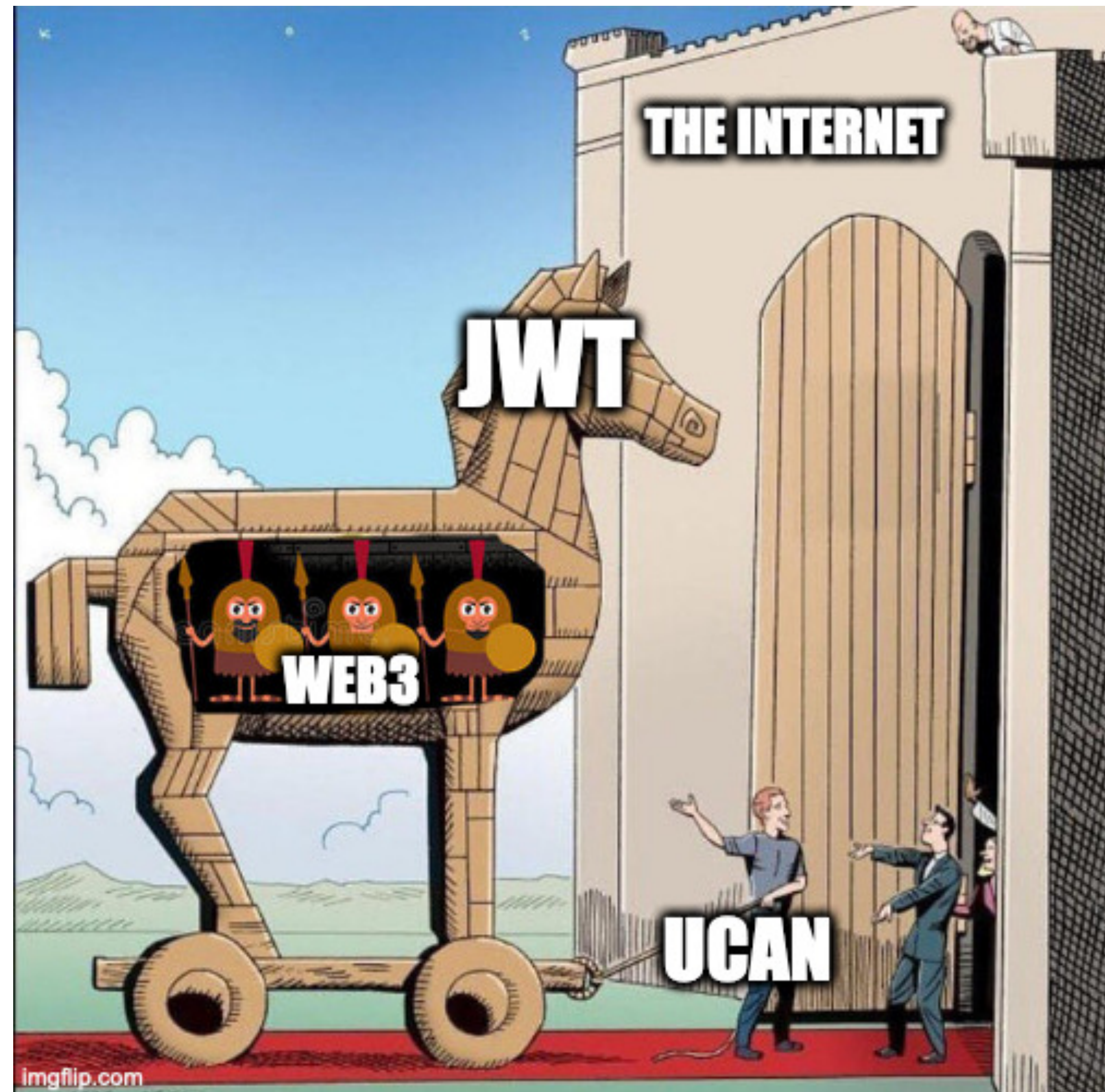


# An Intro to UCAN

Or: how to make the internet web3, from the inside out





***Every program has (at least) two purposes:*** the one for which it was written, and another for which it wasn't

Alan Perlis, Epigram #16



***Cryptography*** is a tool for turning  
lots of ***different problems*** into  
***key management problems***

Dr. Lea Kissner, Google's Global Lead of Privacy Technologies

***Brooklyn Zelenka***

**@expede**



# *Brooklyn Zelenka*

@expede

- Cofounder & CTO at Fission
  - <https://fission.codes> / @FISSIONCodes
  - Chain agnostic from the ground up!



# *Brooklyn Zelenka*

@expede

- Cofounder & CTO at Fission
  - <https://fission.codes> / @FISSIONCodes
  - Chain agnostic from the ground up!
- Editor of the UCAN spec





# *Brooklyn Zelenka*

@expede

- Cofounder & CTO at Fission
  - <https://fission.codes> / @FISSIONCodes
  - Chain agnostic from the ground up!
- Editor of the UCAN spec
- Background: PLT, VMs, Formal Methods, Distributed Systems



# *Brooklyn Zelenka*

@expede

- Cofounder & CTO at Fission
  - <https://fission.codes> / @FISSIONCodes
  - Chain agnostic from the ground up!
- Editor of the UCAN spec
- Background: PLT, VMs, Formal Methods, Distributed Systems
- Meetups: VanFP, Code & Coffee, Distributed Systems Reading Group



# Brooklyn Zelenka

@expede

- Cofounder & CTO at Fission
  - <https://fission.codes> / @FISSIONCodes
  - Chain agnostic from the ground up!
- Editor of the UCAN spec
- Background: PLT, VMs, Formal Methods, Distributed Systems
- Meetups: VanFP, Code & Coffee, Distributed Systems Reading Group



<https://lu.ma/distributed-systems>

Meta

# *Wherefore Art Thou UCAN?*



Meta

*Wherefore Art Thou UCAN?*

***DIDs** say who **you are***



Meta

# *Wherefore Art Thou UCAN?*

***DIDs*** say who ***you are***  
***UCANs*** show what ***you can do***

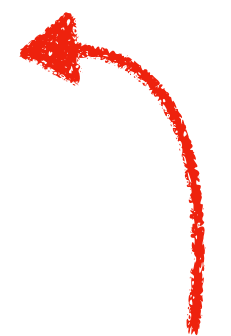


Meta

# *Wherefore Art Thou UCAN?*

***DIDs*** say who ***you are***  
***UCANs*** show what ***you can do***

AuthN



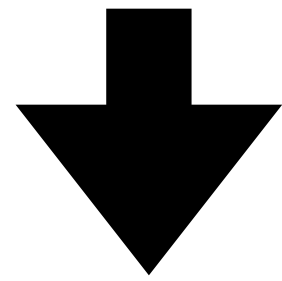
AuthZ



Meta

# Teaser Token

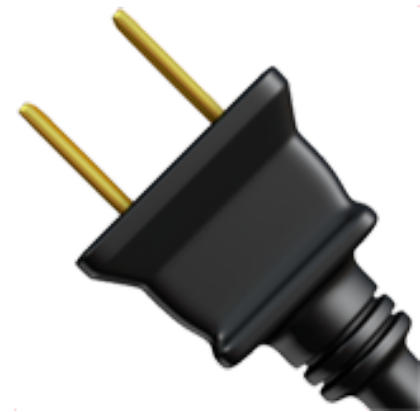
```
eyJhbGciOiJIJZERTQSIiInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V50no2TWtzWFFCZkw4b3d6dFRDSlRtN2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiaWF0IjoiT1ZFUldSSVRFIn1dLCJleHAiOi0jkyNTY5Mzk1MDUsImZcyI6ImRpZDprZXk6ejZNa3A1RXN60XMyTUhzcVl2TG9jY3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjoxNjM5NjA4MjczLCJwcmYiOi0ldfQ.MgYarLqy7RmQ1AIrqYL6cFy9z7a5WIAU--TYARPSgir0Sszvar3_DNr25rbPretHbnT0mMVKyoaQXruR7KbrBg
```



```
{
  "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99",
  "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
  "exp": 9256939505,
  "nbf": 1639608293,
  "att": [
    {
      "with": "wnfs://demouser.fission.name/public/notes/",
      "can": "OVERWRITE"
    }
  ]
}
```



