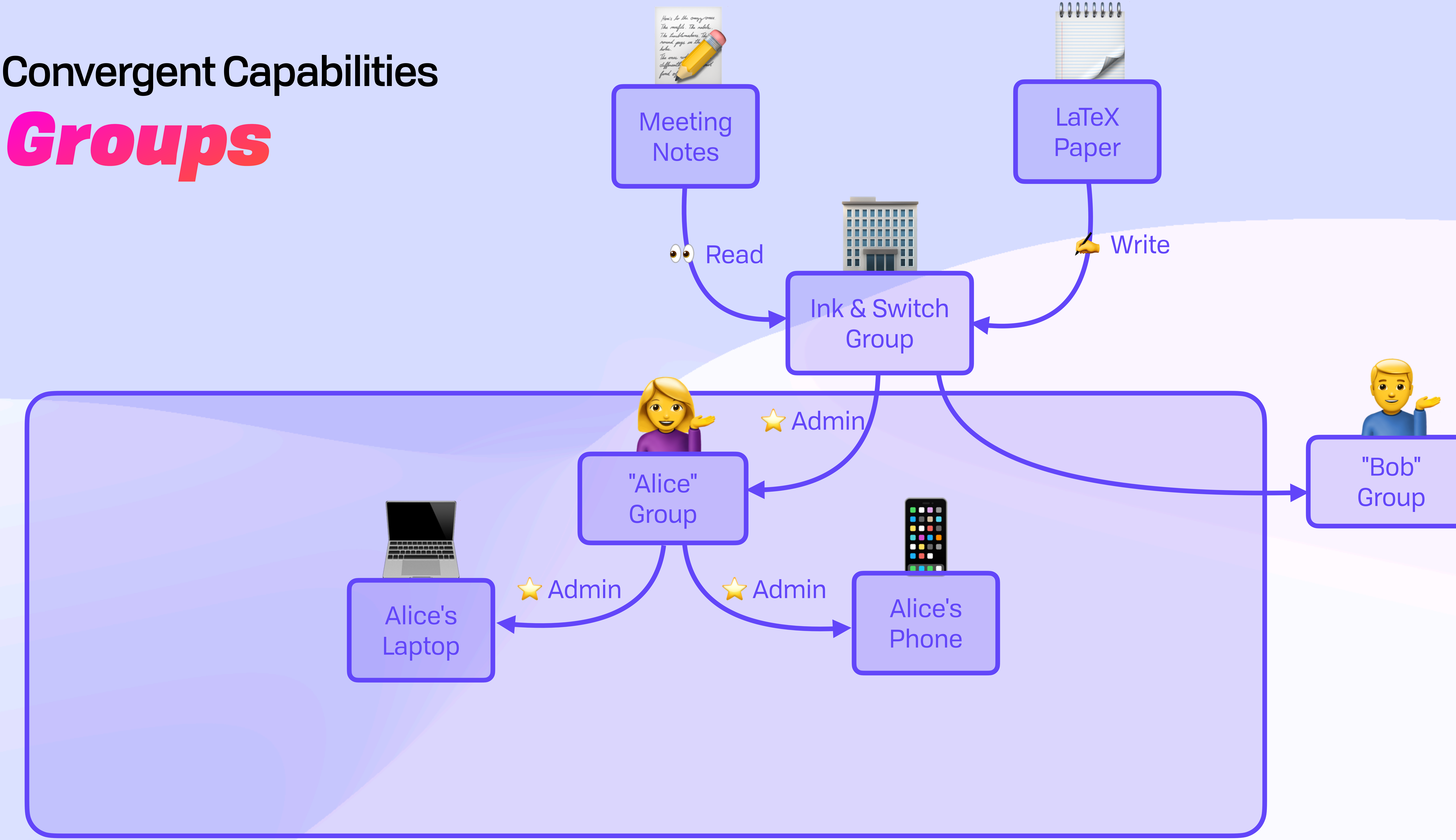
⭐ Admin

Alice's Laptop

Alice's Phone

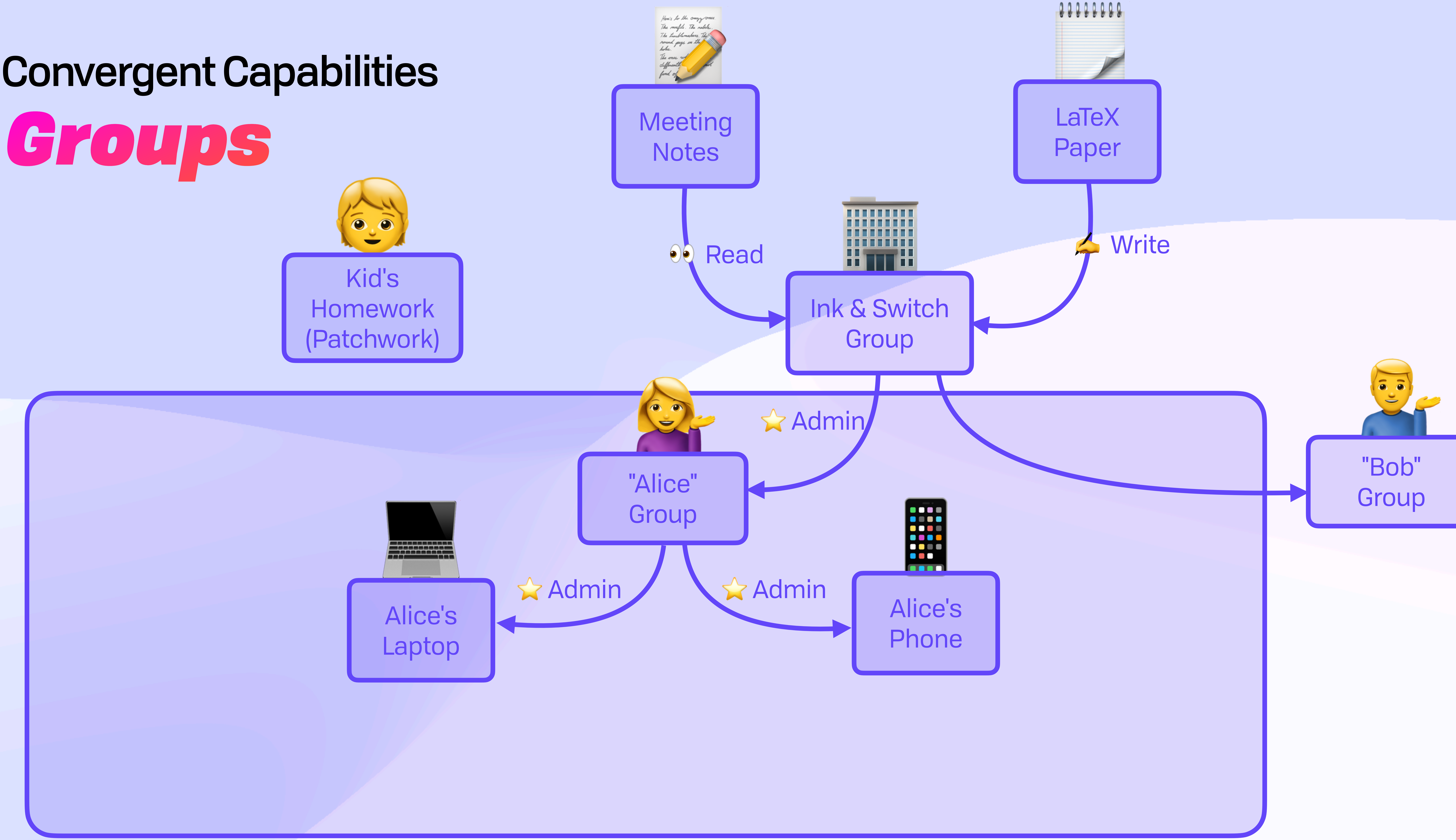
Convergent Capabilities

Groups



Convergent Capabilities

Groups



Kid's Homework (Patchwork)

