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
  - IPVM, 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.

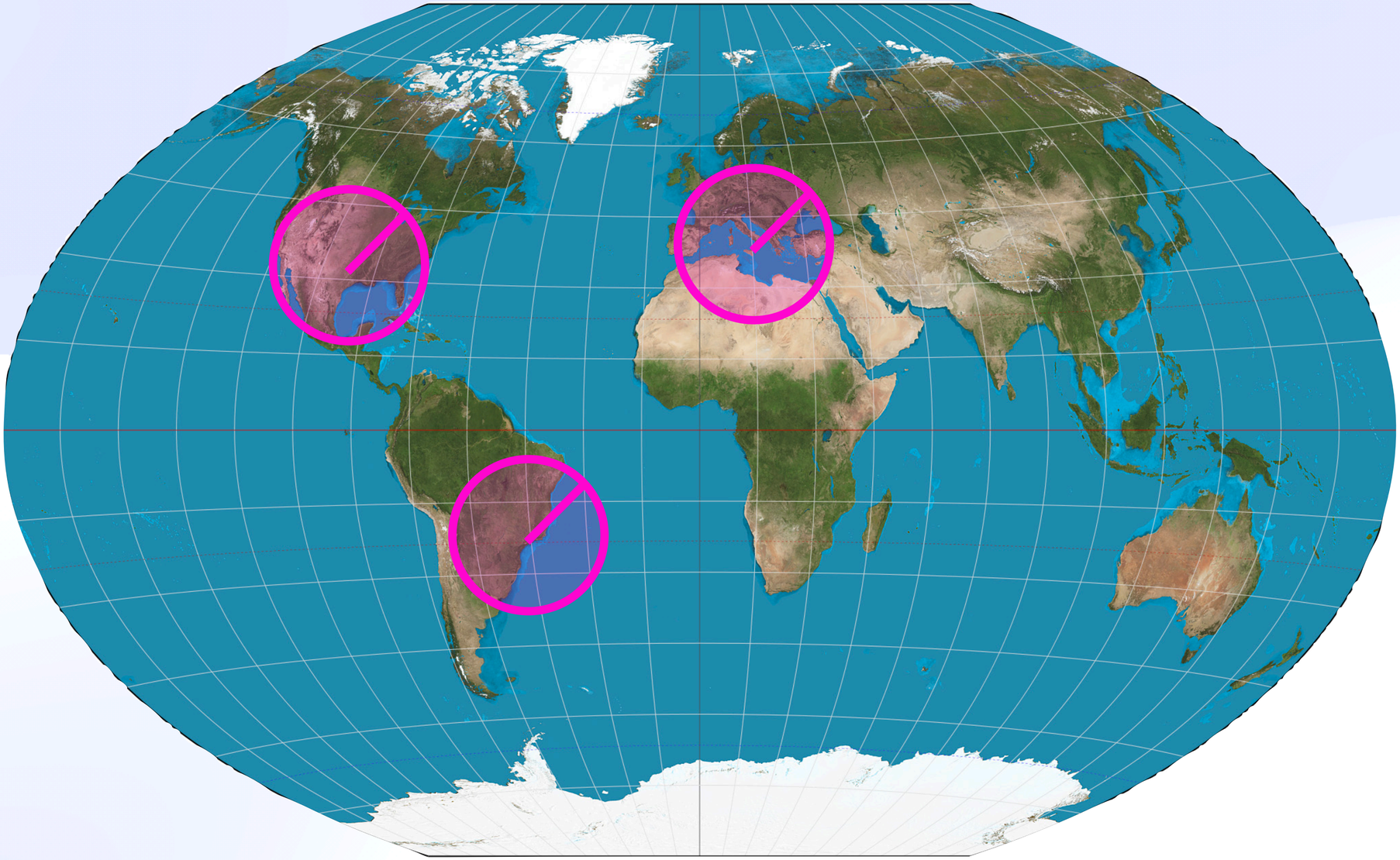
Must be ***substantially*** better than Web 2.0

