UCAN Decentralize Auth

🚀 Authorise Everything, Everywhere, All At Once ✊

github.com/ucan-wg

UCAN Decentralize Auth

UCAN Decentralize Auth

When speaking of computation,
all too much emphasis is often placed on
the [services] themselves. ***The fabric of a system is the dynamic reference graph.***

Mark Miller, An Ode to the Granovetter Diagram

UCAN Decentralize Auth

Brooklyn Zelenka @expede

github.com/expede

UCAN Decentralize Auth

Brooklyn Zelenka @expede

- Cofounder & CTO at Fission
  - discord.gg/fissioncodes
  - @fission@plnetwork.xyz
- Might know a thing or two about UCAN
  - github.com/ucan-wg
- PLT and distributed systems are my jam

github.com/expede

UCAN Decentralize Auth

Everywhere

UCAN Decentralize Auth

Everywhere

Commons

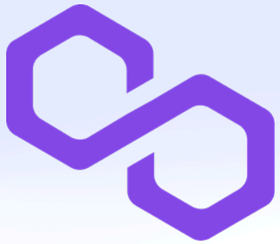
Cloud & Edge

Far Edge

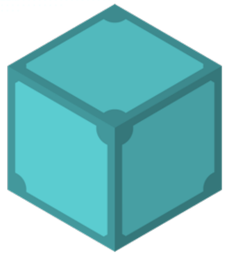
UCAN Decentralize Auth

Everywhere

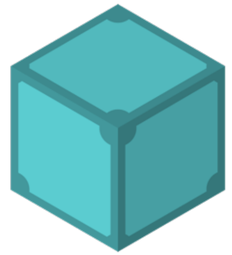
Commons



Far Edge



Cloud & Edge



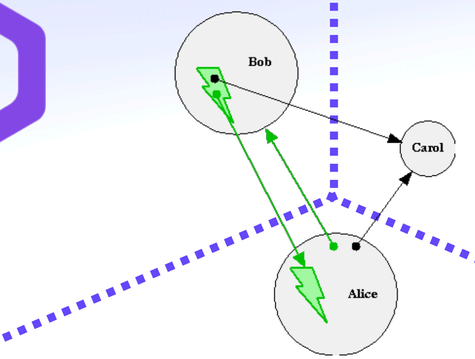
UCAN Decentralize Auth

Everywhere

Commons

Far Edge

Cloud & Edge

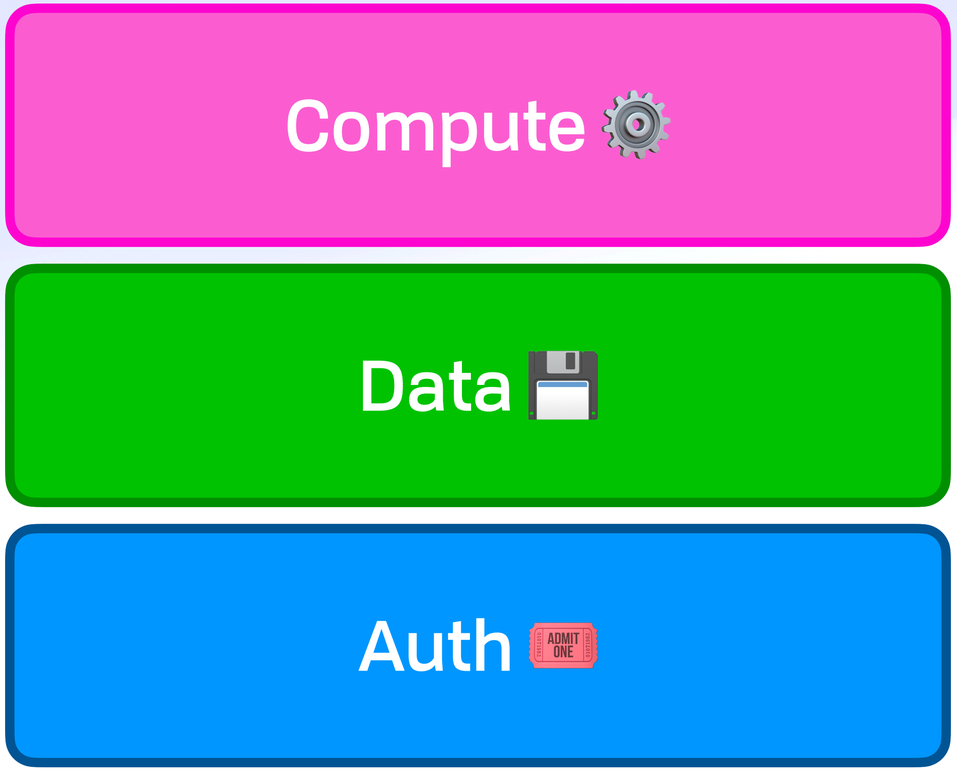


UCAN Decentralize Auth

Open Protocols Everywhere

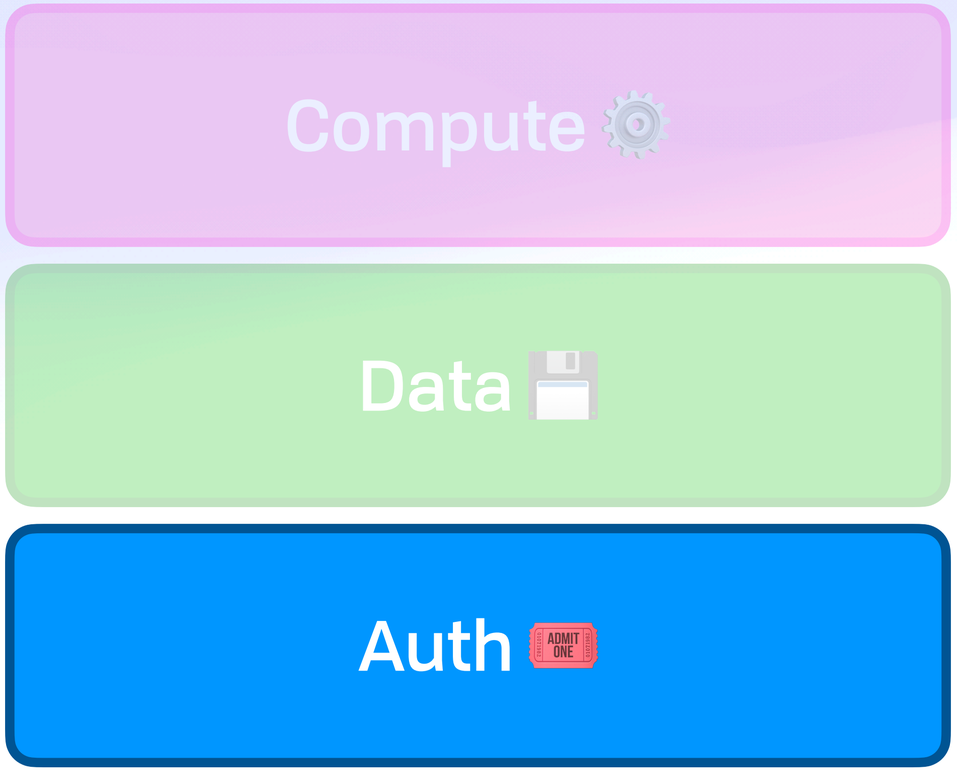
UCAN Decentralize Auth

Open Protocols Everywhere



UCAN Decentralize Auth

Open Protocols Everywhere

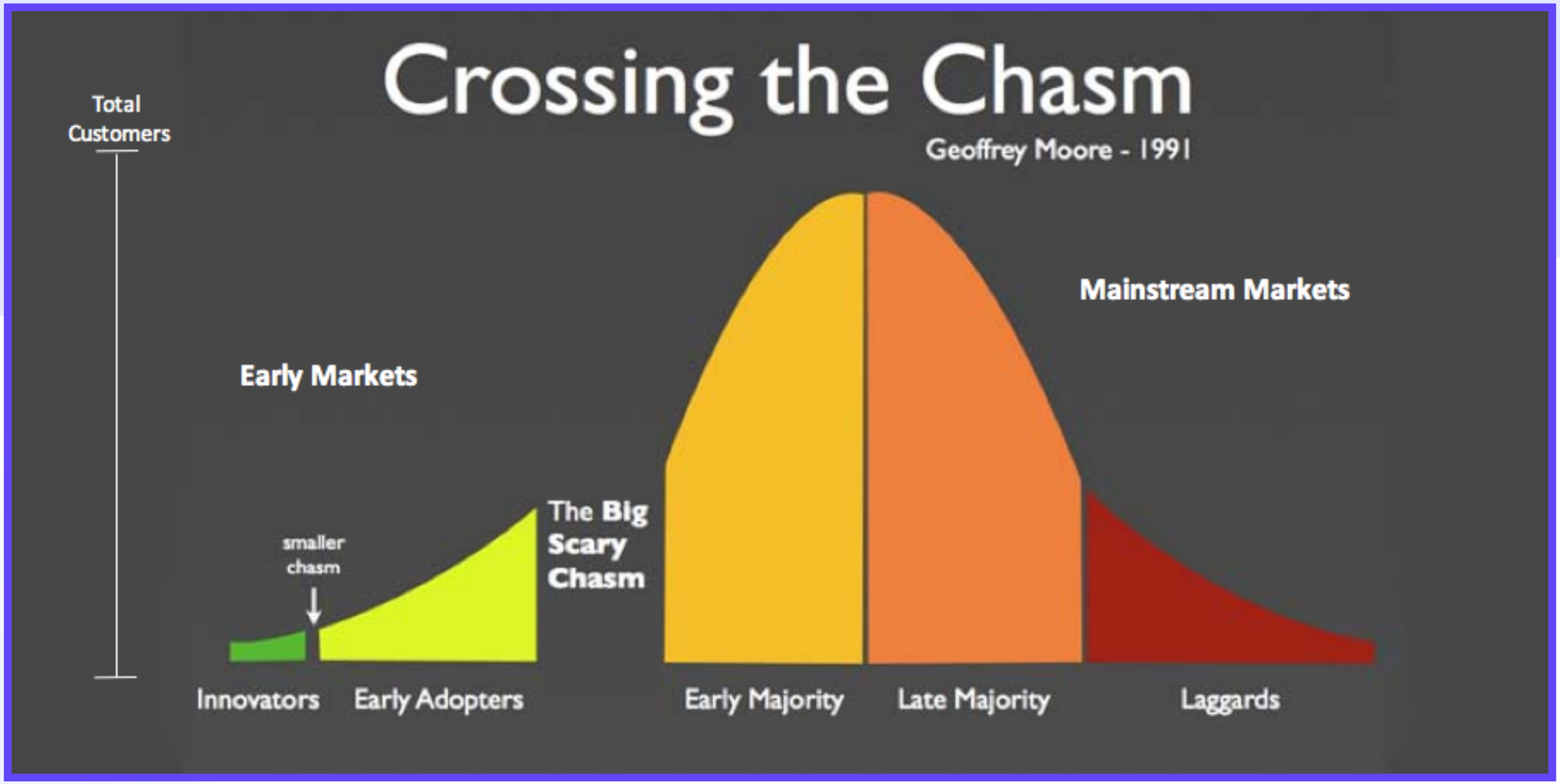


UCAN Decentralize Auth

How to Power a New Internet

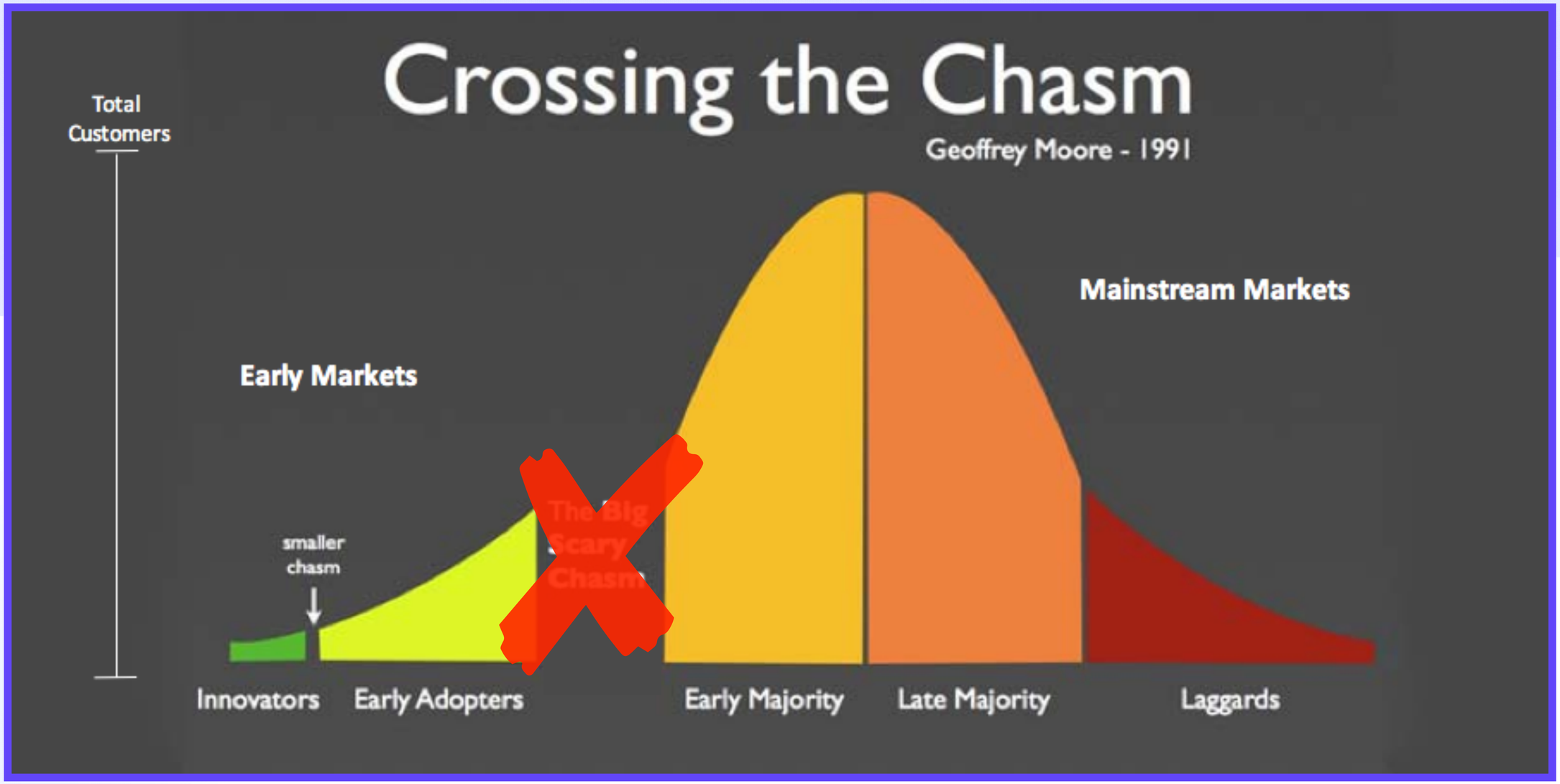
How to Power a New Internet 🔌

Adoption & Audience



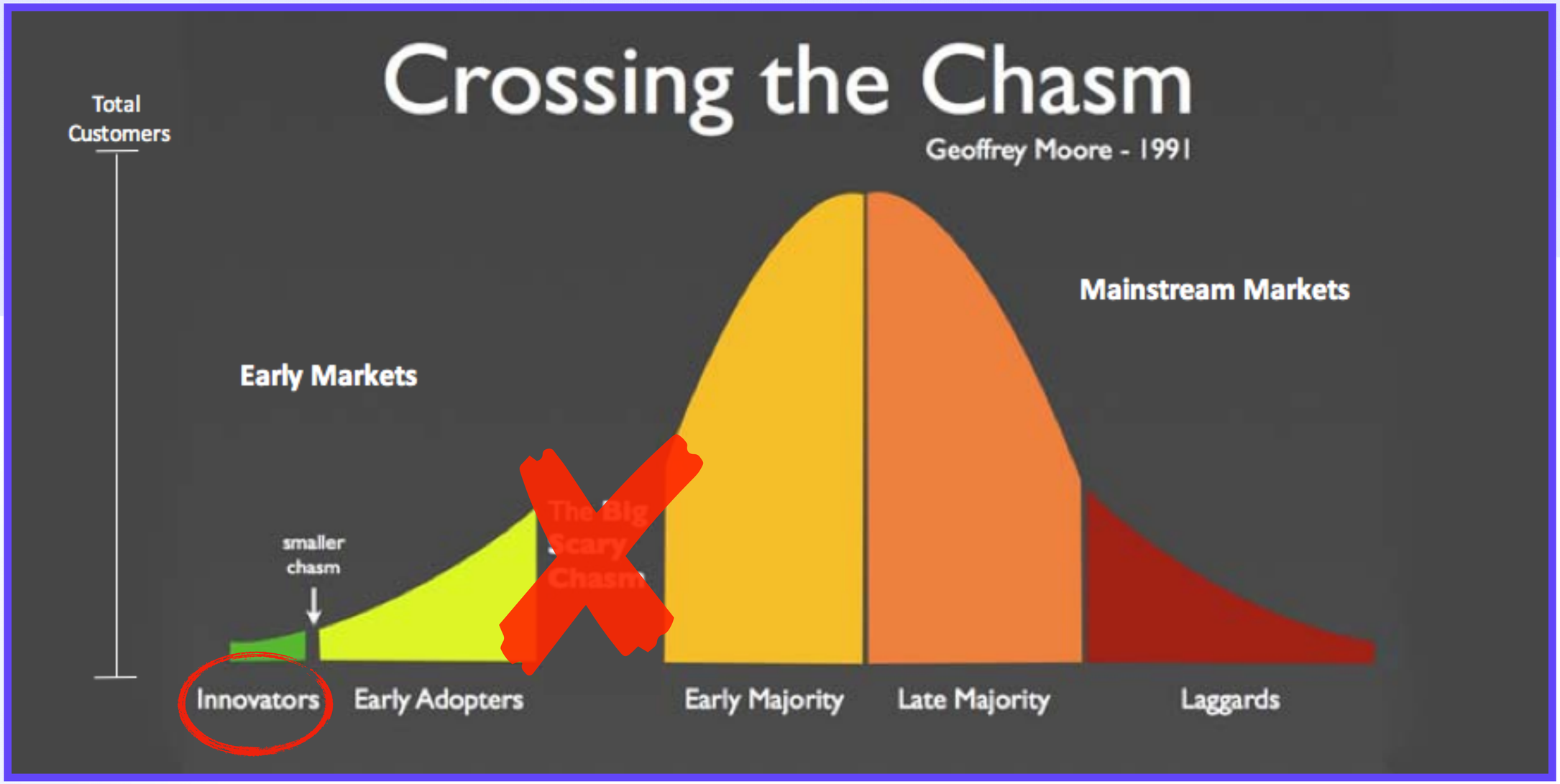
How to Power a New Internet 🔌

Adoption & Audience



