

Decentralized Authorization

Plumbing for Permissionless Interoperation



The limitation of ***local knowledge***
is the ***fundamental fact***
about the setting in which we work,
and it is ***a very powerful limitation***

– Nancy Lynch, A Hundred Impossibility Proofs for Distributed Computing

Brooklyn Zelenka

@expede



Brooklyn Zelenka

@expede



- Cofounder & CTO at Fission
 - @FissionCodes
 - <https://fission.codes>
 - Tools & protocols for edge & web3
 - IPVMM, WNFS, Dialog, UCAN, etc
- Knows a thing or two about the UCAN spec

Nothing less than connecting
all of the world's users & services.

The "HTTP" storage and compute equivalent:
open, interoperable, & everywhere.

Must be ***substantially*** better than Web 2.0

How to Power a New Internet

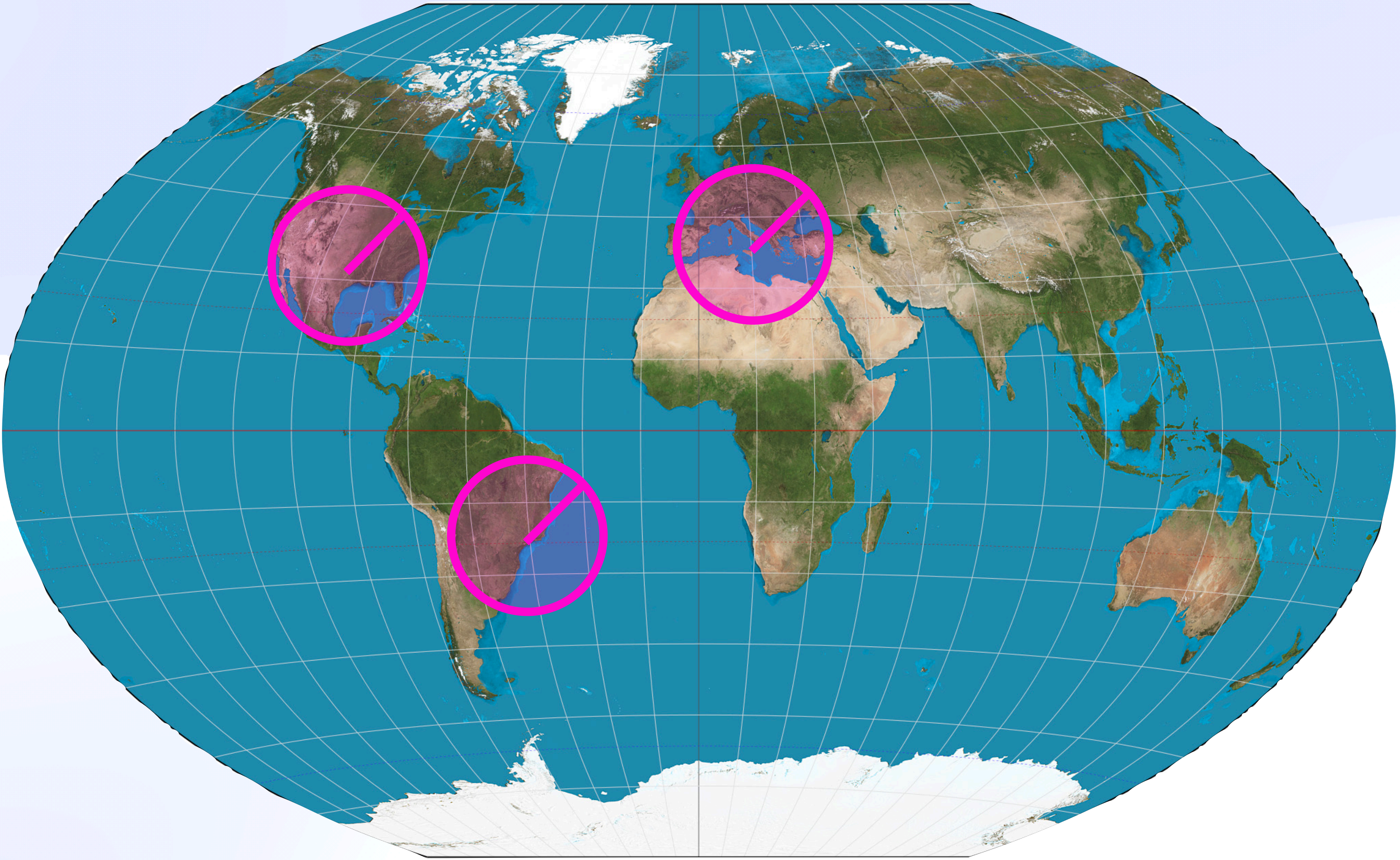


How to Power a New Internet ⚡



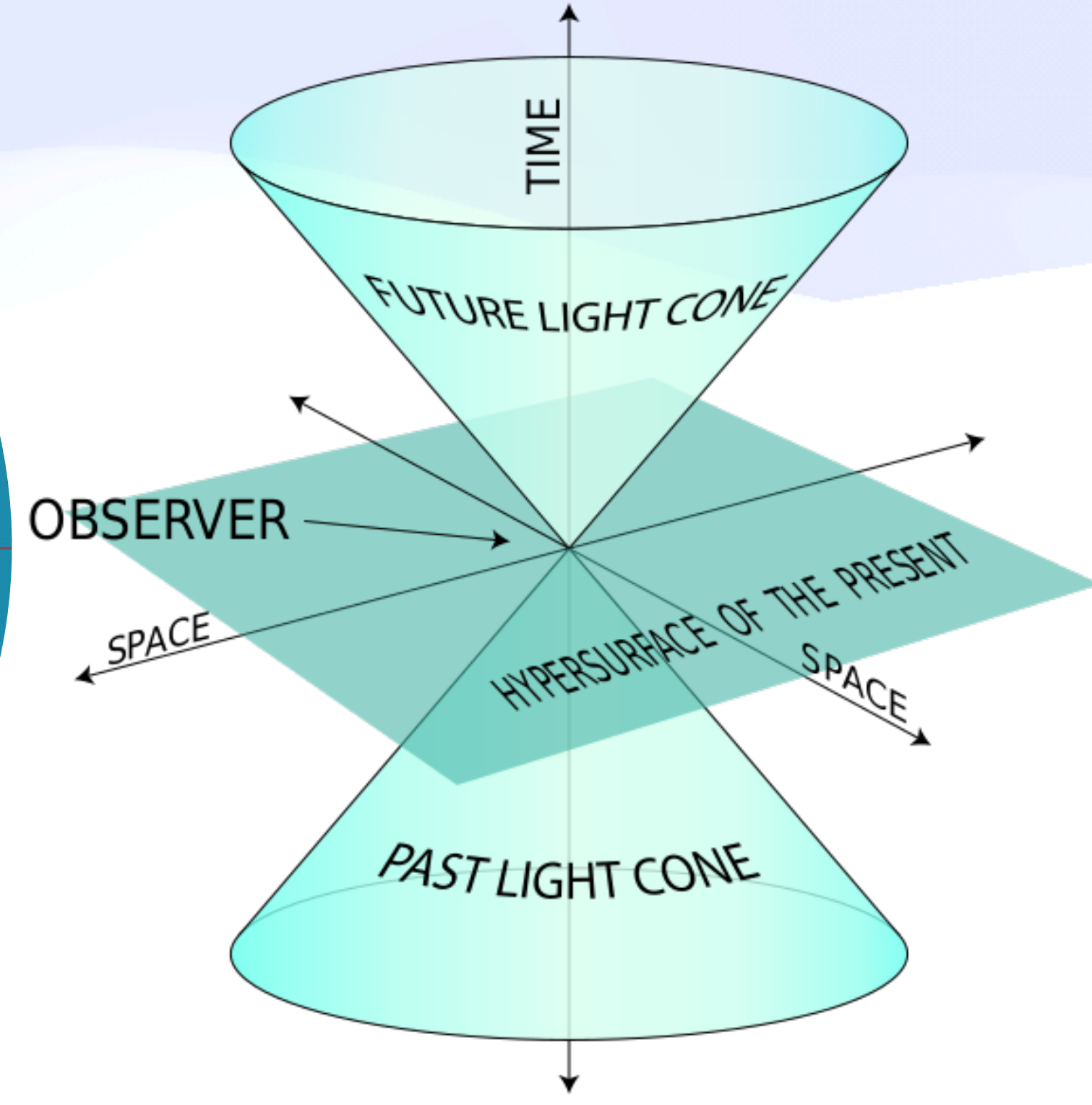
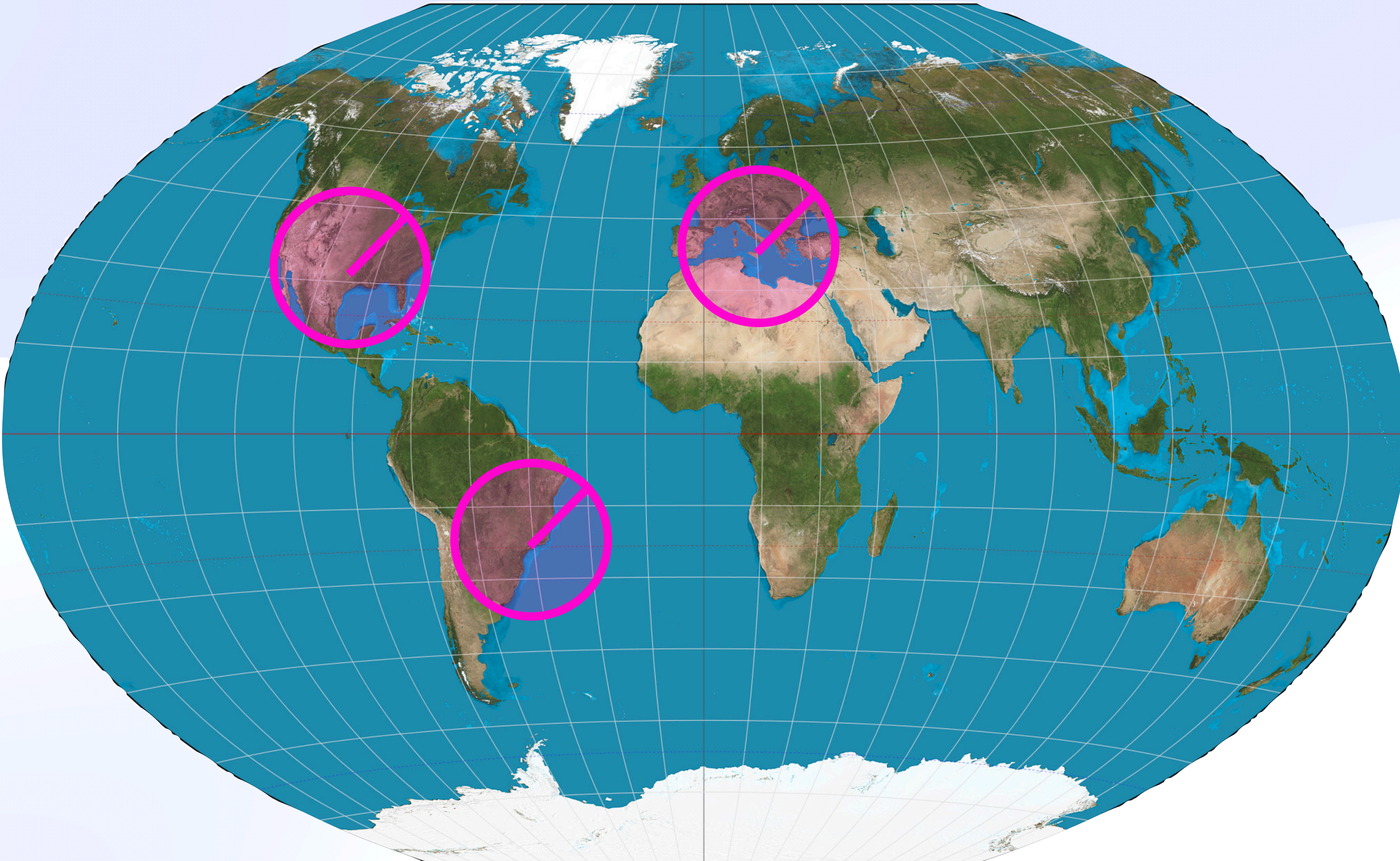
How to Power a New Internet ⚡

Causal Islands 🏖️ 🌴



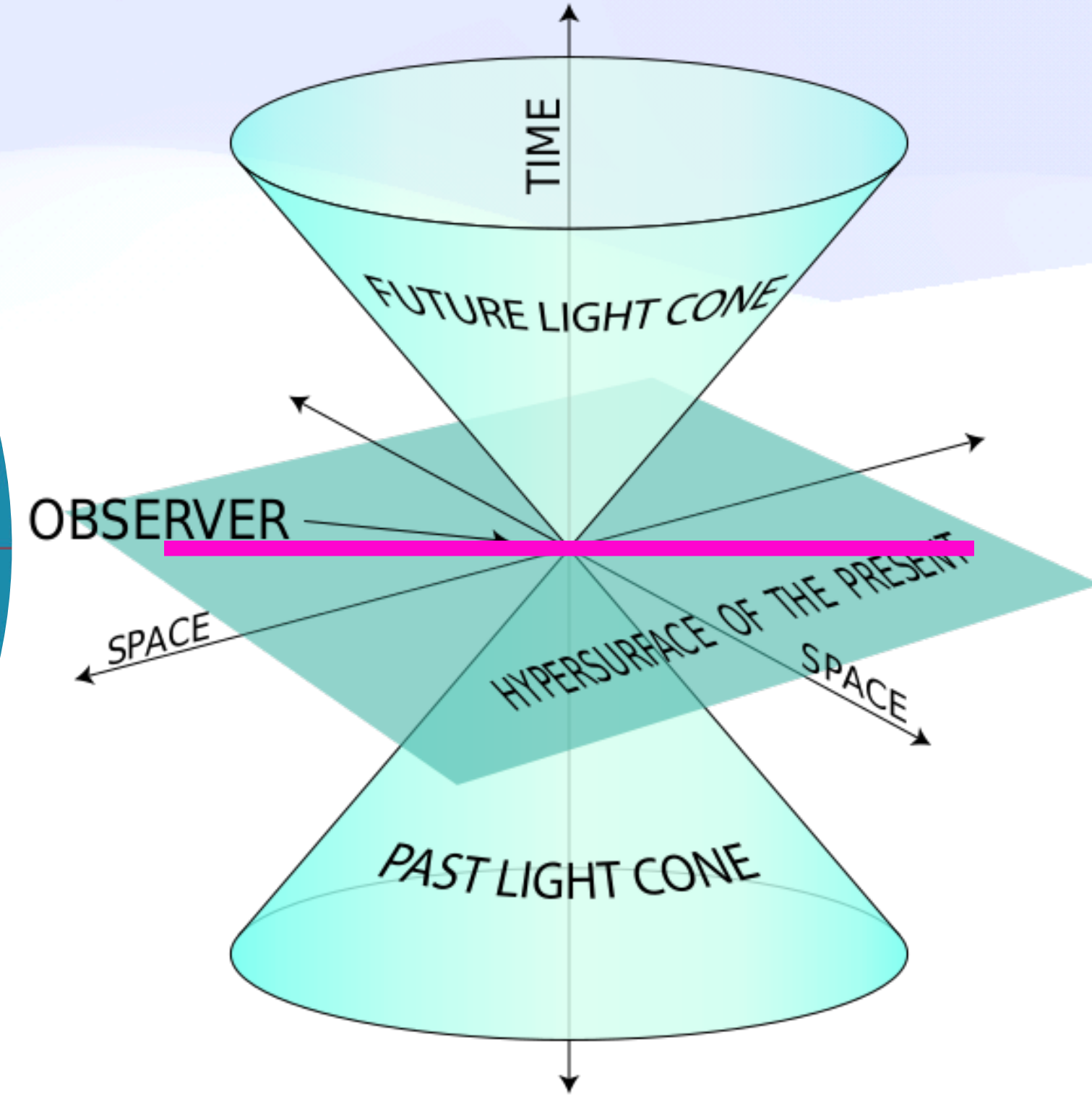
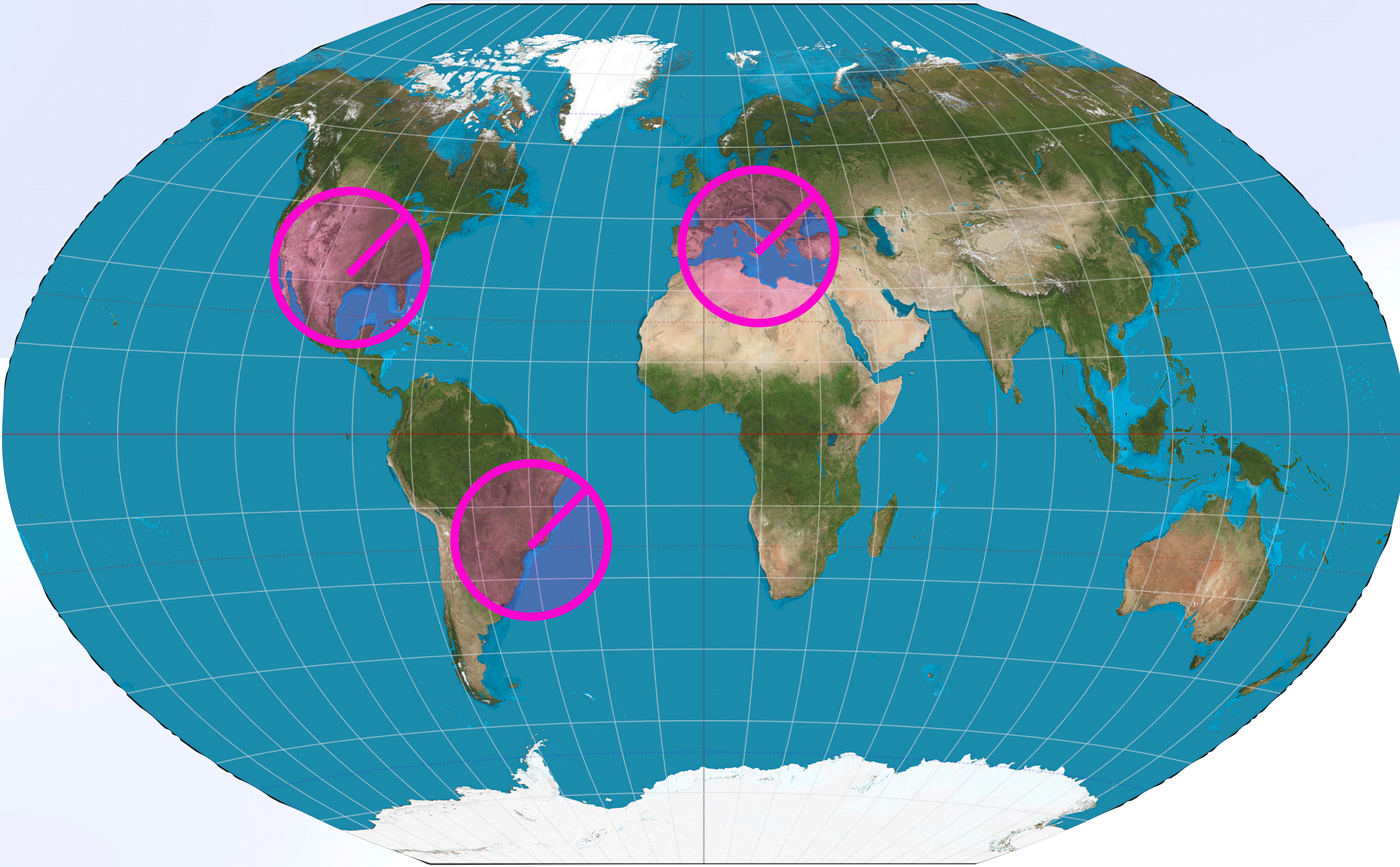
How to Power a New Internet ⚡

Causal Islands 🏖️ 🌴



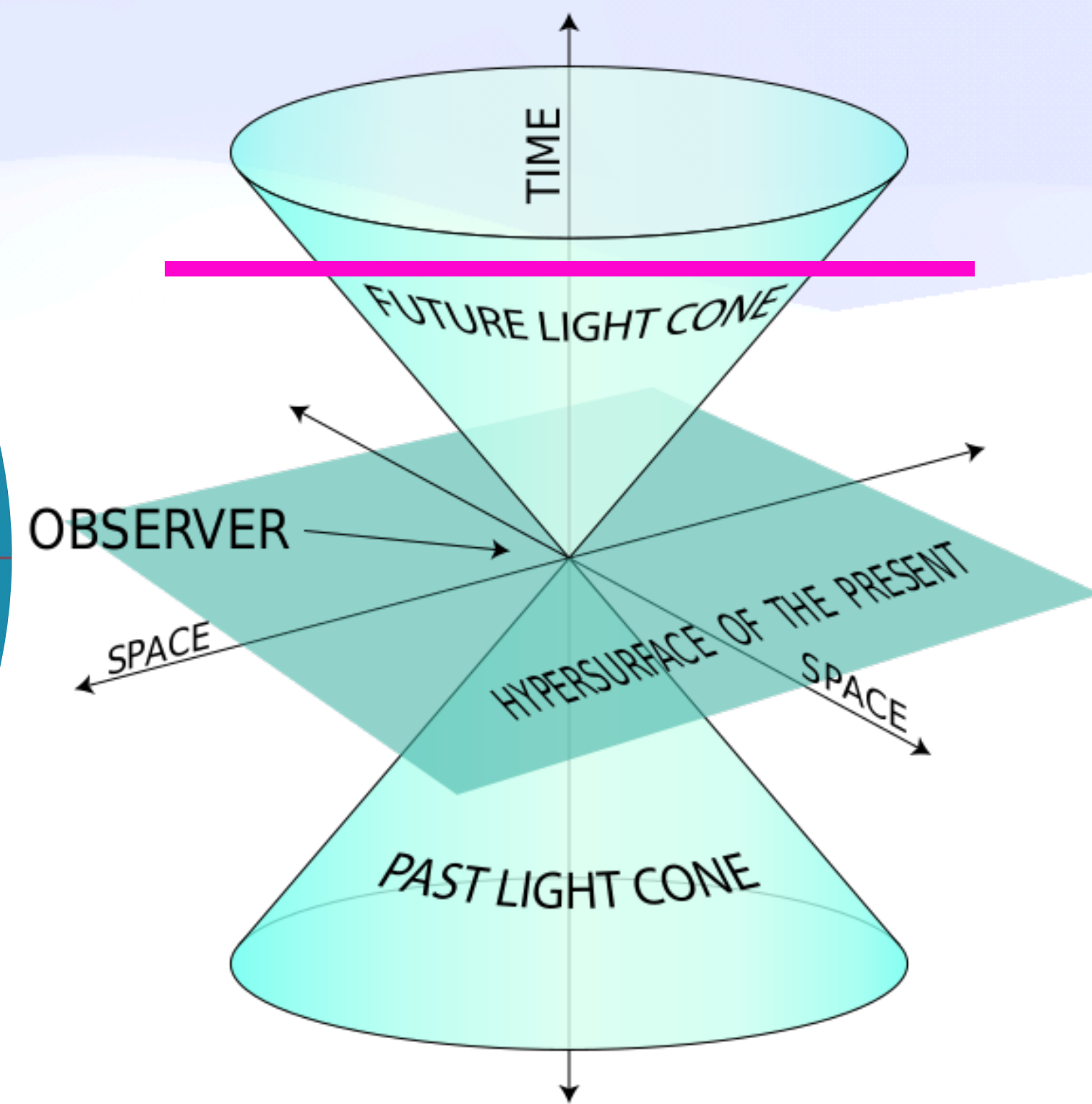
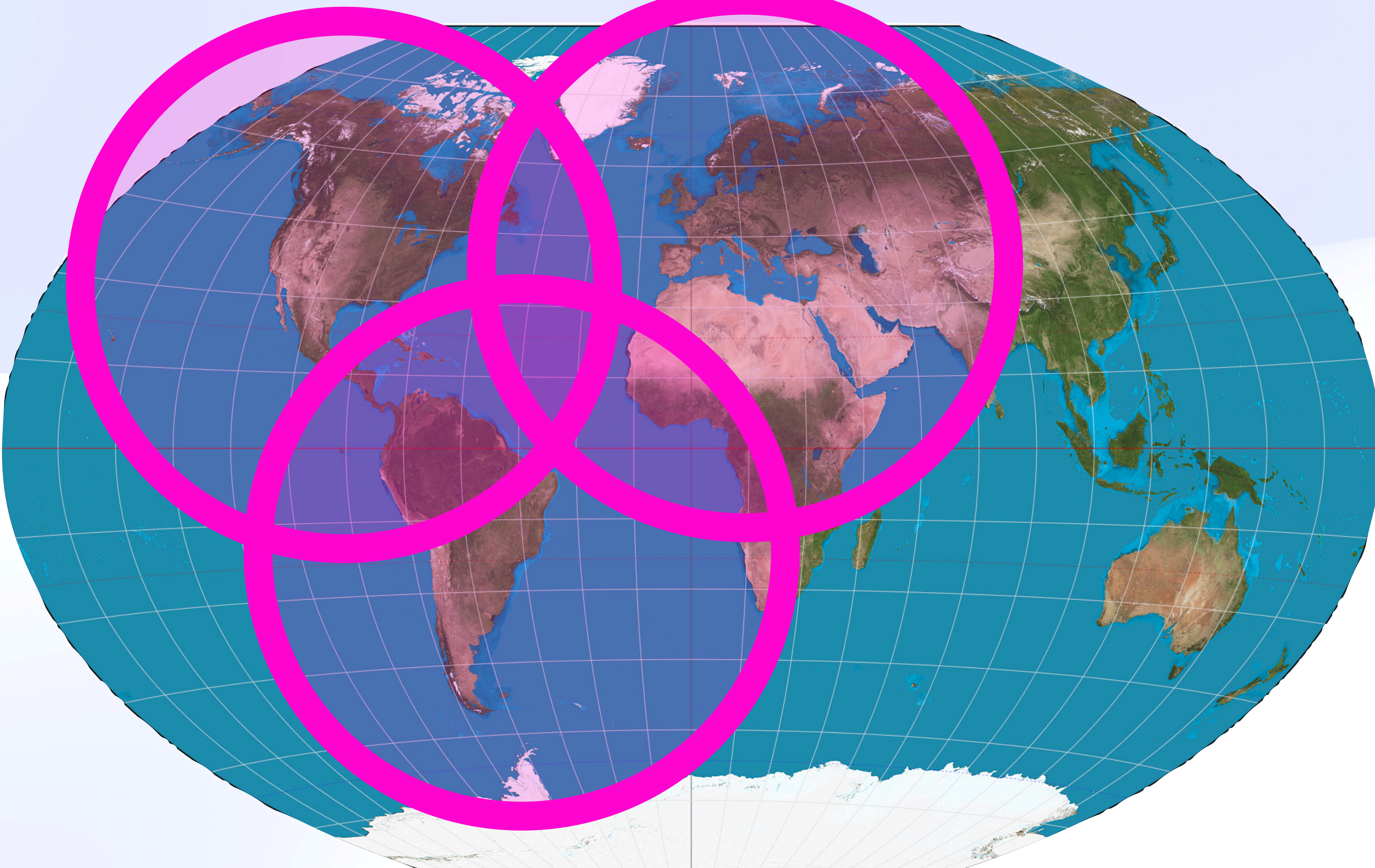
How to Power a New Internet ⚡