How to Power a New Internet

How to Power a New Internet ⚡

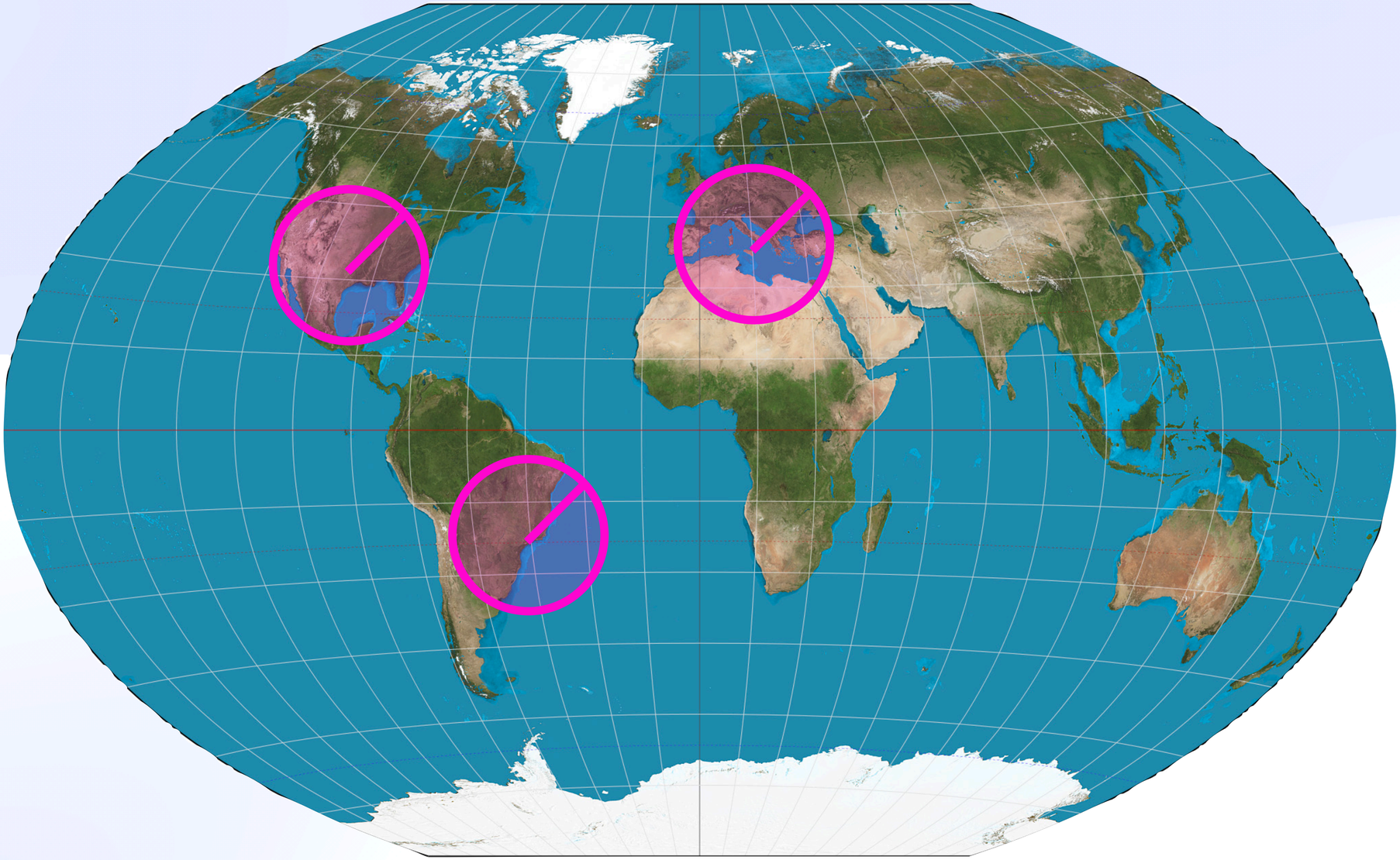
How to Power a New Internet ⚡

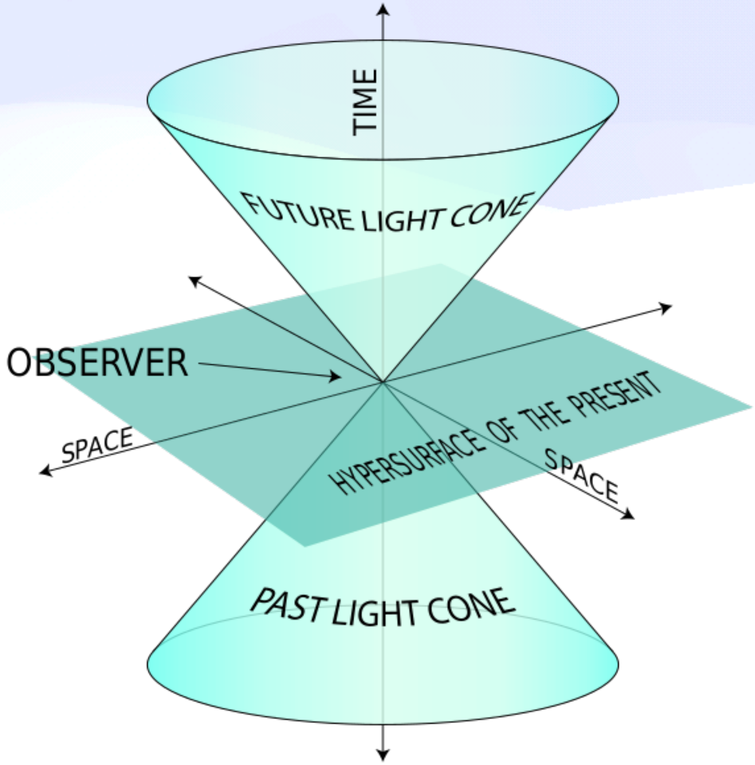
Causal Islands 🏝️🌴



How to Power a New Internet ⚡

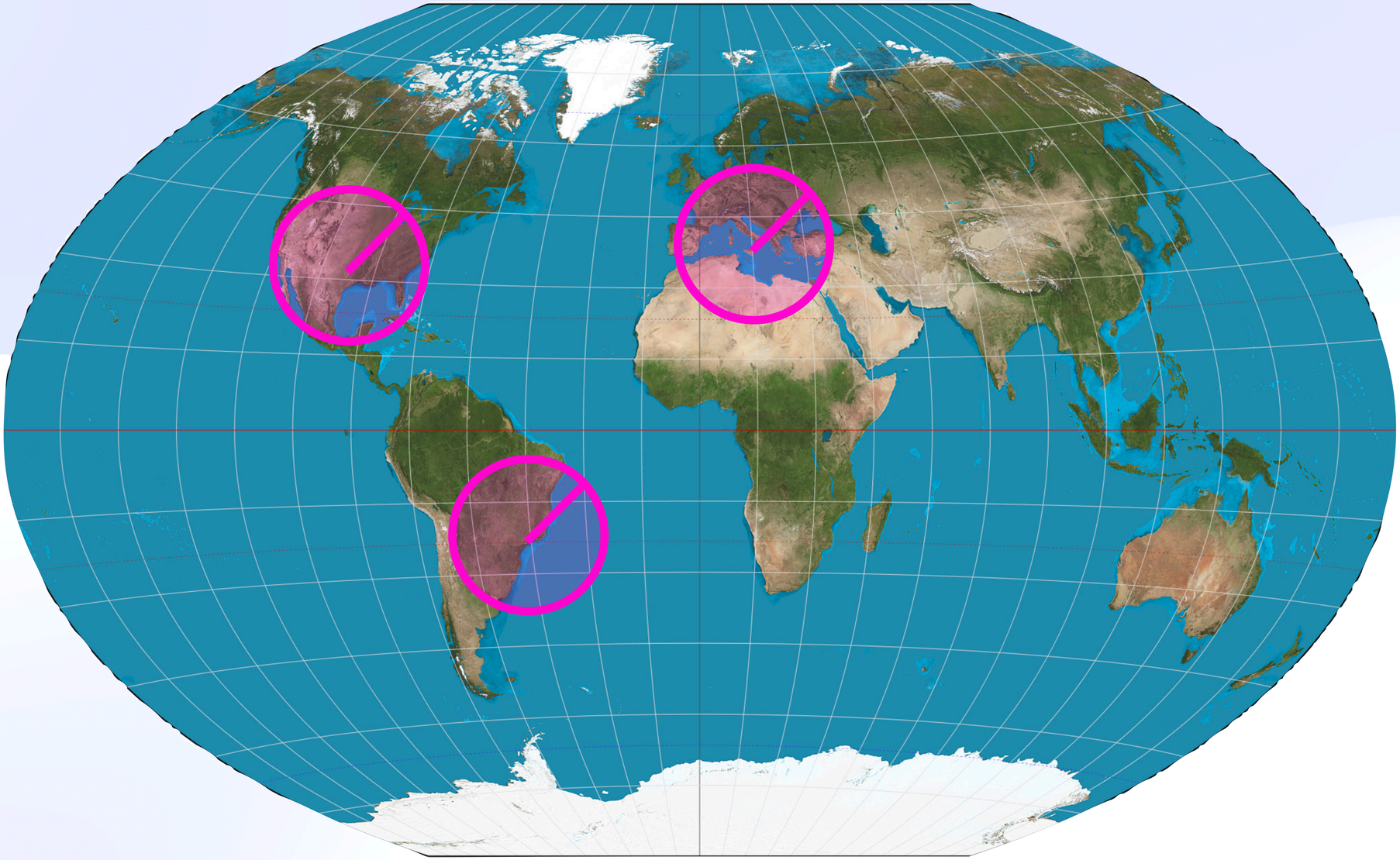
Causal Islands 🏝️🏝️

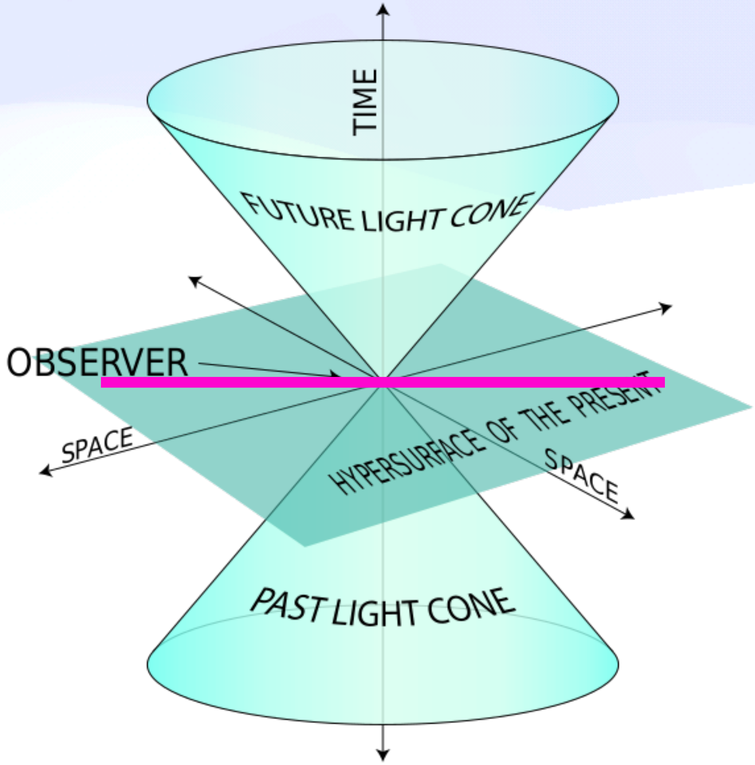




How to Power a New Internet ⚡

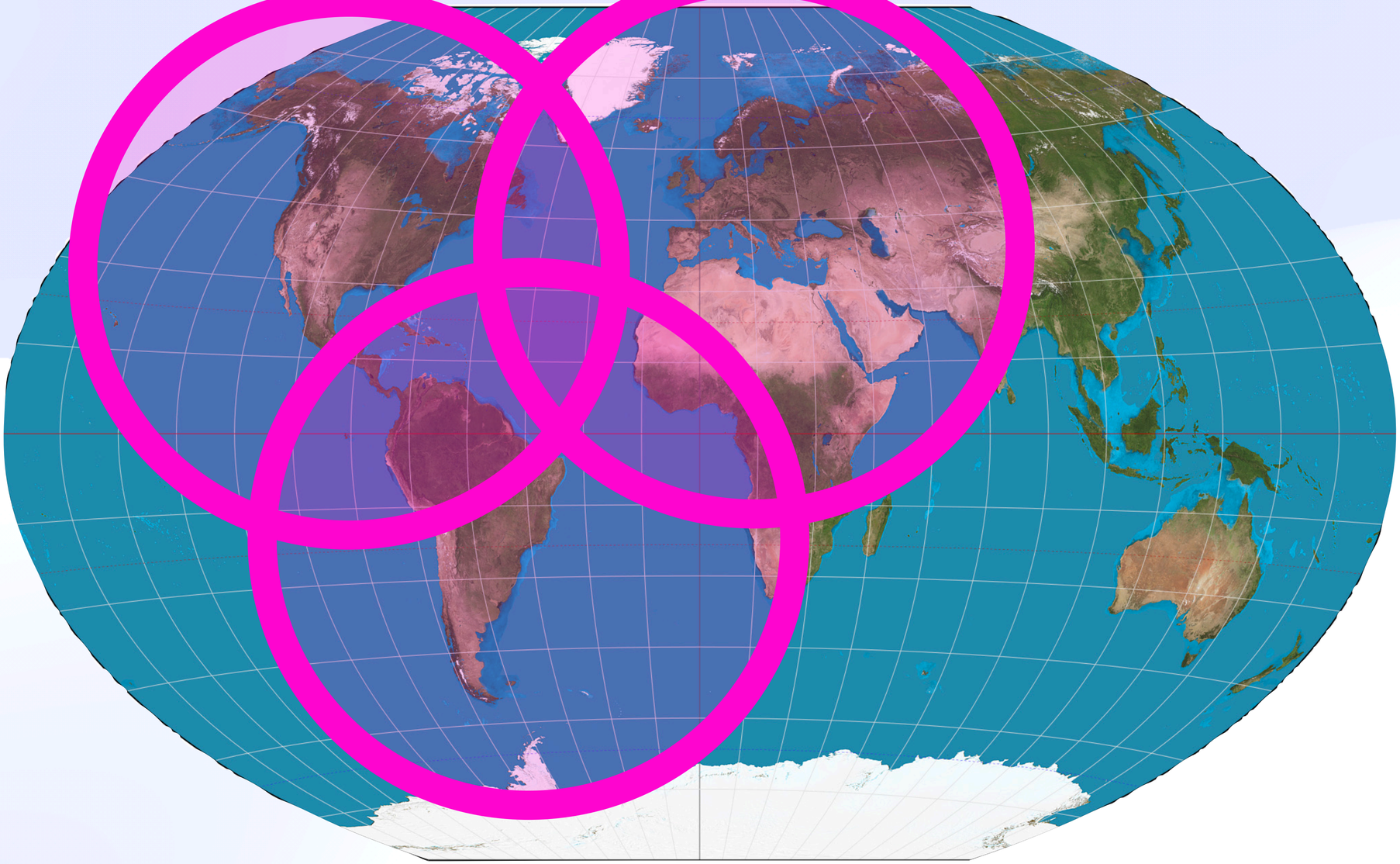
Causal Islands 🏝️🏝️

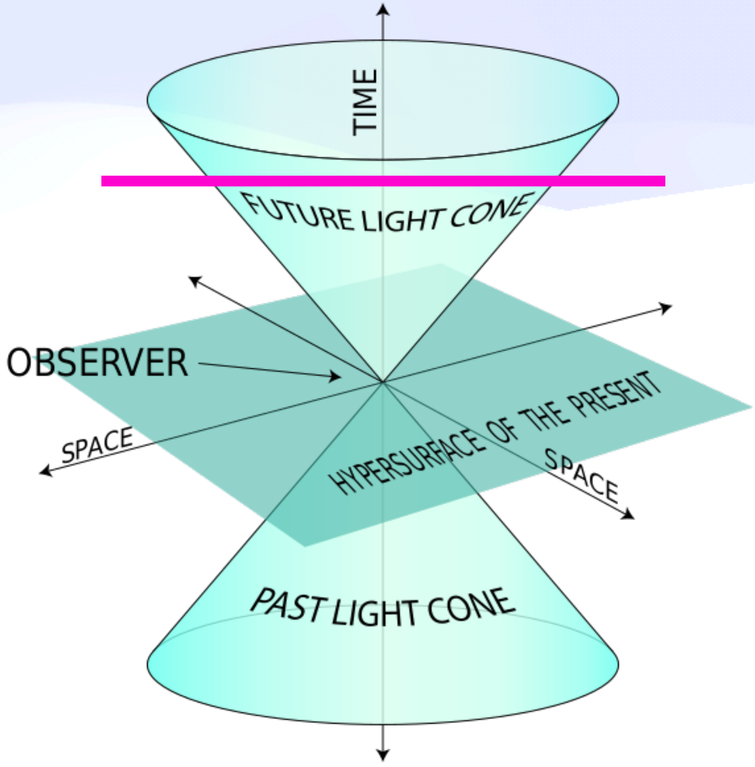




How to Power a New Internet ⚡

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 ⚡

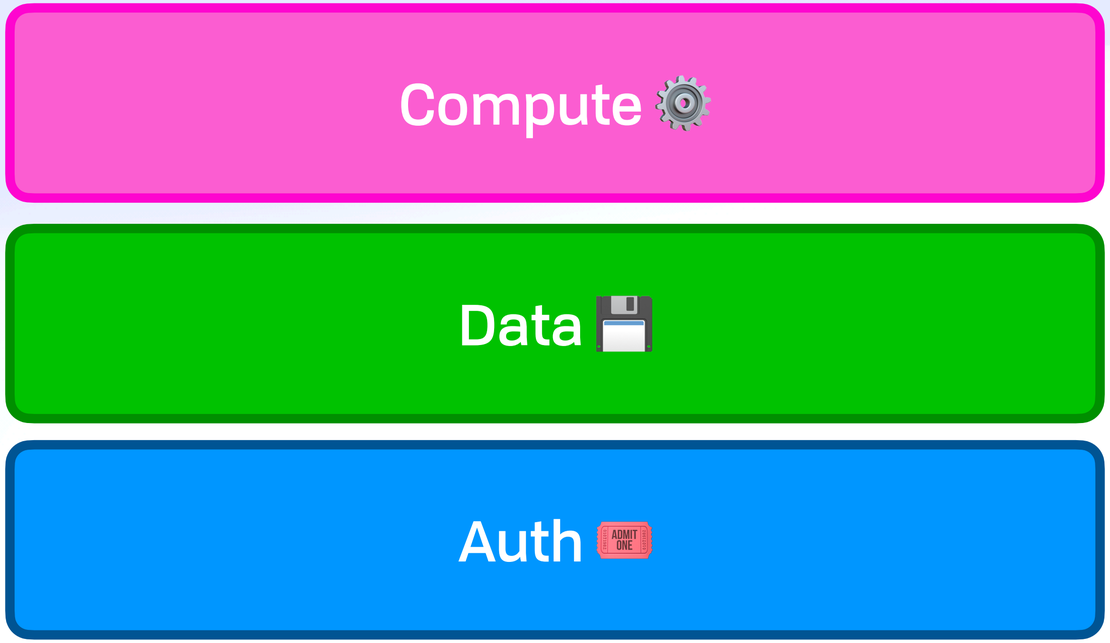
High Level Dependencies

Compute ⚙️

Data 💾

How to Power a New Internet ⚡

High Level Dependencies



How to Power a New Internet ⚡

Too Much & Not Enough

How to Power a New Internet ⚡

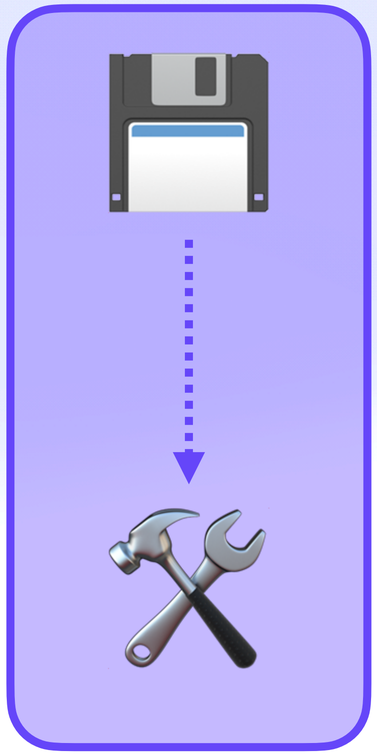
Too Much & Not Enough

How to Power a New Internet ⚡

Too Much & Not Enough

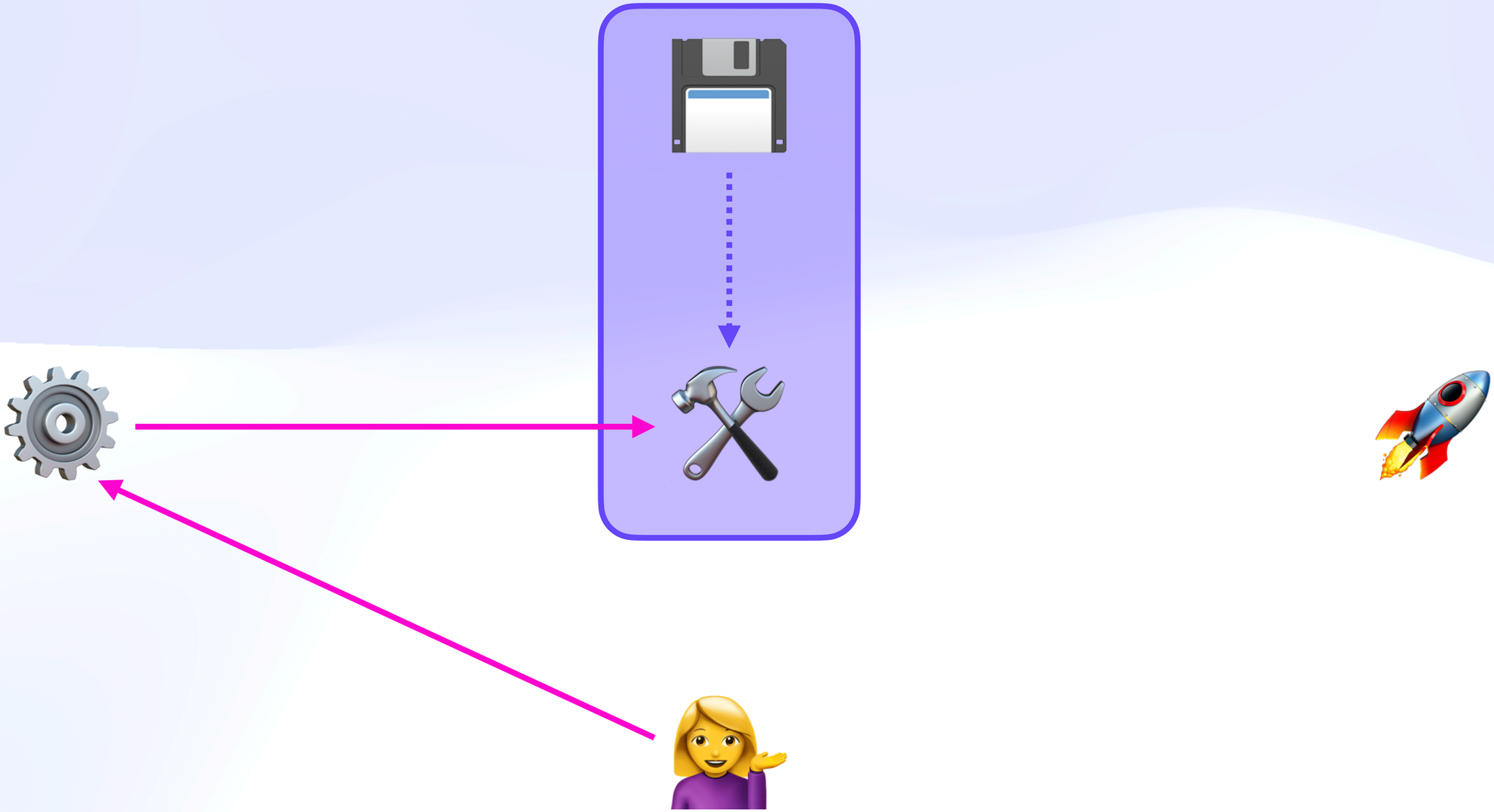
How to Power a New Internet ⚡

Too Much & Not Enough



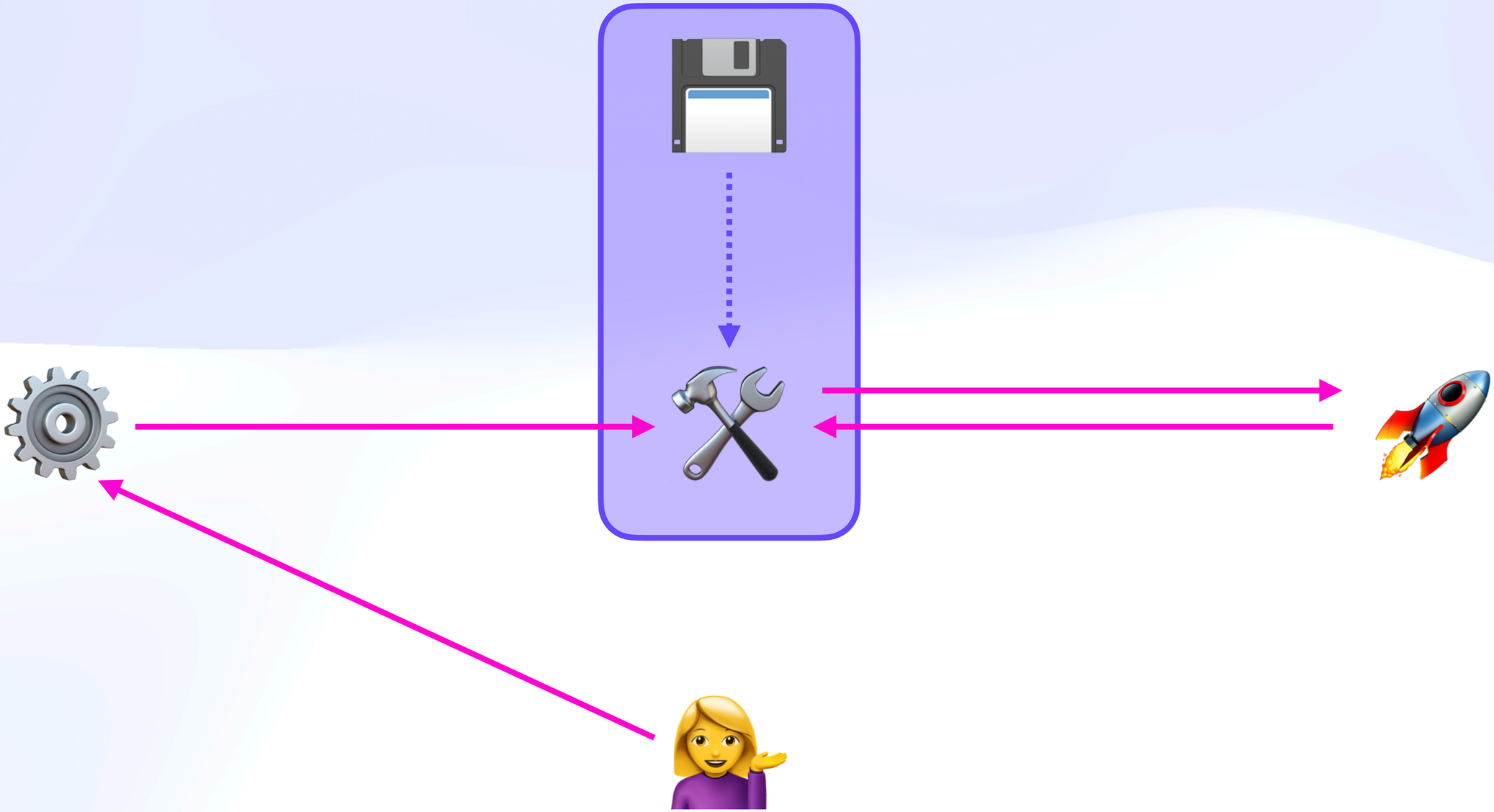
How to Power a New Internet ⚡

Too Much & Not Enough



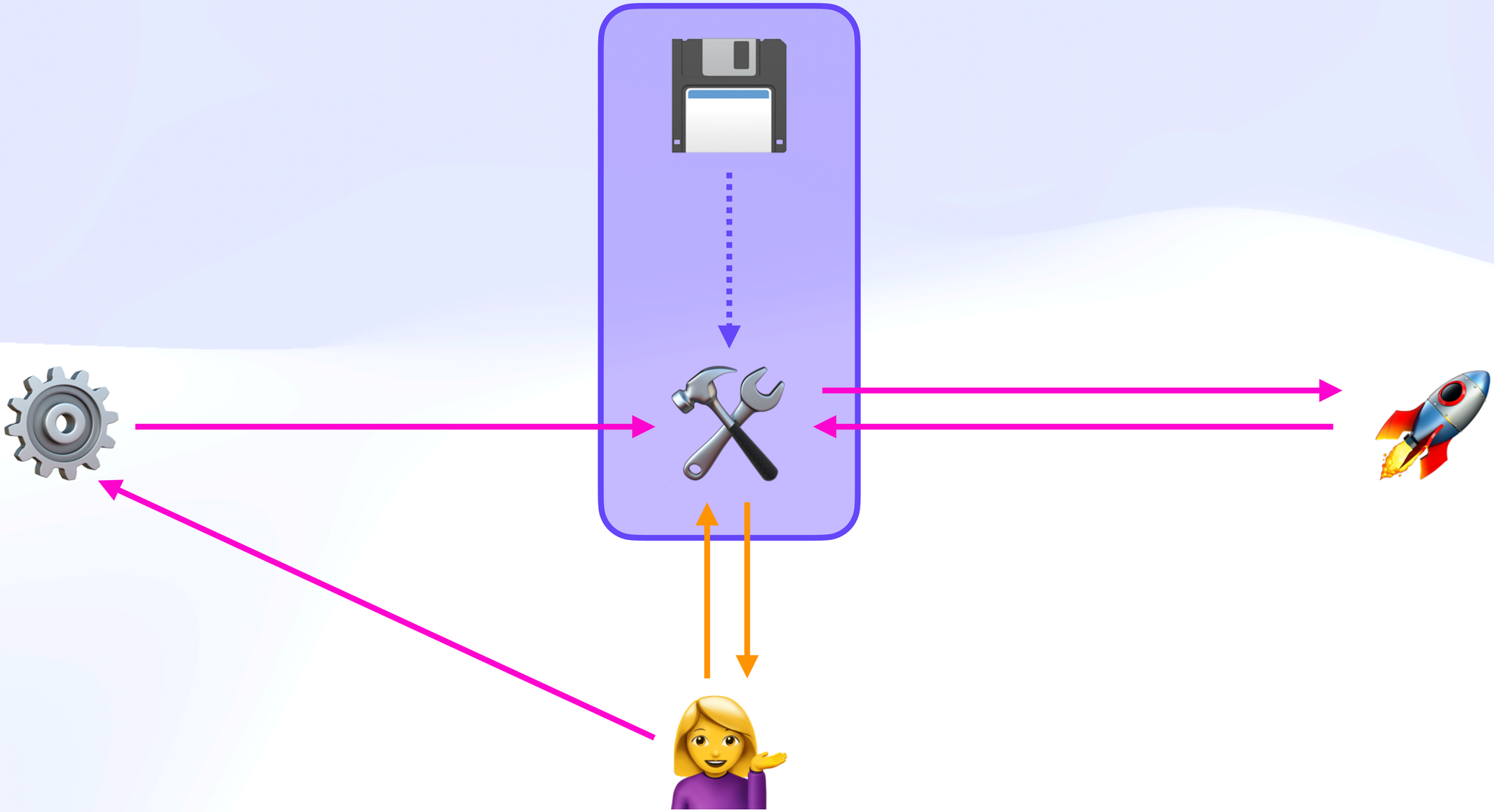
How to Power a New Internet ⚡

Too Much & Not Enough



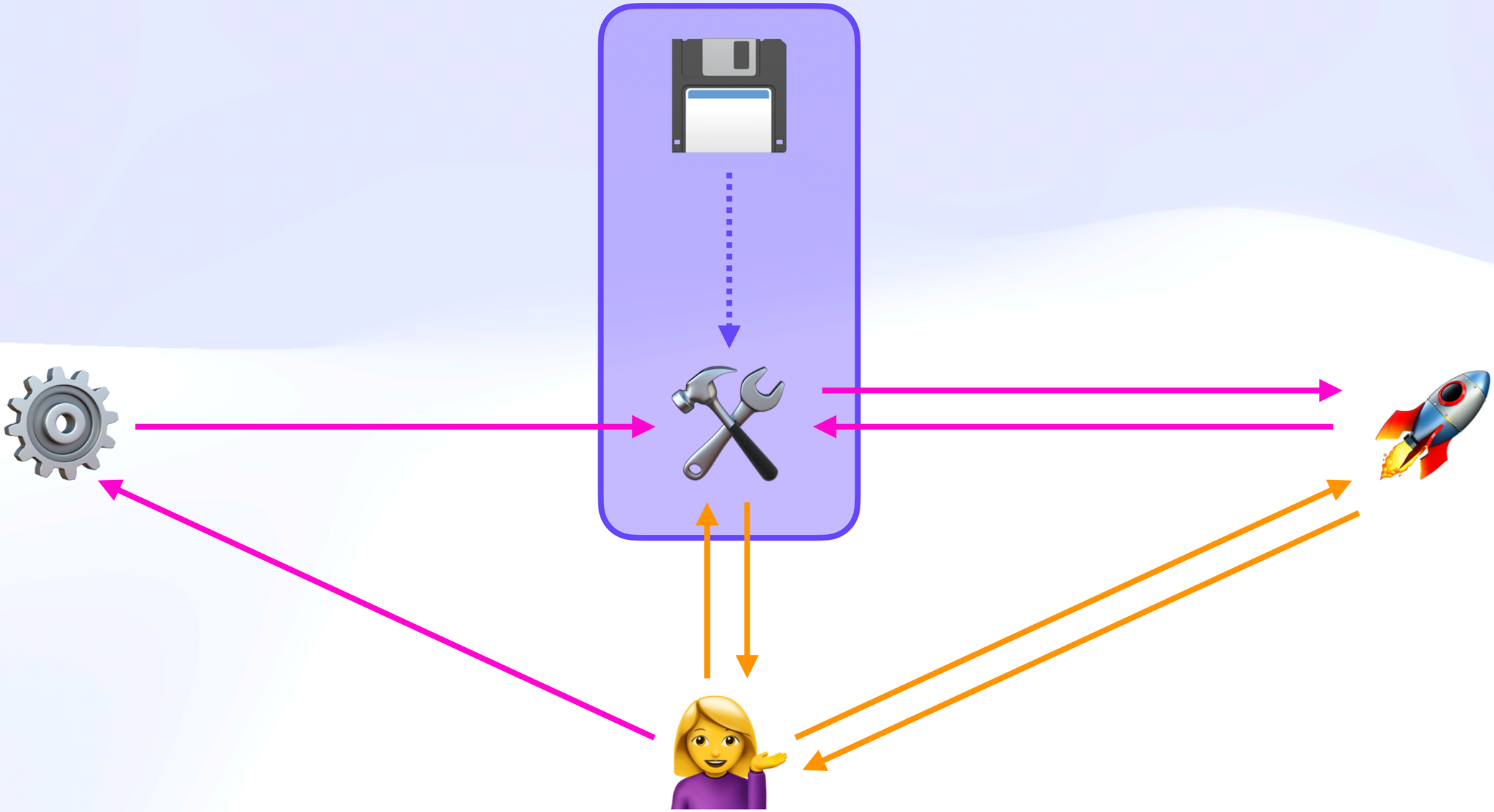
How to Power a New Internet ⚡

Too Much & Not Enough



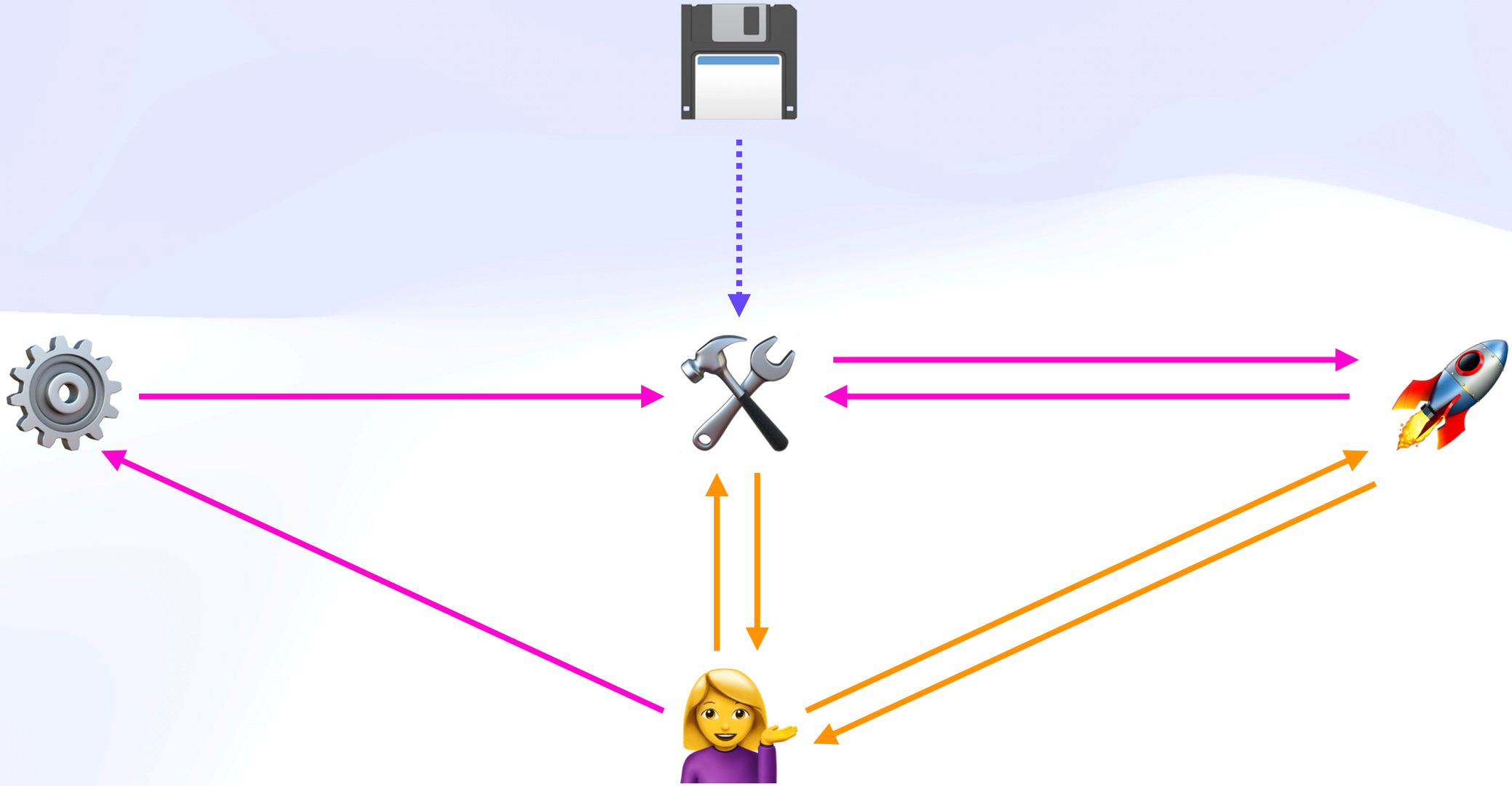
How to Power a New Internet ⚡

Too Much & Not Enough



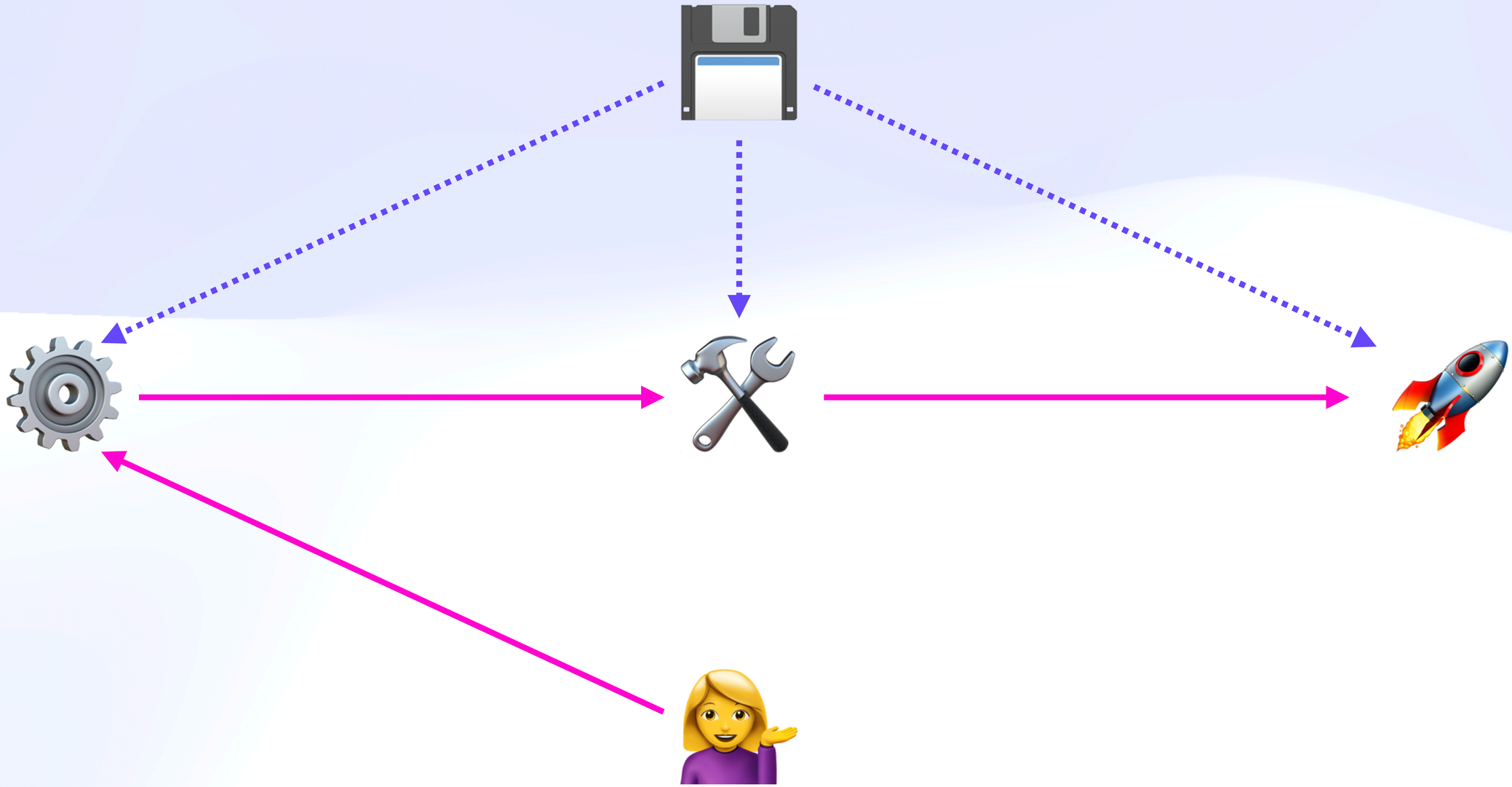
How to Power a New Internet ⚡

Too Much & Not Enough