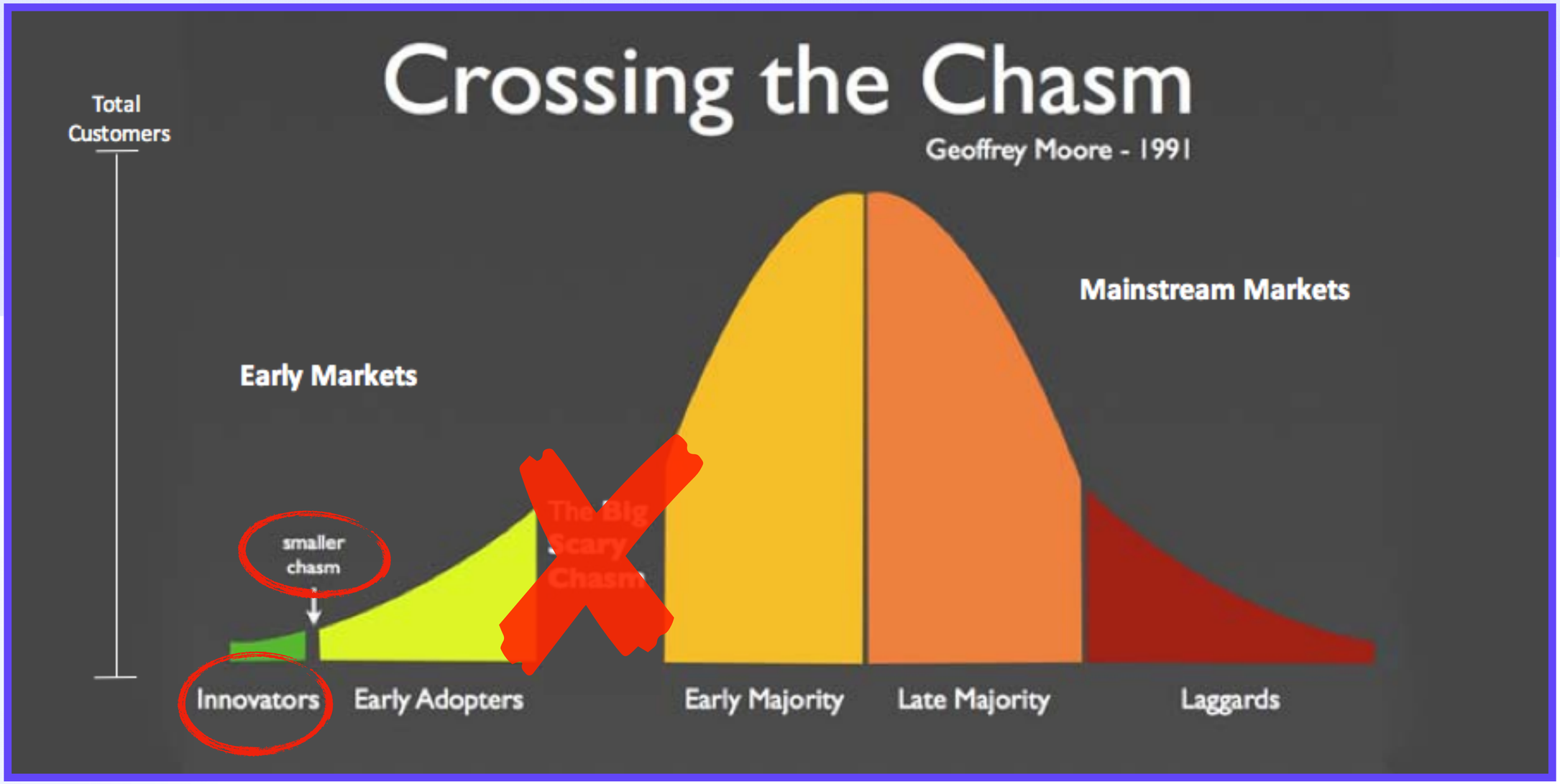
How to Power a New Internet 🔌

Adoption & Audience



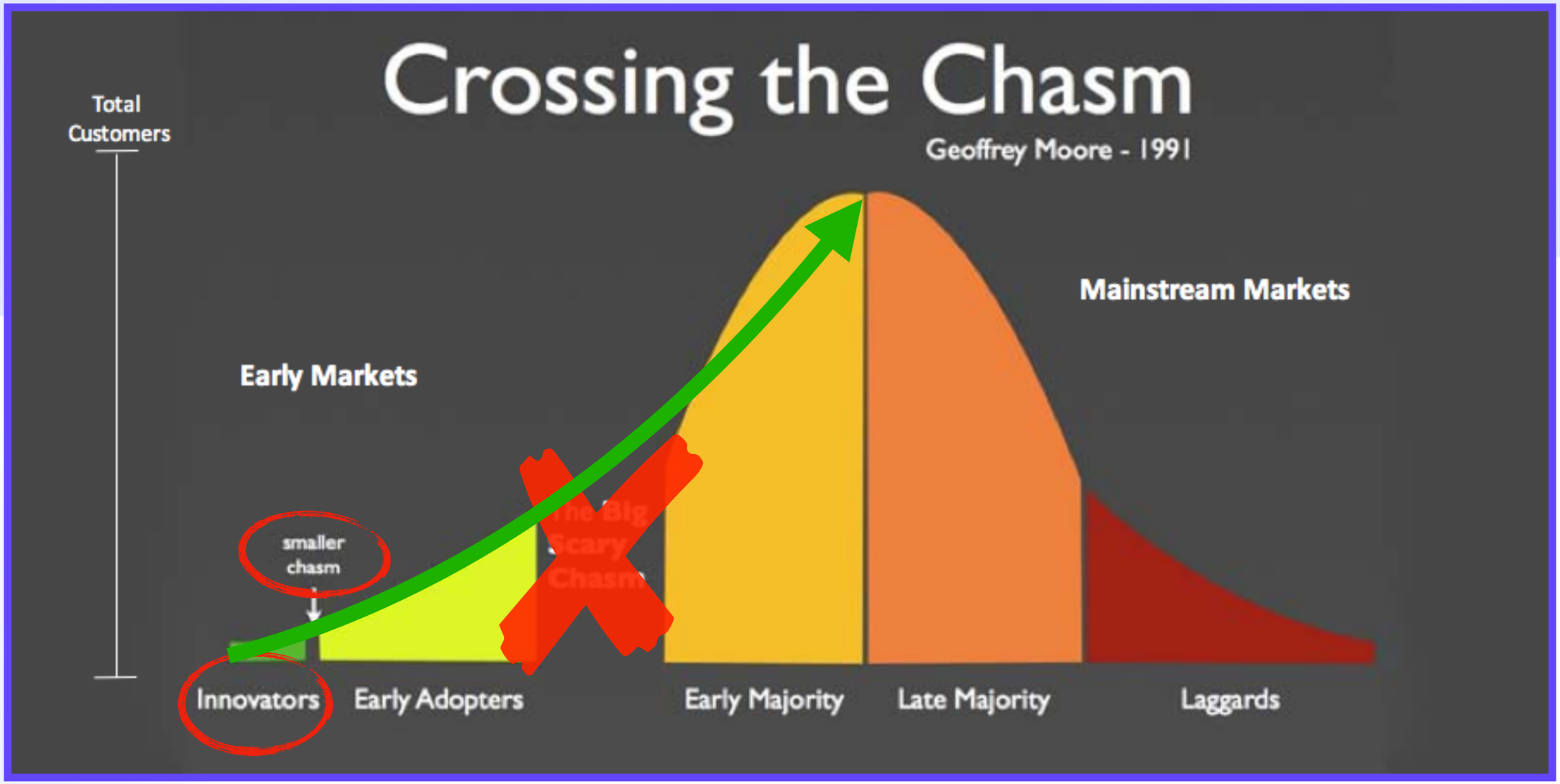
How to Power a New Internet 🔌

Adoption & Audience



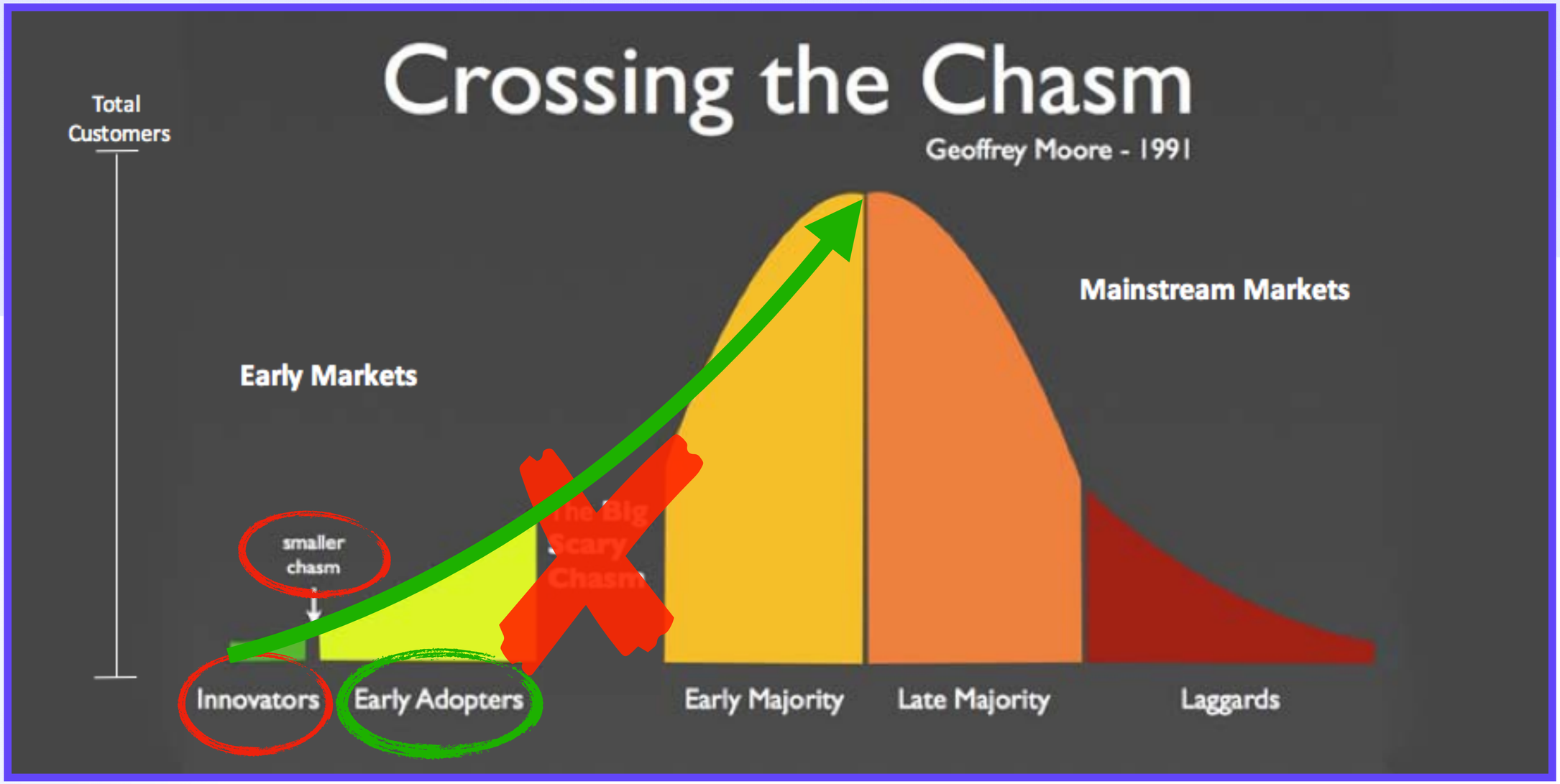
How to Power a New Internet 🔌

Adoption & Audience



How to Power a New Internet 🔌

Adoption & Audience



How to Power a New Internet 🔌

DX & UX

How to Power a New Internet 🔌

DX & UX

Web3 UX is ***too hard*** ~~for many users~~

How to Power a New Internet 🔌

DX & UX

Web3 UX is ***too hard*** fo[illegible]s

FULL STOP

How to Power a New Internet 🔌

Move the Needle

How to Power a New Internet 🔌

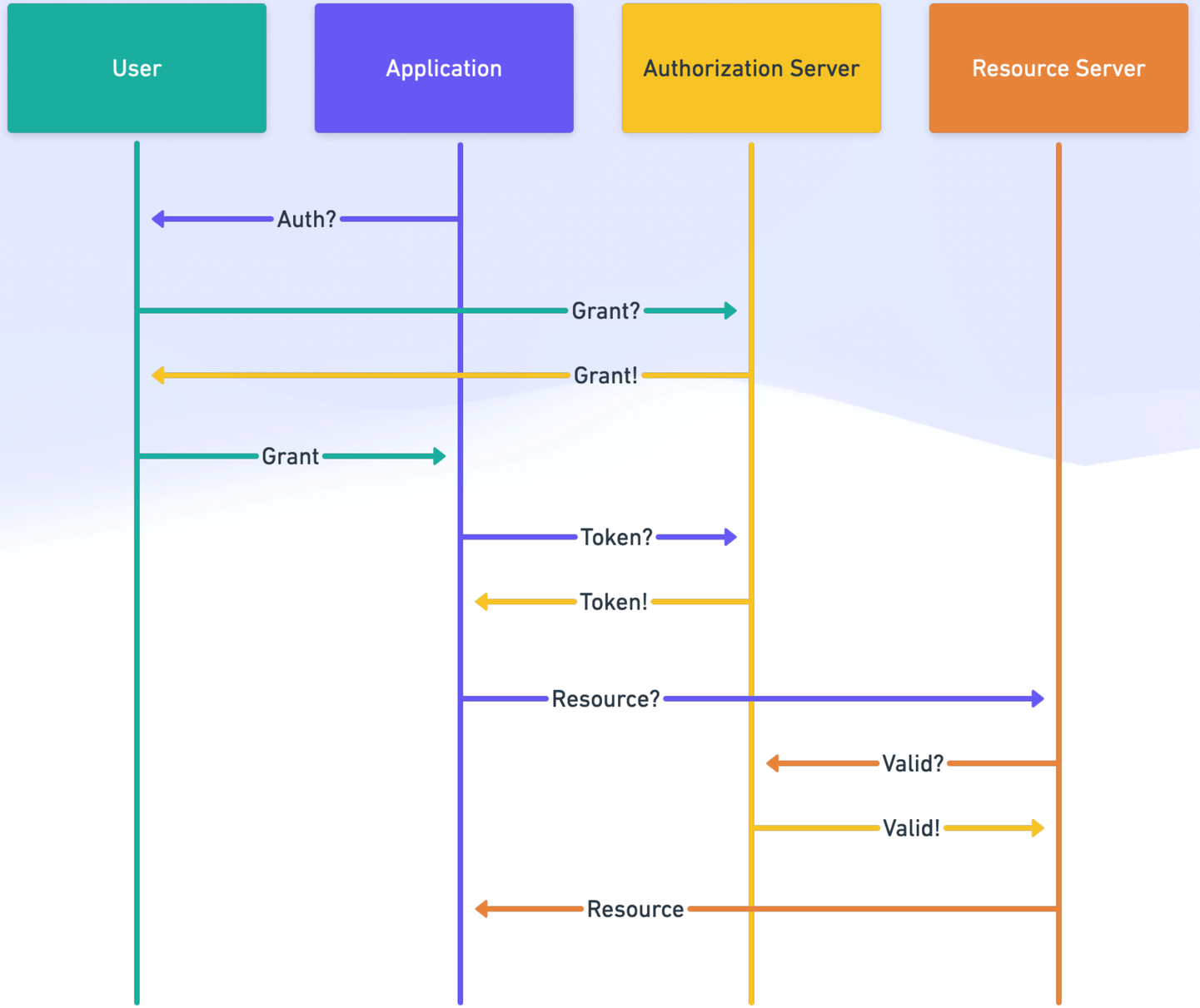
Move the Needle

Realpolitik

Easier, as secure, & more open than:
OAuth, X.509, SAML, Macaroons,
MetaMask, WalletConnect, etc