Meeting Notes

LaTeX Paper

👀 Read

✍️ Write

Ink & Switch Group

⭐ Admin

"Alice" Group

"Bob" Group

⭐ Admin

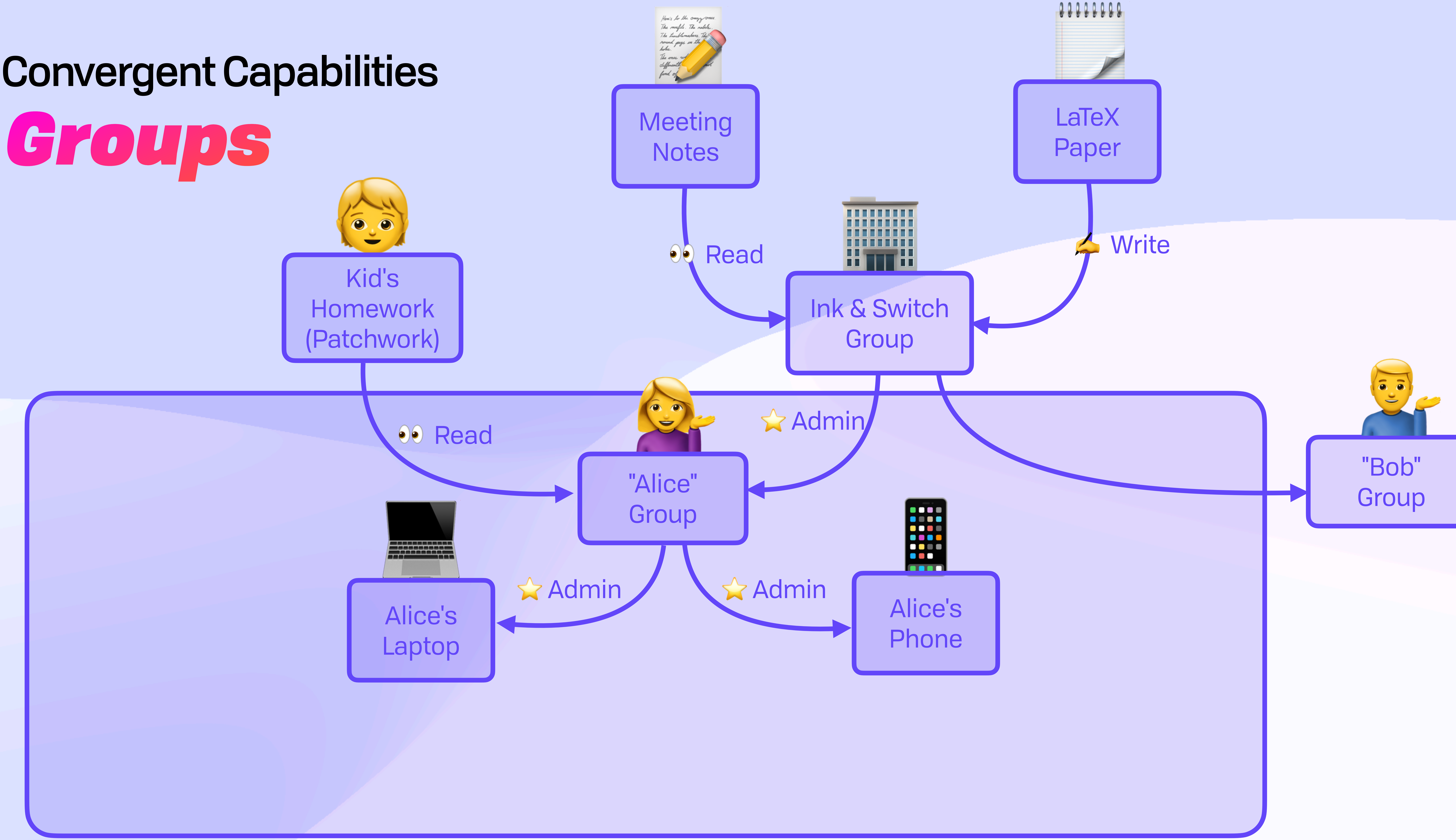
⭐ Admin

Alice's Laptop

Alice's Phone

Convergent Capabilities

Groups



Meeting Notes

LaTeX Paper

Kid's Homework (Patchwork)