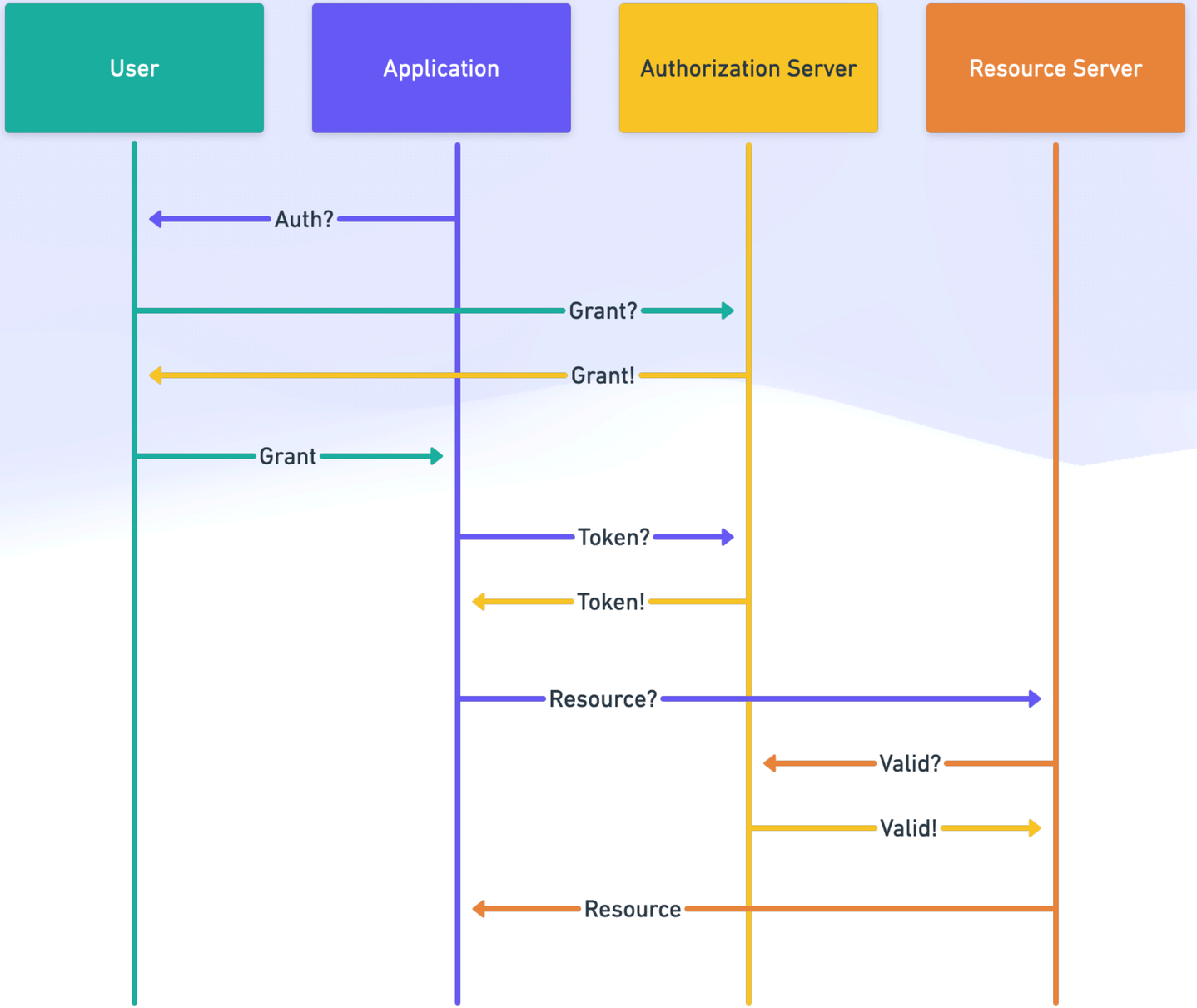
How to Power a New Internet ⚡

What We Want



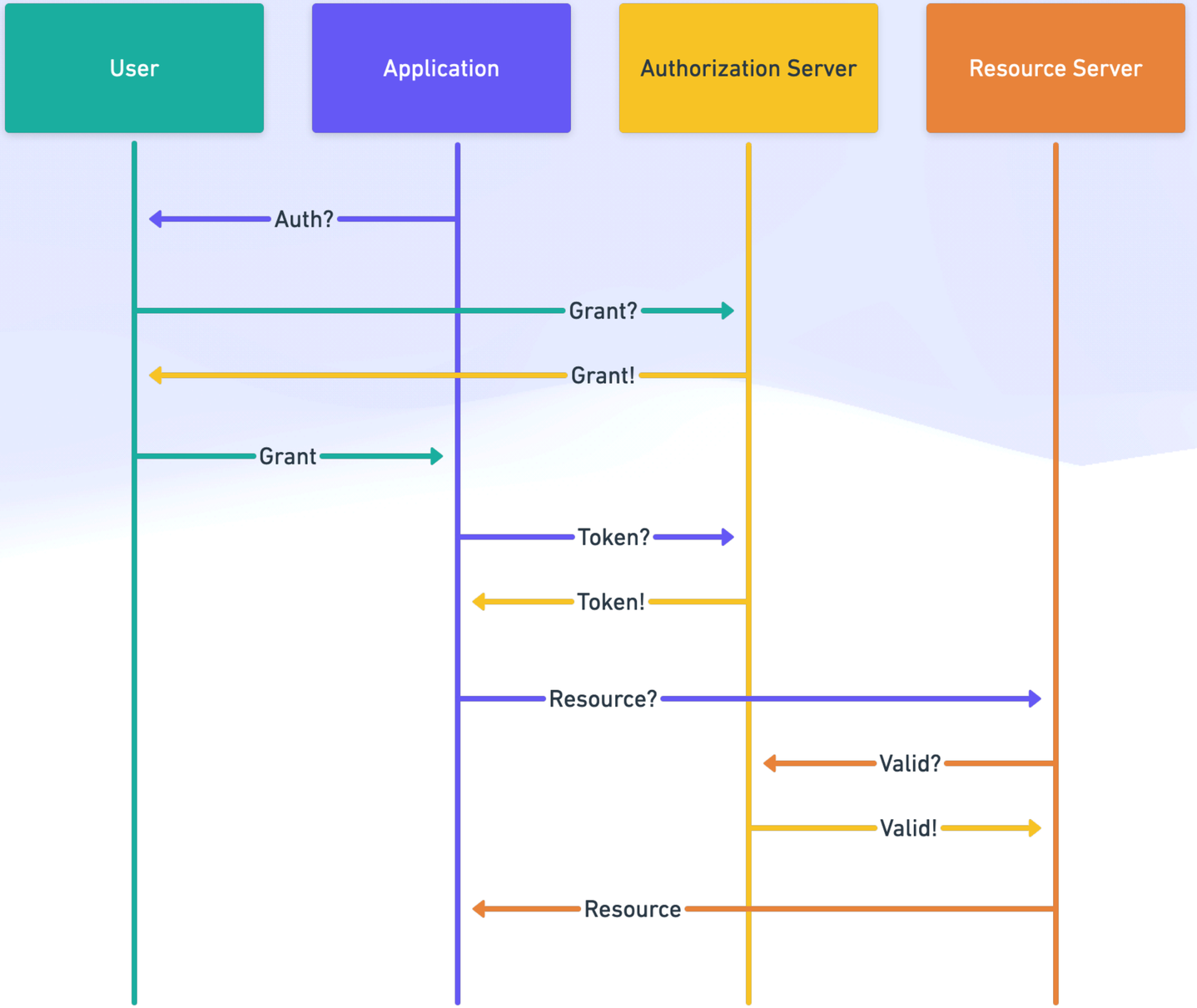
How to Power a New Internet ⚡

OAuth Sequence



How to Power a New Internet ⚡

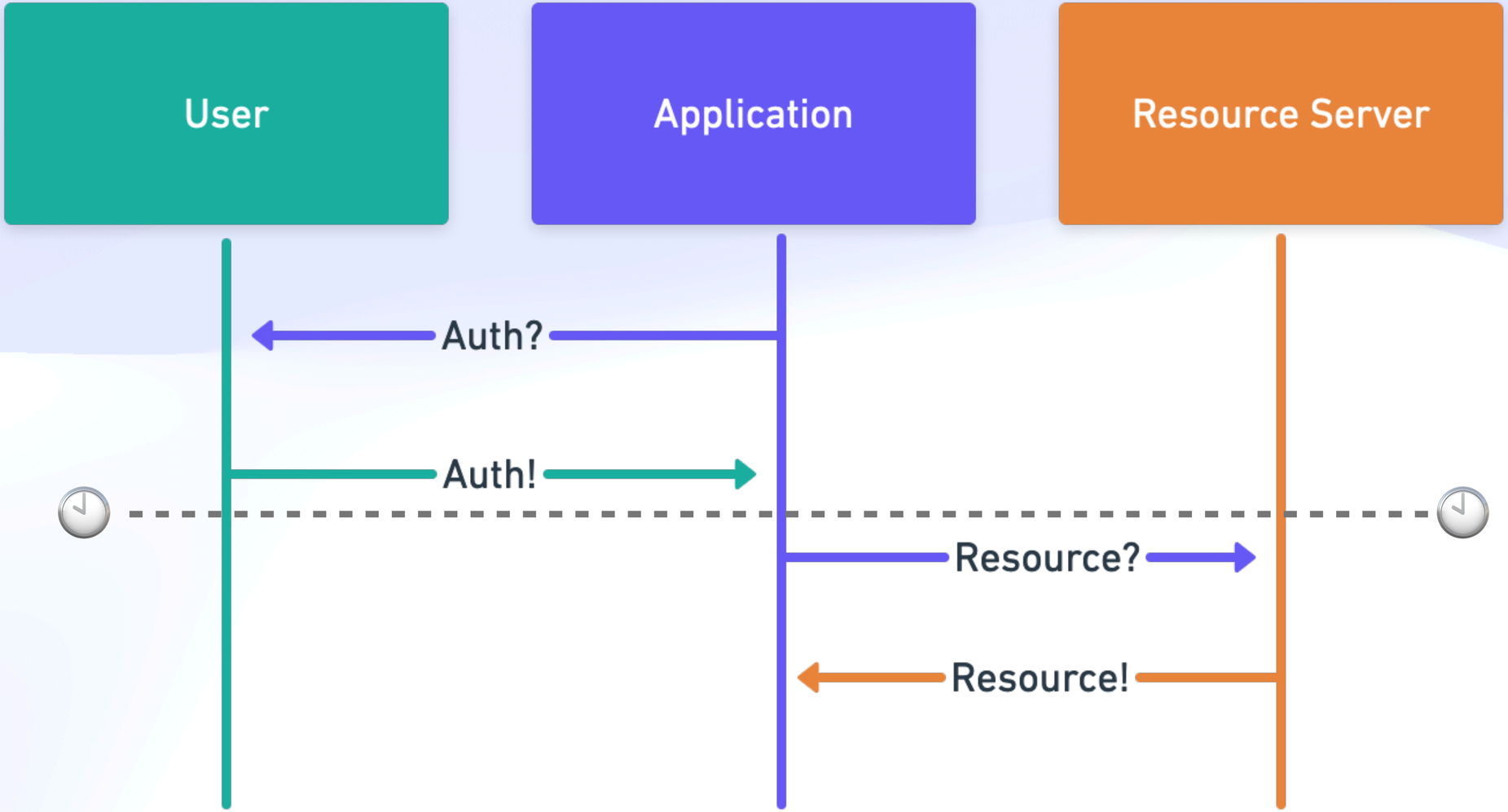
OAuth Sequence



Latency & Locality Problems!

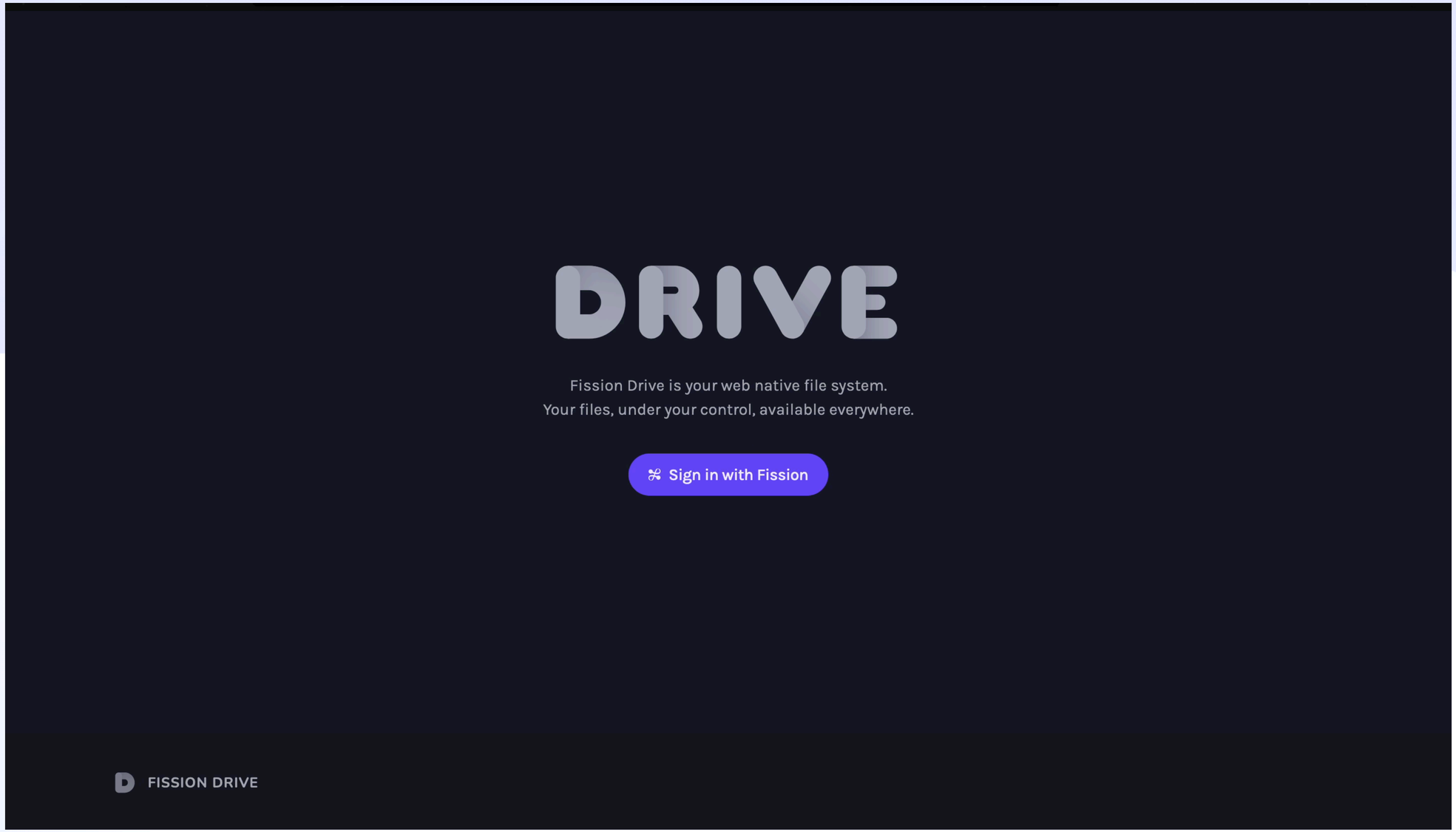
How to Power a New Internet ⚡

UCAN Sequence



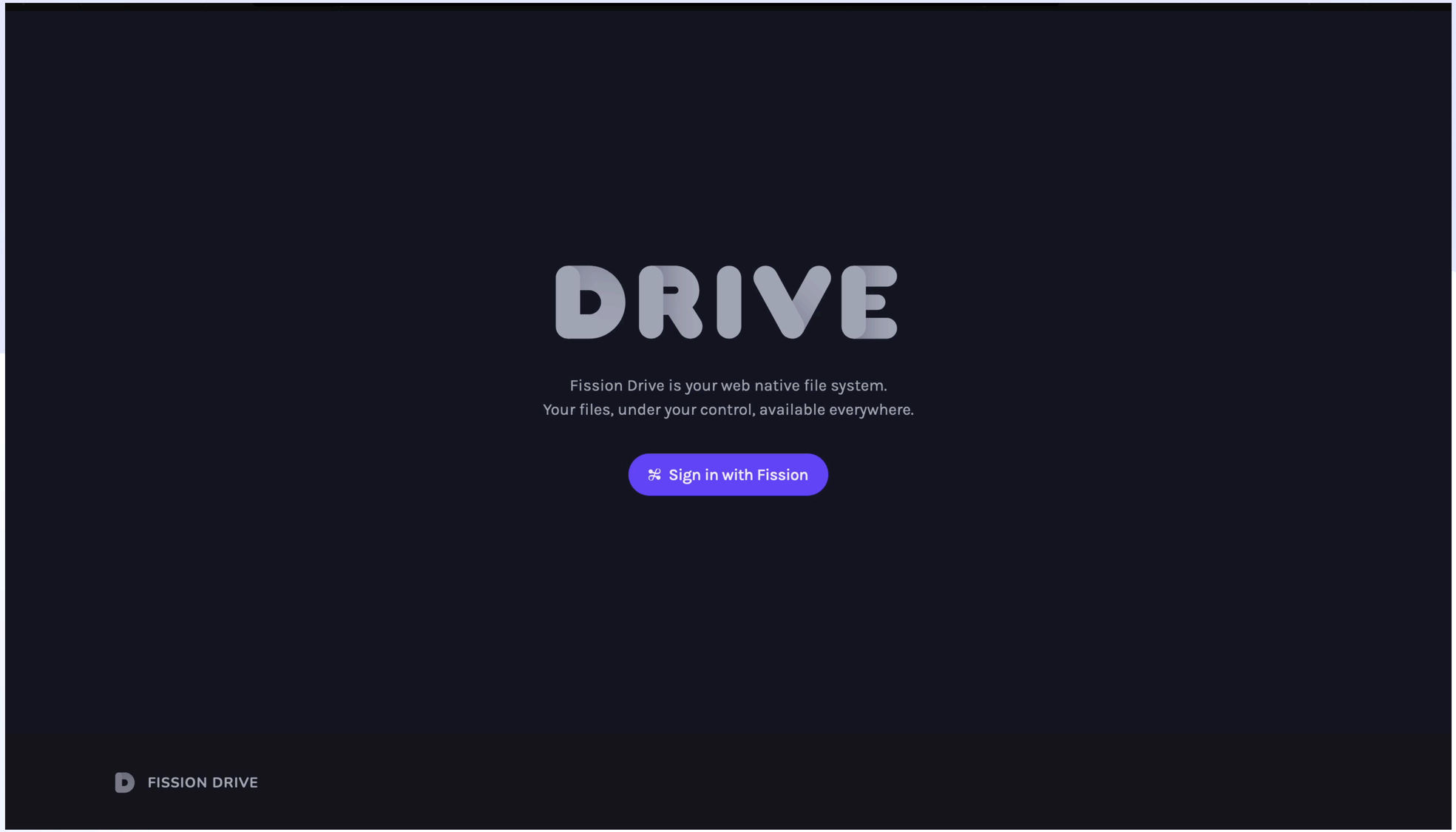
How to Power a New Internet ⚡

Auth Should Be Boring



How to Power a New Internet ⚡

Auth Should Be Boring



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?

AuthN

DIDs say who **you are**

UCANs show what **you can do**

AuthZ

Yes, UCAN!

Teaser Token


```
eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V5Ono2TWtzWFFCZkw4b3d6dFRDSlRt
N2hOUmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90
ZXMvIiwiY2FwIjoiT1ZFUldSSVRFIn1dLCJleHAiOjkyNTY5Mzk1MDUsImlzcyI6ImRpZDprZXk6ejZNa3A1RXN6OXMyTUhzcVl2TG9j
Y3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjoxNjM5NjA4MjkzLCJwcmYiOltdfQ.MgYarLqy7RmQ1AIrqYL6cFy9z7a5W
IAU--TYARPSgirOSszvar3_DNr25rbPretHbnT0mMVKyoaQXruR7KbrBg
```



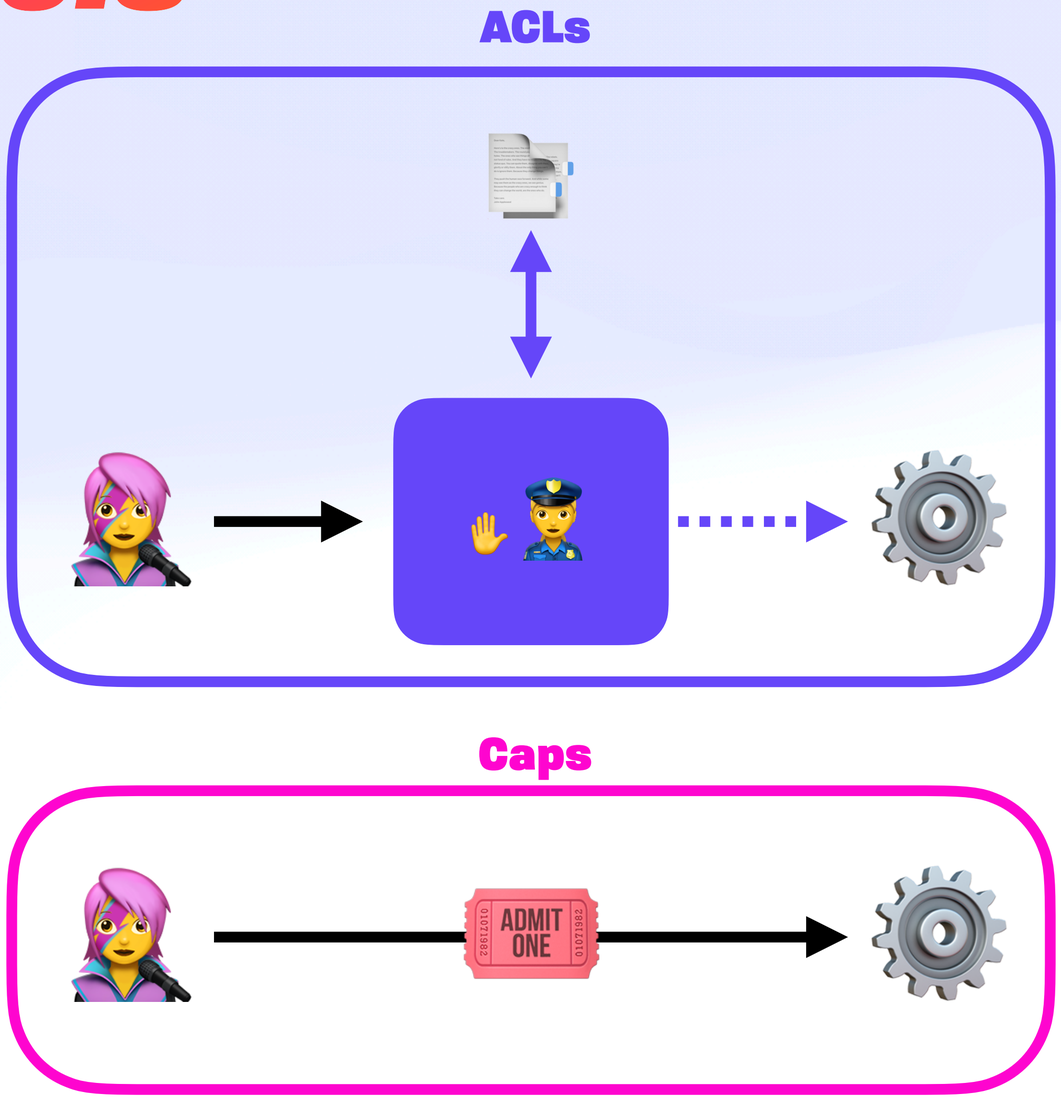
```
{
  "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99",
  "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
  "exp": 9256939505,
  "nbf": 1639608293,
  "att": [
    {
      "with": "wnfs://demouser.fission.name/public/notes/",
      "can": "OVERWRITE"
    }
  ]
}
```

Yes, UCAN!