Causal Islands 🏖️ 🌴



How to Power a New Internet ⚡

Causal Islands 🏖️ 🌴



How to Power a New Internet ⚡

High Level Dependencies

How to Power a New Internet ⚡

High Level Dependencies

Compute 

How to Power a New Internet ⚡

High Level Dependencies

Compute 

Data 

How to Power a New Internet ⚡

High Level Dependencies

Compute 

Data 

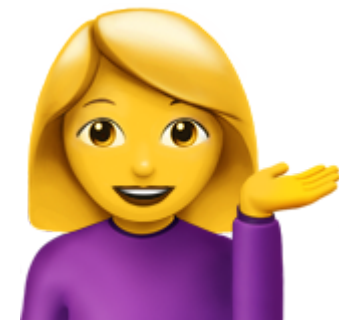
Auth 

How to Power a New Internet ⚡

Too Much & Not Enough

How to Power a New Internet ⚡

Too Much & Not Enough



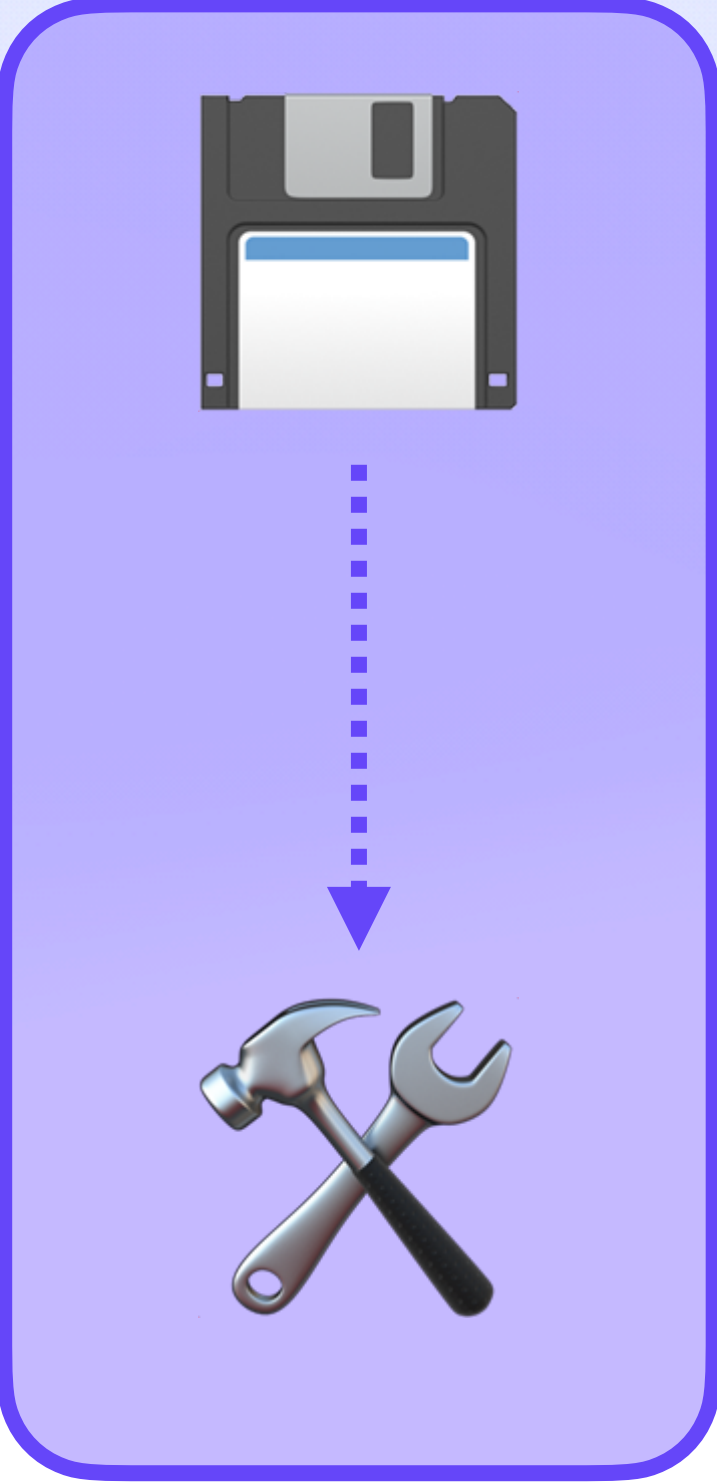
How to Power a New Internet ⚡

Too Much & Not Enough



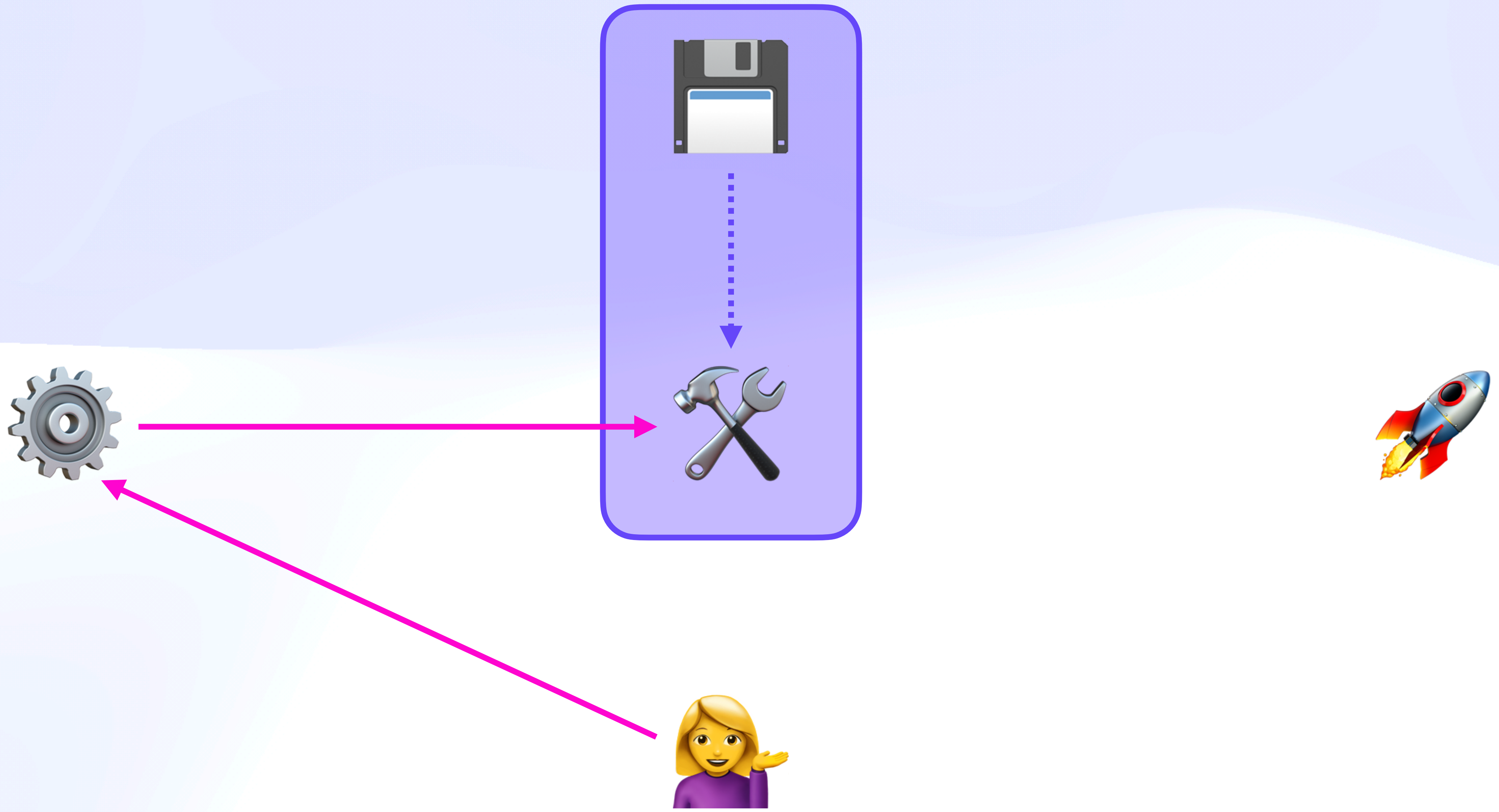
How to Power a New Internet ⚡

Too Much & Not Enough



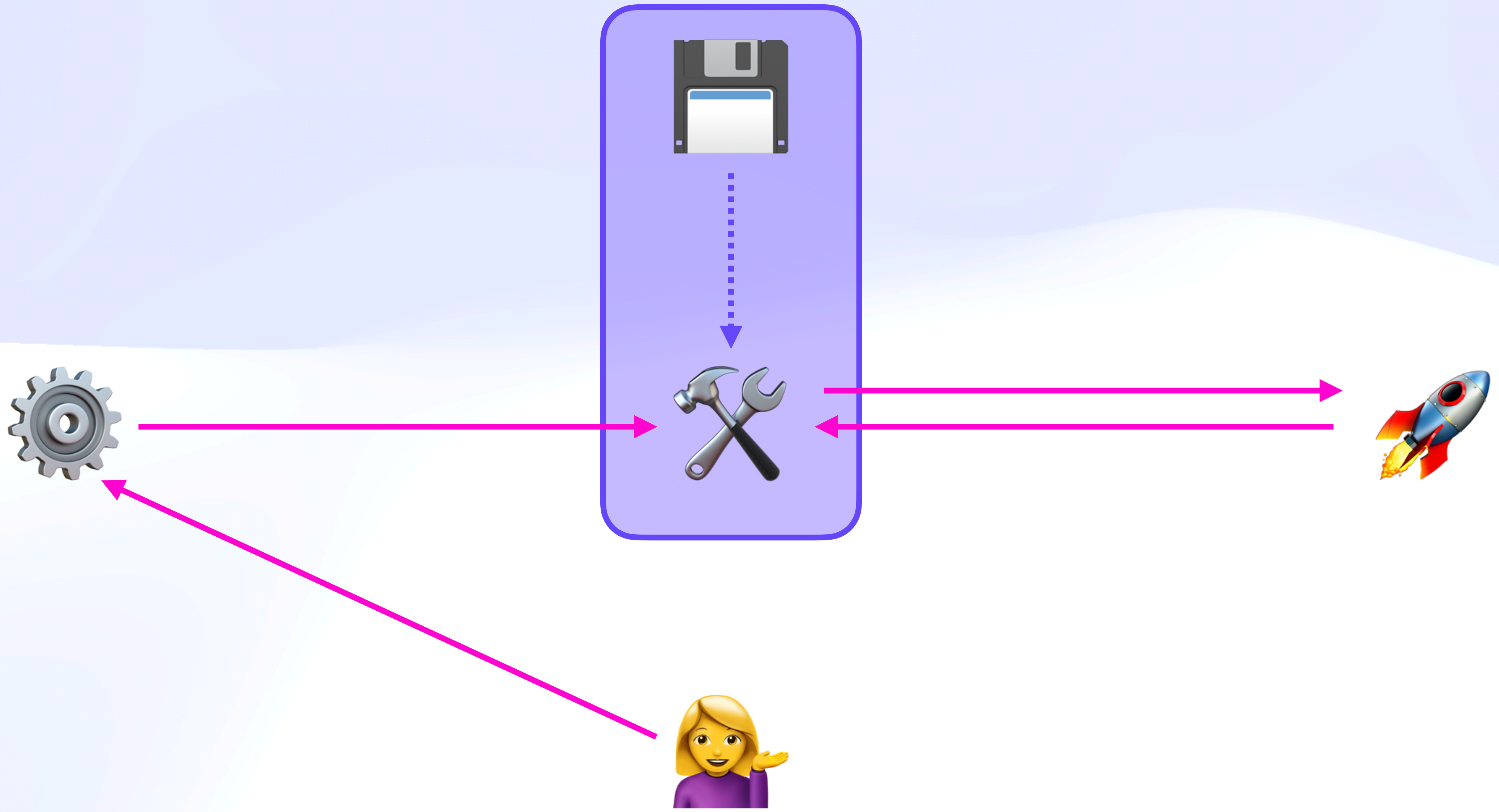
How to Power a New Internet ⚡

Too Much & Not Enough



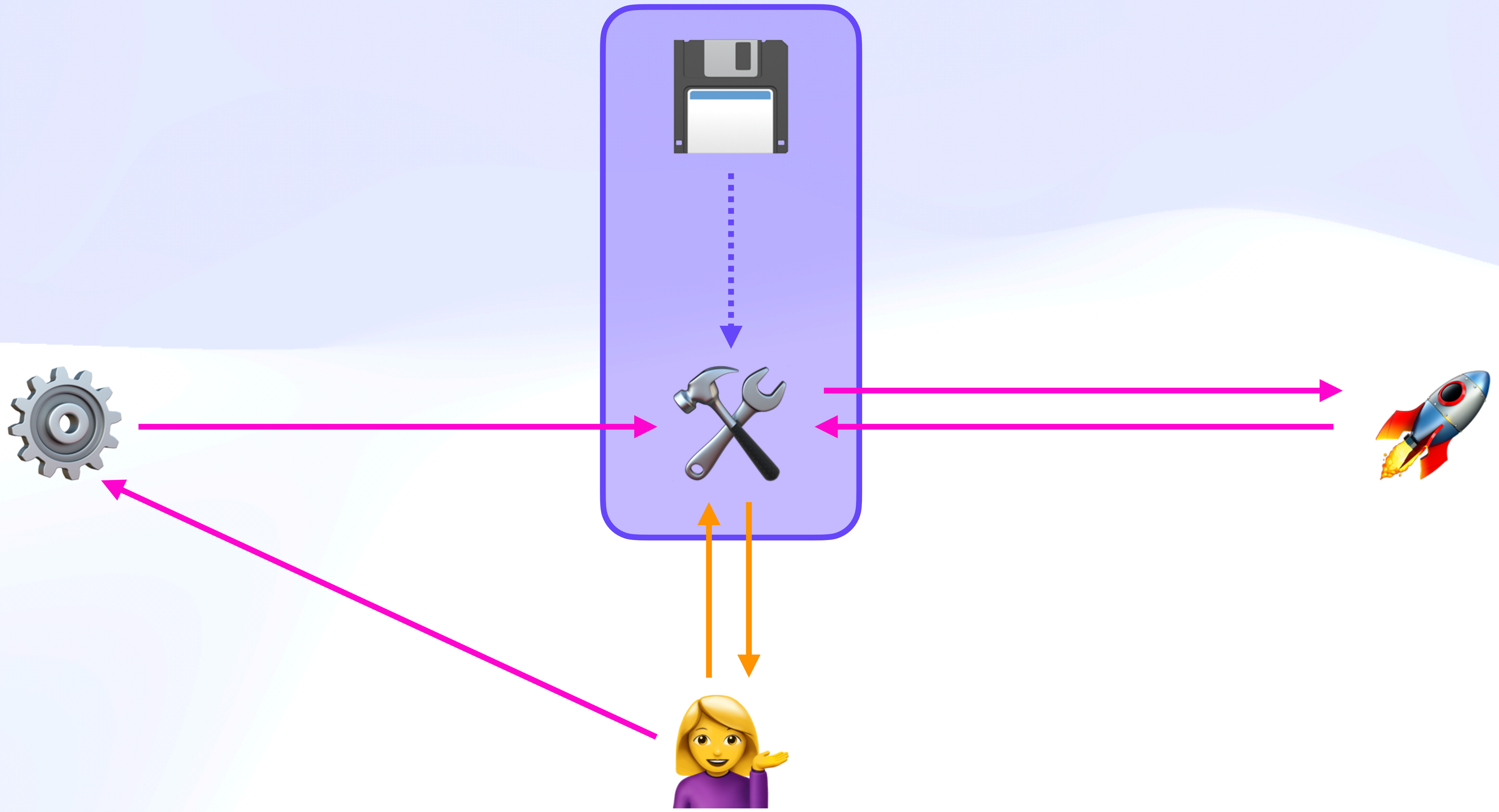
How to Power a New Internet ⚡

Too Much & Not Enough



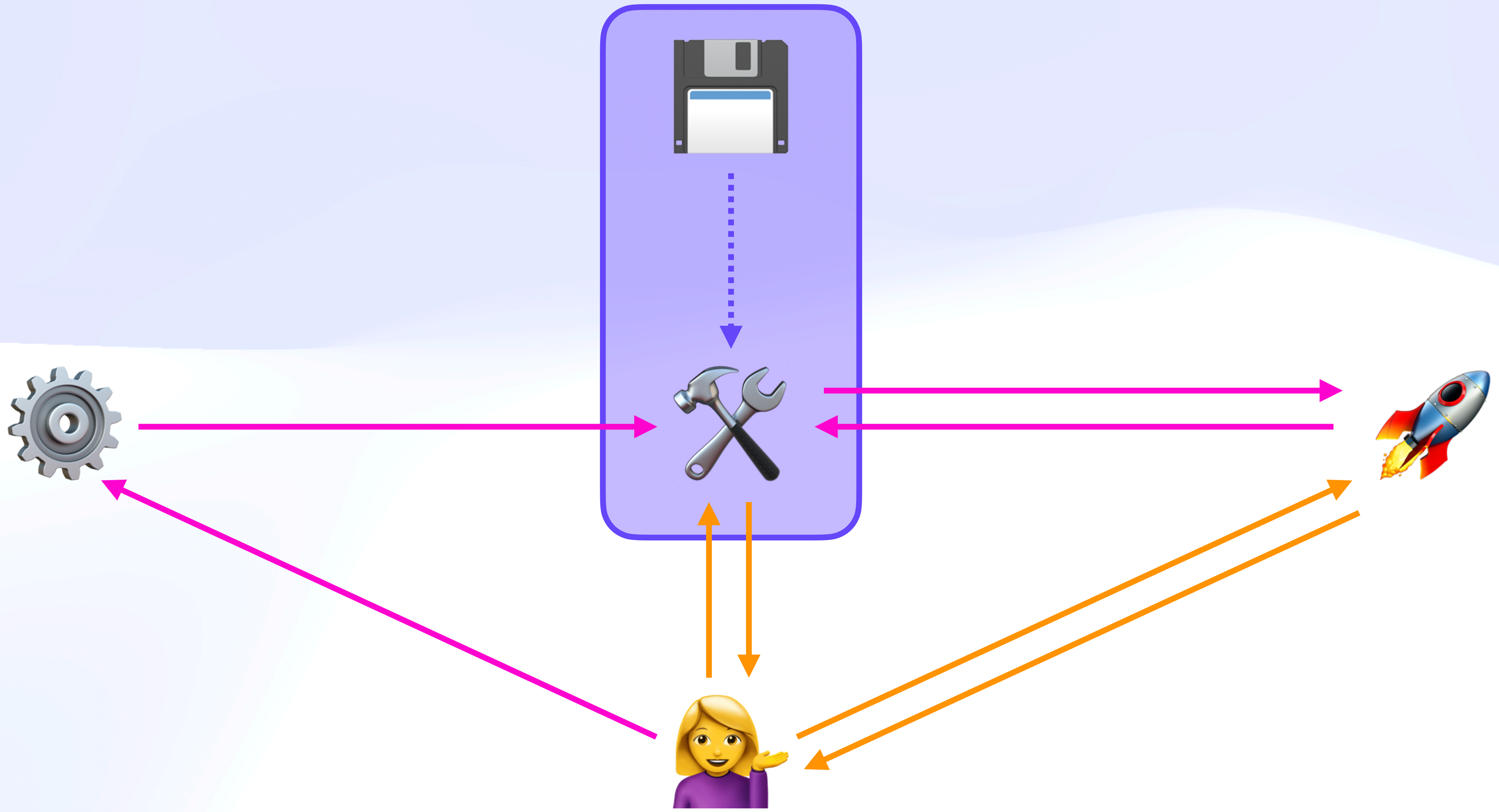
How to Power a New Internet ⚡

Too Much & Not Enough



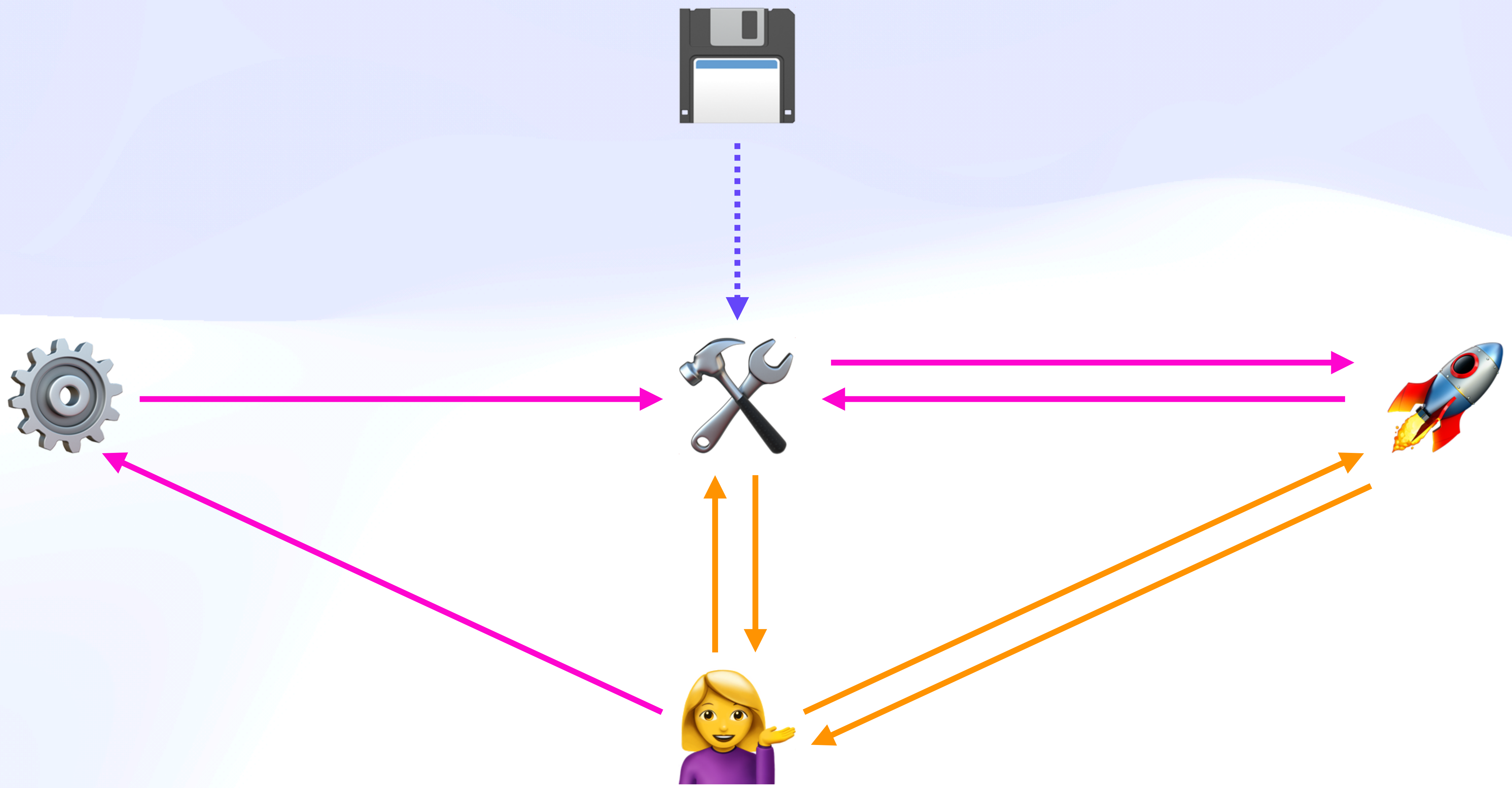
How to Power a New Internet ⚡

Too Much & Not Enough



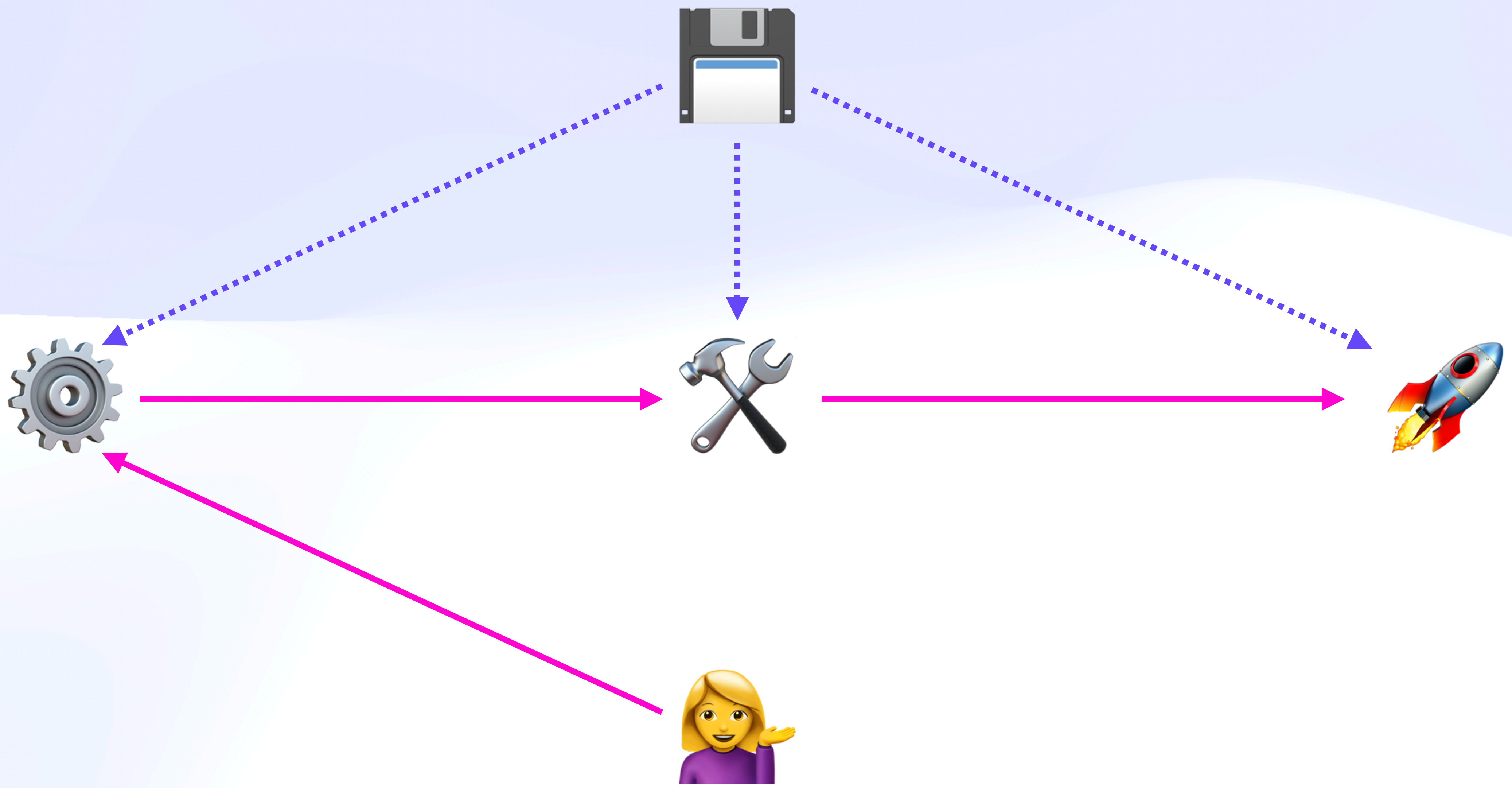
How to Power a New Internet ⚡

Too Much & Not Enough



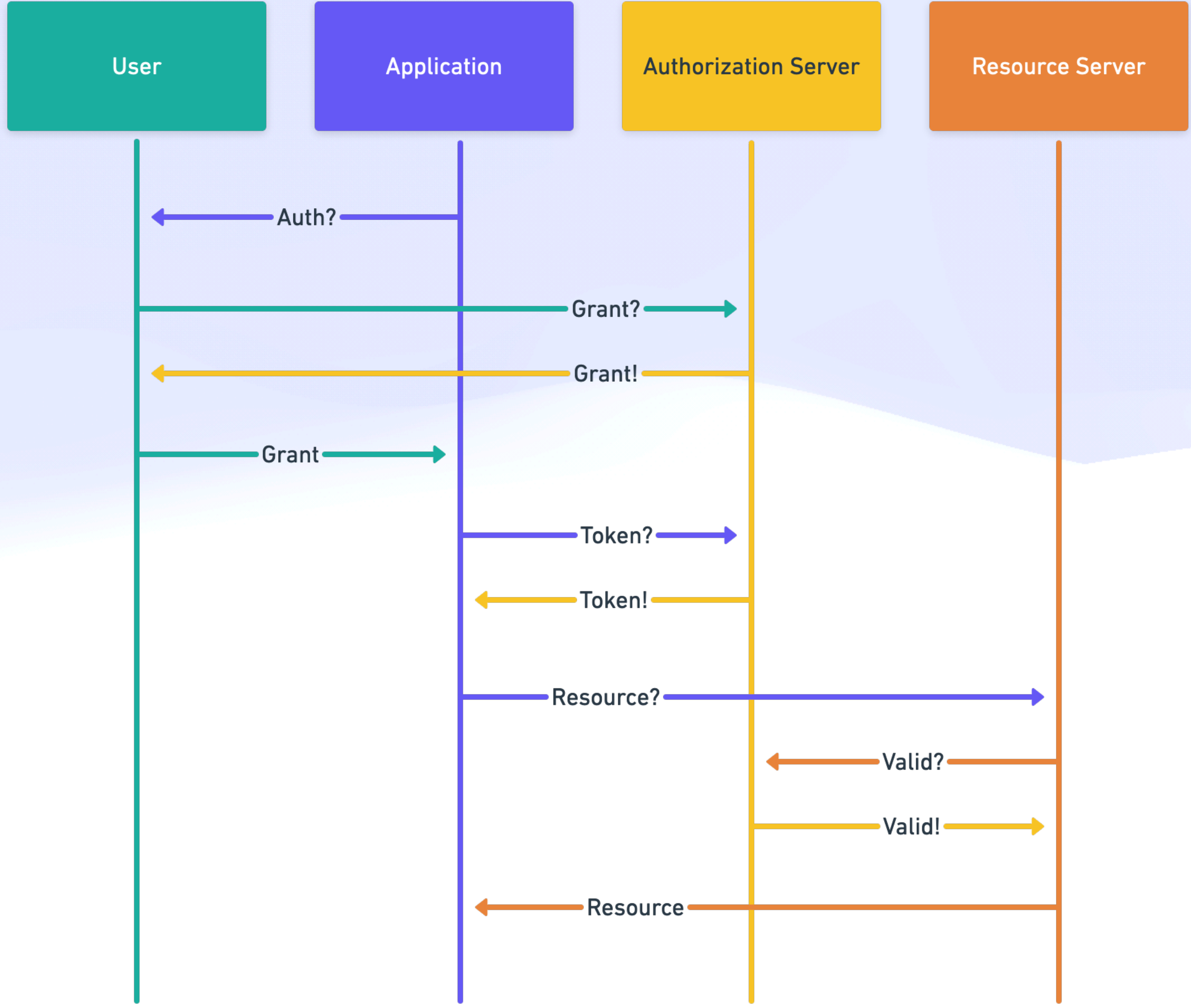
How to Power a New Internet ⚡

What We Want



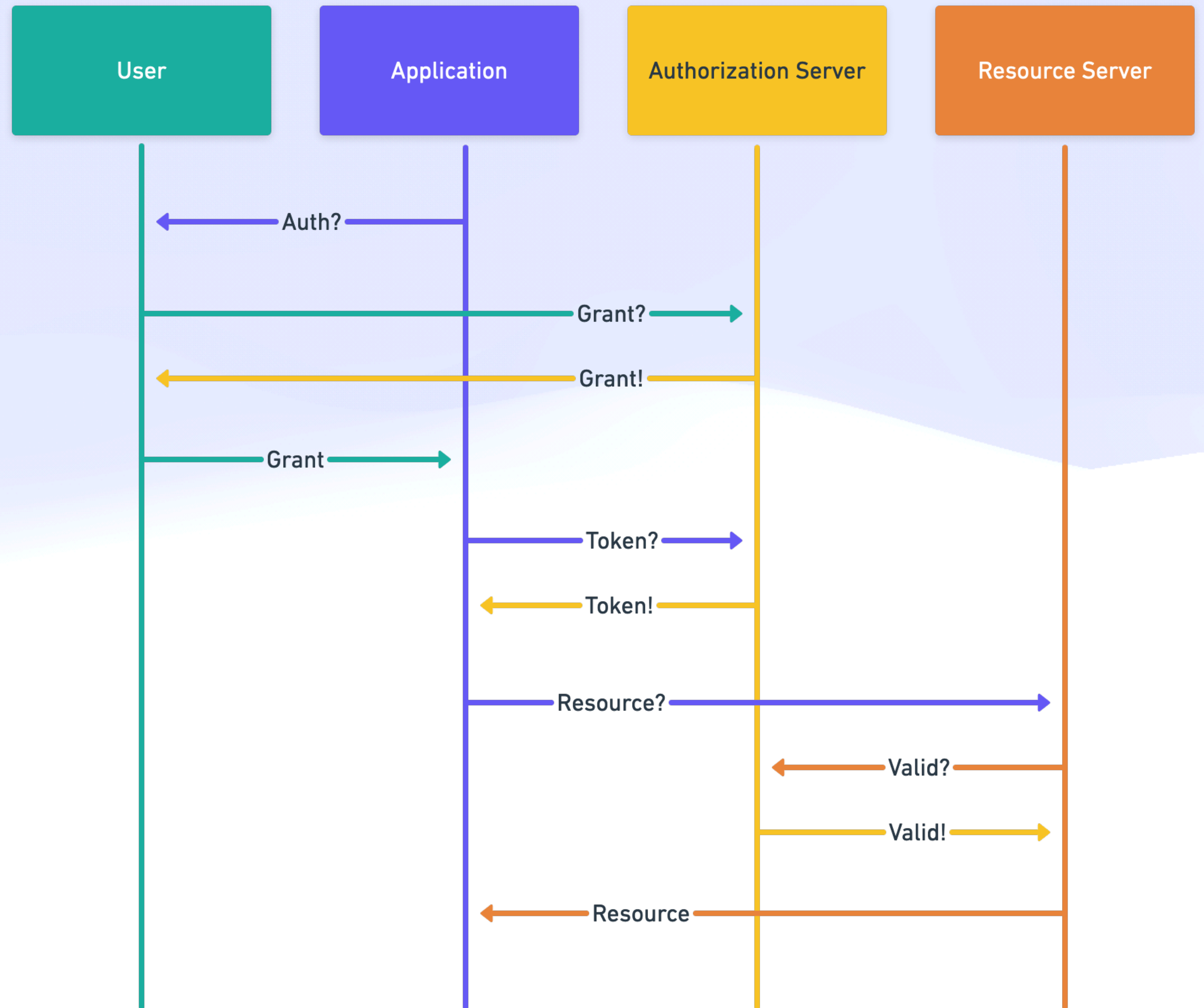
How to Power a New Internet ⚡

OAuth Sequence



How to Power a New Internet ⚡

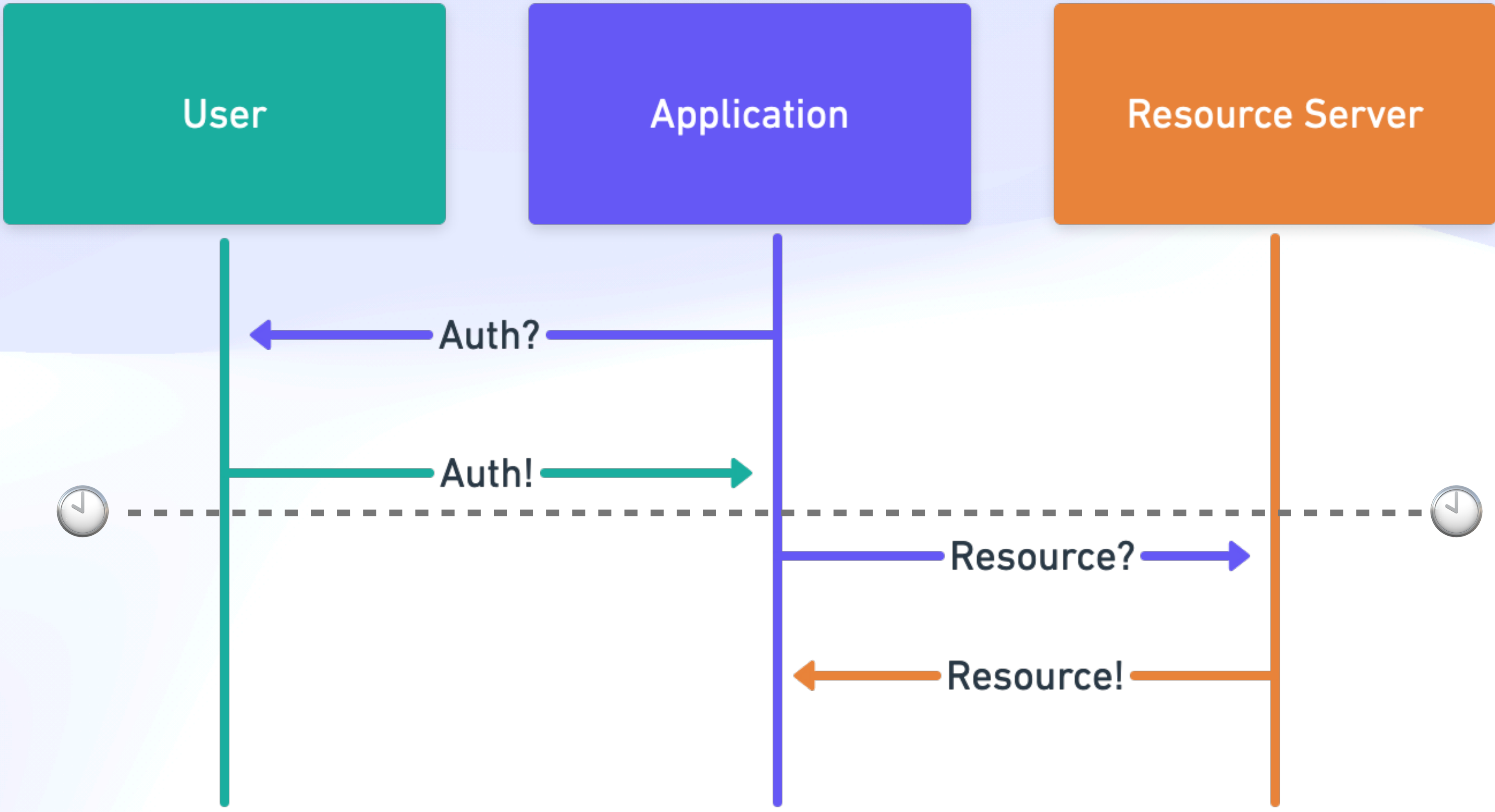
OAuth Sequence



Latency & Locality Problems!

How to Power a New Internet ⚡

UCAN Sequence



How to Power a New Internet ⚡

Auth Should Be Boring

DRIVE

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

🔗 Sign in with Fission

How to Power a New Internet ⚡

Auth Should Be Boring

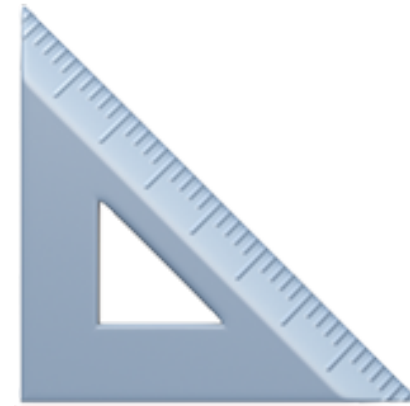
DRIVE

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

🔗 Sign in with Fission

User Controlled, Local-First, Universal Auth

Yes, UCAN!



Yes, UCAN!

Wherefore Art Thou UCAN?



Yes, UCAN!

Wherefore Art Thou UCAN?

DIDs say who ***you are***



Yes, UCAN!

Wherefore Art Thou UCAN?

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

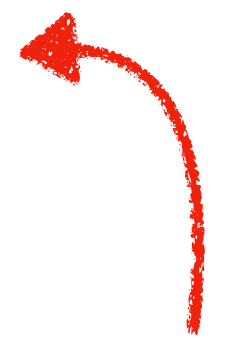


Yes, UCAN!

Wherefore Art Thou UCAN?

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

AuthN



AuthZ



Yes, UCAN!

Teaser Token

```
eyJhbGciOiJIJZERTQSIiInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V50no2TWtzWFFCZkw4b3d6dFRDSlRtN2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiaWF0IjoiT1ZFUldSSVRFIn1dLCJleHAiOi0jkyNTY5Mzk1MDUsImZcyI6ImRpZDprZXk6ejZNa3A1RXN60XMyTUhzcVl2TG9jY3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjoxNjM5NjA4MjkzLCJwcmYiOi0ldtdfQ.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"
    }
  ]
}
```

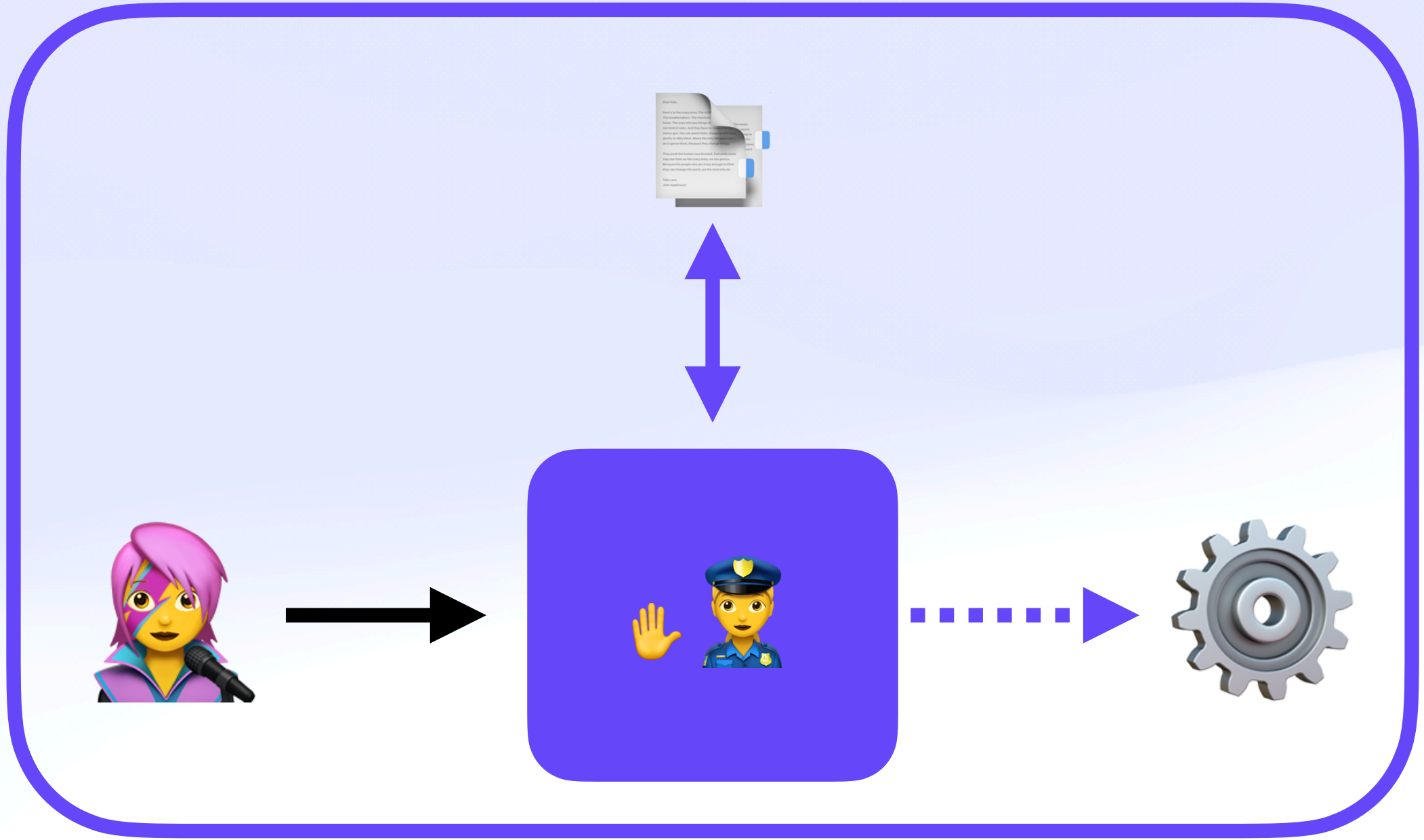
Yes, UCAN!

