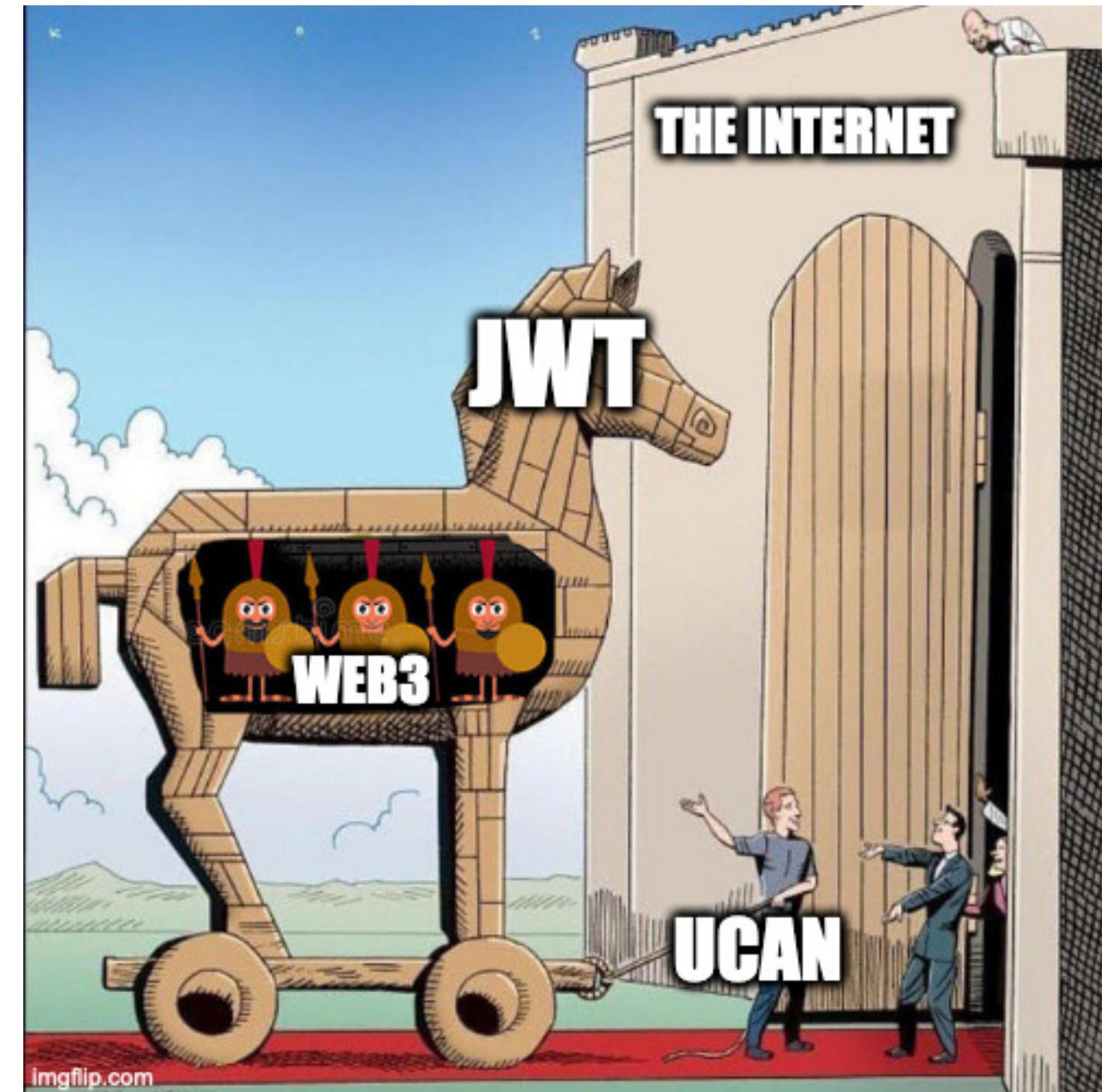


An Intro to UCAN

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



G

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

Wherfore Art Thou UCAN?



Meta

Wherfore Art Thou UCAN?

DIDs say who **you are**



Meta

Wherfore Art Thou UCAN?

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



Meta

Wherfore Art Thou UCAN?

DIDs say who **you are** ↪
UCANS show what **you can do** ↪

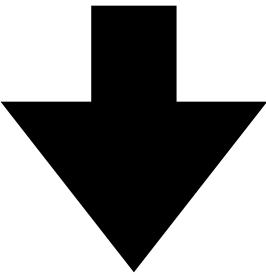


AuthN

AuthZ

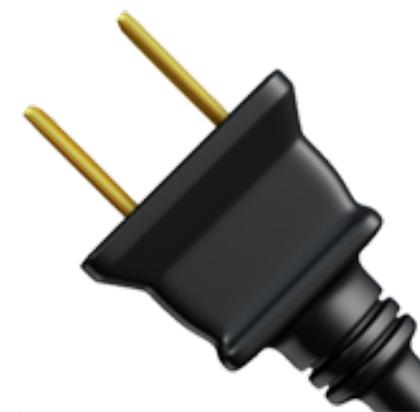
Meta *Teaser Token*

eyJhbGciOiJFZERTQSIssInR5cCI6IkpxVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V50no2TwtzWFFCZkw4b3d6dFRDS1RtN2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMuIiwiY2FwIjoiT1ZFUlSSVRFIIn1dLCJleHAI0jkyNTY5Mzk1MDUsImlzcyI6ImRpZDprZXk6ejZNa3A1RXN60XMyTUhzcVl2TG9jY3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjoxNjM5Nja4MjkzLCJwcmYi0ltdfQ.MgYarLqy7RmQ1AIrqYL6cFy9z7a5WIAU--TYARPSgir0Szvar3_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 ≠ Blockchain

How to Power a New Internet



web3 ≠ Blockchain

P2P, IPFS, Matrix

How to Power a New Internet



web3 ≠ Blockchain

P2P, IPFS, Matrix

Open, accessible, trustless, portable

How to Power a New Internet



web3 ≠ Blockchain

P2P, IPFS, Matrix

Open, accessible, trustless, portable

User sovereignty: mobile browsers, local-first

How to Power a New Internet



web3 ≠ Blockchain

P2P, IPFS, Matrix

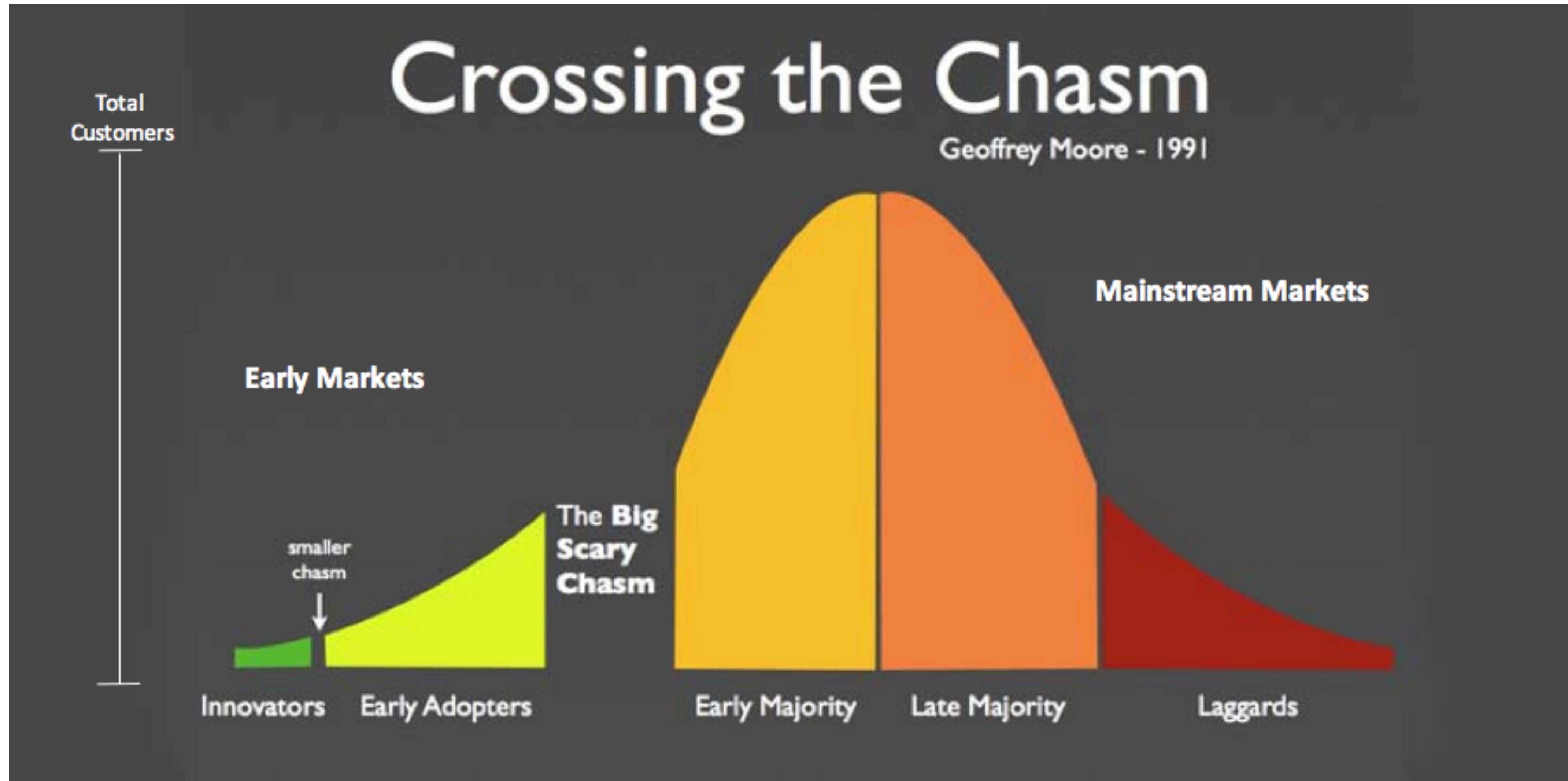
Open, accessible, trustless, portable

User sovereignty: mobile browsers, local-first

...and so on

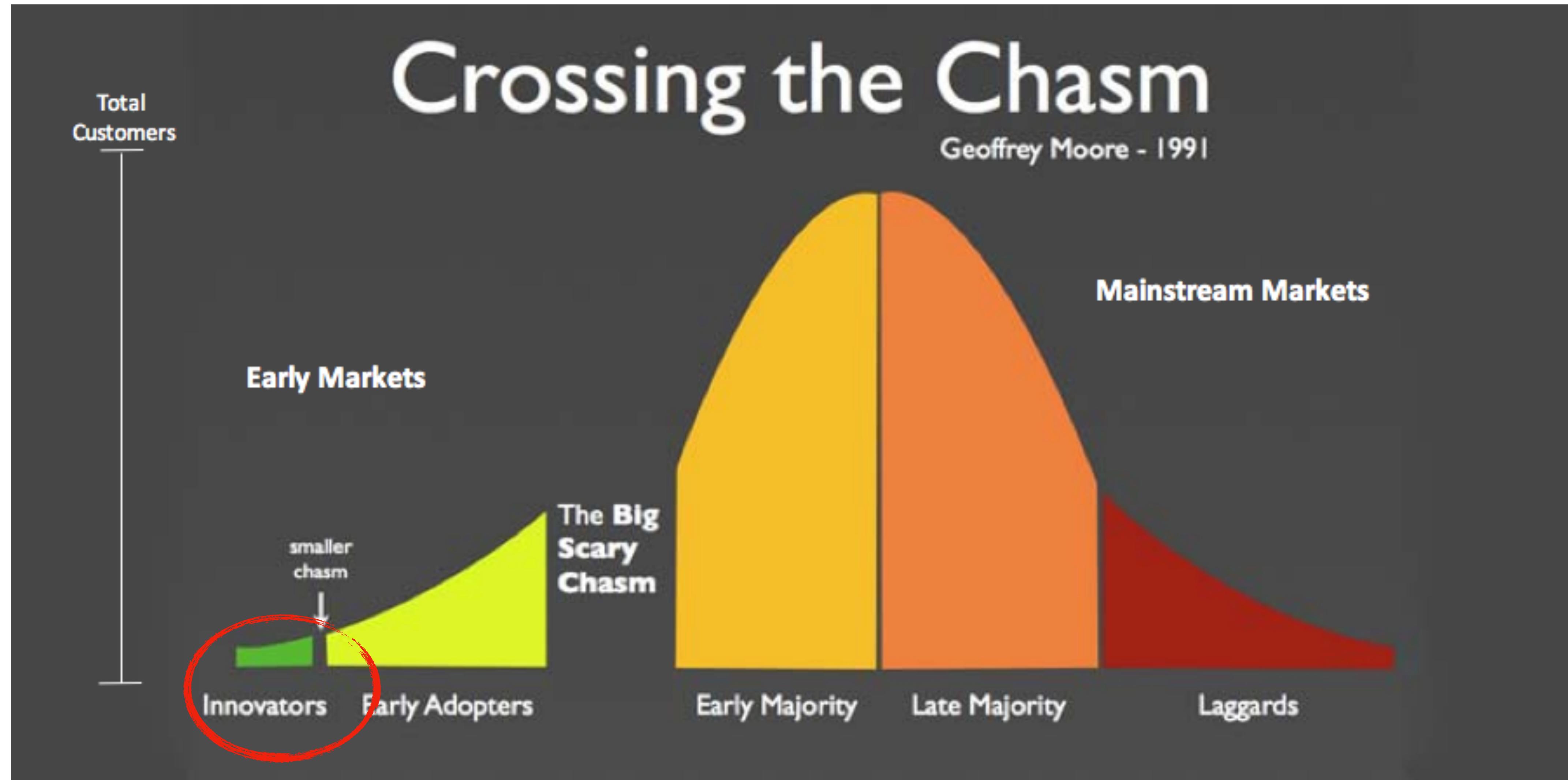
How to Power a New Internet 

It's Still Extremely Early Days!



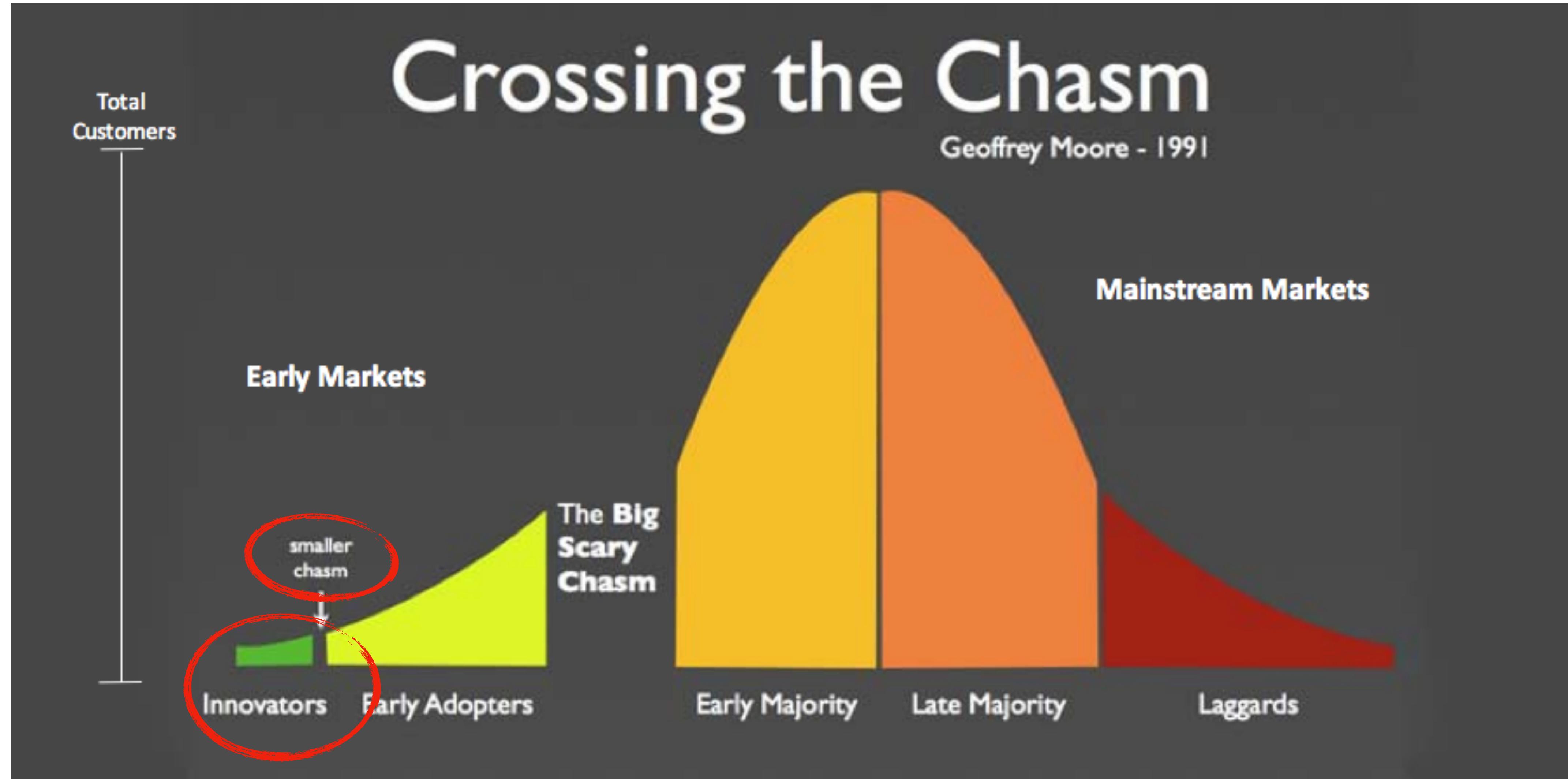
How to Power a New Internet 

It's Still Extremely Early Days!



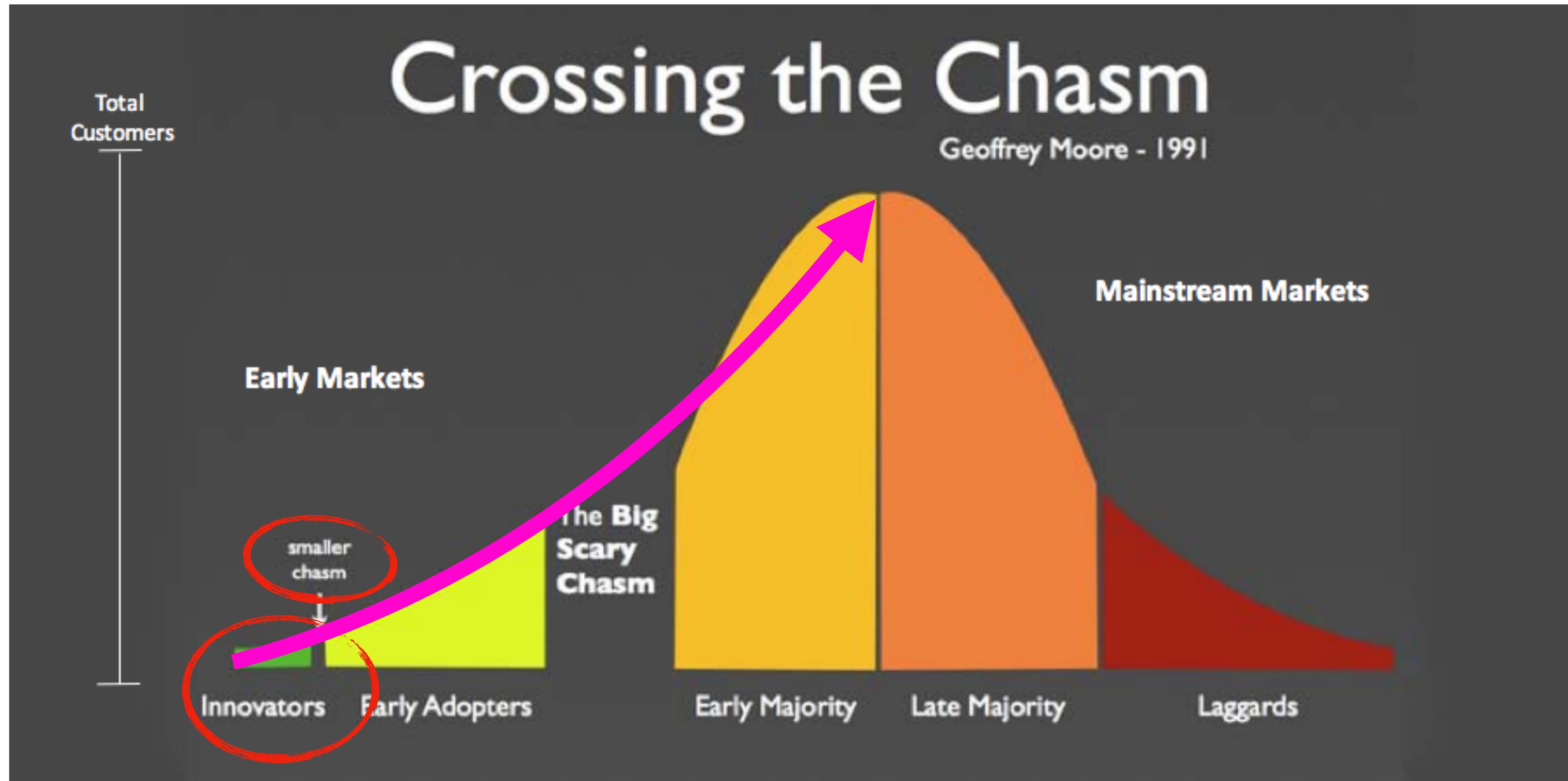
How to Power a New Internet 

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

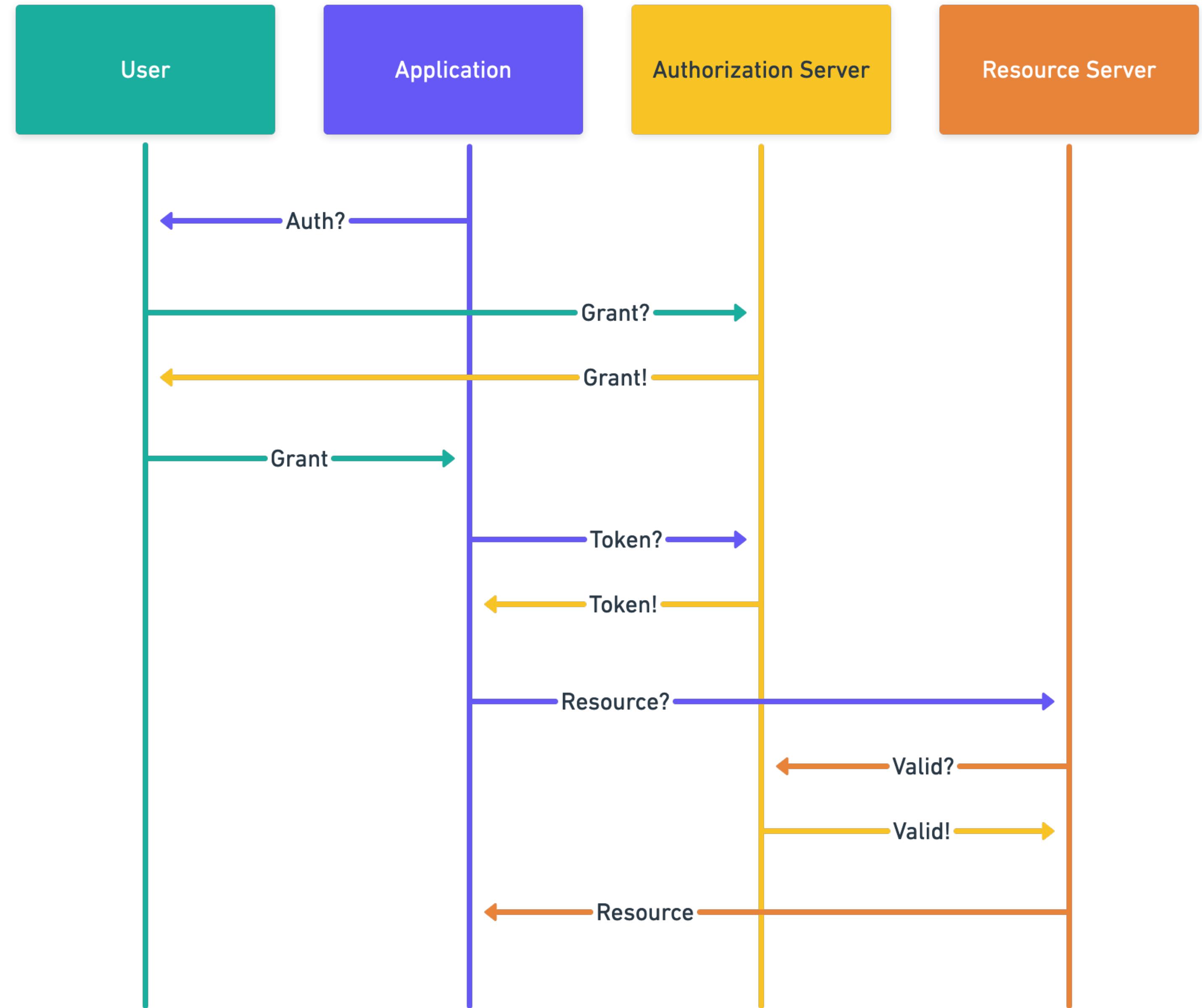
Easier, more secure, & more open than:

OAuth, X.509, SAML,

MetaMask, WalletConnect, etc

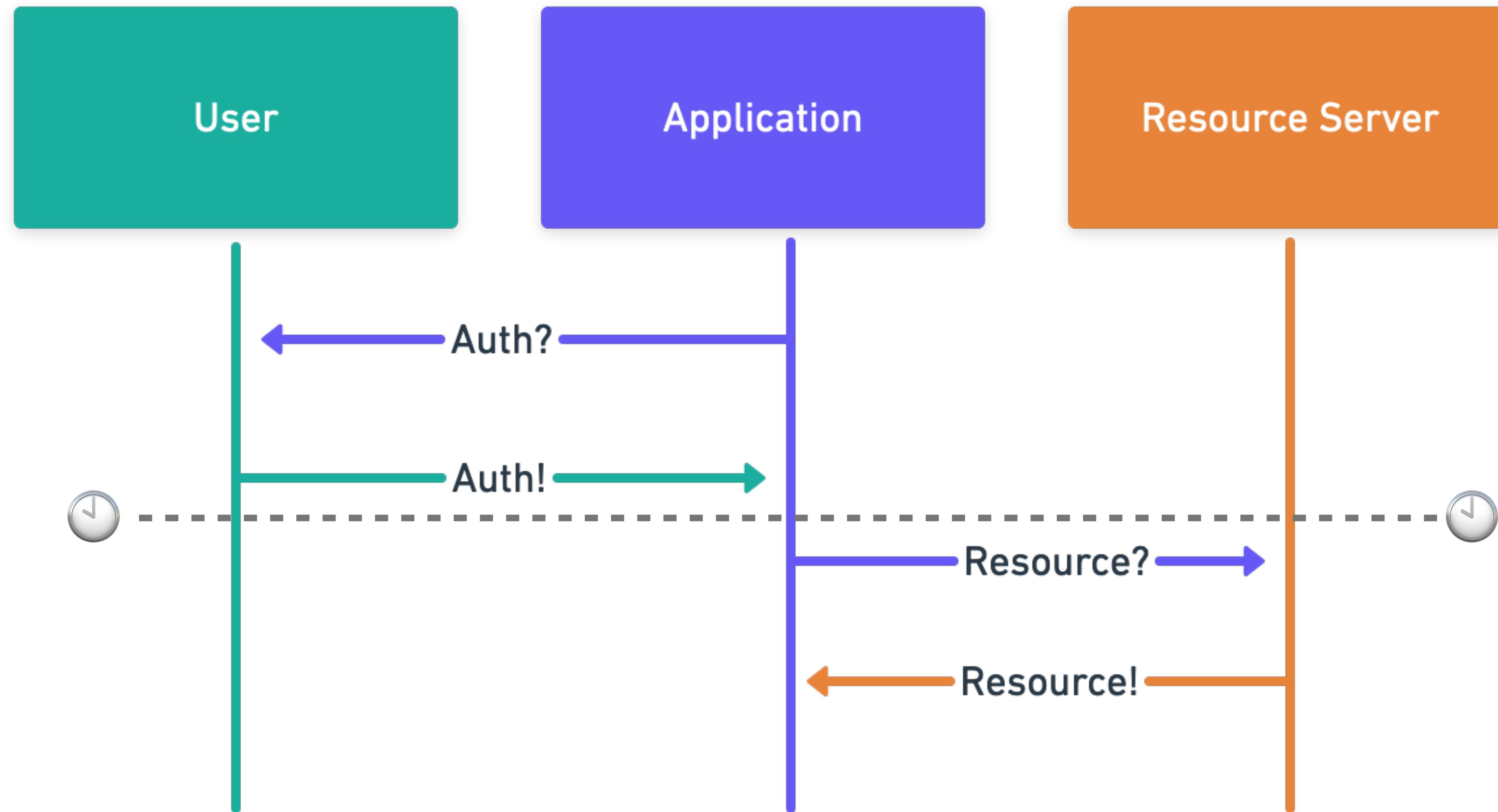
How to Power a New Internet

OAuth Sequence



How to Power a New Internet

UCAN Sequence



Design Principles



Design Principles



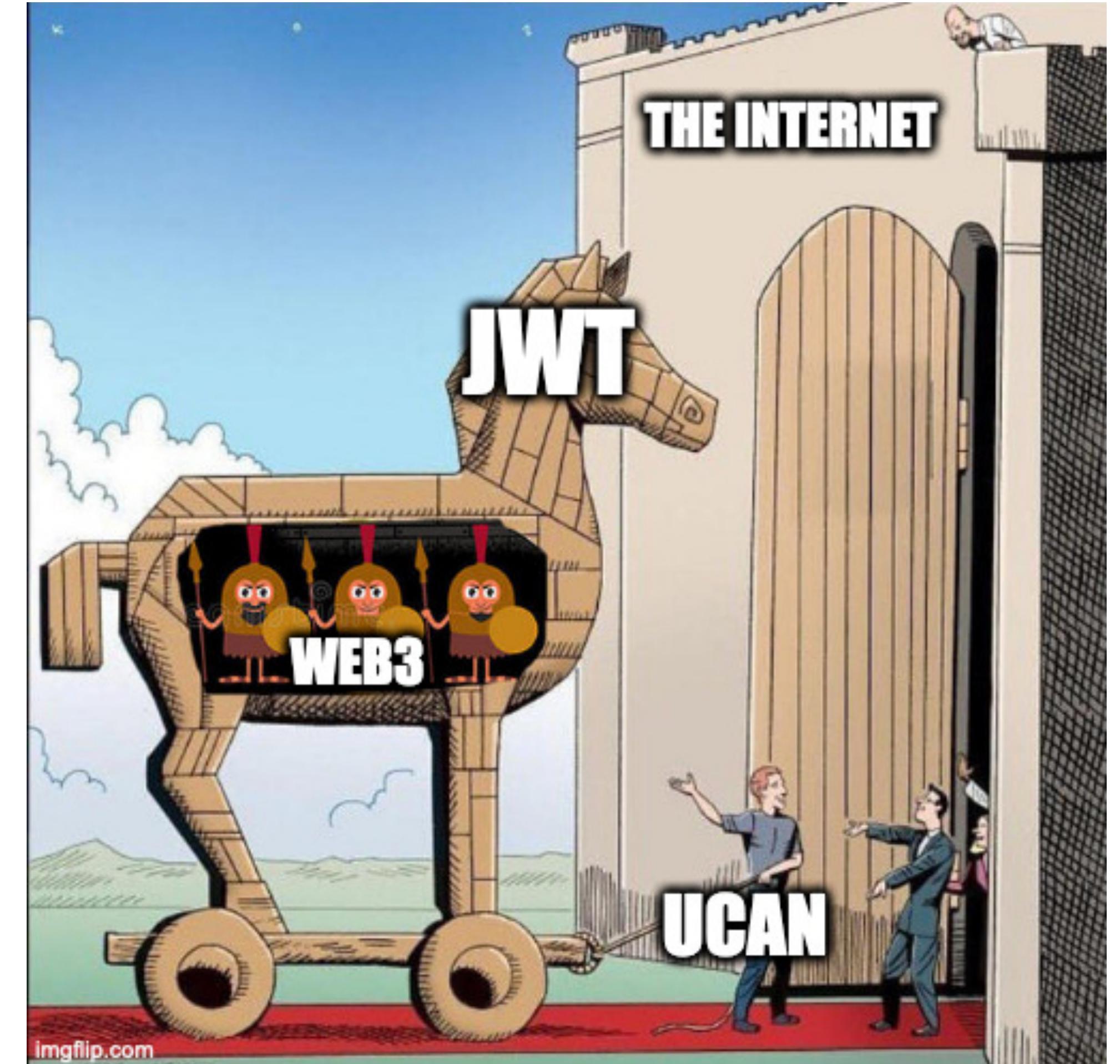
Adoption

Design Principles

Adoption

Be a Trojan Horse

Build on widely supported, familiar, well-understood standards

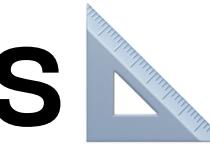


Design Principles



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

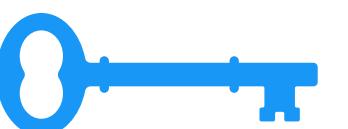
UCAN

Non-Extractable Browser Keys



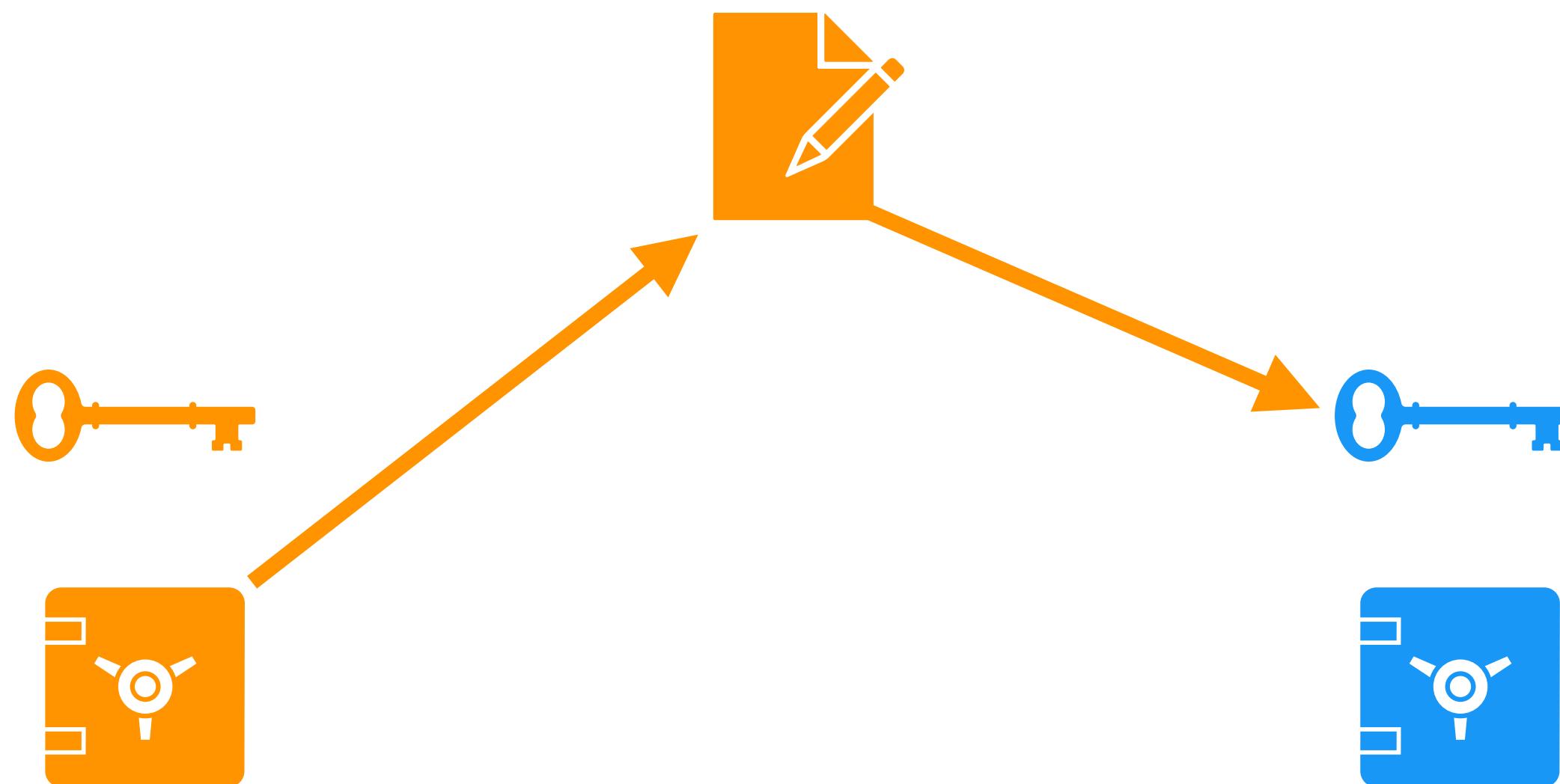
UCAN

Non-Extractable Browser Keys



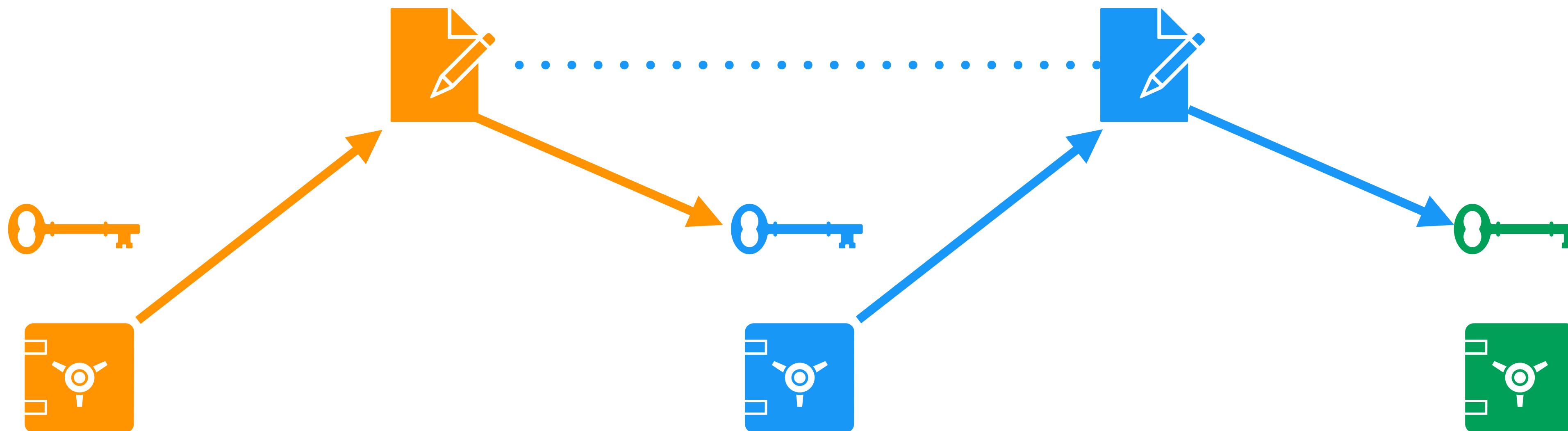
UCAN

Non-Extractable Browser Keys



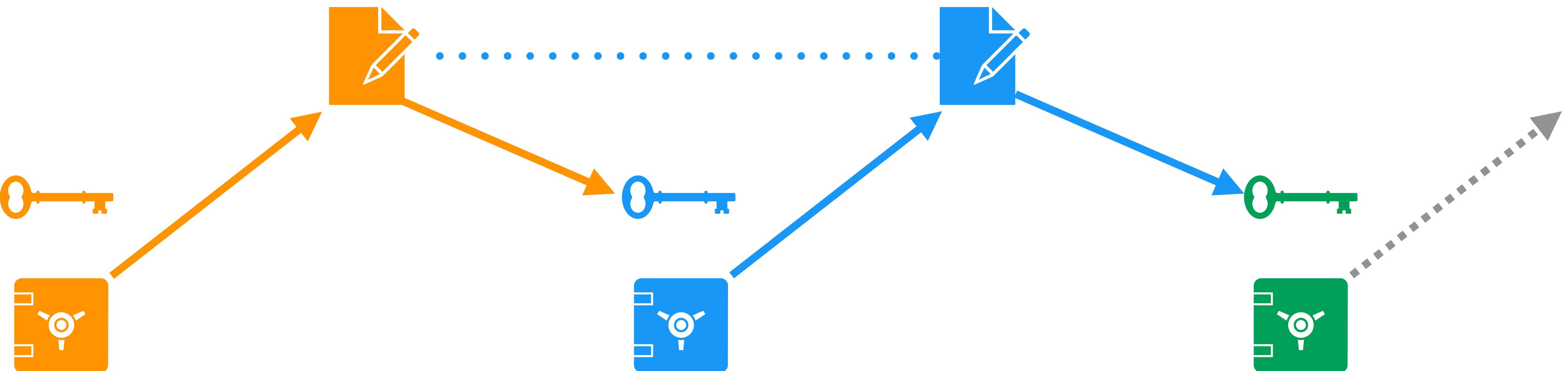
UCAN

Non-Extractable Browser Keys



UCAN

Non-Extractable Browser Keys

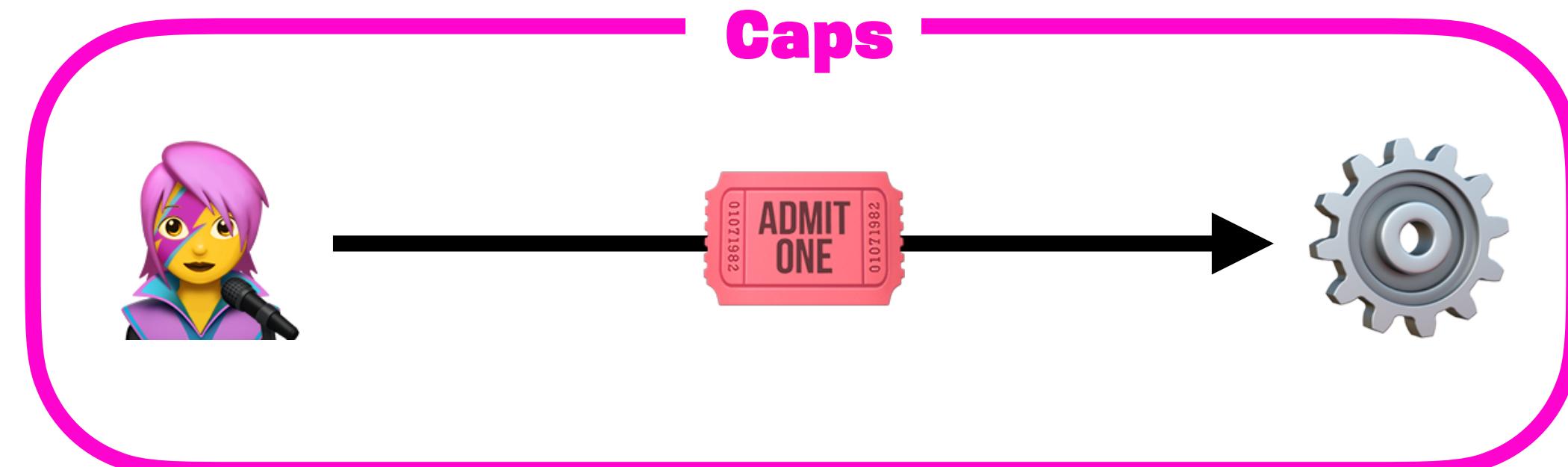
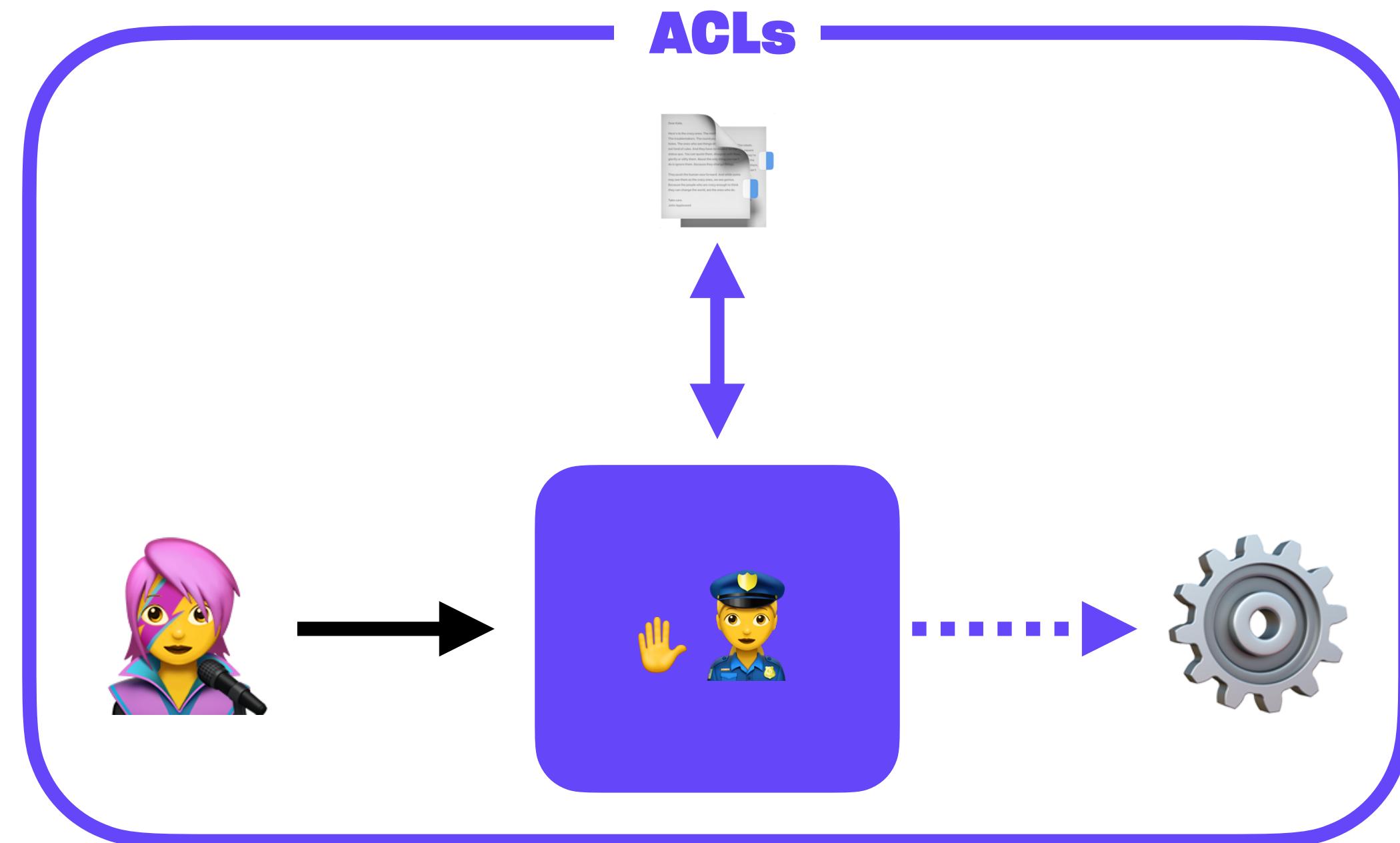