# ***How to Power a New Internet***



# How to Power a New Internet

How to Power a New Internet 

***web3***  $\supsetneq$  ***Blockchain***

# How to Power a New Internet

**web3**  $\supsetneq$  **Blockchain**

P2P, IPFS, Matrix

# How to Power a New Internet

***web3***  $\supsetneq$  ***Blockchain***

P2P, IPFS, Matrix

Open, accessible, trustless, portable

# How to Power a New Internet

**web3**  $\supsetneq$  **Blockchain**

P2P, IPFS, Matrix

Open, accessible, trustless, portable

User sovereignty: mobile browsers, local-first

# How to Power a New Internet

**web3**  $\supsetneq$  **Blockchain**

P2P, IPFS, Matrix

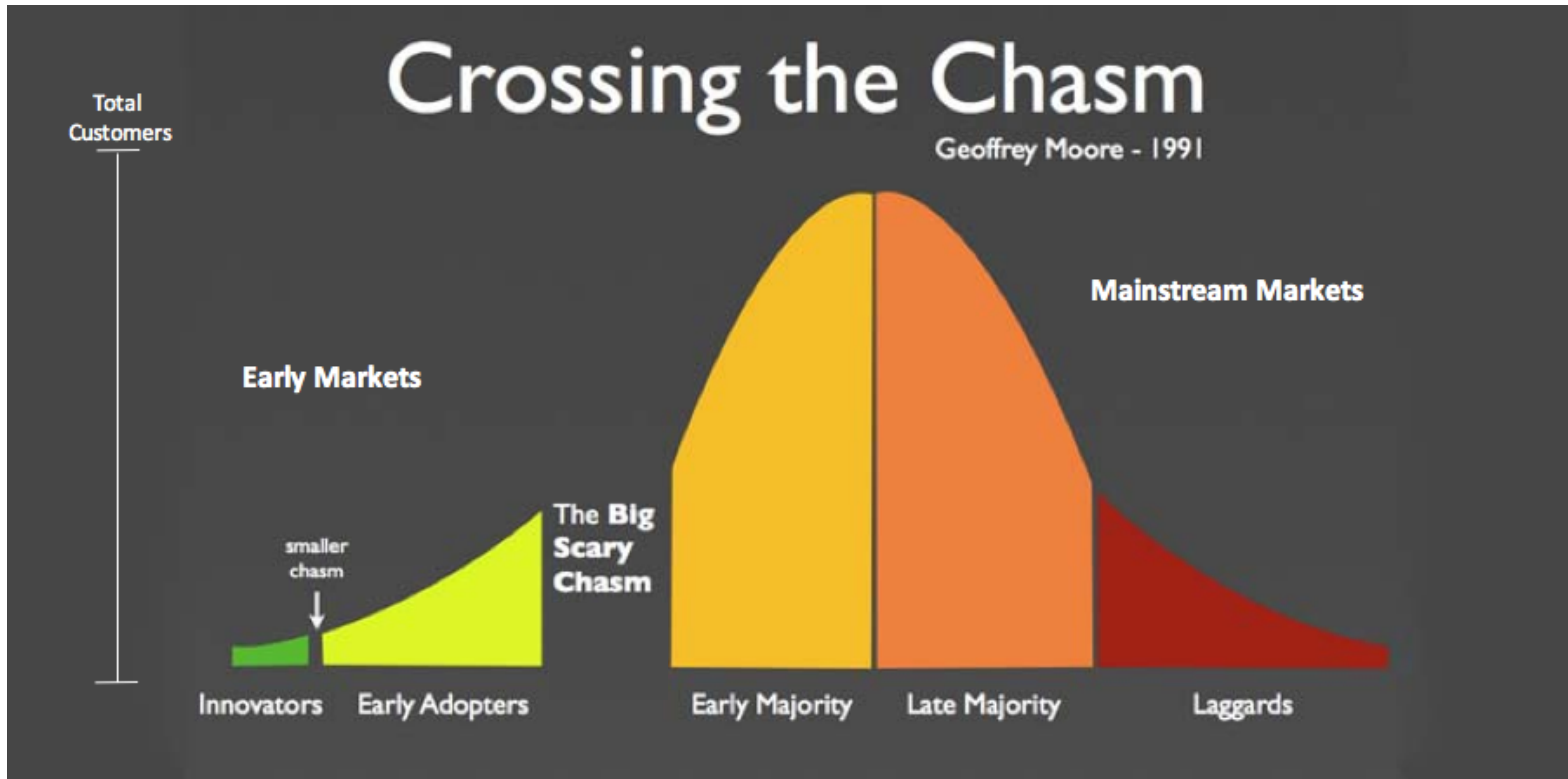
Open, accessible, trustless, portable

User sovereignty: mobile browsers, local-first

...and so on

How to Power a New Internet 🌐

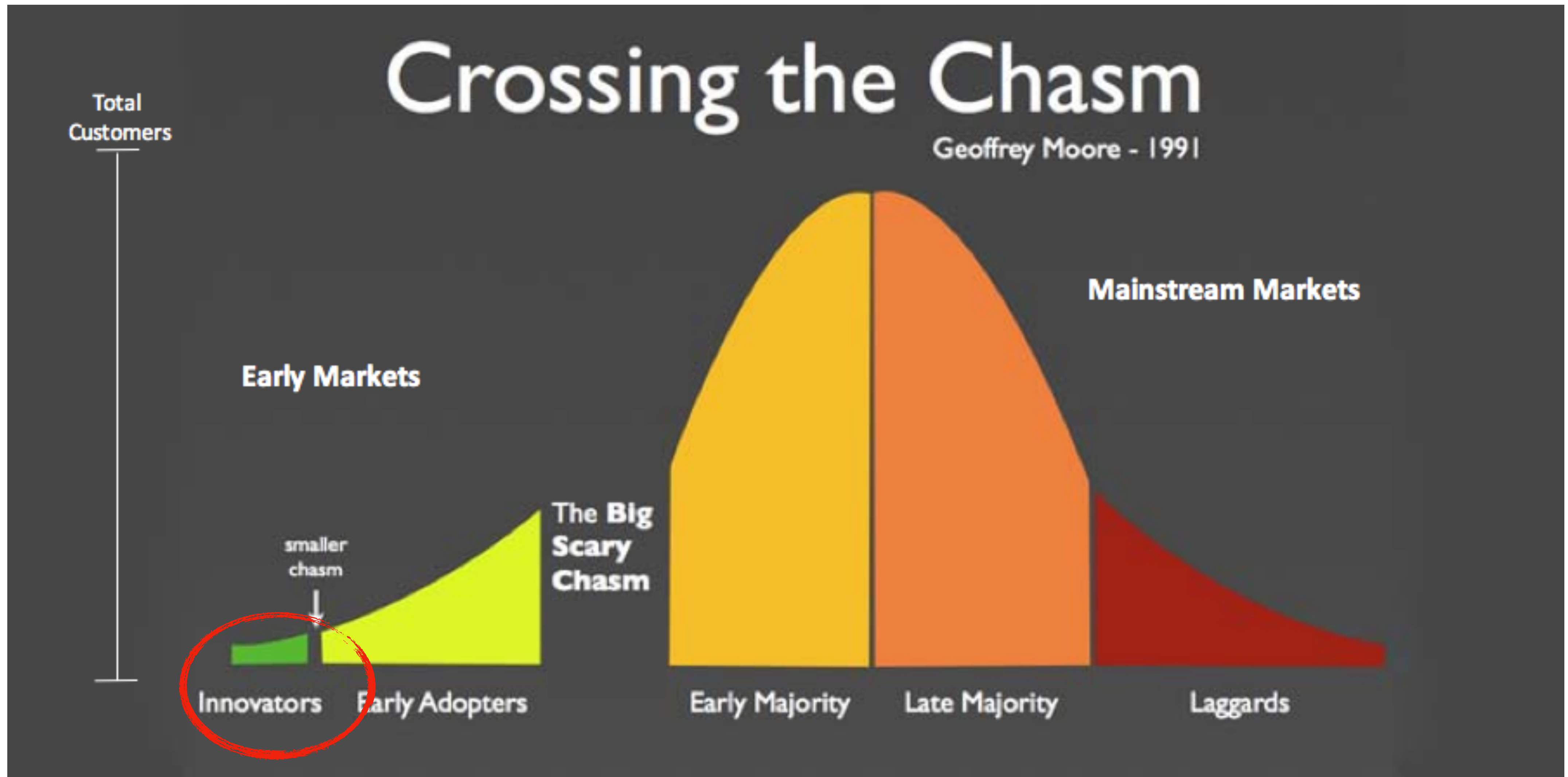
*It's Still Extremely Early Days!*





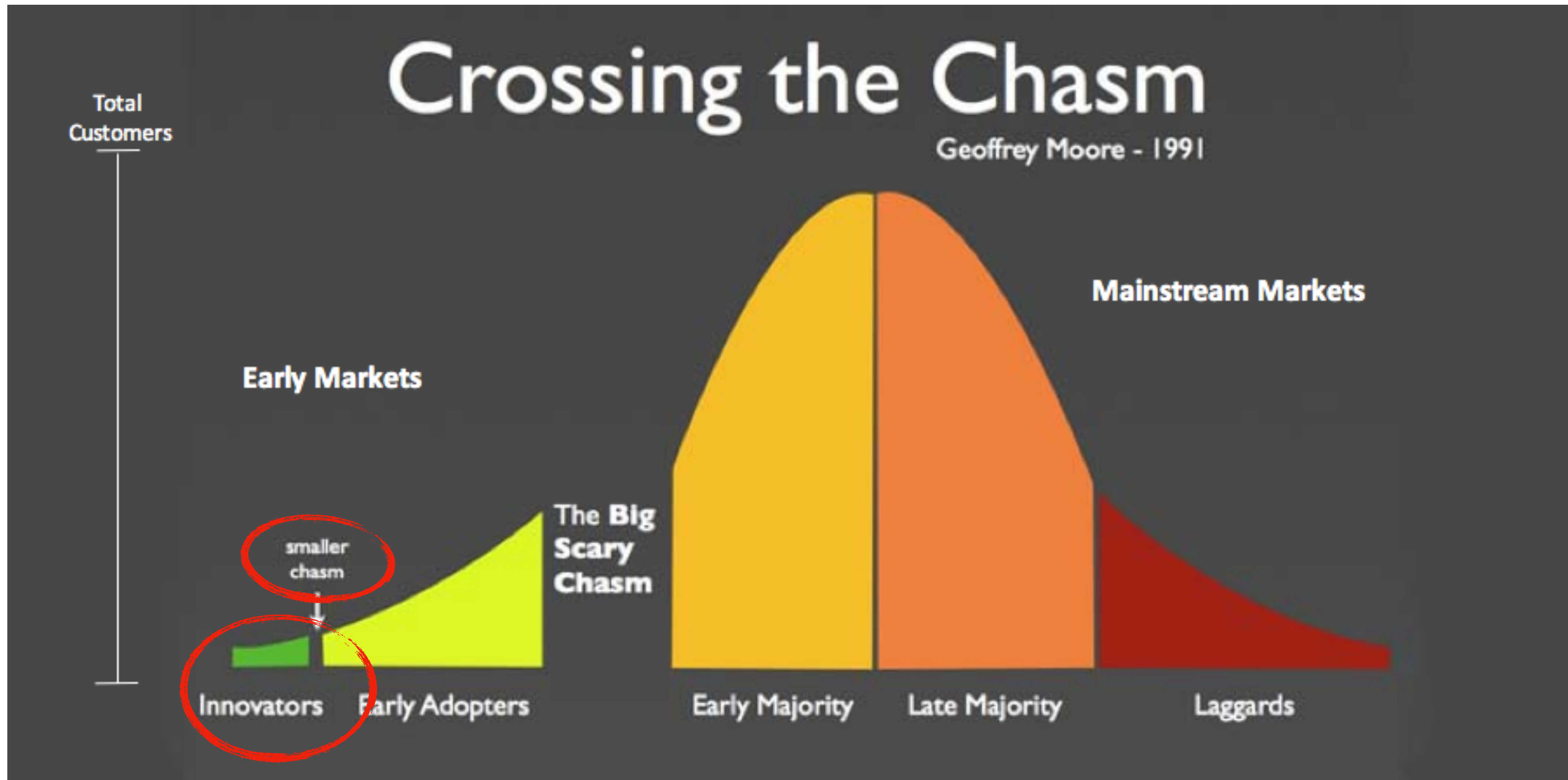
How to Power a New Internet 🌐

*It's Still Extremely Early Days!*



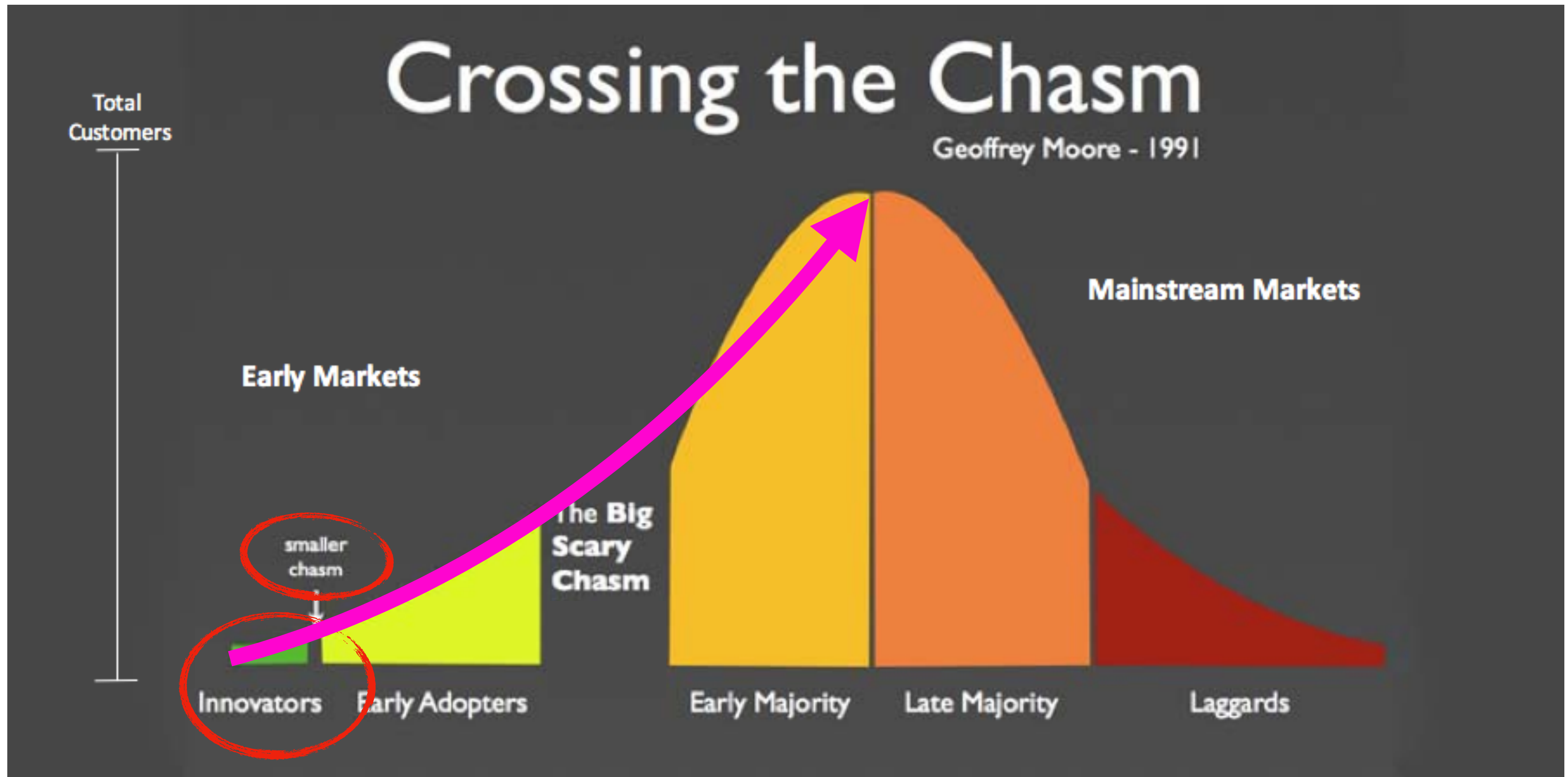
How to Power a New Internet 🌐

*It's Still Extremely Early Days!*



How to Power a New Internet 🌐

*It's Still Extremely Early Days!*



How to Power a New Internet 

*User Problems*

How to Power a New Internet 

# *User Problems*

Dapp UX is **too hard** for many users

How to Power a New Internet 

*Dev Problems*

How to Power a New Internet 

## *Dev Problems*

Too many (d)apps are ***centralized(!)***

How to Power a New Internet 

*Move the Needle*



How to Power a New Internet 

*Move the Needle*

***Realpolitik***

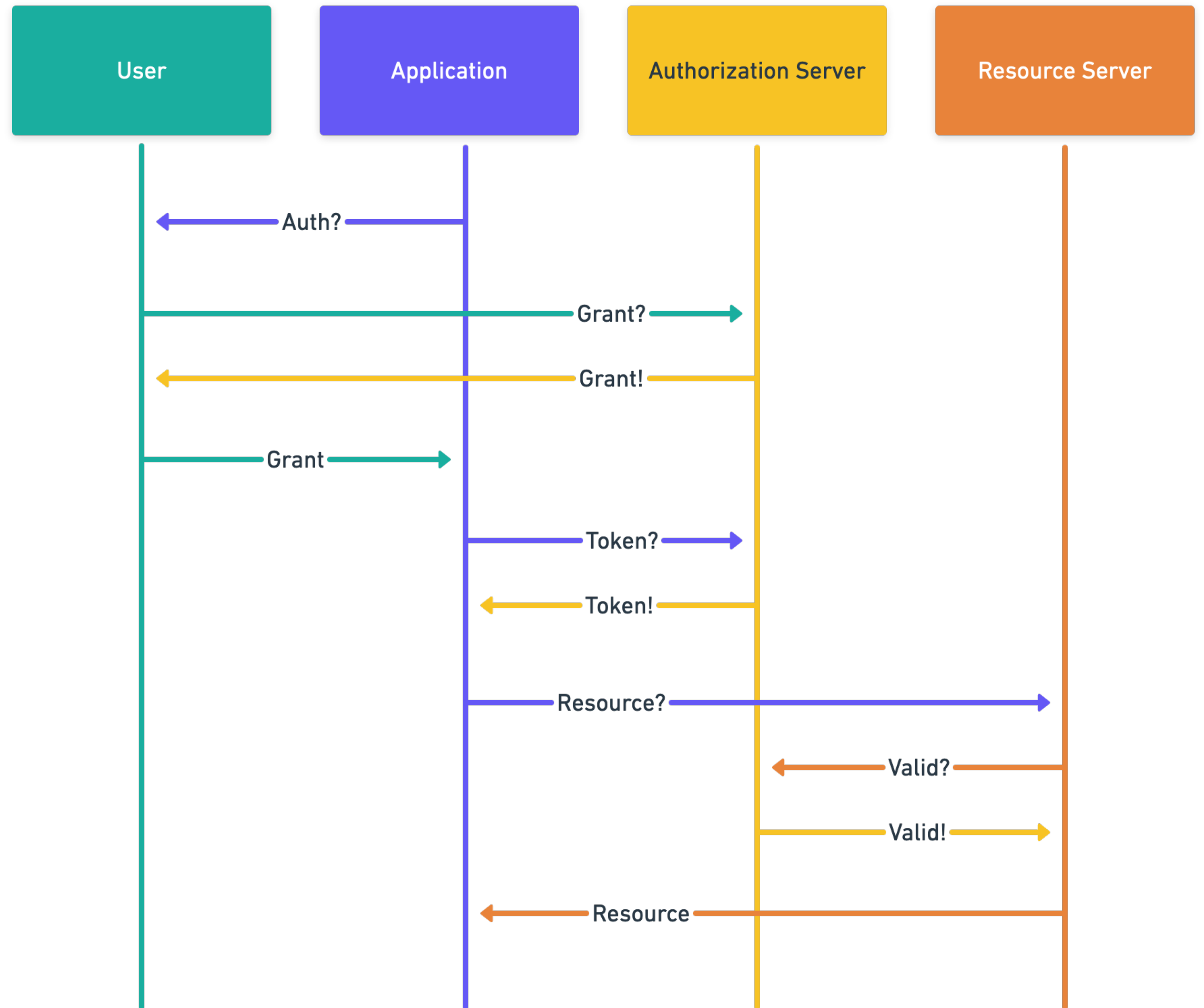
Easier, more secure, & more open than:

OAuth, X.509, SAML,

MetaMask, WalletConnect, etc

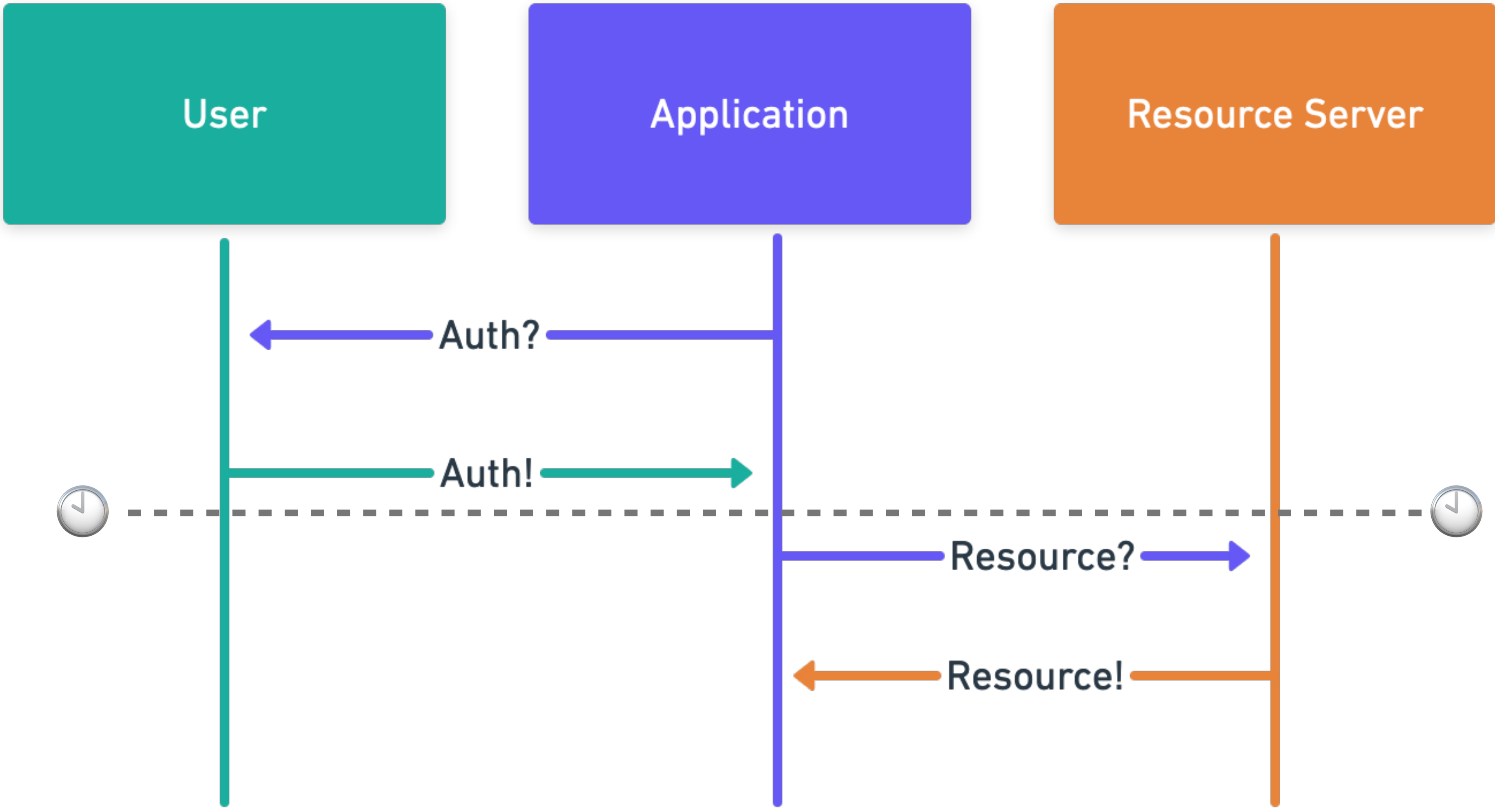
# How to Power a New Internet

## *OAuth Sequence*



# How to Power a New Internet 🌐

## *UCAN Sequence*



# ***Design Principles***



Design Principles 

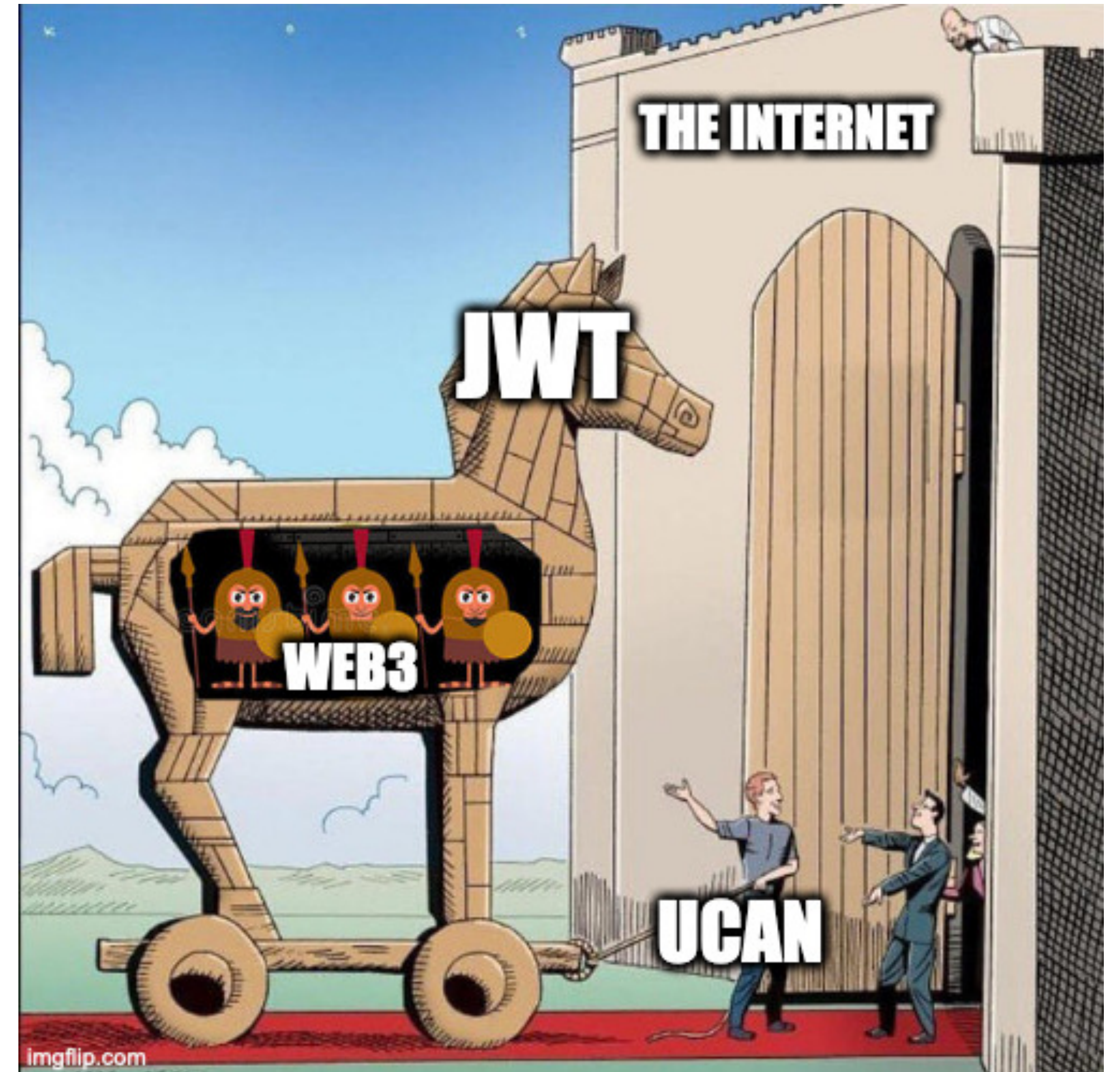
*Adoption*

Design Principles 

# *Adoption*

## *Be a Trojan Horse*

Build on widely supported, familiar, well-understood standards



Design Principles 

*Adoption*

Design Principles 

*Adoption*

***Convenience*** > ideology



Design Principles 

*Adoption*

Design Principles 

# *Adoption*

## ***Play Nice with Others***

Plug into existing tools

Bridge to other standards

Integrate with other systems

**User Controlled, Local-First, Universal Auth**

***UCAN***



UCAN

# *Non-Extractable Browser Keys*

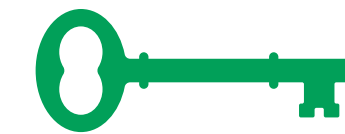
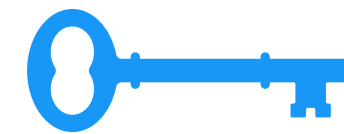
UCAN