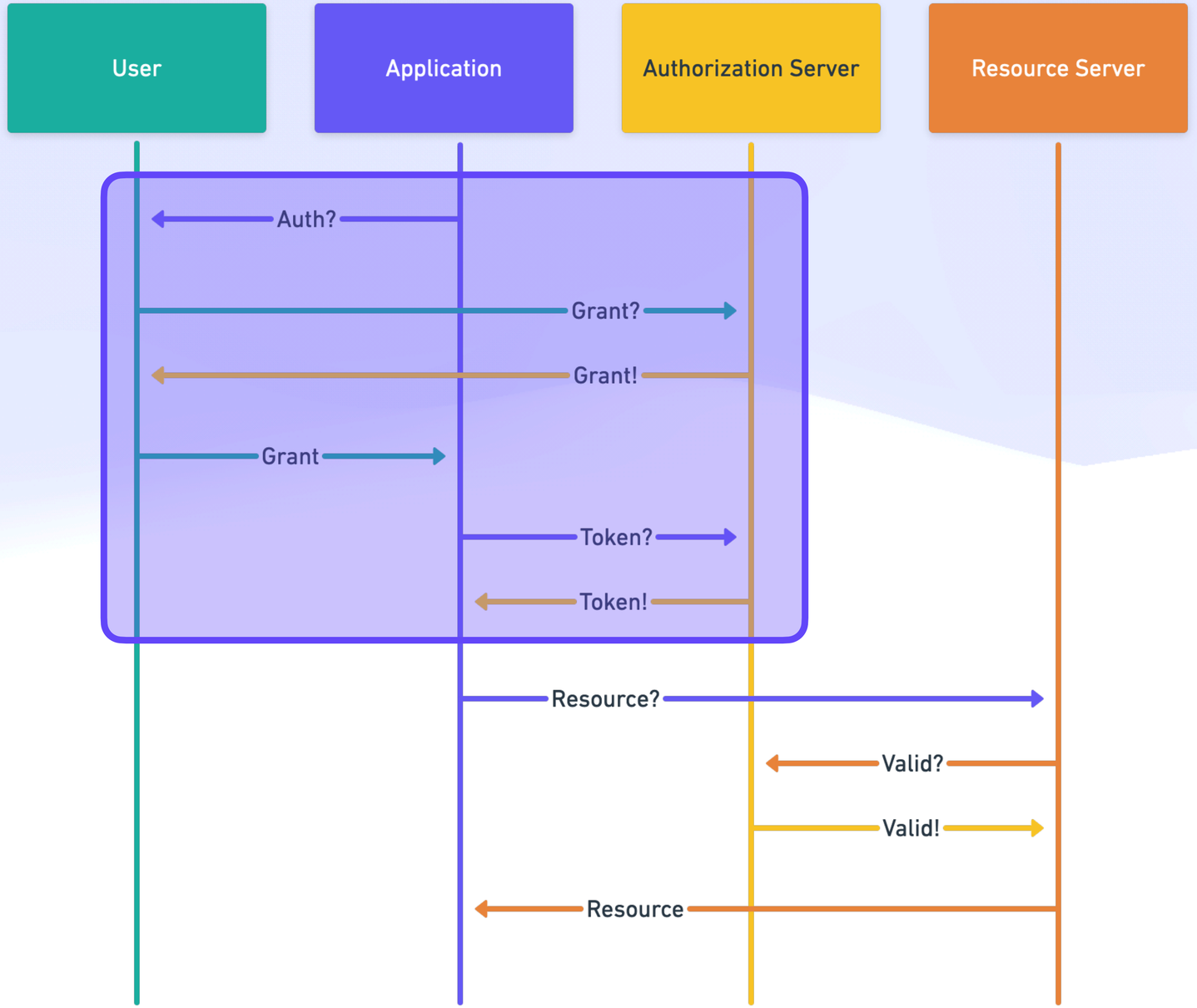
How to Power a New Internet 🔌

OAuth Sequence



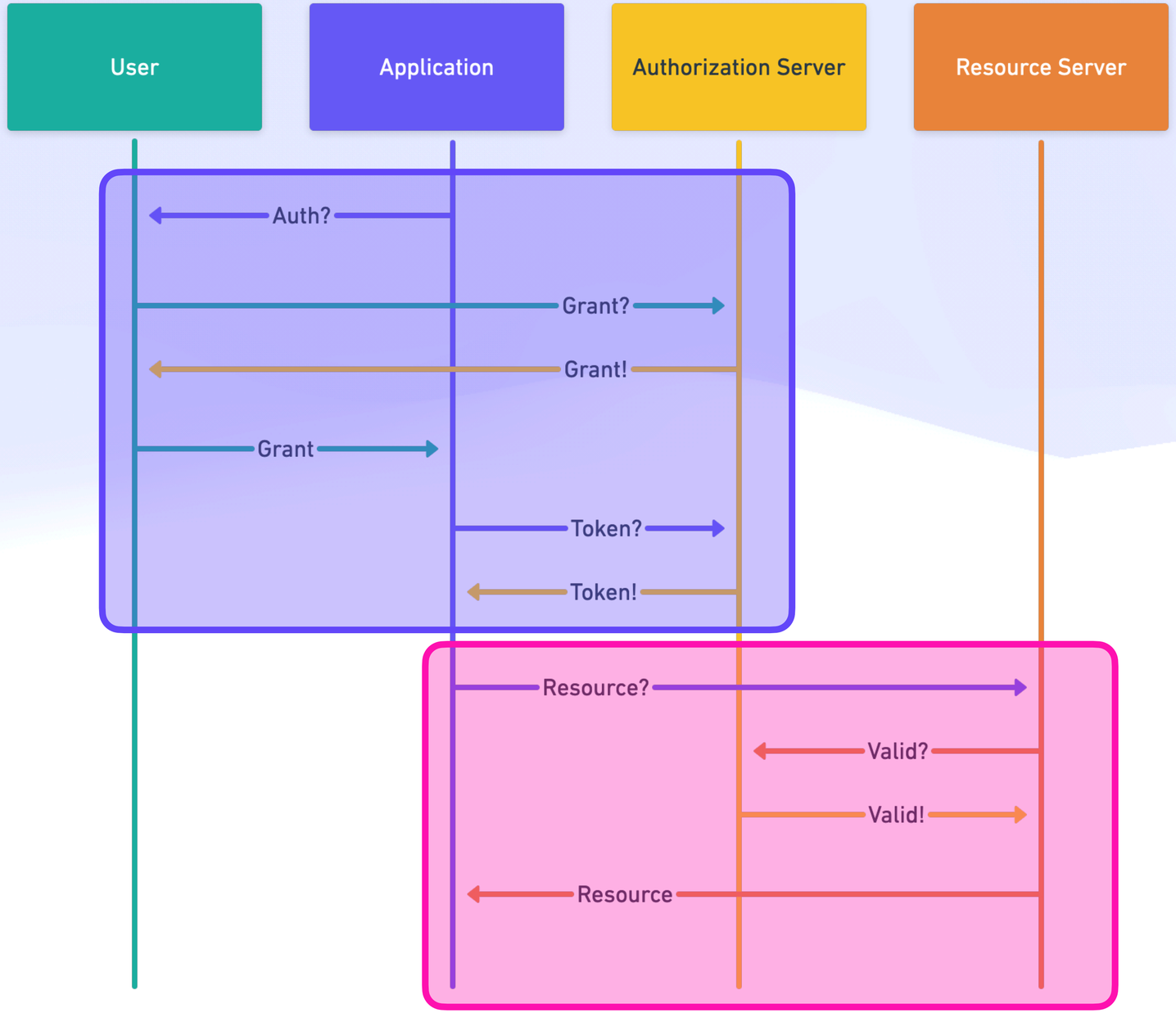
How to Power a New Internet 🔌

OAuth Sequence



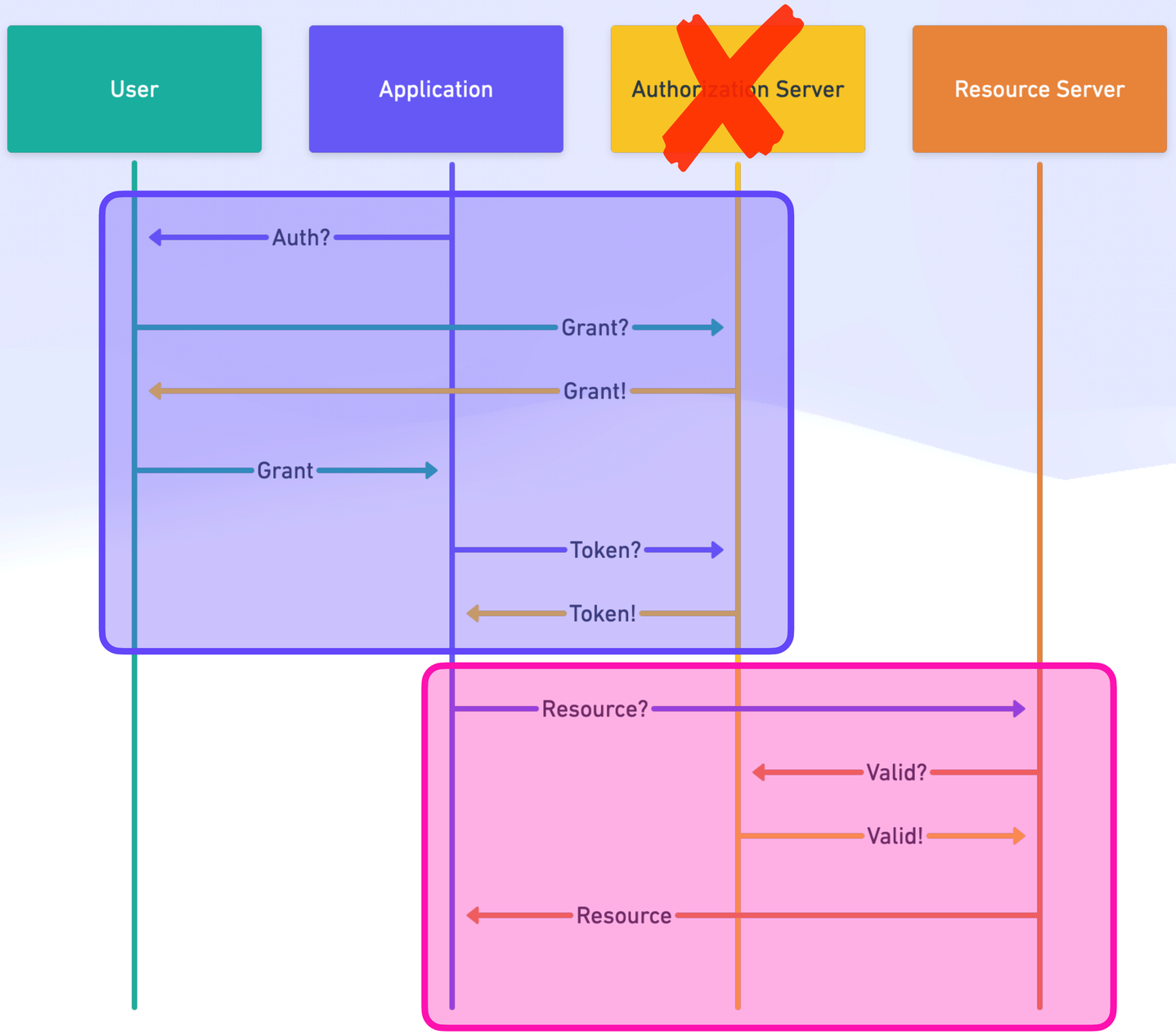
How to Power a New Internet 🔌

OAuth Sequence



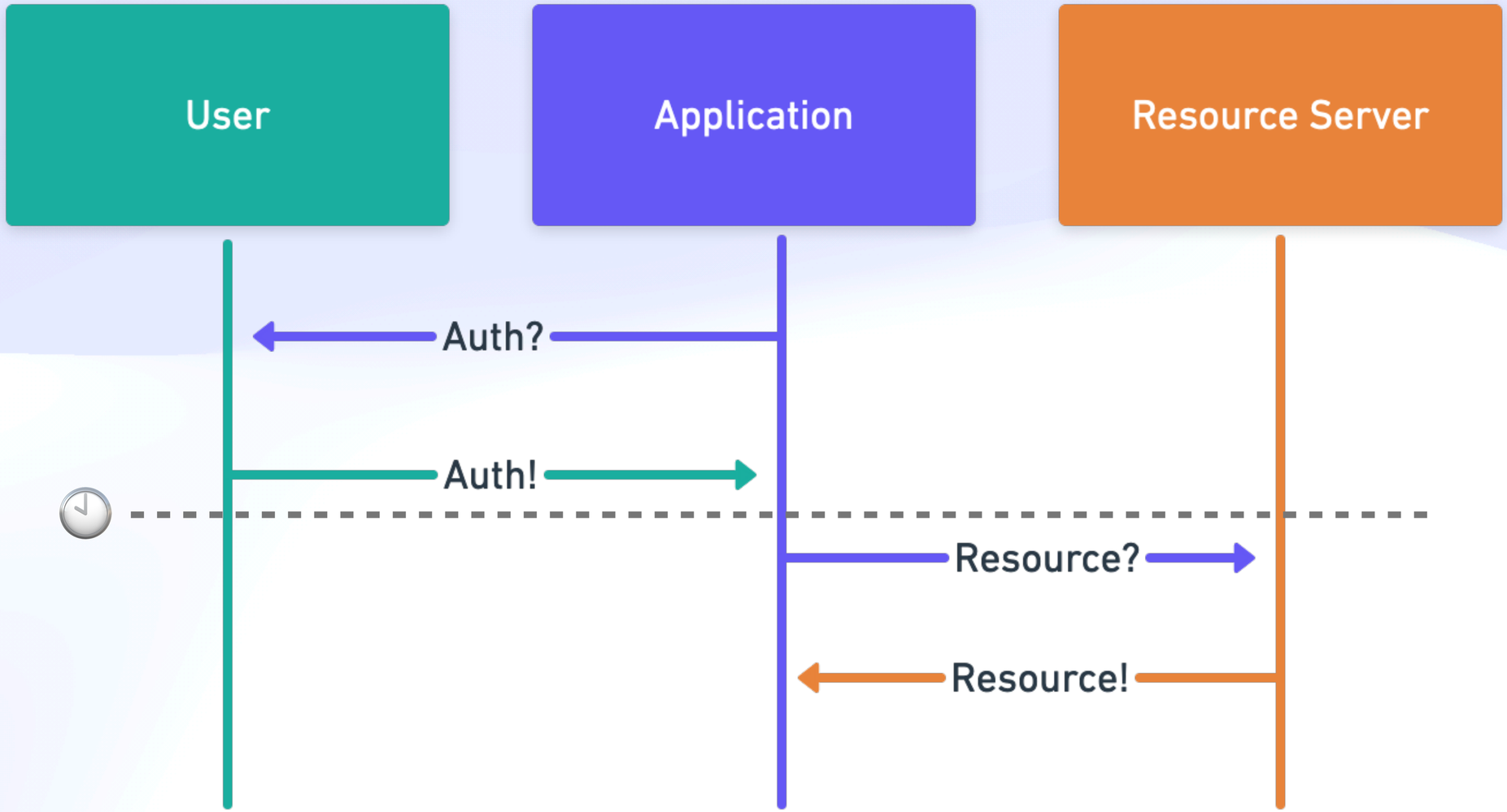
How to Power a New Internet 🔌

OAuth Sequence



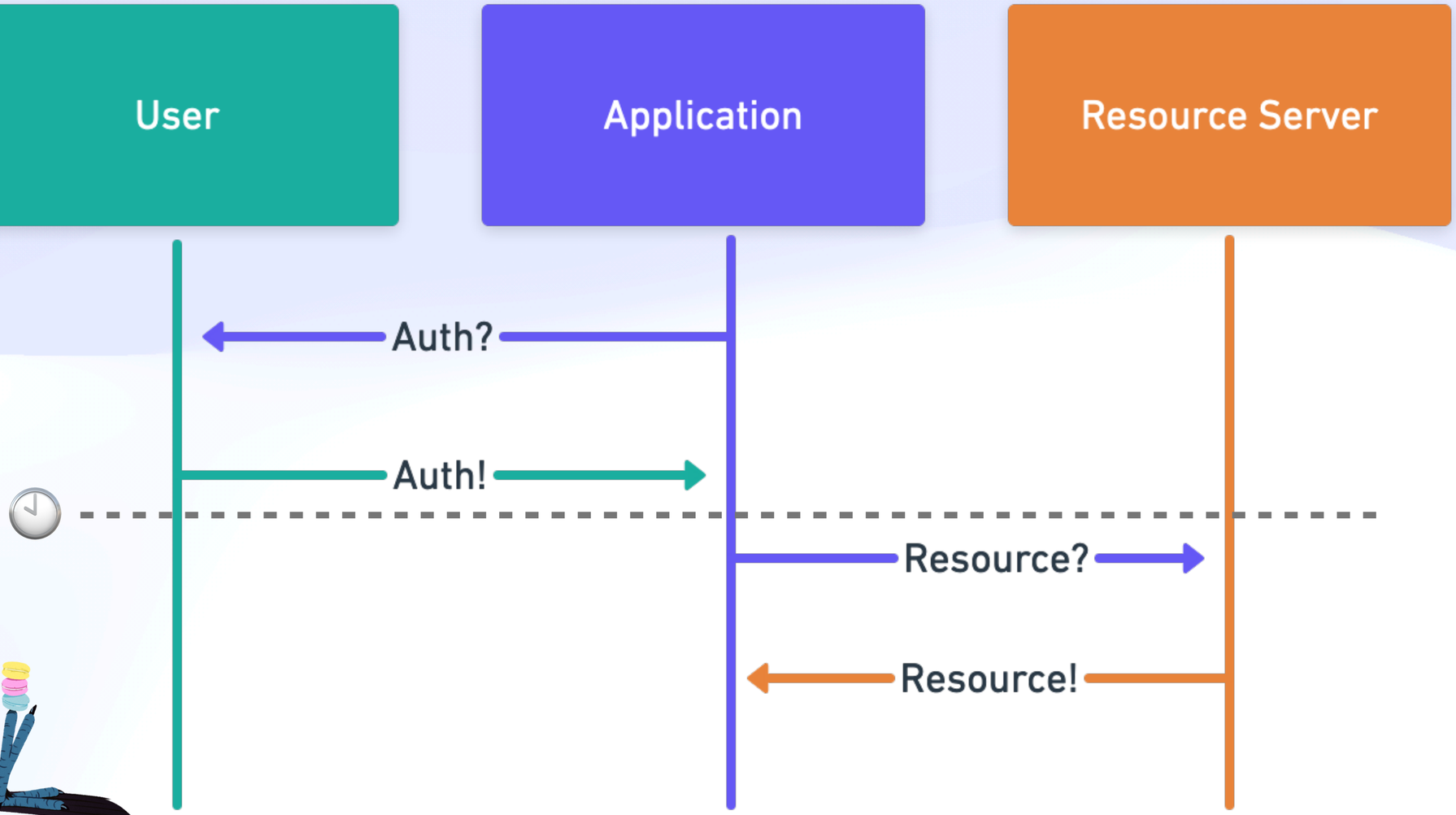
How to Power a New Internet 🔌

UCAN Sequence



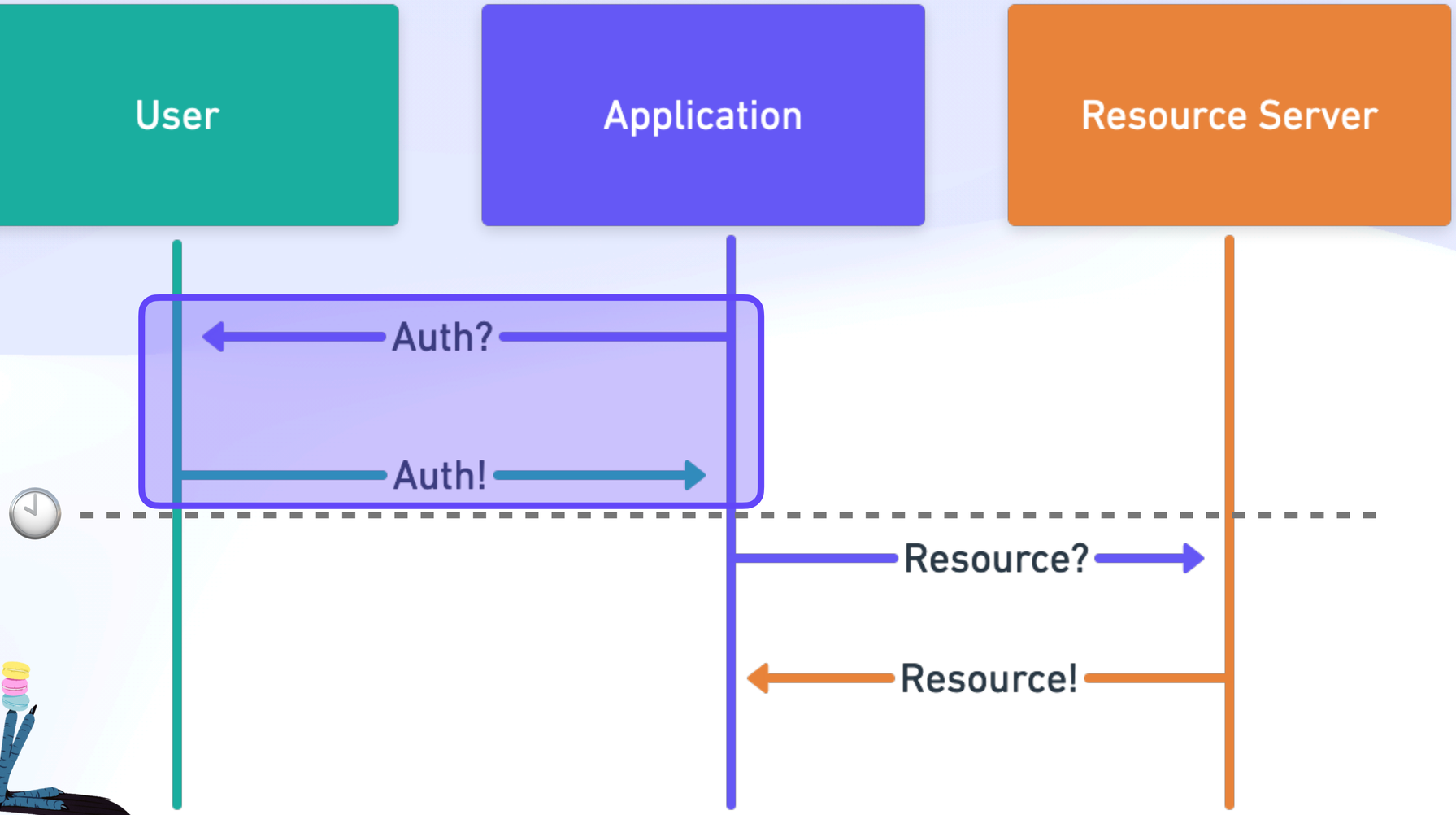
How to Power a New Internet 🔌