👀 Read

✍ Write

Ink & Switch Group

⭐ Admin

👀 Read

"Alice" Group

"Bob" Group

⭐ Admin

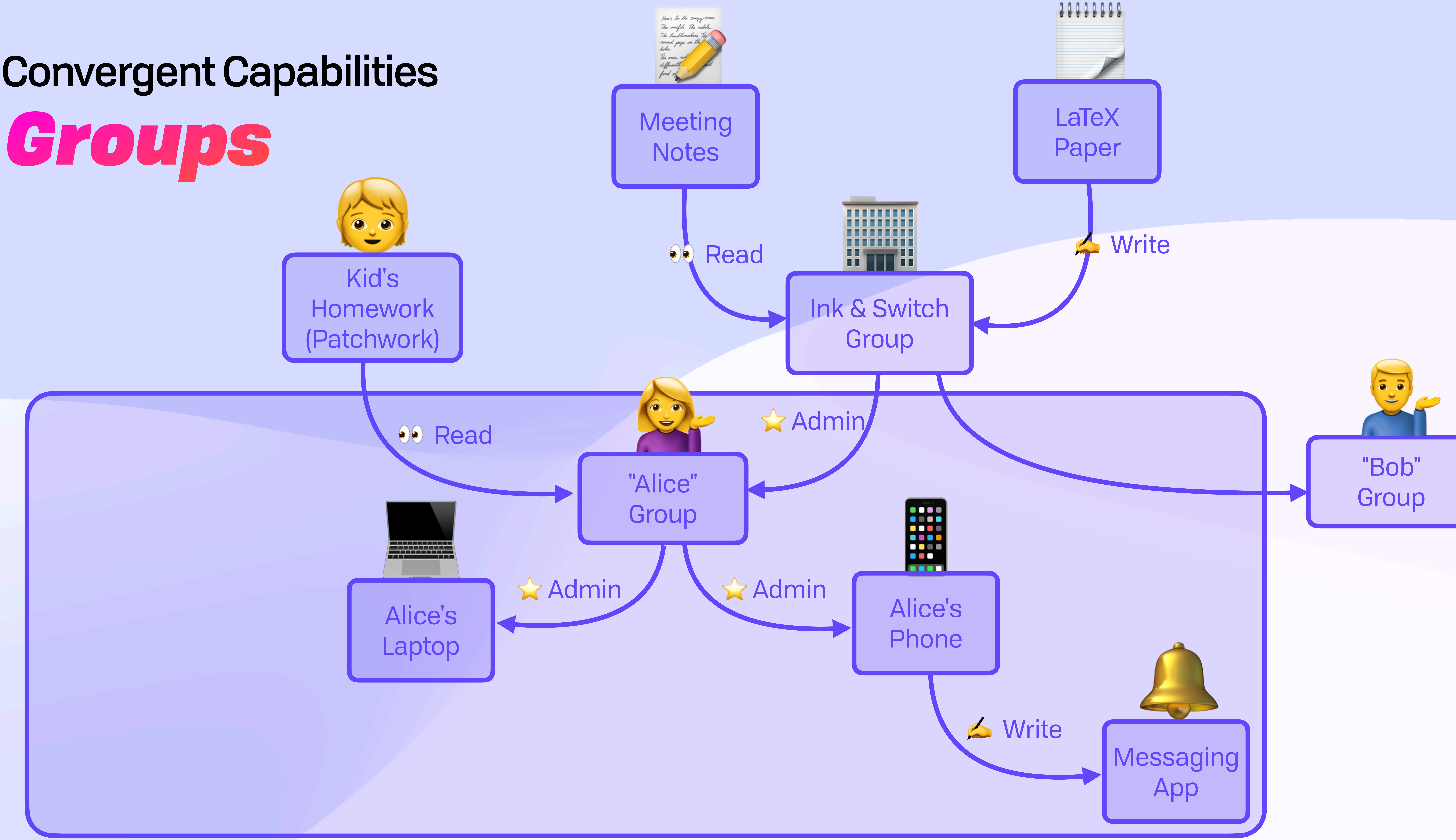
⭐ Admin

Alice's Laptop

Alice's Phone

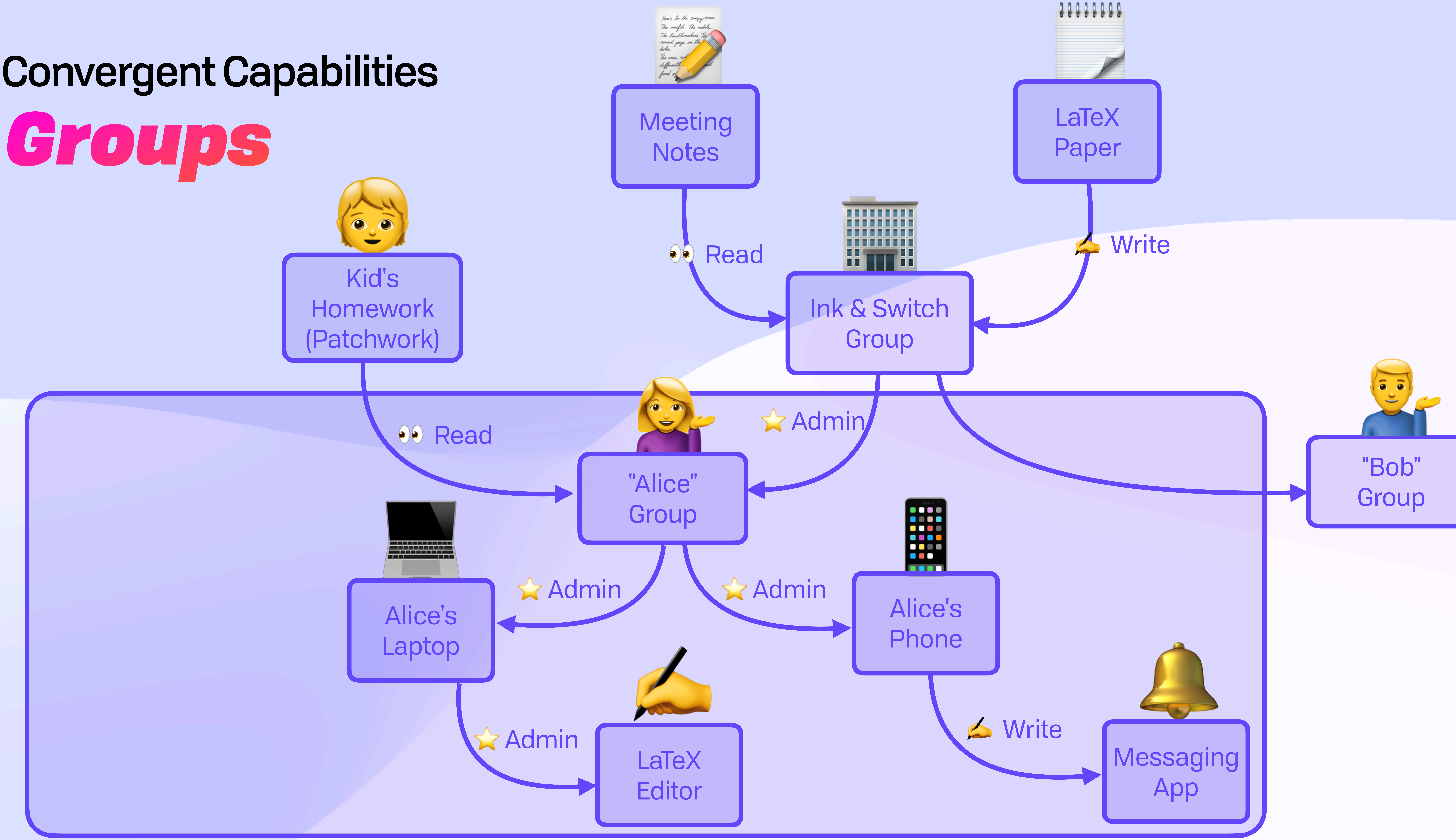
Convergent Capabilities

Groups



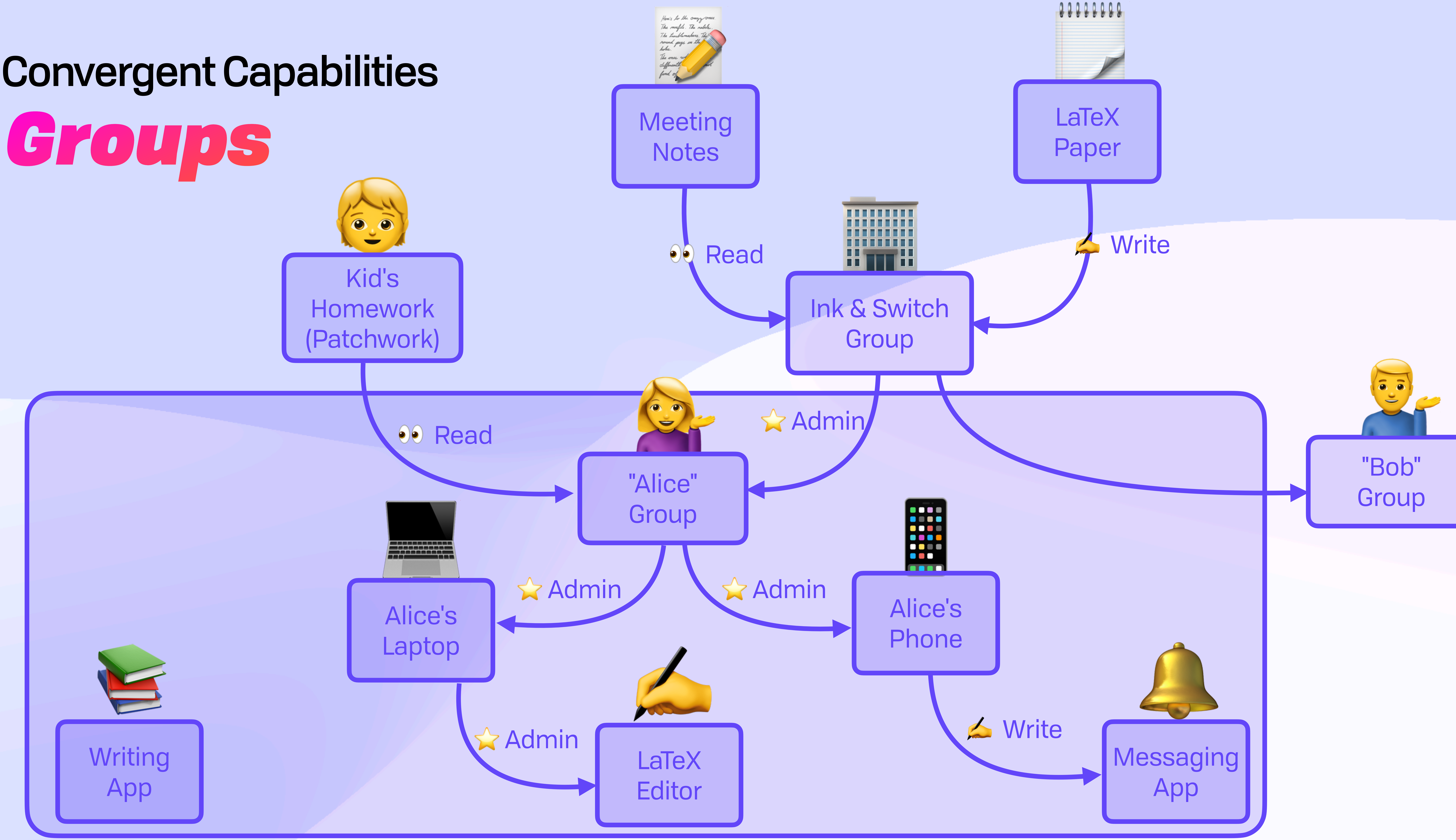