AuthZ Models

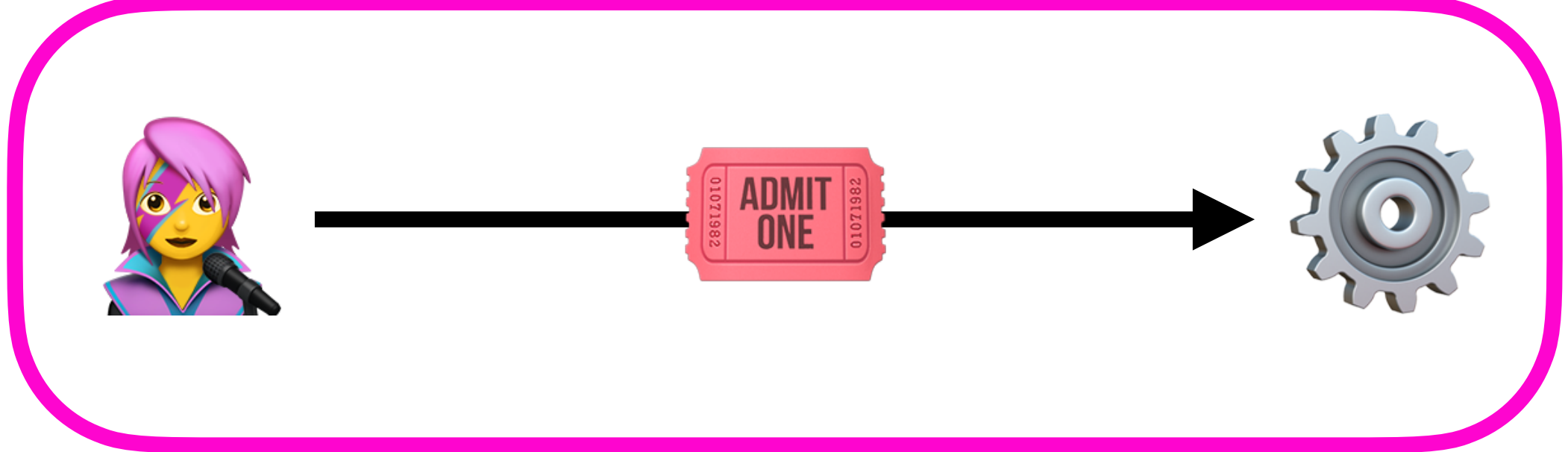
Yes, UCAN!

AuthZ Models

ACLs



Caps



Yes, UCAN!

ACL Read & Write

Yes, U CAN!

ACL Read & Write



Yes, UCAN!

ACL Read & Write



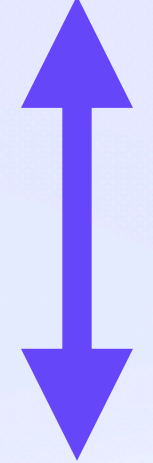
Yes, UCAN!

ACL Read & Write



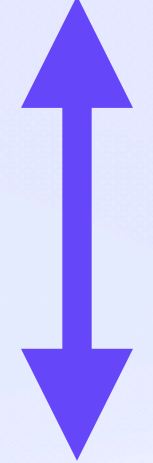
Yes, UCAN!

ACL Read & Write



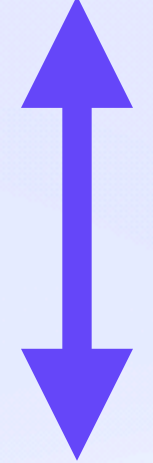
Yes, UCAN!

ACL Read & Write



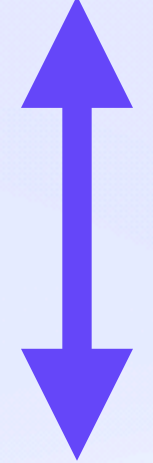
Yes, UCAN!

ACL Read & Write



Yes, UCAN!

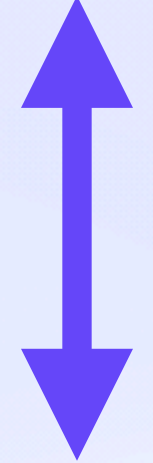
ACL Read & Write



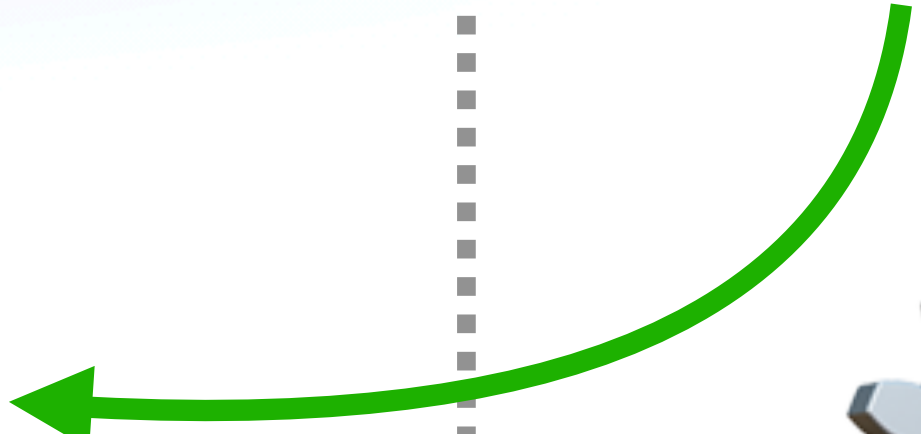
Not in control

Yes, UCAN!

ACL Read & Write



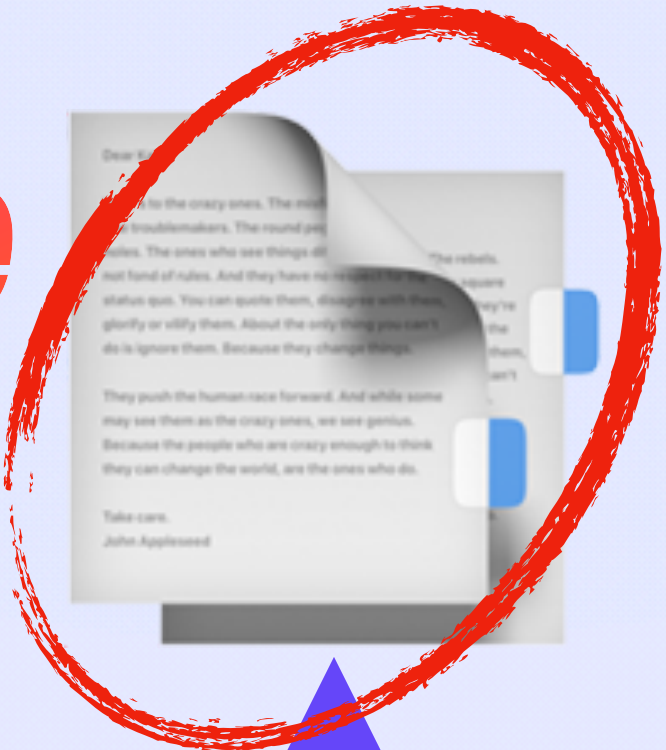
In control



Not in control

Yes, UCAN!

ACL Read & Write



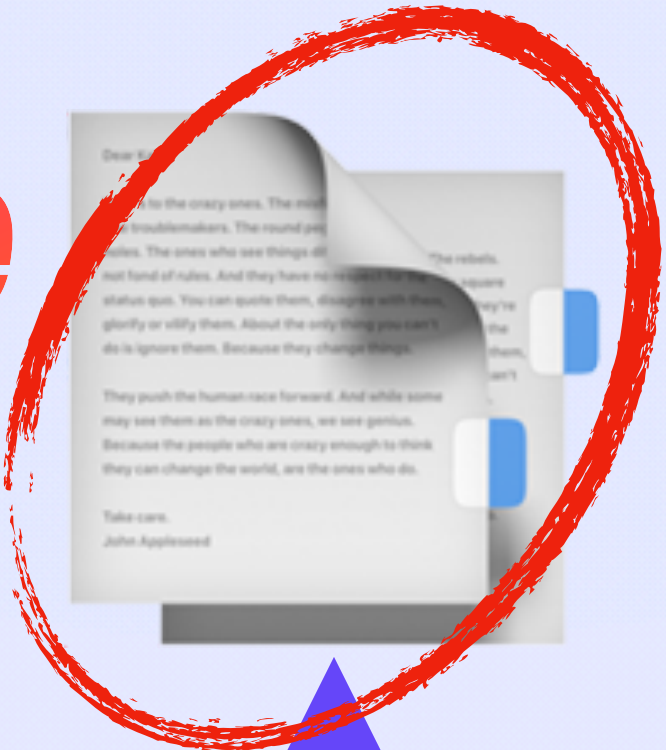
In control



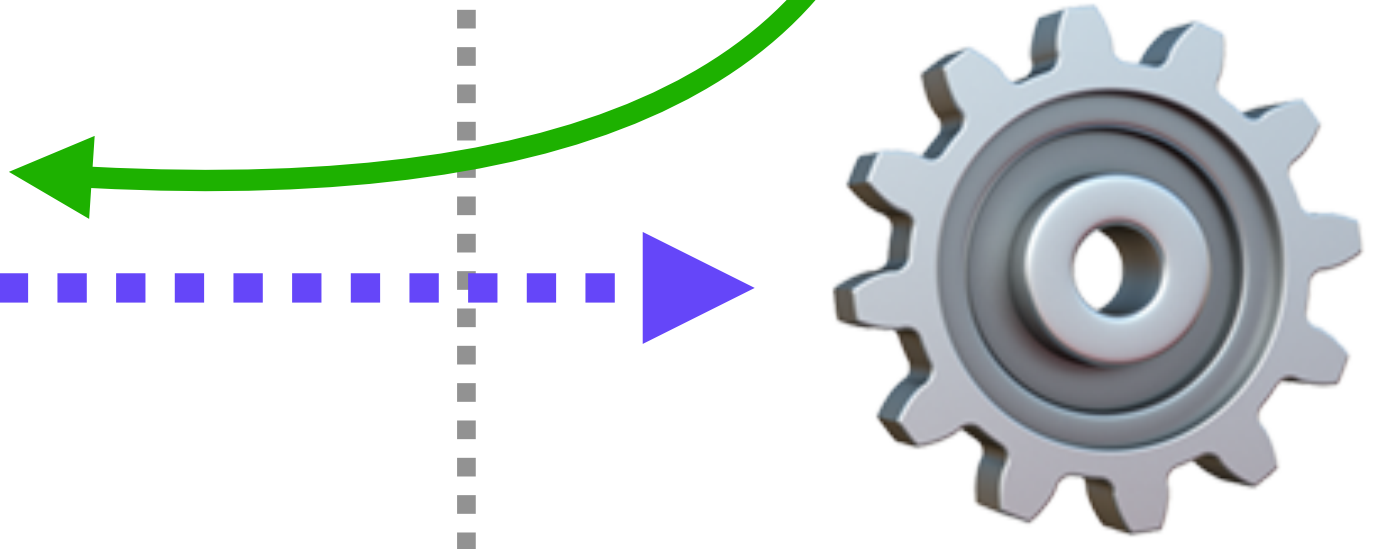
Not in control

Yes, UCAN!

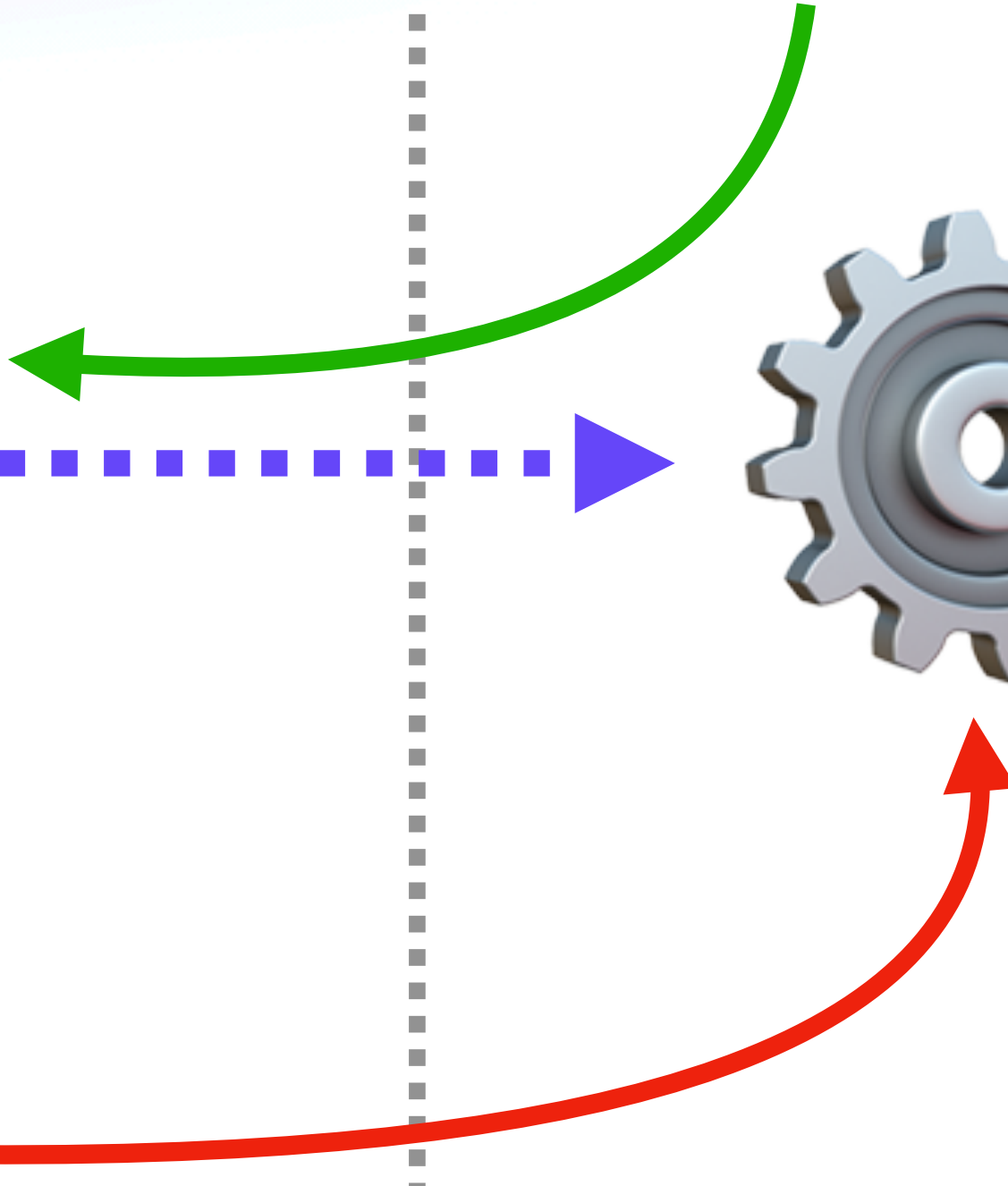
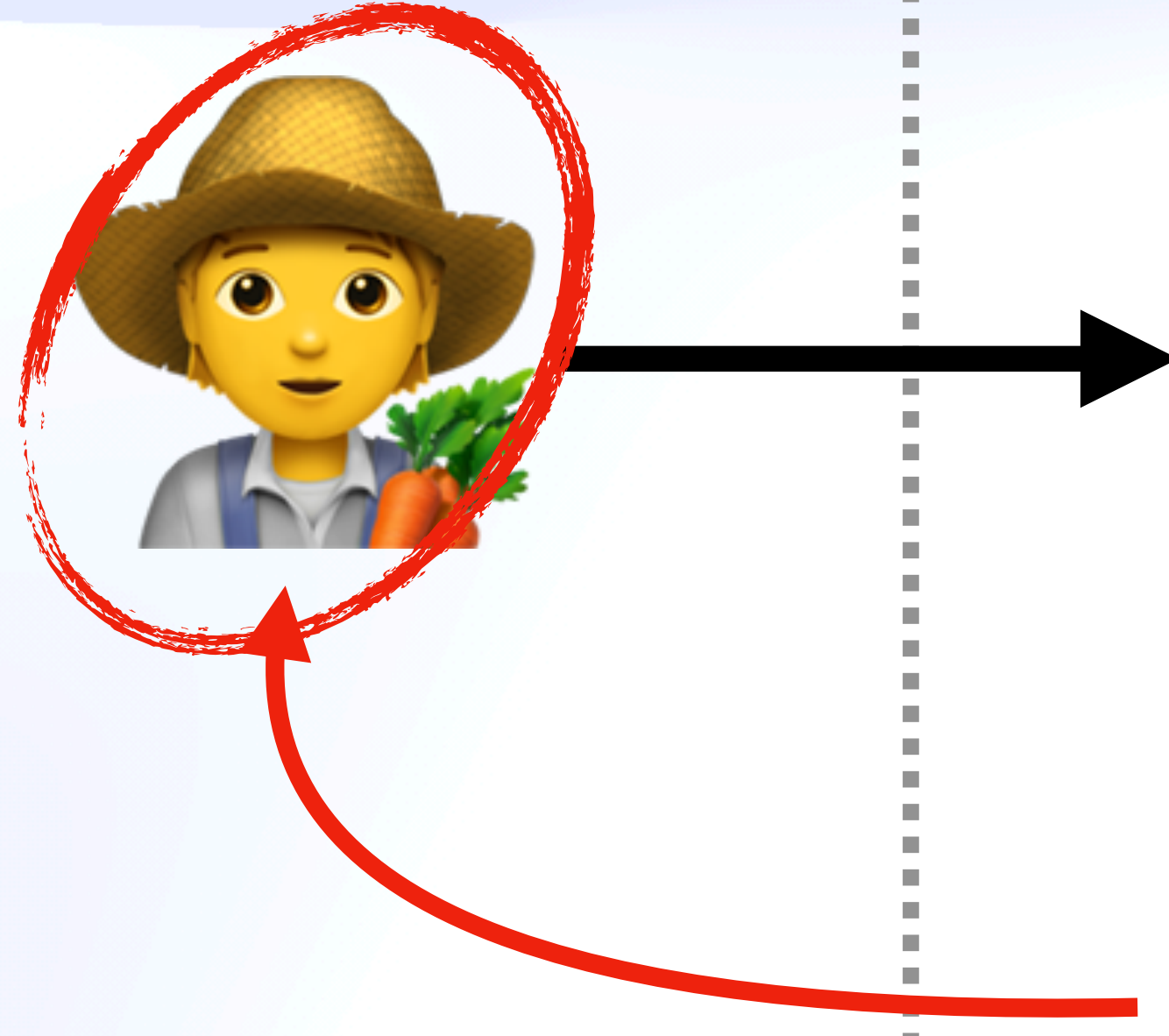
ACL Read & Write



In control



Not in control



Yes, UCAN!

Capabilities-as-Tickets

Yes, UCAN!

Capabilities-as-Tickets



Yes, UCAN!

Capabilities-as-Tickets



Yes, UCAN!

Capabilities-as-Tickets



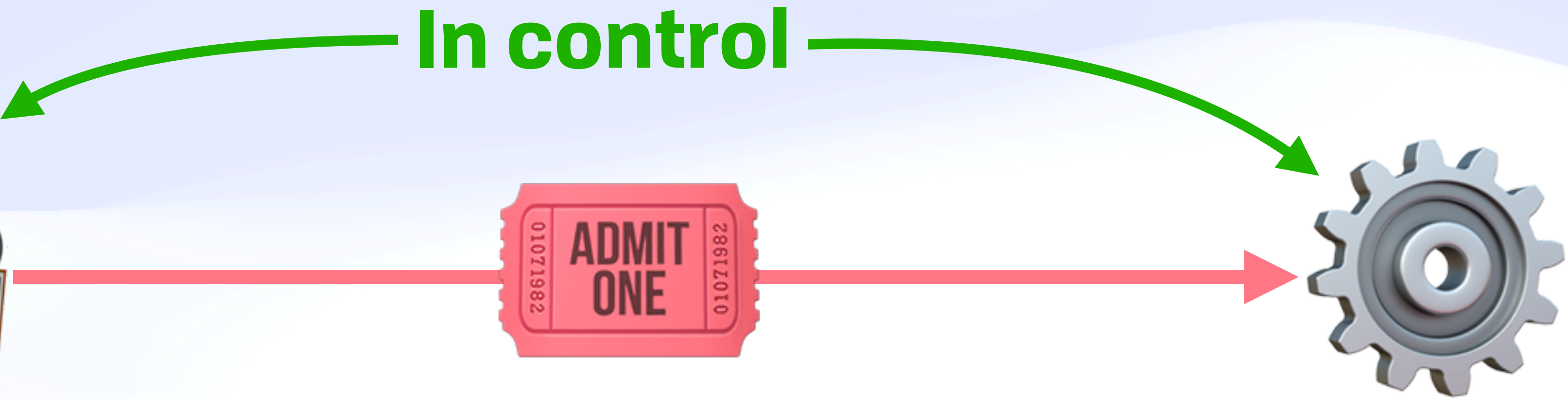
Yes, UCAN!

Capabilities-as-Tickets



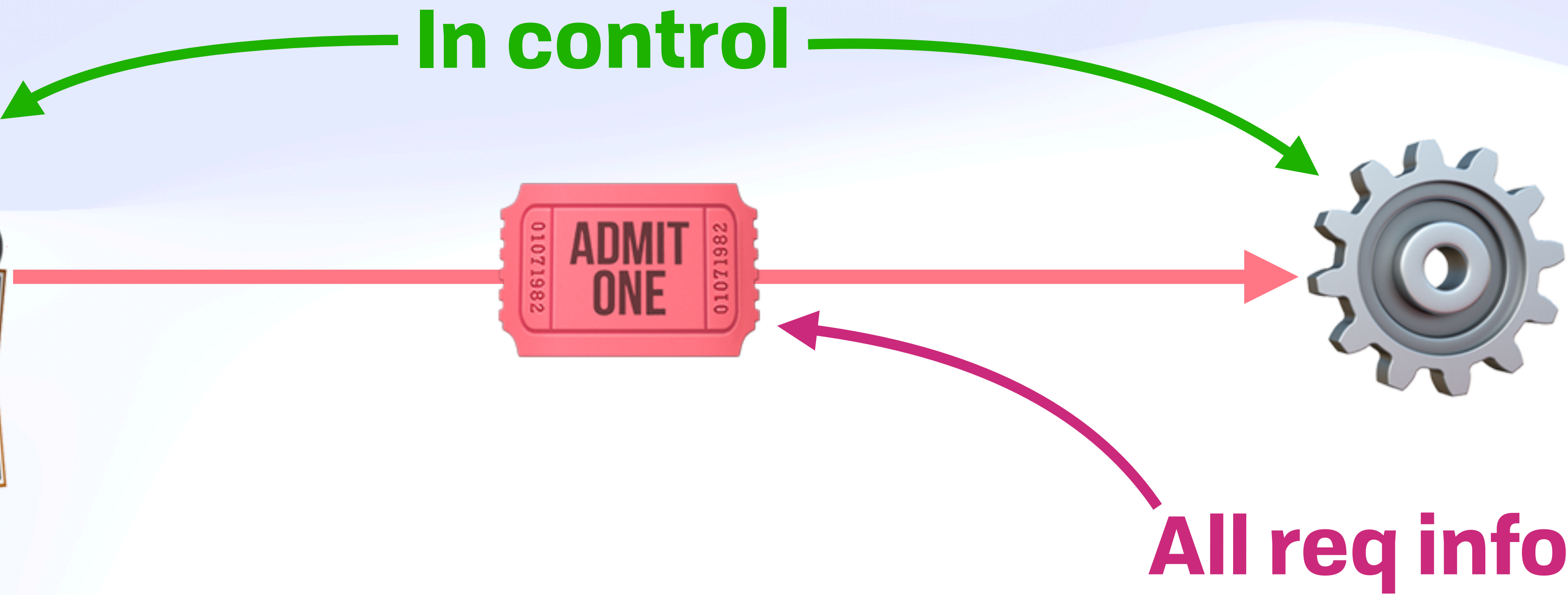
Yes, UCAN!

Capabilities-as-Tickets



Yes, UCAN!

Capabilities-as-Tickets



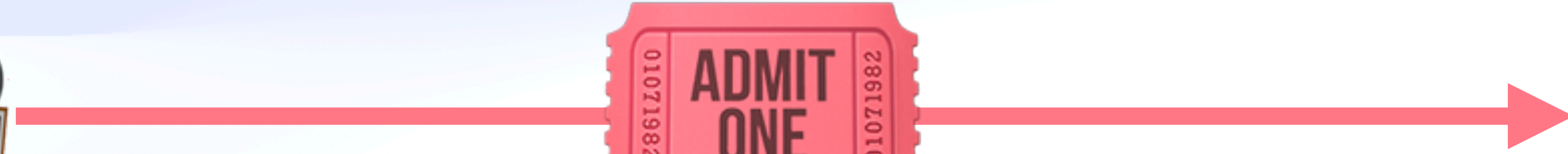
Yes, UCAN!

Capabilities-as-Tickets



Yes, UCAN!

Capabilities-as-Tickets



Yes, UCAN!