UCAN Sequence



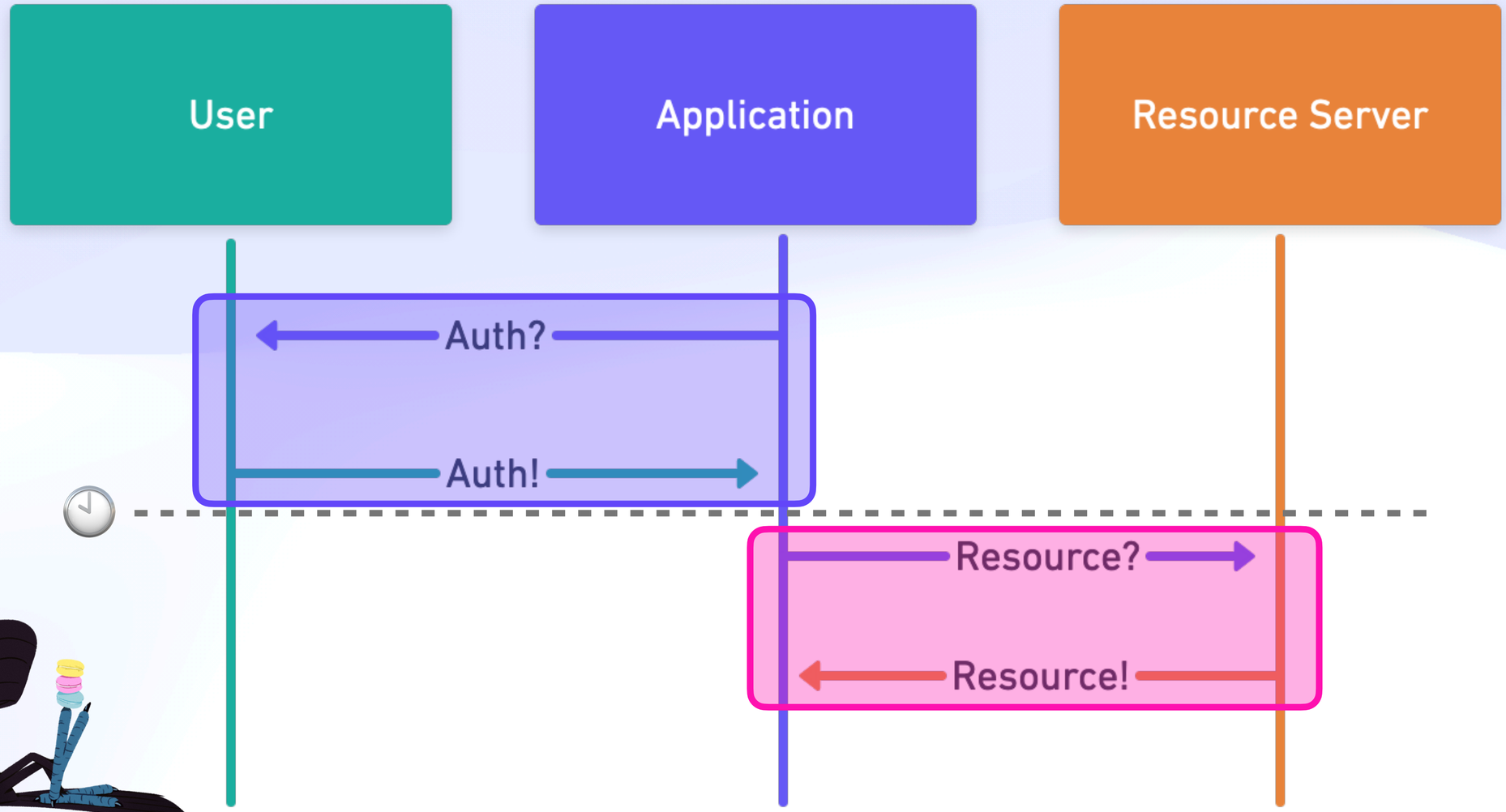
How to Power a New Internet 🔌

UCAN Sequence



How to Power a New Internet 🔌

UCAN Sequence



How to Power a New Internet 🔌

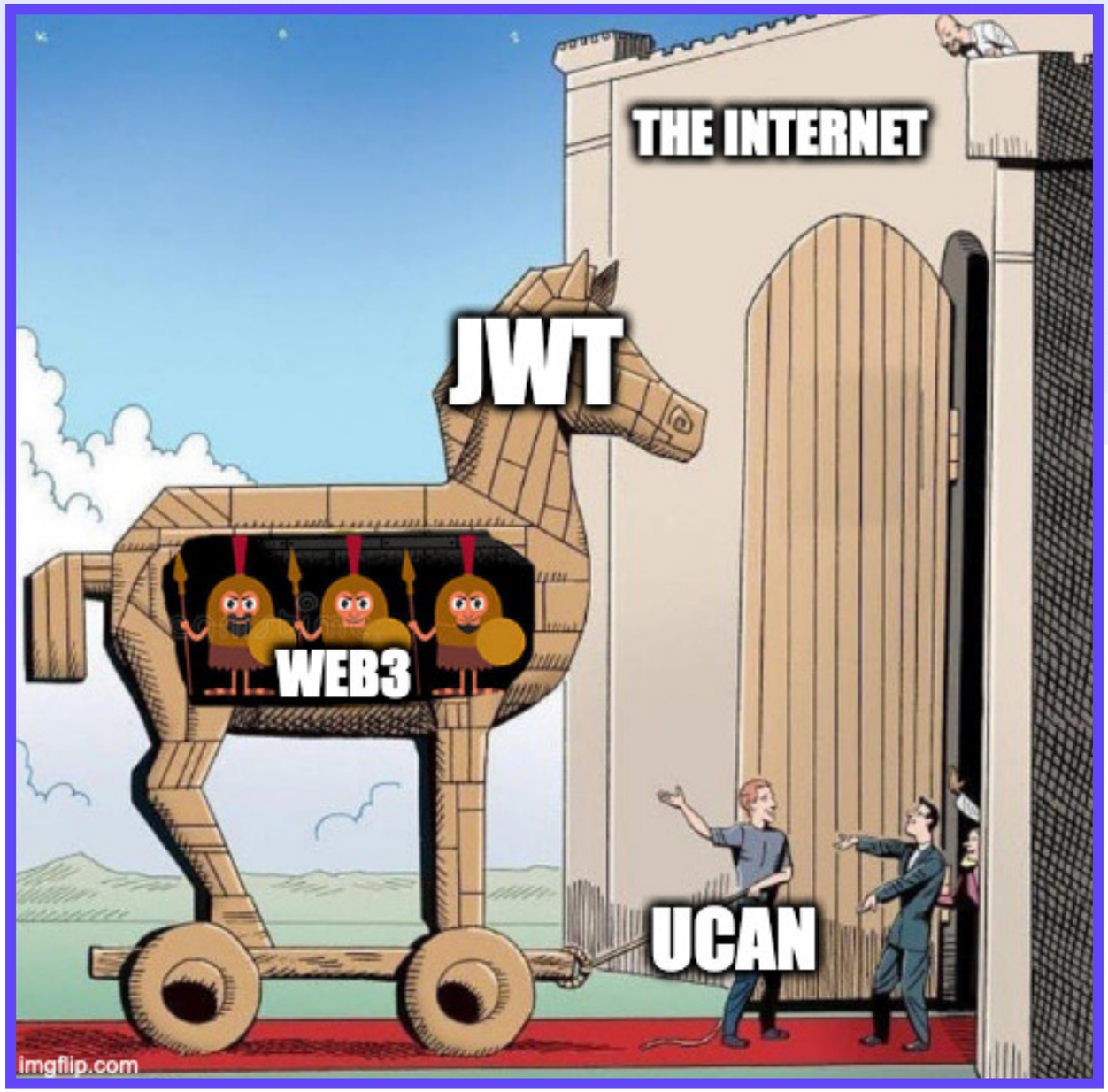
Project Approach

How to Power a New Internet 🔌

Project Approach

Be a Trojan Horse

Build on widely supported, familiar, well-understood standards & tools



How to Power a New Internet 🔌

Tools For Mere Mortals

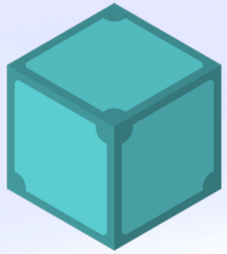
```
HTTP Header
"Authorization: Bearer <ucan>"
```