AuthZ Models

Yes, UCAN!

AuthZ Models



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

Yes, UCAN!

ACL Read & Write

Yes, UCAN!

ACL Read & Write

Not in control

Yes, UCAN!

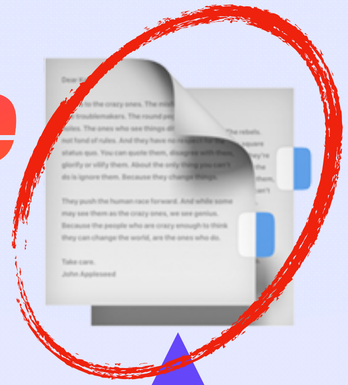
ACL Read & Write

In control

Not in control

Yes, UCAN!

ACL Read & Write

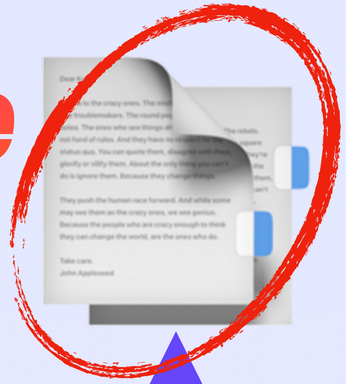


In control

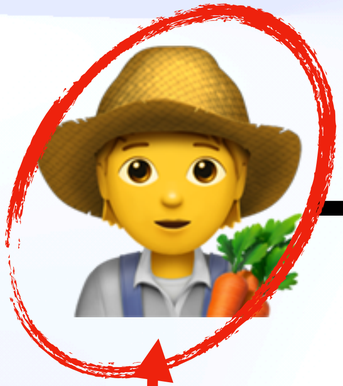
Not in control

Yes, UCAN!

ACL Read & Write



In control



Not in control

Yes, UCAN!

Capabilities-as-Tickets

Yes, UCAN!

Capabilities-as-Tickets

Yes, UCAN!

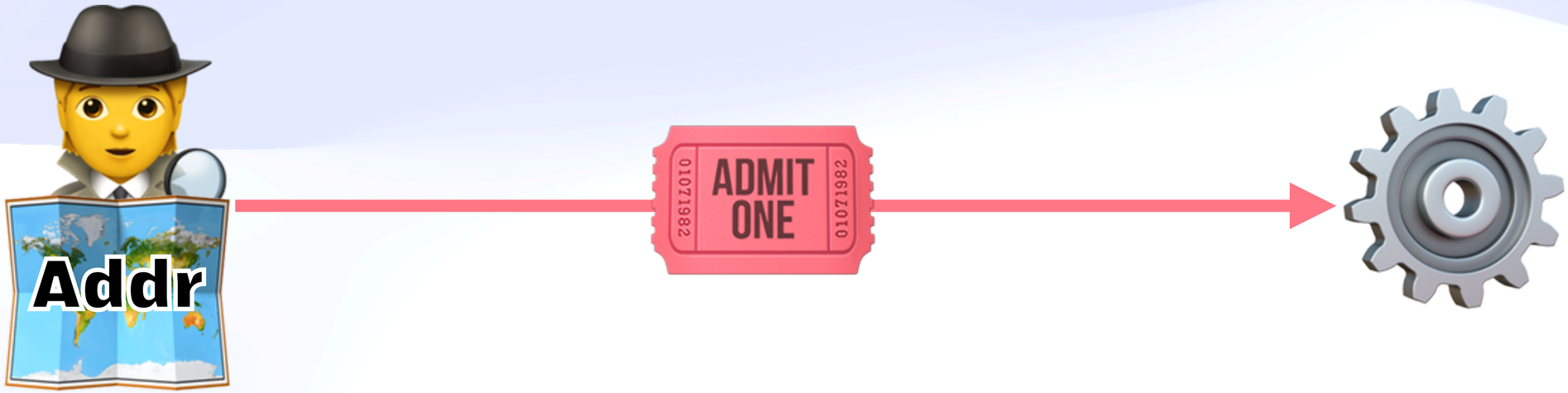
Capabilities-as-Tickets

Yes, UCAN!

Capabilities-as-Tickets

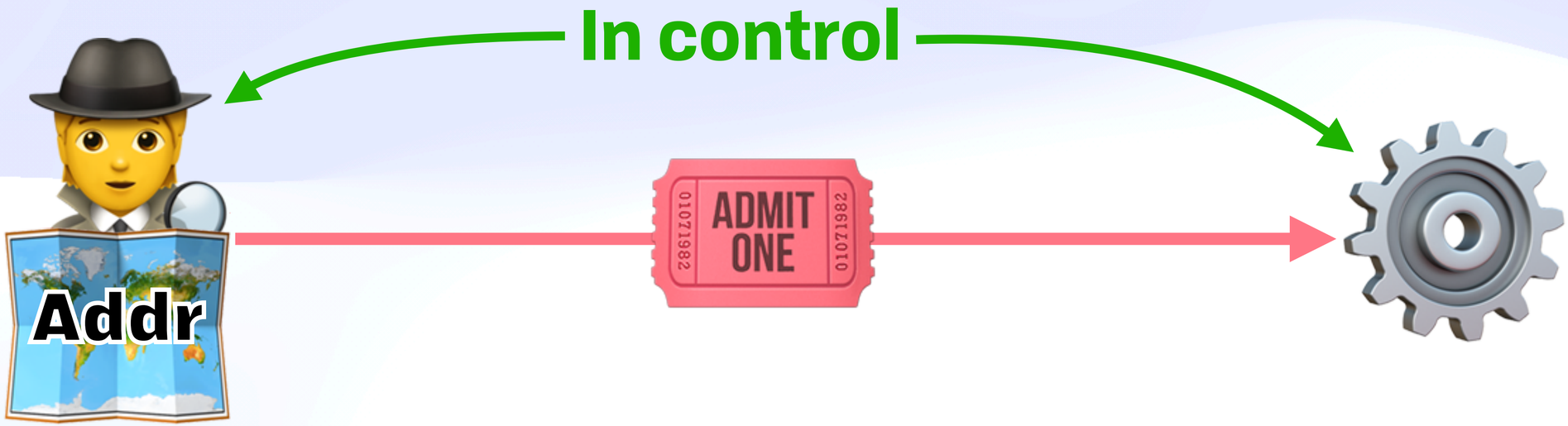
Yes, UCAN!

Capabilities-as-Tickets



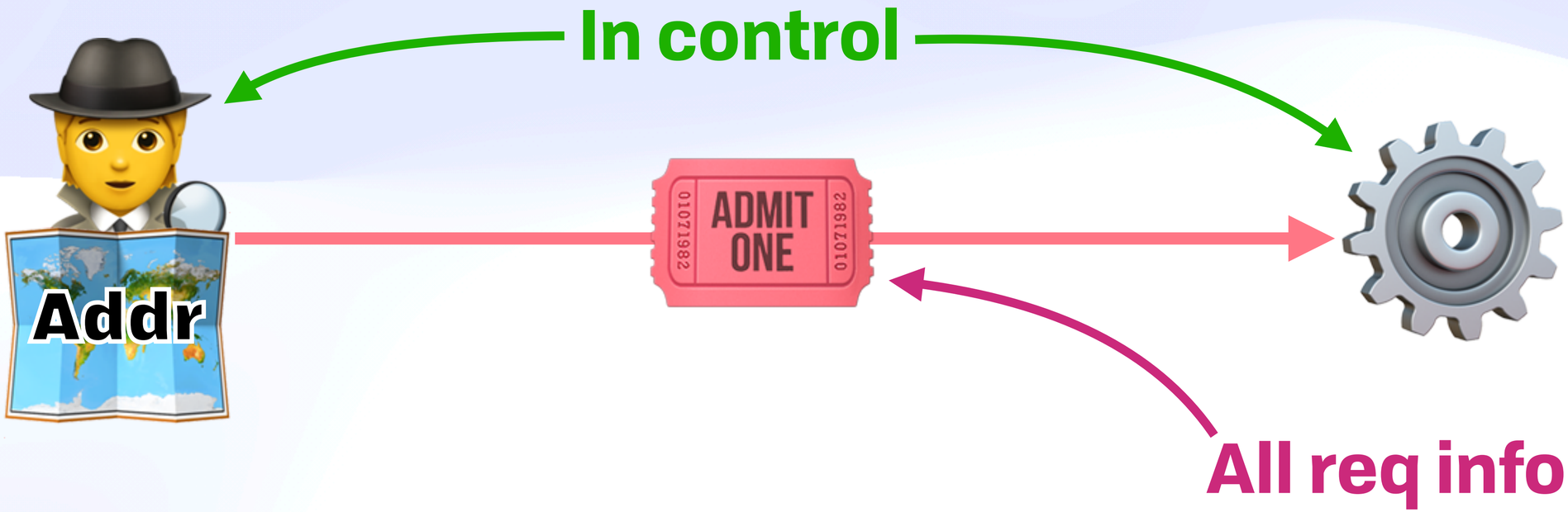
Yes, UCAN!

Capabilities-as-Tickets



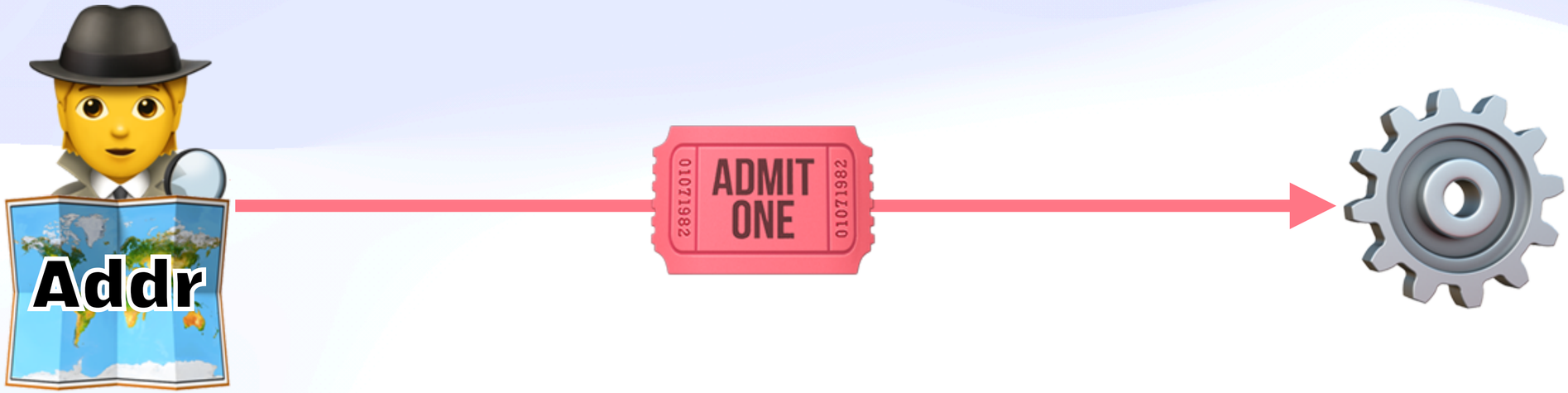
Yes, UCAN!

Capabilities-as-Tickets



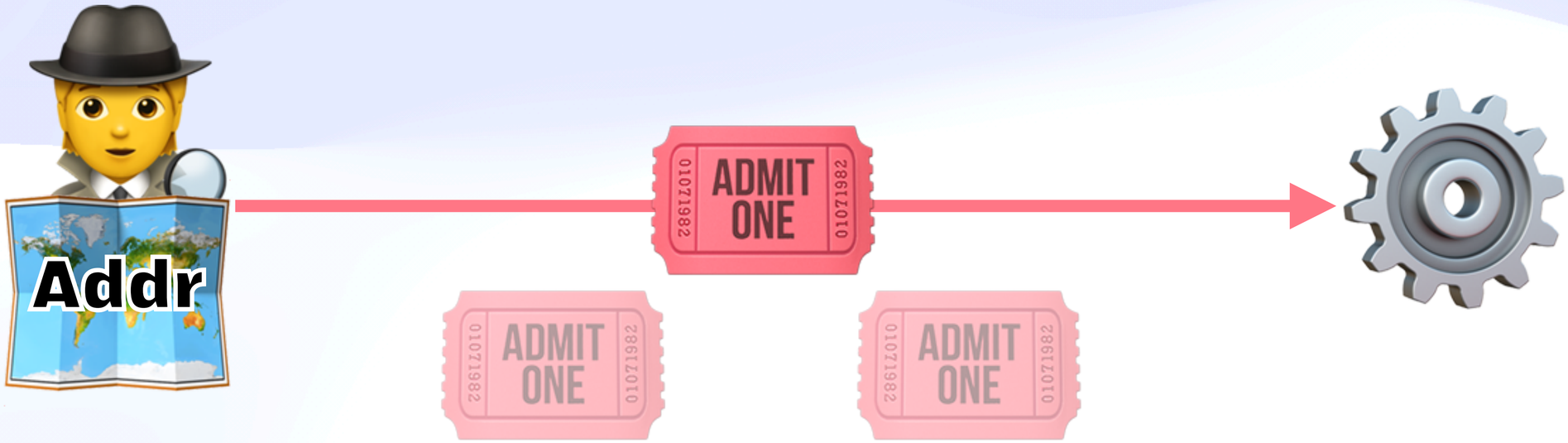
Yes, UCAN!

Capabilities-as-Tickets



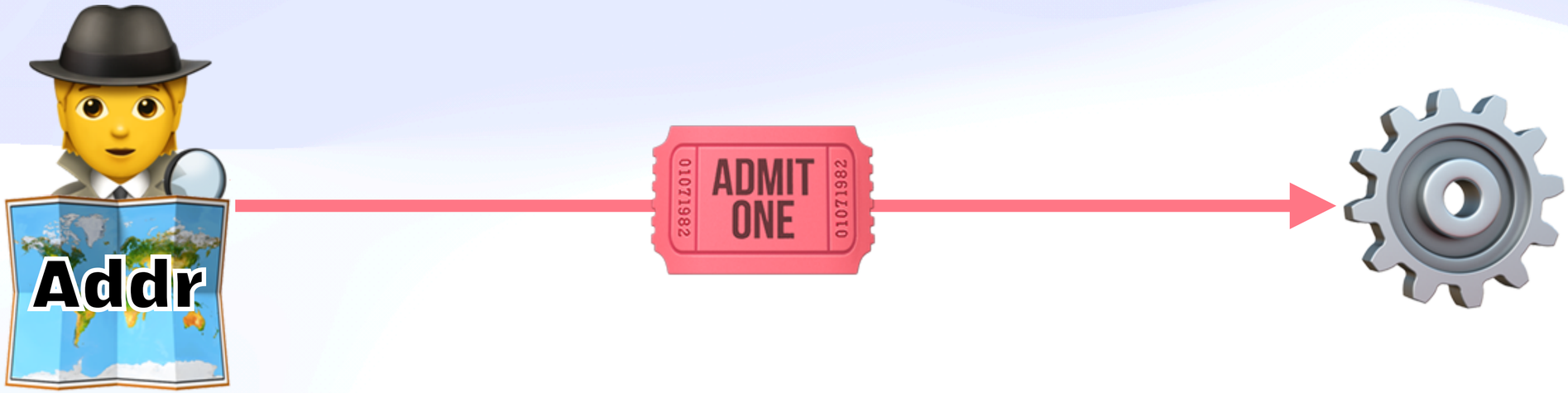
Yes, UCAN!

Capabilities-as-Tickets



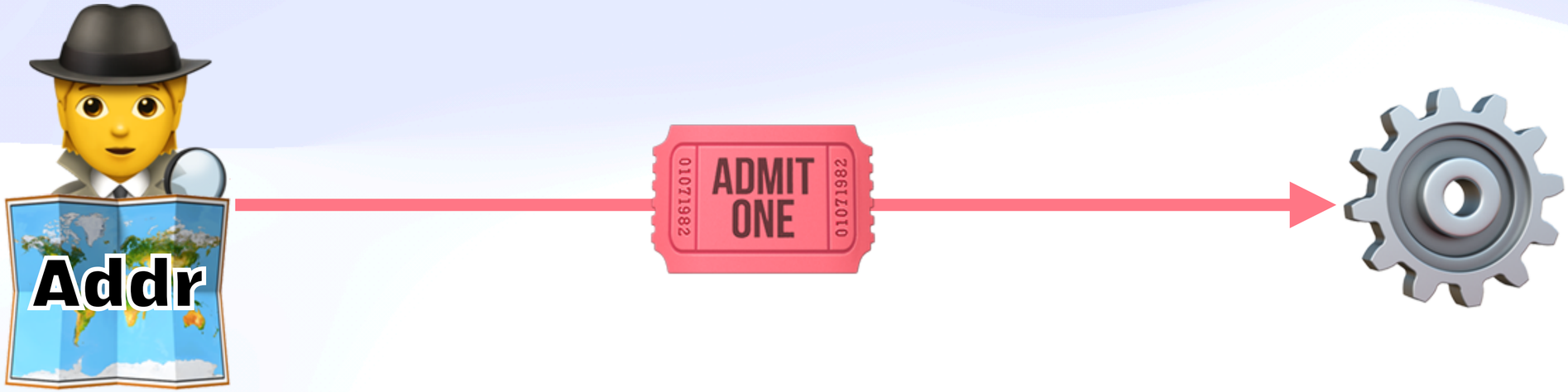
Yes, UCAN!

Capabilities-as-Tickets



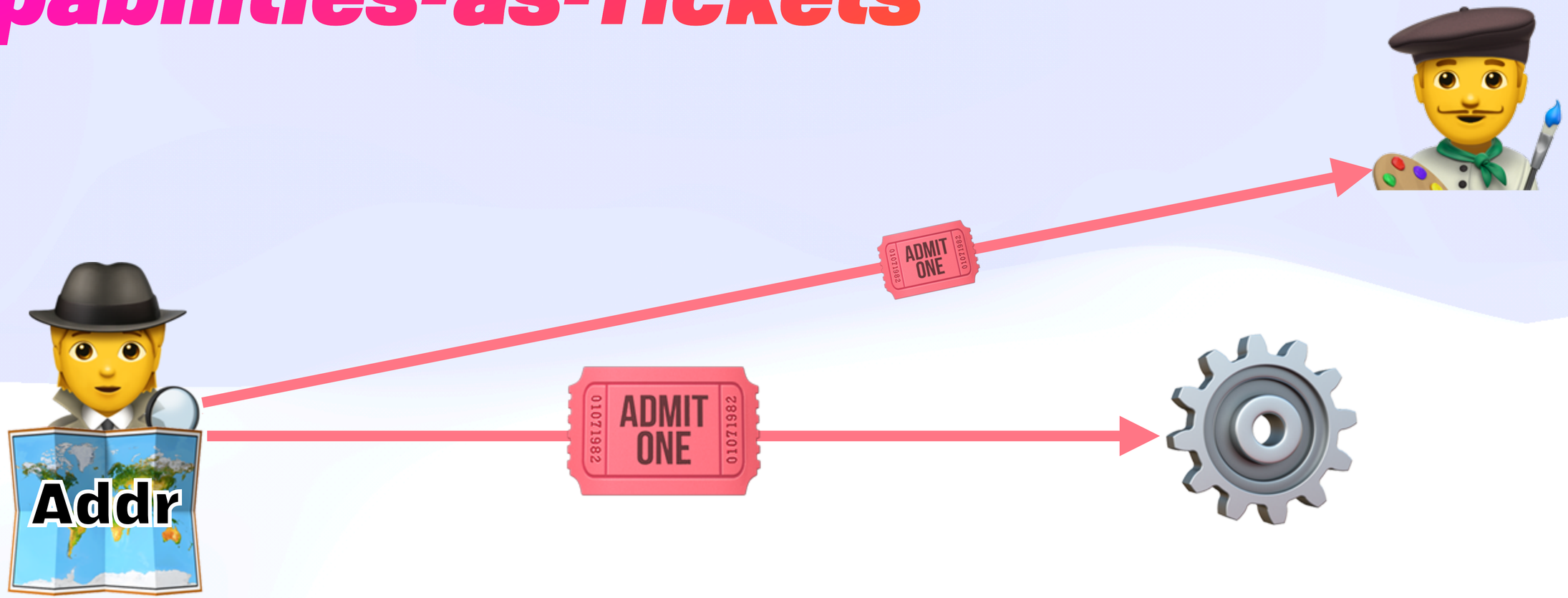
Yes, UCAN!

Capabilities-as-Tickets



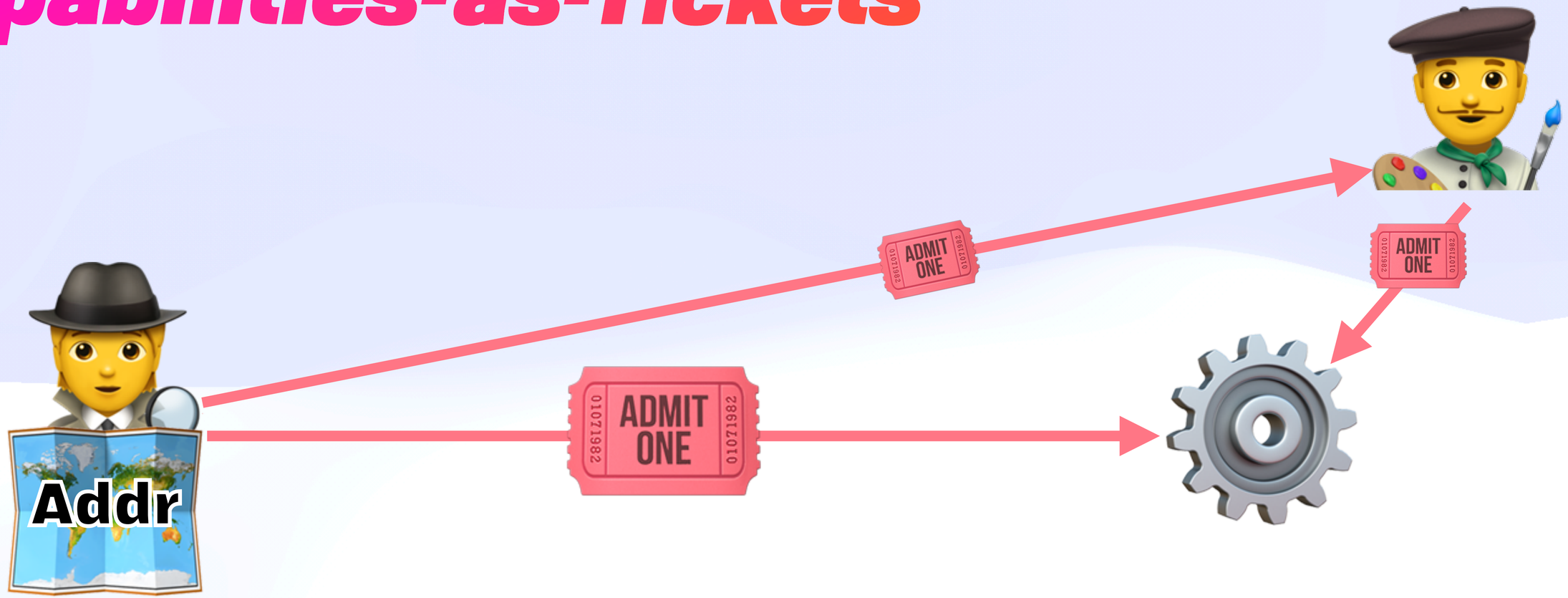
Yes, UCAN!