UCAN

Auth Models

UCAN

Auth Models



UCAN

ACL Read & Write

UCAN

ACL Read & Write



UCAN

ACL Read & Write



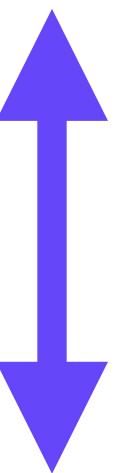
UCAN

ACL Read & Write



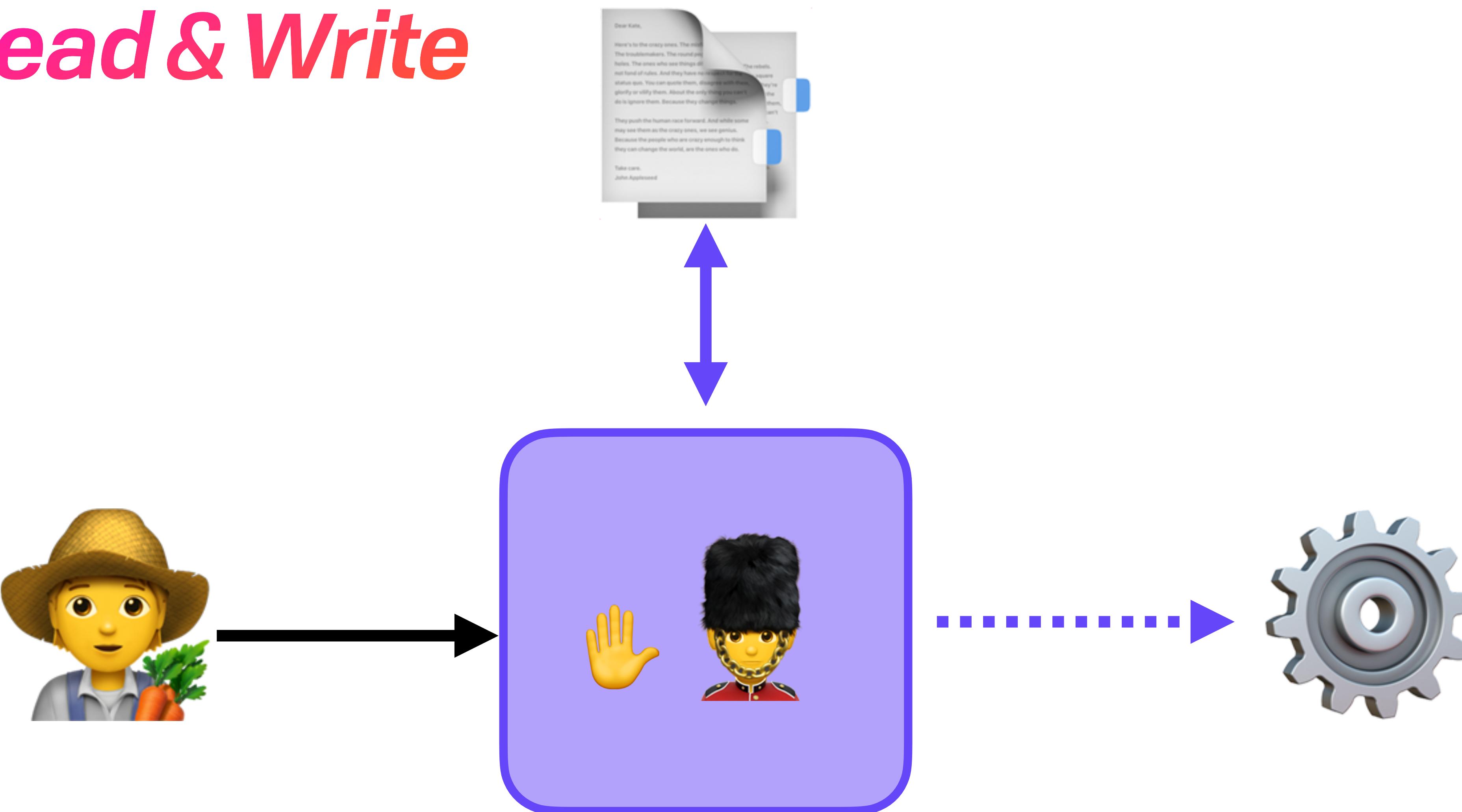
UCAN

ACL Read & Write



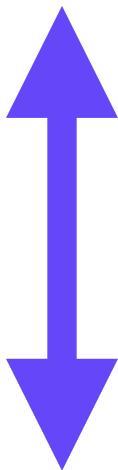
UCAN

ACL Read & Write



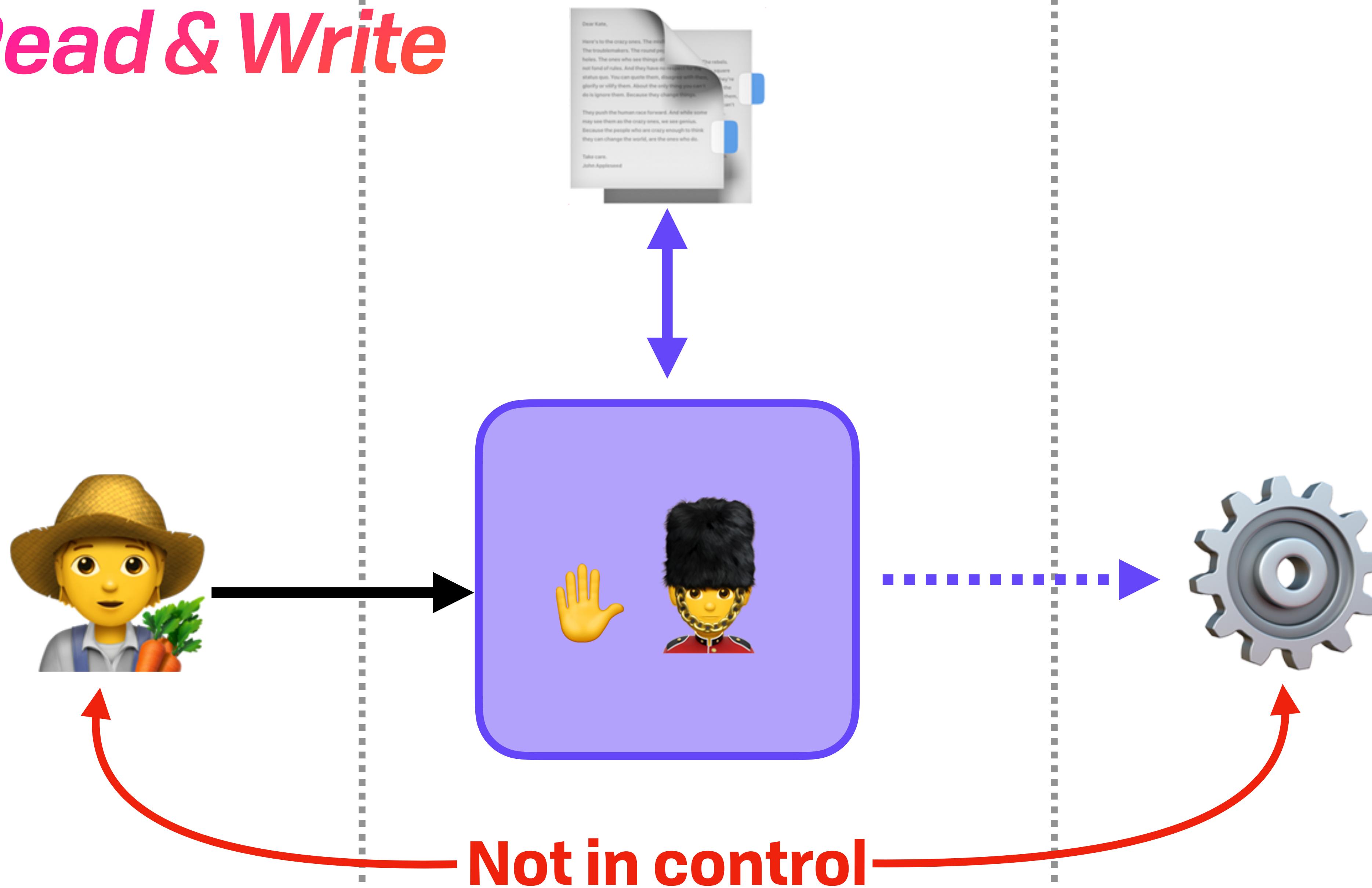
UCAN

ACL Read & Write



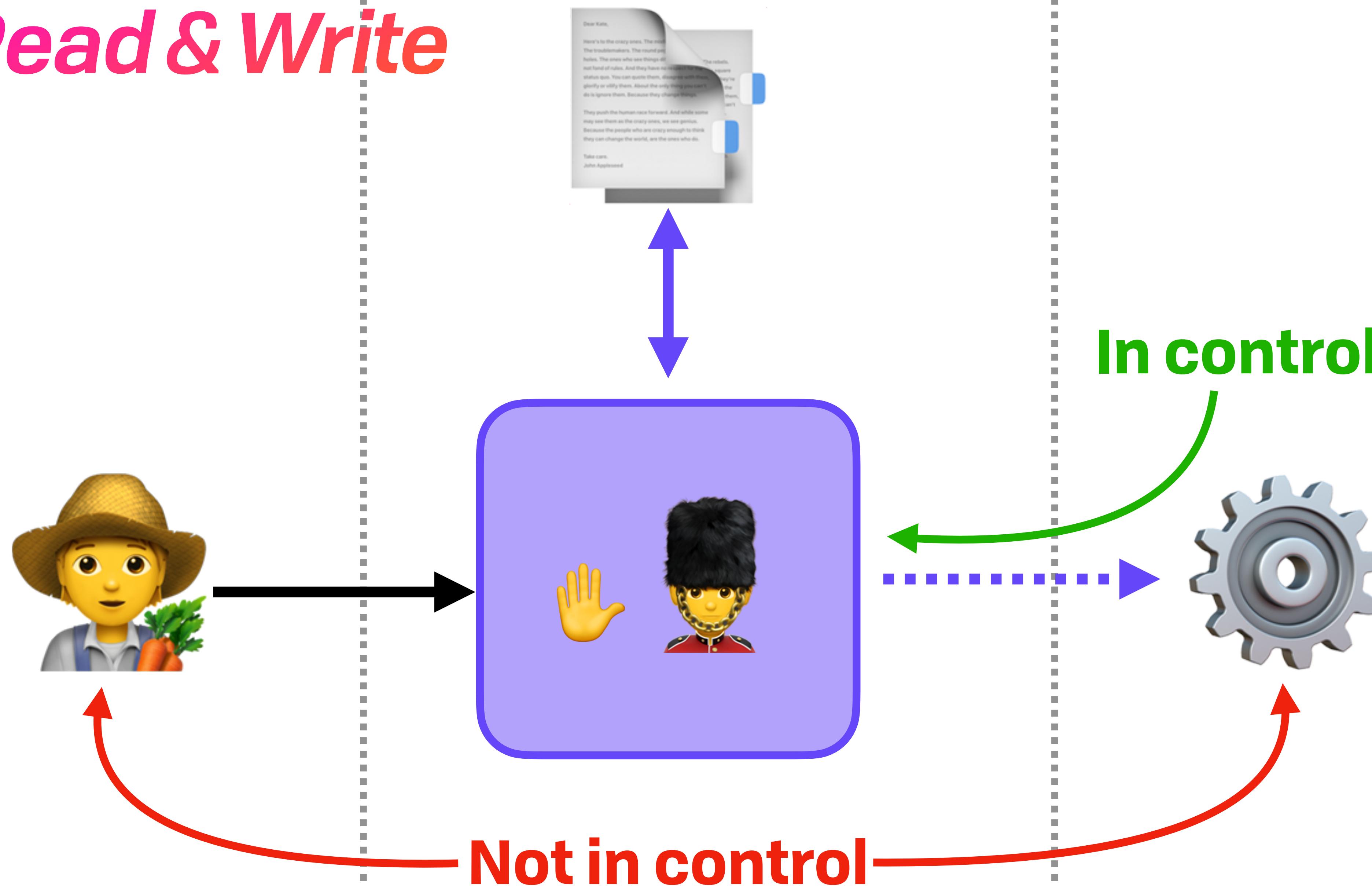
UCAN

ACL Read & Write



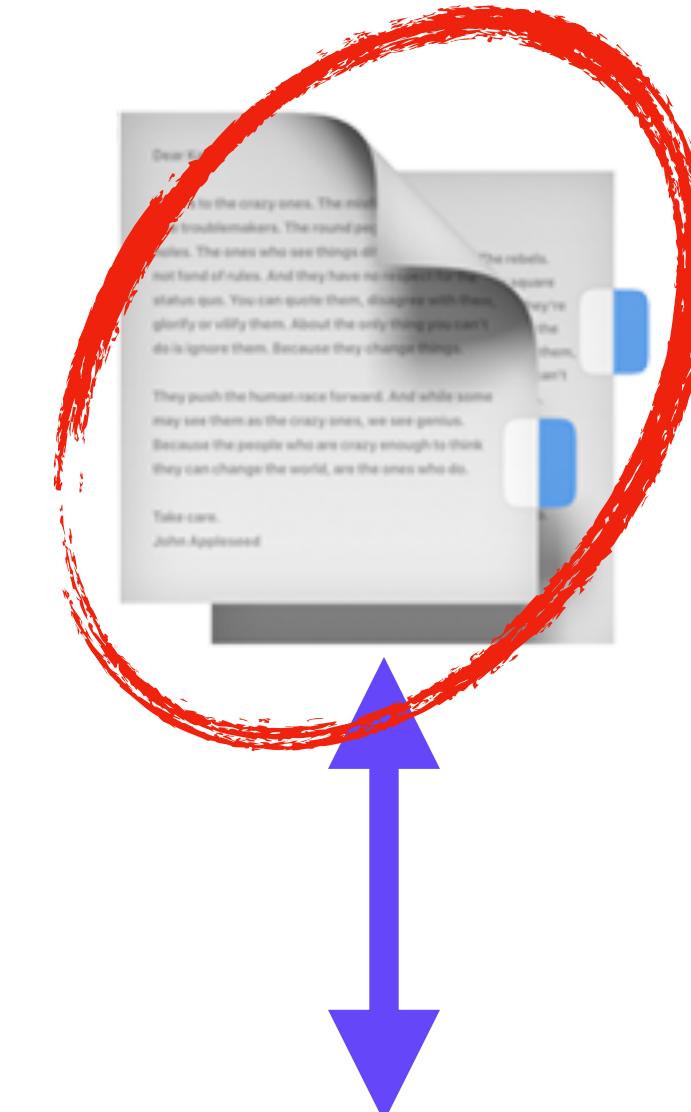
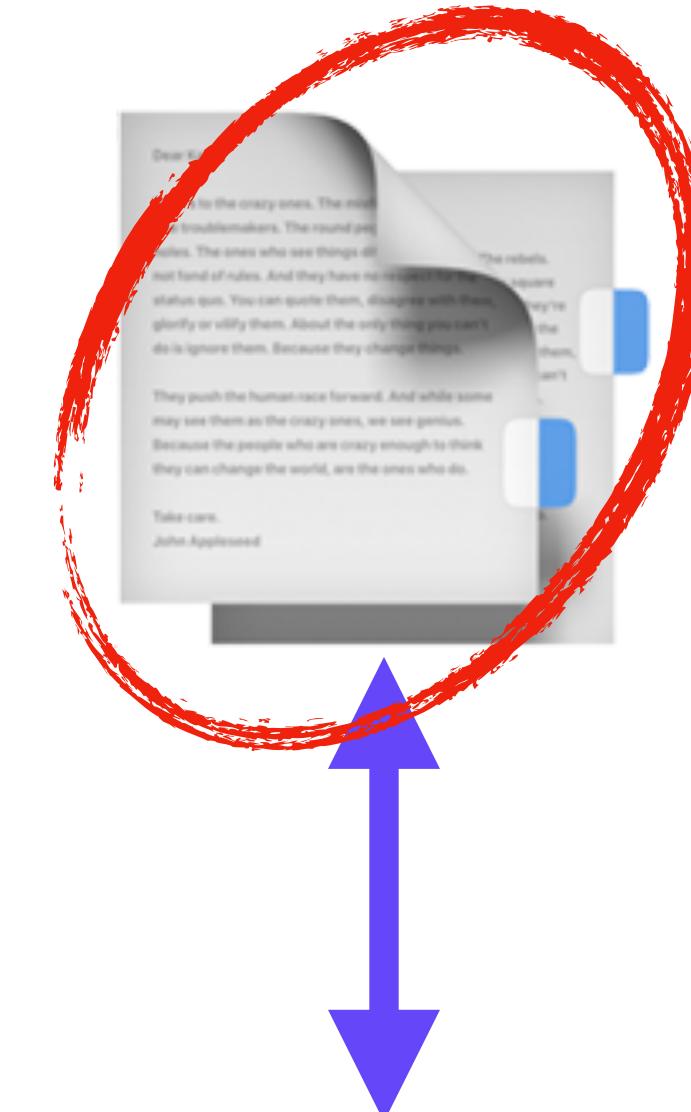
UCAN