UCAN Decentralize Auth

Case Study: IPNS

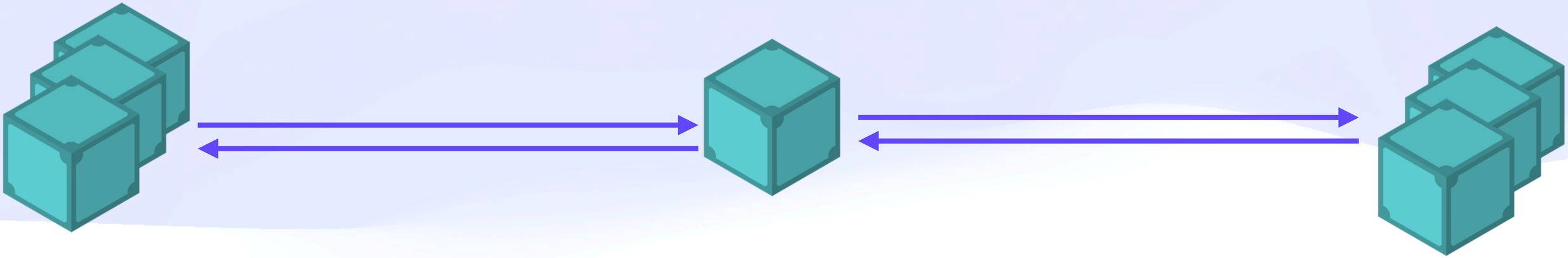
UCAN Decentralize Auth

Case Study: IPNS



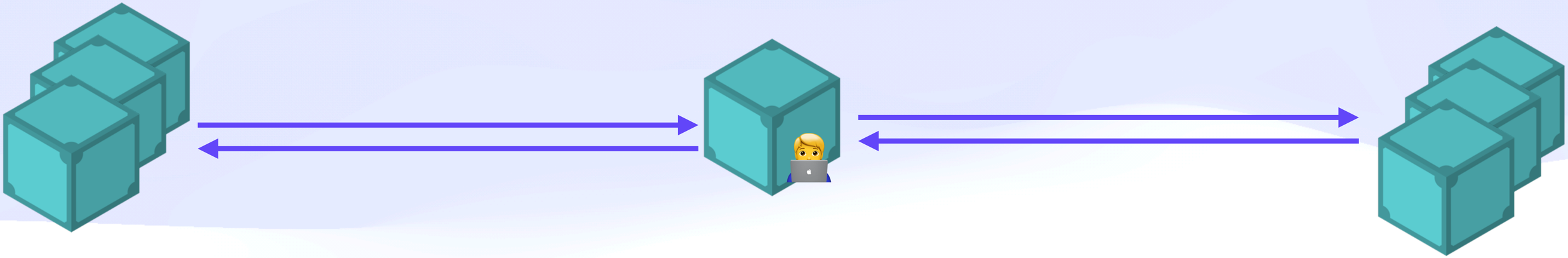
UCAN Decentralize Auth

Case Study: IPNS



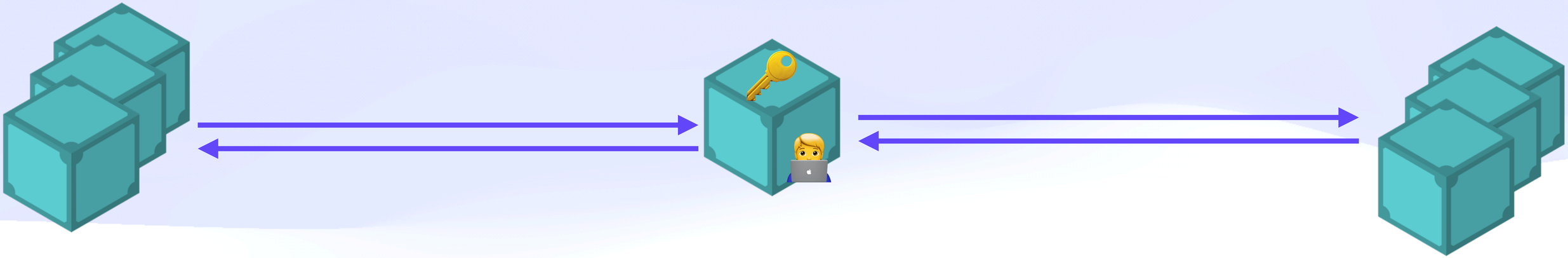
UCAN Decentralize Auth

Case Study: IPNS



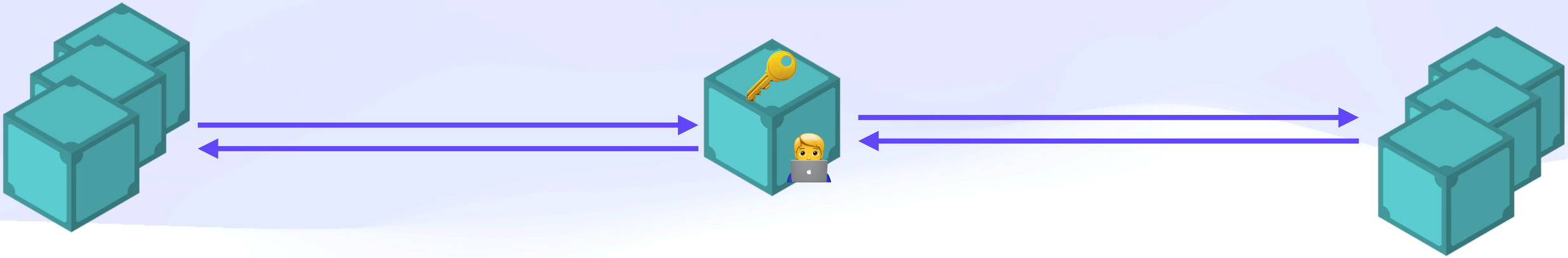
UCAN Decentralize Auth

Case Study: IPNS



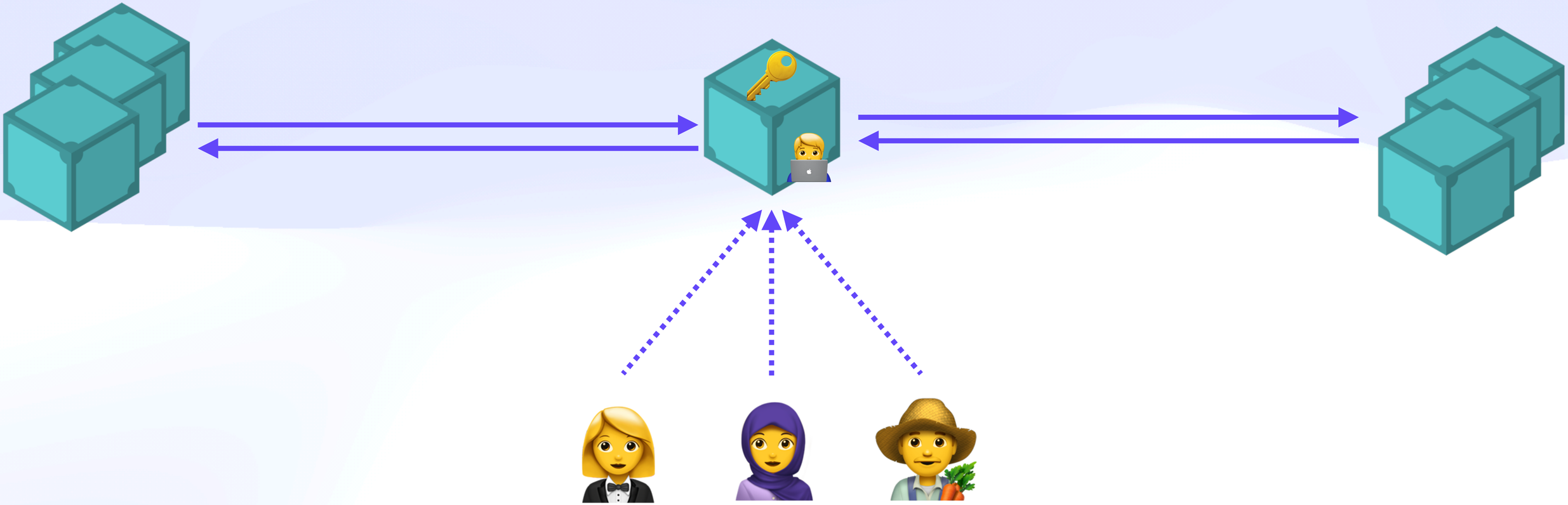
UCAN Decentralize Auth

Case Study: IPNS



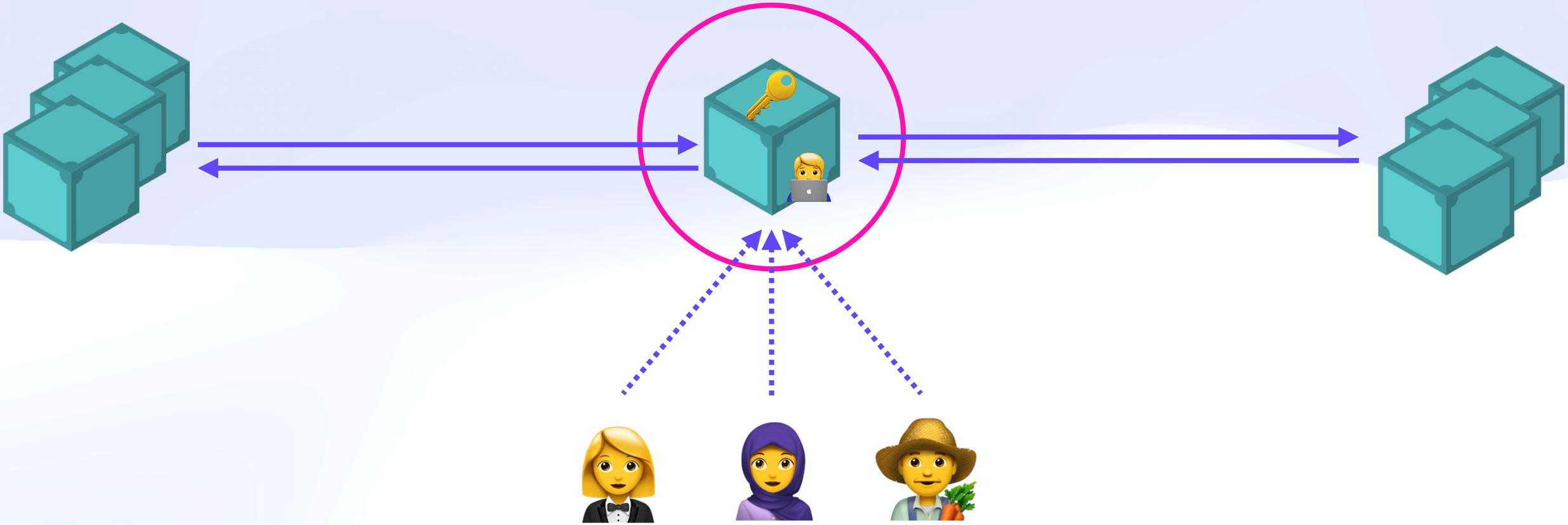
UCAN Decentralize Auth

Case Study: IPNS



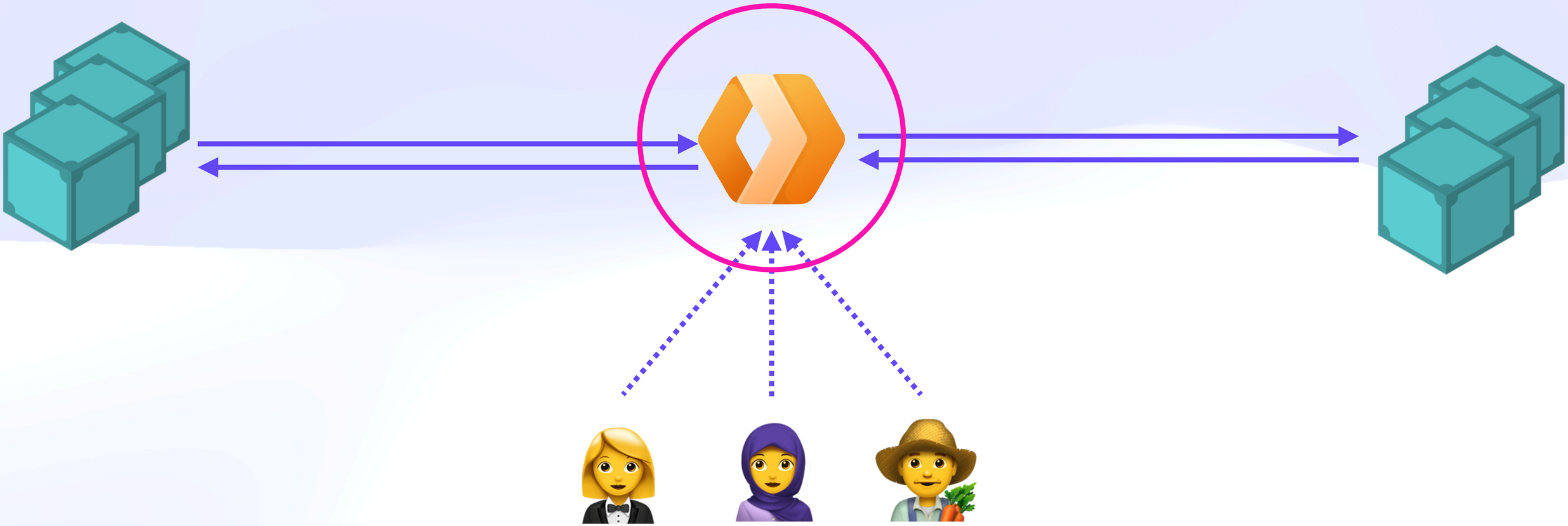
UCAN Decentralize Auth

Case Study: IPNS



UCAN Decentralize Auth

Case Study: Apps



UCAN Decentralize Auth

Case Study: Apps

Capabilities 101

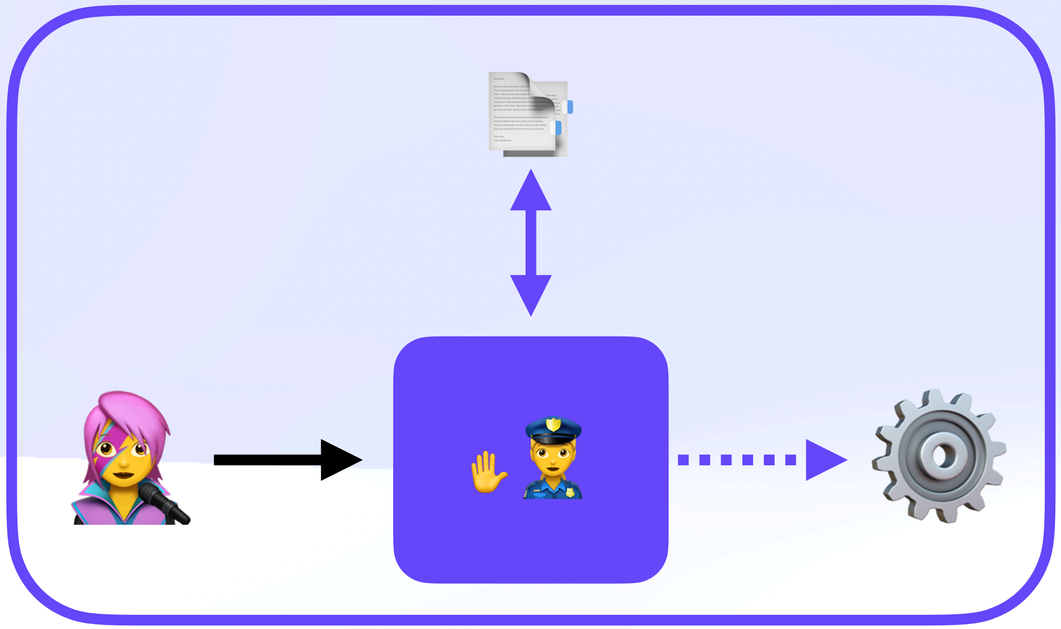
Capabilities 101

Auth Models

Capabilities 101

Auth Models

ACLs

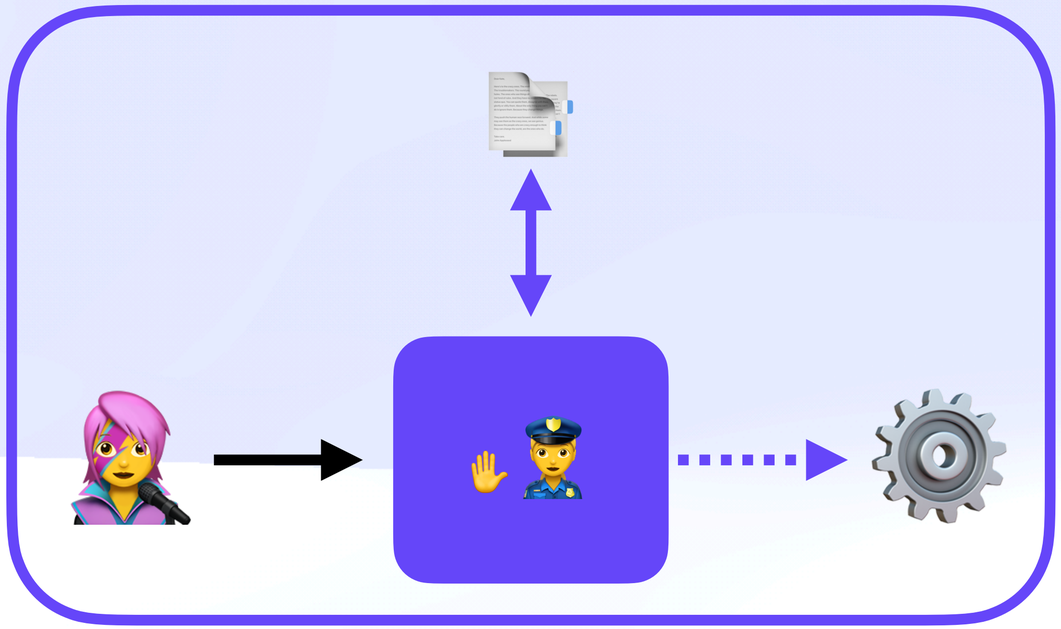


Designed for sharing a terminal (one)

Capabilities 101

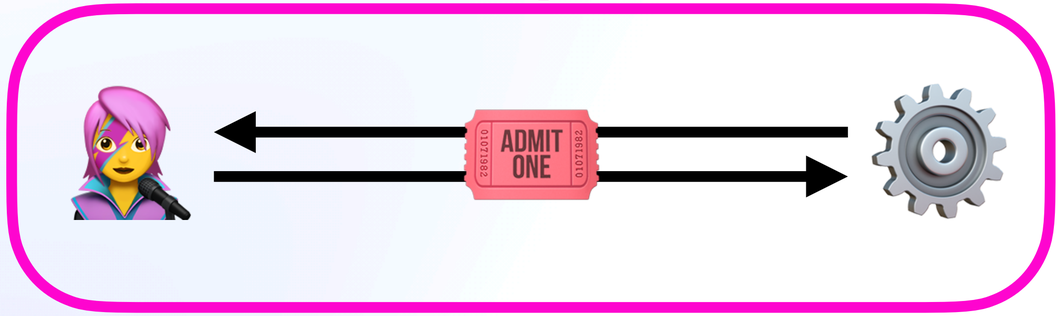
Auth Models

ACLs



Designed for sharing a terminal (one)

Caps



Designed for networking (many)

Capabilities 101

ACLs: Stateful Auth

Capabilities 101 🎟️

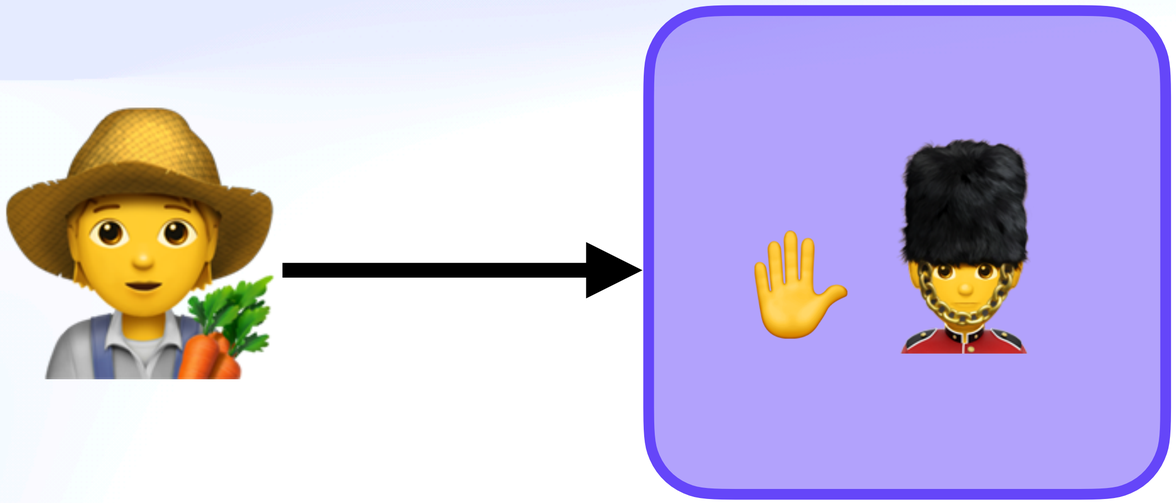
ACLs: Stateful Auth

Capabilities 101 🎟️

ACLs: Stateful Auth

Capabilities 101 🎟️

ACLs: Stateful Auth