Capabilities-as-Tickets



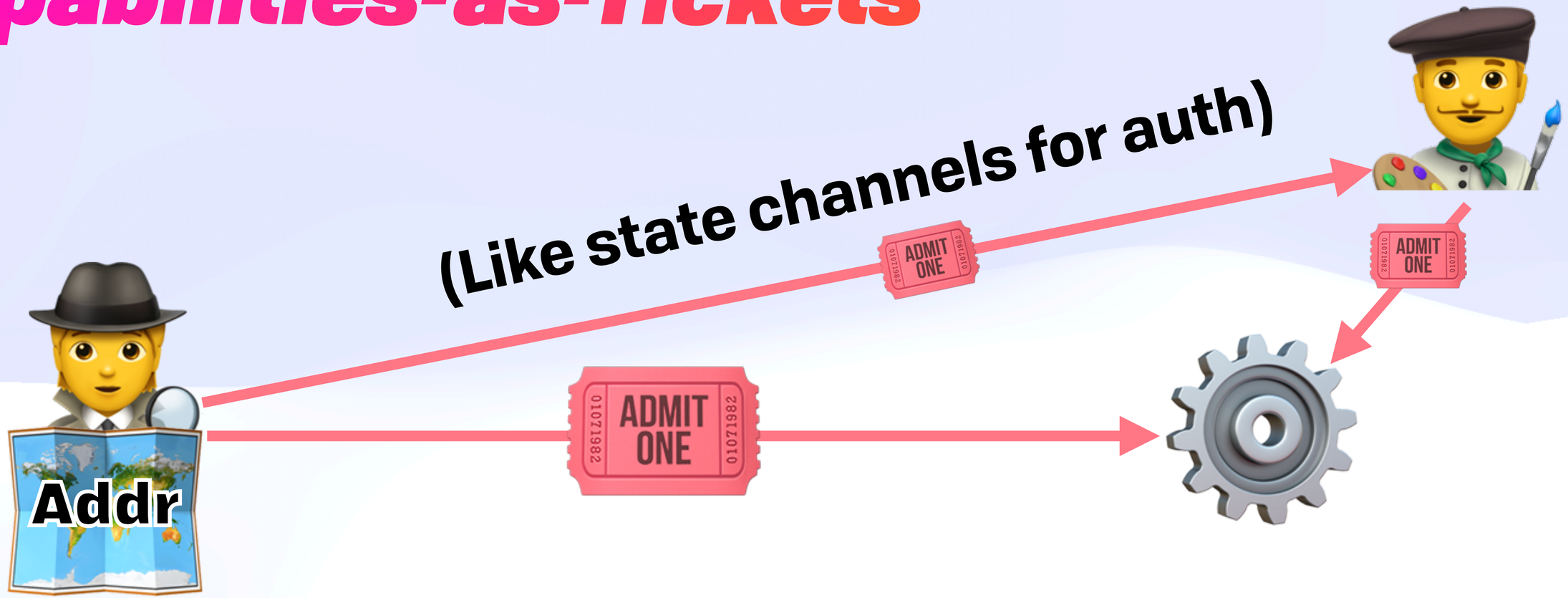
Yes, UCAN!

Capabilities-as-Tickets



Yes, UCAN!

Capabilities-as-Tickets



Yes, UCAN!

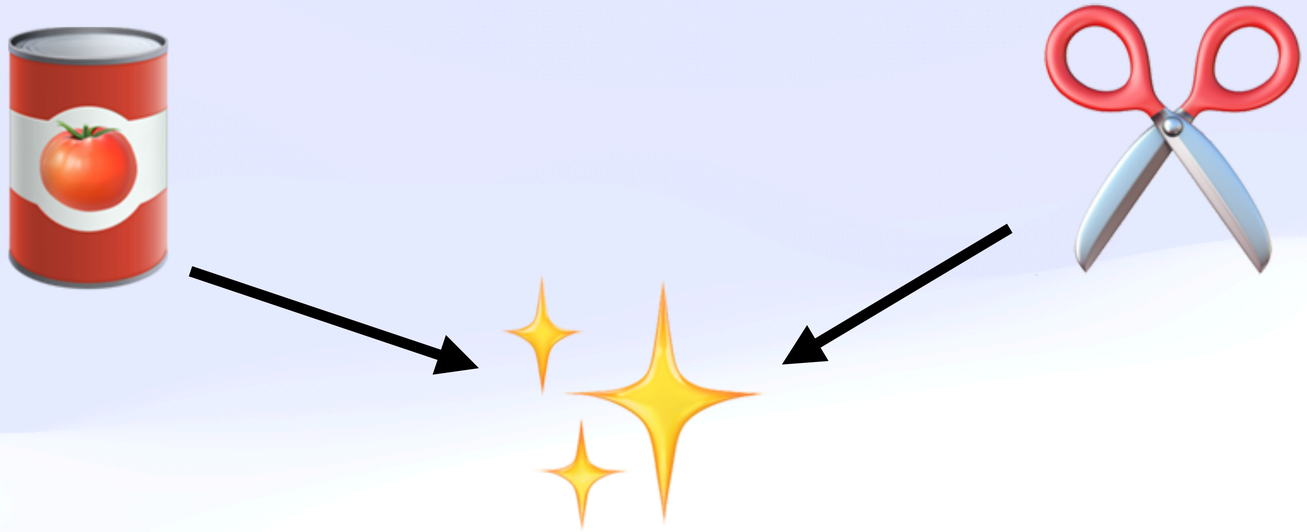
Rights Amplification

Yes, UCAN!

Rights Amplification

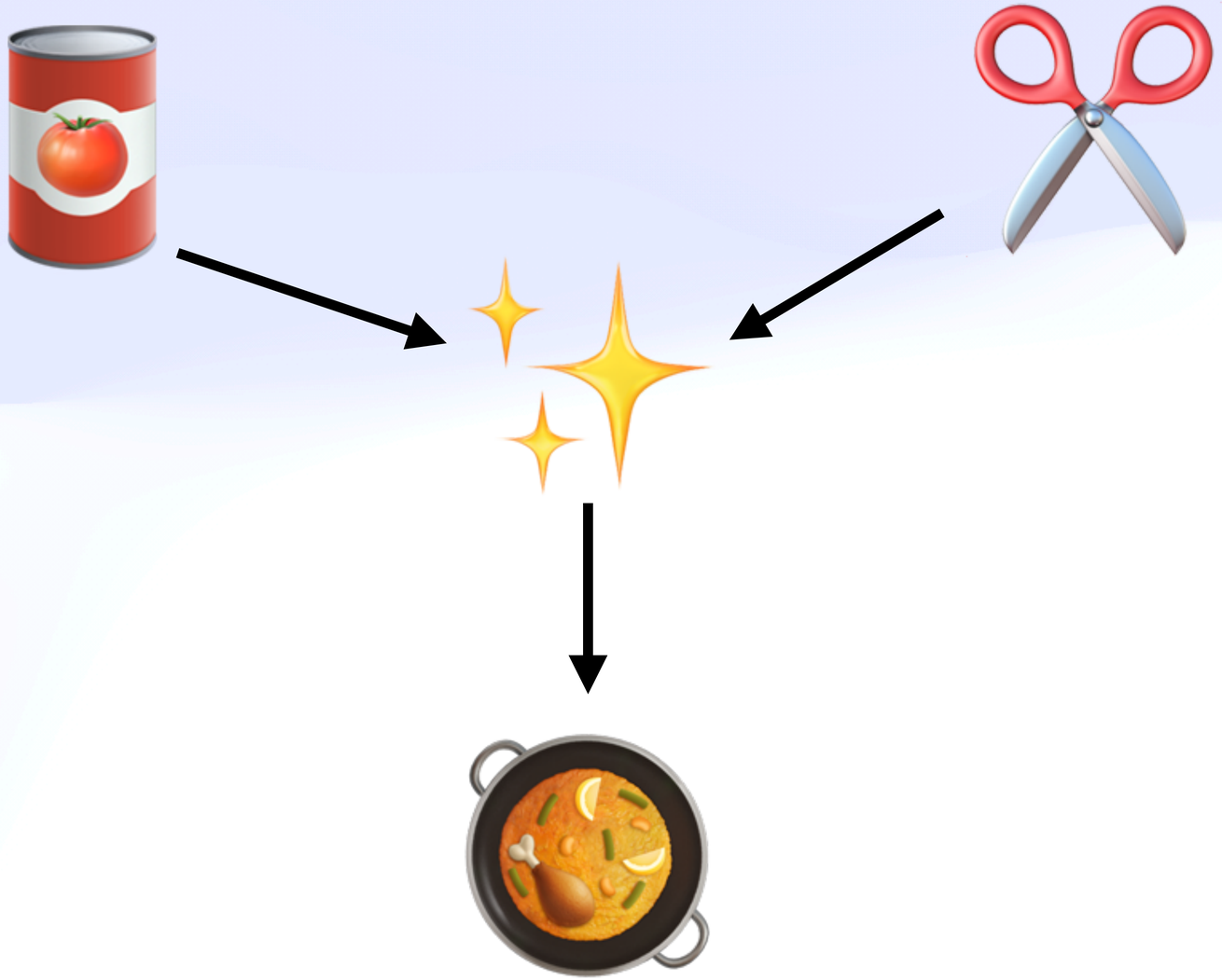
Yes, UCAN!

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

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"
    }
  ]
}
```

Yes, 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"
    }
  ]
}
```

Signature

```
kwRdqPN74pkcpXGgdk7Z7FW3M1mRR
YaDE5ZgkG6srAuu6V6mvMVRdBLnD5
CWid-X4tDIKpliVjlCSLTntB4pCw
```

Yes, UCAN!

JWT → UCAN

Header

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

Payload

```
{
  "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ"
  "aud": "did:key:z6MkvXTPUv8bxtsVQtGo7Ntk4qKJNcgK2tt52pc73teUpRLT",
  "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!

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"

(URI)

```
[
  {
    "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


```
[
  {
    "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

```
[
  {
    "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)	Action (Cap)
https:	crud/create
mailto:	crud/read
file:	crud/update
wnfs:	crud/destroy
dns:	
news:	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!

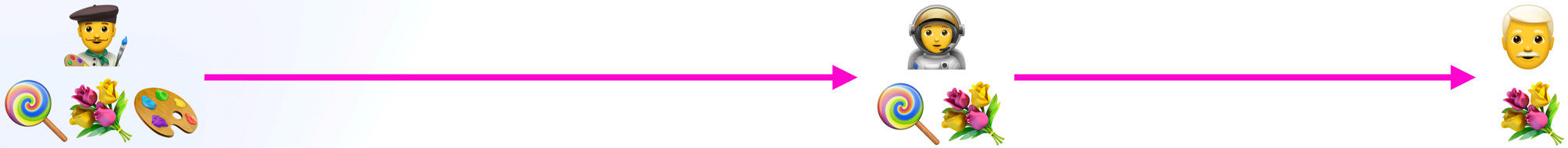
Chain Witnesses

Yes, UCAN!

Chain Witnesses

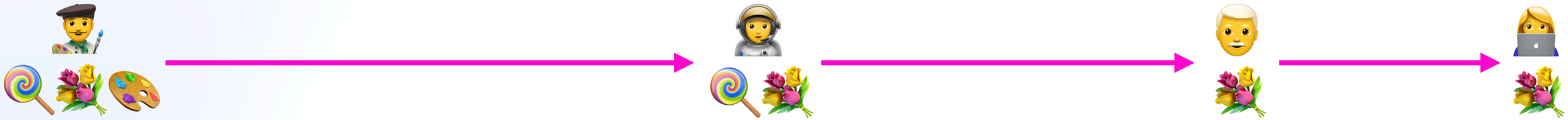
Yes, UCAN!

Chain Witnesses



Yes, UCAN!

Chain Witnesses

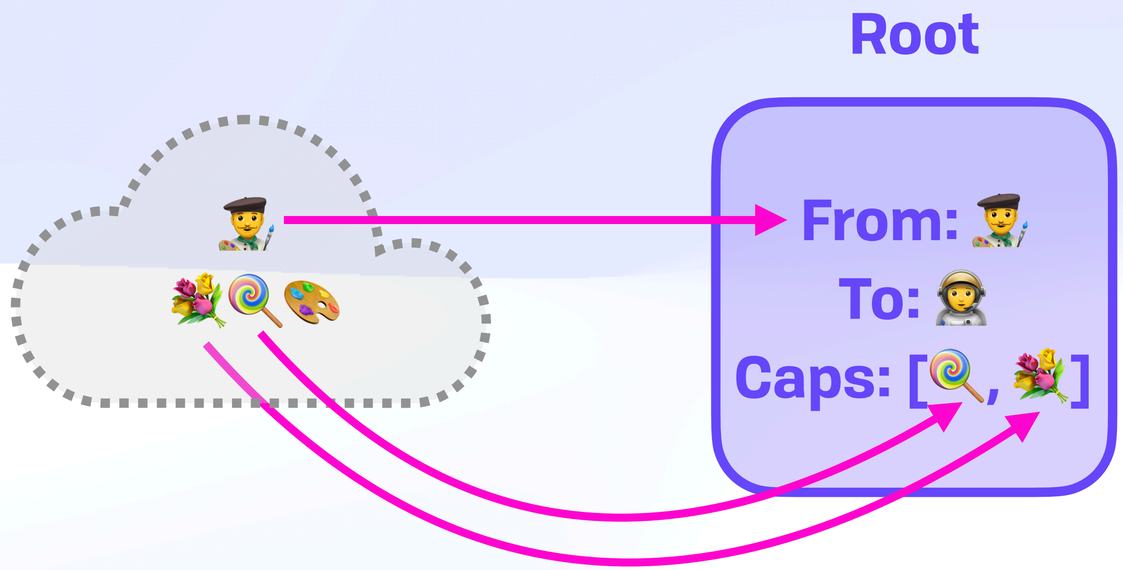


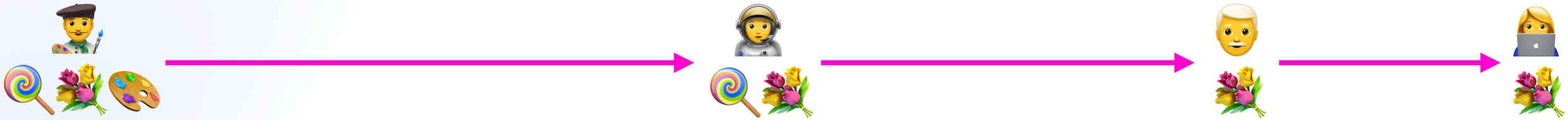
Yes, UCAN!

Chain Witnesses

Yes, UCAN!

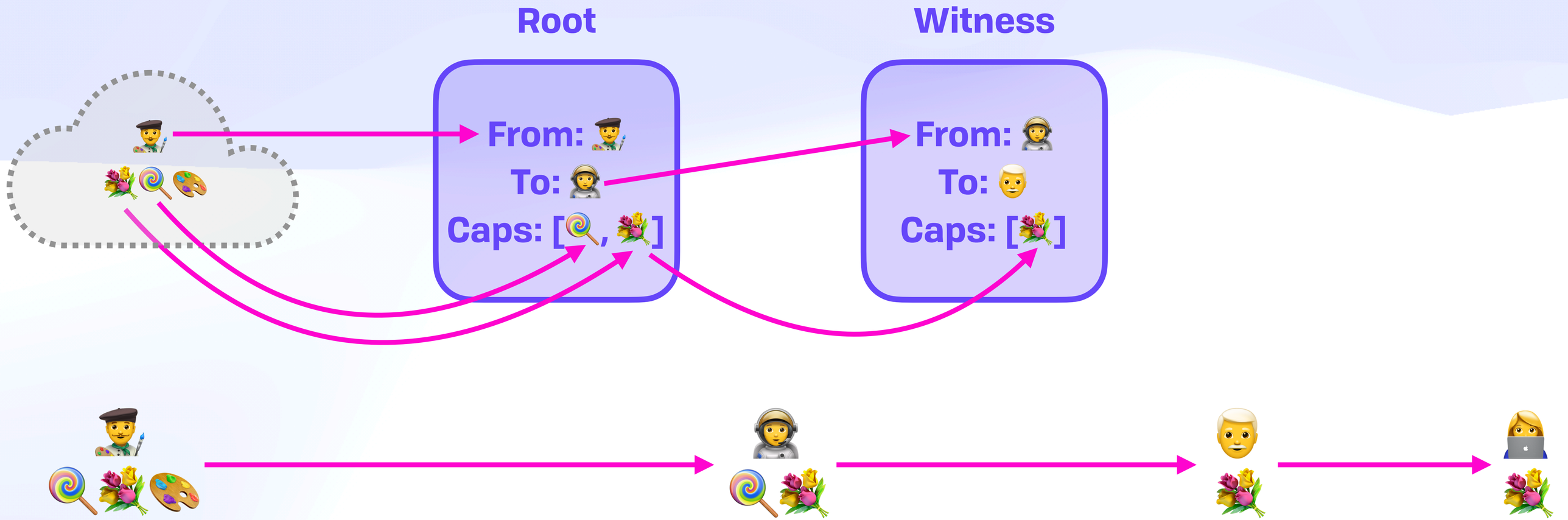
Chain Witnesses





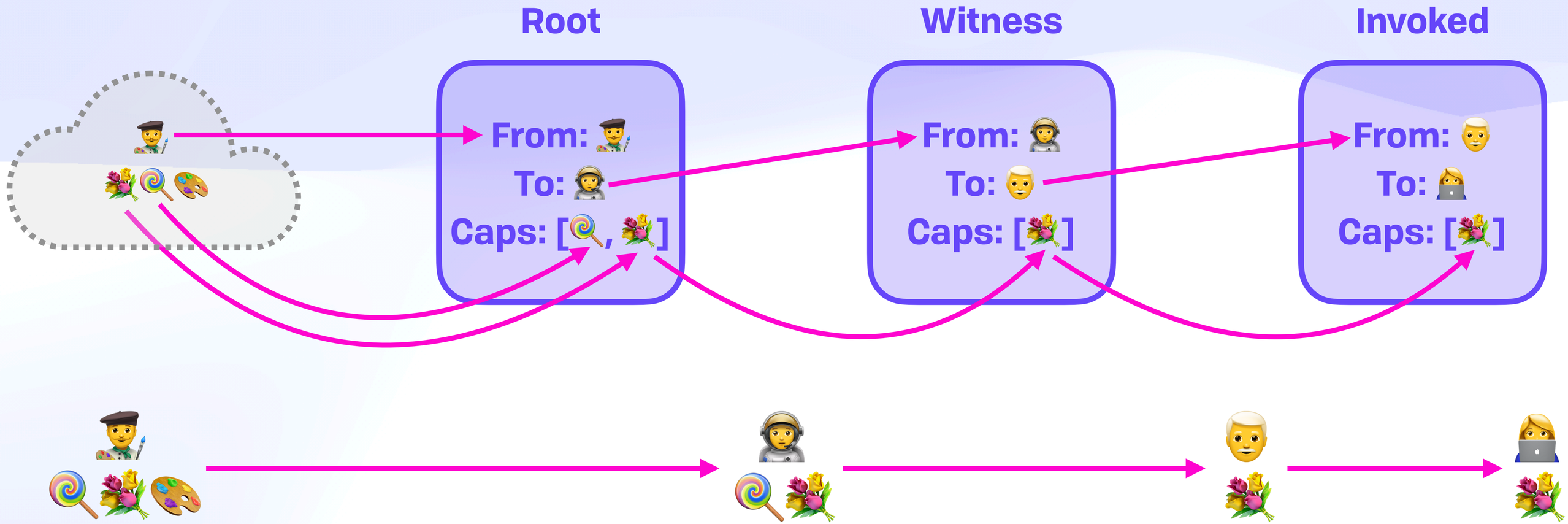
Yes, UCAN!

Chain Witnesses



Yes, UCAN!

Chain Witnesses



Yes, UCAN!

Non-Extractable Browser Keys

Yes, UCAN!

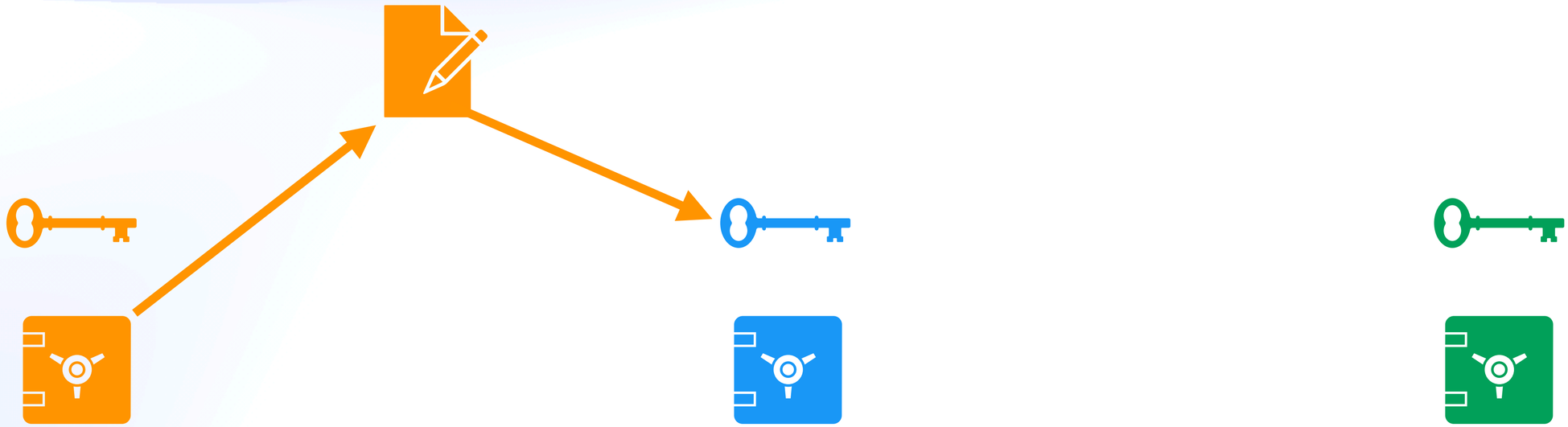
Non-Extractable Browser Keys

Yes, UCAN!

Non-Extractable Browser Keys

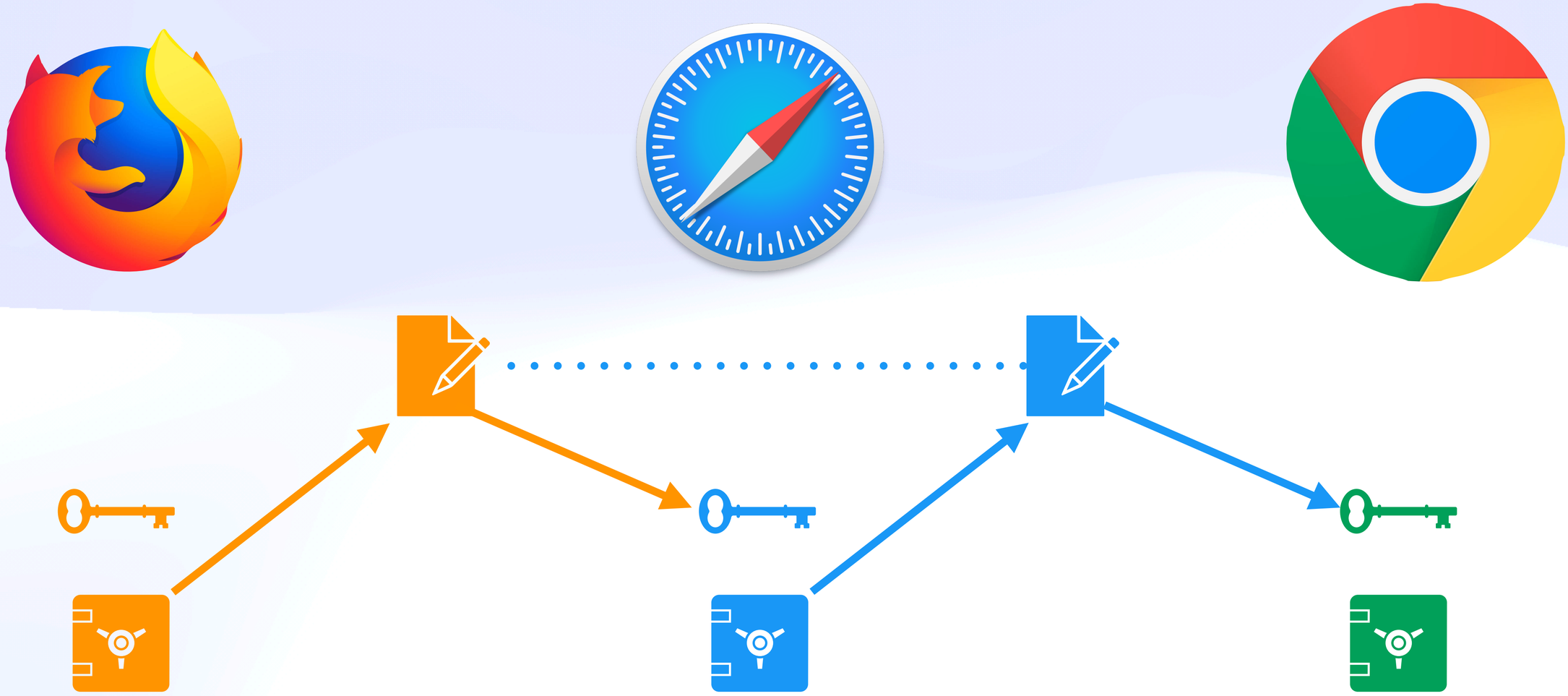
Yes, UCAN!