ACL Read & Write

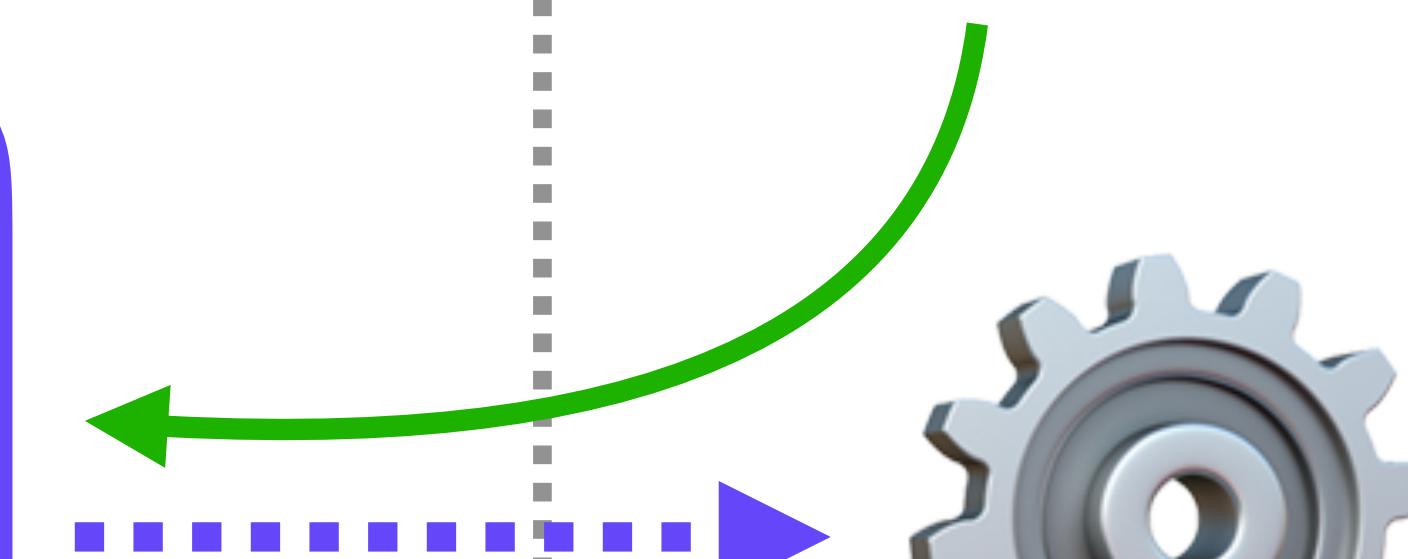


UCAN

ACL Read & Write



In control

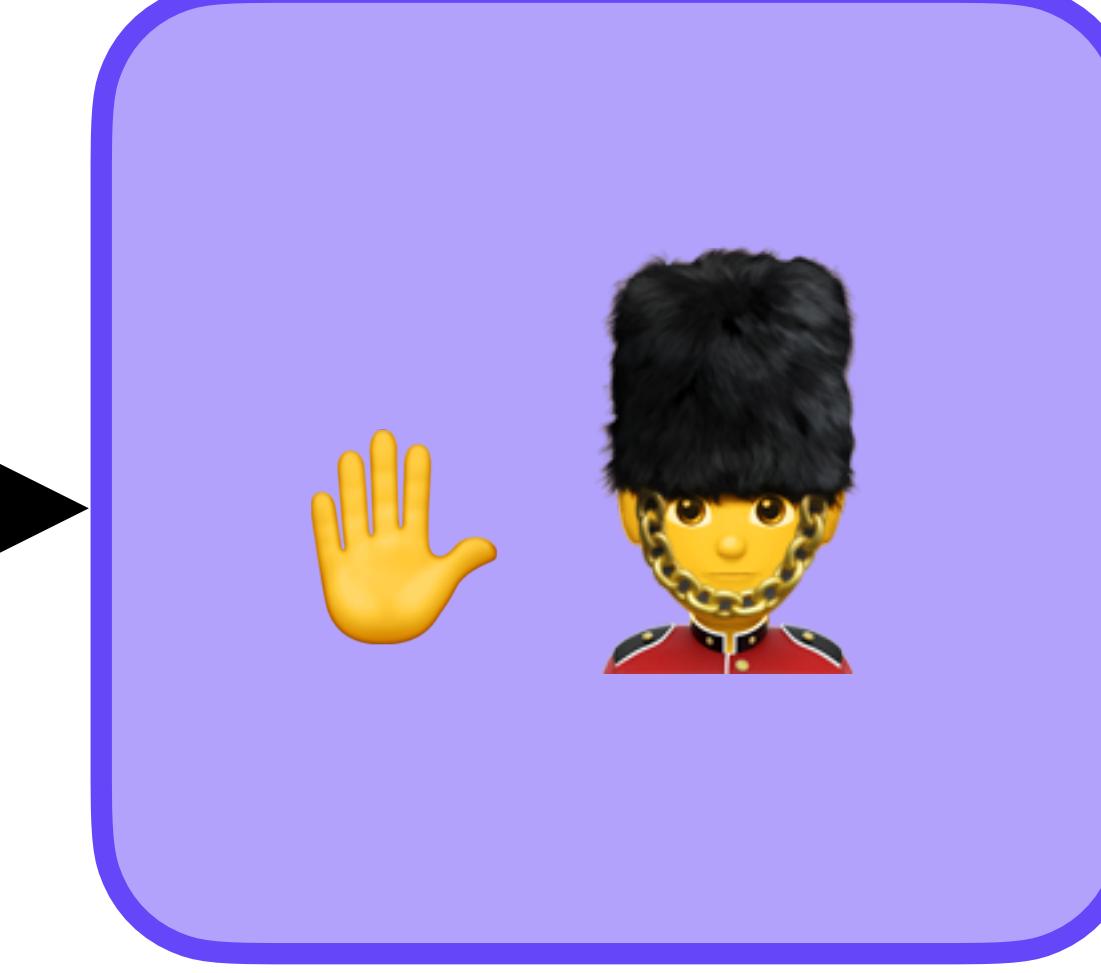


Not in control

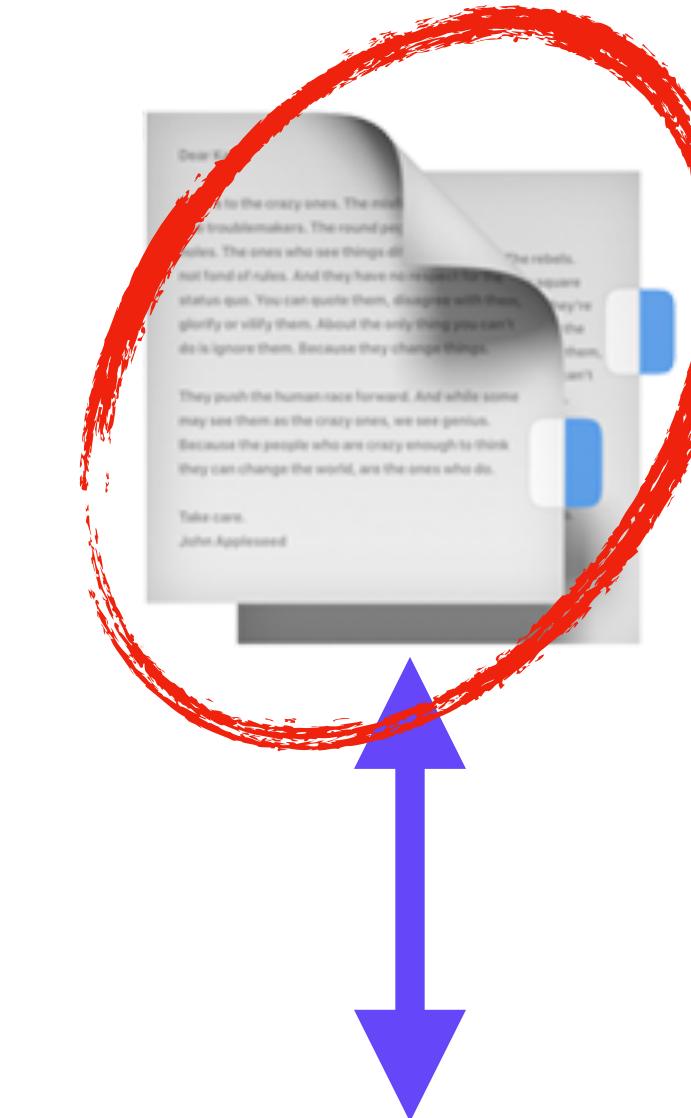


UCAN

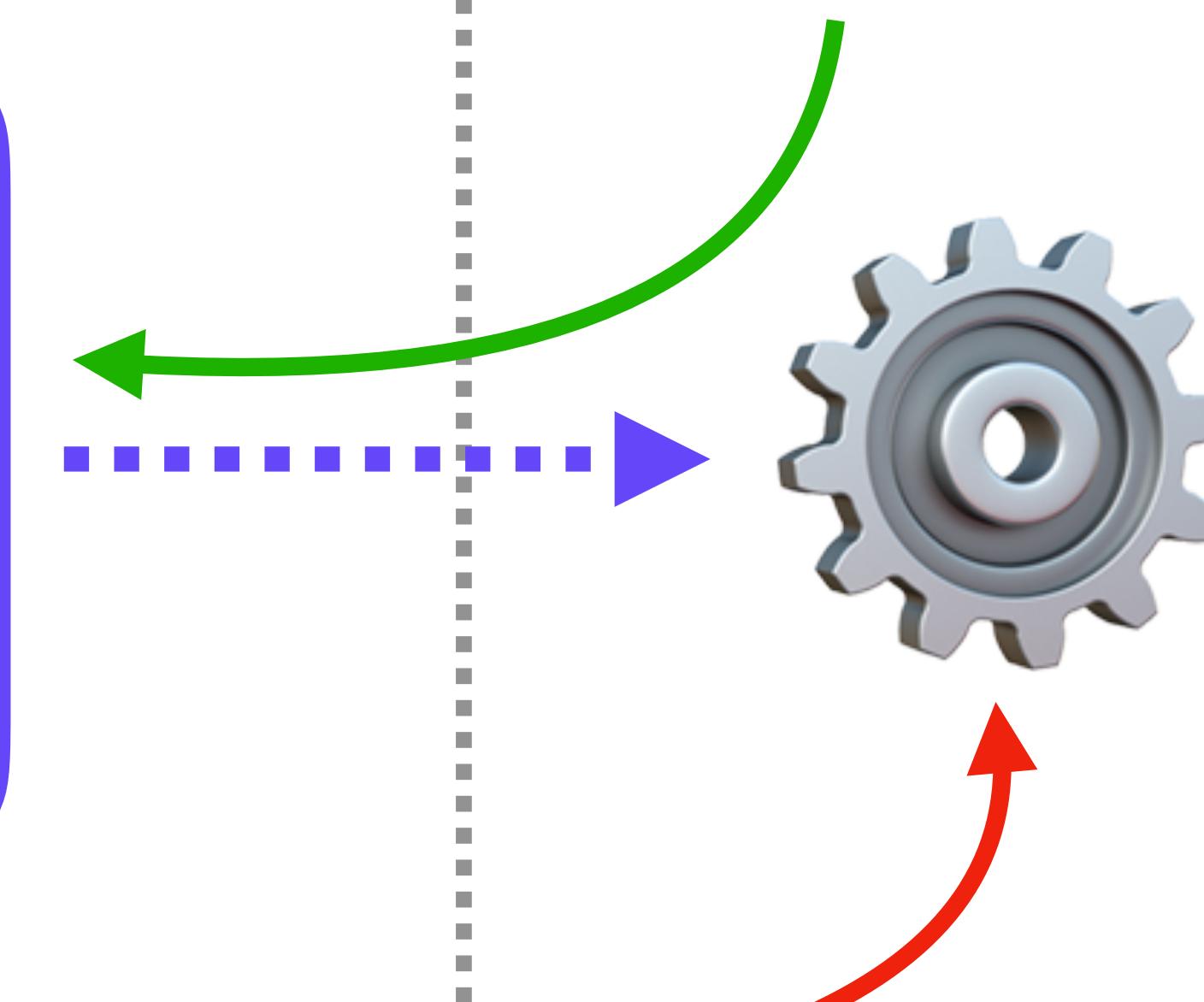
ACL Read & Write



Not in control



In control

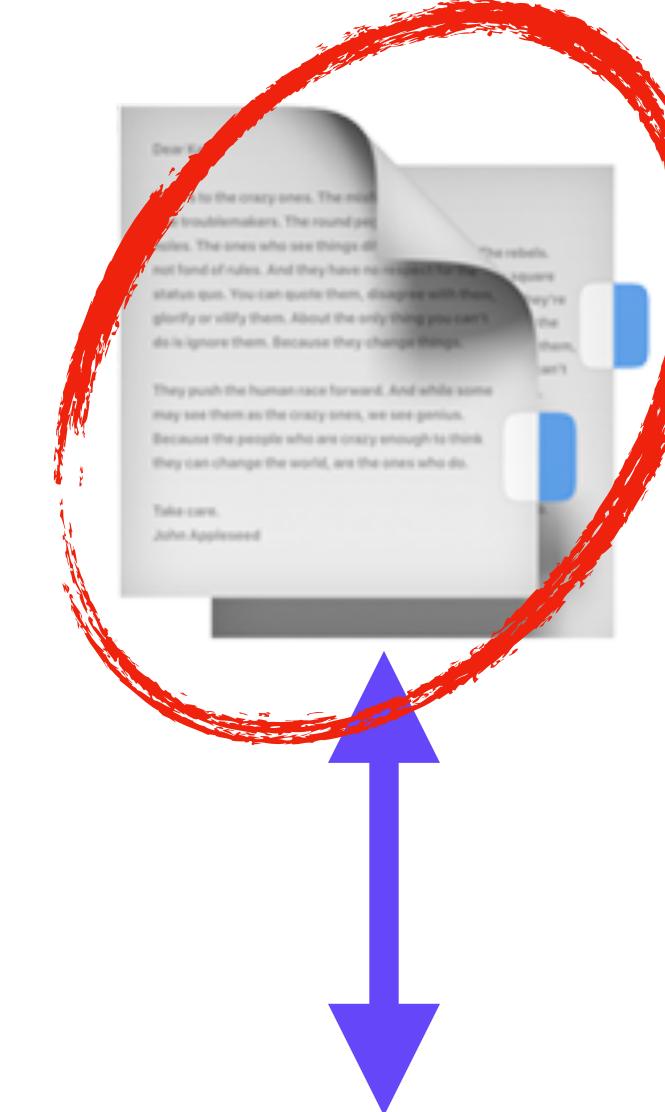
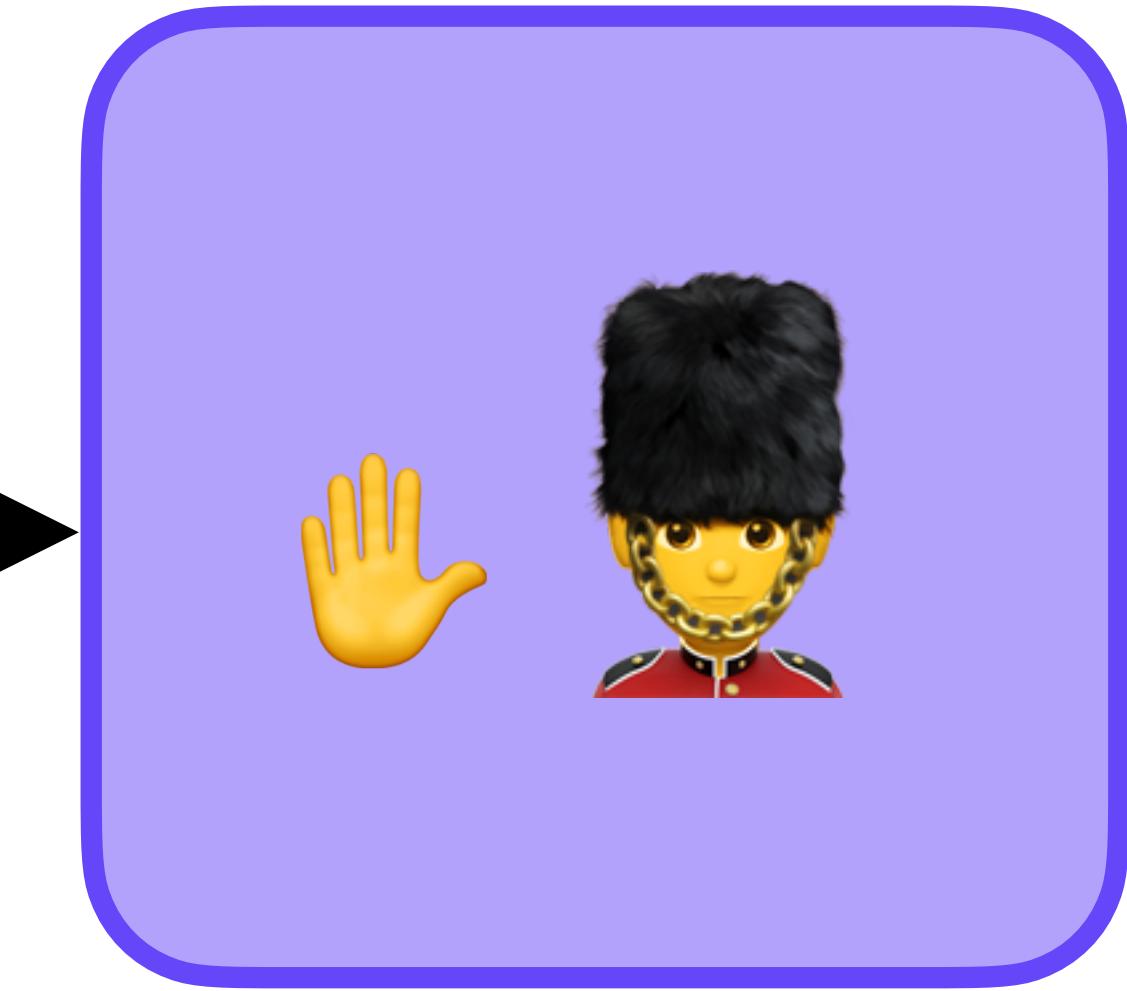