# *Non-Extractable Browser Keys*



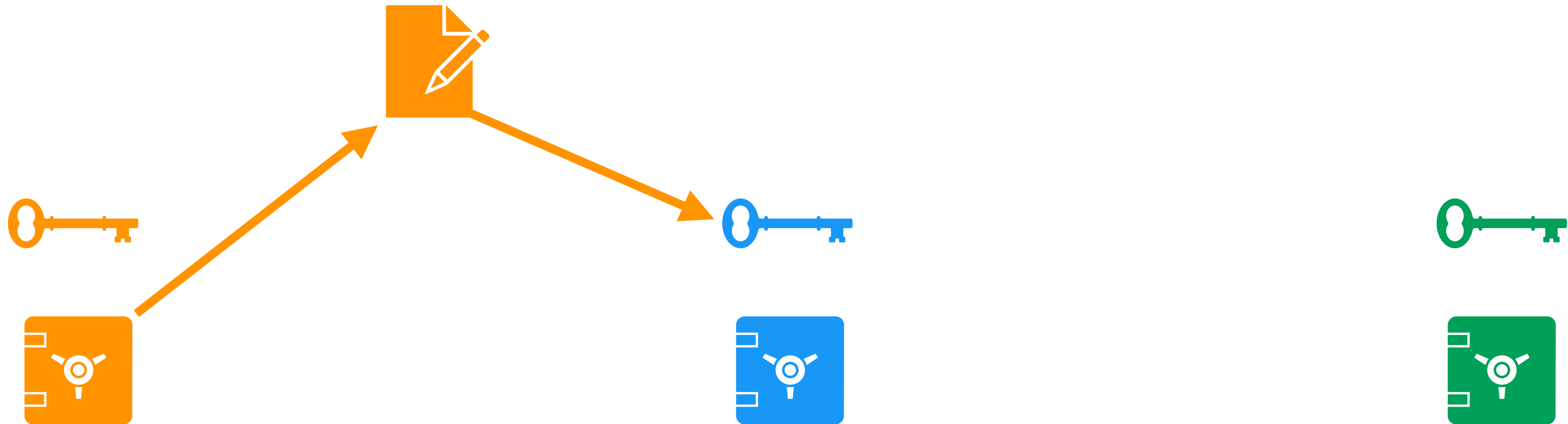
UCAN

# *Non-Extractable Browser Keys*



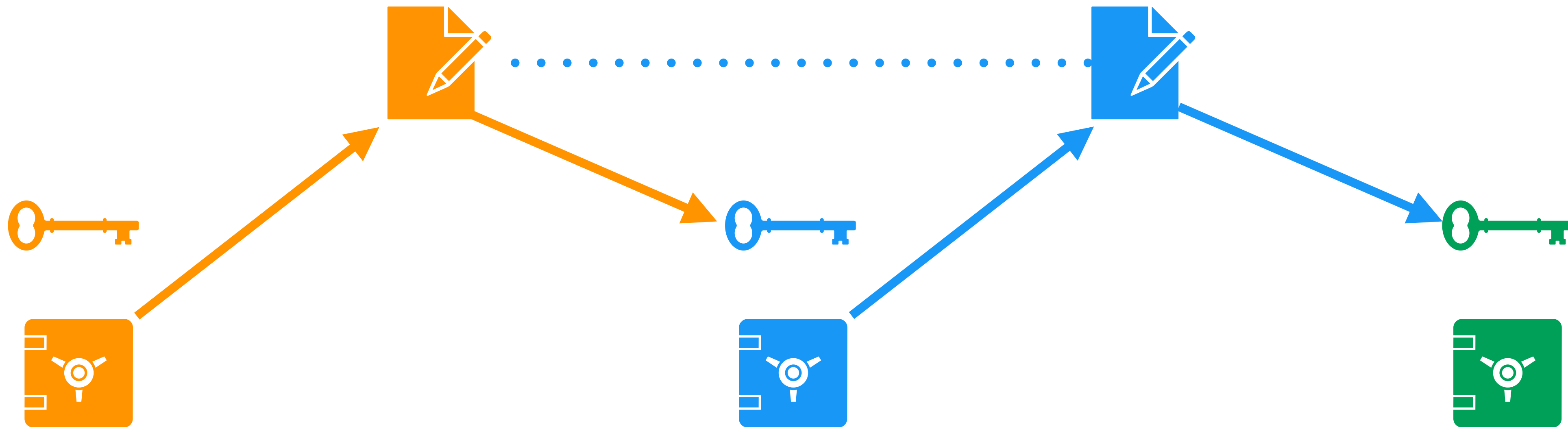
UCAN

# *Non-Extractable Browser Keys*



UCAN

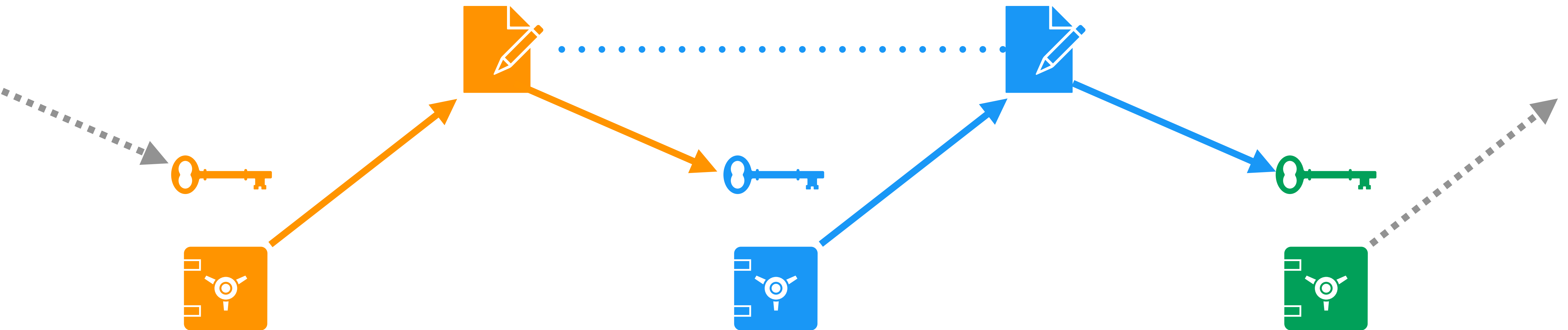
# *Non-Extractable Browser Keys*





UCAN

# *Non-Extractable Browser Keys*

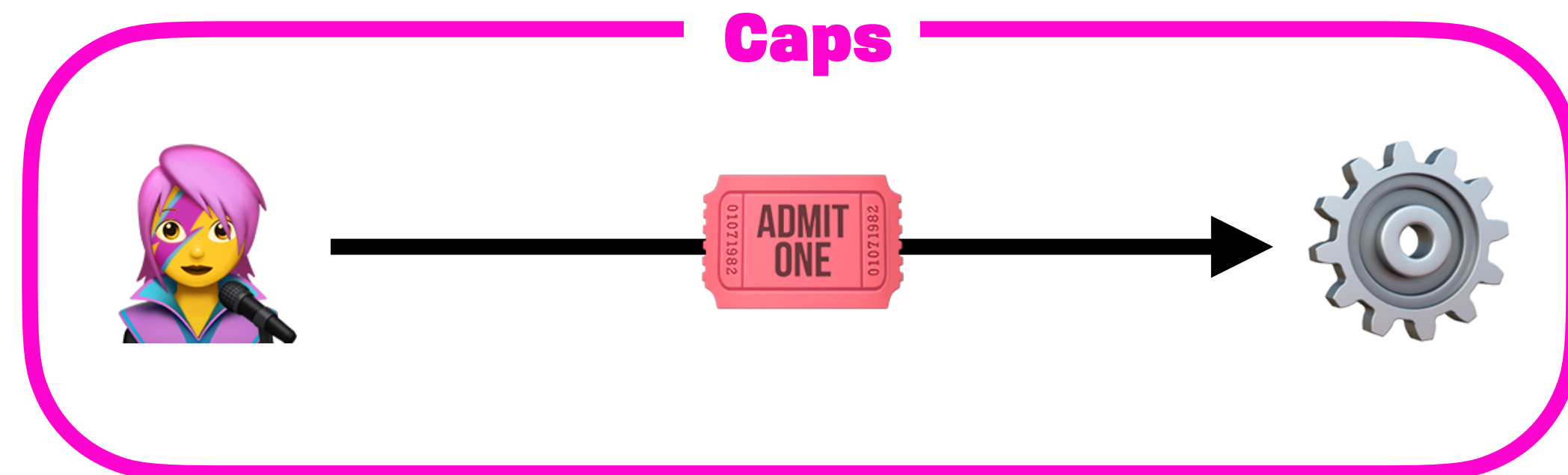
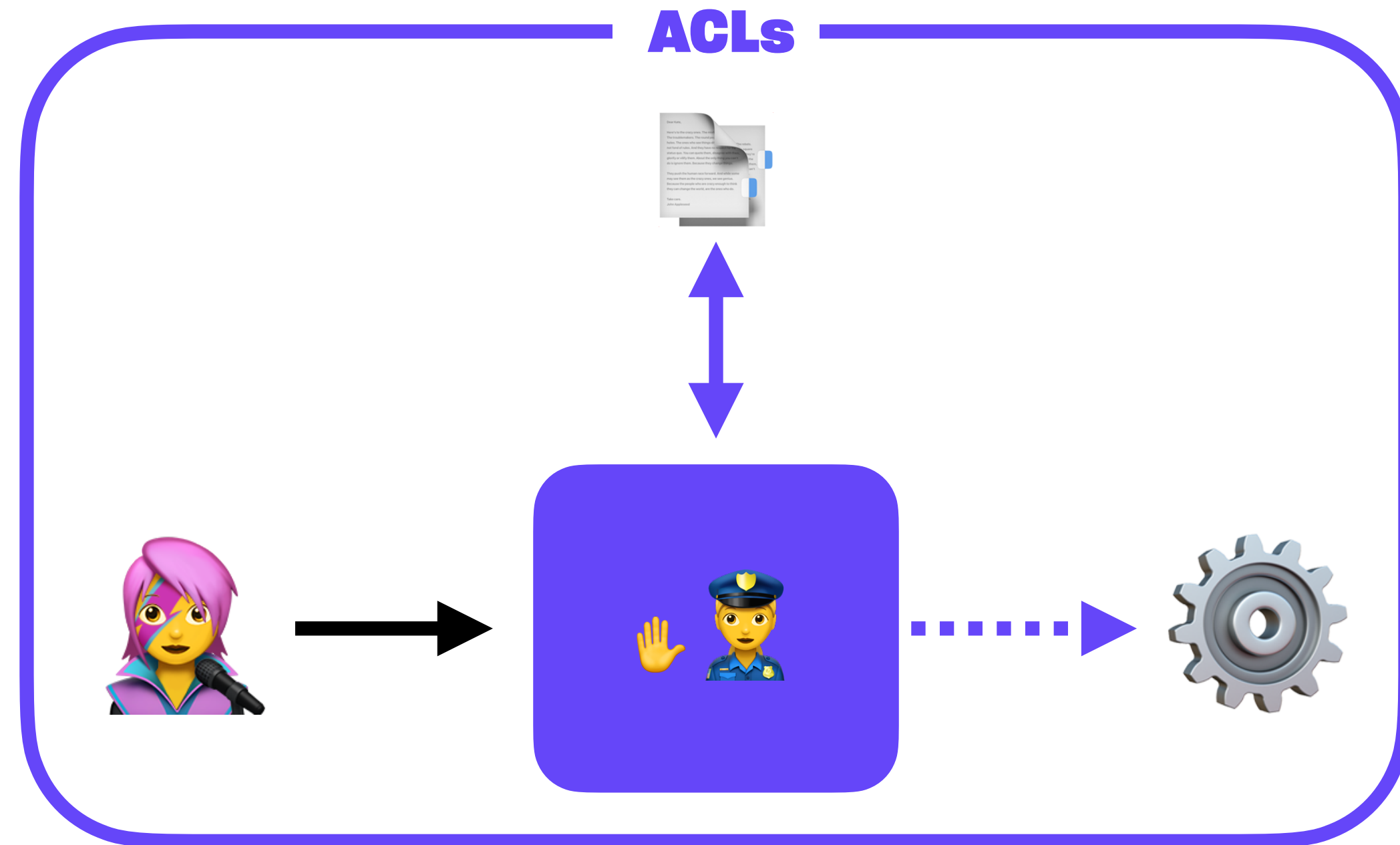