Capabilities-as-Tickets



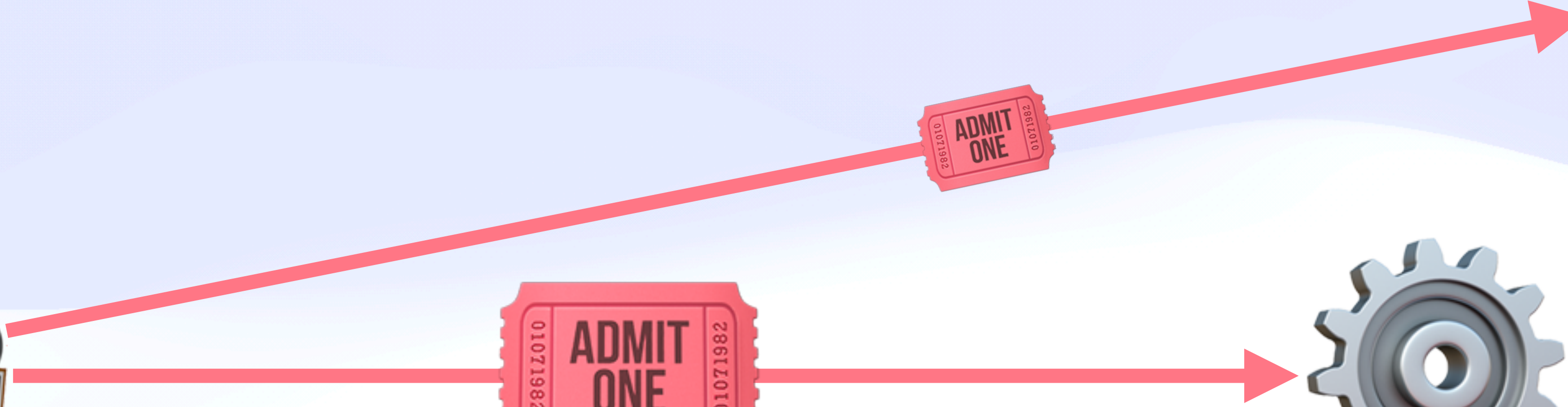
Yes, UCAN!

Capabilities-as-Tickets



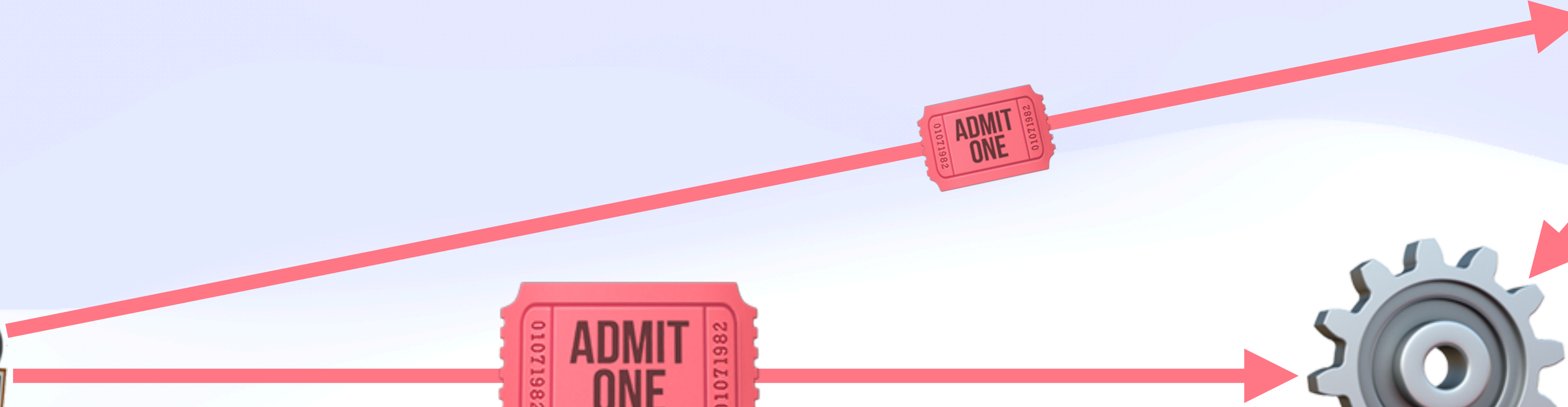
Yes, UCAN!

Capabilities-as-Tickets



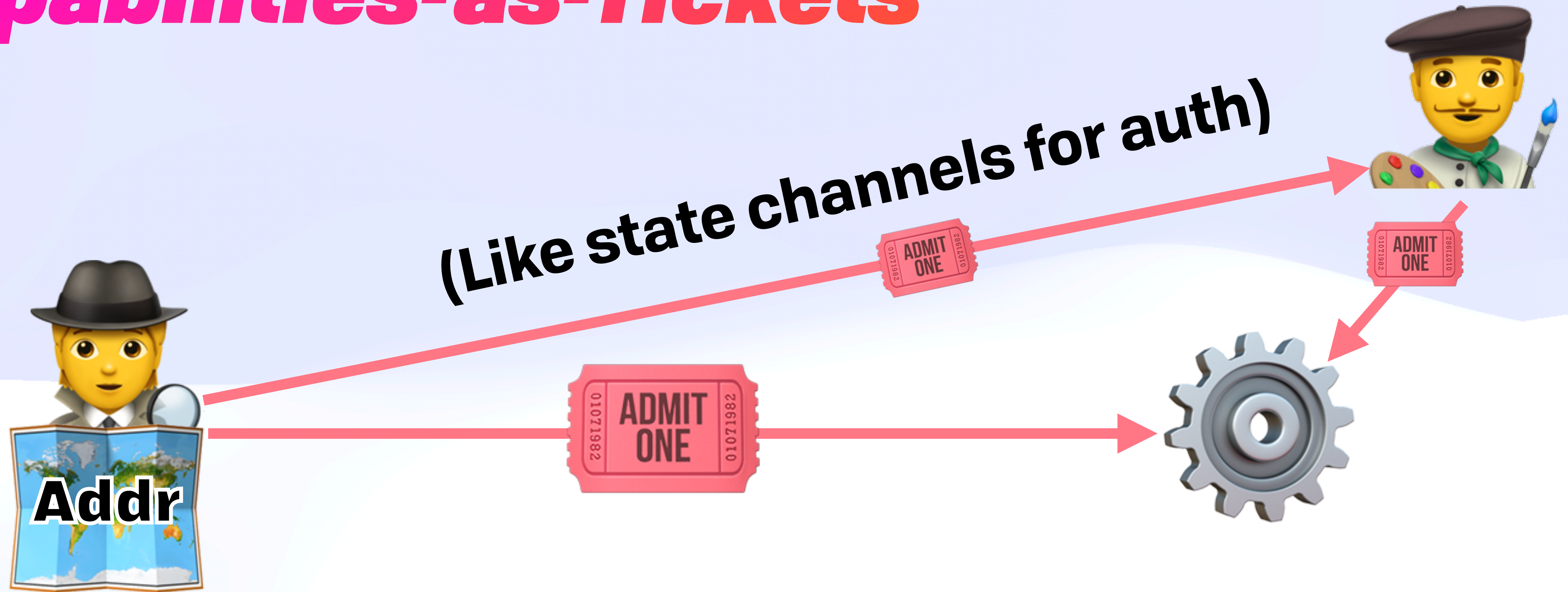
Yes, UCAN!

Capabilities-as-Tickets



Yes, UCAN!

Capabilities-as-Tickets



Yes, UCAN!

Rights Amplification

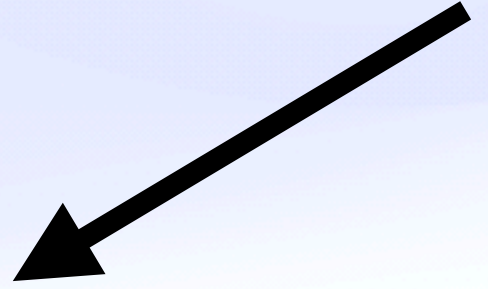
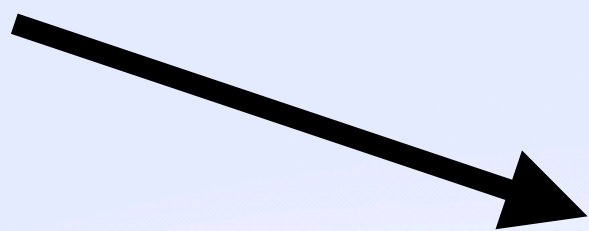
Yes, UCAN!

Rights Amplification



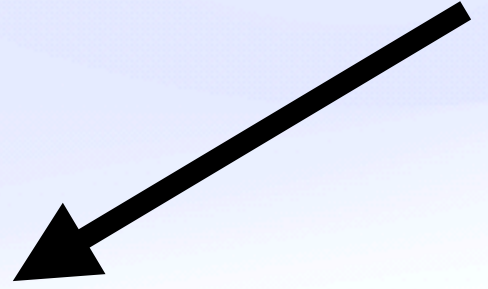
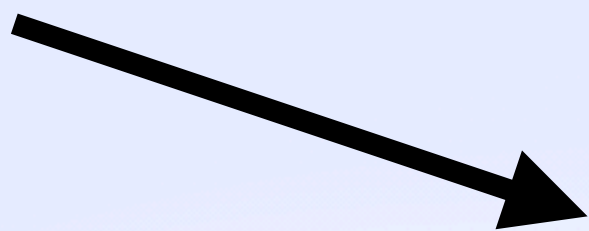
Yes, UCAN!

Rights Amplification



Yes, UCAN!

Rights Amplification



Yes, UCAN!

JWT → ***UCAN***

Yes, UCAN!

JWT → ***UCAN***

Header

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

Yes, UCAN!

JWT → UCAN

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"
    }
  ]
}
```

Header

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


Yes, 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
```

Yes, UCAN!

JWT → **UCAN**

Payload

```
{  
  "iss": "did:key:z6MksXQBfL8owztTCJm7hNRf6b18YxXPp3i66oJHm8L3YGJ",  
  "aud": "did:key:z6MkvXtP0v0bxtsvQcG07NtK4qKJncgKzLc5zpc75te0pKt",  
  "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"  
    }  
  ]  
}
```

Header

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



Signature

```
kwRdqPN74pkcpXGgdk7Z7FW3M1mRR  
YaDE5ZgkG6srAuu6V6mvMVRdBLnD5  
CWid-X4tDIKpliVjlCSLTntB4pCw
```

Yes, UCAN!

Anatomy of a Capability

Yes, 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/"
    }
  }
]
```

Yes, 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/"
    }
  }
]
```

Yes, UCAN!