UCAN

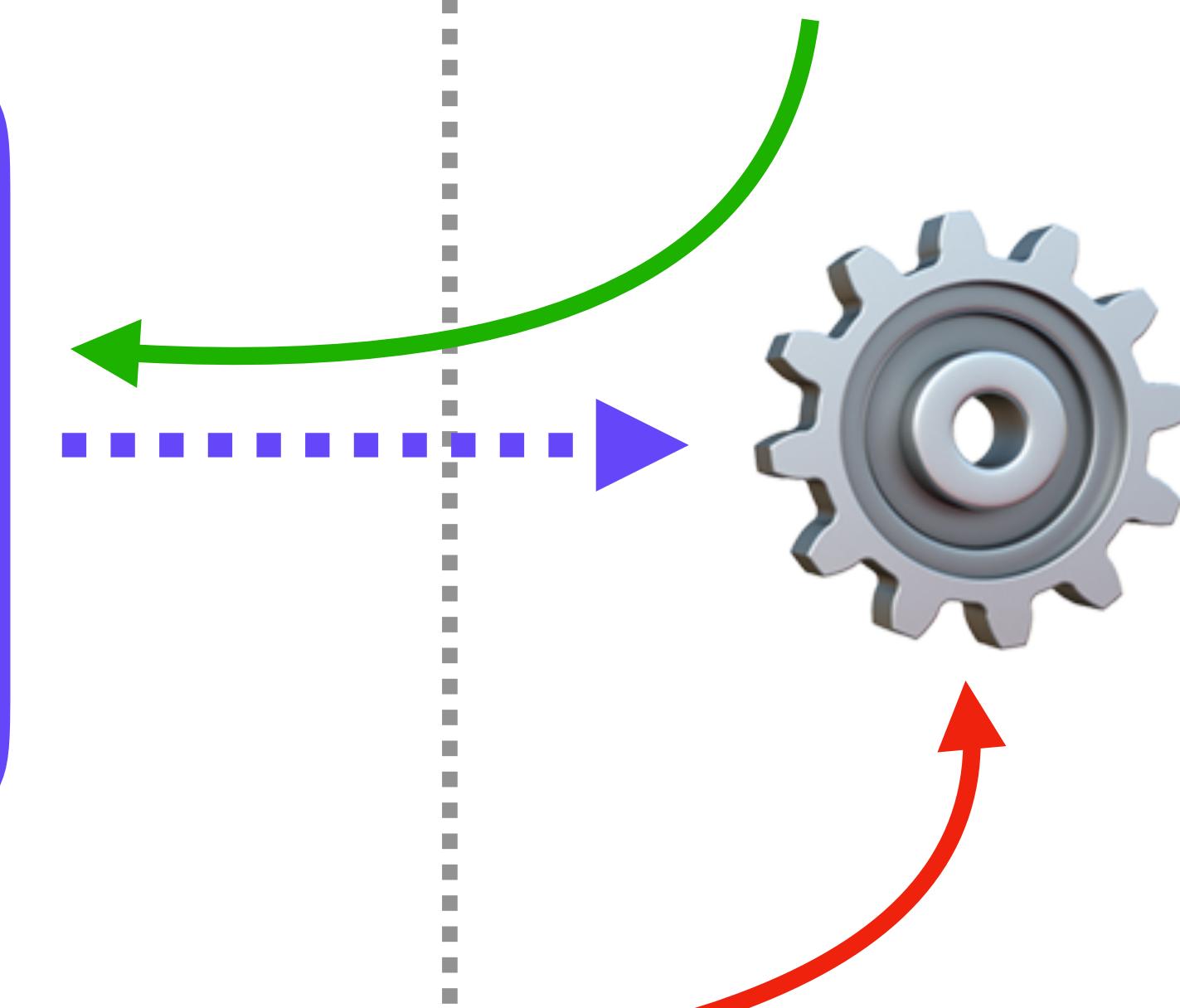
ACL Read & Write



Not in control



In control



UCAN

From Actors to Capabilities

UCAN

From Actors to Capabilities



UCAN

From Actors to Capabilities



UCAN

From Actors to Capabilities



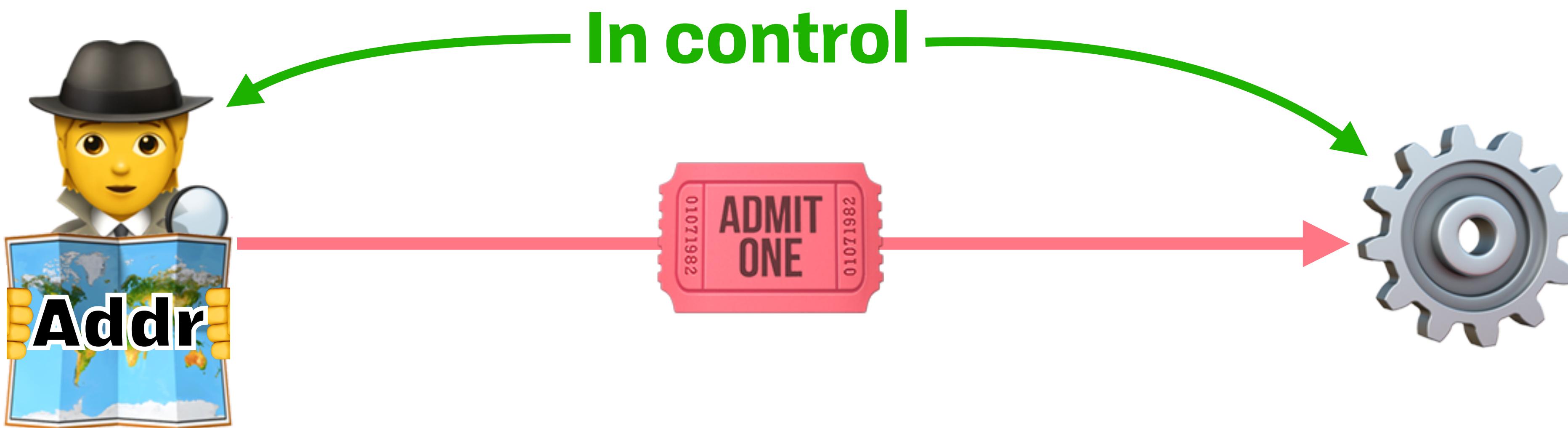
UCAN

From Actors to Capabilities



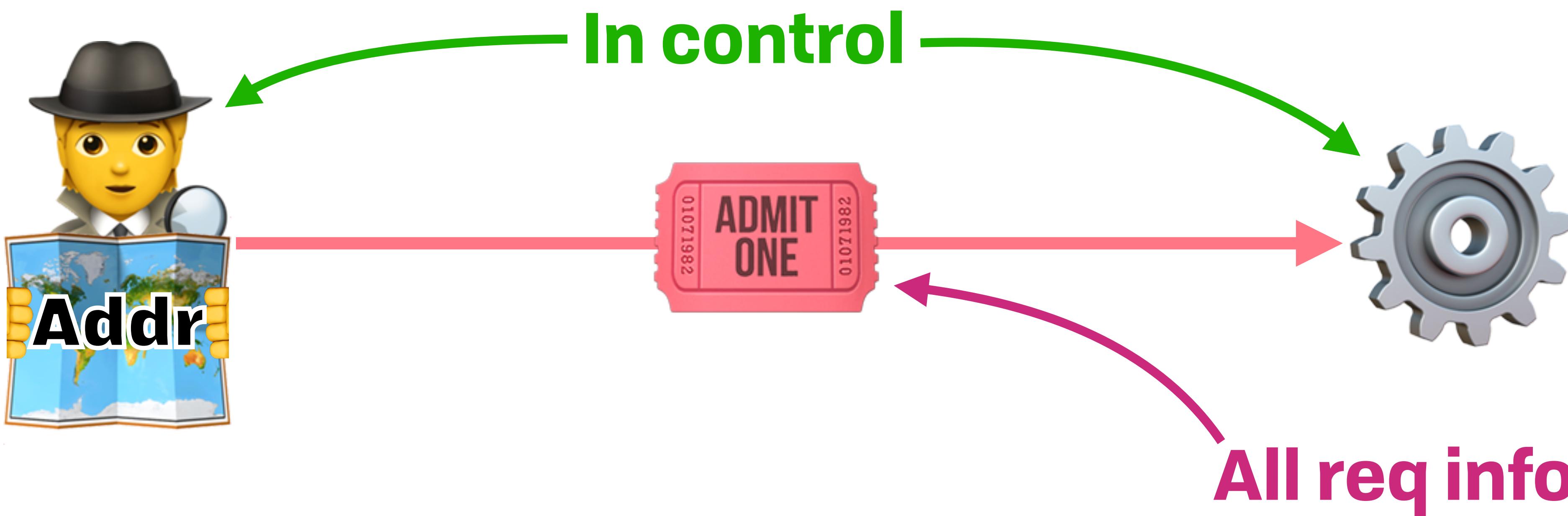
UCAN

From Actors to Capabilities



UCAN

From Actors to Capabilities



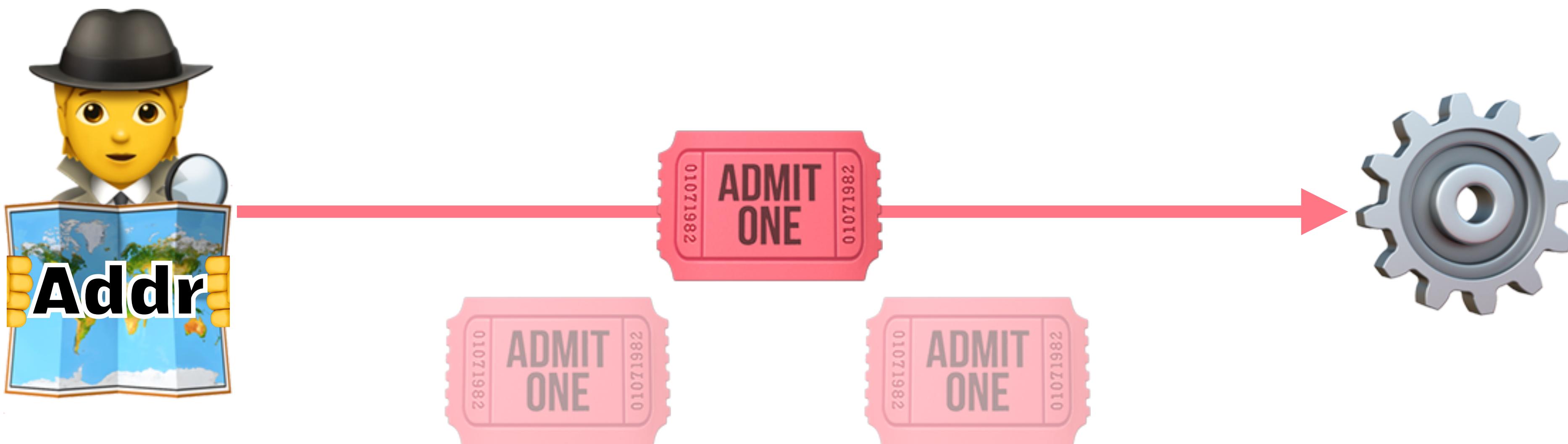
UCAN

From Actors to Capabilities



UCAN

From Actors to Capabilities



UCAN

From Actors to Capabilities



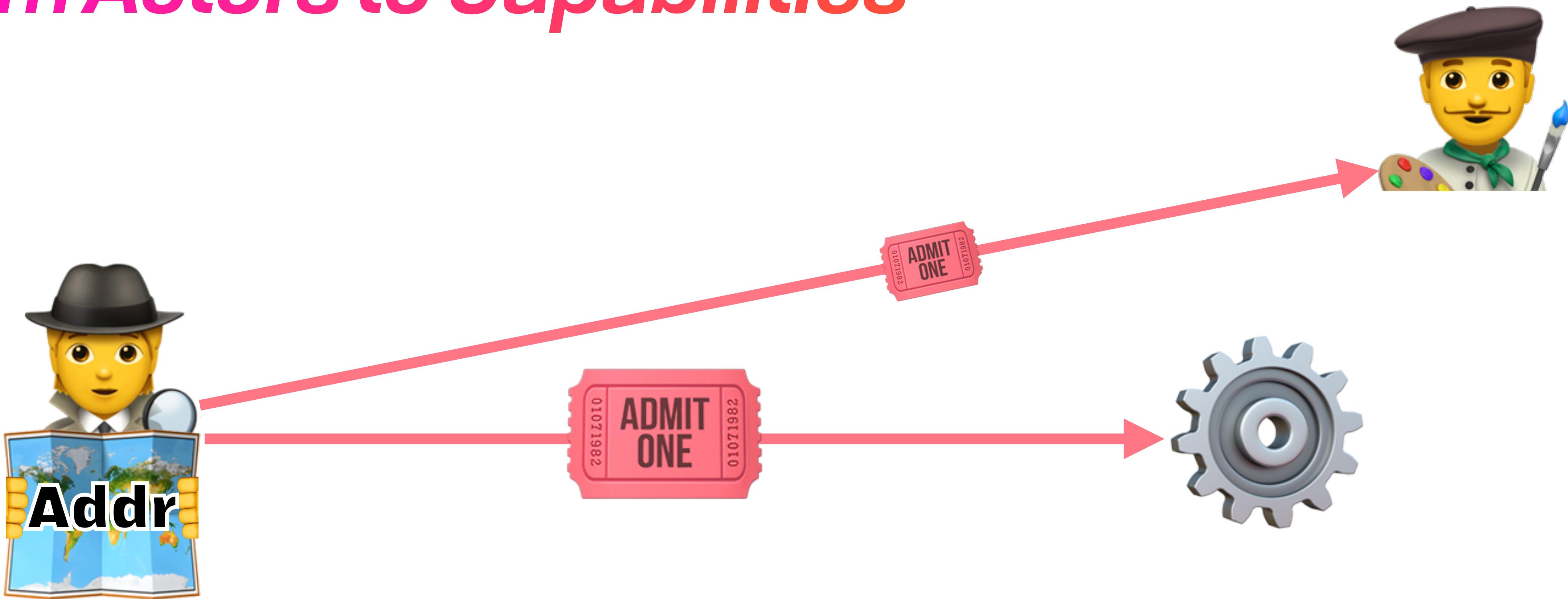
UCAN

From Actors to Capabilities



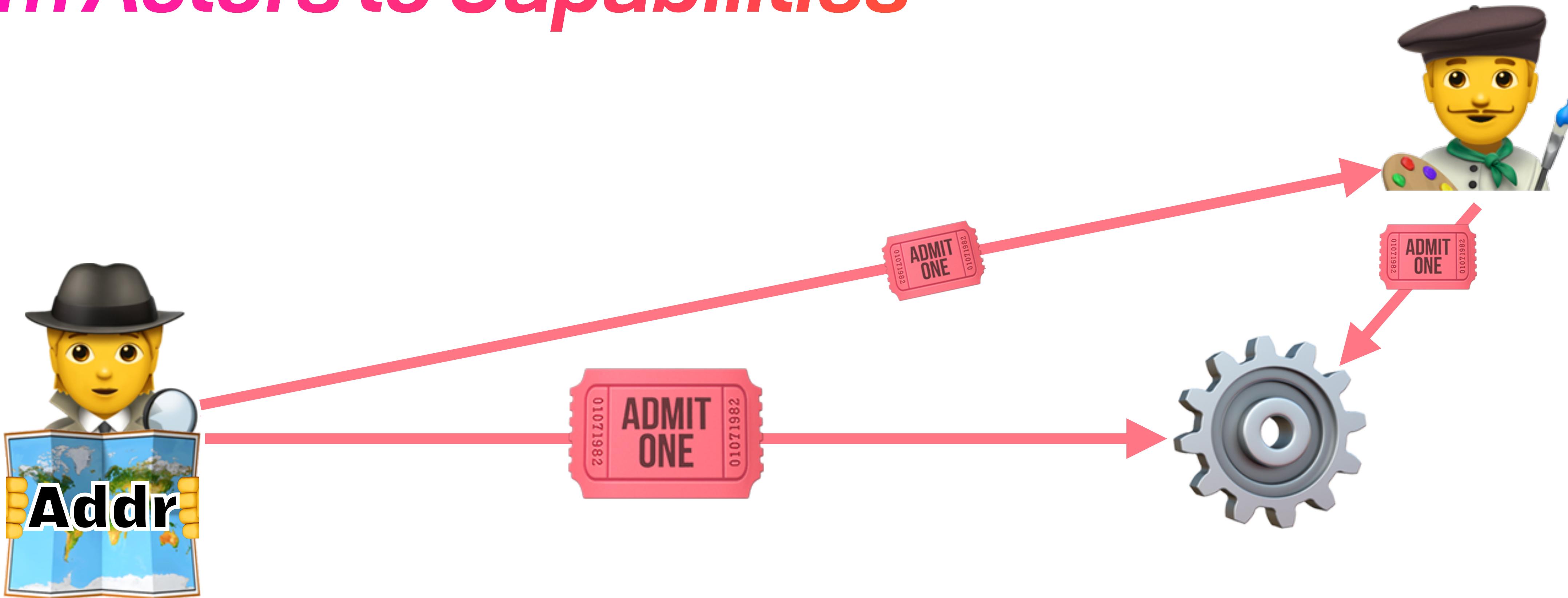
UCAN

From Actors to Capabilities



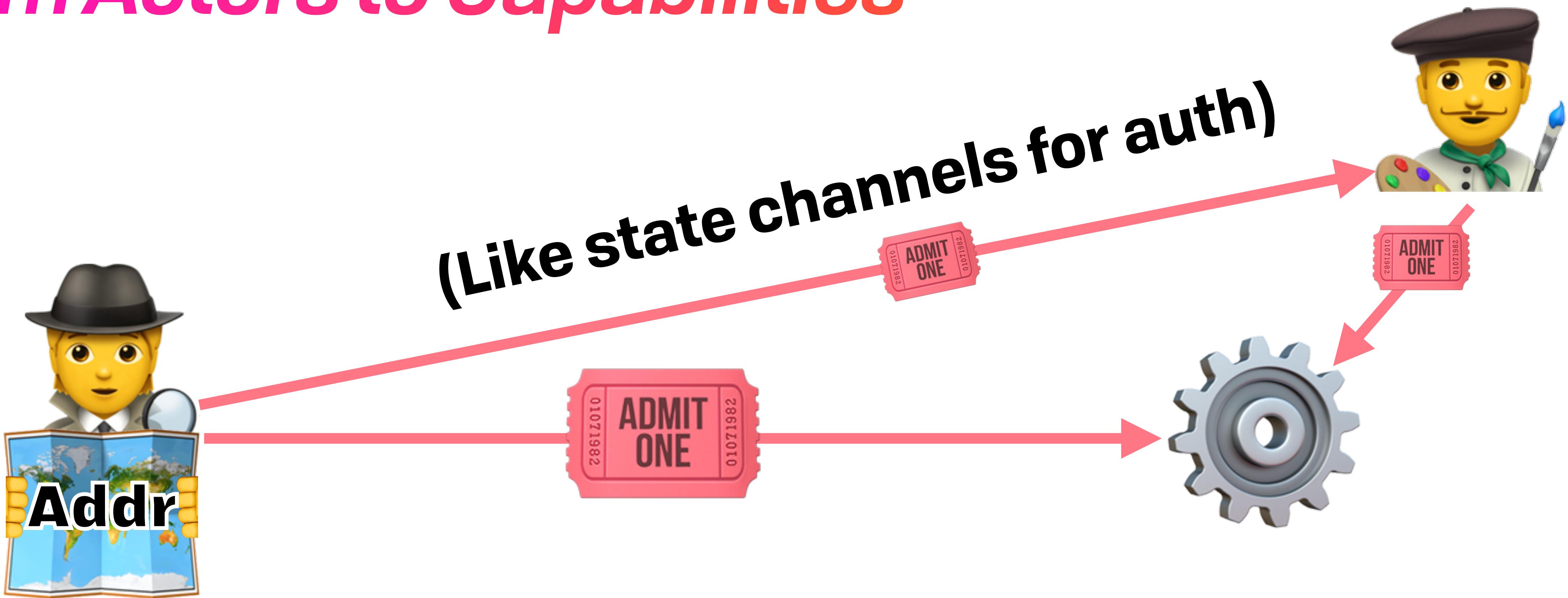
UCAN

From Actors to Capabilities



UCAN

From Actors to Capabilities



UCAN

Rights Amplification

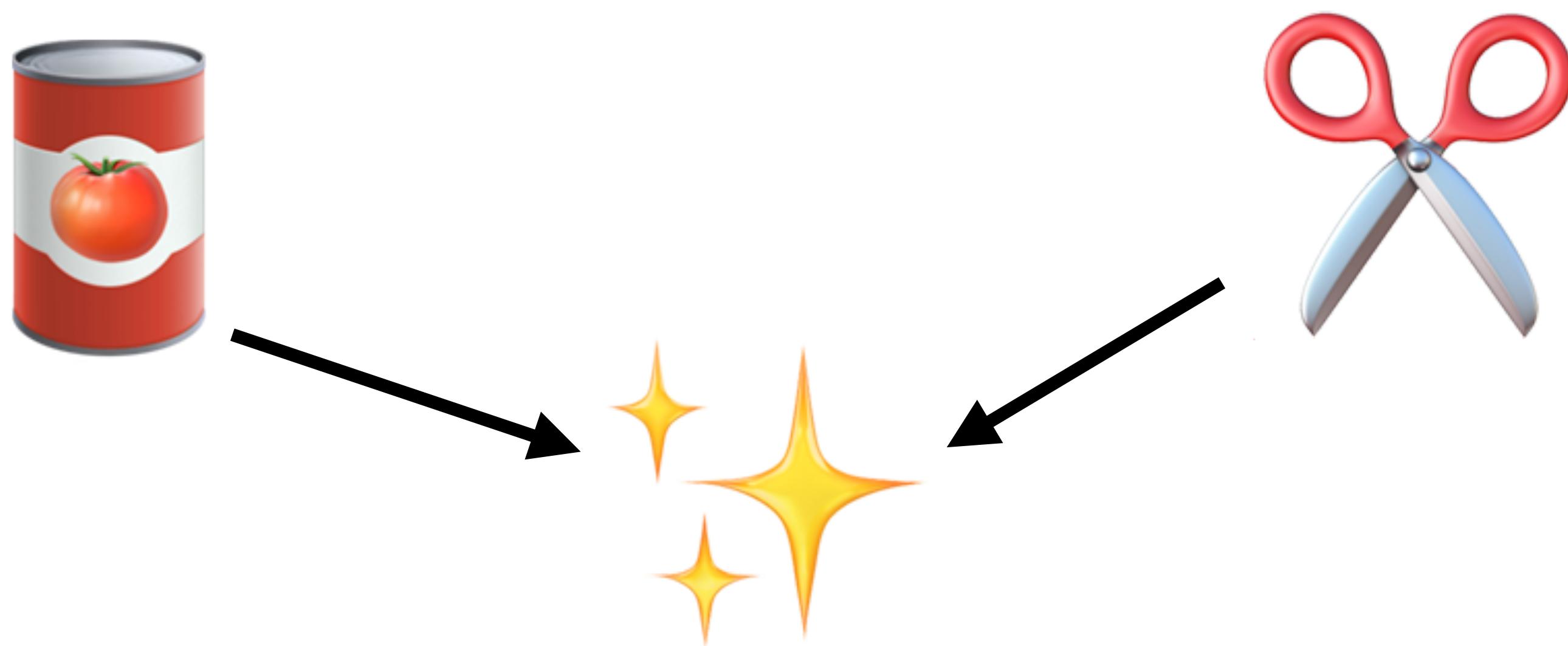
UCAN

Rights Amplification



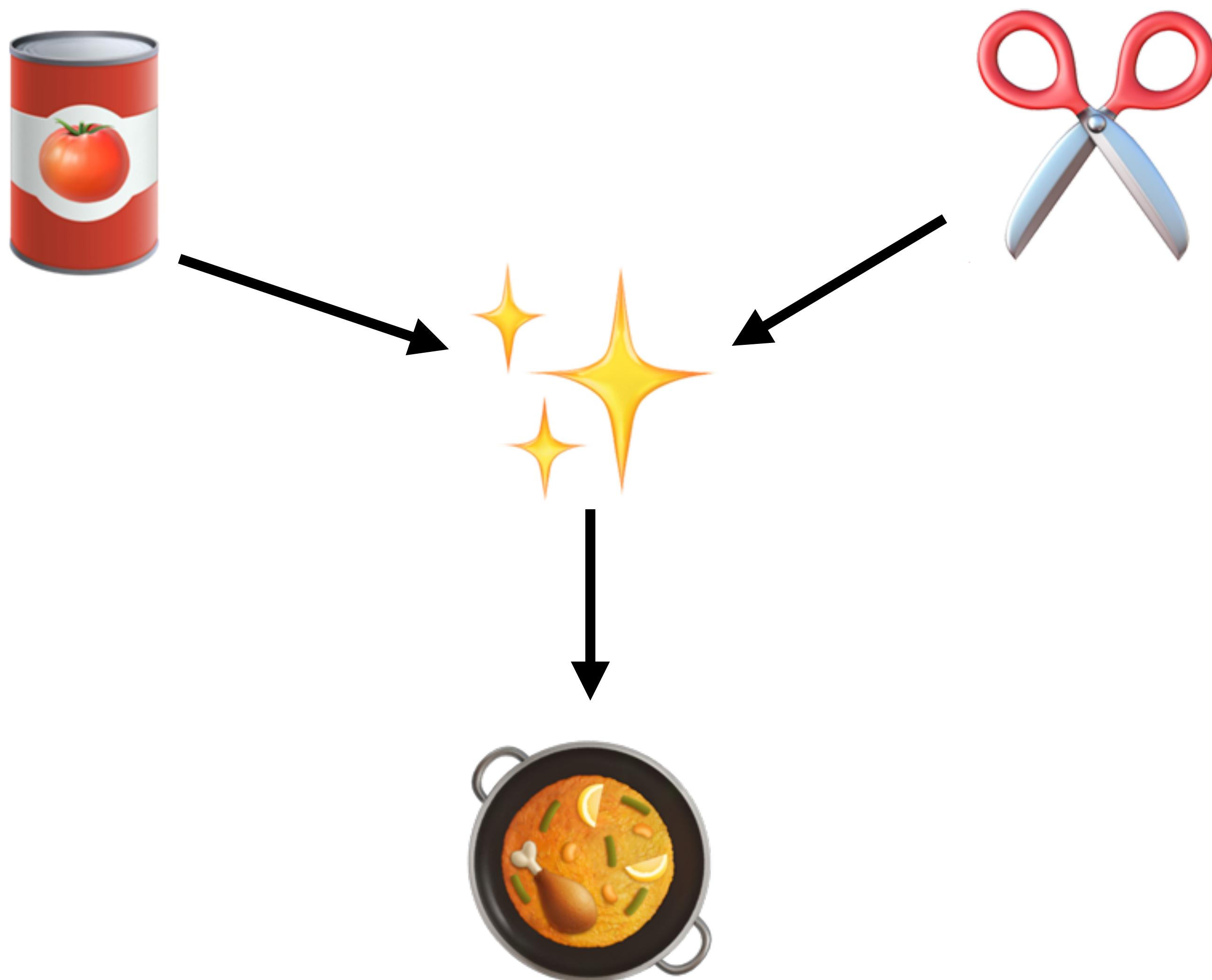
UCAN

Rights Amplification



UCAN

Rights Amplification



UCAN

JWT → UCAN

UCAN

JWT → UCAN

Header

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

UCAN

JWT → UCAN

Header

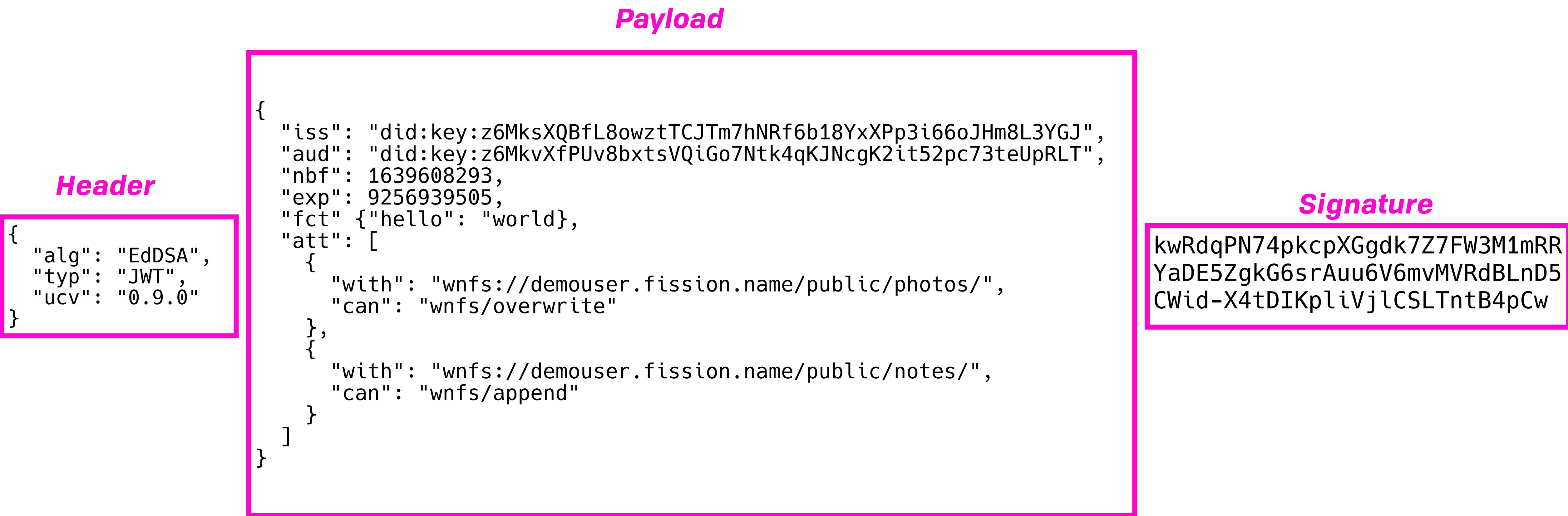
```
{  
  "alg": "EdDSA",  
  "typ": "JWT",  
  "ucv": "0.9.0"  
}
```