Convergent Capabilities

Groups



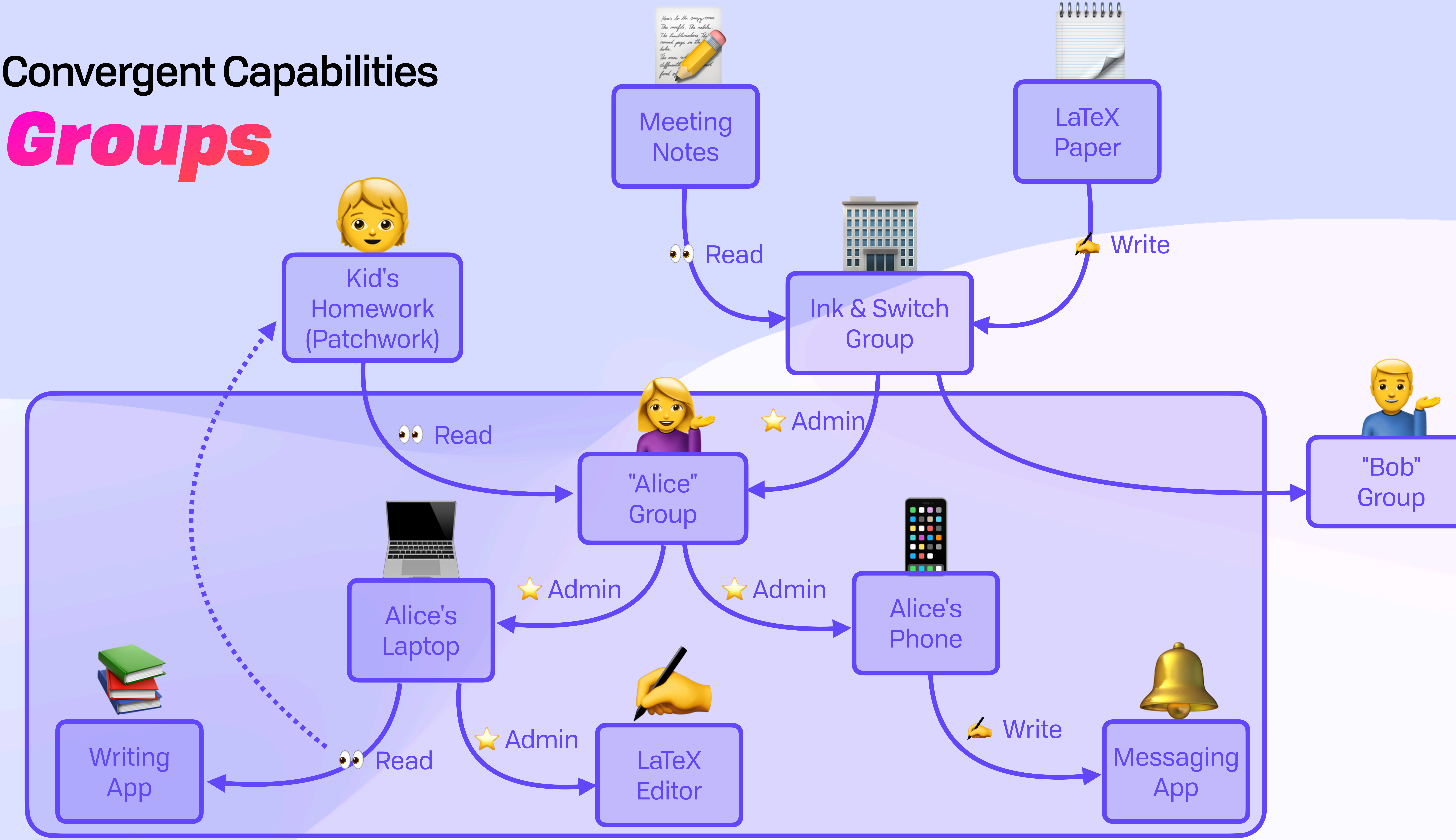
Convergent Capabilities

Groups



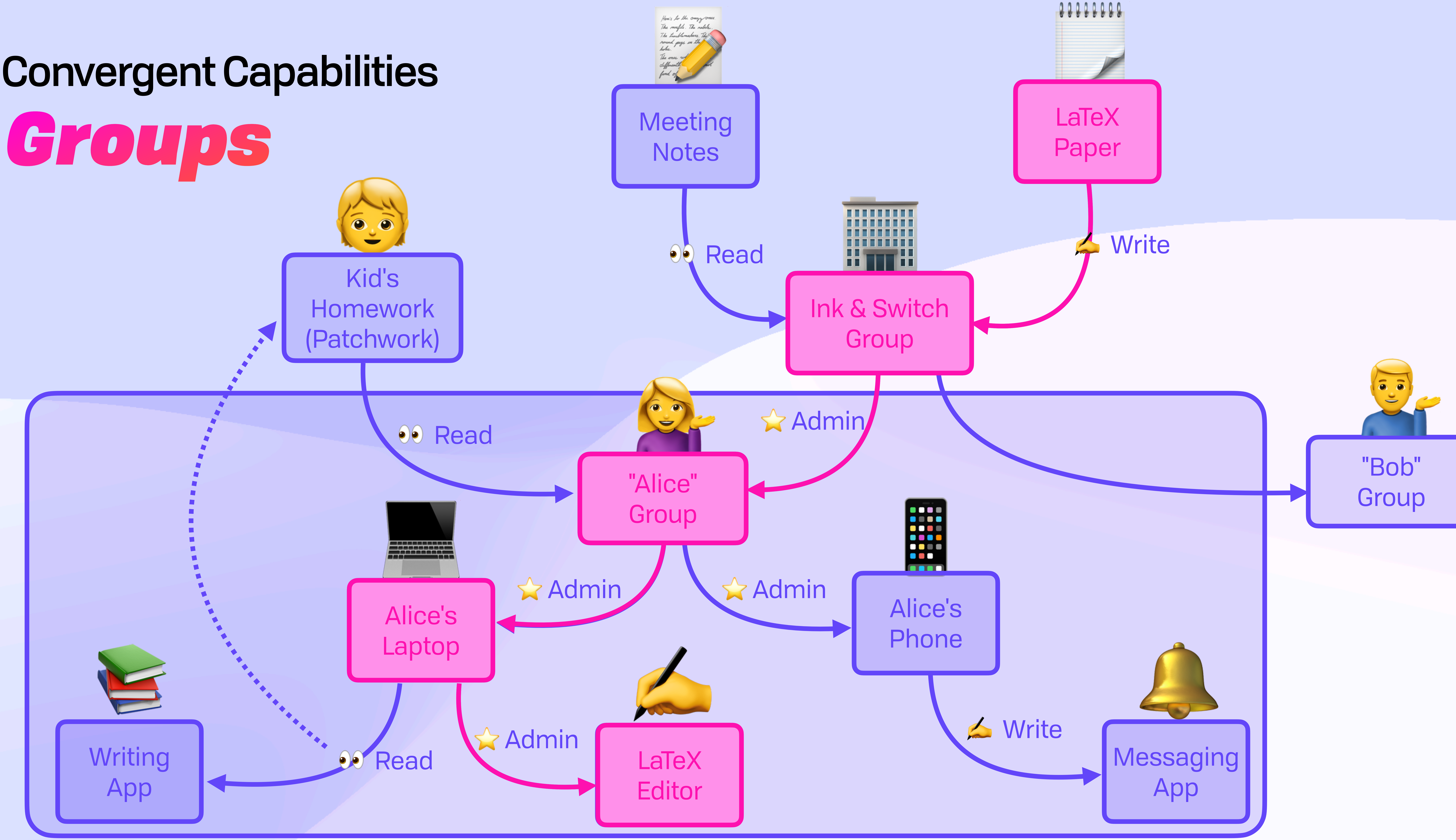
Convergent Capabilities

Groups



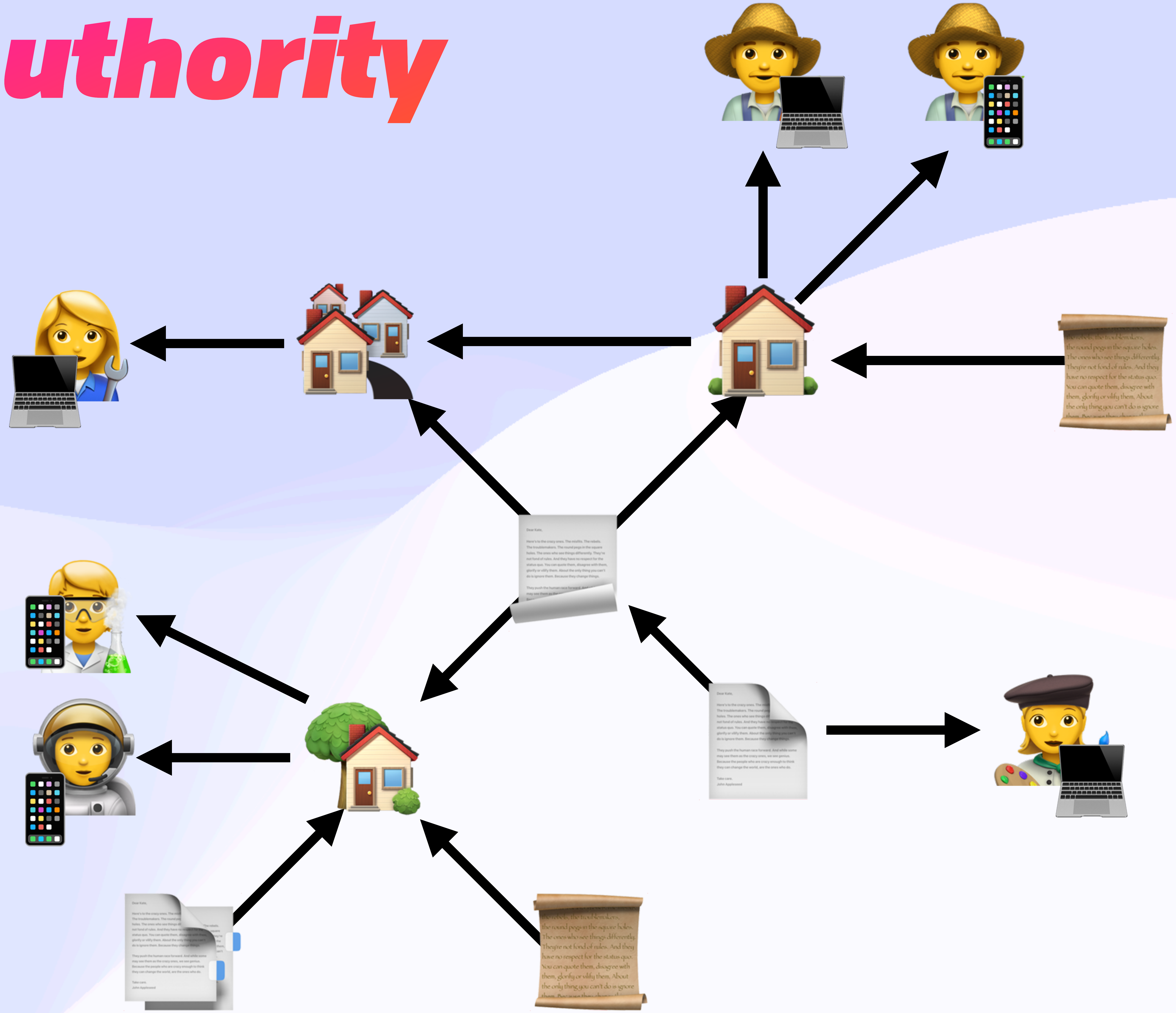
Convergent Capabilities

Groups