Anatomy of a Capability

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

Resource / "noun" →

← *Action / "verb"*

Yes, 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/"  
    }  
  }  
]
```

Resource / "noun" (URI)

Action / "verb"

All the info you need for invocation 😊

Extensible fields

Yes, UCAN!

Composable Standard Library

Yes, 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

Yes, UCAN!

Semantic Extension

Yes, UCAN!

Semantic Extension

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

Yes, UCAN!

Semantic Extension

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

album/publish ⇒ crud/read

Yes, UCAN!

Chain Witnesses

Yes, UCAN!

Chain Witnesses



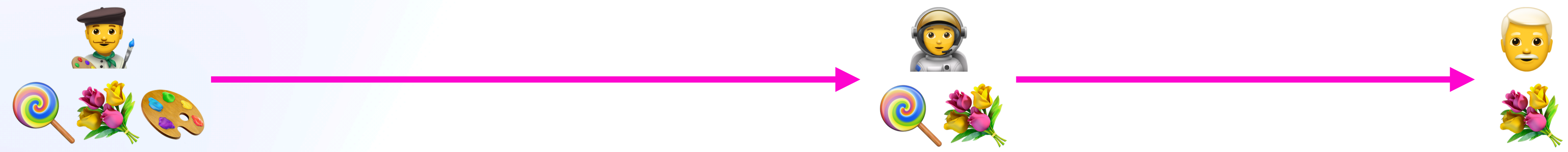
Yes, UCAN!

Chain Witnesses



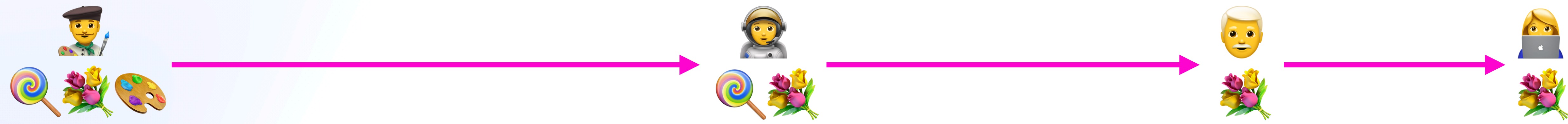
Yes, UCAN!

Chain Witnesses



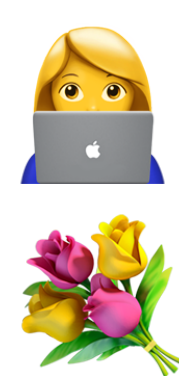
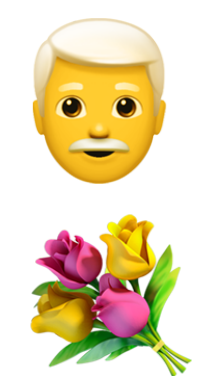
Yes, UCAN!

Chain Witnesses



Yes, UCAN!

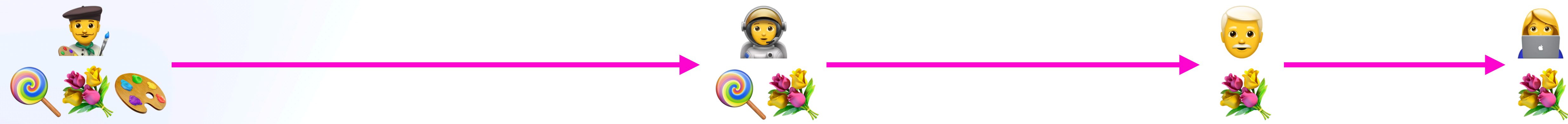
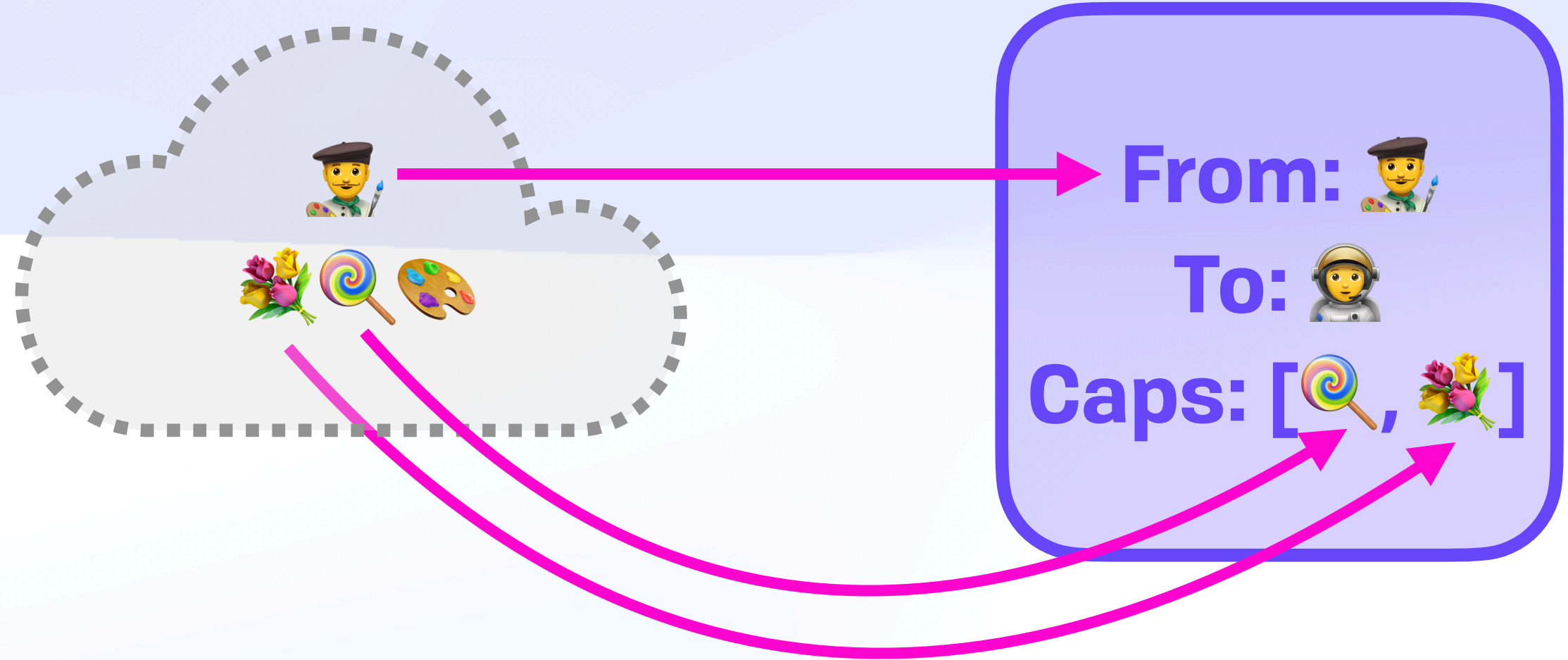
Chain Witnesses



Yes, UCAN!

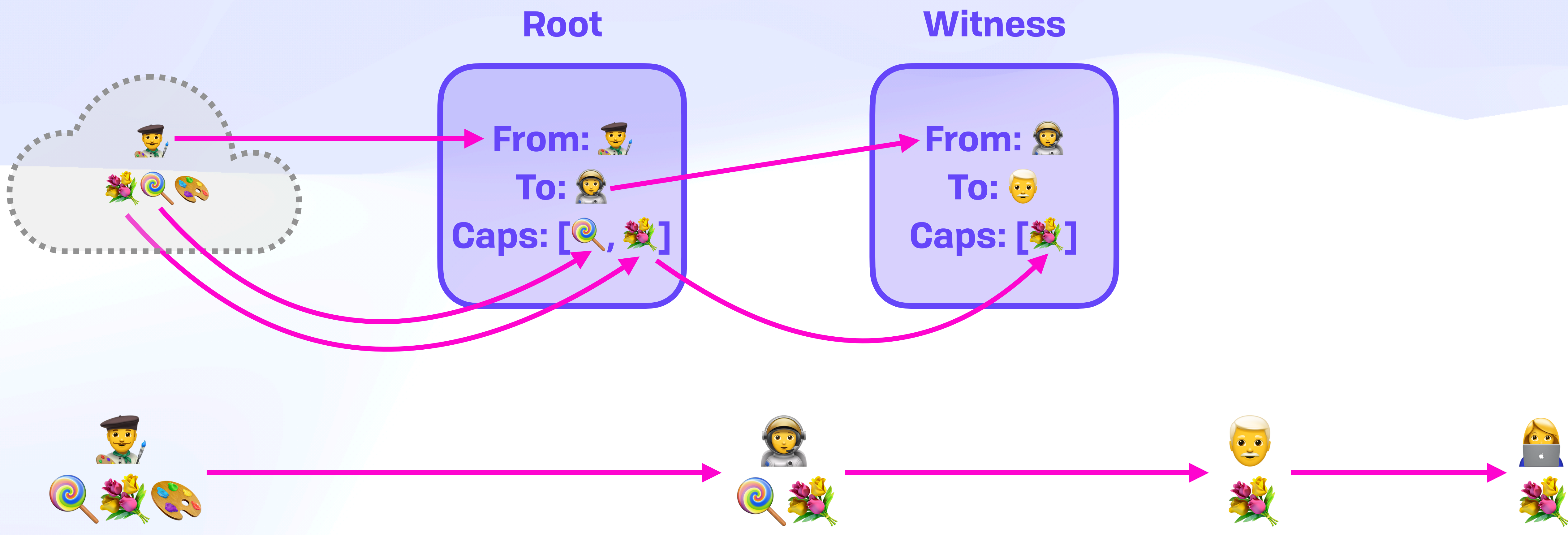
Chain Witnesses

Root



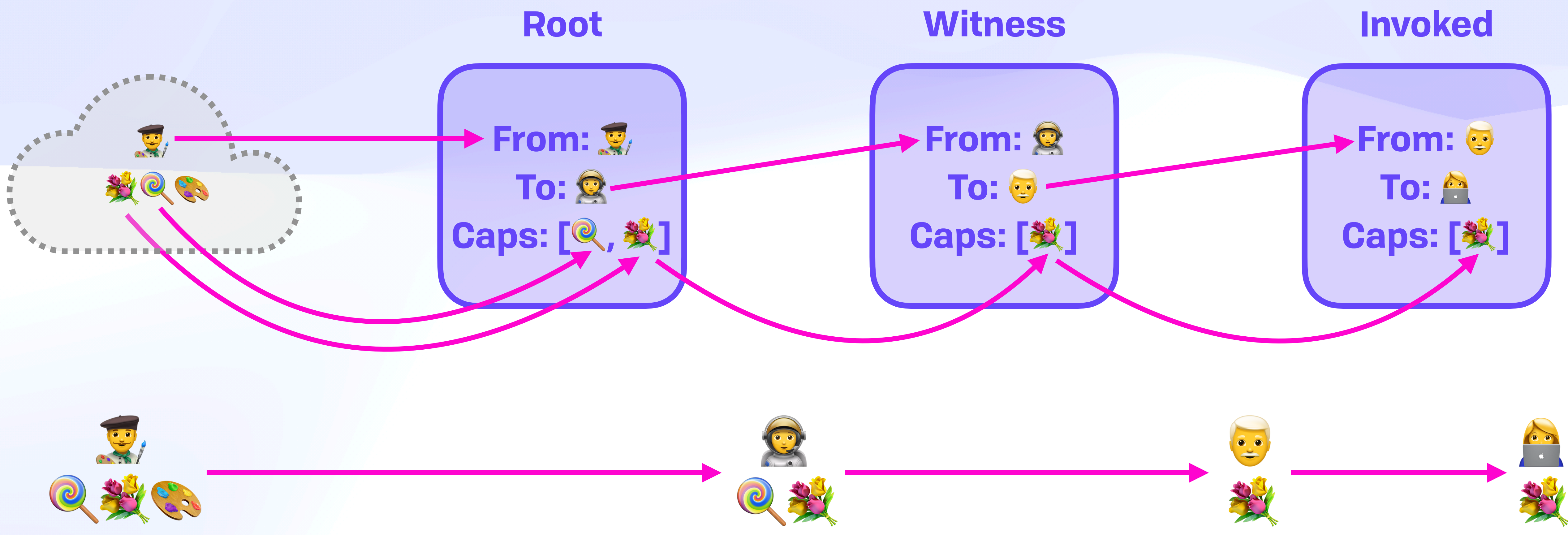
Yes, UCAN!

Chain Witnesses



Yes, UCAN!

Chain Witnesses



Yes, UCAN!

Non-Extractable Browser Keys

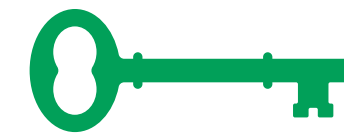
Yes, UCAN!

Non-Extractable Browser Keys



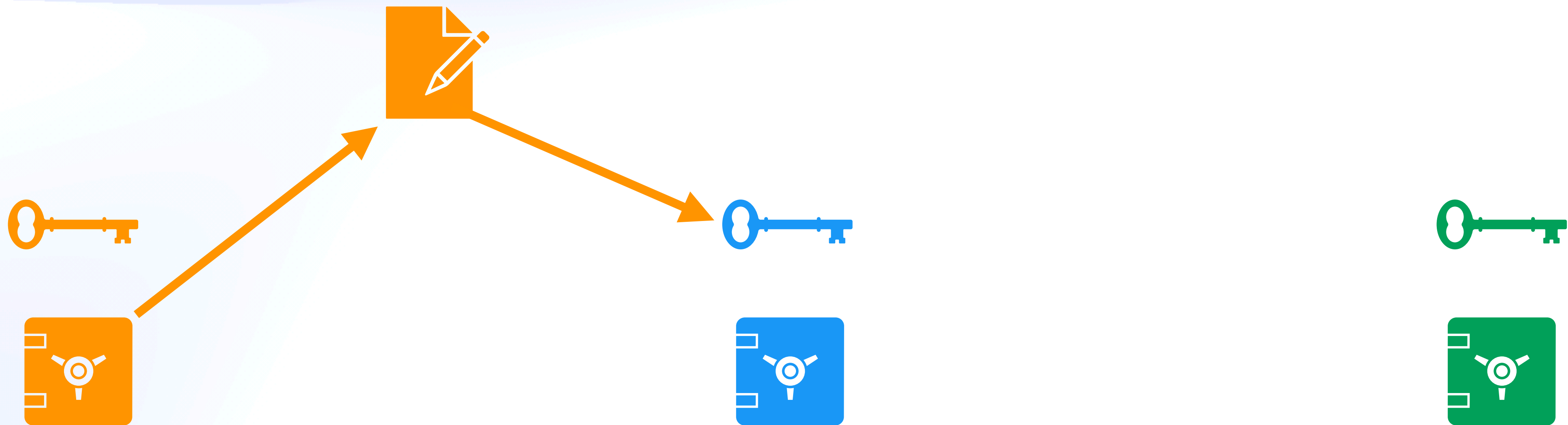
Yes, UCAN!

Non-Extractable Browser Keys



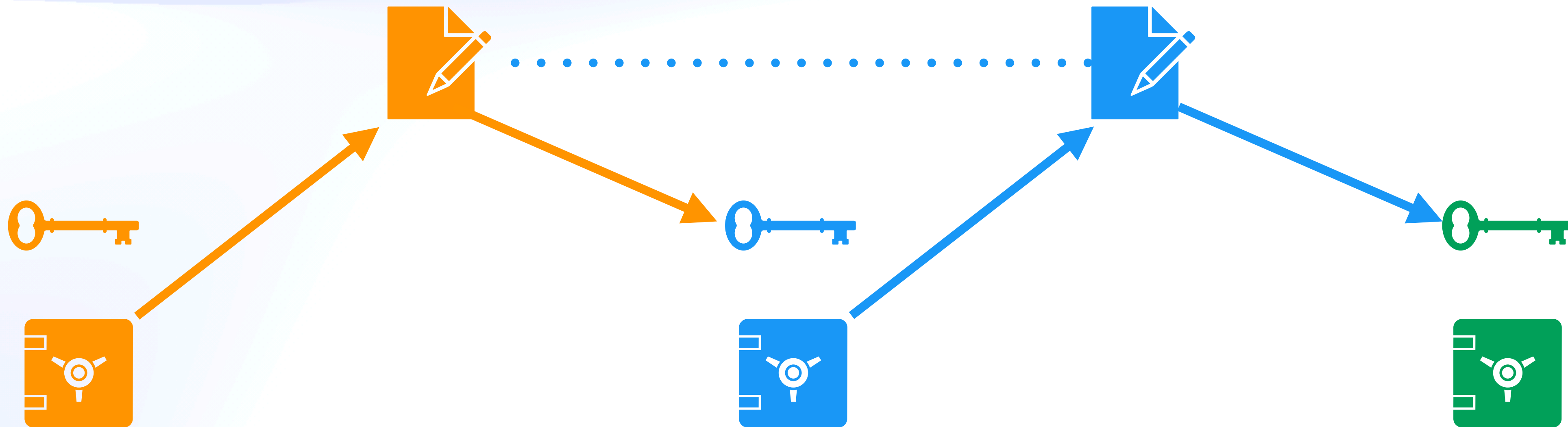
Yes, UCAN!

Non-Extractable Browser Keys



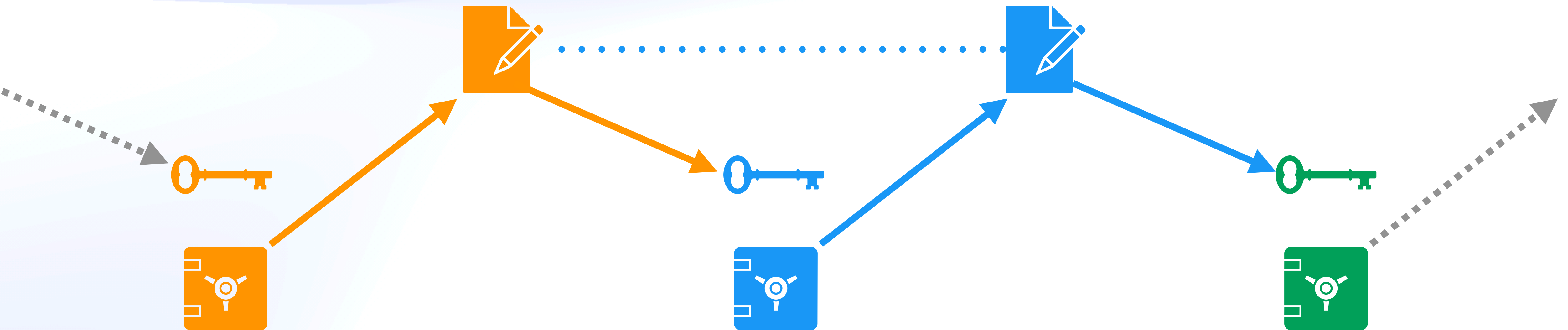
Yes, UCAN!

Non-Extractable Browser Keys



Yes, UCAN!

Non-Extractable Browser Keys



Plugging Things Together

Composition & Flow



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

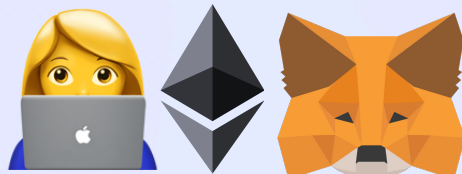
— Alan Perlis, Epigram #16

Composition & Flow

Permissionless

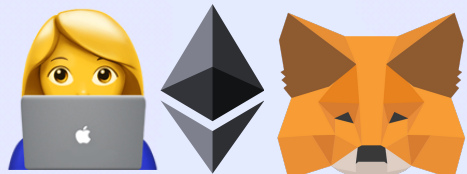
Composition & Flow

Permissionless



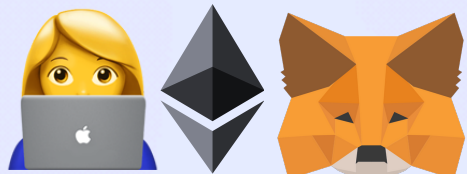
Composition & Flow

Permissionless



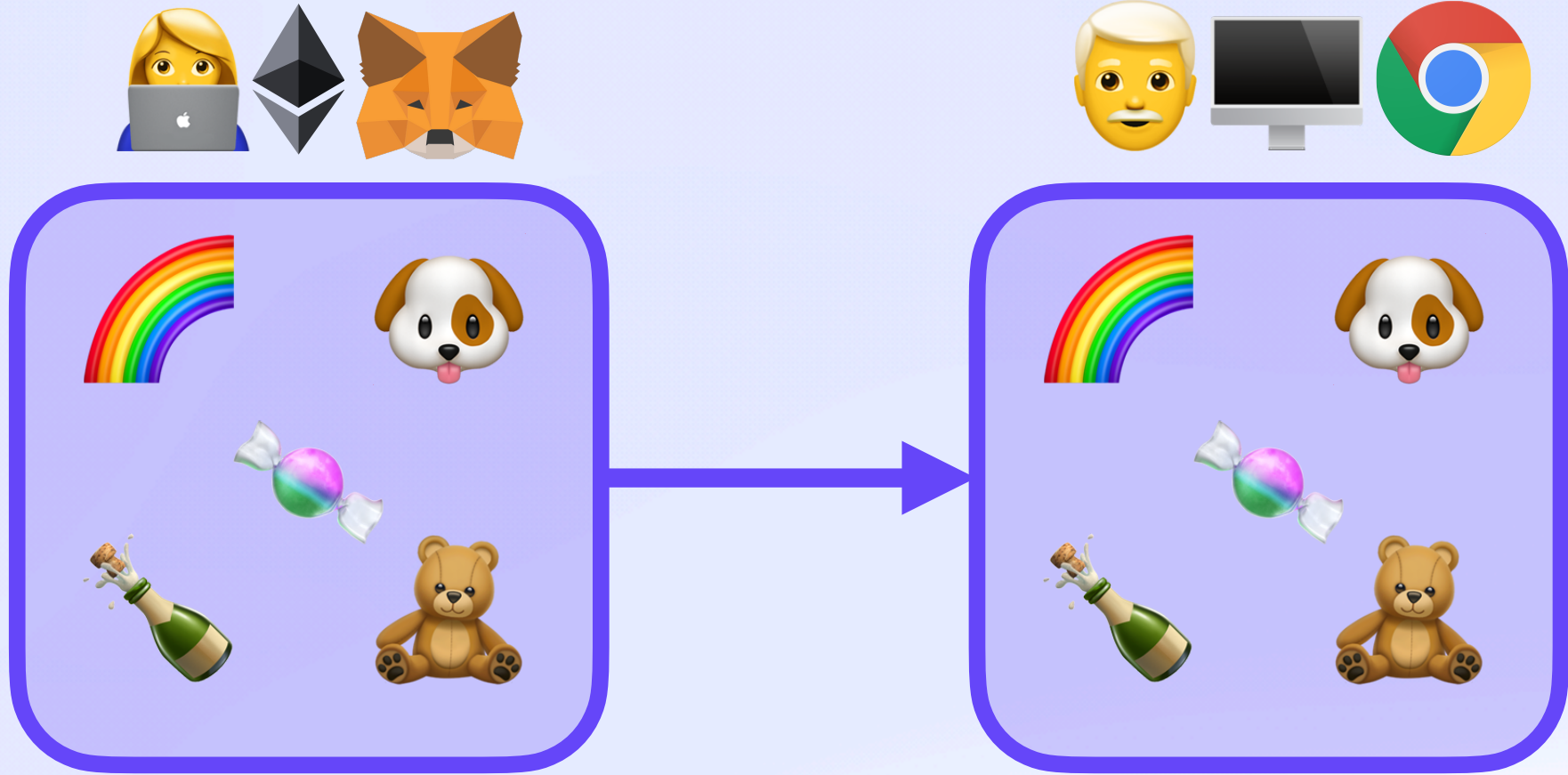
Composition & Flow

Permissionless



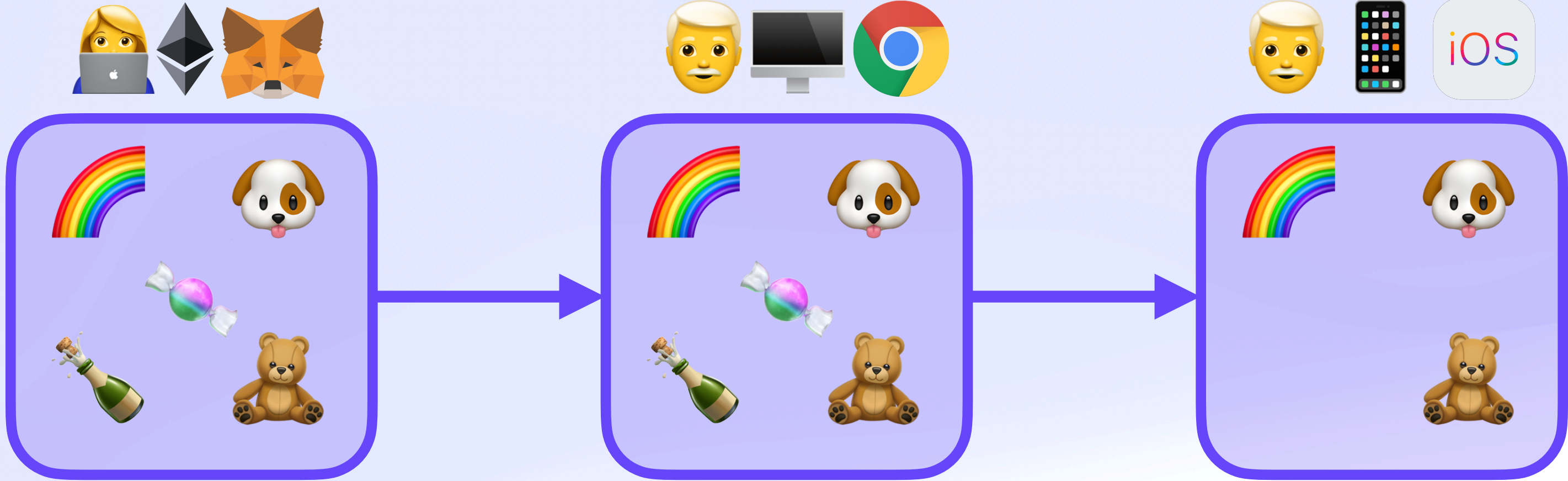
Composition & Flow

Permissionless



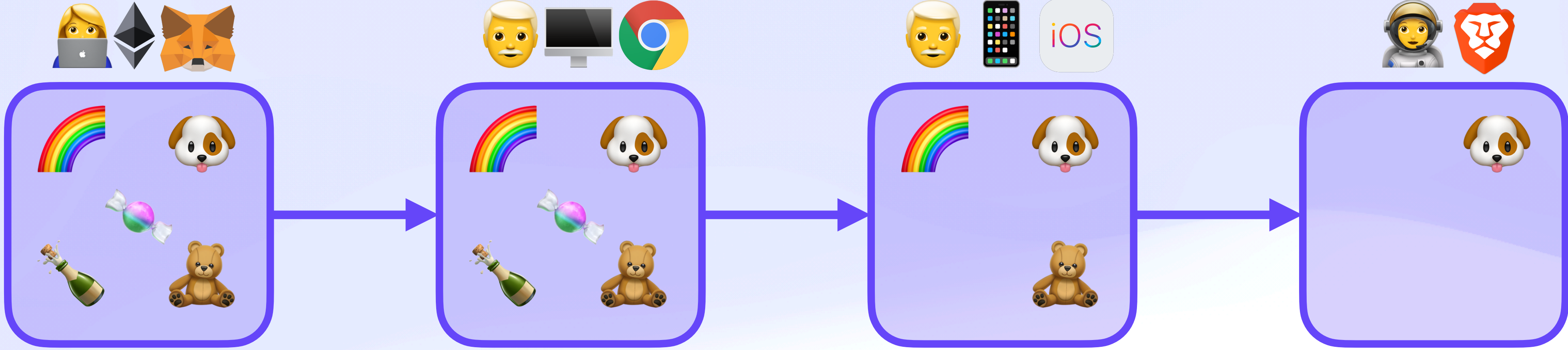
Composition & Flow

Permissionless



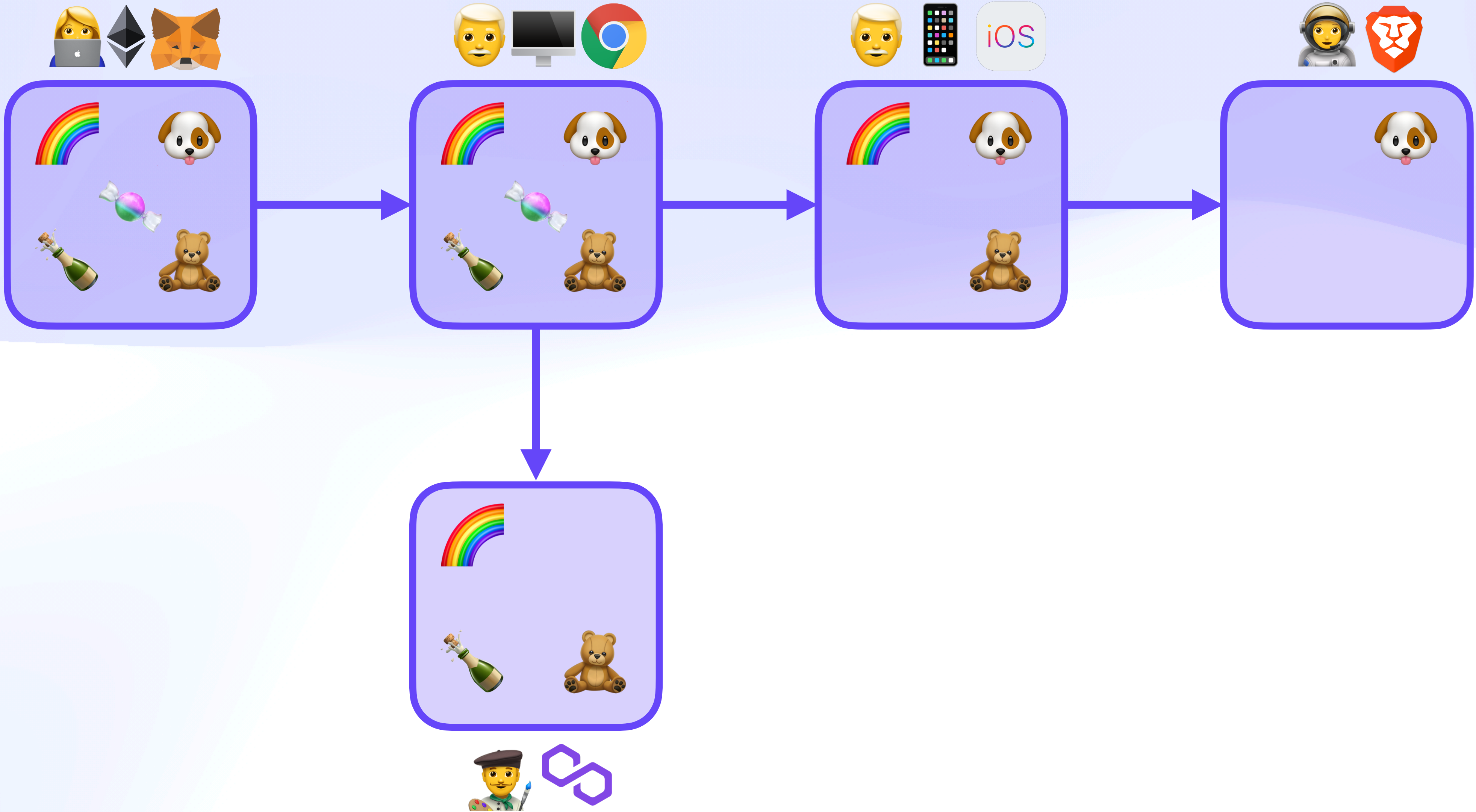
Composition & Flow

Permissionless



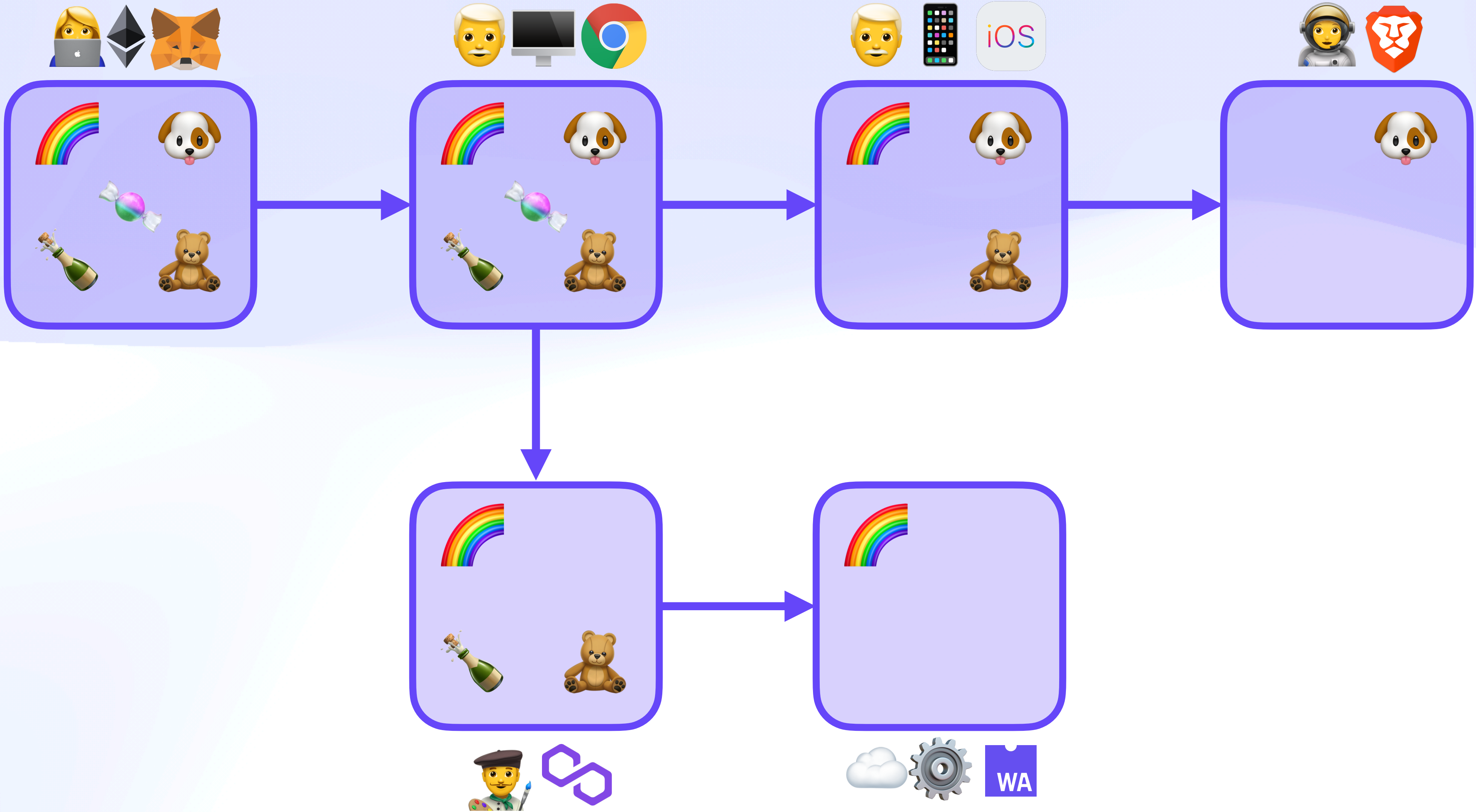
Composition & Flow