UCAN

# *Auth Models*

UCAN

# *Auth Models*



UCAN

*ACL Read & Write*

UCAN

# *ACL Read & Write*



UCAN

# *ACL Read & Write*



UCAN

# *ACL Read & Write*



UCAN

# *ACL Read & Write*





UCAN

# ACL Read & Write



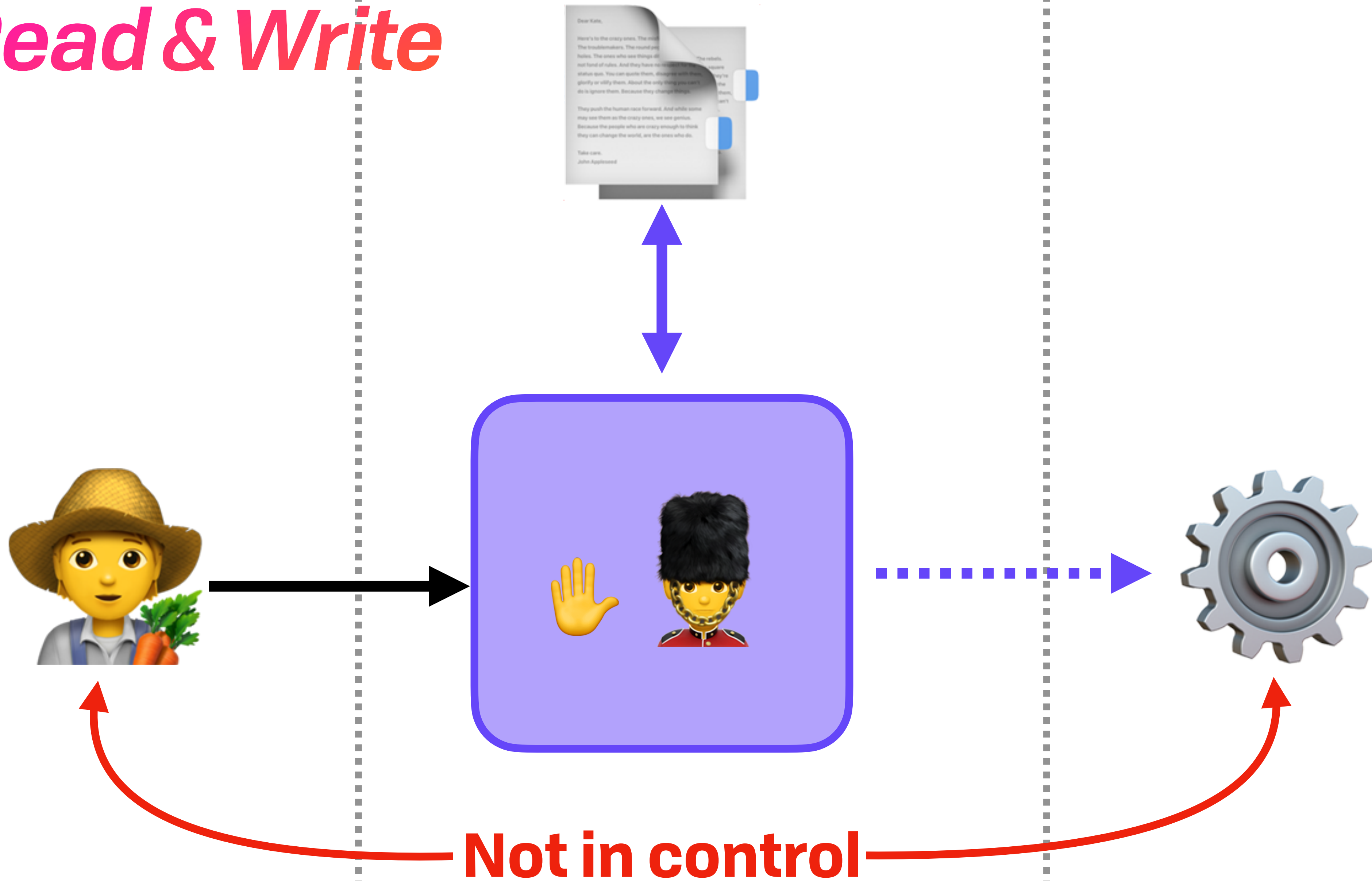
UCAN

# *ACL Read & Write*



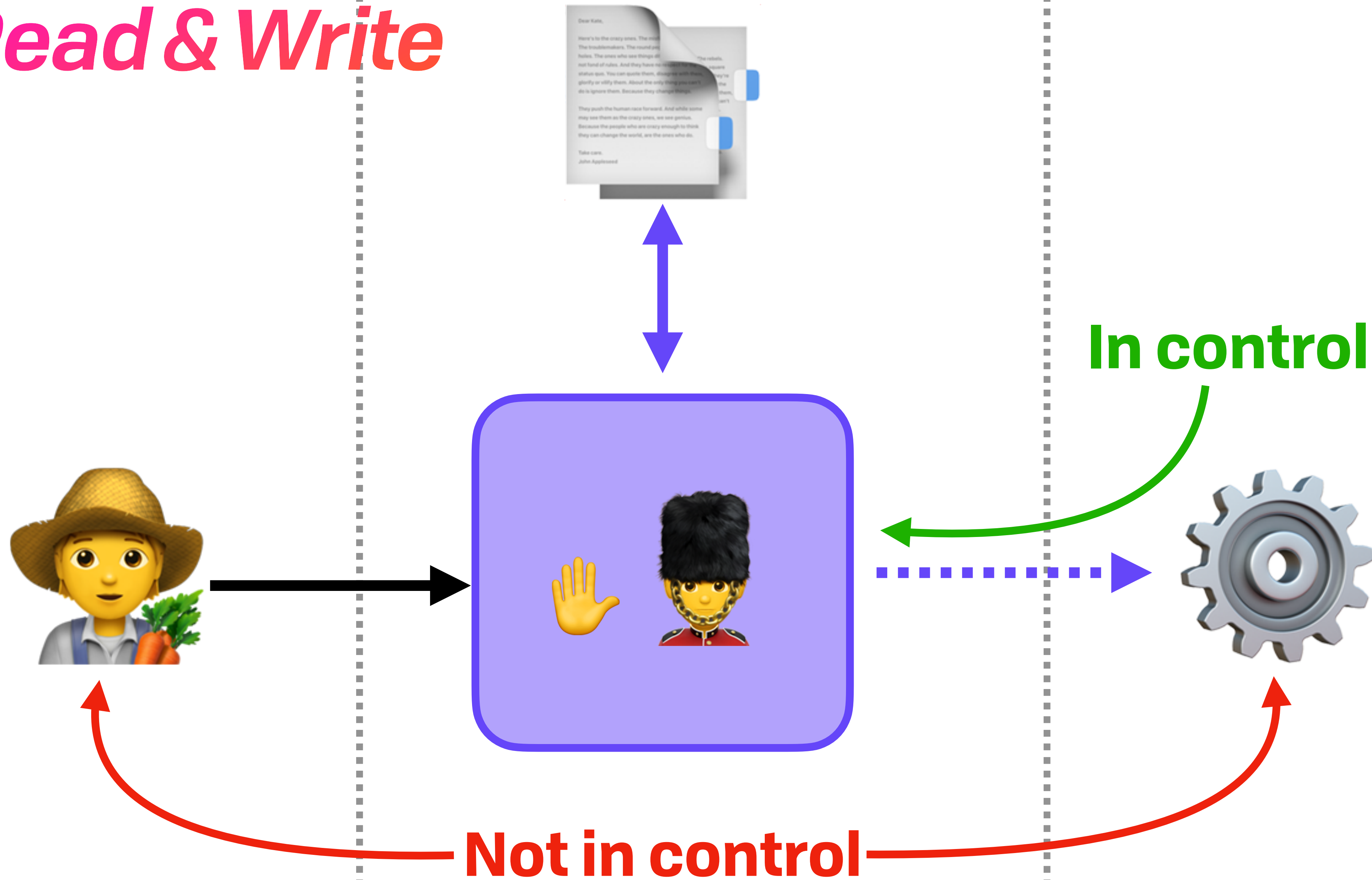
UCAN

# ACL Read & Write



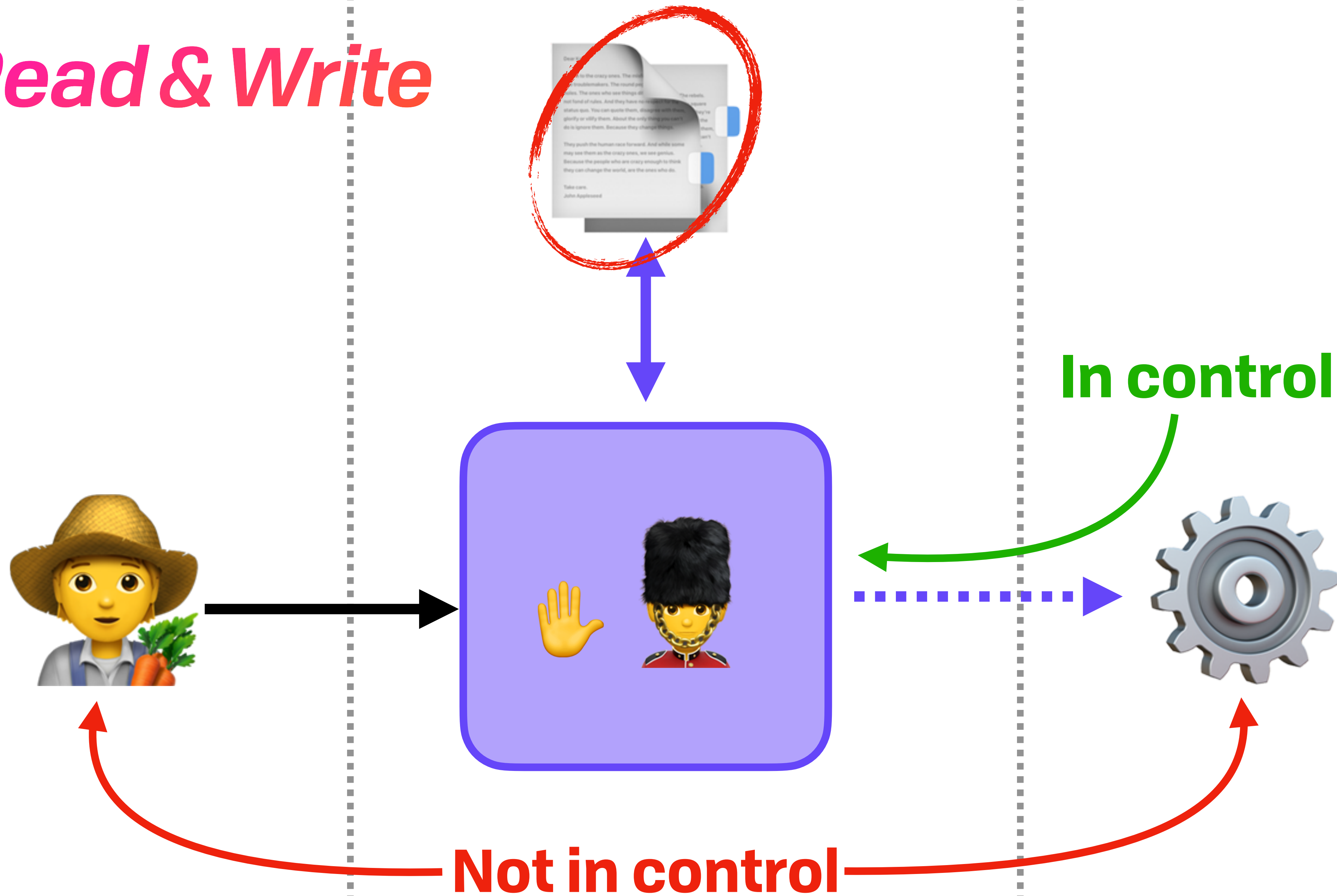
UCAN

# ACL Read & Write



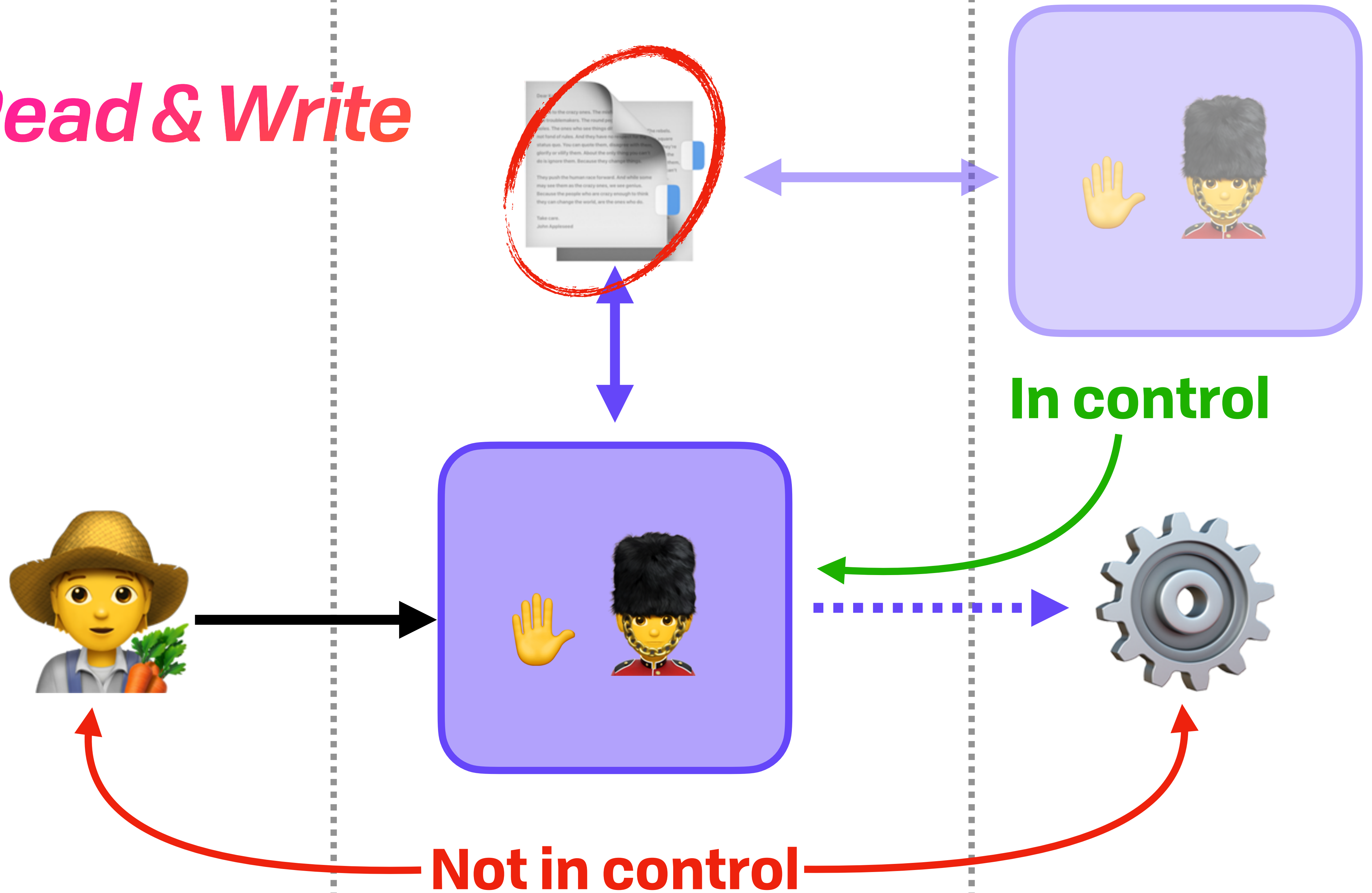
UCAN

# ACL Read & Write



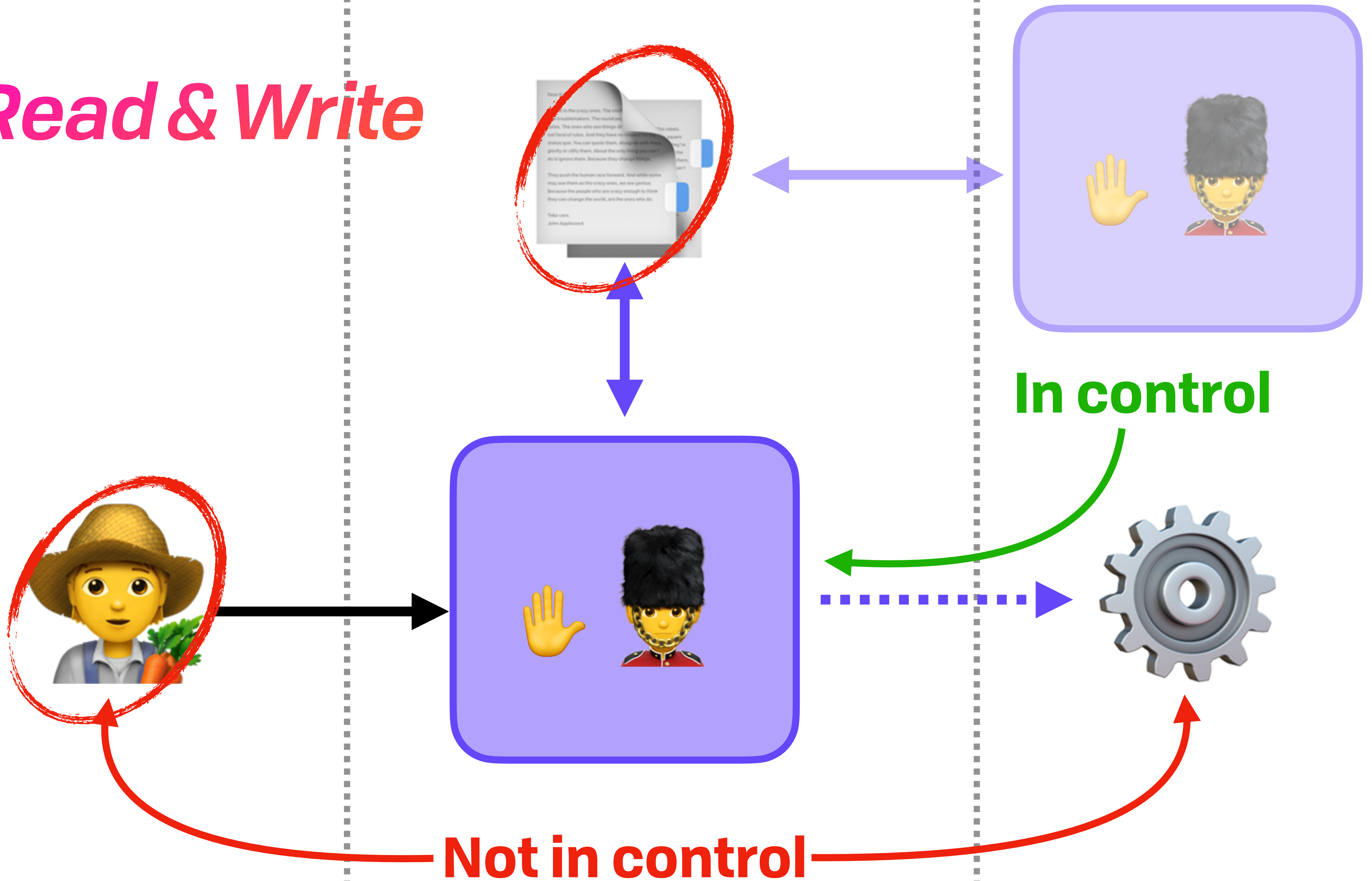
UCAN

# ACL Read & Write



UCAN

# ACL Read & Write



UCAN

# *From Actors to Capabilities*



UCAN

# *From Actors to Capabilities*



UCAN

# *From Actors to Capabilities*



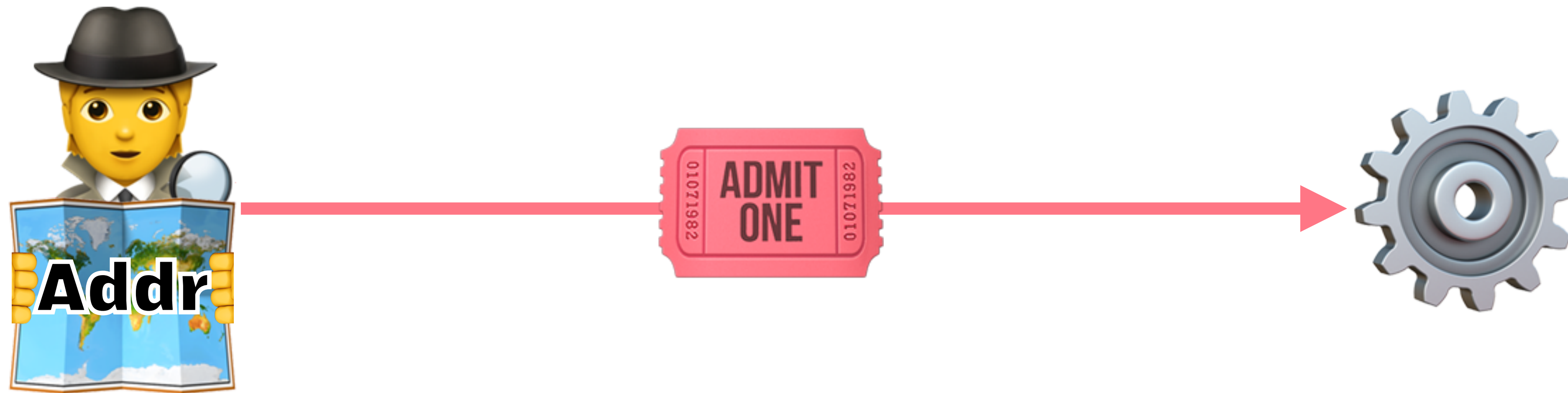
UCAN

# *From Actors to Capabilities*



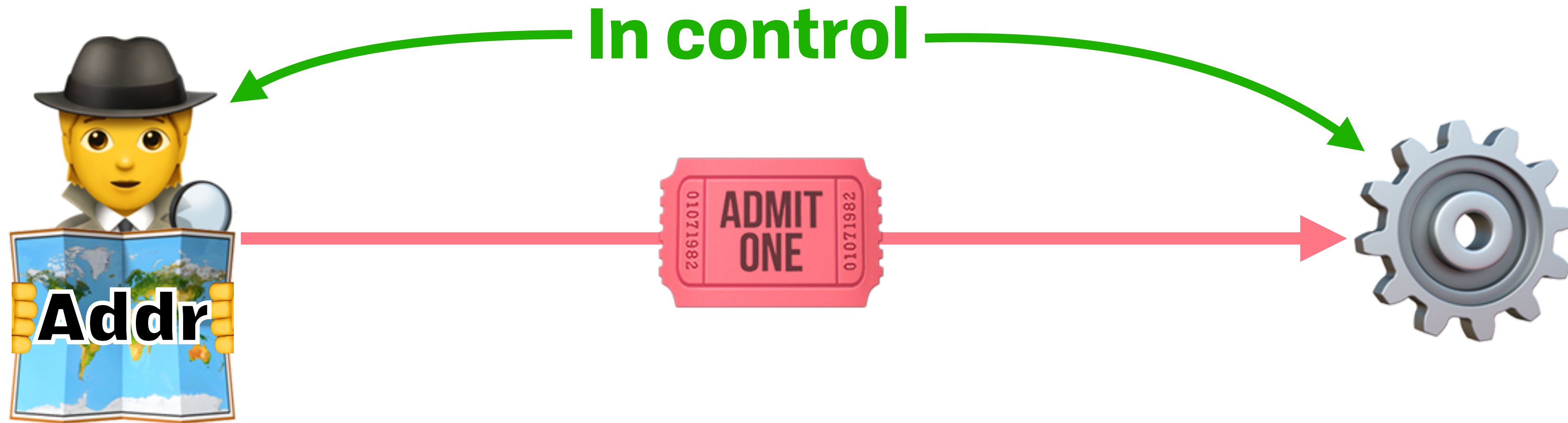
UCAN

# *From Actors to Capabilities*



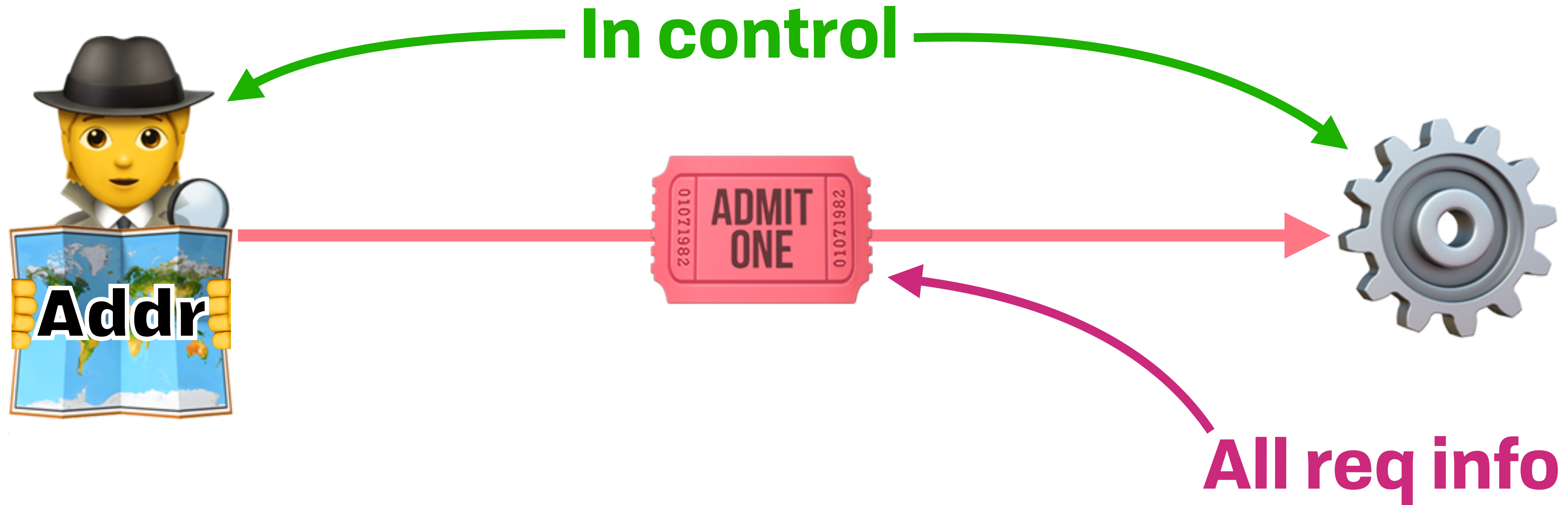
UCAN

# *From Actors to Capabilities*



UCAN

# *From Actors to Capabilities*



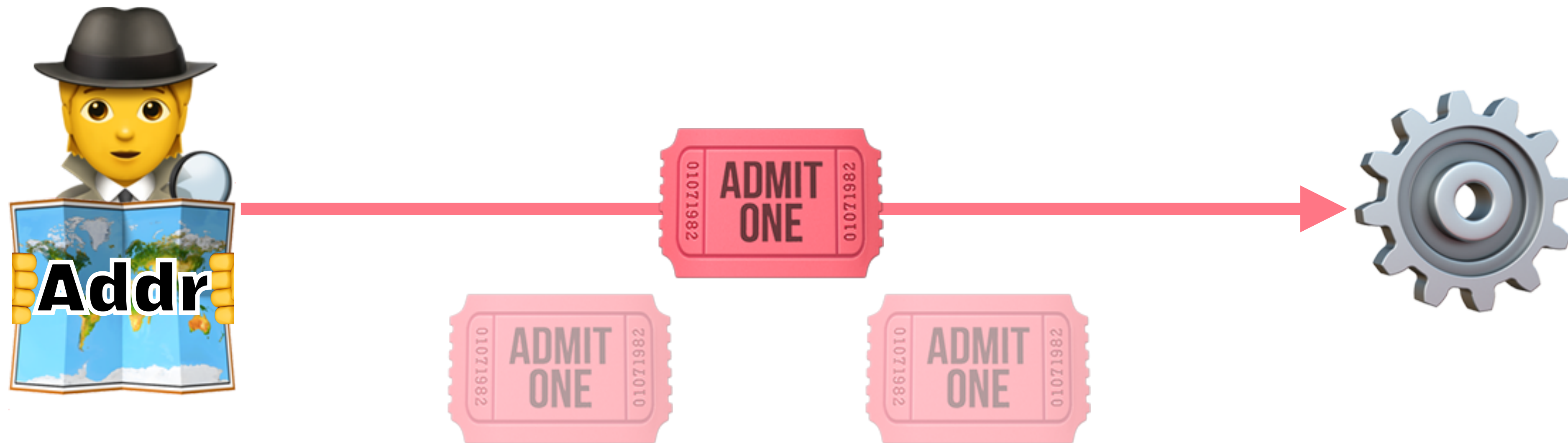
UCAN

# *From Actors to Capabilities*



UCAN

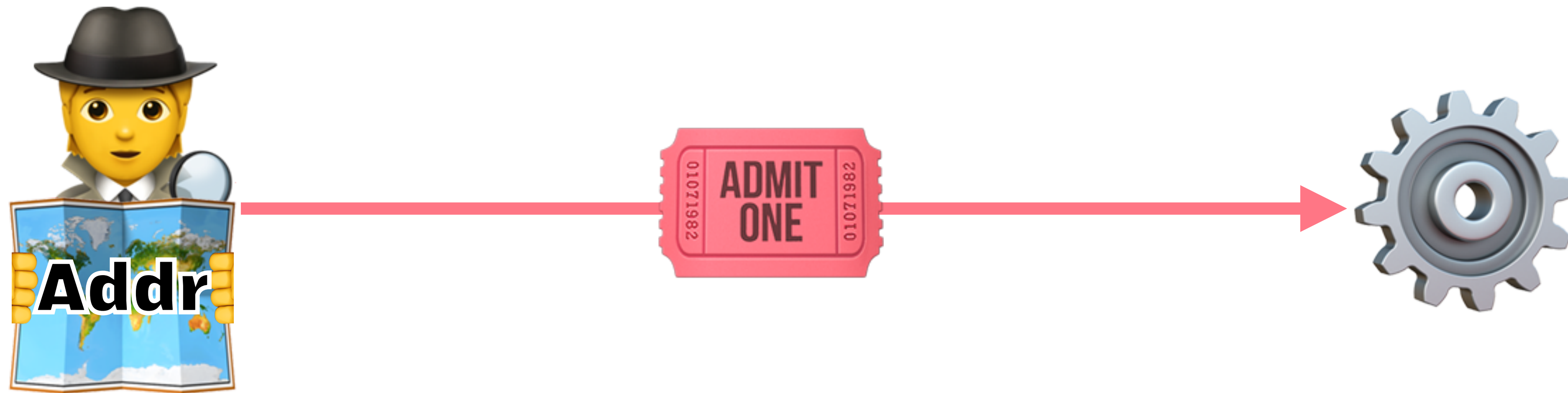
# *From Actors to Capabilities*





UCAN

# *From Actors to Capabilities*



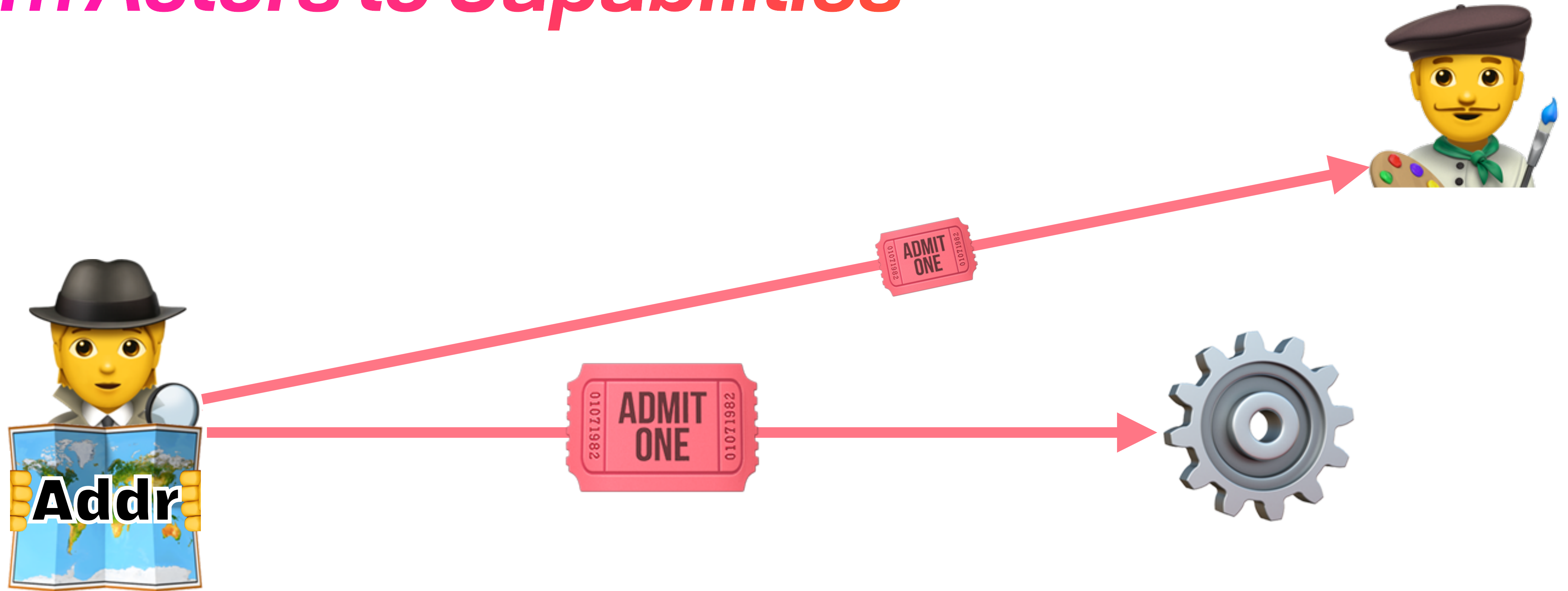
UCAN

# *From Actors to Capabilities*



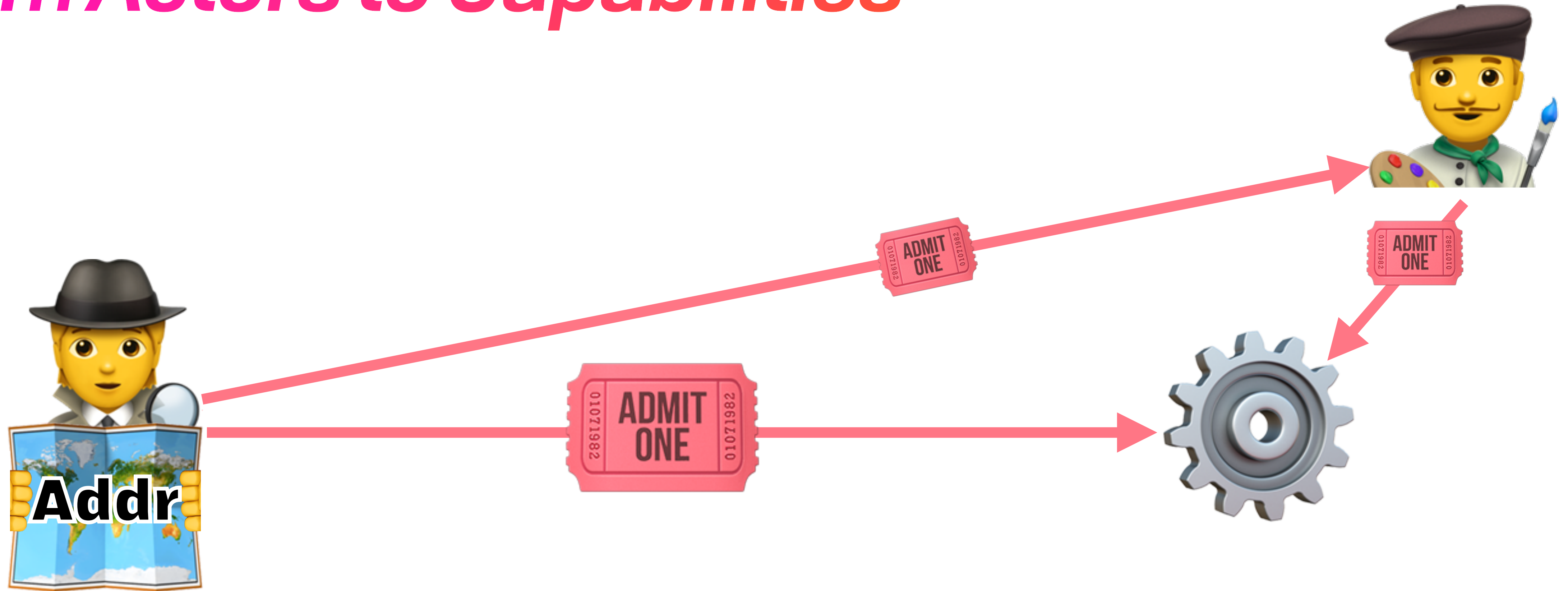
UCAN

# *From Actors to Capabilities*



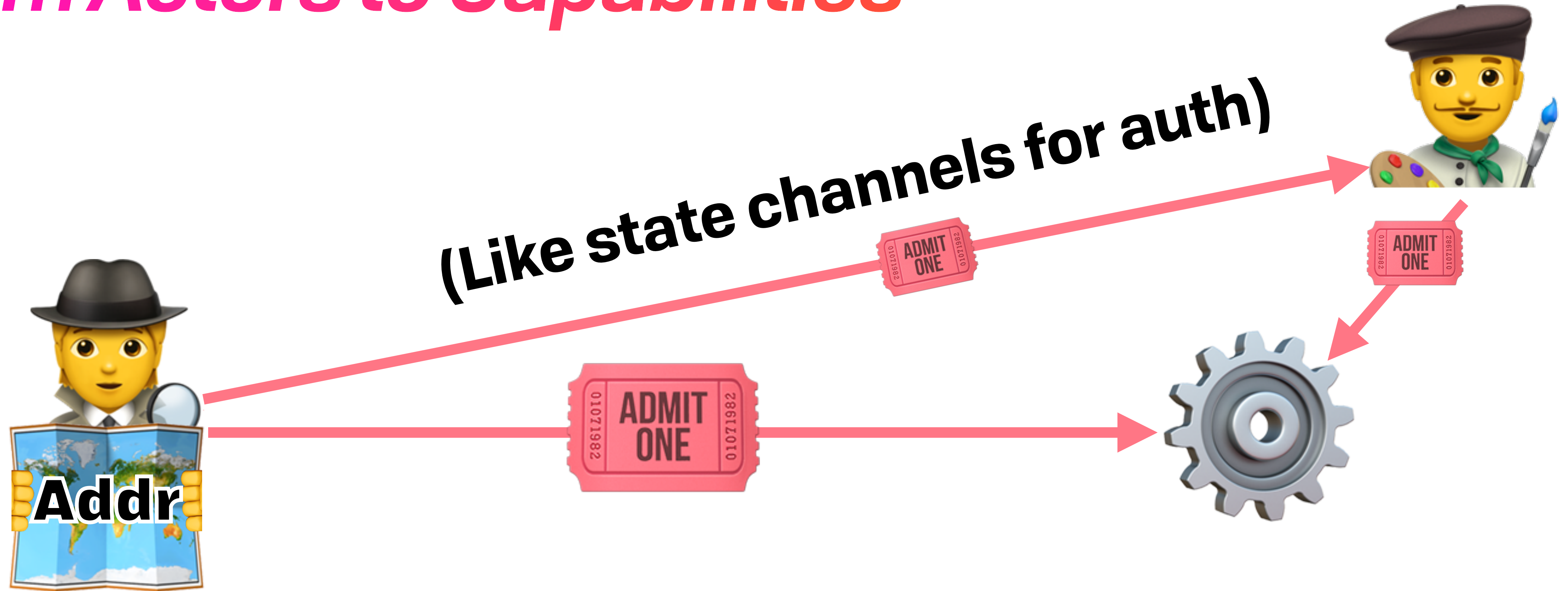
UCAN

# *From Actors to Capabilities*



UCAN

# *From Actors to Capabilities*



UCAN

# *Rights Amplification*

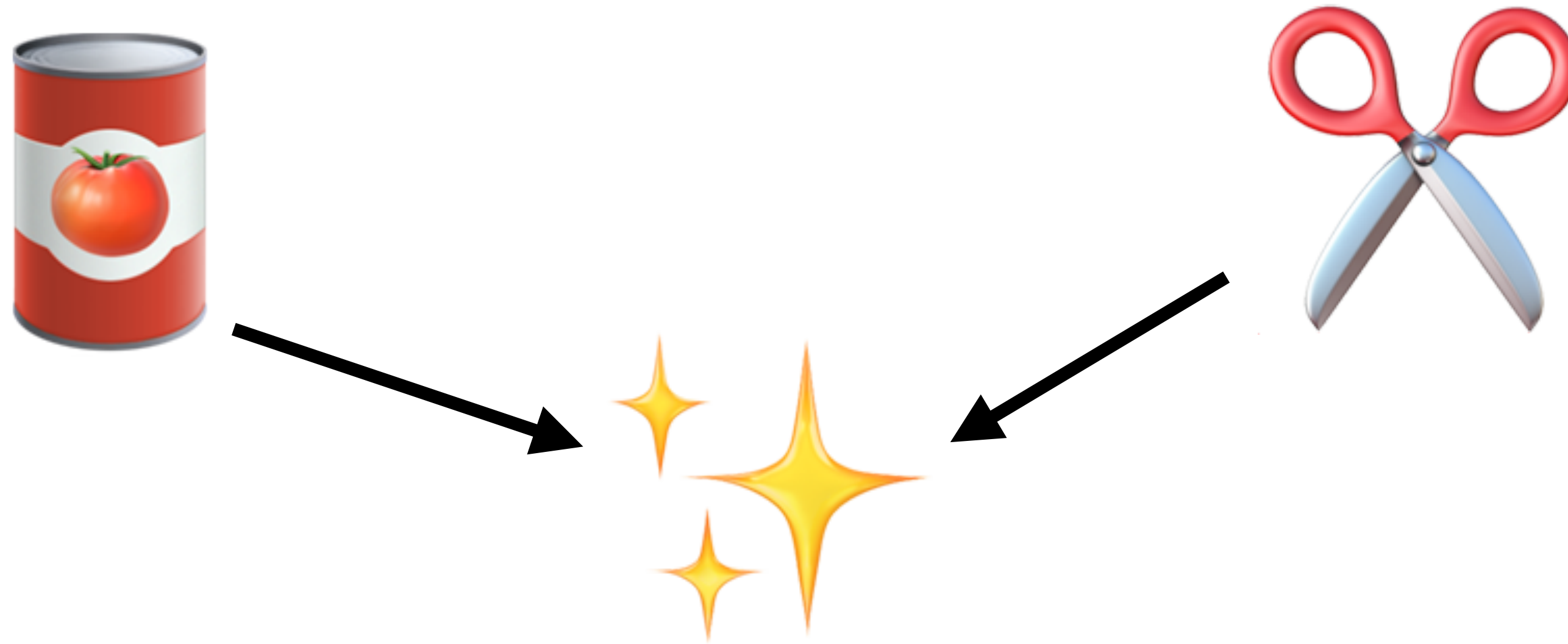
UCAN

# *Rights Amplification*



UCAN

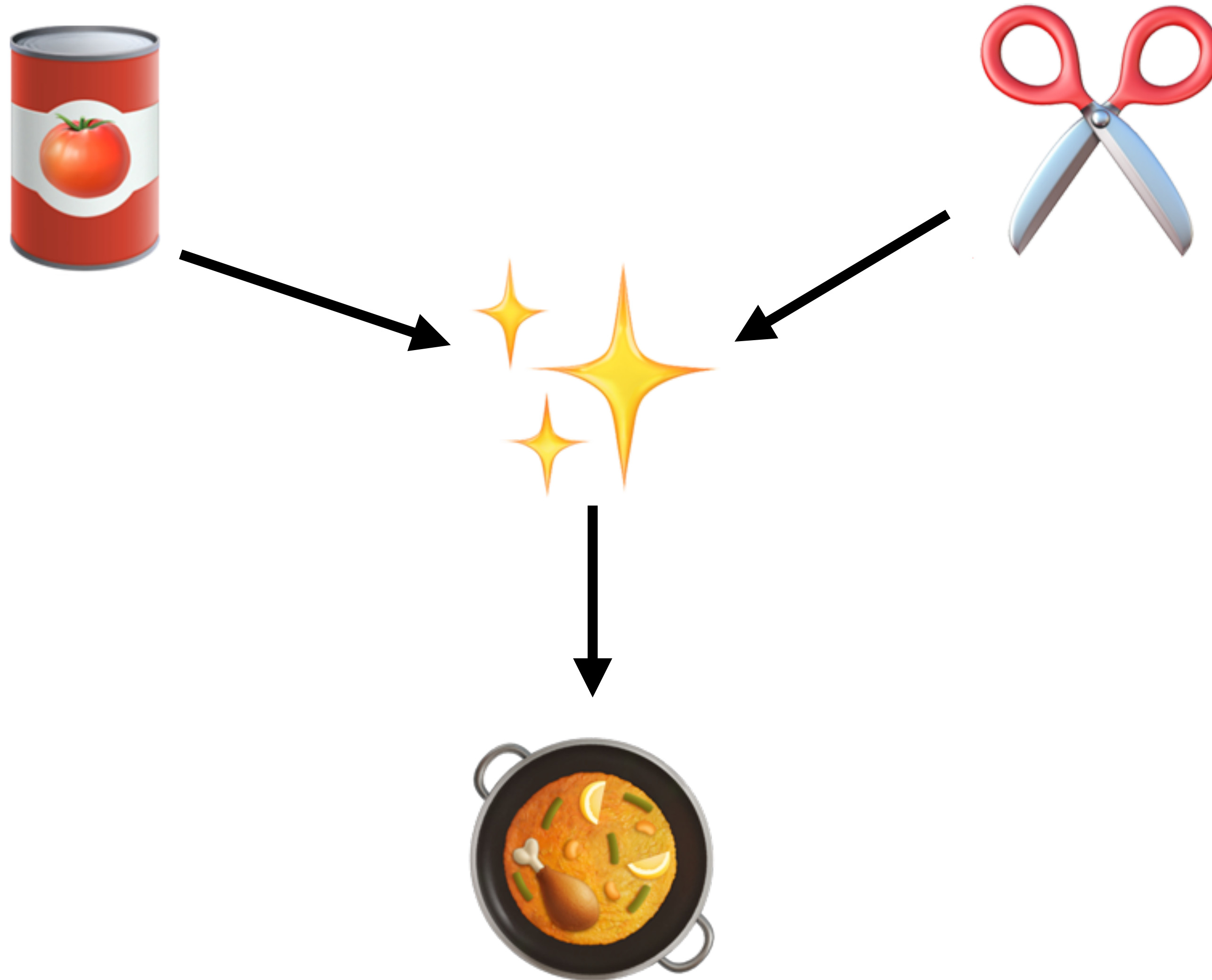
# *Rights Amplification*





UCAN

# *Rights Amplification*



UCAN

*JWT* → *UCAN*

UCAN

*JWT* → *UCAN*

*Header*

```
{  
  "alg": "EdDSA",  
  "typ": "JWT",  
  "ucv": "0.9.0"  
}
```