Payload

```
{  
  "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"  
    }  
  ]  
}
```

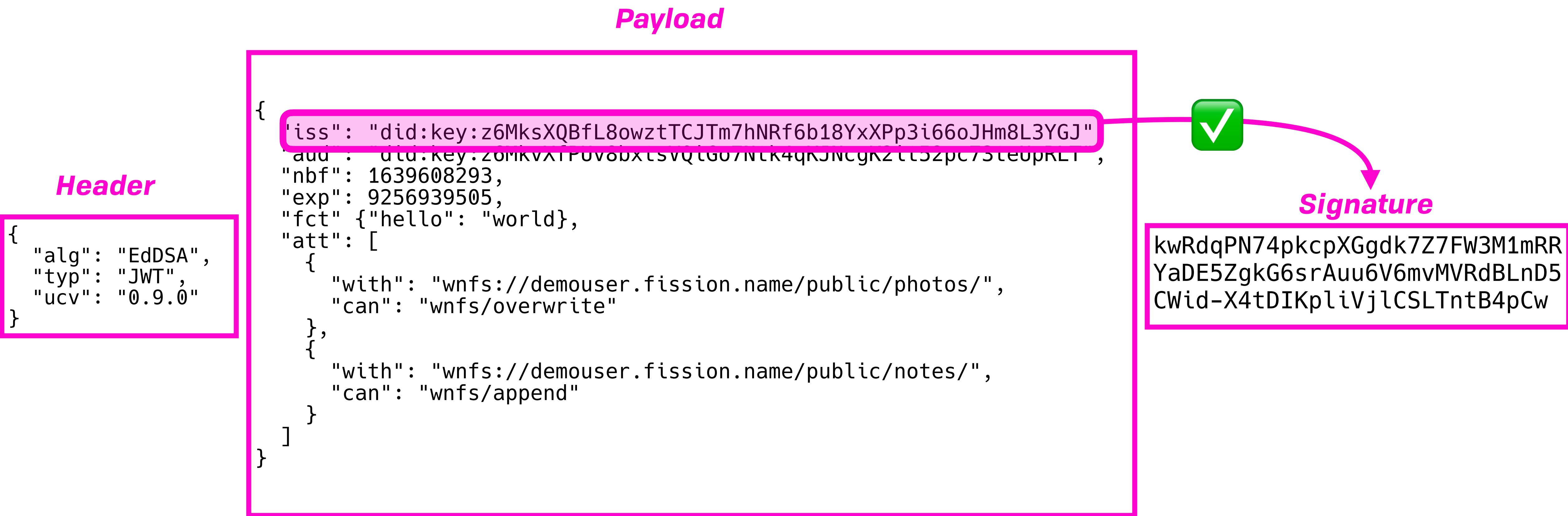
UCAN

JWT → UCAN



UCAN

JWT → UCAN



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/"  
   }  
 }  
 ]
```

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/"  
    }  
  }  
]
```

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/"  
      }  
    }  
  }  
]
```

The diagram illustrates the structure of a UCAN capability. It shows two objects within an array. The first object represents a resource ('noun'), indicated by a dotted arrow pointing to its 'with' field. The second object represents an action ('verb'), indicated by a dotted arrow pointing to its 'with' field.

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/"  
      }  
    }  
  }  
]
```

The diagram illustrates the structure of a UCAN capability object. It consists of an array containing two objects. Each object has a 'Resource / "noun"' field, an 'Action / "verb"' field, and an 'ext' field. The 'Resource' field contains a 'with' key pointing to a URI and a 'can' key pointing to an action. The 'Action' field contains a 'with' key pointing to an email address and a 'can' key pointing to another action. The 'ext' field contains a 'to' key with a regular expression pattern.

UCAN

Chain Witnesses

UCAN

Chain Witnesses



UCAN

Chain Witnesses



UCAN

Chain Witnesses



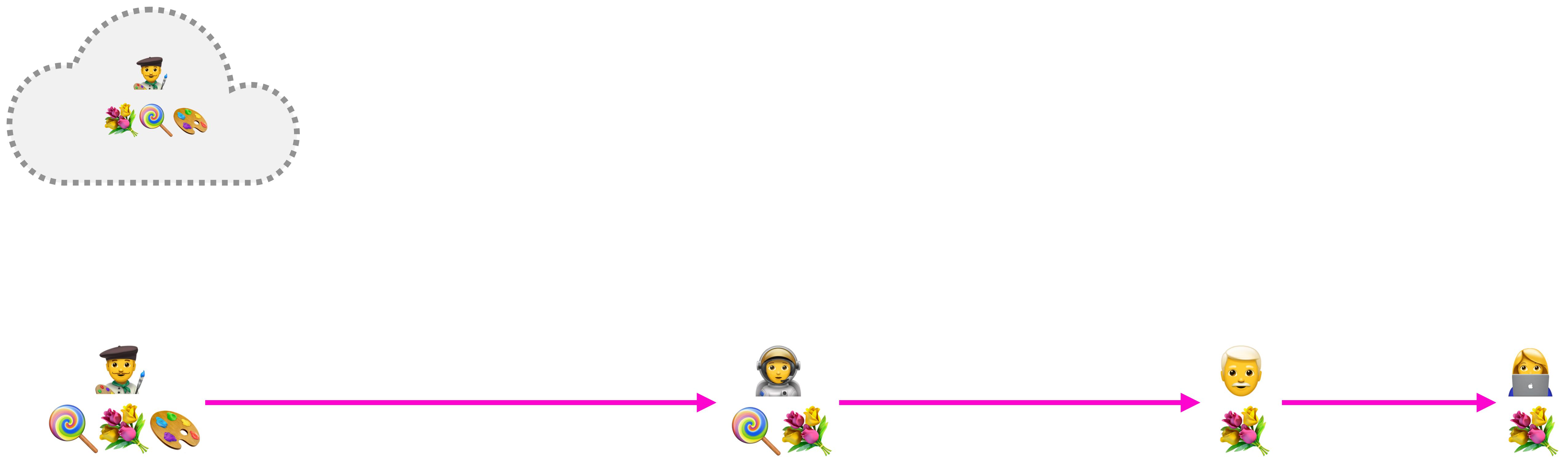
UCAN

Chain Witnesses



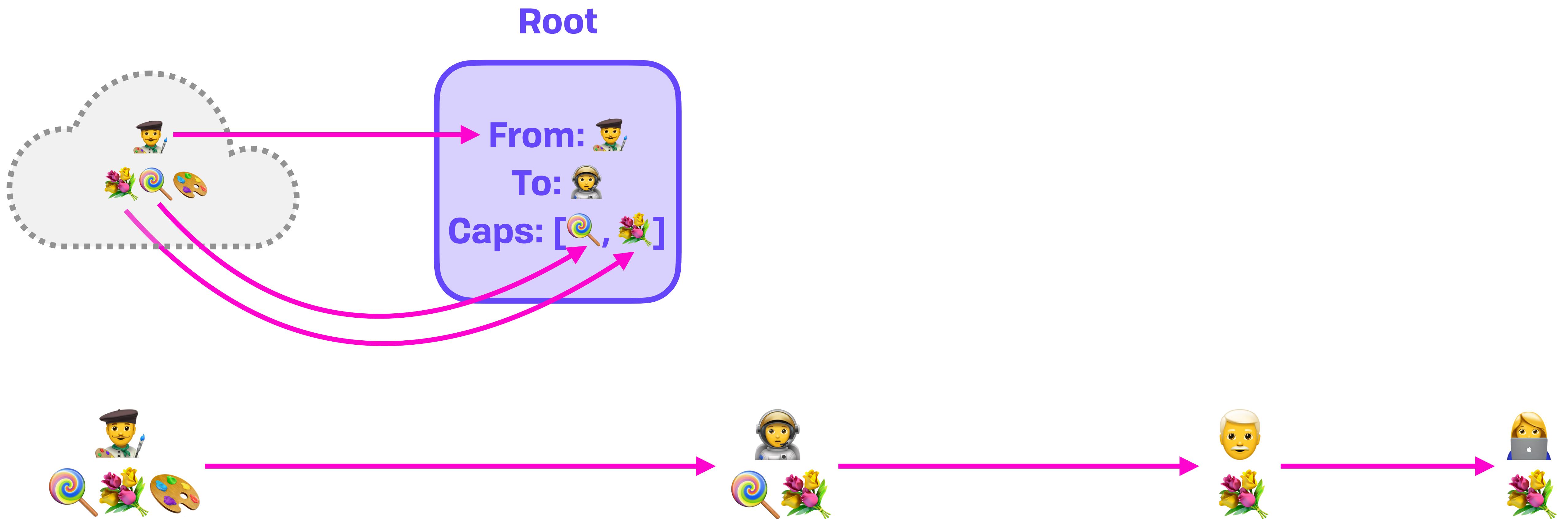
UCAN

Chain Witnesses



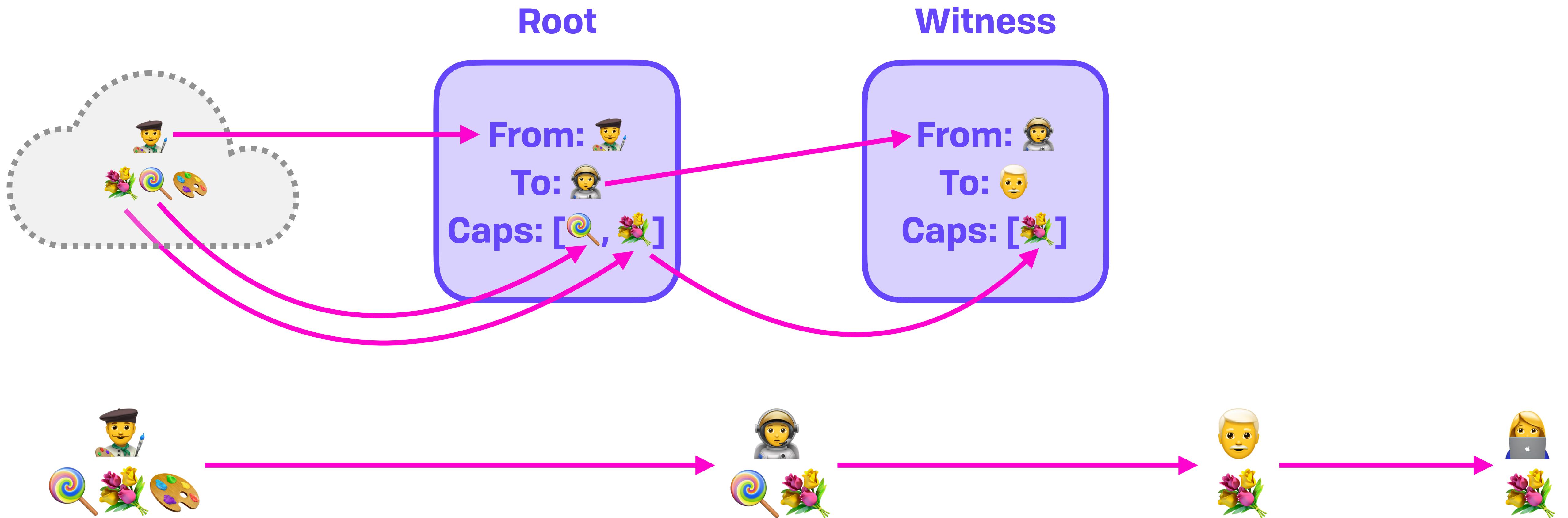
UCAN

Chain Witnesses



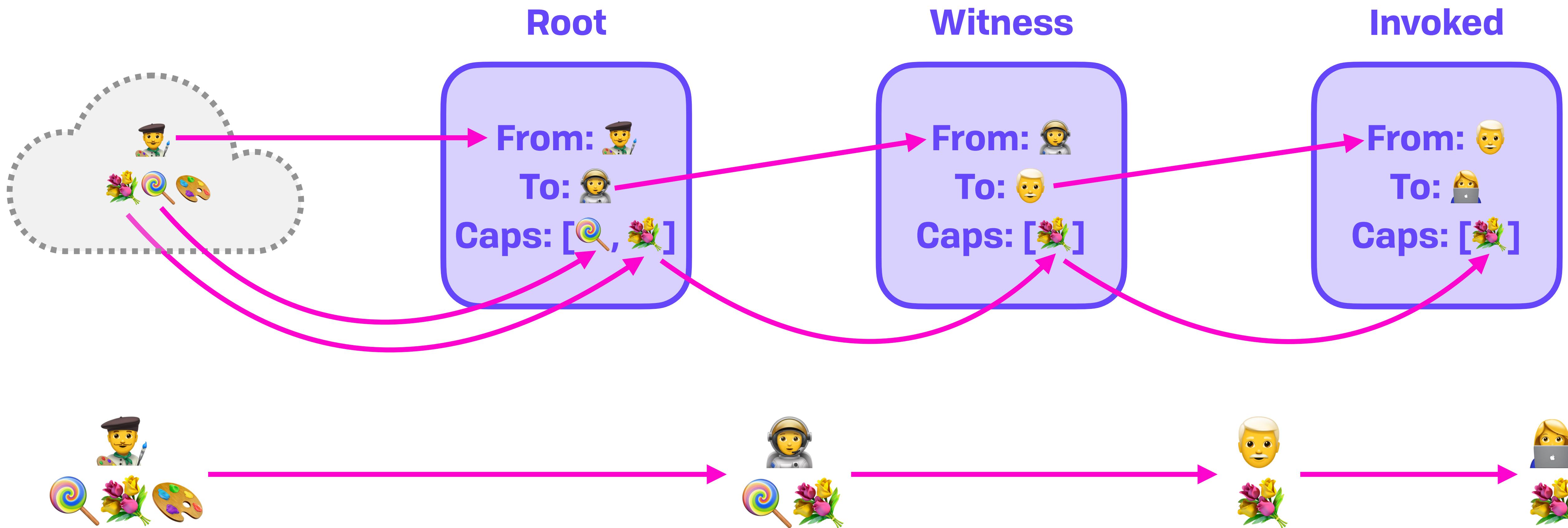
UCAN

Chain Witnesses



UCAN

Chain Witnesses



UCAN

Zoomed Out

UCAN

Zoomed Out



UCAN

Zoomed Out



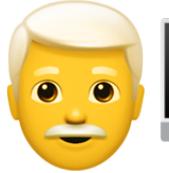
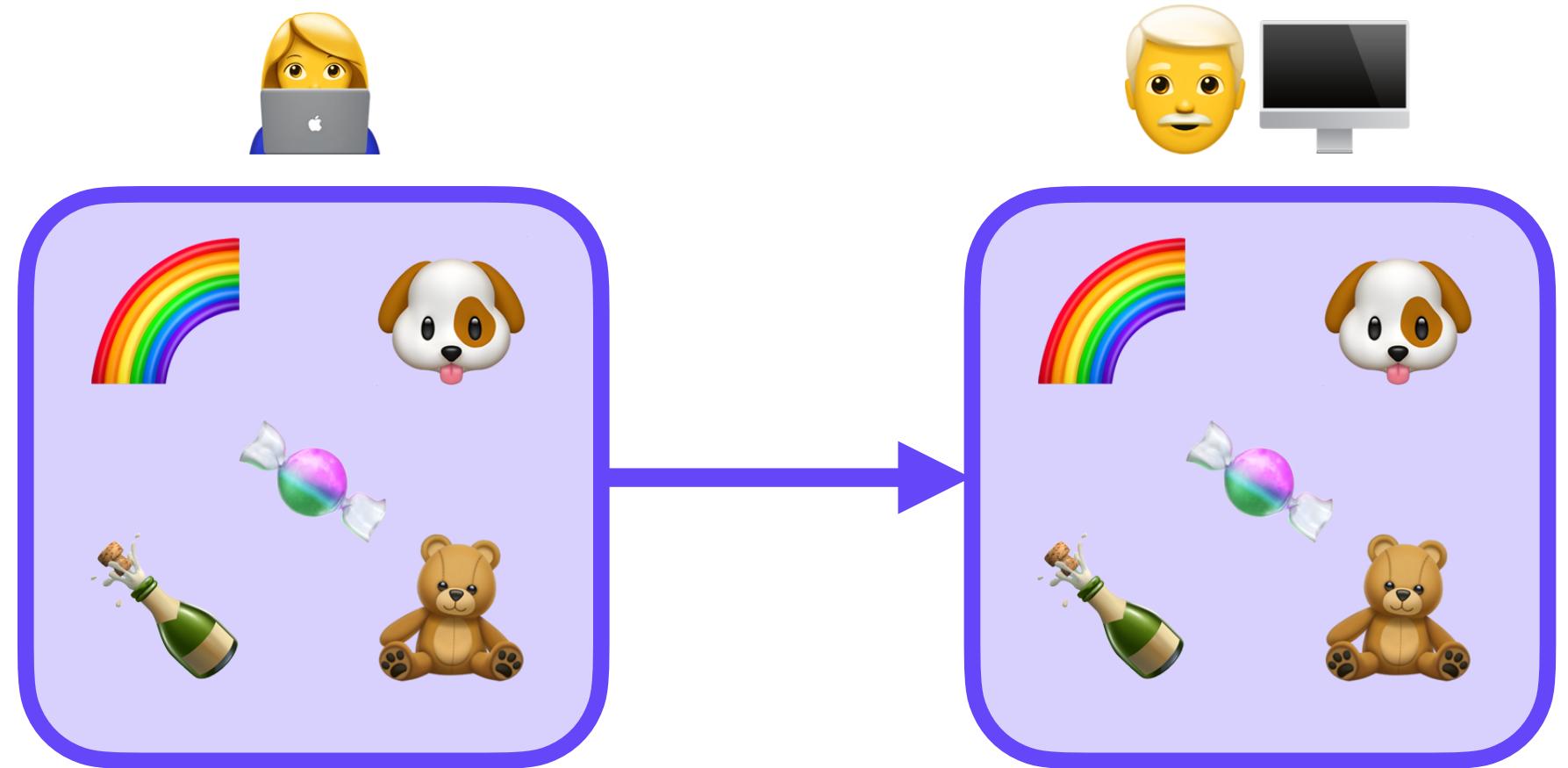
UCAN