Permissionless



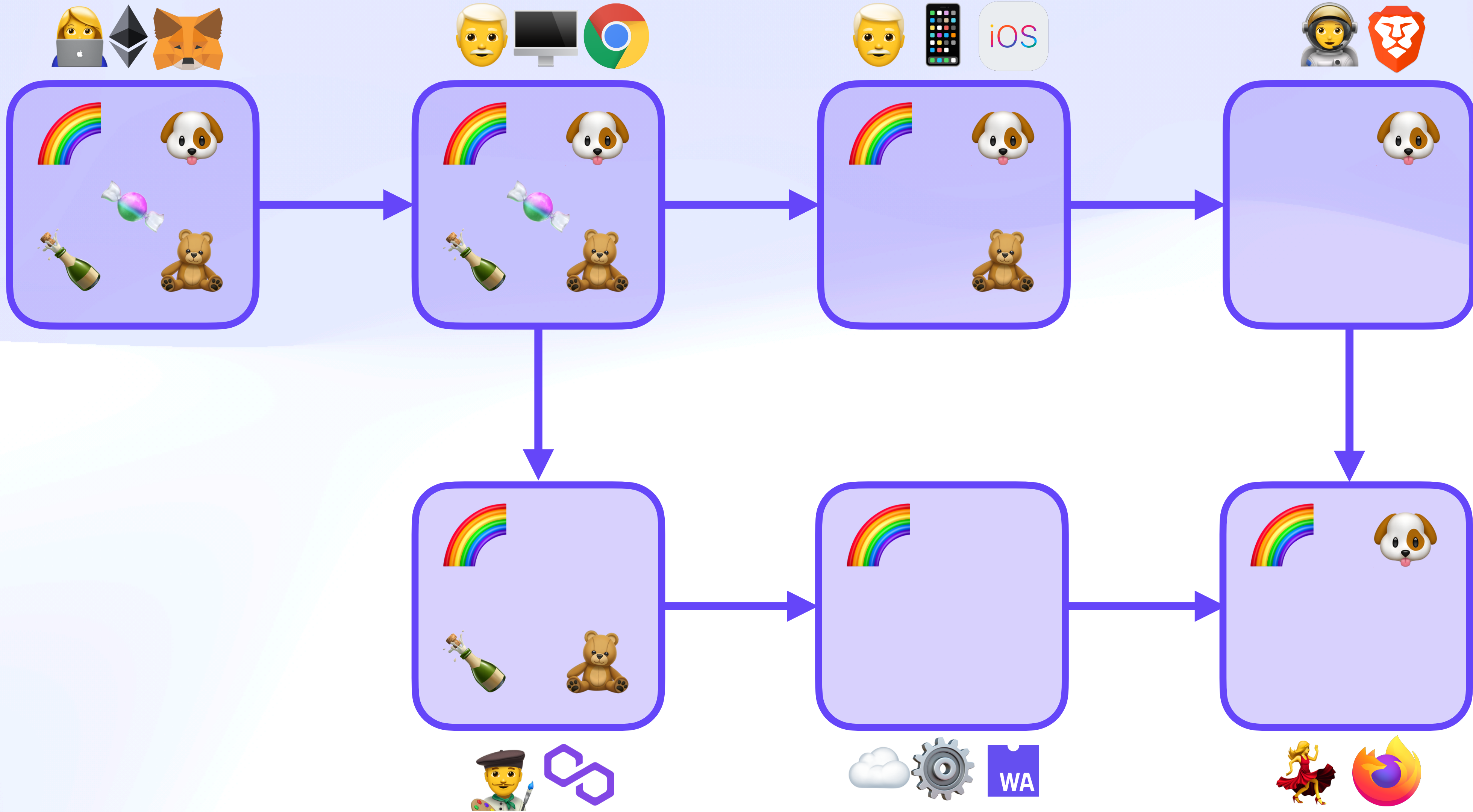
Composition & Flow

Permissionless



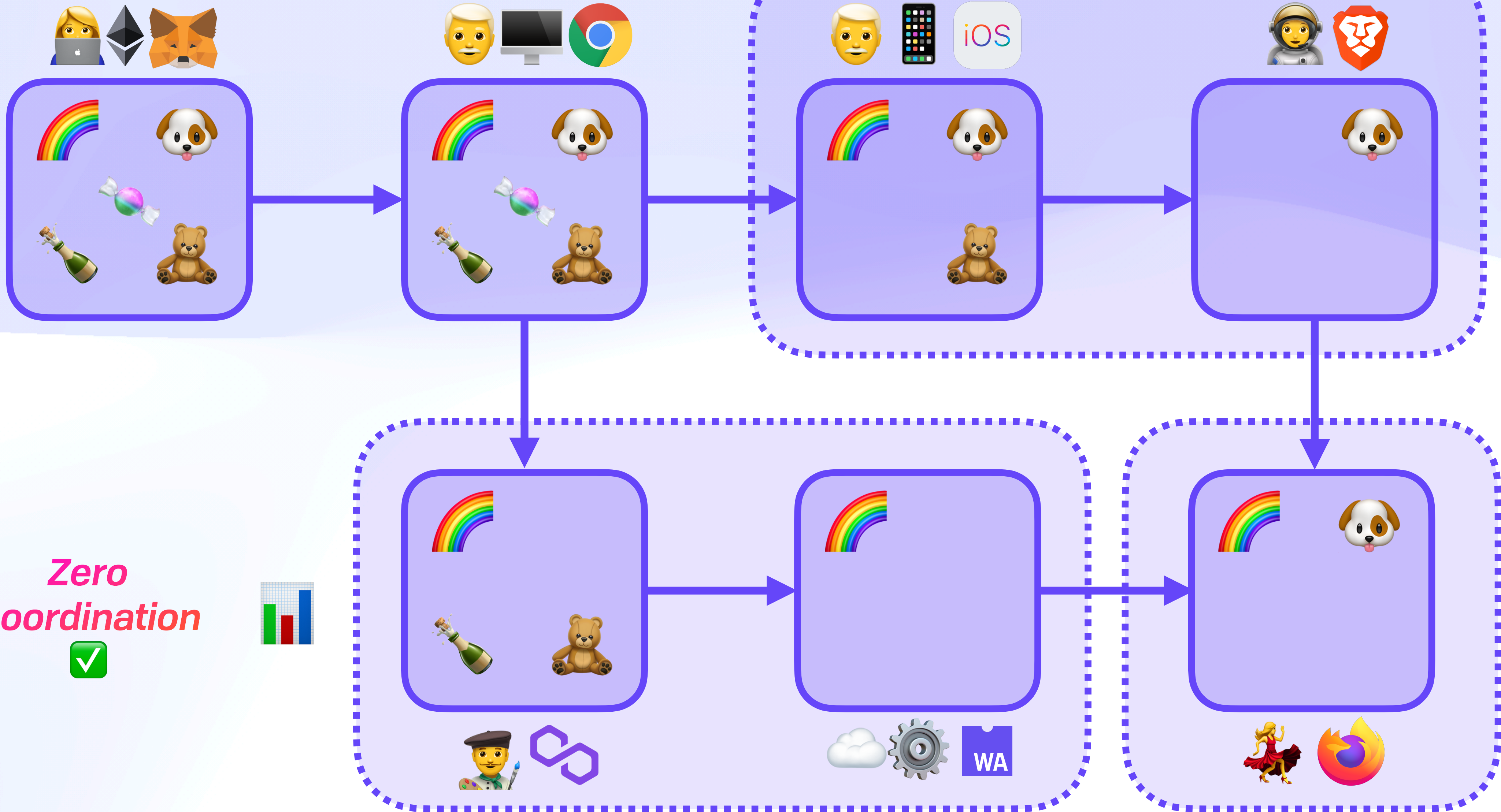
Composition & Flow

Permissionless



Composition & Flow

Permissionless

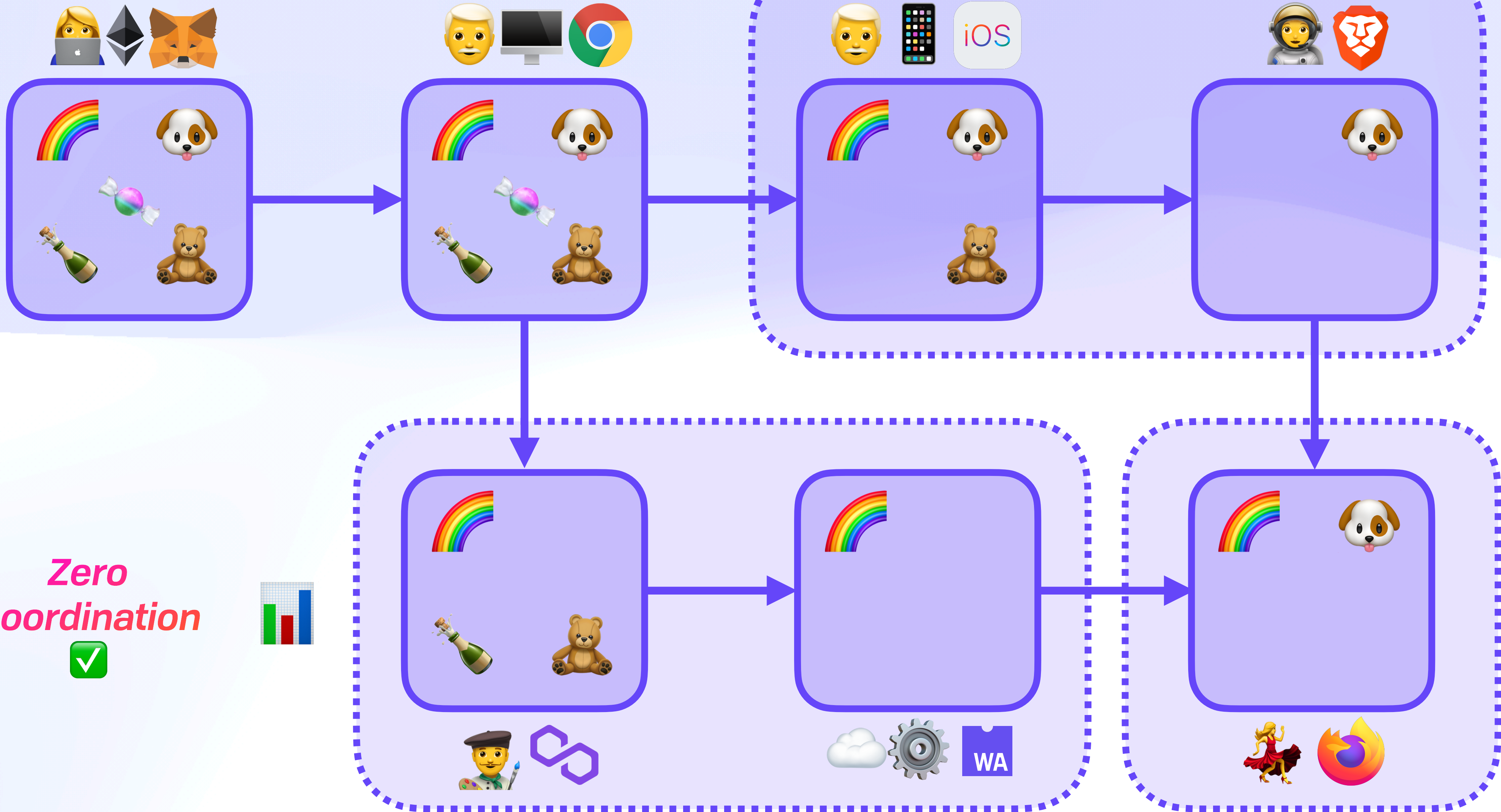


Zero
Coordination
✓



Composition & Flow

Revocation

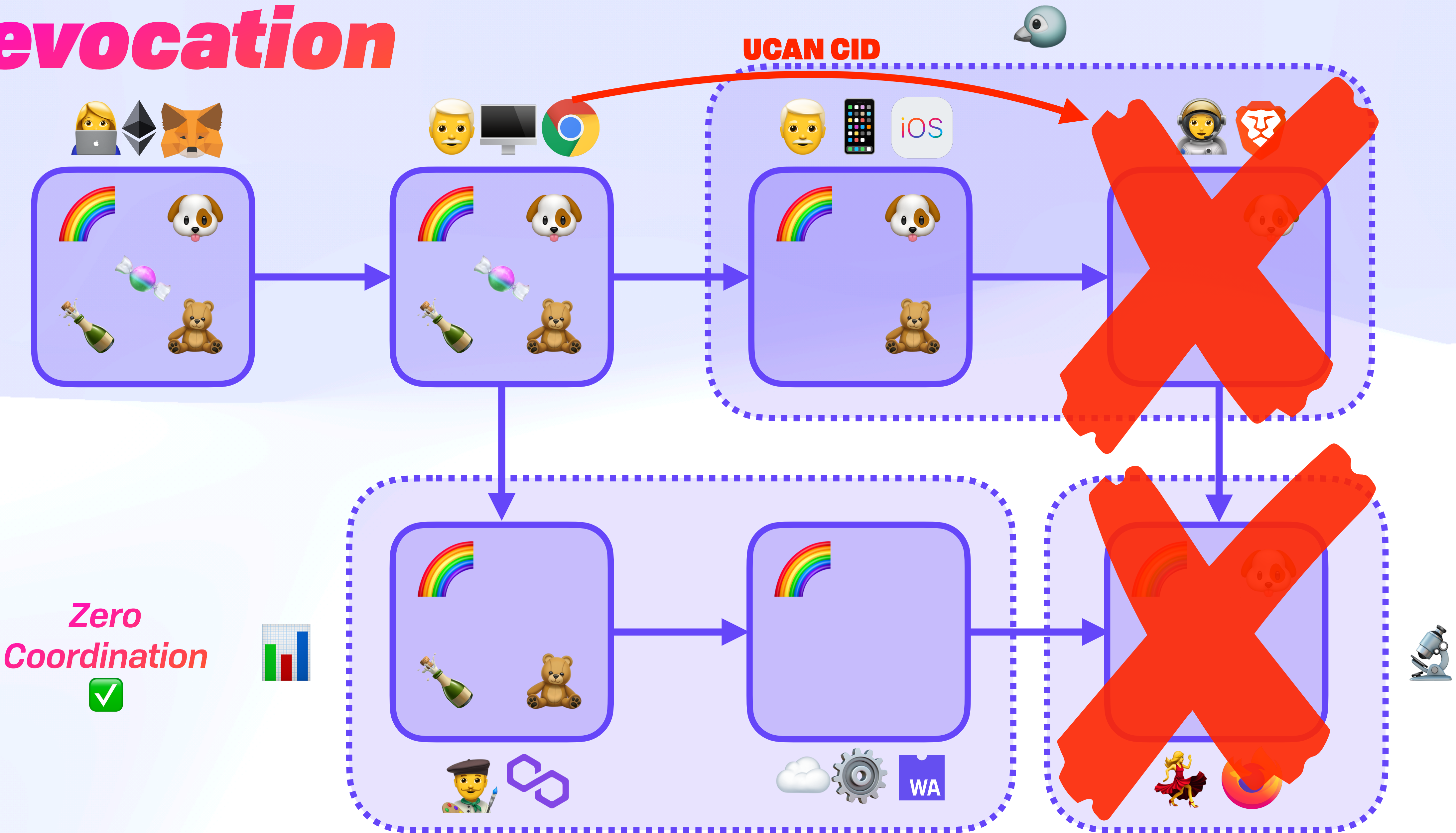


Zero
Coordination
✓



Composition & Flow

Revocation



Nice theory, how about a...

Nontrivial Example



Nontrivial Example

Encoded

Nontrivial Example

Encoded

eyJhbGciOiJFZERTQSIiInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V50no2T
Wt2WGZQVXY4Ynh0c1ZRaUdvN050azRxS0p0Y2dLMml0NTJwYzcdGVVcFJMVCIiImF0dCI6W3sid25mcy
I6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNhci6I6Ik9WRVJXUklURSJ9LHs
id25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwY2FwIjoiT1ZFUldSSVRF
In1dLCJleHAiOiJkyNTY5Mzk1MDUsImZcyI6ImRpZDprZXk6ejZNa3NYUUJmTDhvd3p0VENKVG03aE5SZ
jZiMThZeFhQcDNpNjZvSkht0EwzWUdKIiwibmJmIjoxNjM5NjA4MjkzLCJwcmYiOiIsiZXLKaGJHY2lPaU
pGwkVSVFFTSXNjblI1Y0NjNkIrcFhWQ0lzSW5WamRpSTZJakF1Tnk0d0luMC5leUpoZFdRaU9pSmthV1E
2YTJWNU9ubzJUV3R6V0ZGQ1prdzRiM2Q2ZEZSRFNsUnR0MmhPVW1ZMllqRTRXWGhZVUhBemFUWTJiMHBj
YlRoTU0xbEhTaUlsSW1GMGRDSTZXM3NpZDI1bWN5STZJbVJsYlc5MWMYVnIMbVpwYzN0cGIyNHVibUZ0W
LM5d2RXSnNhV012Y0dodmRH0XpMeUlsSW10aGNDSTZJazlXUlsZKWFVrbFVSU0o5WFN3aVpYaHdJam81TW
pVMk9UTTV0VEExTENKcGMzTWlPaUprYVdRNmEyVjVPbm8yVFd0d05VVnplamx6TWsxSWMzRlpka3h2WTJ
ONVNIzFl0VksZVZwTGNIrTNPVWQwTkRwbVJrZEZxbEk1T1Njc0ltNWlaaUk2TVRZek9UWXDPREk1TXl3
aWNISm1JanBiWFgwLjRUTmh1SFJyUEc5YUhv0DY5SFhsc05L0F9GbWXTaFE1R3pHNGl0TjJ0S2steUtUY
kFNb0Z3VHVwdEcwWEZnTkI2SHVsUHBsVnpaWURWRGV4bzc2a0F3IiwZXLKaGJHY2lPaUpGwkVSVFFTSX
NjblI1Y0NjNkIrcFhWQ0lzSW5WamRpSTZJakF1Tnk0d0luMC5leUpoZFdRaU9pSmthV1E2YTJWNU9ubzJ
UV3R6V0ZGQ1prdzRiM2Q2ZEZSRFNsUnR0MmhPVW1ZMllqRTRXWGhZVUhBemFUWTJiMHBjYlRoTU0xbEhT
aUlsSW1GMGRDSTZXM3NpZDI1bWN5STZJbVJsYlc5MWMYVnIMbVpwYzN0cGIyNHVibUZ0WLM5d2RXSnNhV
012Ym05MFpYTXZJaXdpWTJGd0lqb2lUMVpGVWxkU1NWUkZJbjFkTENKbGVIQWlPamt5TlRZNU16azFNRF
VzSW1semN5STZJbVJwWkRwclpYazZla0YTnBMVJYTjZPWE15VFVoemNwbDJURzlwWTNsSWQxZzFVMlY
1V2t0d2NUYzVSM1EwTldaR1IwVmFVams1SWl3aWJtSm1Jam94TmPNUU5qQTRNamt6TENKd2NtWwlpbHRk
ZlEuTWdZYXJMcXk3Um1RMUFJcnFZTDZjRnk5ejdhNVdJQVUtLVRZQVJQU2dpck9Tc3p2YXIzX0R0cjI1c
mJQcmV0SGJuVDBtTVZLeW9hUVhydVI3S2JyQmciXX0.kwRdqPN74pkcpXGgdk7Z7FW3M1mRRYaDE5ZgkG
6srAuu6V6mvMVRdBLnD5Cwid-X4tDIKplivjlCSLTntB4pCw

Nontrivial Example

Decoded

Payload

Header