# UCAN

## JWT → UCAN

### Payload

### Header

```
{  
  "alg": "EdDSA",  
  "typ": "JWT",  
  "ucv": "0.9.0"  
}
```

```
{  
  "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",  
  "aud": "did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",  
  "nbf": 1639608293,  
  "exp": 9256939505,  
  "fct" {"hello": "world"},  
  "att": [  
    {  
      "with": "wnfs://demouser.fission.name/public/photos/",  
      "can": "wnfs/overwrite"  
    },  
    {  
      "with": "wnfs://demouser.fission.name/public/notes/",  
      "can": "wnfs/append"  
    }  
  ]  
}
```

# UCAN

## JWT → UCAN

### Payload

### Header

```
{  
  "alg": "EdDSA",  
  "typ": "JWT",  
  "ucv": "0.9.0"  
}
```

```
{  
  "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",  
  "aud": "did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",  
  "nbf": 1639608293,  
  "exp": 9256939505,  
  "fct" {"hello": "world"},  
  "att": [  
    {  
      "with": "wnfs://demouser.fission.name/public/photos/",  
      "can": "wnfs/overwrite"  
    },  
    {  
      "with": "wnfs://demouser.fission.name/public/notes/",  
      "can": "wnfs/append"  
    }  
  ]  
}
```

### Signature

```
kwRdqPN74pkcpXGgdk7Z7FW3M1mRR  
YaDE5ZgkG6srAuu6V6mvMVRdBLnD5  
CWid-X4tDIKpliVjlCSLTntB4pCw
```

# UCAN

## JWT → UCAN

### Payload

### Header

```
{  
  "alg": "EdDSA",  
  "typ": "JWT",  
  "ucv": "0.9.0"  
}
```

```
{  
  "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",  
  "aud": "did:key:z6MkvXtP0v0bxtsvQlG07NtK4qKJncgKzLc5zpc75teupKt",  
  "nbf": 1639608293,  
  "exp": 9256939505,  
  "fct": {"hello": "world"},  
  "att": [  
    {  
      "with": "wnfs://demouser.fission.name/public/photos/",  
      "can": "wnfs/overwrite"  
    },  
    {  
      "with": "wnfs://demouser.fission.name/public/notes/",  
      "can": "wnfs/append"  
    }  
  ]  
}
```