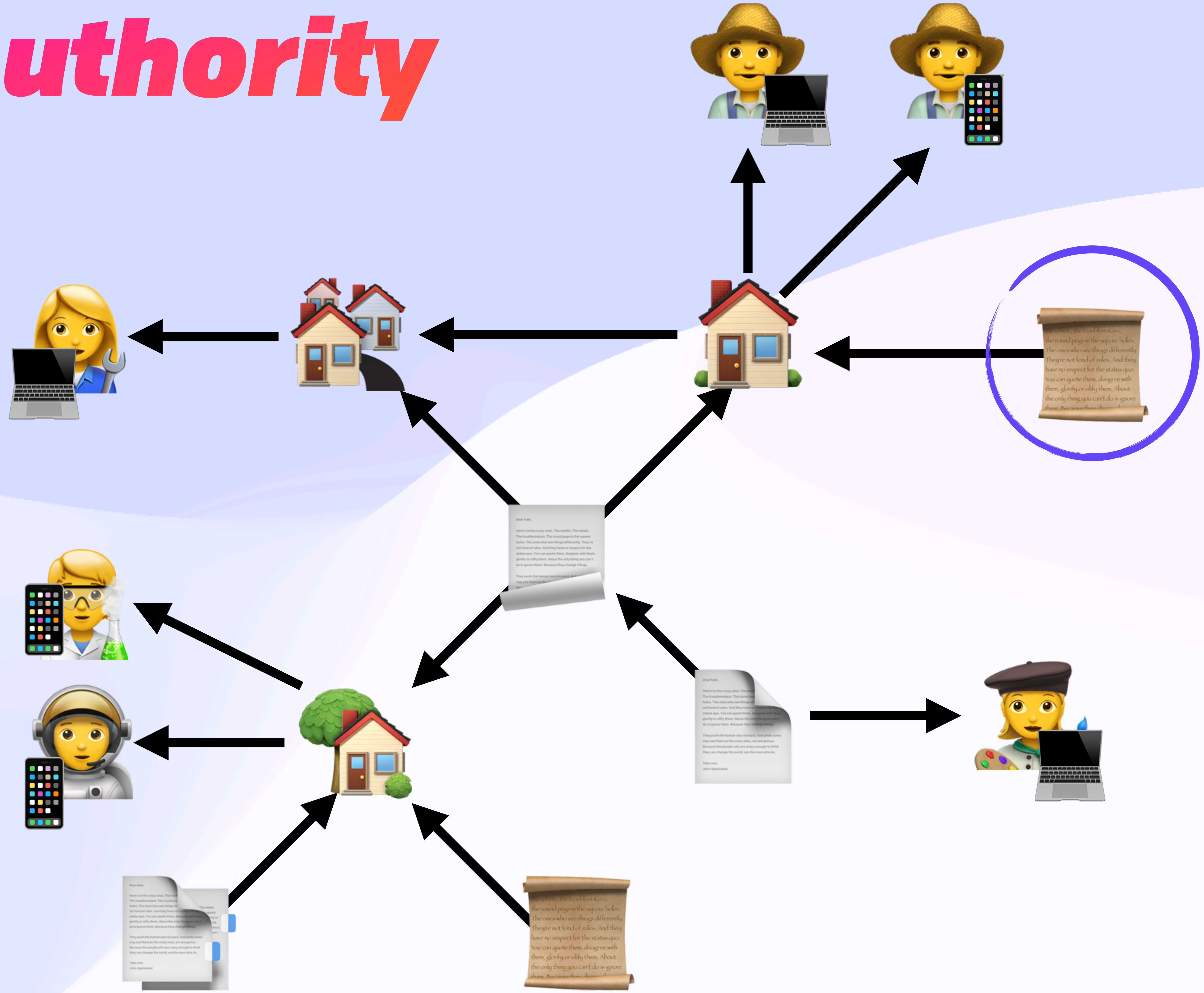
Convergent Capabilities

Flow of Authority



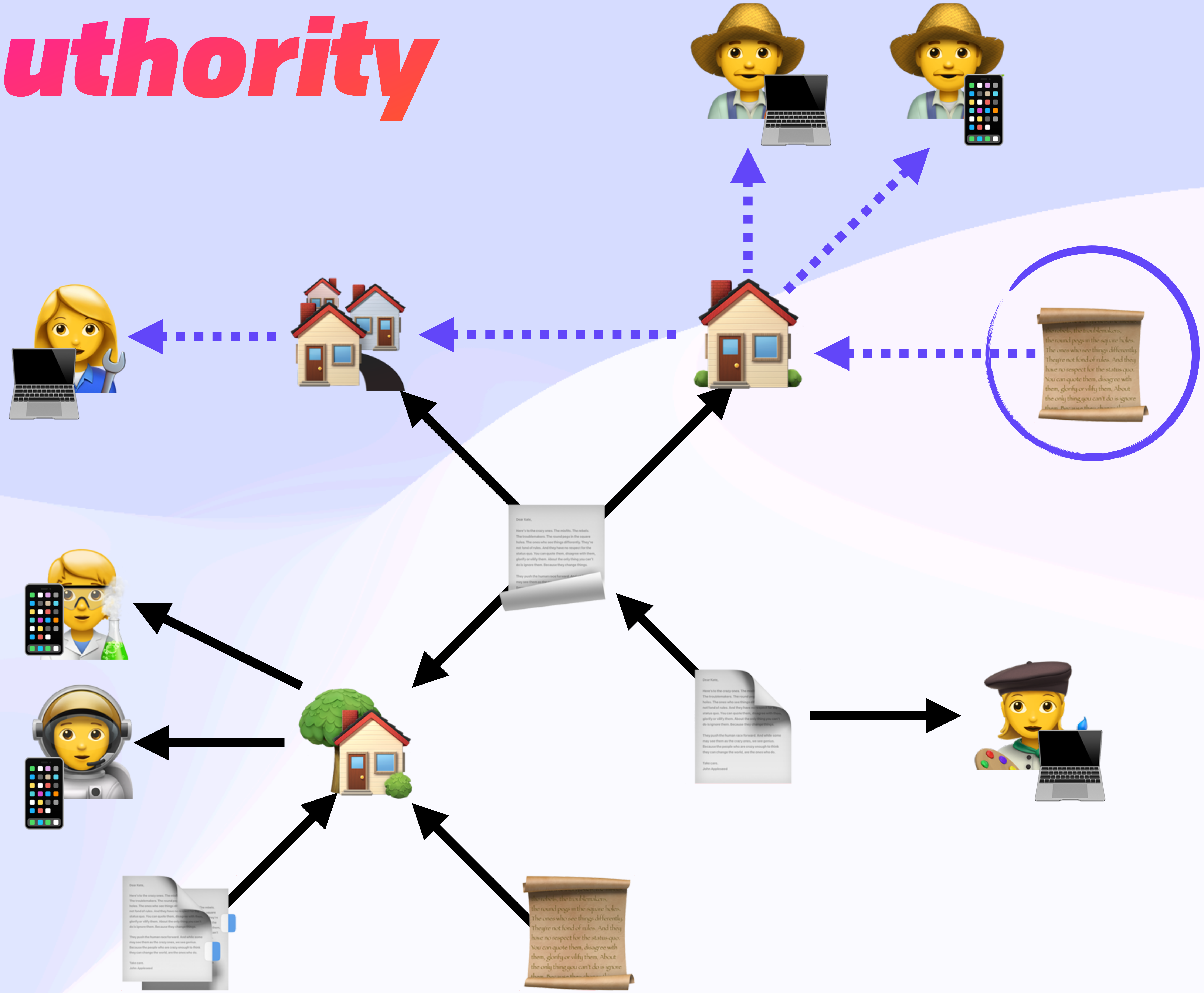
Convergent Capabilities

Flow of Authority



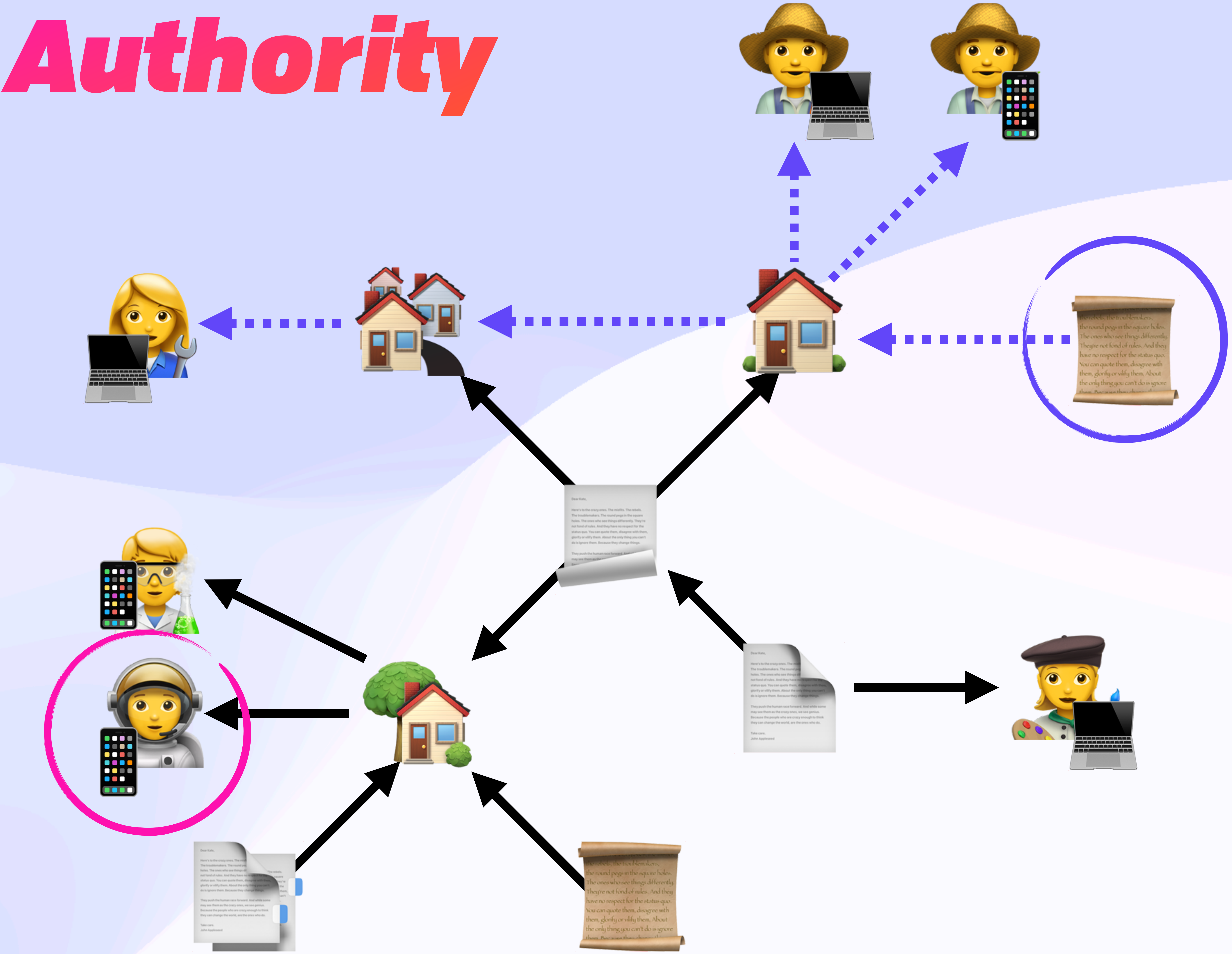
Convergent Capabilities

Flow of Authority



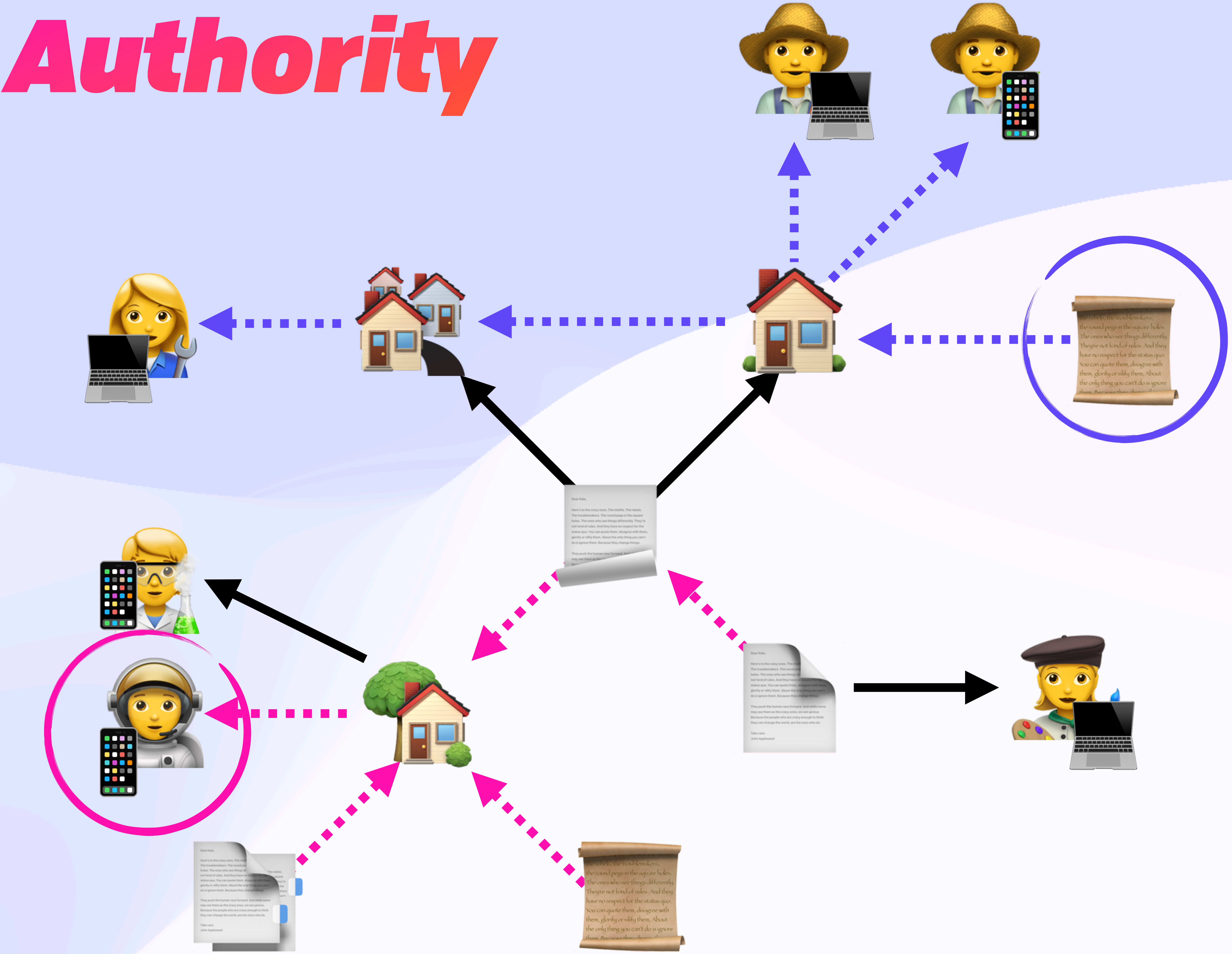