```
{  
  "alg": "EdDSA",  
  "typ": "JWT",  
  "ucv": "0.9.1"  
}
```

```
{  
  "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",  
  "aud": "did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",  
  "nbf": 1639608293,  
  "exp": 9256939505,  
  "att": [  
    {  
      "with": "wnfs://boris.fission.name/public/photos/",  
      "can": "fs/append"  
    },  
    {  
      "with": "wnfs://boris.fission.name/public/notes/",  
      "can": "fs/append"  
    }  
  ],  
  "prf": [  
    "eyJhbGciOiJIJFZERTQSIiwiaWF0IjOiIjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V5O  
    no2TWtzWFFCZkw4b3d6dFRDSLrTn2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF  
    0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNhc  
    CI6Ik9WRVJXUklURSJ9XSwiZXhwIjo5MjU2MDU5NTA1LCJpc3MiOiJkaWQ6a2V5O  
    no2TWtwNUVzejlzMk1Ic3FZdkxvY2N5SHdYNVNleVpLcHE3OUd0NDVmRkdFWlI5O  
    SIiwiaWF0IjoiIjE5MTYzOTYwOjE1MywiczHmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_Fm  
    lShQ5GzG4itN2NKK-yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDexo76kAw",  
    "eyJhbGciOiJIJFZERTQSIiwiaWF0IjOiIjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V5O  
    no2TWtzWFFCZkw4b3d6dFRDSLrTn2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF  
    0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiaWF0IjoiIjE5MTYzOTYwOjE1MywiczHmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_Fm  
    lShQ5GzG4itN2NKK-yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDexo76kAw"  
  ]  
}
```

Signature

```
kwRdqPN74pkcpXGgdK7Z7FW3M1mRR  
YaDE5ZgkG6srAuu6V6mvMVRdBLnD5  
CWid-X4tDIKpliVjlCSLTntB4pCw
```

```
eyJhbGciOiJIJFZERTQSIiwiaWF0IjOiIjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V5O  
no2TWtzWFFCZkw4b3d6dFRDSLrTn2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF  
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNhc  
CI6Ik9WRVJXUklURSJ9XSwiZXhwIjo5MjU2MDU5NTA1LCJpc3MiOiJkaWQ6a2V5O  
no2TWtwNUVzejlzMk1Ic3FZdkxvY2N5SHdYNVNleVpLcHE3OUd0NDVmRkdFWlI5O  
SIiwiaWF0IjoiIjE5MTYzOTYwOjE1MywiczHmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_Fm  
lShQ5GzG4itN2NKK-yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDexo76kAw",
```

```
eyJhbGciOiJIJFZERTQSIiwiaWF0IjOiIjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V5O  
no2TWtzWFFCZkw4b3d6dFRDSLrTn2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF  
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiaWF0IjoiIjE5MTYzOTYwOjE1MywiczHmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_Fm  
lShQ5GzG4itN2NKK-yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDexo76kAw"  
joit1ZFULdSSVRFIn1dLCJleHAiOiIjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V5O  
no2TWtzWFFCZkw4b3d6dFRDSLrTn2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF  
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiaWF0IjoiIjE5MTYzOTYwOjE1MywiczHmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_Fm  
lShQ5GzG4itN2NKK-yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDexo76kAw"  
50XMyTUhzcVl2TG9jY3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_Fm  
lShQ5GzG4itN2NKK-yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDexo76kAw"  
jkzLCJwcmYiOiIjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V5O  
no2TWtzWFFCZkw4b3d6dFRDSLrTn2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF  
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiaWF0IjoiIjE5MTYzOTYwOjE1MywiczHmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_Fm  
lShQ5GzG4itN2NKK-yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDexo76kAw"  
YARPSgir0Sszvar3_DNr25rbPretHbnT0mMVkyoaQXruR7KbrBg"
```


Nontrivial Example

Decoded Witness

Payload

Header

```
{  
  "alg": "EdDSA",  
  "typ": "JWT",  
  "ucv": "0.9.1"  
}
```

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

Signature

```
4TNhuHRrPG9aHo869HXlsNK8_Fm1ShQ5GzG  
4itN2NKk-  
yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDe  
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

Paste an encoded UCAN

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXZWQ6a2V5Ono2TWZlZWFFCzkw43d6dFRD5IRnZ2Y2YjE4WXhYUHAzaTY2b0plbThMM1HS1sImF0dCI6W3sid25mcy16ImRlbnW91c2VYlMzpc3Npb24ubmFIZS9wdWJ3aWVmcGhvdG9zLzYlImNhcCI6Ikh9WRV3XUkiUR5J9XSzXhwj05MjU2OTM5NTA1LCJpc3MiOiJkaWQ6a2V5Ono2TWZlZWVzejIic3FzdikxvY2N5SHdYVWVlLnVlcHE3OUd0NDVmRkdFWlI5OStIm5IZi6MTYzOTYwODI5MywiczH3mTjpbXX0.4TNhuHRrPG9aHo869HXlsNKB_FmIshQ5GzG4iHN2NKK-ykTbAMoFwTuptG0XFgNivHulPp1VzZYDvDexo76kAw
```

Decoded

Header

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

Payload

```
{  "aud": "did:key:z6MksXQBfLBoztTCJTm7hNRf6b18YxXpP3i66oJHm8L3YGJ",  "att": [    {    "wnfs": "demouser.fission.name/public/photos/",    "cap": "OVERWRITE"    }  ],  "exp": 9256939505,  "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45FGEZR99",  "nbf": 1639688293,  "prf": []}
```

Signature