Non-Extractable Browser Keys



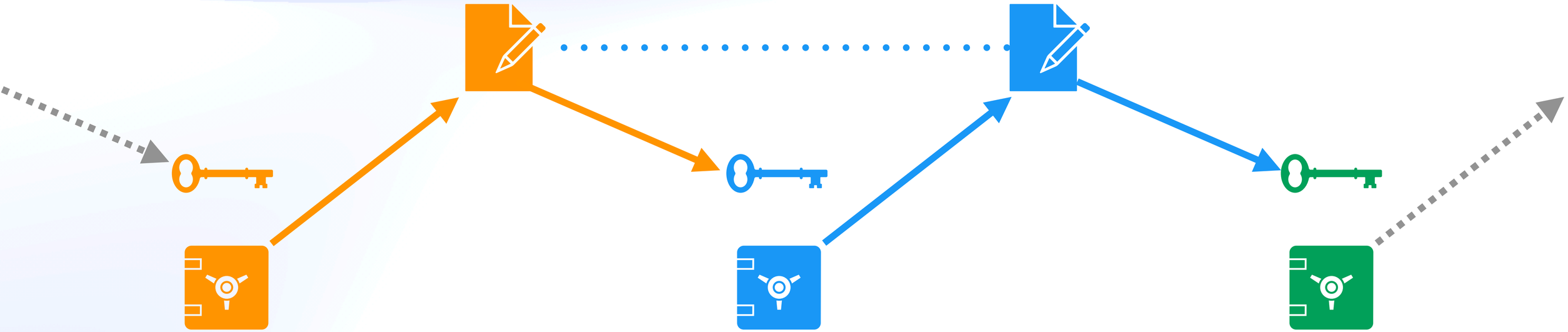
Yes, UCAN!