Zoomed Out



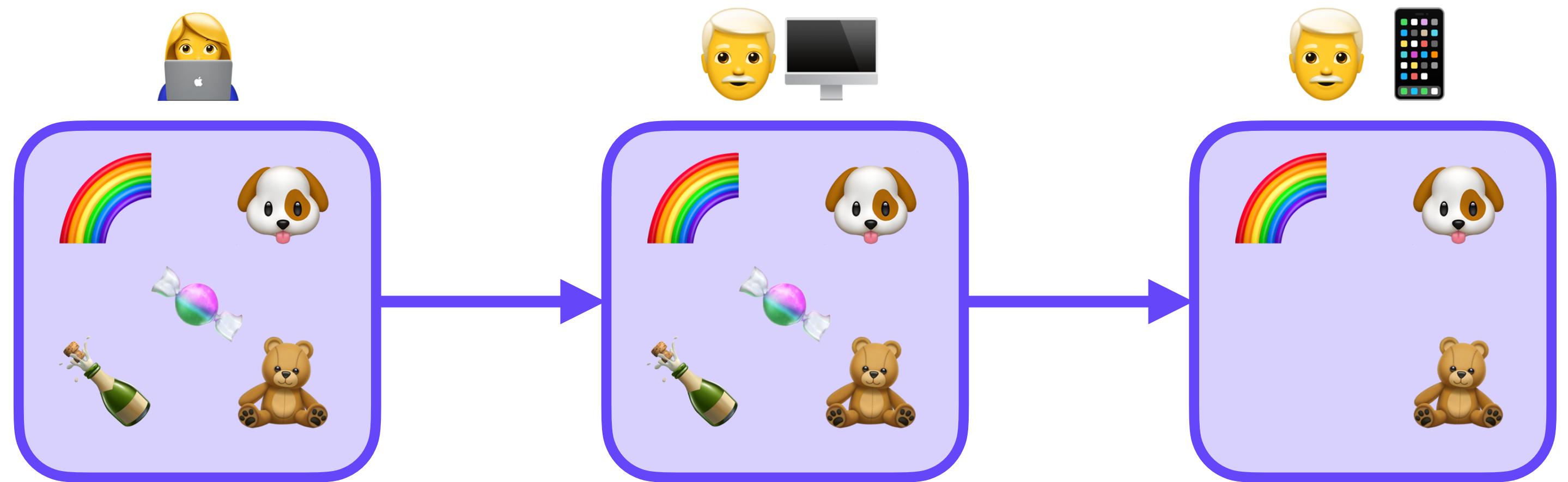
UCAN

Zoomed Out



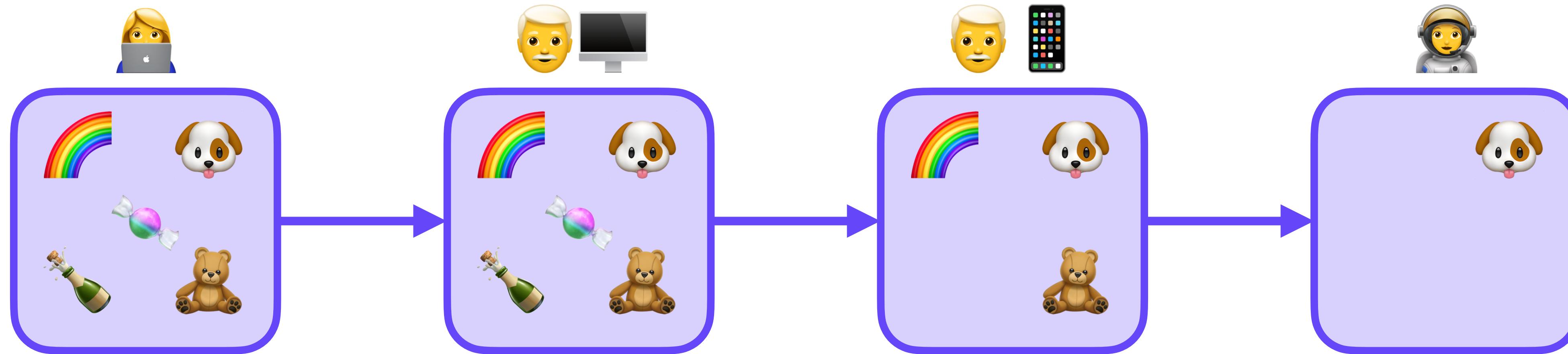
UCAN

Zoomed Out



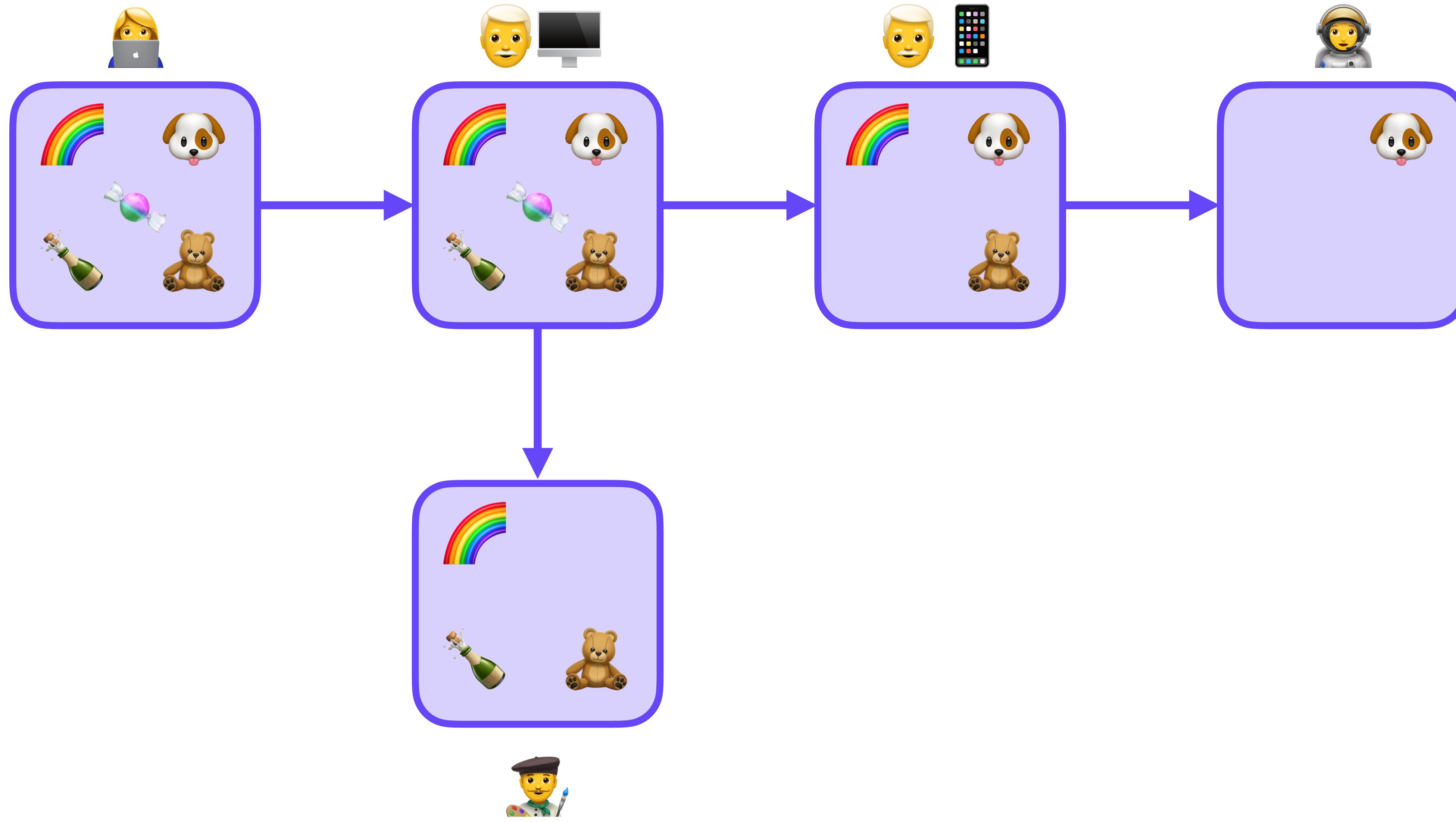
UCAN

Zoomed Out

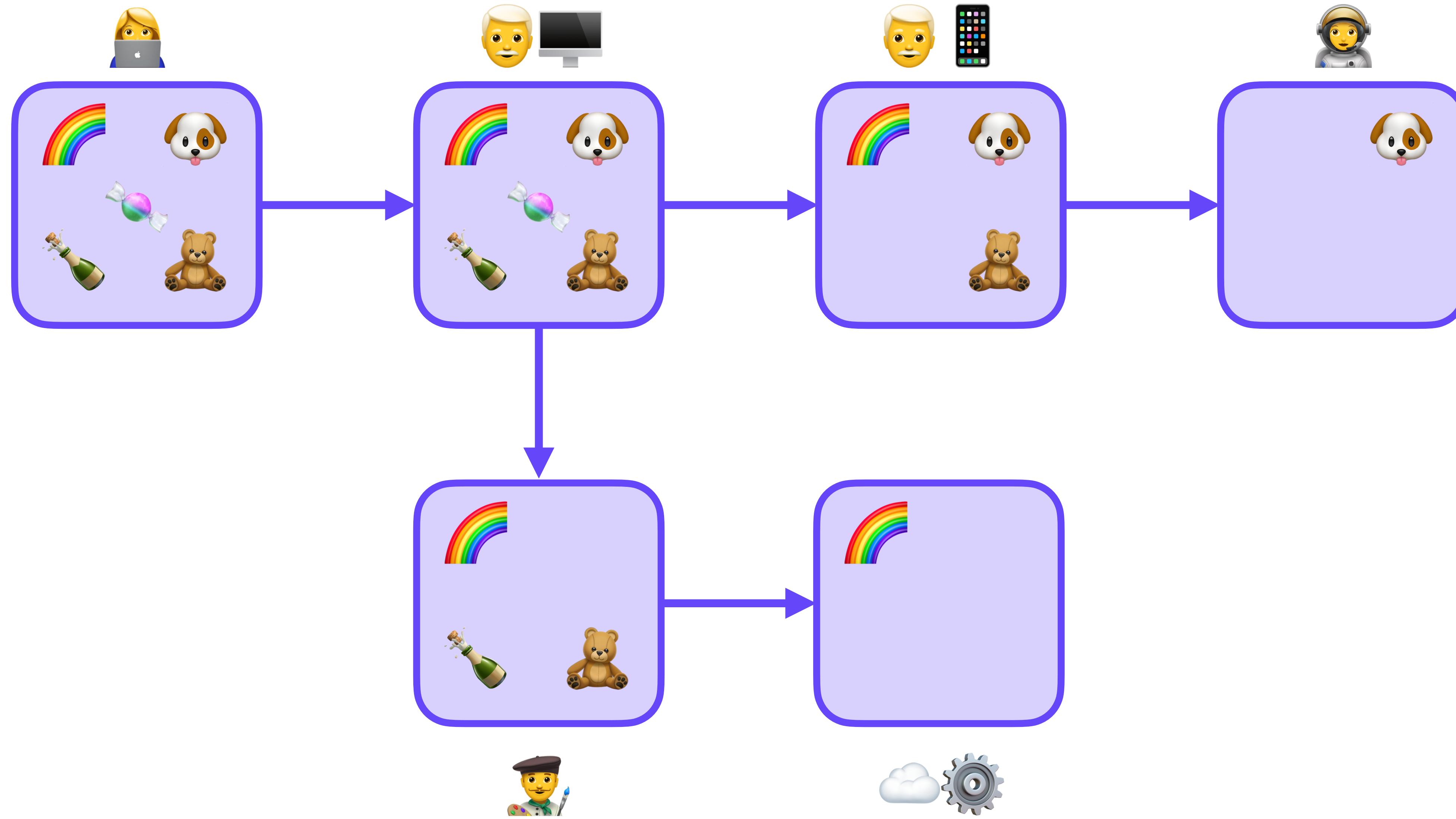


UCAN

Zoomed Out

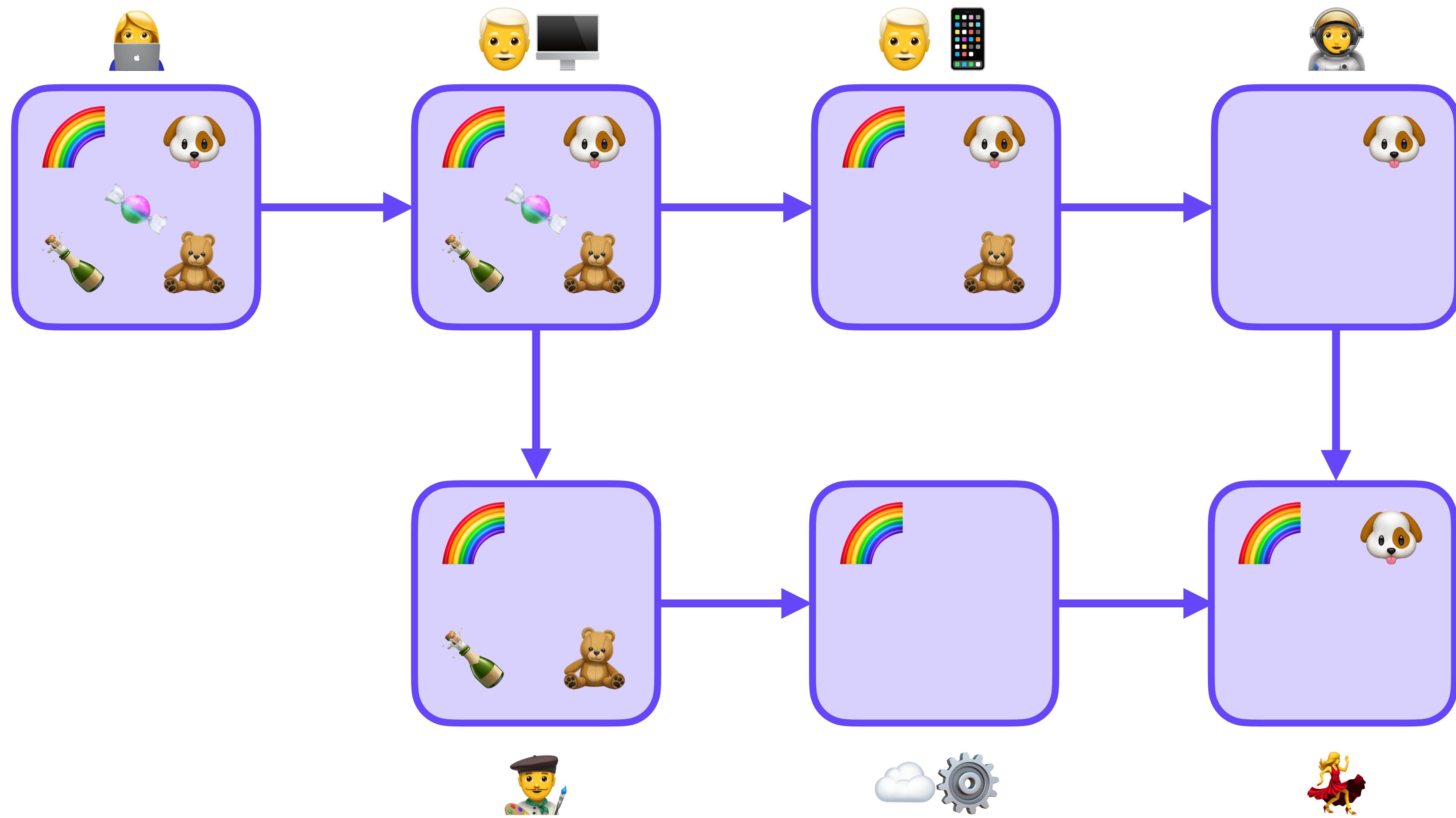


UCAN *Zoomed Out*



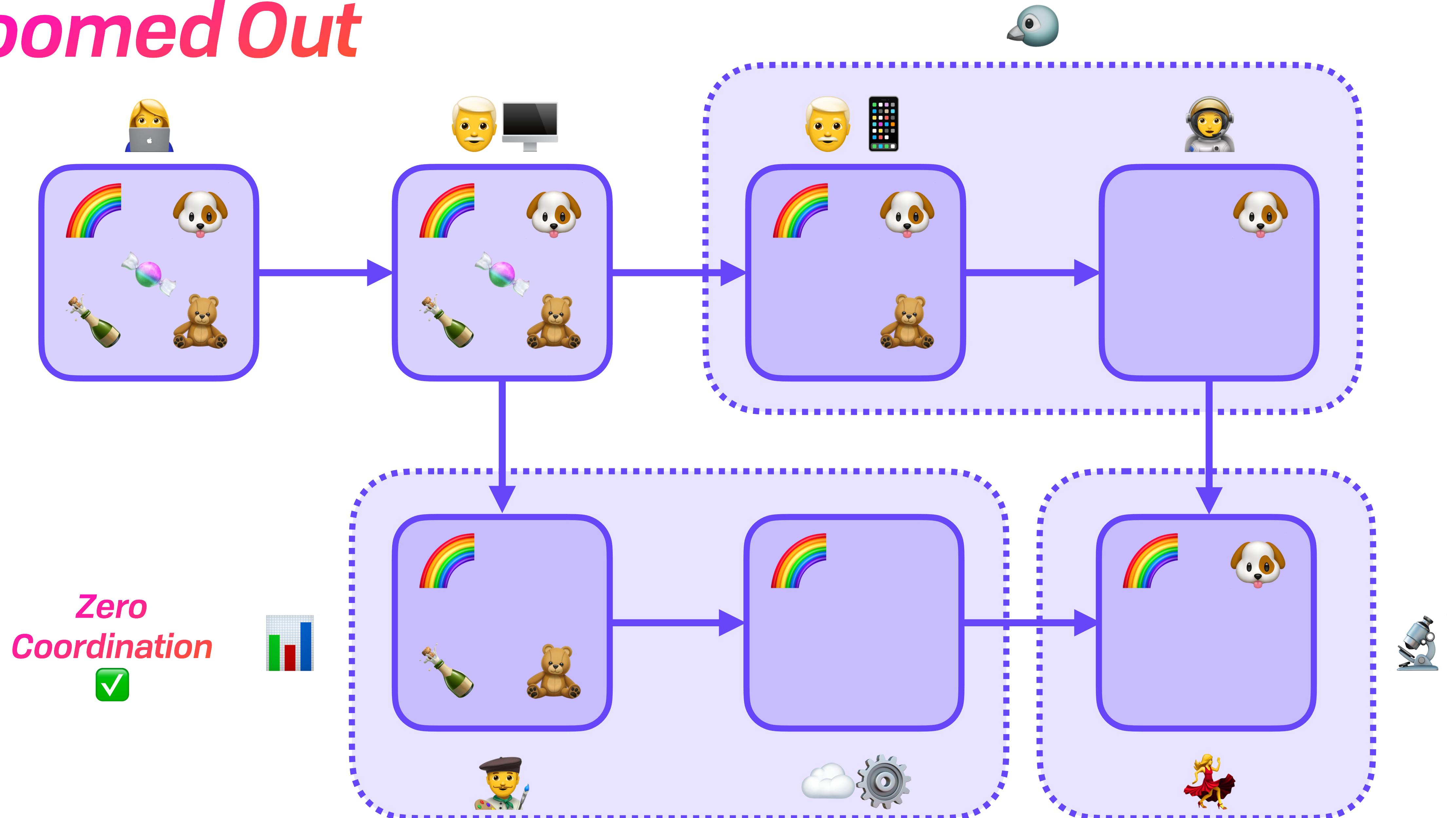
UCAN

Zoomed Out



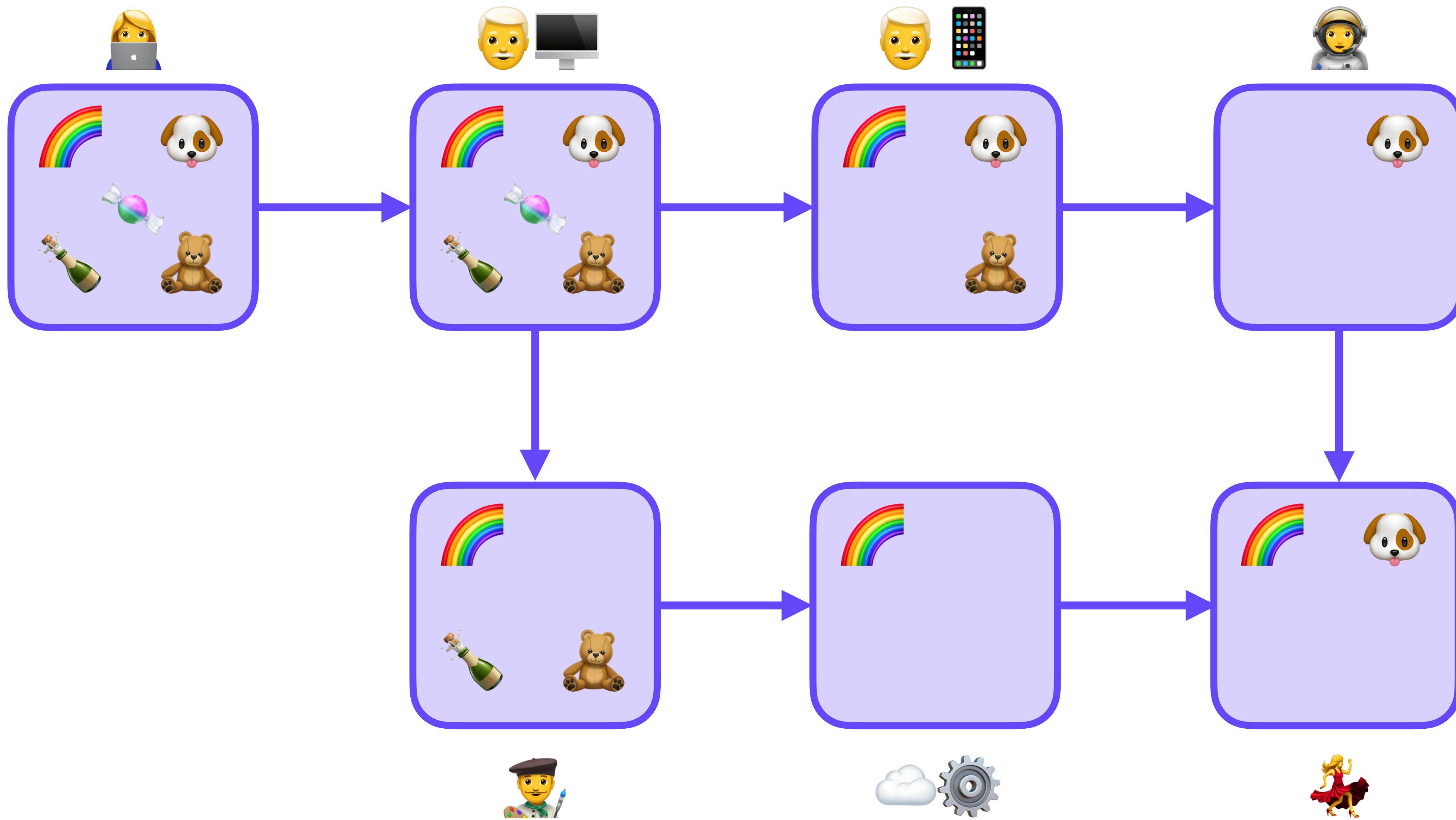
UCAN

Zoomed Out



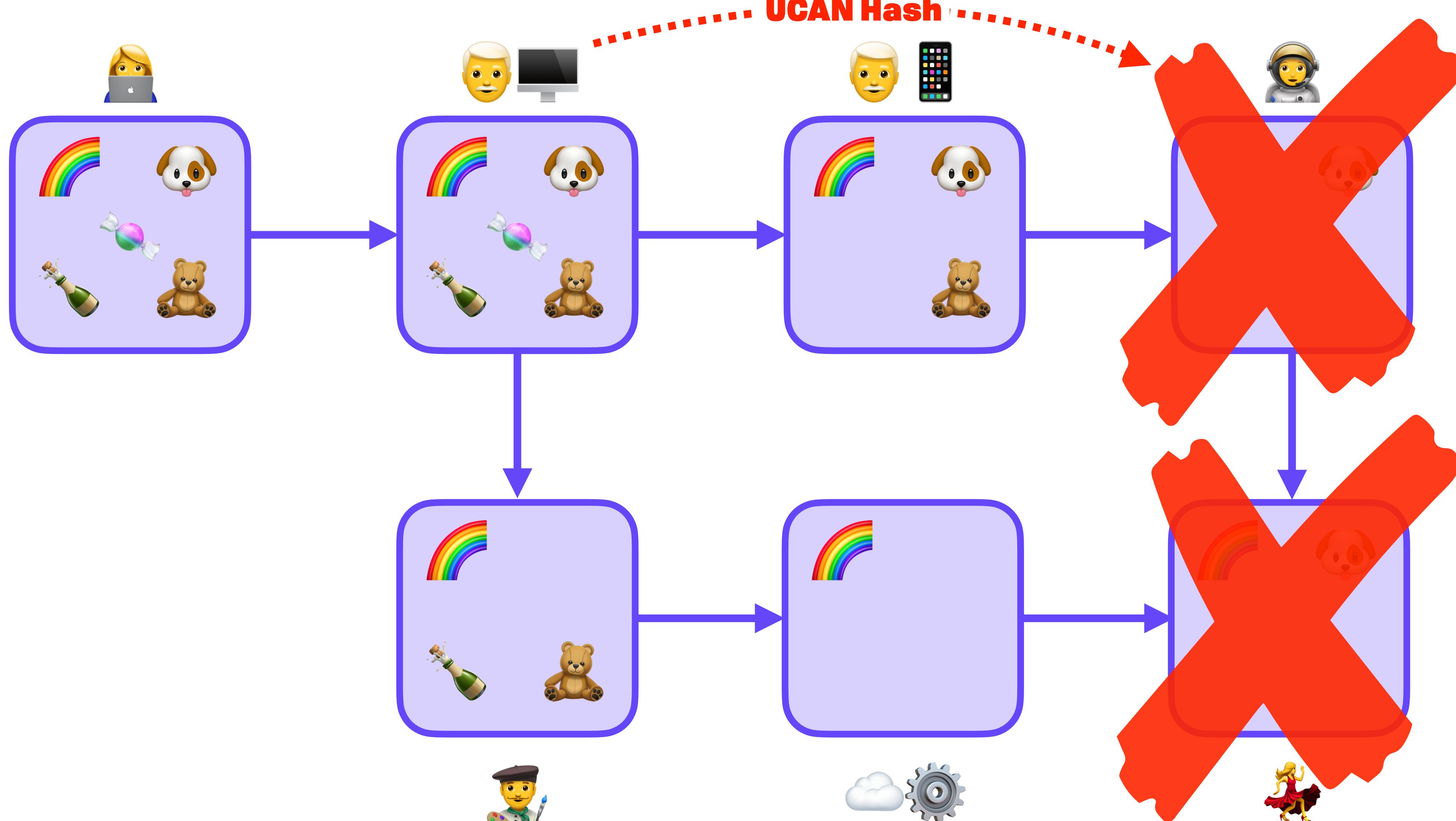
UCAN

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

eyJhbGciOiJFZERTQSI_sInR5cCI6IkpxVCIsInVjdiiI6IjAuNy4wIn0.eyJhdWQiOijkaWQ6a2V50no2T
Wt2WGZQVXY4Ynh0c1ZRaUdvN050azRxS0p0Y2dLMml0NTJwYzczdGVcFJMVCIsImF0dCI6W3sid25mcy
I6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsawMvcGhvdG9zLyIsImNhC_I6Ik9WRVJXUklURSJ9LHs
id25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsawMvb90ZX_MvIiwiY2FwIjoiT1ZFUl_{dSSVRF}
In1dLCJleHAiOjkyNTY5Mzk1MDUsImlzcyI6ImRpZDprZXk6ejZNa3NYUUJmTDhvd3p0VENKG03aE5SZ
jZiMThZeFhQcDNpNjZvSkht0EwzWUdKIiwibmJmIjoxNjM5NjA4MjkzLCJwcmYi0lsizXlKaGJHY2lPaU
pGwkVSFFT_{SXNJblI1Y0NJKlrcFhWQ0lzSw5WamRpSTZJakF1Tnk0d0luMC5leUpoZFdRaU9pSmthV1E}
2YTJWNU9ubzJUV3R6V0ZGQ1prdzRiM2Q2ZEZSRFNsUnROMmhPVW1ZMllqRTXW_{GhZVUhBemFUWTJiMHBJ}
YlRoTU0xbEhTaUlzSw1GMGRDSTZXM3NpZDI1bWN5STZJbVJsYlc5MWMyVnlMbVpwYzN0cGIyNHVi_{bUZ0W}
lM5d2RXSnNhV012Y0dodmRH0XpMeUlzSw10aGNDSTZJazlXULKWFVrbFVSU0o5WFN3aVpYaHdJam81TW
pVMk9UTTV0VEExTENKcGMzTwlPaUprYVdRNmEyVjVPbm8yVFd0d05VVnplamx6Tw_{sxSwMzRlpka3h2WTJ}
ONVNIZFl0V_{k5sZVZwTGNIRTNPVWQwTkRwbVJrZEZXbEk1T1NJc0ltNWlaaUk2TVRZek9UWXdPREk1TXl3}
aWNISm1JanBiWFgwLjRUTmh1SFJyUEc5YUhv0DY5SFhsc05L0F9GbWxTaFE1R3pHNGl0TjJ0S2steUtUY
kFnB0Z3VHVwdEcwWEZnTk12SHVsUHBsVnpaWURWRGV4bzc2a0F3IiwiZ_{XlKaGJHY2lPaUpGwkVSFFT}
NJblI1Y0NJKlrcFhWQ0lzSw5WamRpSTZJakF1Tnk0d0luMC5leUpoZFdRaU9pSmthV1E2YTJWNU9ubzJ
UV3R6V0ZGQ1prdzRiM2Q2ZEZSRFNsUnROMmhPVW1ZMllqRTXW_{GhZVUhBemFUWTJiMHBJYlRoTU0xbEhT}
aUlzSw1GMGRDSTZXM3NpZDI1bWN5STZJbVJsYlc5MWMyVnlMbVpwYzN0cGIyNHVi_{bUZ0WlM5d2RXSnNhV}
012Ym05MFpYTXZJaXdpWTJGd0lqb2lUMVpGVWxkU1NWUkZJbjFkTENKbGVIQwlPamt5TlRZNU16azFNRF
VzSw1semN5STZJbVJwWkRwc1pYazZlalp0YTNBMVJYTjZPWE15VFVoemNwbDJURzlqWTNsSWQxZzFVMLY
1V2t0d2NUYzVSM1EwTldaR1IwVmFVams1Swl3aWJtSm1Jam94TmpNNU5qQTRNam_{t6TENKd2NtWwlPbHRk}
Z1EuTw_{dZYXJMcXk3Um1RMUFJcnFZTDZjRnk5ejdhNVdJQVUtLVRZQVJQU2dpck9Tc3p2YXIzX0R0cjI1c}
mJQcmV0SGJuVDBtTVZLeW9hUVhydVI3S2JyQmcixX0.kwRdqPN74pkcpXGgdk7Z7FW3M1mRRYaDE5ZgkG
6srAuu6V6mvMVRdBlnD5Cwid-X4tDIKpliVjlCSLTntB4pCw

Nontrivial Example

Decoded

Payload

Header

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

```
{  
  "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",  
  "aud": "did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",  
  "nbf": 1639608293,  
  "exp": 9256939505,  
  "att": [  
    {  
      "with": "wnfs://demouser.fission.name/public/photos/",  
      "can": "OVERWRITE"  
    },  
    {  
      "with": "wnfs://demouser.fission.name/public/notes/",  
      "can": "APPEND"  
    }  
  ],  
  "prf": [  
    "eyJhbGciOiJFZERTQSIssInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a  
2V50no2TwtzWFFCZkw4b3d6dFRDSlRtN2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF  
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNh  
CI6Ik9WRVJXUk1URSJ9XSwizXhwIjo5MjU20TM5NTA1LCJpc3Mi0iJkaWQ6a2V50no2TwNUV  
zejlzMk1Ic3FZdkxvY2N5SHdYNVNleVpLcHE30Ud0NDVmRkdFwlI50SIssIm5iZiI6MTYz0TYw0  
DI5MywicHJmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_FmlShQ5GzG4itN2NKK-  
yKTbAMoFwTuptG0XFgNIvHu1PplVzZYDxDexo76kAw",  
  
    "eyJhbGciOiJFZERTQSIssInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a  
2V50no2TwtzWFFCZkw4b3d6dFRDSlRtN2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF  
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNh  
joiT1ZFuldSSVRFIIn1dLCJleHAi0jkyNTY5Mzk1MDUsImlzcyI6ImRpZDprZXk6ejZNa3A1RXN  
60XMyTUhzcVl2TG9jY3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjoxNjM5Nja4M  
jkzLCJwcmYi0ltdfQ.MgYarLqy7RmQ1AIrqYL6cFy9z7a5WIAU--  
TYARPSgir0Szvar3_DNr25rbPretHbnT0mMVkyoaQXruR7KbrBg"  
  ]  
}
```

Signature

```
kwRdqPN74pkcpXG gdk7Z7FW3M1mRR  
YaDE5ZgkG6srAuu6V6mvMVRdBlnD5  
Cwid-X4tDIKpliVjlCSLTntB4pCw
```

Nontrivial Example

Decoded

Payload

Header

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

```
{  
  "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",  
  "aud": "did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",  
  "nbf": 1639608293,  
  "exp": 9256939505,  
  "att": [  
    {  
      "with": "wnfs://demouser.fission.name/public/photos/",  
      "can": "OVERWRITE"  
    },  
    {  
      "with": "wnfs://demouser.fission.name/public/notes/",  
      "can": "APPEND"  
    }  
  ],  
  "prf": [
```

```
'eyJhbGciOiJFZERTQSIssInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a  
2V50no2TwtzWFFCZkw4b3d6dFRDSlRtN2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF  
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNh  
CI6Ik9WRVJXUk1URSJ9XSwizXhwIjo5MjU20TM5NTA1LCJpc3Mi0iJkaWQ6a2V50no2TwNUV  
zejlzMk1Ic3FZdkxvY2N5SHdYNVNleVpLcHE30Ud0NDVmRkdFWlI50SIssIm5iZiI6MTYz0TYw0  
DI5MywicHJmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_FmlShQ5GzG4itN2Nkk-  