Capabilities 101 🎟️

ACLs: Stateful Auth

Capabilities 101

ACLs: Stateful Auth

Capabilities 101

ACLs: Stateful Auth

Capabilities 101

ACLs: Stateful Auth

Not in control

Capabilities 101

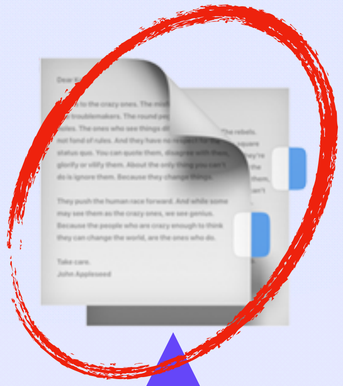
ACLs: Stateful Auth

In control

Not in control

Capabilities 101

ACLs: Stateful Auth

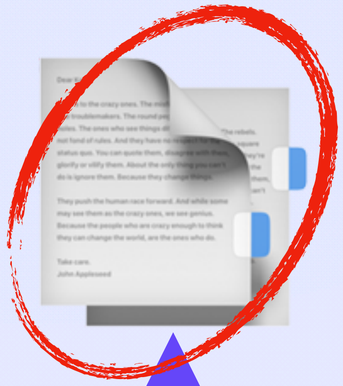


In control

Not in control

Capabilities 101

ACLs: Stateful Auth

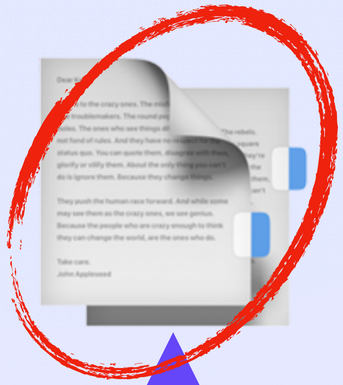


In control

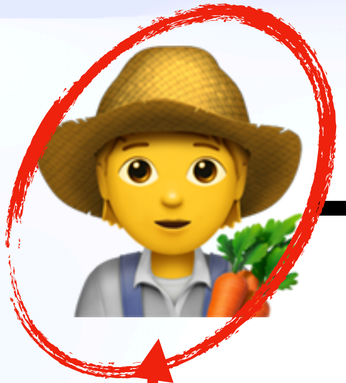
Not in control

Capabilities 101

ACLs: Stateful Auth



In control



Not in control

Capabilities 101 🎟️

PSA: ACLs Don't CRDT Well

RFP-004: Data laced with permissions: Decentralised access control in CRDTs

Brief description Conflict-free replicated data types (CRDTs) provide a framework for creating eventually consistent data types that can be shared amongst replicas and that guarantees liveliness and monotonicity. To allow replica creators and owners to keep control over who has read and write access to a CRDT instance, we seek a decentralised Access control list (ACL) type that has typical ACL security properties and that, when applied to a CRDT instance, still guarantees CRDT safety (that it provably converges to the same value on all replicas).