### Signature

```
kwRdqPN74pkcpXGgdk7Z7FW3M1mRR  
YaDE5ZgkG6srAuu6V6mvMVRdBLnD5  
CWid-X4tDIKpliVjlCSLTntB4pCw
```

UCAN

# *Anatomy of a Capability*

UCAN

# *Anatomy of a Capability*

```
[
  {
    "with": "http://example.com/alice/photos/",
    "can": "crud/read"
  },
  {
    "with": "mailto:boris@fission.codes",
    "can": "msg/send",
    "ext": {
      "to": "/*@fission.codes/"
    }
  }
]
```



# UCAN

## *Anatomy of a Capability*

```
[  
  {  
    Resource / "noun" .....  
    "with": "http://example.com/alice/photos/", (URI)  
    "can": "crud/read"  
  },  
  {  
    "with": "mailto:boris@fission.codes",  
    "can": "msg/send",  
    "ext": {  
      "to": "/*@fission.codes/"  
    }  
  }  
]
```

# UCAN

## *Anatomy of a Capability*

```
[  
  {  
    Resource / "noun"  
    "with": "http://example.com/alice/photos/", (URI)  
    "can": "crud/read"  
  },  
  {  
    Action / "verb"  
    "with": "mailto:boris@fission.codes",  
    "can": "msg/send",  
    "ext": {  
      to: "/*@fission.codes/"  
    }  
  }  
]
```

# UCAN

## *Anatomy of a Capability*

```
[  
  {  
    Resource / "noun"  
    "with": "http://example.com/alice/photos/", (URI)  
    "can": "crud/read"  
  },  
  {  
    Action / "verb"  
    "with": "mailto:boris@fission.codes",  
    "can": "msg/send",  
    "ext": {  
      to: "/*@fission.codes/"  
    }  
  }  
]
```