Convergent Capabilities

Flow of Authority



Convergent Capabilities

Flow of Authority



Wrap Up

🎁

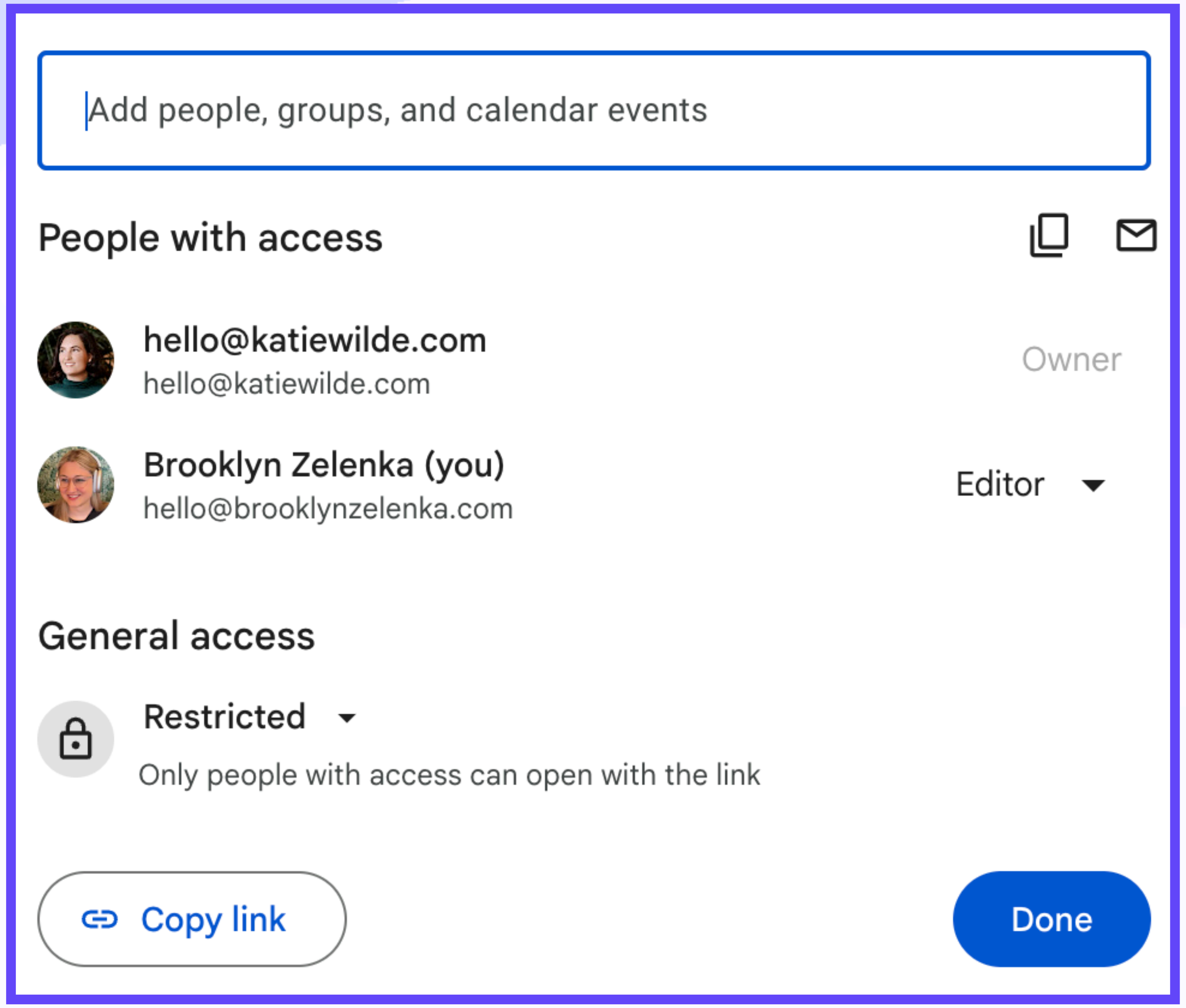
Wrap Up

But Wait, There's More!

Wrap Up

But Wait, There's More!

- Mutation Control ✍️
  - Convergent capabilities
  - Concurrent revocation
- Read Control 👀
  - End-to-end encryption
  - Causal encryption
- Further Reading 📚
  - Concurrency-friendly variant of MLS
  - Revocation & admin revocation cycle breaking



Add people, groups, and calendar events

People with access

hello@katiewilde.com
hello@katiewilde.com — Owner

Brooklyn Zelenka (you)
hello@brooklynzelenka.com — Editor

General access

Restricted
Only people with access can open with the link

🦋 @expede.wtf
🐘 @expede@types.pl
✍️ notes.brooklynzelenka.com

🎉 Thank You, Berlin 🇩🇪

🐝 inkandswitch.com/keyhive