```
4TNhuHRrPG9aHo869HXlsNKB_FmIshQ5GzG4iHN2NKK-ykTbAMoFwTuptG0XFgNivHulPp1VzZYDvDexo76kAw
```

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:z6MksXQBfLBoztTCJTm7hNRf6b18YxXpP3i66oJHm8L3YGJ	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.

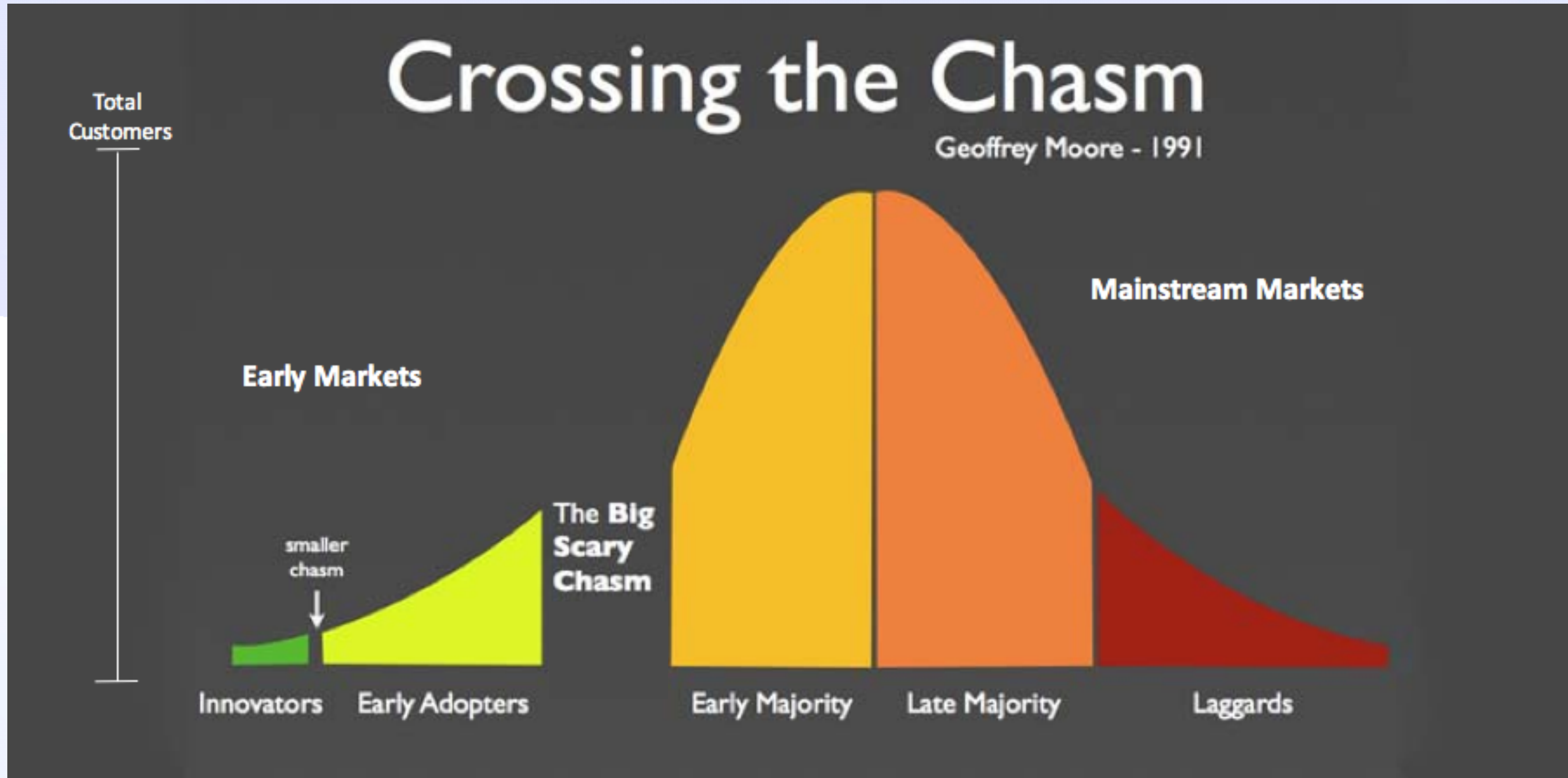
Further Reading

Adoption



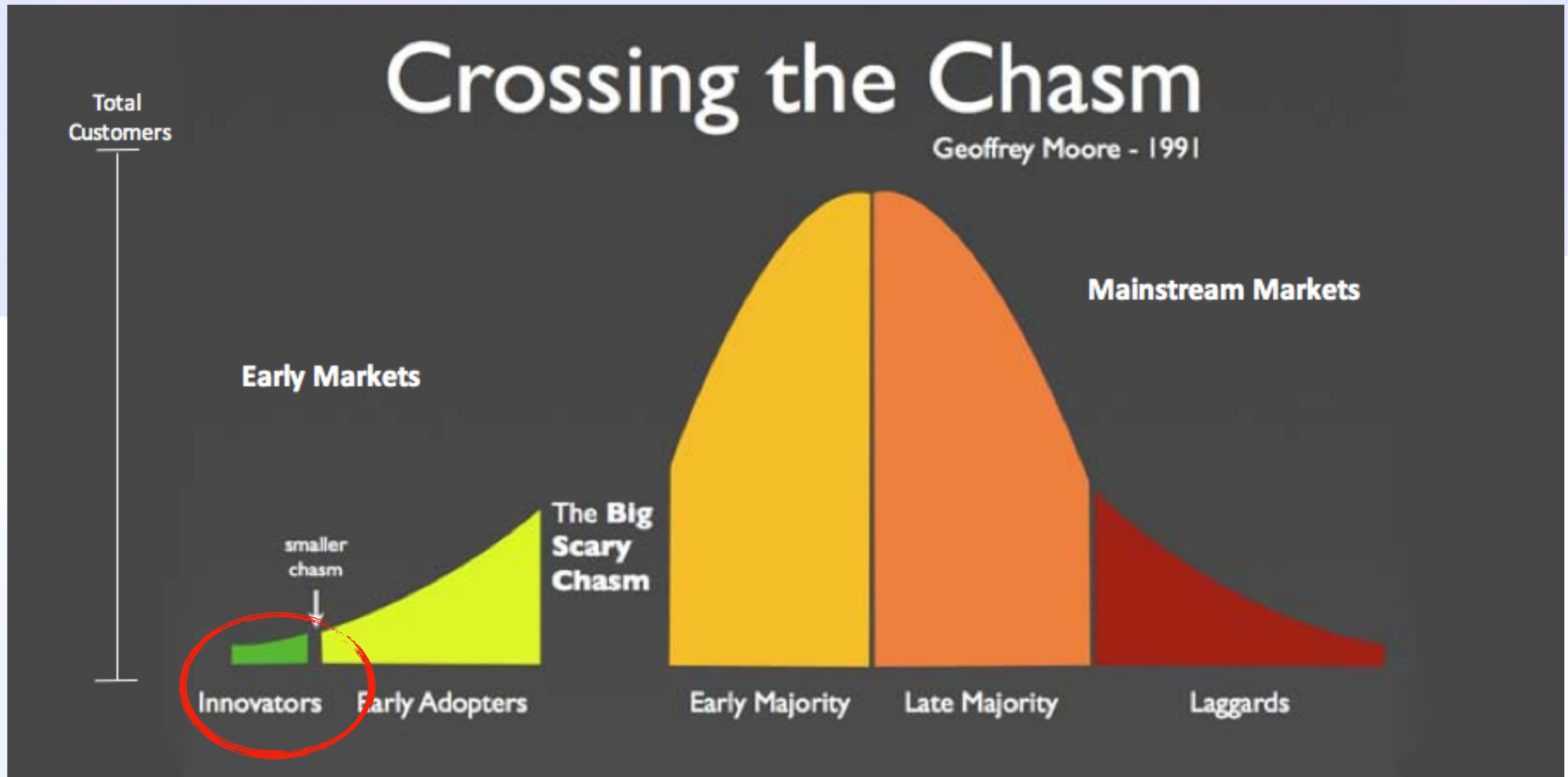
How to Power a New Internet ⚡

Still Extremely Early Days for Web3!



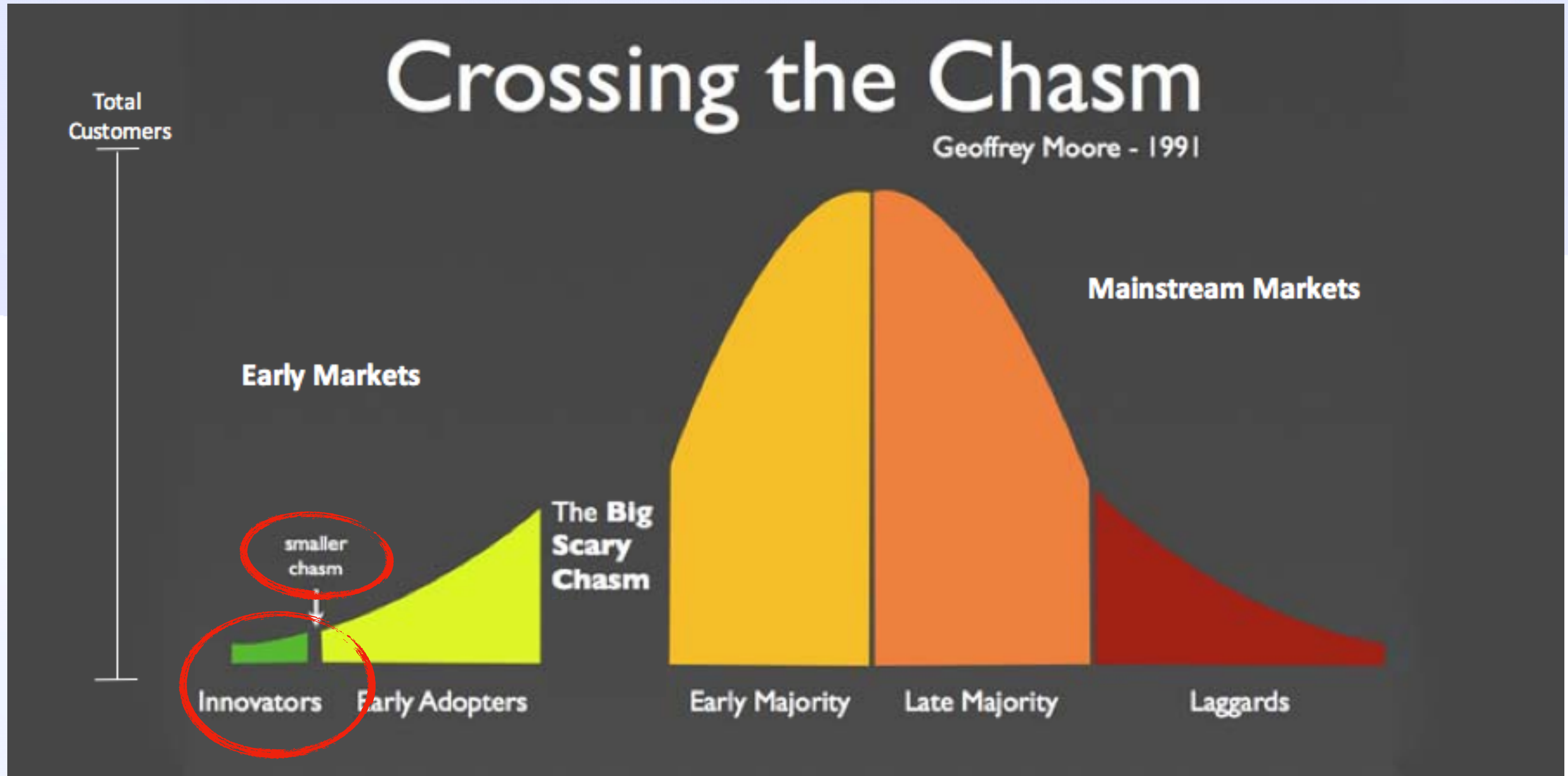
How to Power a New Internet ⚡

Still Extremely Early Days for Web3!



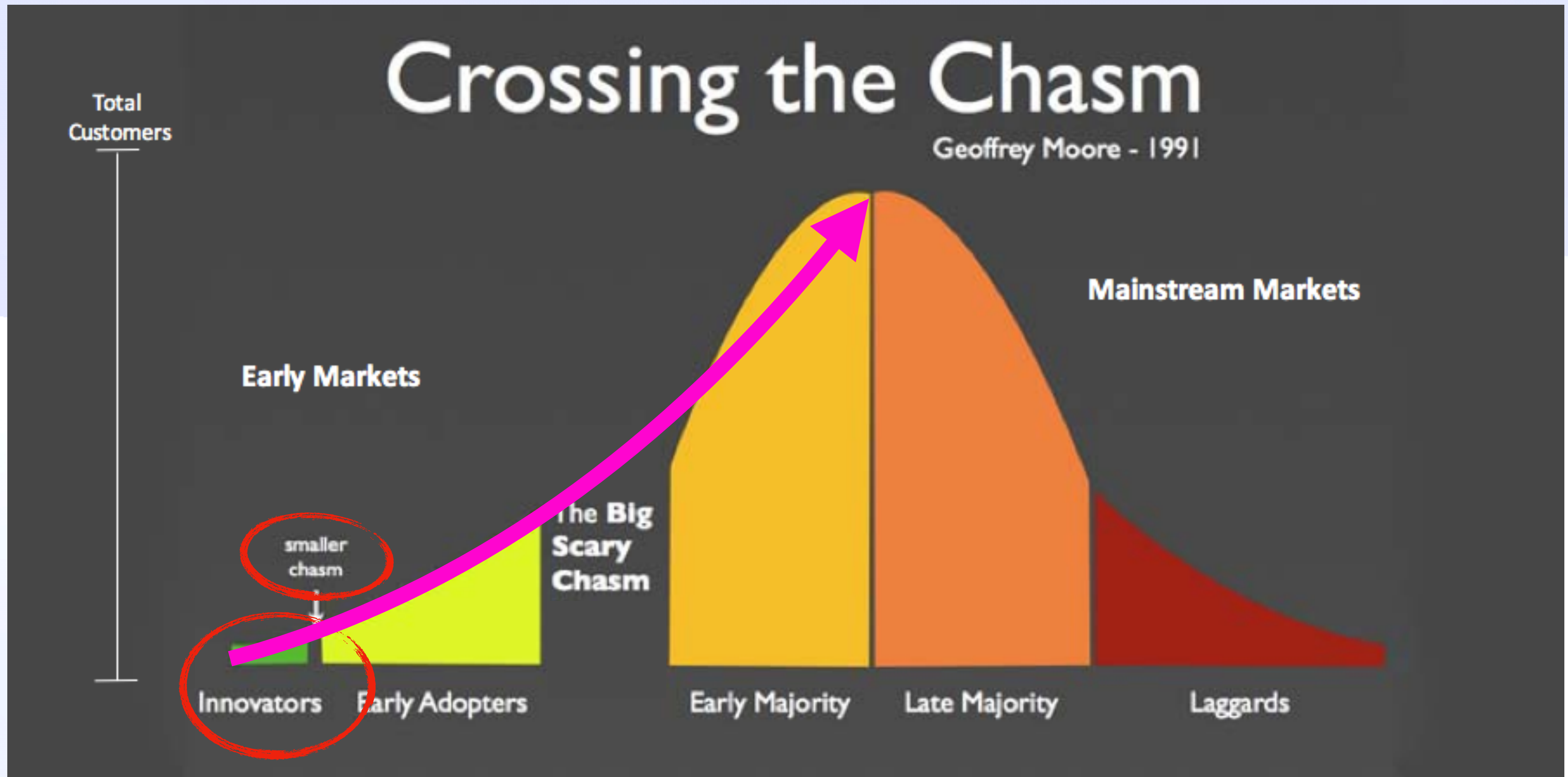
How to Power a New Internet ⚡

Still Extremely Early Days for Web3!



How to Power a New Internet ⚡

Still Extremely Early Days for Web3!



How to Power a New Internet ⚡

User Problems

How to Power a New Internet ⚡ ***User Problems***

Service composition is ***too hard*** for many devs

How to Power a New Internet ⚡

User Problems

Service composition is ***too hard*** for many devs
(D)app UX is ***too hard*** for many users

How to Power a New Internet ⚡

User Problems

Service composition is ***too hard*** for many devs

(D)app UX is ***too hard*** for many users

No one is in ***control*** of their data or compute

How to Power a New Internet ⚡

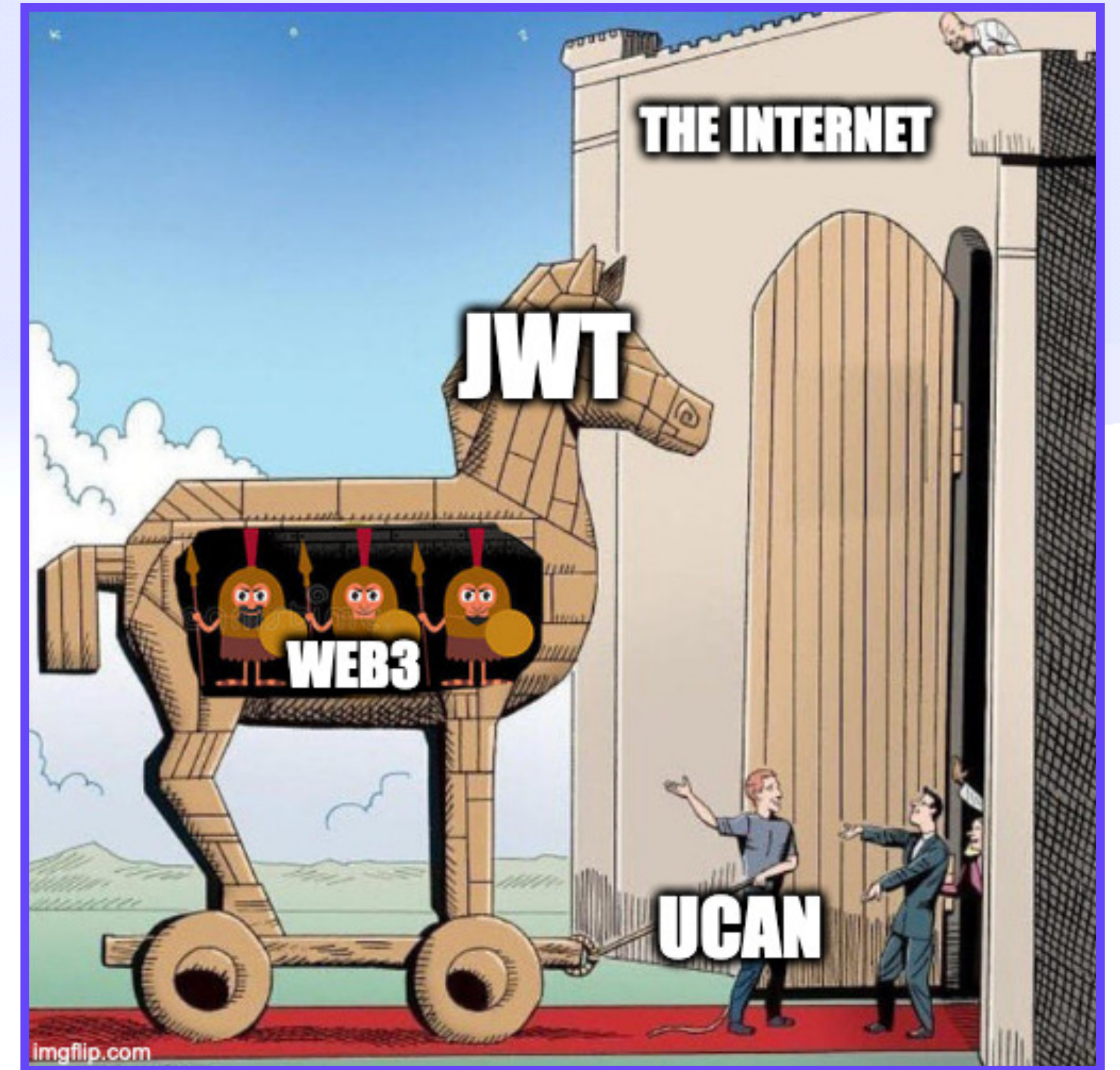
Adoption

How to Power a New Internet ⚡

Adoption

Be a Trojan Horse

Build on widely supported, familiar, well-understood standards



How to Power a New Internet ⚡

Adoption

How to Power a New Internet ⚡

Adoption

Play Nice with Others

Plug into existing tools

Bridge to other standards

Integrate with other systems

Realpolitik

Easier, as secure,

& more open than:

OAuth, X.509, SAML,

MetaMask, WalletConnect,

etc

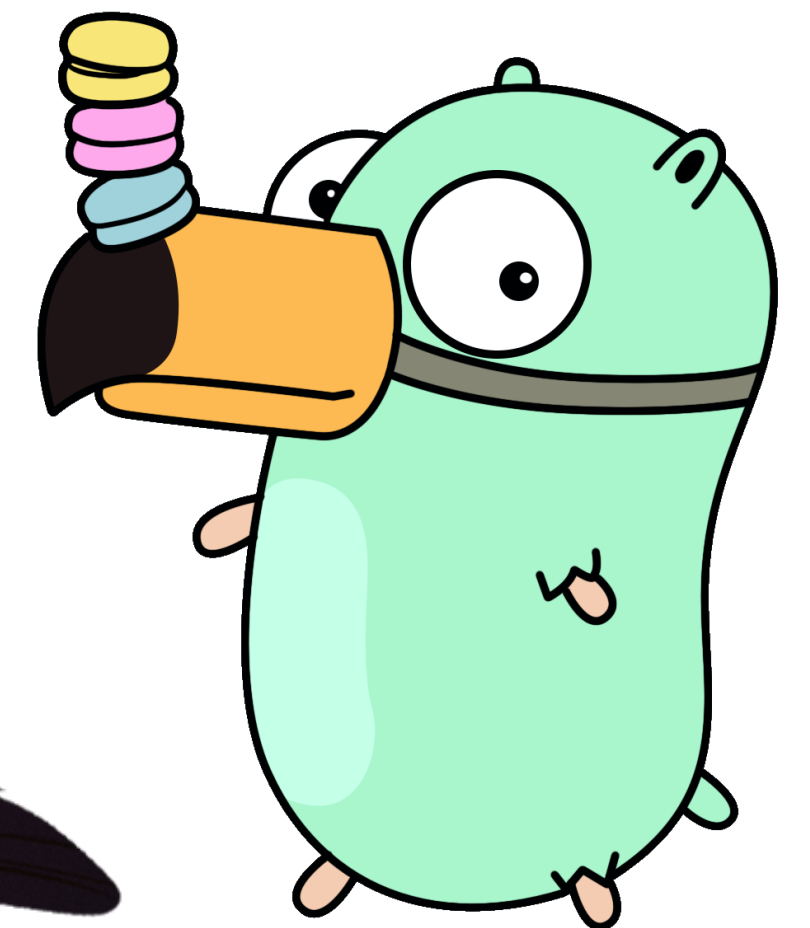
Further Reading
Resources



Resources

(Some) Existing Subprojects

AWAKE



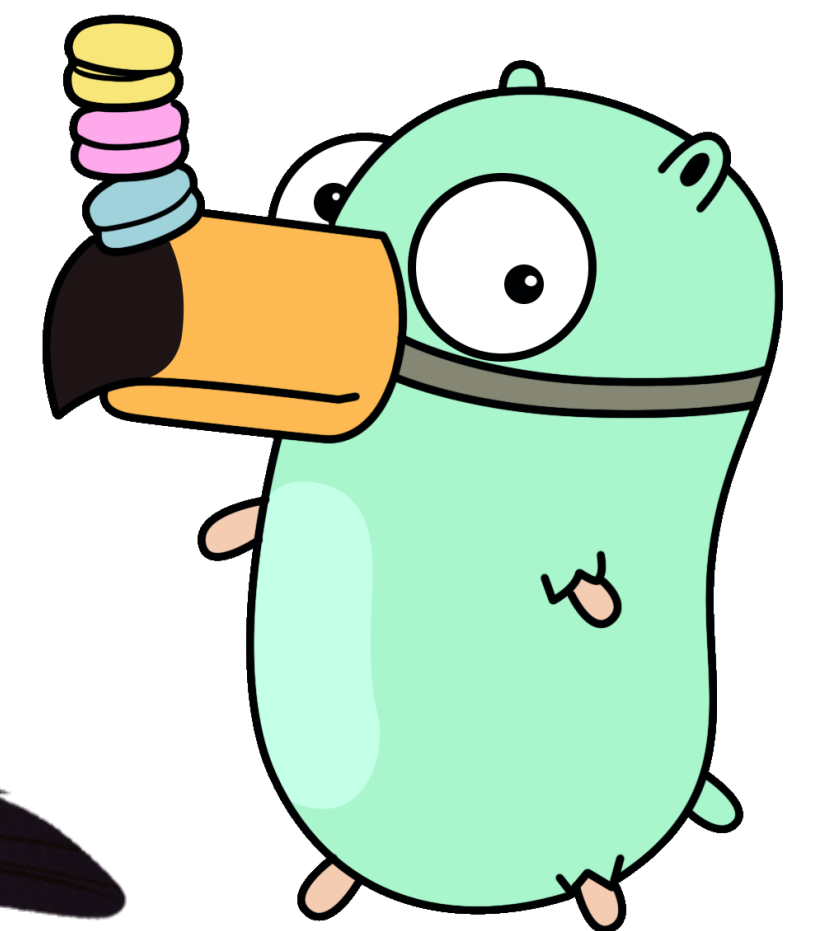
Resources

(Some) Existing Subprojects

- ◆ <https://github.com/ucan-wg/>
 - ◆ Spec, Improvement Proposals
- ◆ ts-ucan
- ◆ rs-ucan
- ◆ go-ucan
- ◆ hs-ucan
- ◆ ucan-ipld
- ◆ ucan-bearer-token
- ◆ AWAKE



AWAKE




Resources

Upcoming

Resources

Upcoming

- ◆ Get to a "LTS" v1.0 — Q1 2023
- ◆ ucan-cacao / SIWE
- ◆ WhoCAN 
- ◆ ucan-invocation
- ◆ ucan-chan (state channels)
- ◆ ucan-wg/cosigner

Resources

Invocation

Resources

Invocation

- ◆ UCAN as RPC
 - ◆ System at DAG House
 - ◆ IPVM

Resources

Further Reading

Resources

Further Reading

- ◆ <https://talk.fission.codes/t/user-controlled-authorization-networks-ucan-resources/1122>
- ◆ 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, CoD Summit 🇵🇹

brooklyn@fission.codes

<https://fission.codes>

github.com/expede

@expede