*Extensible fields*

UCAN

# *Chain Witnesses*

UCAN

# *Chain Witnesses*



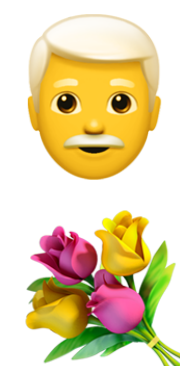
UCAN

# *Chain Witnesses*



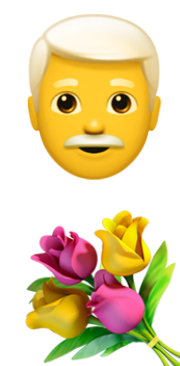
UCAN

# *Chain Witnesses*



UCAN

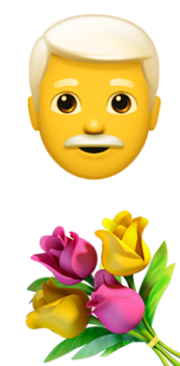
# *Chain Witnesses*





UCAN

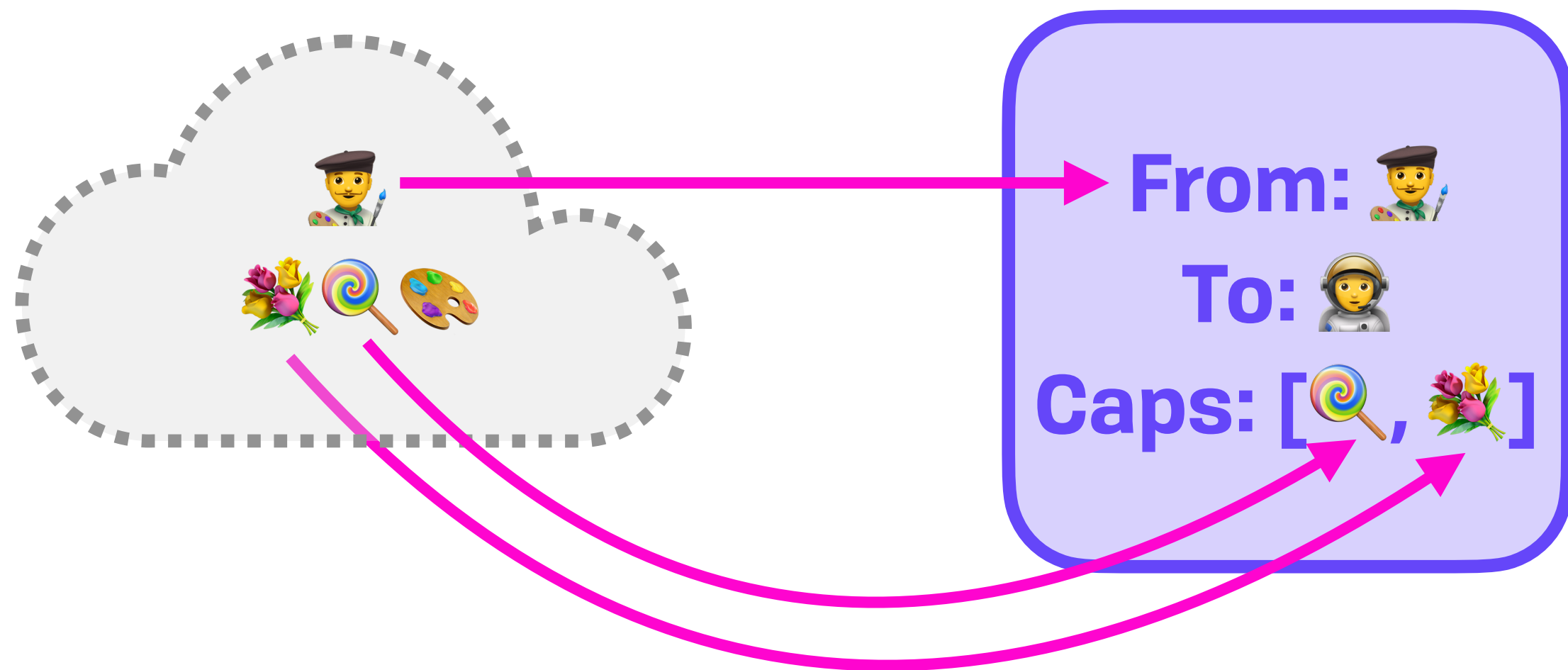
# *Chain Witnesses*



UCAN

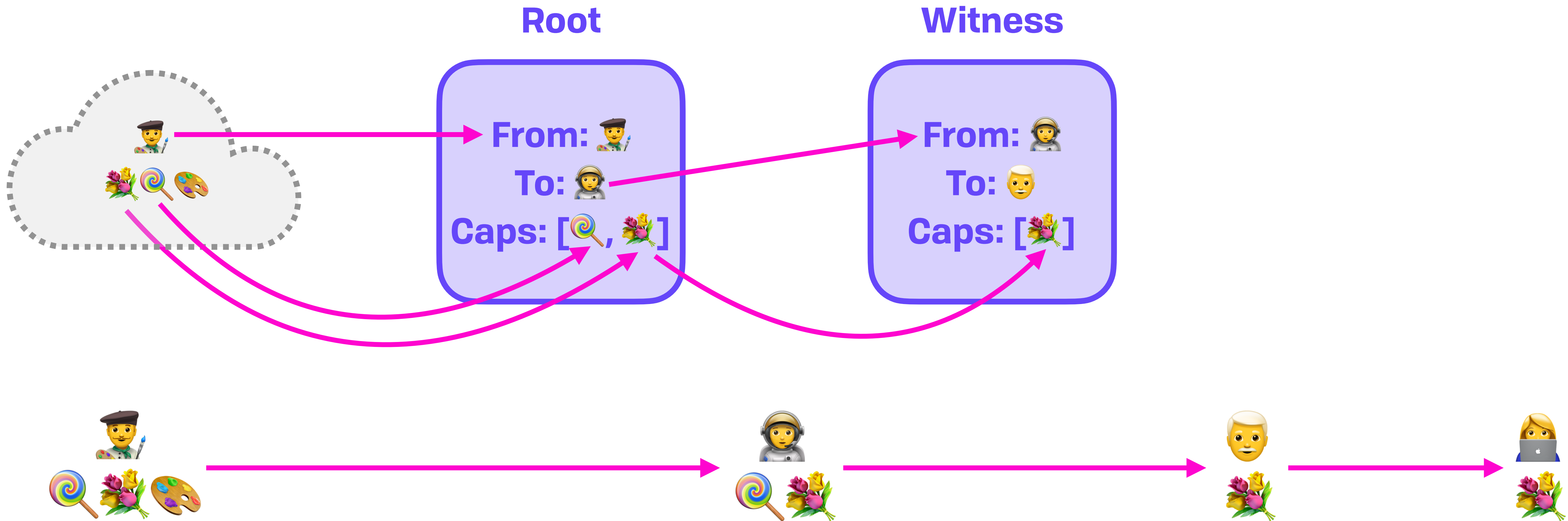
# Chain Witnesses

Root



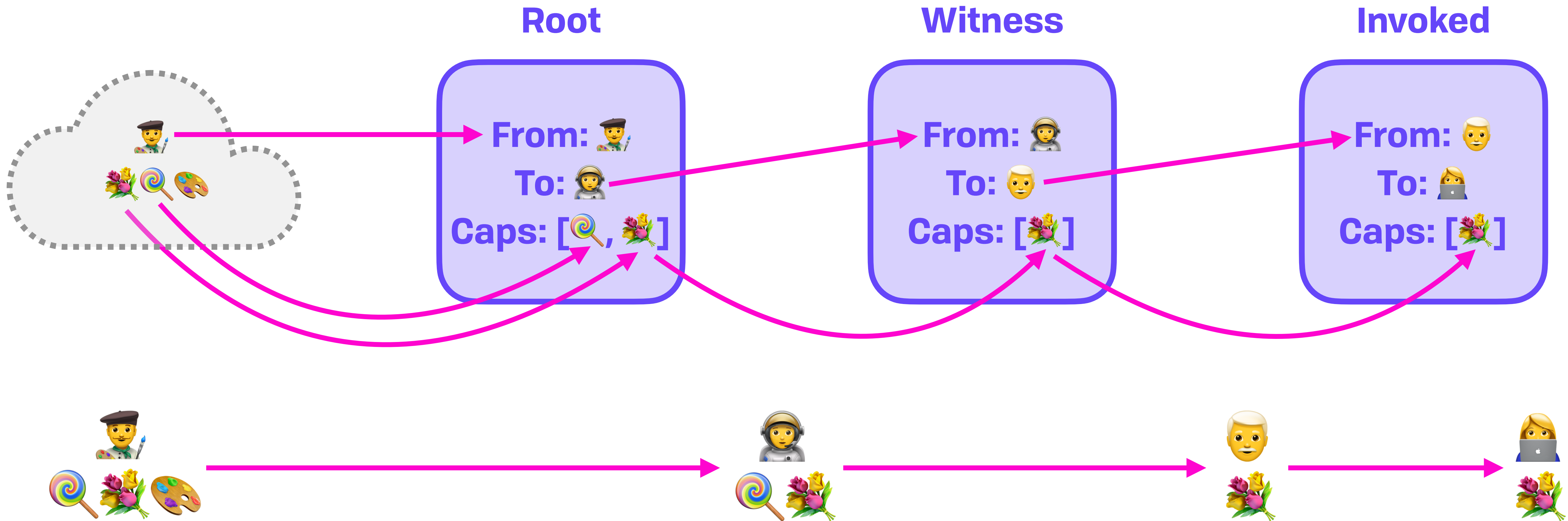
UCAN

# Chain Witnesses



UCAN

# Chain Witnesses



UCAN

*Zoomed Out*

UCAN

# *Zoomed Out*



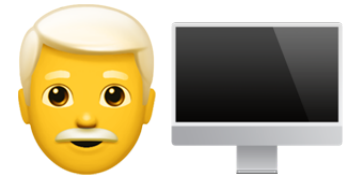
UCAN

# *Zoomed Out*



UCAN

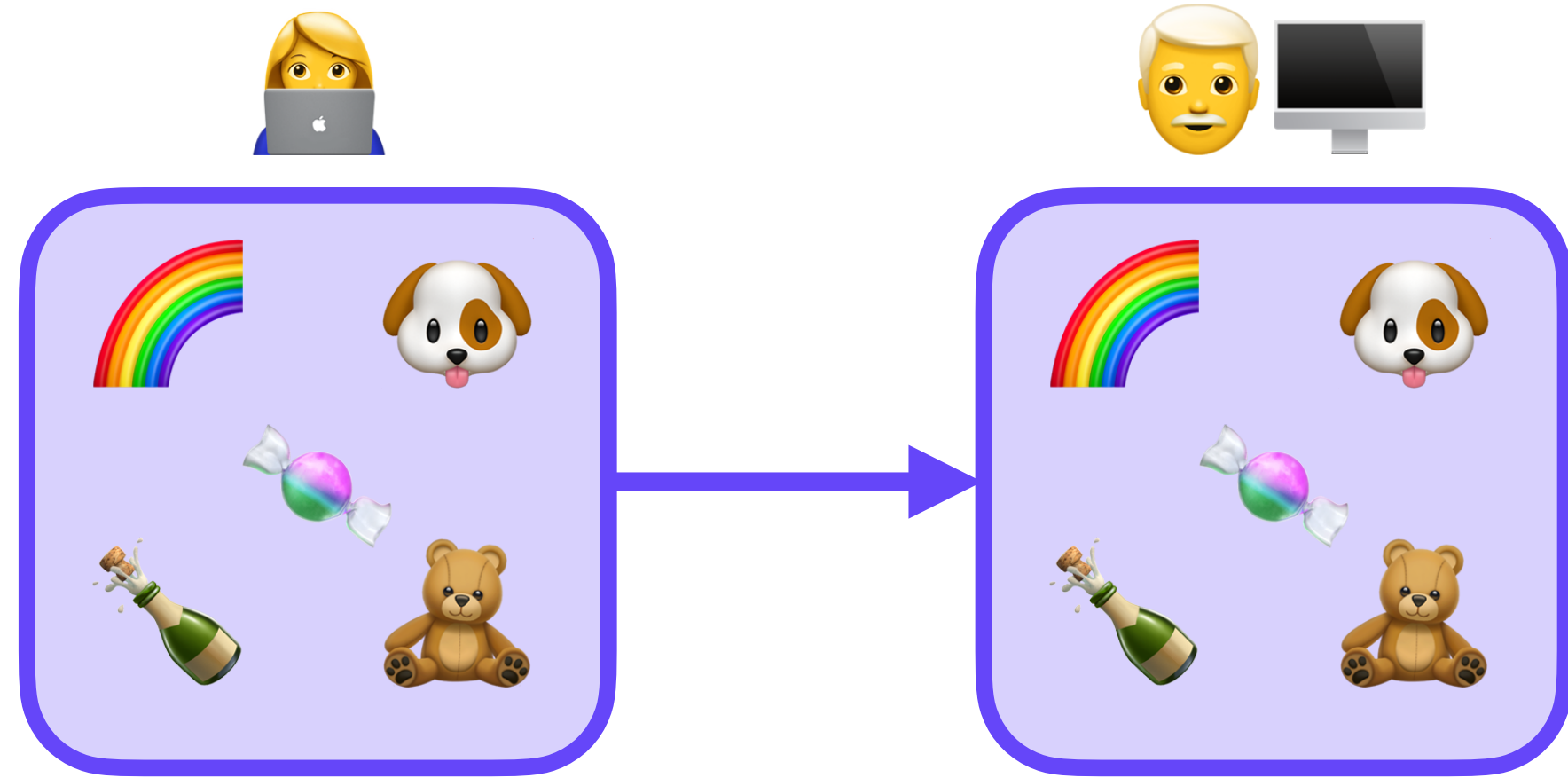
# *Zoomed Out*





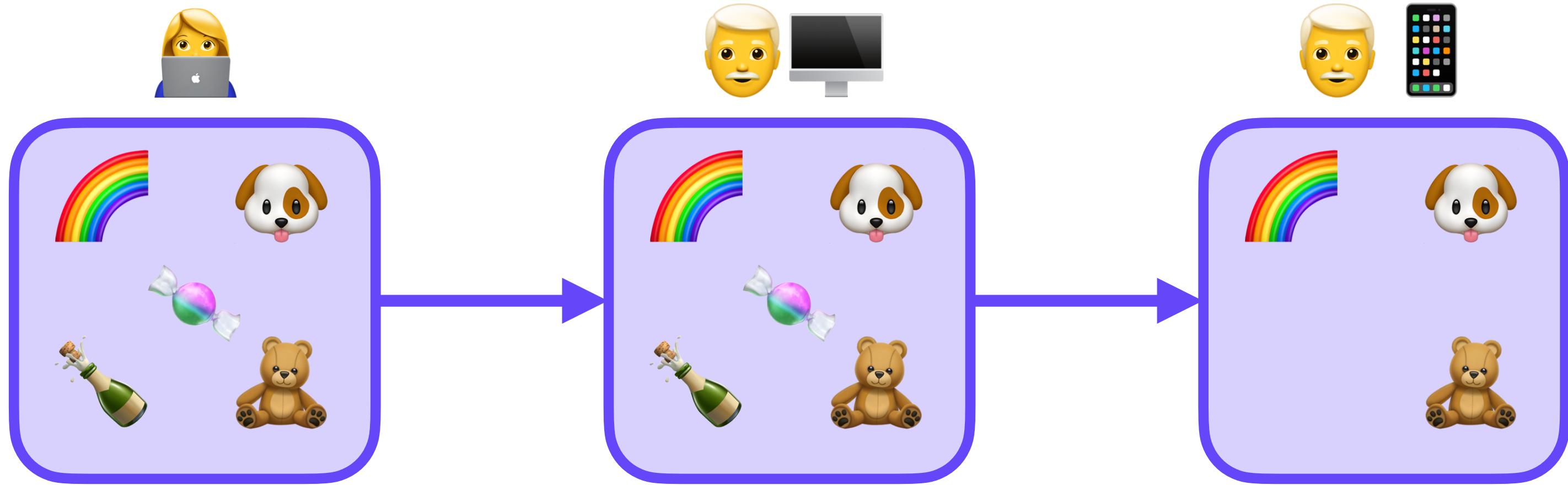
UCAN

# *Zoomed Out*



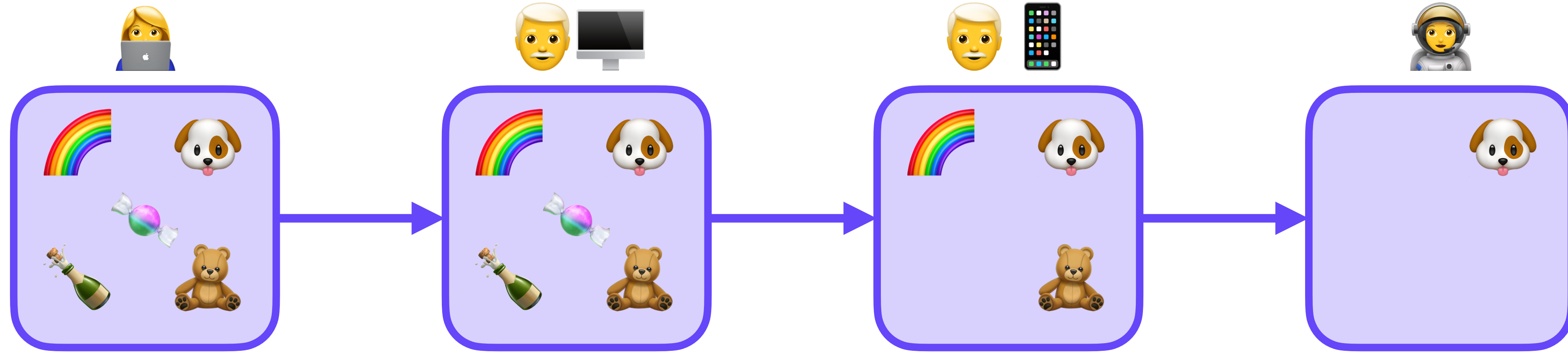
UCAN

# Zoomed Out



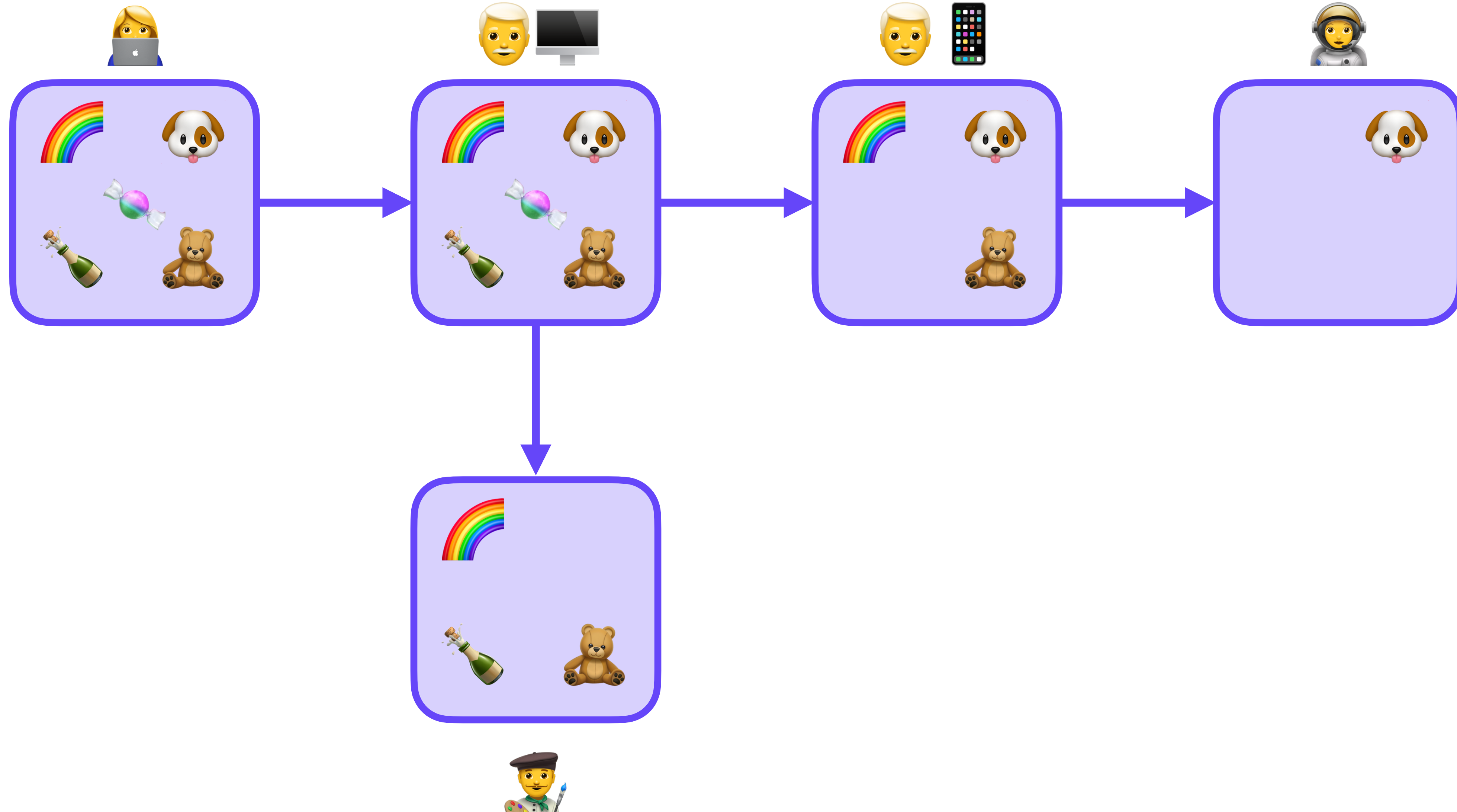
UCAN

# *Zoomed Out*



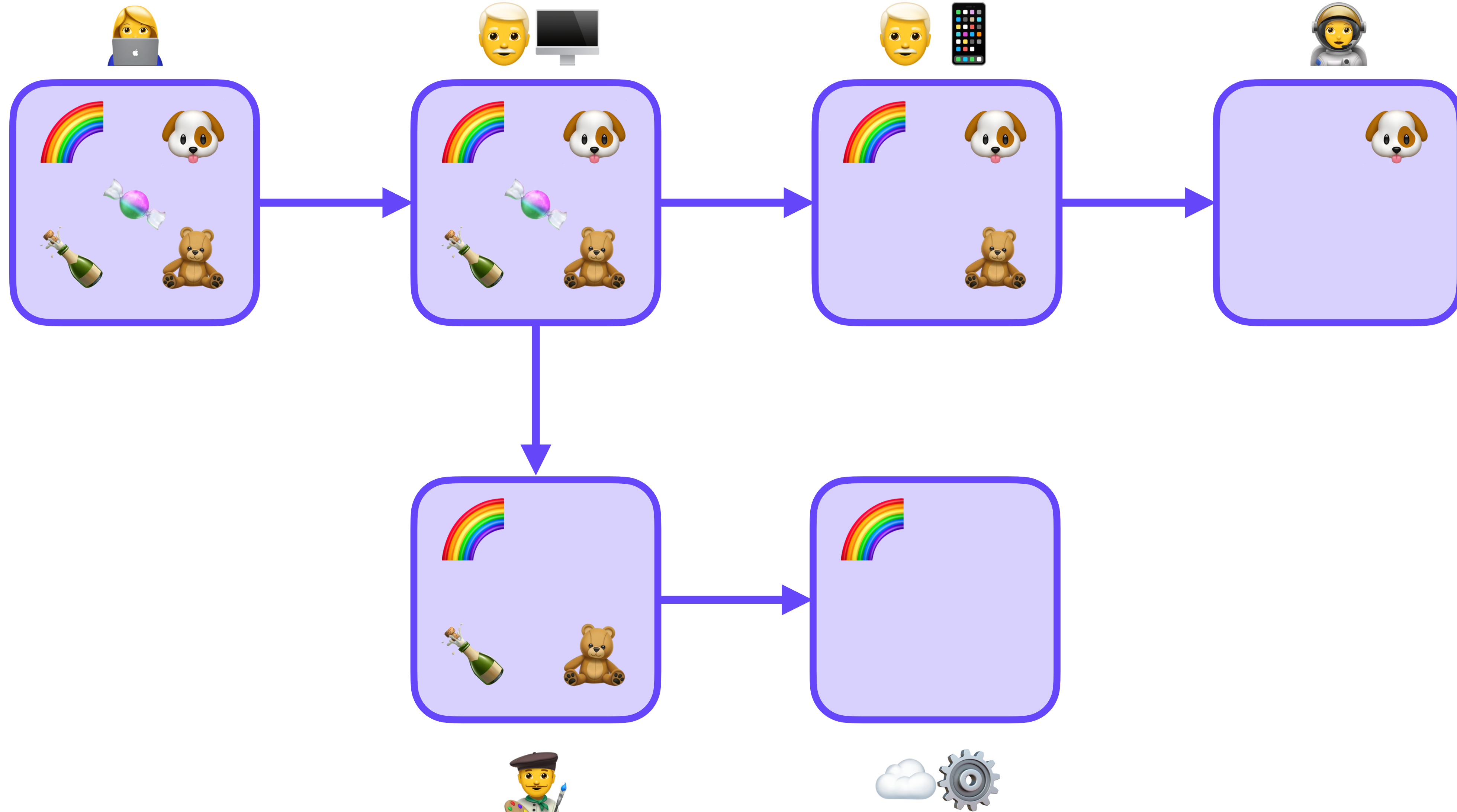
UCAN

# Zoomed Out



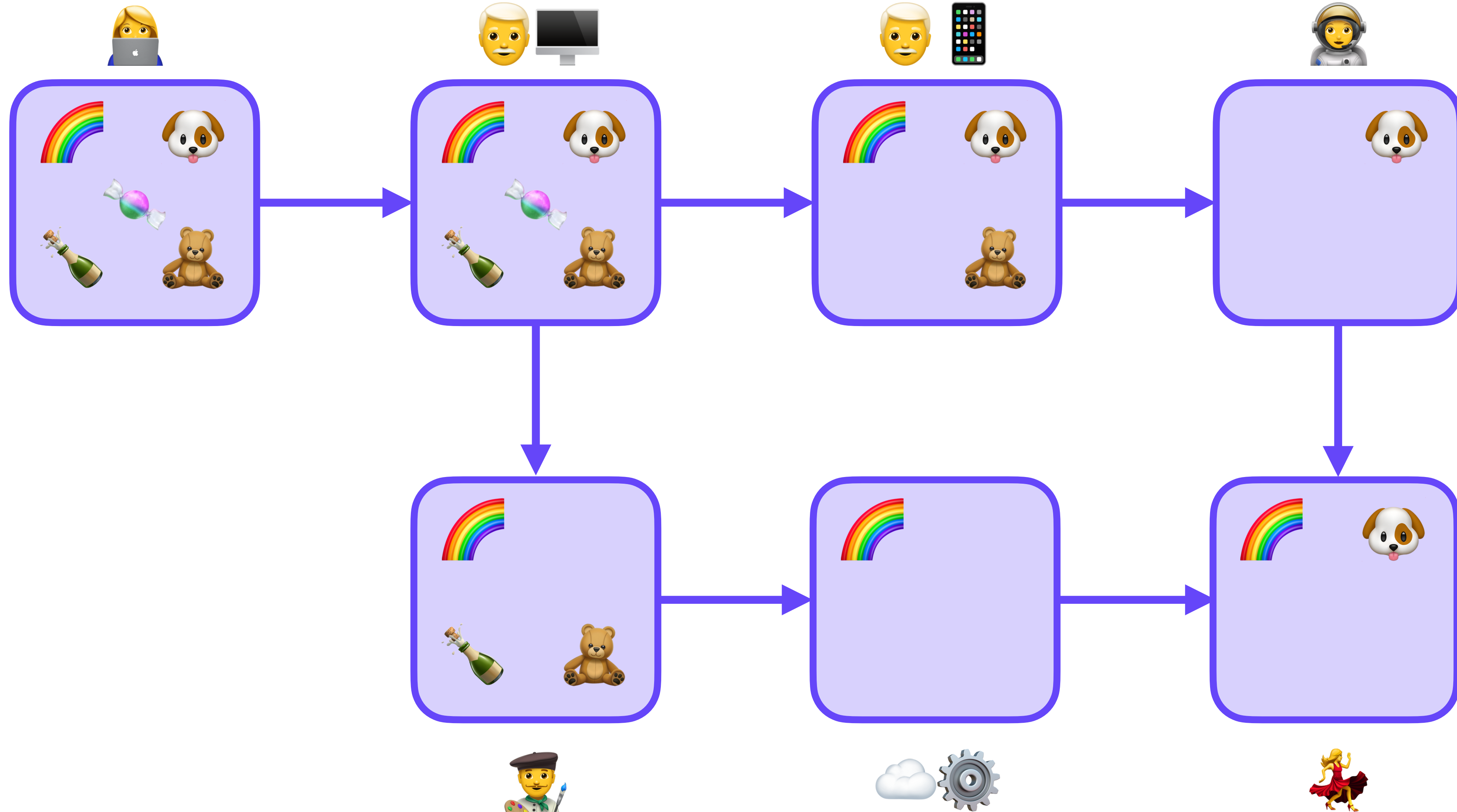
UCAN

# Zoomed Out



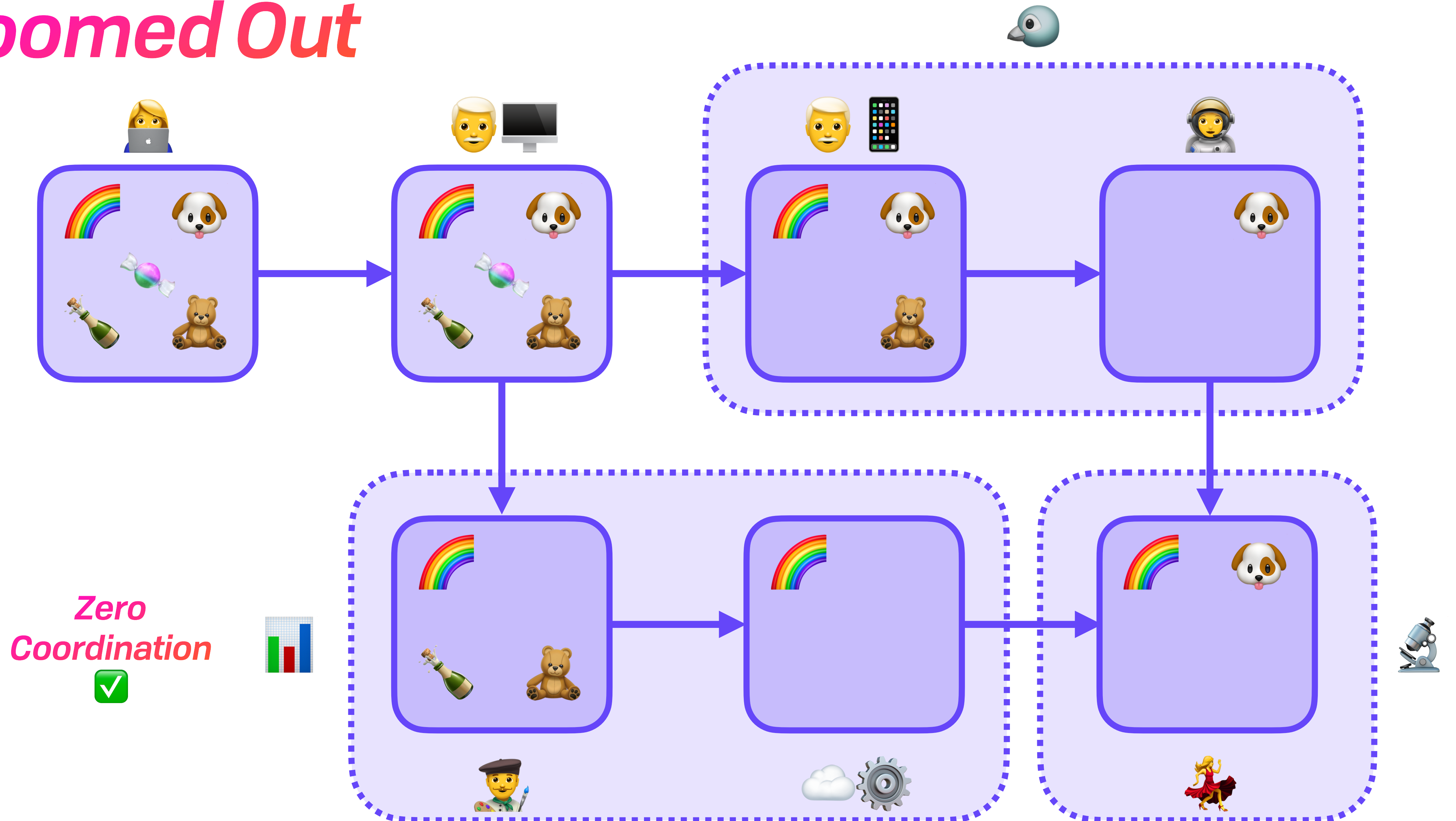
UCAN

# Zoomed Out



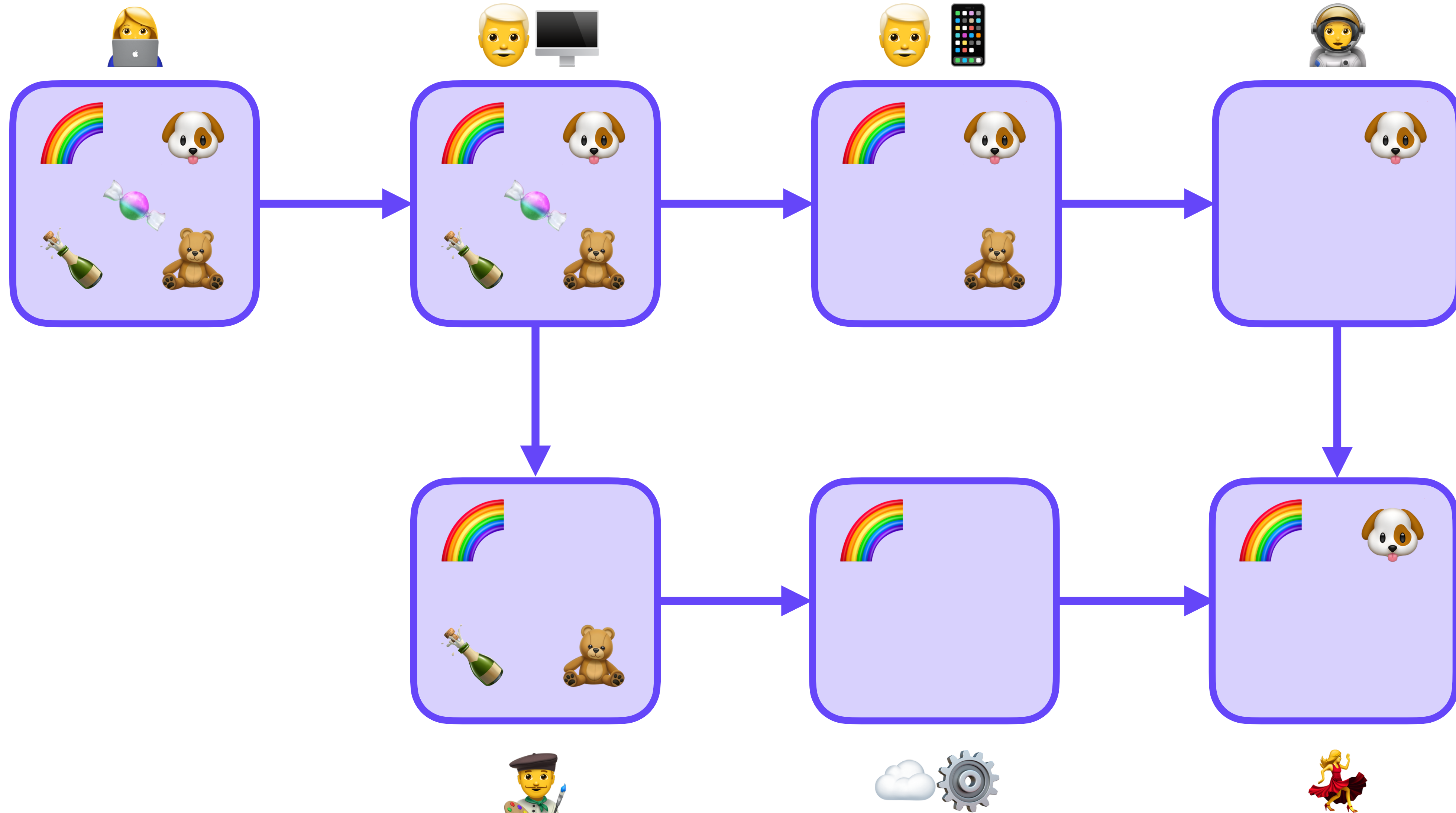
UCAN

# Zoomed Out



UCAN

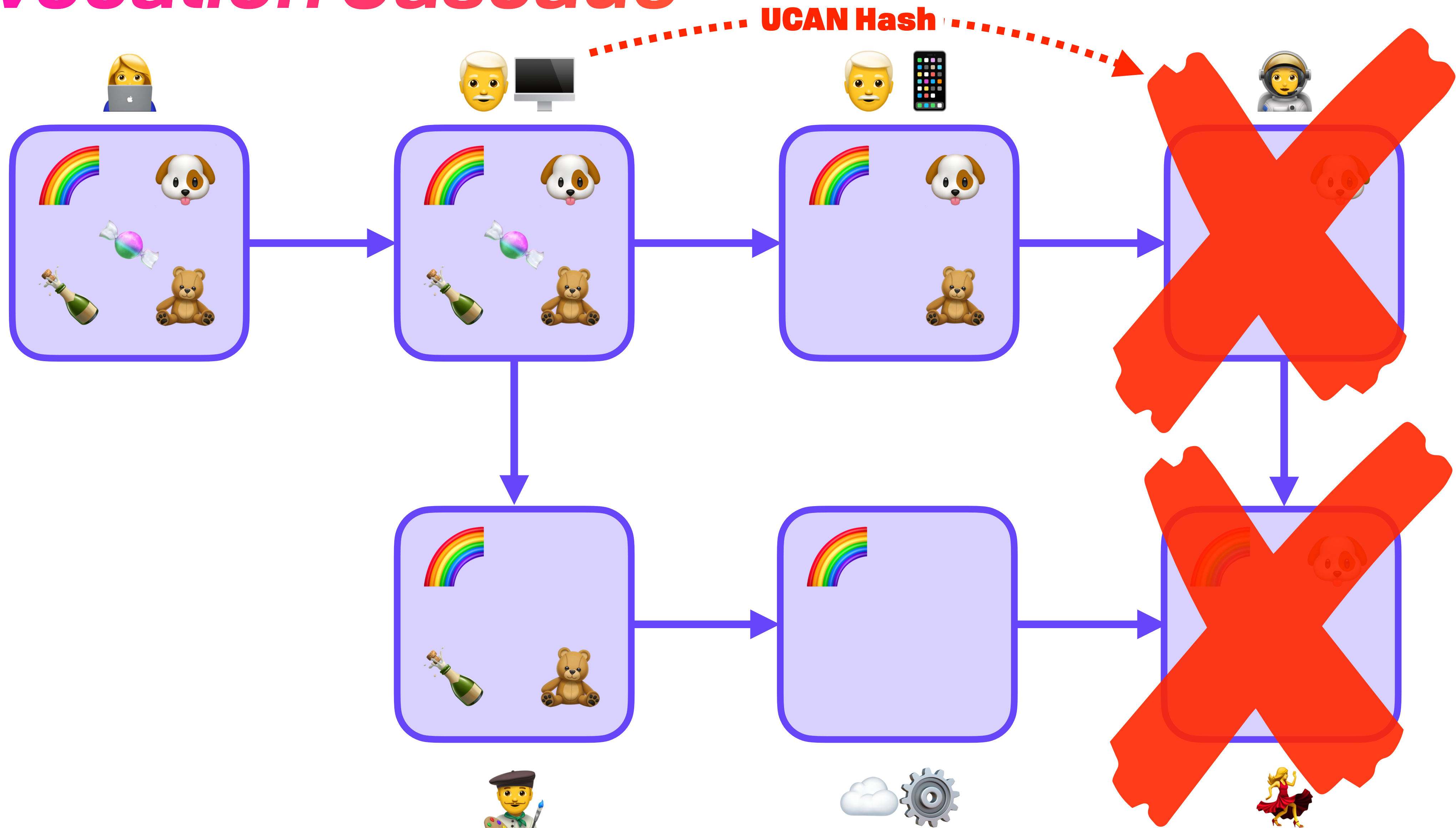
# Revocation Cascade





UCAN

# Revocation Cascade



UCAN

# *Composable Standard Library*

UCAN

# *Composable Standard Library*

## ***Resource (URI)***

https:

mailto:

file:

wnfs:

dns:

news:

## ***Action (Cap)***

crud/create

crud/read

crud/update

crud/destroy

msg/send

msg/receive

group/ban

group/join

UCAN

# *Semantic Extension*

UCAN

# *Semantic Extension*

```
{  
  "with": "http://example.com/alice/photos/",  
  "can": "crud/read"  
}  
  
{  
  "with": "http://example.com/alice/photos/devconnect/",  
  "can": "album/publish"  
}
```

UCAN

# *Semantic Extension*

```
{  
  "with": "http://example.com/alice/photos/",  
  "can": "crud/read"  
}  
  
{  
  "with": "http://example.com/alice/photos/devconnect/",  
  "can": "album/publish"  
}
```

album/publish ⇒ crud/read

# *Nontrivial Example*



Nontrivial Example

*Encoded*



# Nontrivial Example

## *Encoded*

eyJhbGciOiJFZERTQSIiInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V50no2T  
Wt2WGZQVXY4Ynh0c1ZRaUdvN050azRxS0p0Y2dLMml0NTJwYzcdGVVcFJMVCIiImF0dCI6W3sid25mcy  
I6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNhci6I6Ik9WRVJXUklURSJ9LHs  
id25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwY2FwIjoiT1ZFUldSSVRF  
In1dLCJleHAiOiJkyNTY5Mzk1MDUsImZcyI6ImRpZDprZXk6ejZNa3NYUUJmTDhvd3p0VENKVG03aE5SZ  
jZiMThZeFhQcDNpNjZvSkht0EwzWUdKIiwibmJmIjoxNjM5NjA4MjkzLCJwcmYiOiIsiZlKaGJHY2lPaU  
pGwkVSVFFTSXNjblI1Y0NjNkIrcFhWQ0lzSW5WamRpSTZJakF1Tnk0d0luMC5leUpoZFdRaU9pSmthV1E  
2YTJWNU9ubzJUV3R6V0ZGQ1prdzRiM2Q2ZEZSRFNsUnR0MmhPVW1ZMllqRTRXWGhZVUhBemFUWTJiMHBj  
YlRoTU0xbEhTaUlsSW1GMGRDSTZXM3NpZDI1bWN5STZJbVJsYlc5MWMvVnI6ImVpwYzN0cGIyNHVibUZ0W  
LM5d2RXSnNhV012Y0dodmRH0XpMeUlsSW10aGNDSTZJazlXUllZKWFVrbFVSU0o5WFN3aVpYaHdJam81TW  
pVMk9UTTV0VEExTENKcGMzTWlPaUprYVdRNmEyVjVPbm8yVFd0d05VVnplamx6TWsxSWMzRlpka3h2WTJ  
0NVNIZFl0Vks5sZVZwTGNIrTNPVWQwTkRwbVJrZEZXBek1T1Njc0ltNWlaaUk2TVRZek9UWXDPREk1TXl3  
aWNISm1JanBiWFgwLjRUTmh1SFJyUEc5YUhv0DY5SFhsc05L0F9GbWXTaFE1R3pHNGl0TjJ0S2steUtUY  
kFNb0Z3VHVwdEcwWEZnTkI2SHVsUHBsVnpaWURWRGV4bzc2a0F3IiwZlKaGJHY2lPaUpGwkVSVFFTSX  
NjblI1Y0NjNkIrcFhWQ0lzSW5WamRpSTZJakF1Tnk0d0luMC5leUpoZFdRaU9pSmthV1E2YTJWNU9ubzJ  
UV3R6V0ZGQ1prdzRiM2Q2ZEZSRFNsUnR0MmhPVW1ZMllqRTRXWGhZVUhBemFUWTJiMHBjYlRoTU0xbEhT  
aUlsSW1GMGRDSTZXM3NpZDI1bWN5STZJbVJsYlc5MWMvVnI6ImVpwYzN0cGIyNHVibUZ0WLM5d2RXSnNhV  
012Ym05MFpYTXZJaXdpWTJGd0lqb2lUMVpGVWxkU1NWUkZJbjFkTENKbGVIQWlPamt5TlRZNU16azFNRF  
VzSW1semN5STZJbVJwWkRwclpYazZla0YTnBMVJYTjZPWE15VFVoemNwbDJURzlwWTNsSWQxZzFVMlY  
1V2t0d2NUYzVSM1EwTldaR1IwVmFVams1SWl3aWJtSm1Jam94TmPNUU5qQTRNamt6TENKd2NtWwlpbHRk  
ZlEuTWdZYXJMcXk3Um1RMUFJcnFZTDZjRnk5ejdhNVdJQVUtLVRZQVJQU2dpck9Tc3p2YXIzX0R0cjI1c  
mJQcmV0SGJuVDBtTVZLeW9hUVhydVI3S2JyQmciXX0.kwRdqPN74pkcpXGgdk7Z7FW3M1mRRYaDE5ZgkG  
6srAuu6V6mvMVRdBLnD5Cwid-X4tDIKplivjlCSLTntB4pCw





# Nontrivial Example

## *Decoded Witness #1*

### *Payload*

#### *Header*

```
{  
  "alg": "EdDSA",  
  "typ": "JWT",  
  "ucv": "0.8.0"  
}
```

```
{  
  "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99",  
  "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",  
  "nbf": 1639608293,  
  "exp": 9256939505,  
  "att": [  
    {  
      "with": "wnfs://demouser.fission.name/public/photos/",  
      "can": "OVERWRITE"  
    }  
  ],  
  "prf": []  
}
```

#### *Signature*

```
4TNhuHRrPG9aHo869HXlsNK8_Fm1ShQ5GzG  
4itN2NKk-  
yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDe  
xo76kAw
```

Nontrivial Example

*uican.xyz — Online Explorer / Validator*

# Nontrivial Example

# *ucan.xyz* — Online Explorer / Validator

**Hey there** 🤖  
You are using a preview version of UCAN Check. This version only supports the latest UCAN version. Try out the [UCAN library](#) to make some!

## UCAN Check

### Encoded

Paste an encoded UCAN

```
eyJhbGciOiJIJzERTQSIrR5cCI6IkpXVCIsInVjdjI6IjAuNy4wIn0_eyJhdWQiOiJkaWQ6a2V5Ondo2TWtZWFFCZkw4b3d6dFRDSiRIN2hOUmY2YjE4WXhYUHAzaTY2b0plbThMM1IHSIsImF0dCI6I3d2cmcyI6ImRlbW91c2VyLmZpc3Npb24ubmFIZS9wdWJ3aWMvcGhvdG9zLyIsImNhcCI6Ikh9WRV3XUkiURS39XSWiZKhWj05MjU2OTM5NTA1LCJpc3MiOiJkaWQ6a2V5Ondo2TWtWNUVzejlzMK1Iic3FZdkxvY2N5SHdYVWVNeVpLcHE3OUd0NDVmRkdFWlI5OStsIm5iZiI6MTYzOTYwODI5MywicHJmIjpbXX0.4TNhuHRrPG9aHo869HXlsNKB_FmIshQ5GzG4iHN2NKK-yKTbAMoFwTuptG0XFgNivHulPpIVzZYDvDexo76kAw
```

### Decoded

Header

```
{  "alg": "EdDSA",  "typ": "JWT",  "ucv": "0.7.0"}
```

Payload

```
{  "aud": "did:key:z6MksXQBfLBowztTCJTm7hNRf6b18YxXp3i66oJHm8L3YGJ",  "att": [    {      "wnfs": "demouser.fission.name/public/photos/",      "cap": "OVERWRITE"    }  ],  "exp": 9256939505,  "iss": "did:key:z6Mkp5EsZ9s2MHsqYvLoccyHwX5SeyZKpq79Gt45FGEZR99",  "nbf": 1639688293,  "prf": []}
```

Signature

```
4TNhuHRrPG9aHo869HXlsNKB_FmIshQ5GzG4iHN2NKK-yKTbAMoFwTuptG0XFgNivHulPpIVzZYDvDexo76kAw
```

Delegate 1 Selected

**Valid UCAN.** The UCAN is valid and has not expired.

## Explanation

Please see the [JWT RFC](#) and the [UCAN specification](#) for more details.

Field	Long Name	Value	Details
alg	Signature Algorithm	EdDSA	The algorithm used to sign the UCAN
typ	Type	JWT	UCANs are JWTs
ucv	UCAN Version	0.7.0	The UCAN version
iss	Issuer	did:key:z6Mkp5EsZ9s2MHsqYvLoccyHwX5SeyZKpq79Gt45FGEZR99	The DID of the issuer. The UCAN must be signed with the private key of the issuer to be valid.
aud	Audience	did:key:z6MksXQBfLBowztTCJTm7hNRf6b18YxXp3i66oJHm8L3YGJ	The DID of the audience
att	Attenuation	{ "wnfs": "demouser.fission.name/public/photos/", "cap": "OVERWRITE" }	Capabilities granted or delegated to the audience
exp	Expires At	9256939505	The UNIX time when the UCAN expires. This UCAN expires on May 5, 2263 at 5:05:05 AM PDT.
nbf	Not Before	1639688293	The UNIX time after which the UCAN is valid. This UCAN became valid on December 15, 2021 at 2:44:53 PM PST.

# Nontrivial Example

# ucan.xyz — Online Explorer / Validator

Hey there 🤖  
You are using a preview version of UCAN Check. This version only supports the latest UCAN version. Try out the [UCAN library](#) to make some!

## UCAN Check

### Encoded

Paste an encoded UCAN

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXLTJ0IiwiaWF0IjoiYXNjaWwuan0uY2h0dWQvOjkaWQ6a2V5Ono2TWtZWFFCZkw4b3d6dFRDSiRlN2h0UmY2YjE4WkYyUHZAzaTY2b0plbThMM1HSIsImF0dCI6W3sid25mcyI6ImRlbnW91c2VyLmZpc3Npb24ubmF1ZS9wdWJ3aWVmcGhvdG9zLyIsImNhcCI6Ikh9WRV3XUkiUR539S5wzXhwJjo5MjU2OTM5NTA1LCJpc3MiOiJkaWQ6a2V5Ono2TWtWNUVzejIzMK1Ic3FZdkxvY2N5SHdYVnNleVpLcHE3OUd0NDVmRkdFWlI5OStIm5iZi6MTYzOTYwODI5MywiczHmIjpbXX0.4TNhuHRrPG9aHo869HXlsNKB_FmIshQ5GzG4iHN2NKK-ykTbAMoFwTuptG0XFGNivHulPpIvZyYDvDexo76kAw
```

### Decoded

Header

```
{ "alg": "EdDSA", "typ": "JWT", "ucv": "0.7.0" }
```

Payload

```
{ "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ", "att": [ { "wnfs": "demouser.fission.name/public/photos/", "cap": "OVERWRITE" } ], "exp": 9256939505, "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99", "nbf": 1639608293, "prf": [] }
```

Signature

```
4TNhuHRrPG9aHo869HXlsNKB_FmIshQ5GzG4iHN2NKK-ykTbAMoFwTuptG0XFGNivHulPpIvZyYDvDexo76kAw
```

### Payload

```
{ "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ", "att": [ { "wnfs": "demouser.fission.name/public/photos/", "cap": "OVERWRITE" } ], "exp": 9256939505, "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99", "nbf": 1639608293, "prf": [] }
```

Delegate 1 Selected

Valid UCAN. The UCAN is valid and has not expired.

## Explanation

Please see the [JWT RFC](#) and the [UCAN specification](#) for more details.

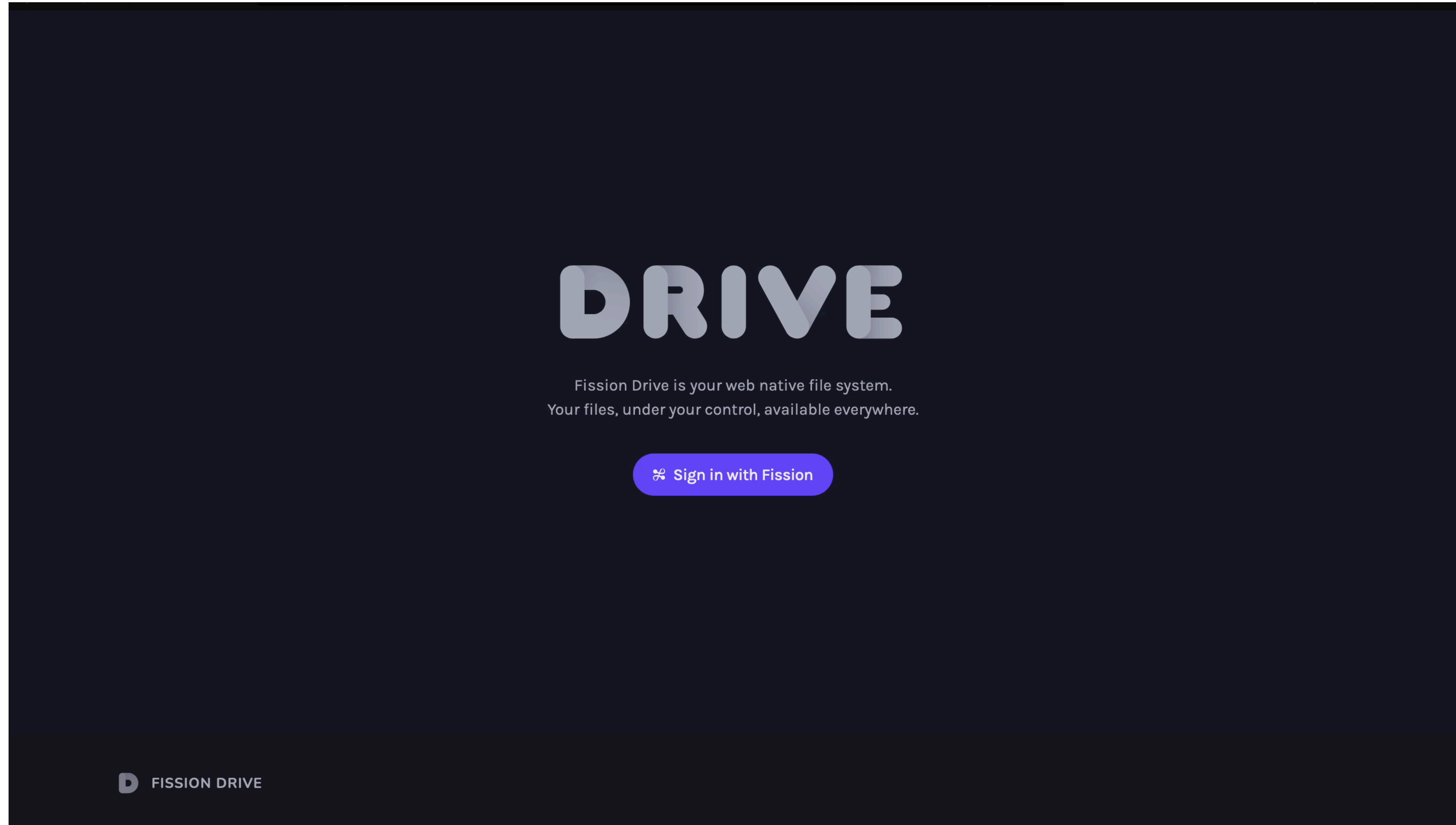
Field	Long Name	Value	Details
alg	Signature Algorithm	EdDSA	The algorithm used to sign the UCAN
typ	Type	JWT	UCANs are JWTs
ucv	UCAN Version	0.7.0	The UCAN version
iss	Issuer	did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99	The DID of the issuer. The UCAN must be signed with the private key of the issuer to be valid.
aud	Audience	did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ	The DID of the audience
att	Attenuation	{ "wnfs": "demouser.fission.name/public/photos/", "cap": "OVERWRITE" }	Capabilities granted or delegated to the audience
exp	Expires At	9256939505	The UNIX time when the UCAN expires. This UCAN expires on May 5, 2263 at 5:05:05 AM PDT.
nbf	Not Before	1639608293	The UNIX time after which the UCAN is valid. This UCAN became valid on December 15, 2021 at 2:44:53 PM PST.





Nontrivial Example

*Auth Should be Boring!*



Nontrivial Example

*Auth Should be Boring!*

DRIVE

Fission Drive is your web native file system.  
Your files, under your control, available everywhere.

 Sign in with Fission

# *Resources*



Resources

*Further Reading*

## Resources

# *Further Reading*

- <https://talk.fission.codes/t/user-controlled-authorization-networks-ucan-resources/1122>
- <https://github.com/ucan-wg/>
  - Spec, Improvement Proposals
  - Libraries in TypeScript, Rust, Golang, Haskell
- Capability Myths Demolished (<https://srl.cs.jhu.edu/pubs/SRL2003-02.pdf>)
- ACLs Don't (<http://waterken.sourceforge.net/acldsont/current.pdf>)
- <https://erights.org>
- <https://theworld.com/~cme/html/spki.html>

<https://ucan.xyz>

<https://github.com/ucan-wg>



***Thank You, CASA Amsterdam*** 🇳🇱

brooklyn@fission.codes

<https://fission.codes>

[github.com/expede](https://github.com/expede)

@expede