yKTbAMoFwTuptG0XFgNIvHu1PplVzZYDxDexo76kAw",
```

```
'eyJhbGciOiJFZERTQSIssInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a  
2V50no2TwtzWFFCZkw4b3d6dFRDSlRtN2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF  
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNh  
joiT1ZFuldSSVRFIIn1dLCJleHAi0jkyNTY5Mzk1MDUsImlzcyI6ImRpZDprZXk6ejZNa3A1RXN  
50XMyTUhzcVl2TG9jY3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjoxNjM5Nja4M  
jkzLCJwcmYi0ltdfQ.MgYarLqy7RmQ1AIrqYL6cFy9z7a5WIAU--  
TYARPSgirOSszvar3_DNr25rbPretHbnT0mMVKyoaQXruR7KbrBg"
```

```
}
```

Signature

```
kwRdqPN74pkcpXG gdk7Z7FW3M1mRR  
YaDE5ZgkG6srAuu6V6mvMVRdB LnD5  
Cwid-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_FmlShQ5GzG  
4itN2NKk-  
yKTbAMoFwTuptG0XFgNIvHuPPplVzZYDVDe  
xo76kAw
```

Nontrivial Example

ucan.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

```
eyJhbGciOiJFZERTQSIsInR5cCI6IkpxVCIsInVjdjAuNy4wIn0eyJhdWQiOiKaWQ6a2v5Ono2TWtzWFFCZkw4b3d6dRDSiRtN2hOUmY2YjE4WxHUAzaTz2b0pThMM1lHSiisImFdC16W3sid25mcy16InRlbW91c2VylmZpc3Npb24ubmFzZ9wdJsaWMvcGhvdG9zly1sImNhcC16k19WRVJXUkURS39XSwizXhwIj05MjU2OTMsNTA1L3Cpc3MlOjkaVQ6a2V5Ono2TWiwNUVzejLMk1c3FZdkvY2NSHdYNVNleVpLchE30Ud0NDVmRkdFW15OSIsIm5iZl6MTYzOTYwOD15MyicHjmjp8X0.4TNhuHRrPG9aHoB69HXlsNK8_FmlShQ5GzG4itN2NKK-yKTbAMoFwTuptGOXFgNivHuPpIVzZYDvDexo76kAw
```

Decoded

Header

```
{ "alg": "EdDSA", "typ": "JWT", "ucv": "0.7..0" }
```

Payload

```
{ "aud": "did:key:z6MksXQBflBowztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ", "att": [ { "wnfs": "demouser.fission.name/public/photos/", "cap": "OVERWRITE" } ], "exp": 9256939505, "iss": "did:key:z6Mkp5Esz9s2MhsqYvLoccyHwX5Sey2Kpq79Gt45fFGEZ99", "nbf": 1639608293, "prf": [] }
```

Signature

```
4TNhuHRrPG9aHoB69HXlsNK8_FmlShQ5GzG4itN2NKK-yKTbAMoFwTuptGOXFgNivHuPpIVzZYDvDexo76kAw
```

Actions

Result

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:z6Mkp5Esz9s2MhsqYvLoccyHwX5Sey2Kpq79Gt45fFGEZ99	The DID of the issuer. The UCAN must be signed with the private key of the issuer to be valid.
aud	Audience	did:key:z6MksXQBflBowztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ	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 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

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

```
eyJhbGciOiJFZERTQSIsInR5cCI6IkpxVCIsInVjdjAuNy4wIn0eyJhdWQiOiKaWQ6a2v5Ono2TWtzwFFCZkwB3d6dRDSIRtN2h0UmY2YjE4WxHUhazTAy2boIbThMM1lHSiisImFdC16W3sid25mcy16InRlbW91c2VlMzpc3Nb24ubmFzZ9wdJsaWMvcGhvdG9zly1sImNhcC161k9WRVJXUlkURs39XswiZkhwIj05MJu2OTMSNTA1Lc3pc3MlOjkaWQ6a2v5Ono2TWtwhNUVzejIzMk1lC3FdKvY2NSHdYNVNleVpLchE30Ud0NDVmRkdFWI5OSIsIm5iZl6MTYzOTYwOD15MyicHjmjp8X0.4TNhuHRrPG9aHoB69HXlsNKB_FmlShQ5GzG4itN2NKK-yKTbAMoFwTuptG0XFgNivHuPplVzZYDvDexo76kAw
```

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:z6Mkp5Es9s2MhsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99", "nbf": 1639608293, "prf": [] }
```

Signature

```
4TNhuHRrPG9aHoB69HXlsNKB_FmlShQ5GzG4itN2NKK-yKTbAMoFwTuptG0XFgNivHuPplVzZYDvDexo76kAw
```

Delegate 1 **Selected**

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

Payload

```
{ "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ", "att": [ { "wnfs": "demouser.fission.name/public/photos/", "cap": "OVERWRITE" } ], "exp": 9256939505, "iss": "did:key:z6Mkp5Es9s2MhsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99", "nbf": 1639608293, "prf": [] }
```

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:z6Mkp5Es9s2MhsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99	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

ucan.xyz – Online Explorer / Validator

The diagram illustrates the process of validating a complex UCAN string using the ucan.xyz online explorer/validator.

UCAN Check

Encoded

Paste an encoded UCAN

```
eyJhbGciOiJFZERTQSIsInR5cCI6IkpxVCIsInVjdIjAuNy4wIn0eyJhdWQiOiKaWQ6a2v5Ono2TWtzwFFCZkw4b3ddedRDSIRtN2h0UmY2YjE4WxHUhaztaY2boIbThMM1lHSiisImFdC16W3sid25mcyI6InRlbW91c2Vlmzpc3Nb4ubmFzZ9wdJsaWMvcGhvdG9zlyIsImNncC16k19WRVJXUkURs39XswiZkhwIj5MJu20TM5NTA1C3pc3MlOjkaVQ6a2v5Ono2TWhwNUVzejIzMk1lC3FZdkvY2NSHdYNVNleVpLchE30Ud0NDVmRkdFWI5OSIsIm5iZl6MTYzOTYwOD15MywicHjmjp8X0_4TNhuHrPG9aHoB69HxIsNKB_FmlShQ5GzG4itN2NKK-yKTbAMoFwTuptGOXFgNivHuIpIVzZYDvDexo76kAw
```

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

```
4TNhuHrPG9aHoB69HxIsNKB_FmlShQ5GzG4itN2NKK-yKTbAMoFwTuptGOXFgNivHuIpIVzZYDvDexo76kAw
```

Payload

A large pink box highlights the "Payload" section of the decoded UCAN, which is then pointed to by a pink arrow.

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.

Validation Results

Valid	true
Issuer	did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99
Audience	did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ

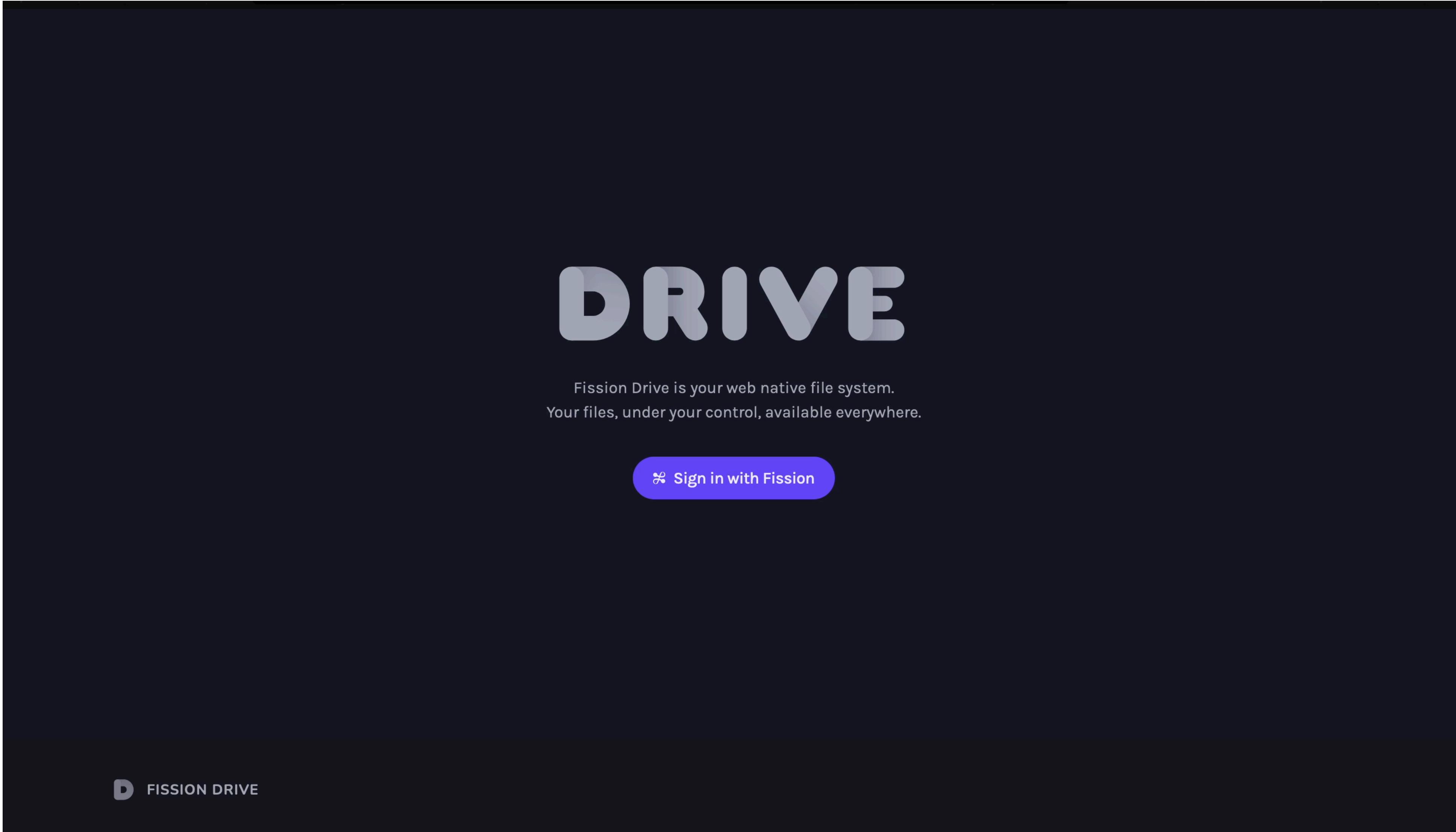
Buttons

Explanation

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

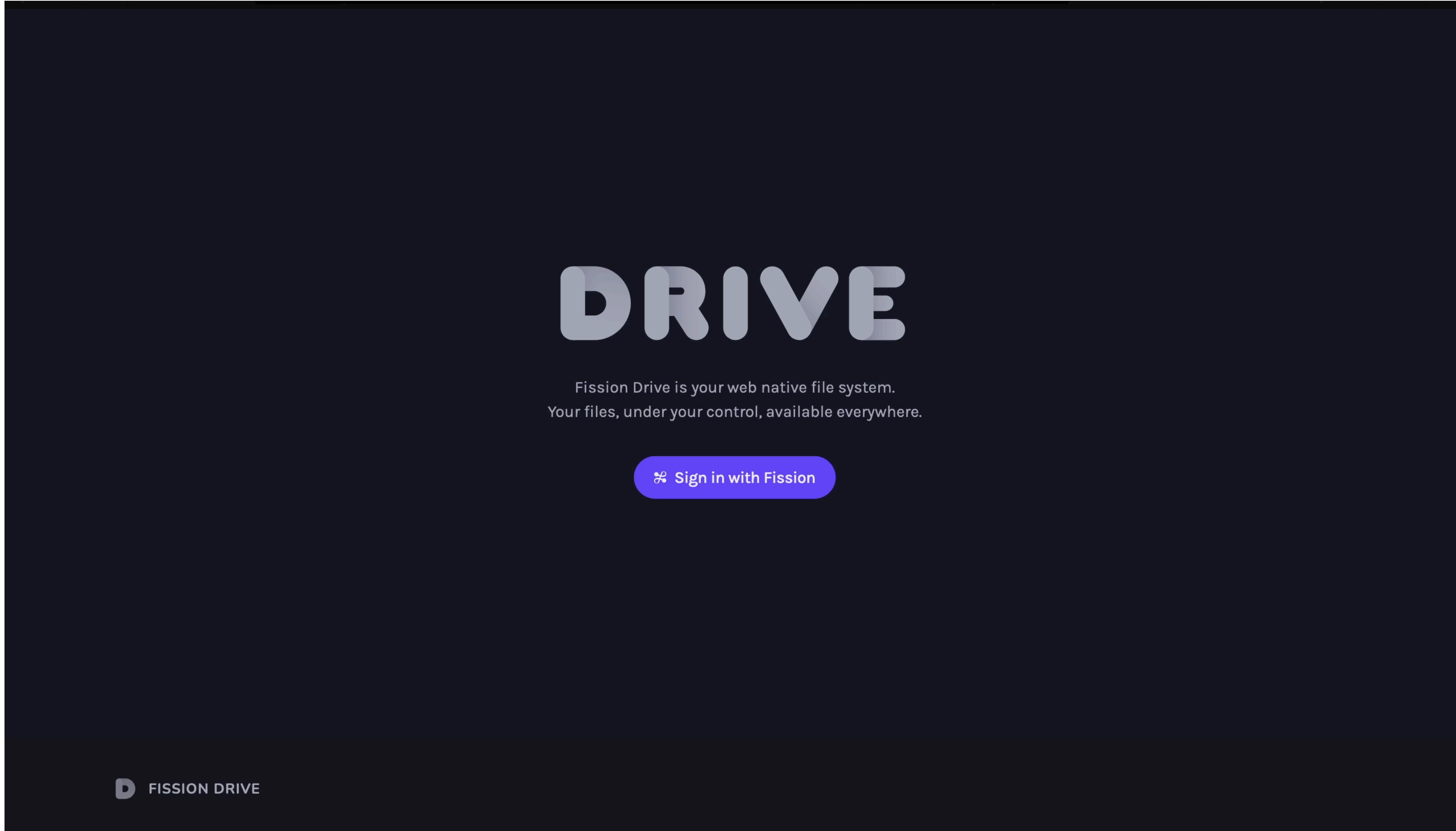
Nontrivial Example

Auth Should be Boring!



Nontrivial Example

Auth Should be Boring!



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/aclsdont/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

@expede