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

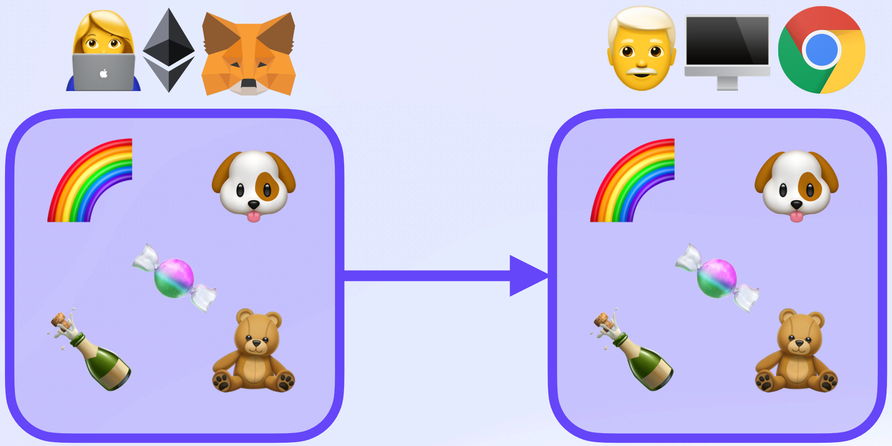
Permissionless

Composition & Flow

Permissionless

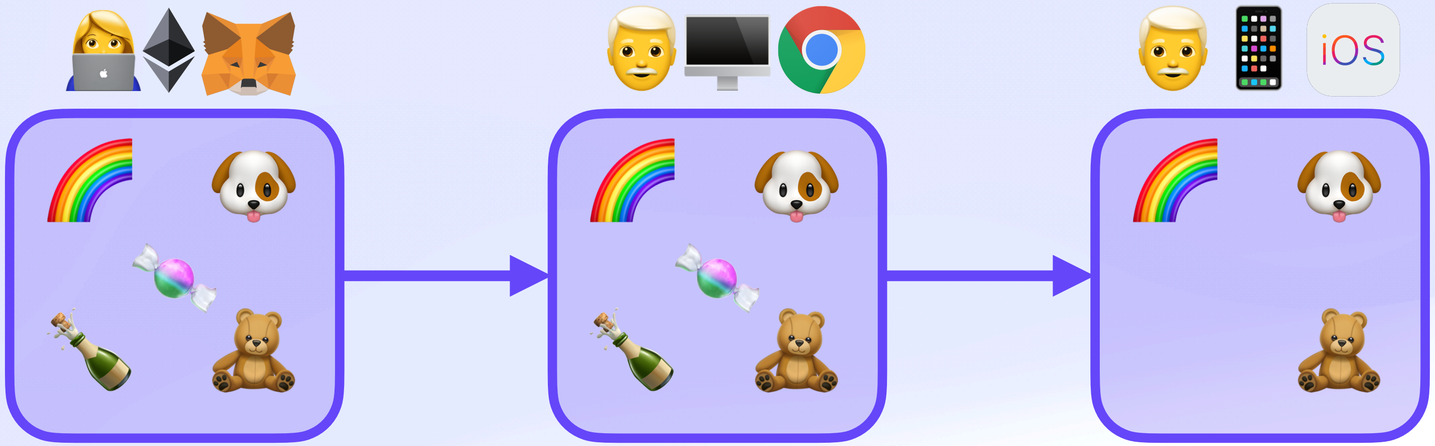
Composition & Flow

Permissionless



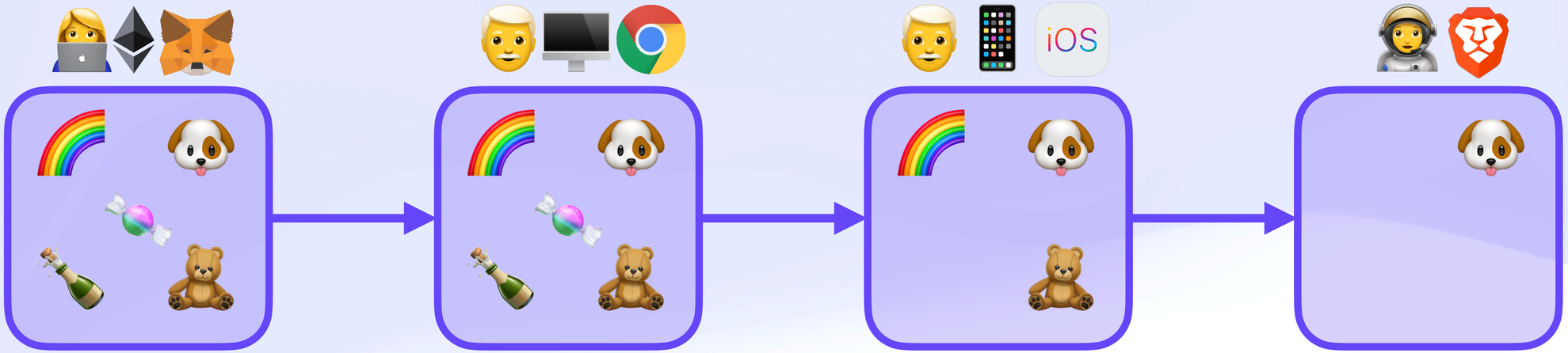
Composition & Flow

Permissionless



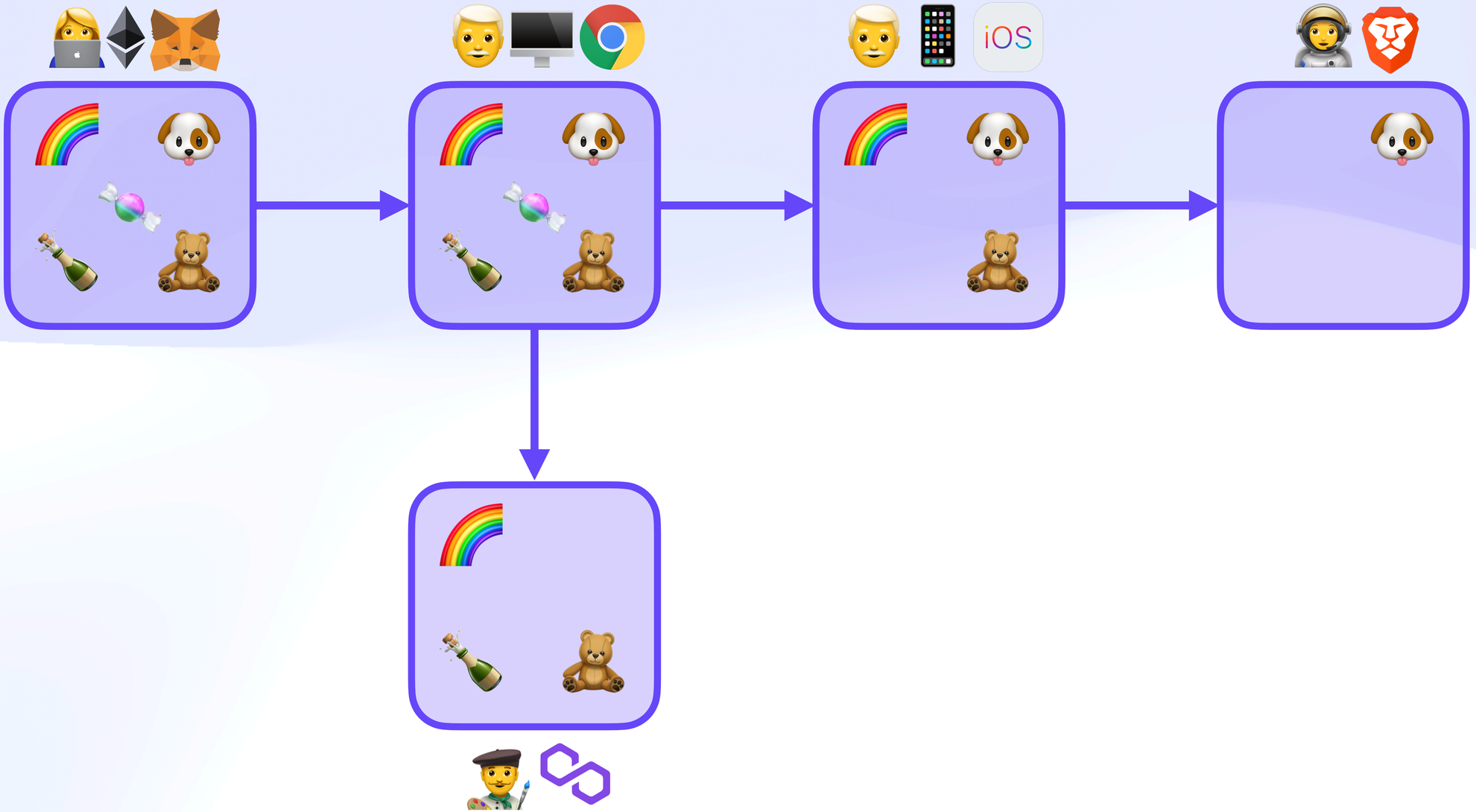
Composition & Flow

Permissionless



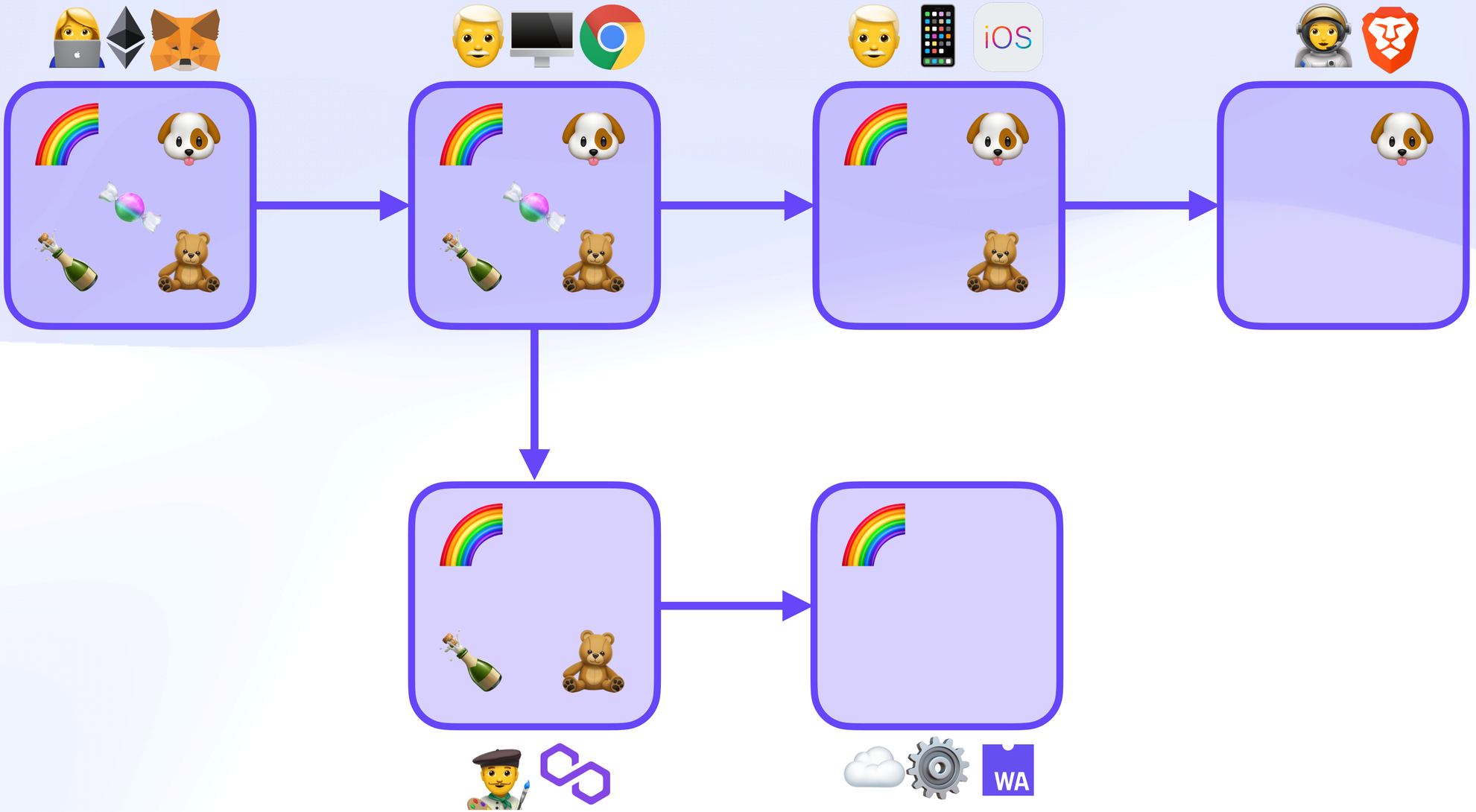
Composition & Flow

Permissionless



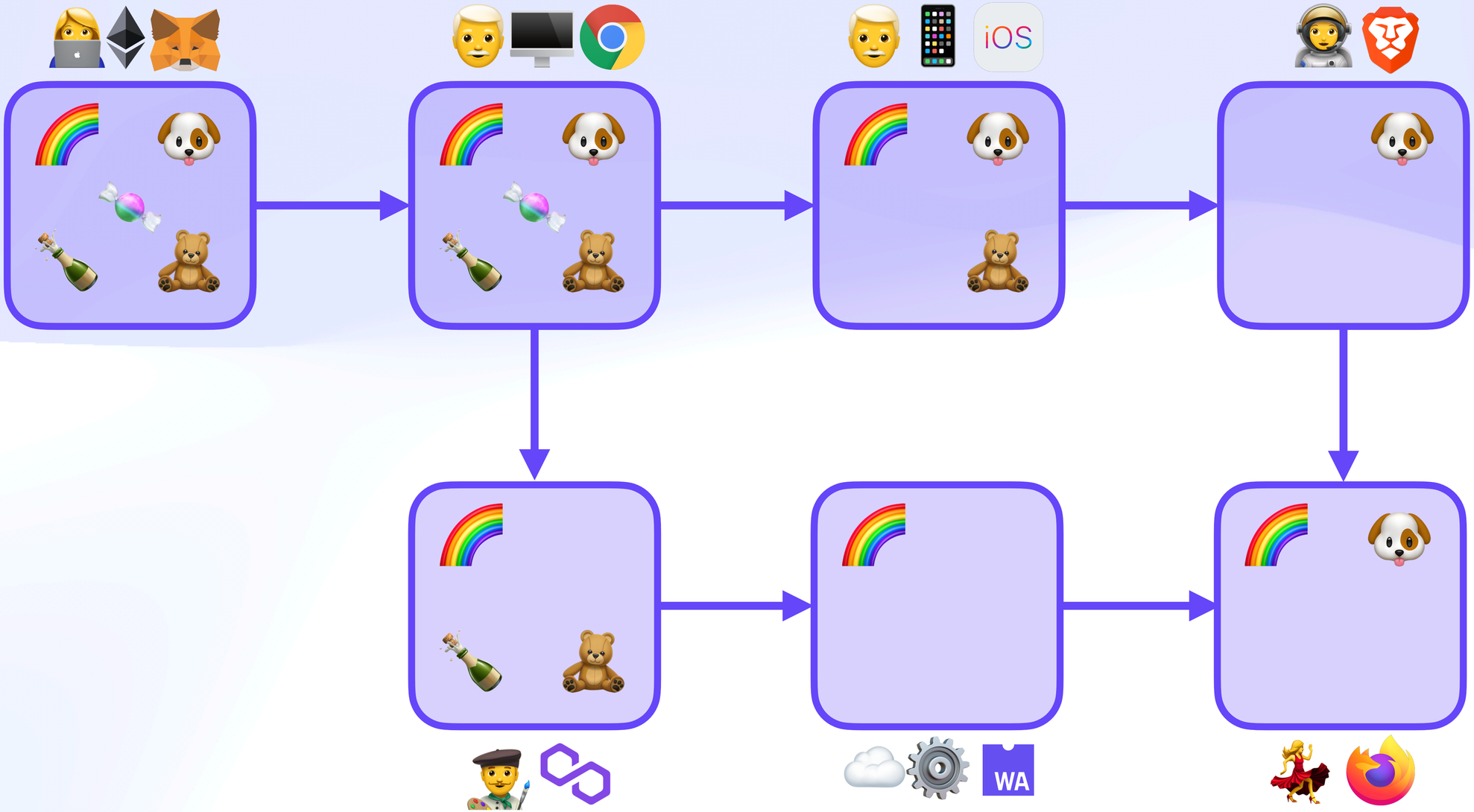
Composition & Flow

Permissionless



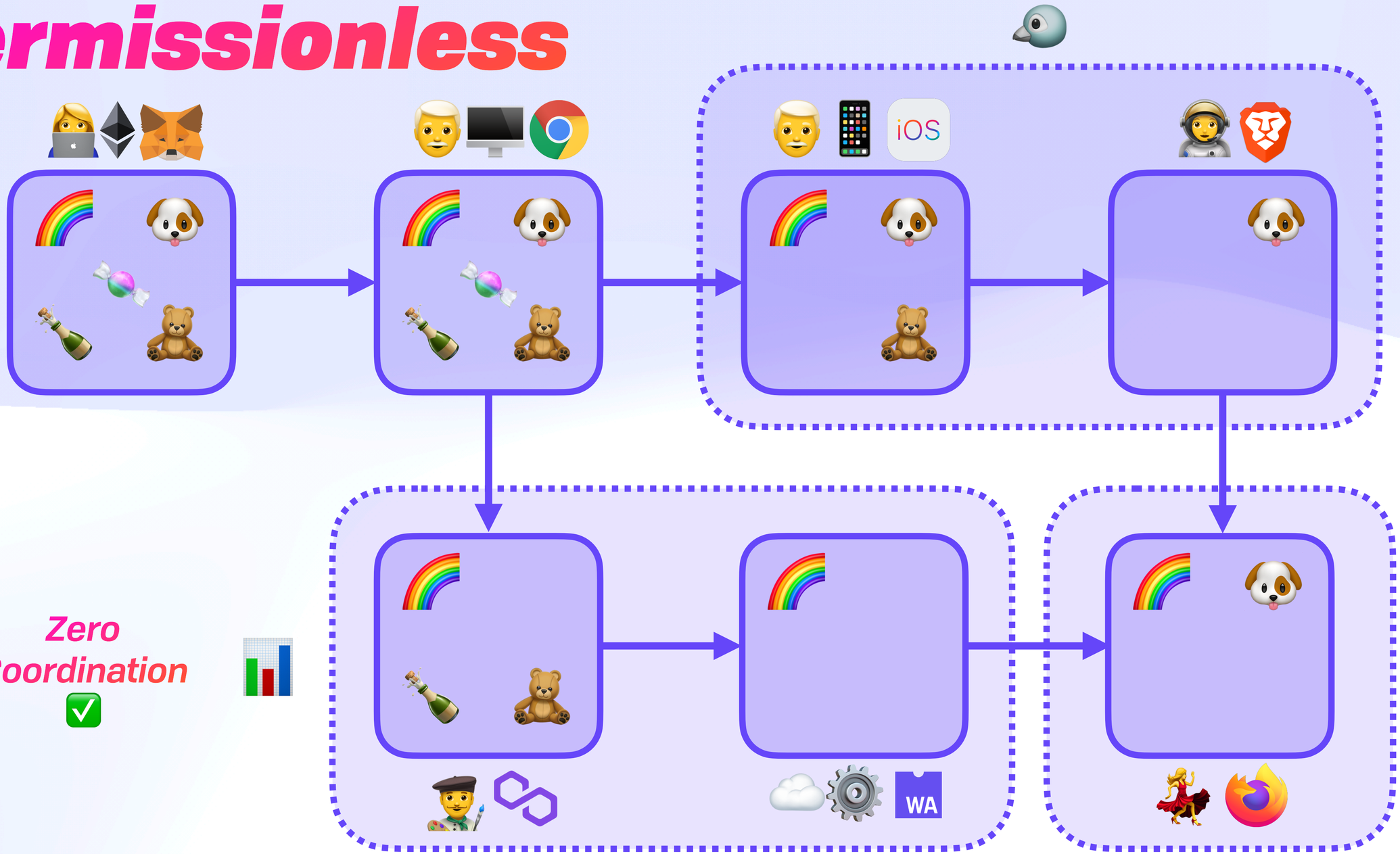
Composition & Flow

Permissionless



Composition & Flow

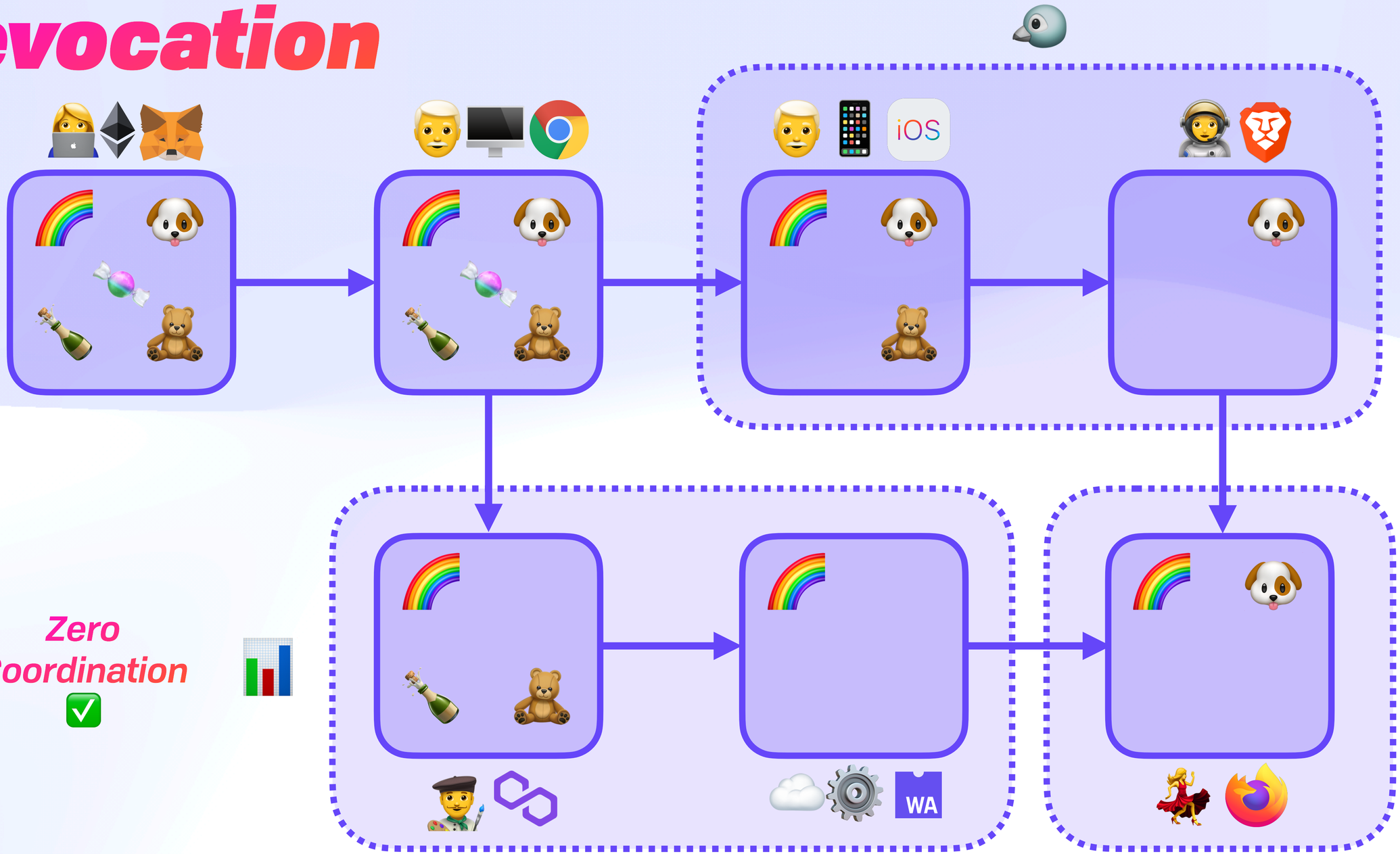
Permissionless



Zero Coordination

Composition & Flow

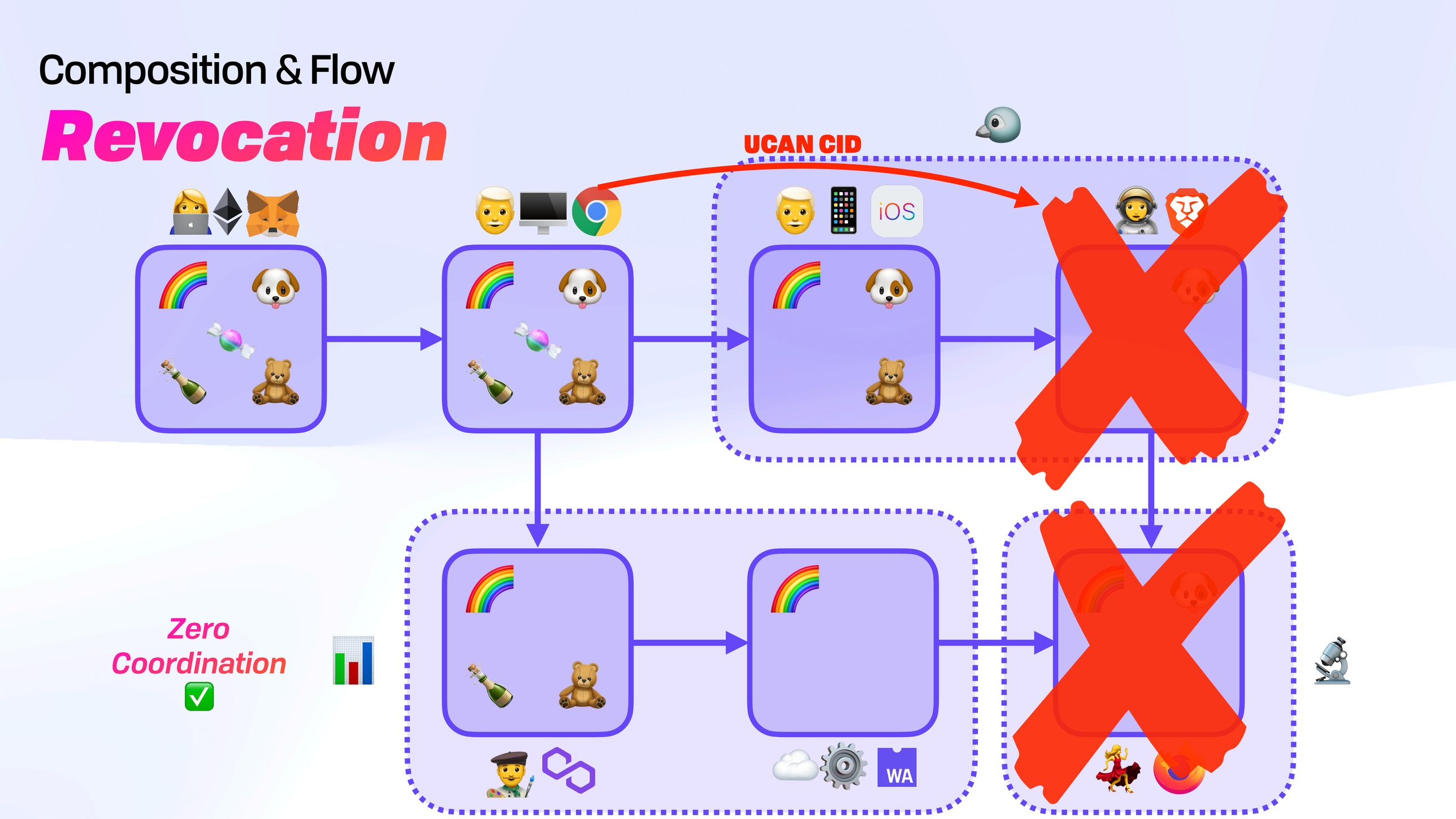
Revocation



Zero Coordination ✅

Composition & Flow

Revocation



Zero Coordination

Nice theory, how about a...

Nontrivial Example

Nontrivial Example

Encoded

Nontrivial Example

Encoded


```
eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V5Ono2T
Wt2WGZQVXY4Ynh0c1ZRaUdvN050azRxS0pOY2dLMml0NTJwYzczdGVVcFJMVCIsImF0dCI6W3sid25mcy
I6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNhcCI6Ik9WRVJXUklURSJ9LHs
id25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiY2FwIjoiT1ZFUldSSVRF
In1dLCJleHAiOjkyNTY5Mzk1MDUsImlzcyI6ImRpZDprZXk6ejZNa3NYUUJmTDhvd3p0VENKVG03aE5SZ
jZiMThZeFhQcDNpNjZvSkhtOEwzWUdKIiwibmJmIjoxNjM5NjA4MjkzLCJwcmYiOlsiZXlKaGJHY2lPaU
pGWkVSVFFTSXNJblI1Y0NJNklrcFhWQ0lzSW5WamRpSTZJakF1Tnk0d0luMC5leUpoZFdRaU9pSmthV1E
2YTJWNU9ubzJUV3R6V0ZGQ1prdzRiM2Q2ZEZSRFNsUnROMmhPVW1ZMllqRTRXWGhZVUhBemFUWTJiMHBJ
YlRoTU0xbEhTaUlzSW1GMGRDSTZXM3NpZDI1bWN5STZJbVJsYlc5MWMyVnlMbVpwYzNOcGIyNHVibUZ0W
lM5d2RXSnNhV012Y0dodmRHOXpMeUlzSW1OaGNDSTZJazlXUlZKWFVrbFVSU0o5WFN3aVpYaHdJam81TW
pVMk9UTTVOVEExTENKcGMzTWlPaUprYVdRNmEyVjVPbm8yVFd0d05VVnplamx6TWsxSWMzRlpka3h2WTJ
ONVNIZFlOVk5sZVZwTGNIRTNPVWQwTkRWbVJrZEZXbEk1T1NJc0ltNWlaaUk2TVRZek9UWXdPREk1TXl3
aWNISm1JanBiWFgwLjRUTmh1SFJyUEc5YUhvODY5SFhsc05LOF9GbWxTaFE1R3pHNGl0TjJOS2steUtUY
kFNb0Z3VHVwdEcwWEZnTkl2SHVsUHBsVnpaWURWRGV4bzc2a0F3IiwiZXlKaGJHY2lPaUpGWkVSVFFTSX
NJblI1Y0NJNklrcFhWQ0lzSW5WamRpSTZJakF1Tnk0d0luMC5leUpoZFdRaU9pSmthV1E2YTJWNU9ubzJ
UV3R6V0ZGQ1prdzRiM2Q2ZEZSRFNsUnROMmhPVW1ZMllqRTRXWGhZVUhBemFUWTJiMHBJYlRoTU0xbEhT
aUlzSW1GMGRDSTZXM3NpZDI1bWN5STZJbVJsYlc5MWMyVnlMbVpwYzNOcGIyNHVibUZ0WlM5d2RXSnNhV
012Ym05MFpYTXZJaXdpWTJGd0lqb2lUMVpGVWxkU1NWUkZJbjFkTENKbGVIQWlPamt5TlRZNU16azFNRF
VzSW1semN5STZJbVJwWkRwclpYazZlalpOYTNBMVJYTjZPWE15VFVoemNWbDJURzlqWTNsSWQxZzFVMlY
1V2t0d2NUYzVSM1EwTldaR1IwVmFVams1SWl3aWJtSm1Jam94TmpNNU5qQTRNamt6TENKd2NtWWlPbHRk
ZlEuTWdZYXJMcXk3Um1RMUFJcnFZTDZjRnk5ejdhNVdJQVUtLVRZQVJQU2dpck9Tc3p2YXIzX0ROcjI1c
mJQcmV0SGJuVDBtTVZLeW9hUVhydVI3S2JyQmciXX0.kwRdqPN74pkcpXGgdk7Z7FW3M1mRRYaDE5ZgkG
6srAuu6V6mvMVRdBLnD5CWid-X4tDIKpliVjlCSLTntB4pCw
```

Nontrivial Example

Decoded

Header

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

Payload

```
{
  "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": [
"eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a
2V5Ono2TWtzWFFCZkw4b3d6dFRDSlRtN2hOUmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNhc
CI6Ik9WRVJXUklURSJ9XSwiZXhwIjo5MjU2OTM5NTA1LCJpc3MiOiJkaWQ6a2V5Ono2TWtwNUV
zejlzMk1Ic3FZdkxvY2N5SHdYNVNleVpLcHE3OUd0NDVmRkdFWlI5OSIsIm5iZiI6MTYzOTYwO
DI5MywicHJmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_FmlShQ5GzG4itN2NKk-
yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDexo76kAw",

"eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a
2V5Ono2TWtzWFFCZkw4b3d6dFRDSlRtN2hOUmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiY2FwI
joiT1ZFUldSSVRFIn1dLCJleHAiOjkyNTY5Mzk1MDUsImlzcyI6ImRpZDprZXk6ejZNa3A1RXN
6OXMyTUhzcVl2TG9jY3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjoxNjM5NjA4M
jkzLCJwcmYiOltdfQ.MgYarLqy7RmQ1AIrqYL6cFy9z7a5WIAU--
TYARPSgirOSszvar3_DNr25rbPretHbnT0mMVKyoaQXruR7KbrBg"
  ]
}
```

Signature

```
kwRdqPN74pkcpXGgdk7Z7FW3M1mRR
YaDE5ZgkG6srAuu6V6mvMVRdBLnD5
CWid-X4tDIKpliVjlCSLTntB4pCw
```

Nontrivial Example

Decoded

Header

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

Payload

```
{
  "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": [
"eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a
2V5Ono2TWtzWFFCZkw4b3d6dFRDSlRtN2hOUmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNhc
CI6Ik9WRVJXUklURSJ9XSwiZXhwIjo5MjU2OTM5NTA1LCJpc3MiOiJkaWQ6a2V5Ono2TWtwNUV
zejlzMk1Ic3FZdkxvY2N5SHdYNVNleVpLcHE3OUd0NDVmRkdFWlI5OSIsIm5iZiI6MTYzOTYwO
DI5MywicHJmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_FmlShQ5GzG4itN2NKk-
yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDexo76kAw",
"eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a
2V5Ono2TWtzWFFCZkw4b3d6dFRDSlRtN2hOUmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiY2FwI
joiT1ZFUldSSVRFIn1dLCJleHAiOjkyNTY5Mzk1MDUsImlzcyI6ImRpZDprZXk6ejZNa3A1RXN
6OXMyTUhzcVl2TG9jY3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjoxNjM5NjA4M
jkzLCJwcmYiOltdfQ.MgYarLqy7RmQ1AIrqYL6cFy9z7a5WIAU--
TYARPSgirOSszvar3_DNr25rbPretHbnT0mMVKyoaQXruR7KbrBg"
  ]
}
```

Signature

```
kwRdqPN74pkcpXGgdk7Z7FW3M1mRR
YaDE5ZgkG6srAuu6V6mvMVRdBLnD5
CWid-X4tDIKpliVjlCSLTntB4pCw
```

Nontrivial Example

Decoded Witness

Header

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

Payload

```
{
  "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

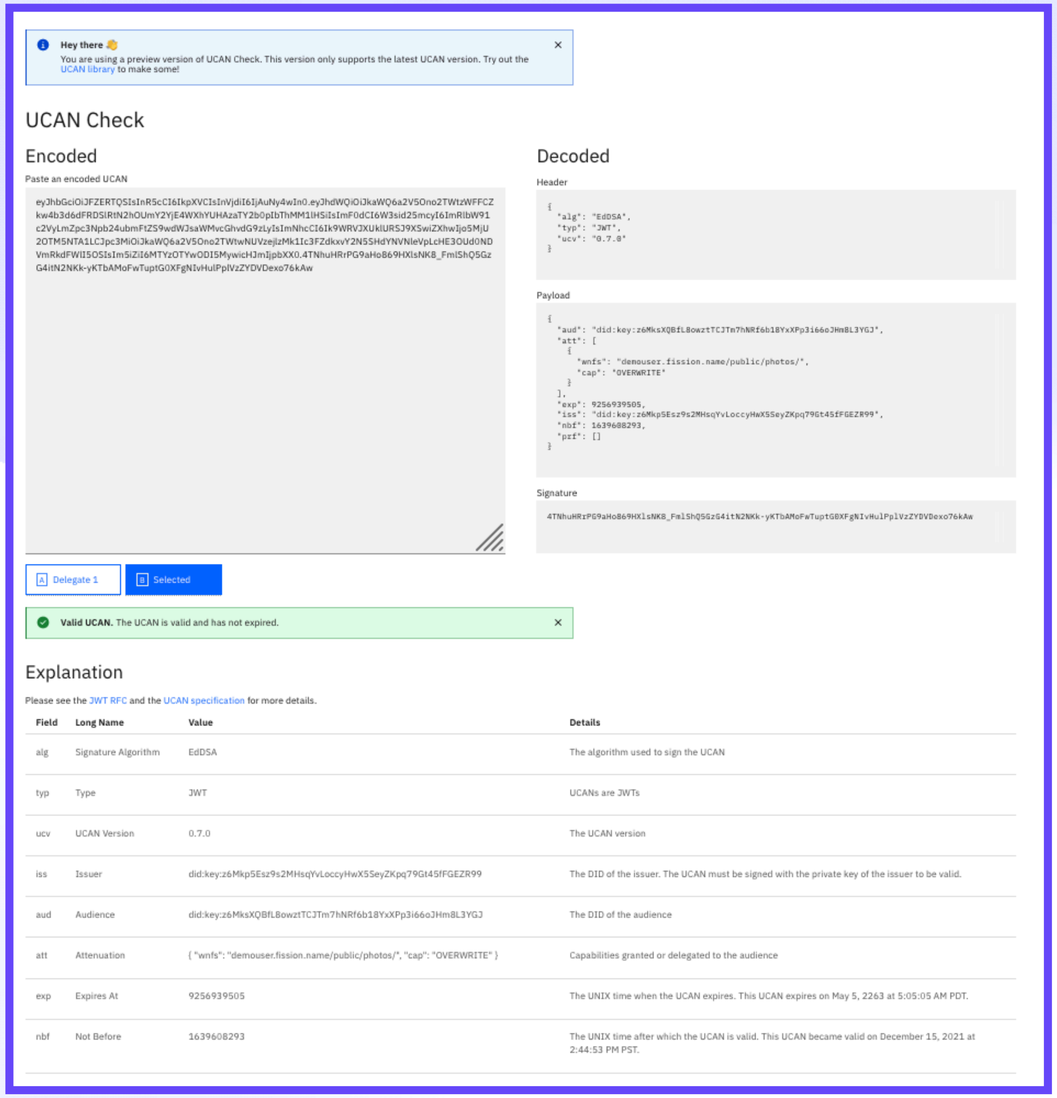
```
4TNhuHRrPG9aHo869HXlsNK8_FmlShQ5GzG
4itN2NKk-
yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDe
xo76kAw
```

Nontrivial Example

ucan.xyz — Online Explorer / Validator

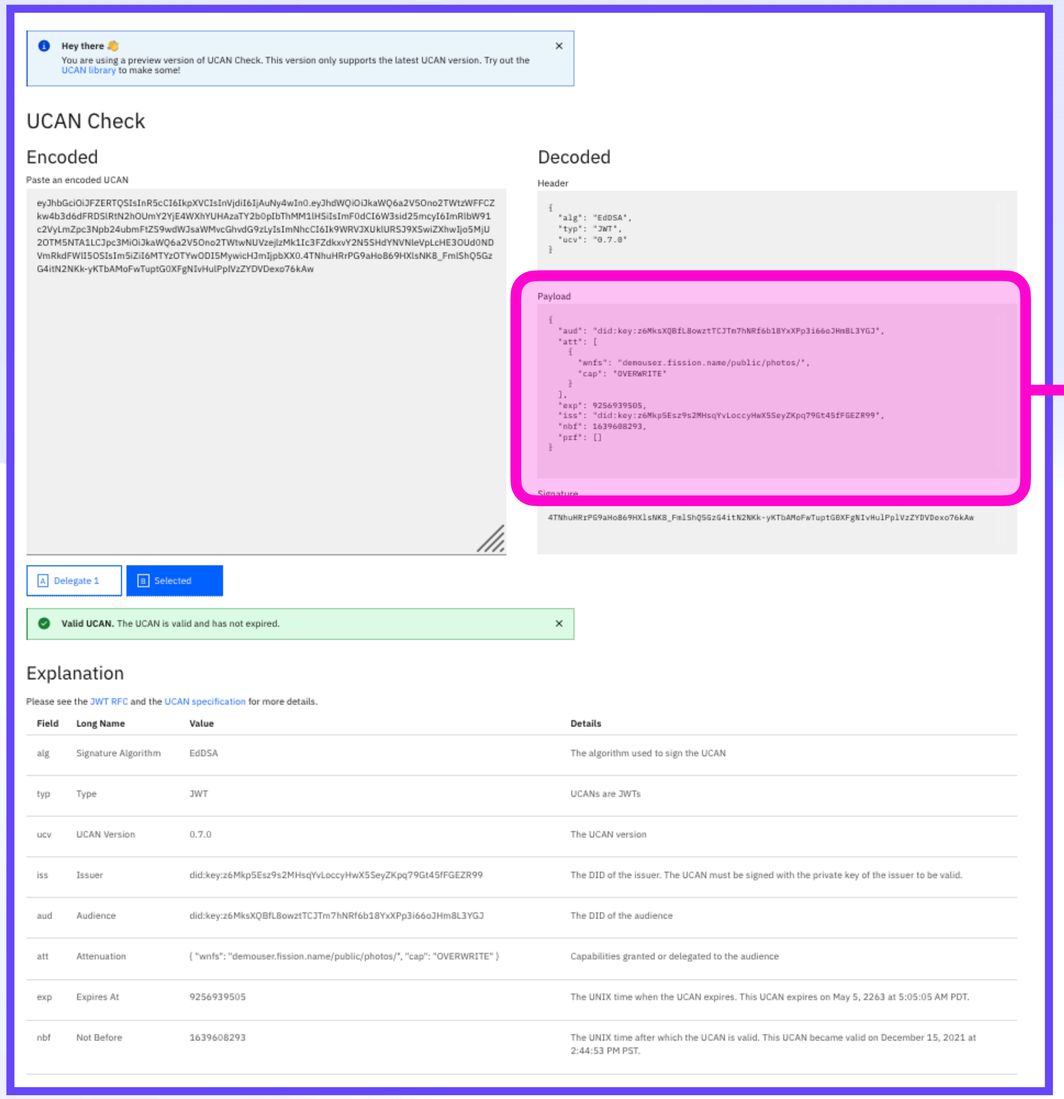
Nontrivial Example

ucan.xyz — Online Explorer / Validator



Nontrivial Example

ucan.xyz — Online Explorer / Validator

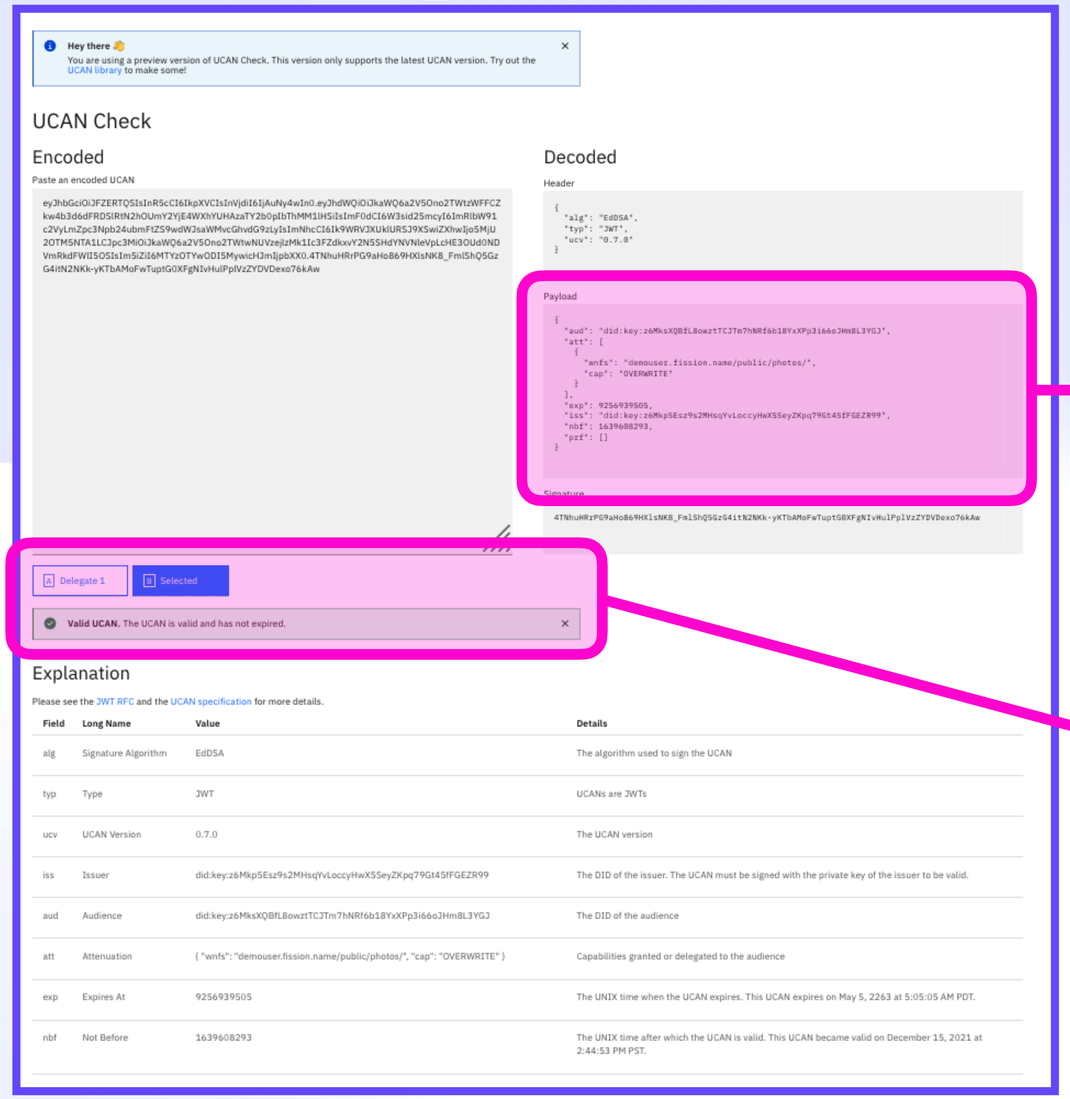


Payload


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

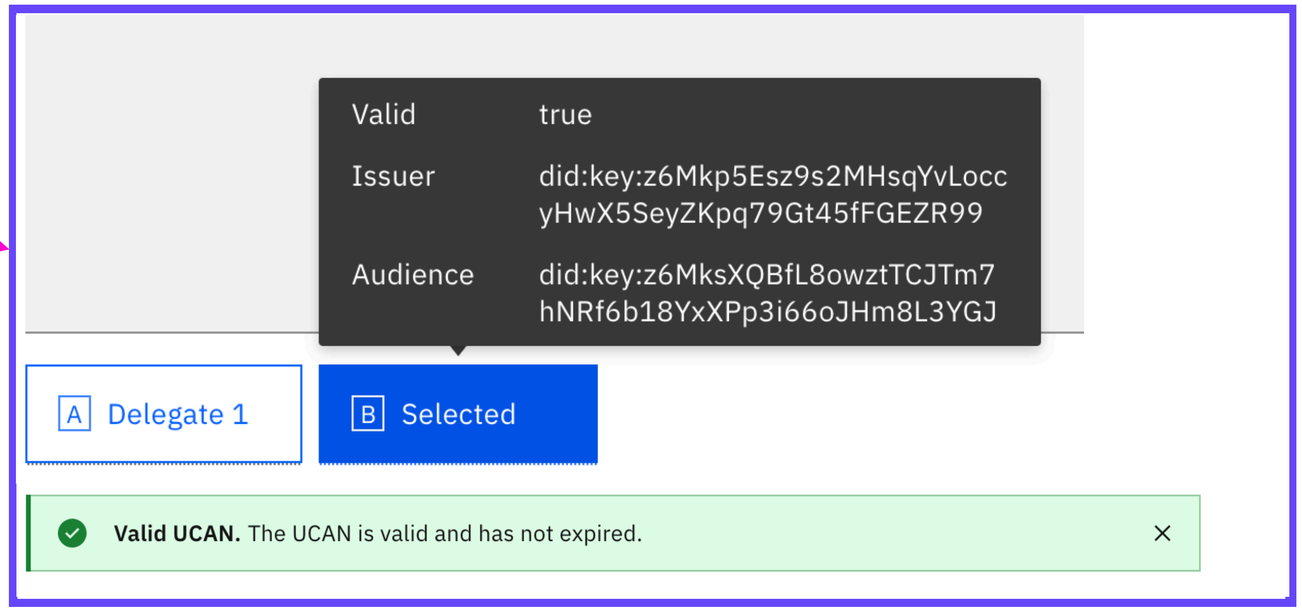
Nontrivial Example

ucan.xyz — Online Explorer / Validator



Payload

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

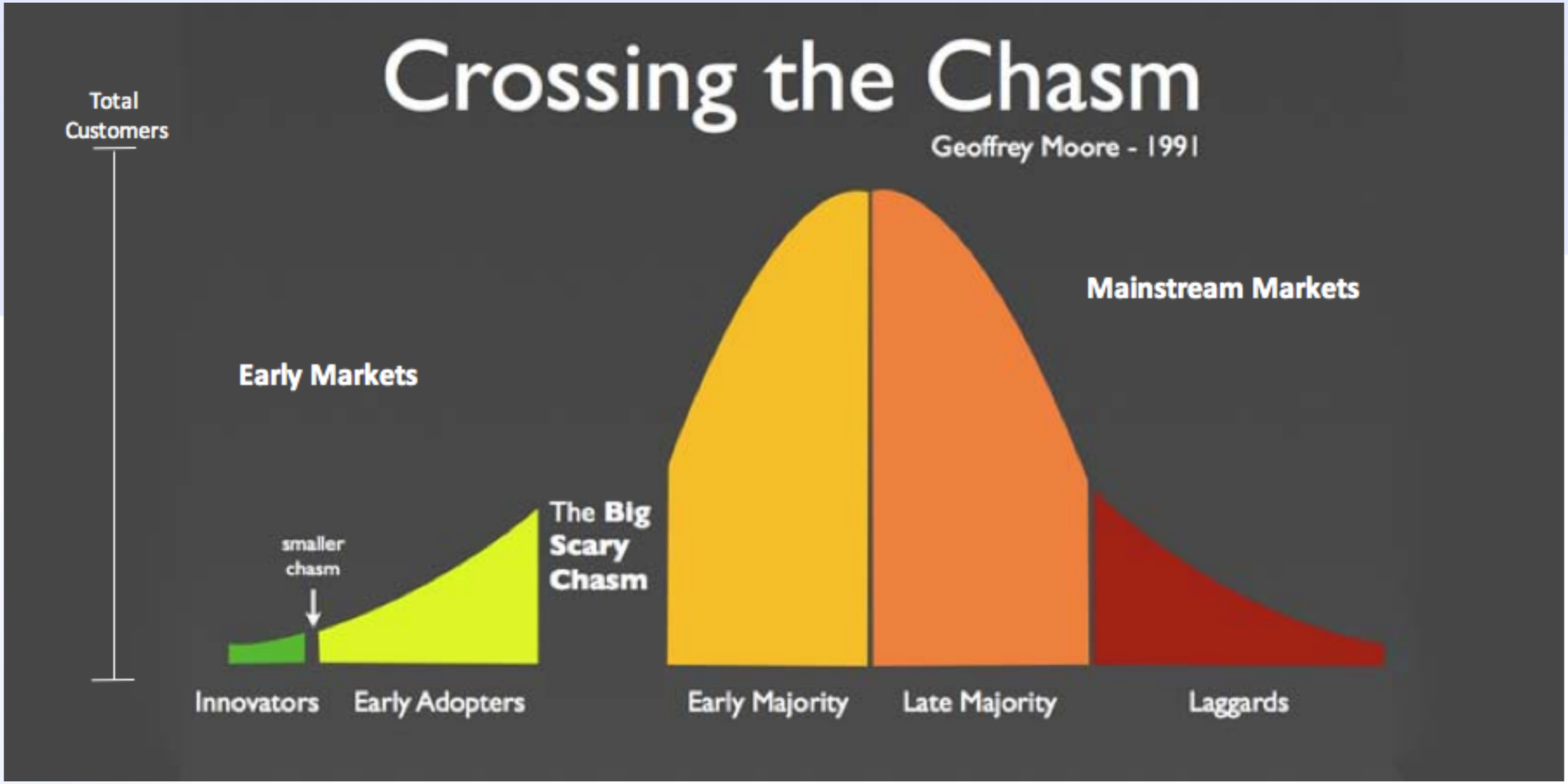


Further Reading

Adoption

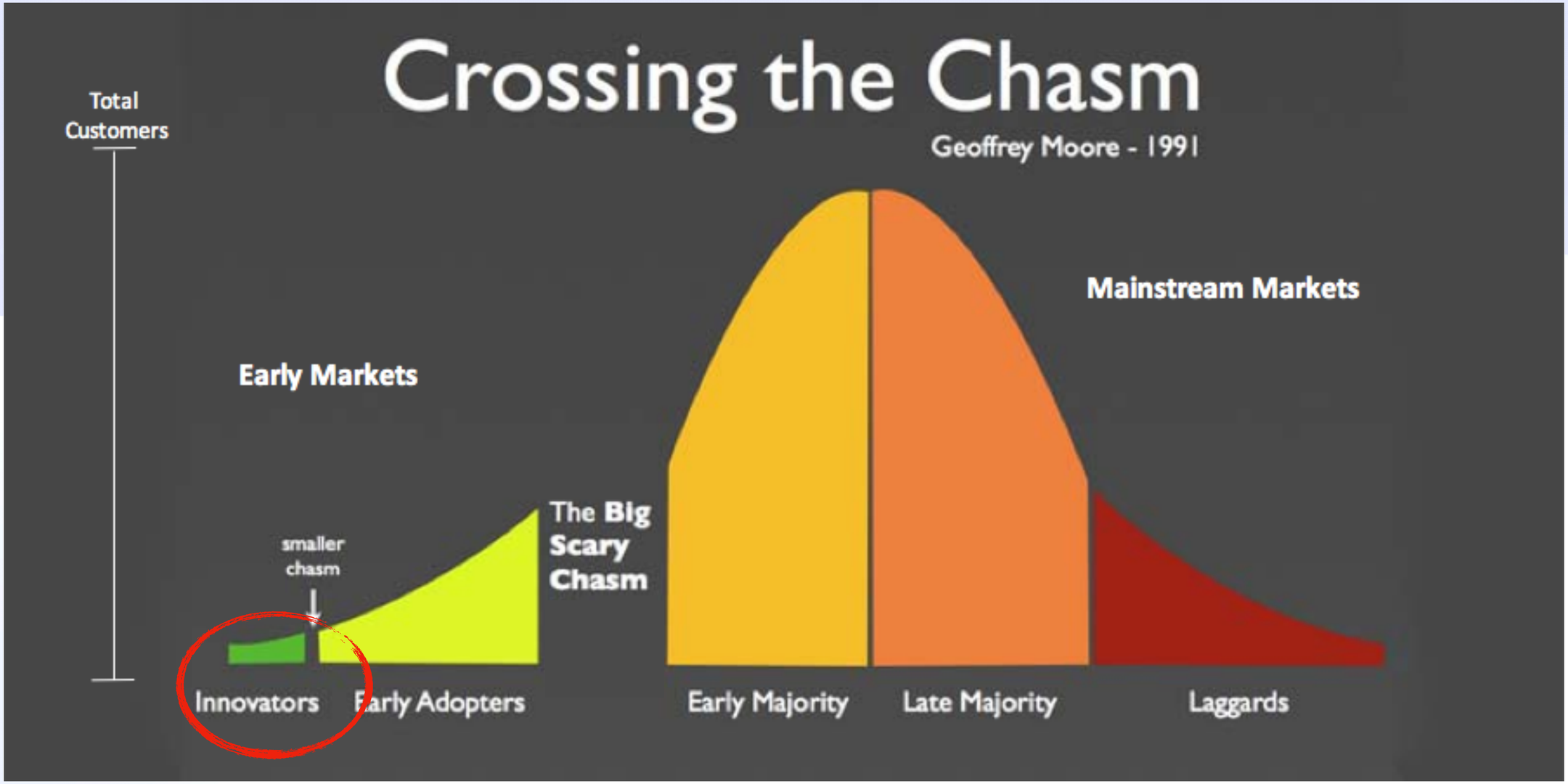
How to Power a New Internet ⚡

Still Extremely Early Days for Web3!



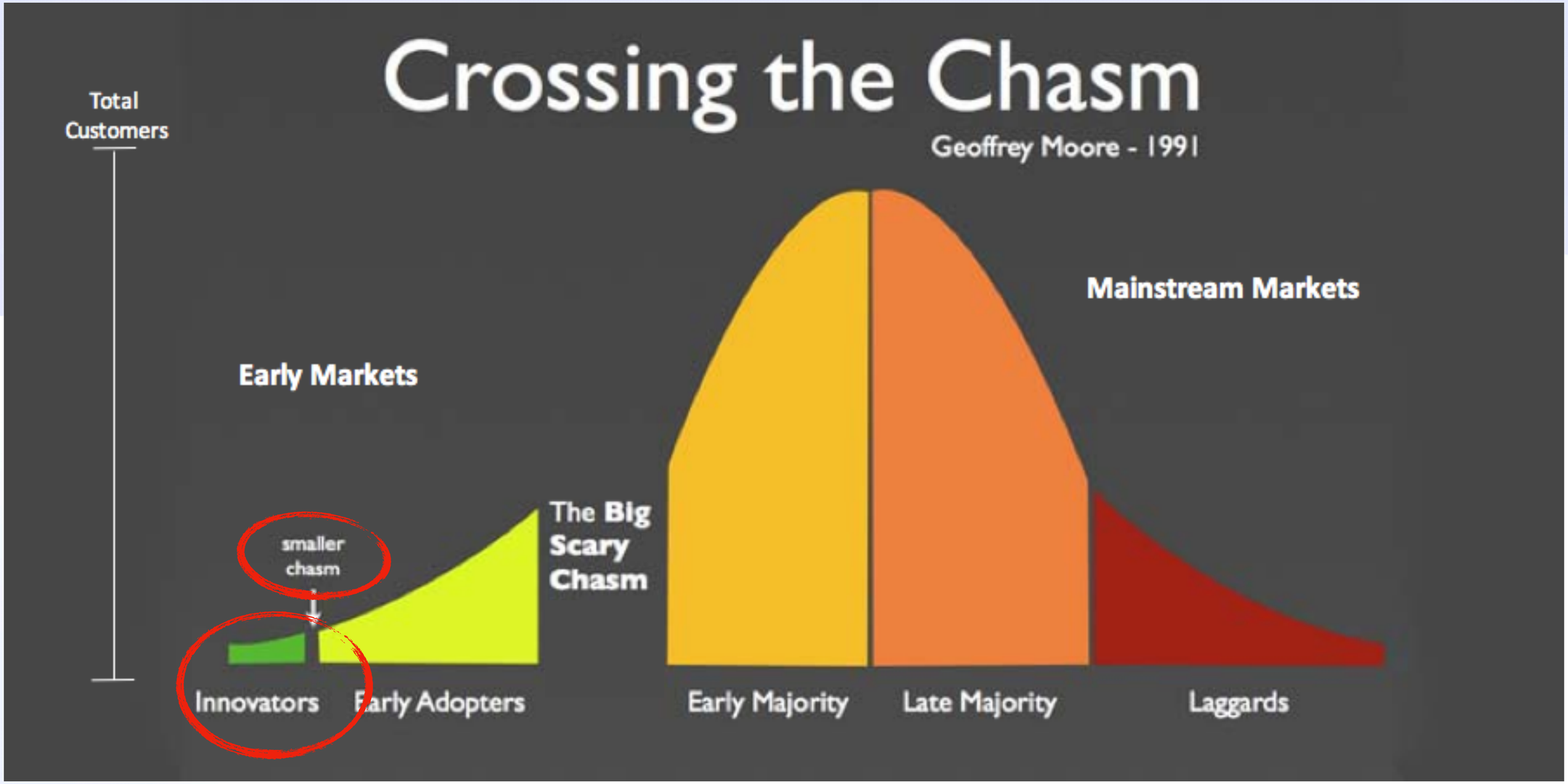
How to Power a New Internet ⚡

Still Extremely Early Days for Web3!



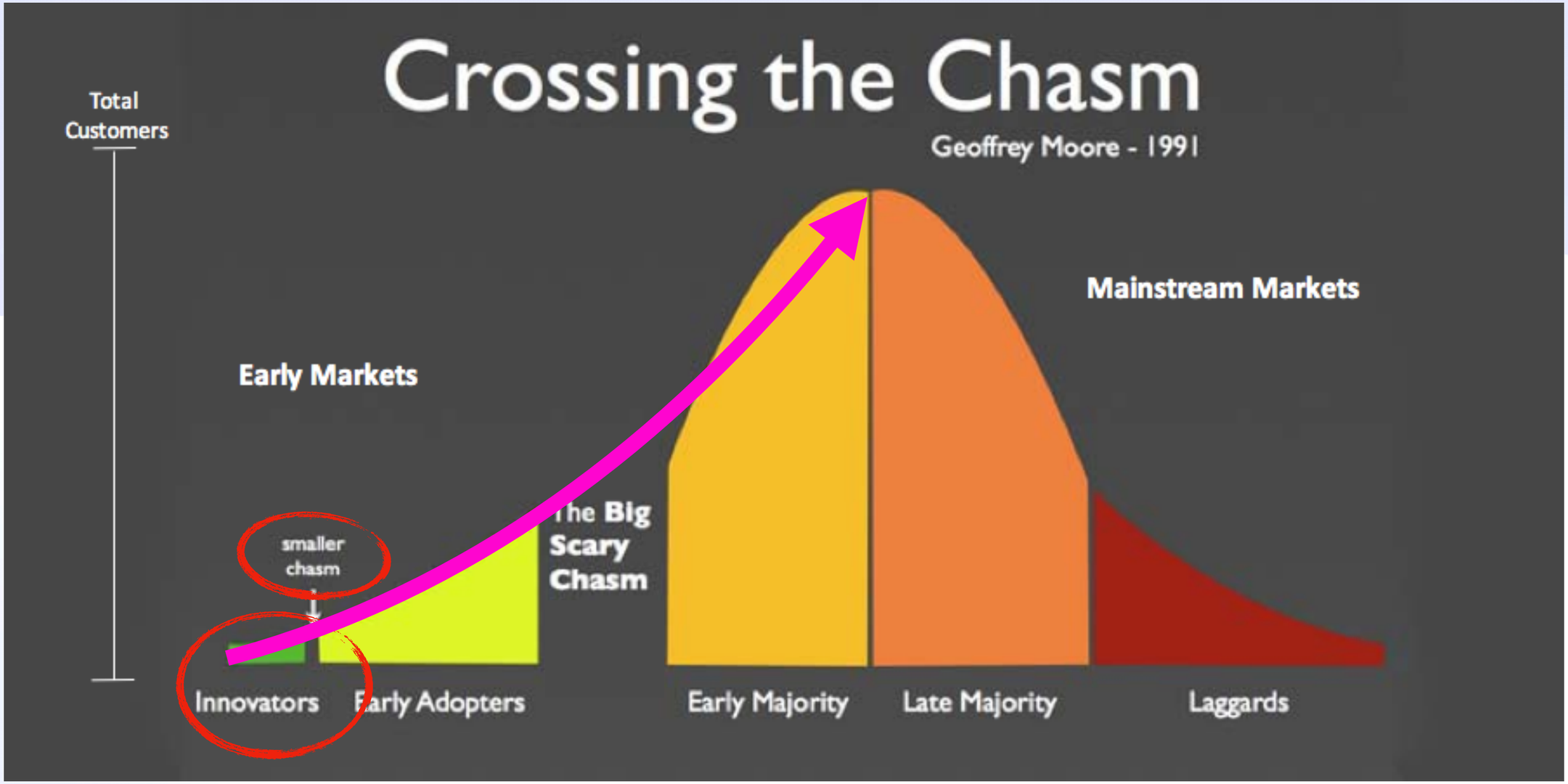
How to Power a New Internet ⚡

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 ⚡

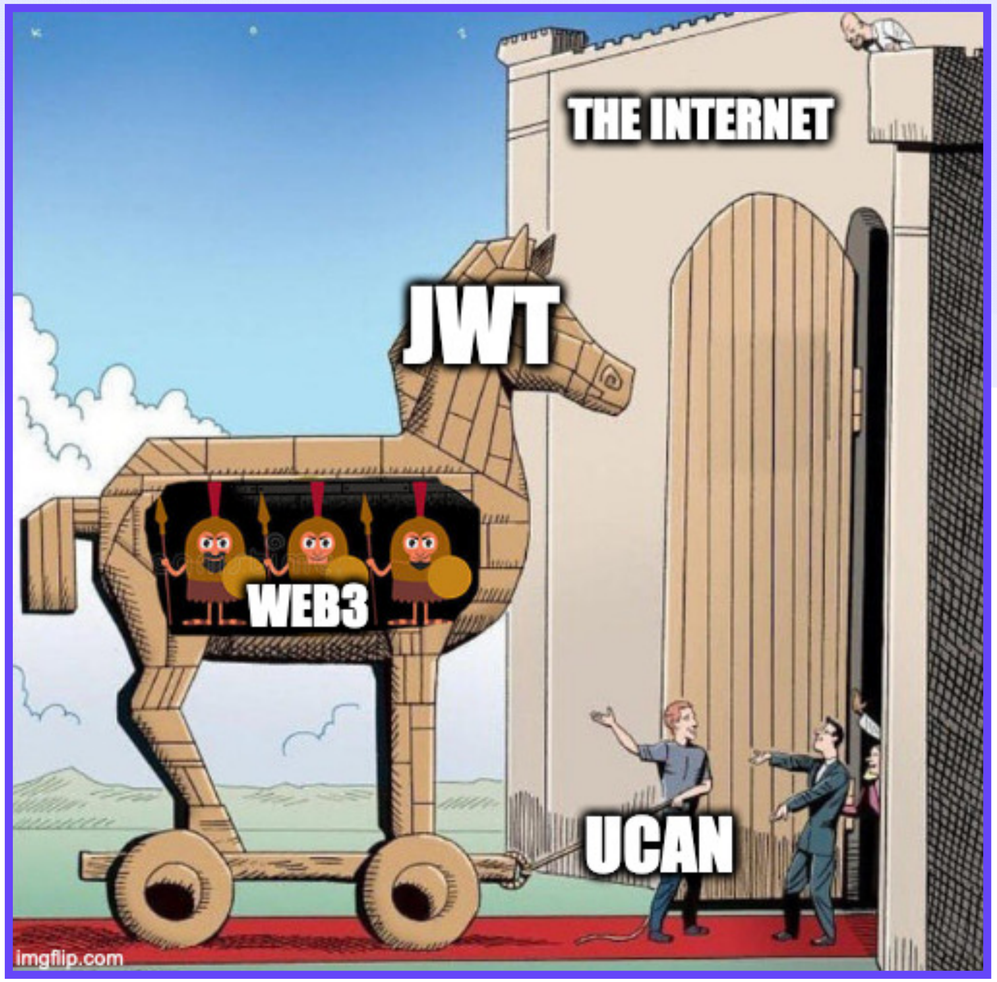
Adoption

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

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

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