Capabilities 101 🎟️

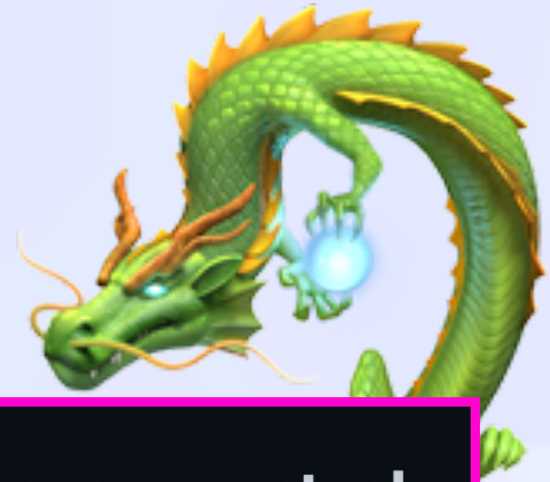
PSA: ACLs Don't CRDT Well

RFP-004: Data laced with permissions: Decentralised access control in CRDTs

escription Conflict-free replicated data types (CRDTs) provide a framework for creating eventually consistent data types that ed amongst replicas and that guarantees liveliness and monotonicity. To allow replica creators and owners to keep control s read and ess to a CRDT instance, we seek a decentralised Access control list (ACL) type that has typical ACL rties ar n applied to a CRDT instance, still guarantees CRDT safety (that it provably converges to the same blicas).

Capabilities 101 🎟️

PSA: ACLs Don't CRDT Well



RFP-004: Data laced with permissions: Decentralised access control in CRDTs

escription Conflict-free replicated data types (CRDTs) provide a framework for creating eventually consistent data types that ed amongst replicas and that guarantees liveliness and monotonicity. To allow replica creators and owners to keep control s read and ess to a CRDT instance, we seek a decentralised Access control list (ACL) type that has typical ACL rties ar n applied to a CRDT instance, still guarantees CRDT safety (that it provably converges to the same blicas).

Capabilities 101

Caps: Stateless Auth

Capabilities 101 🎟️

Caps: Stateless Auth

Capabilities 101 🎟️

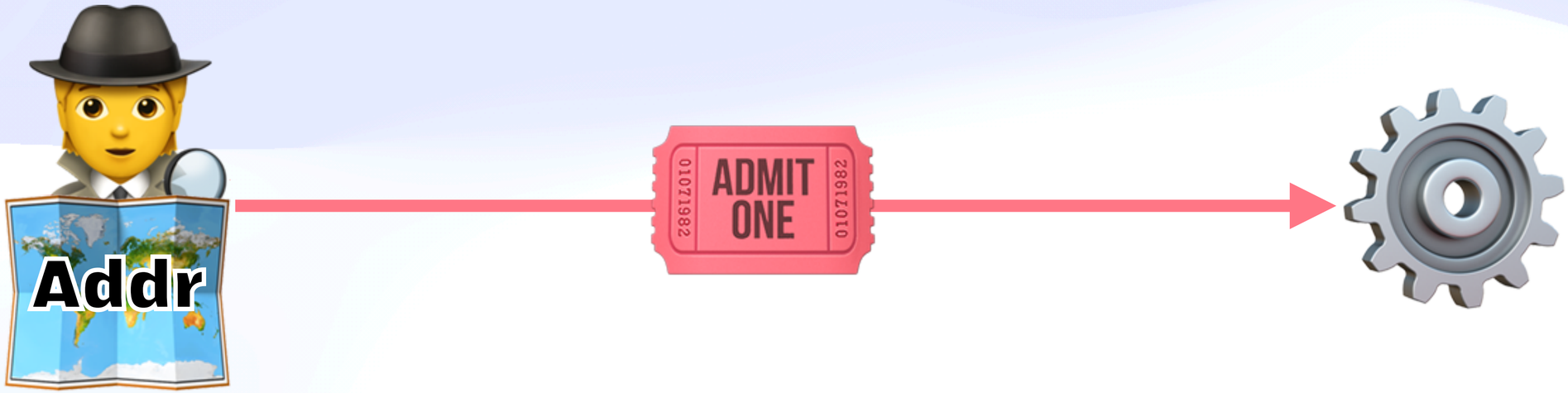
Caps: Stateless Auth

Capabilities 101 🎟️

Caps: Stateless Auth

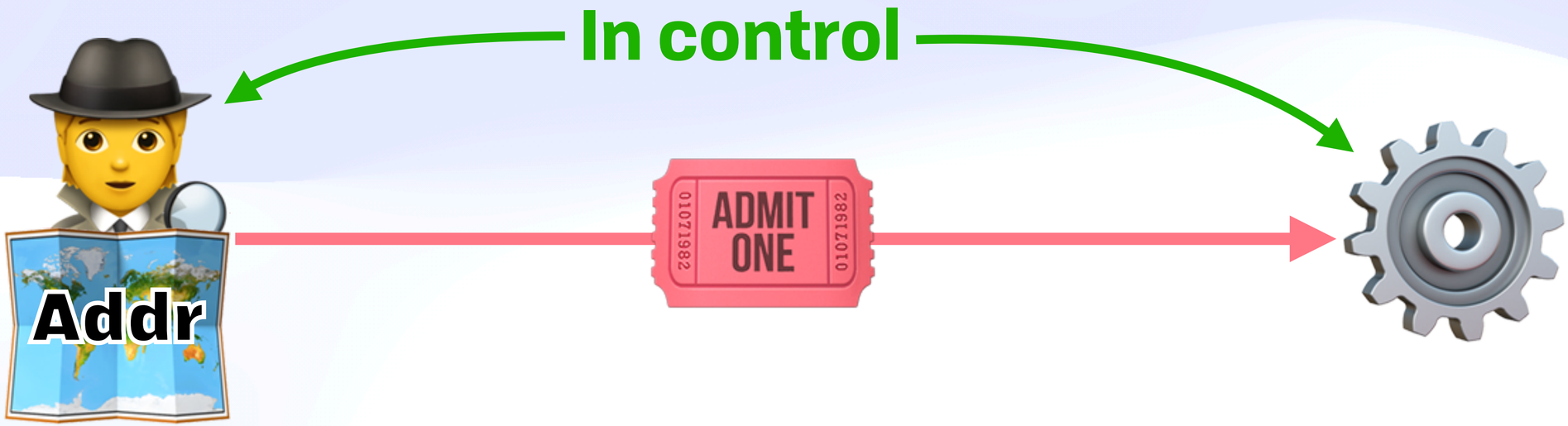
Capabilities 101

Caps: Stateless Auth



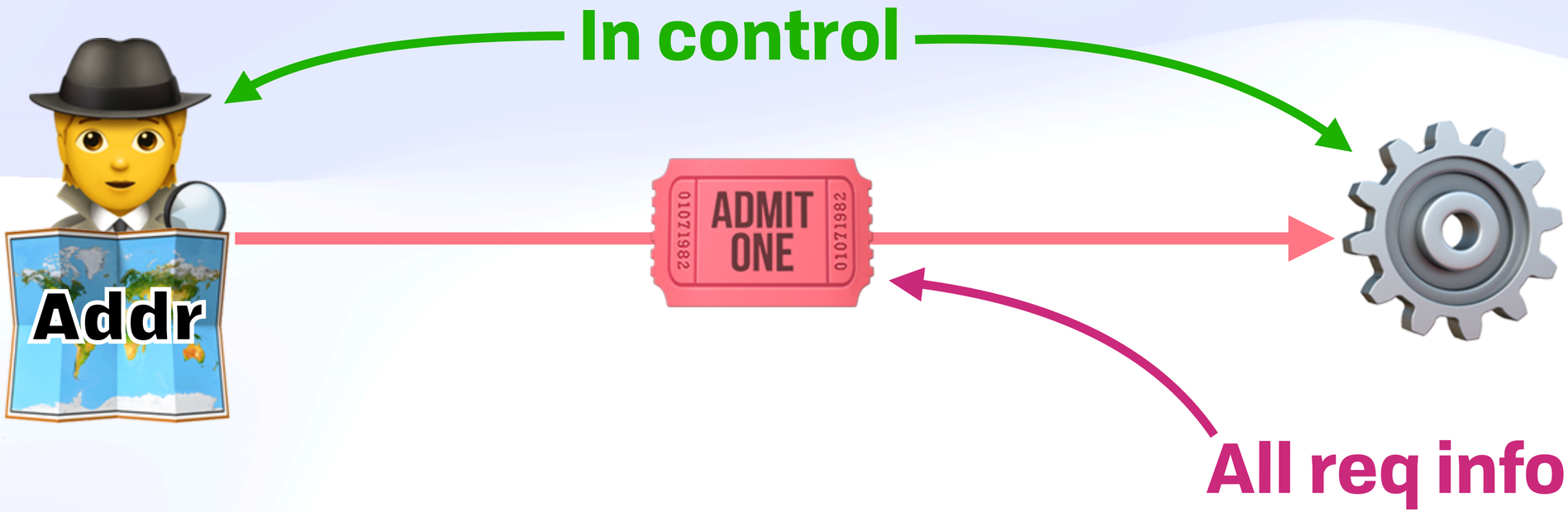
Capabilities 101

Caps: Stateless Auth



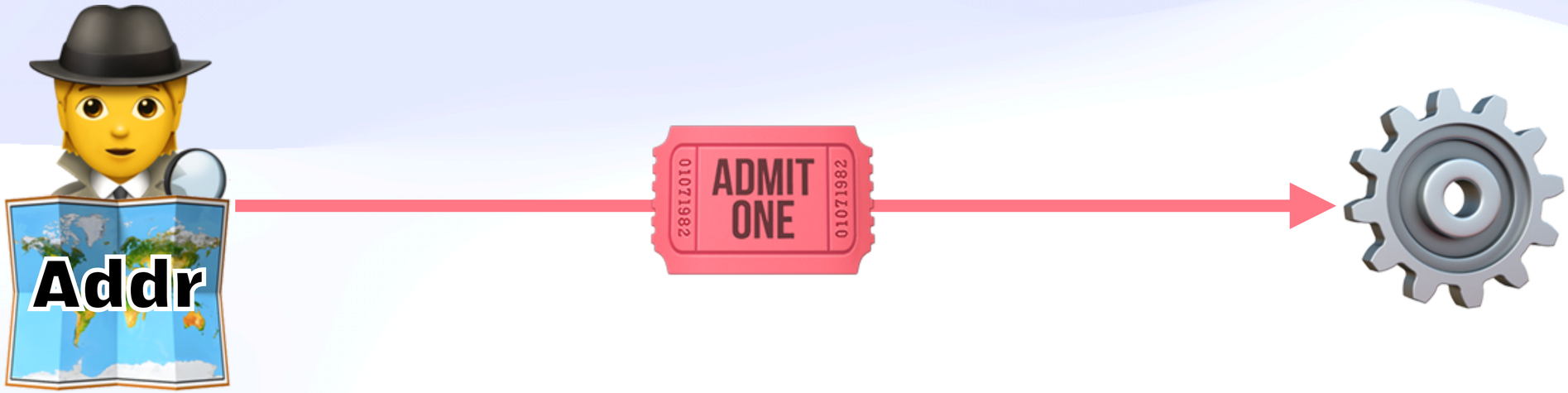
Capabilities 101

Caps: Stateless Auth



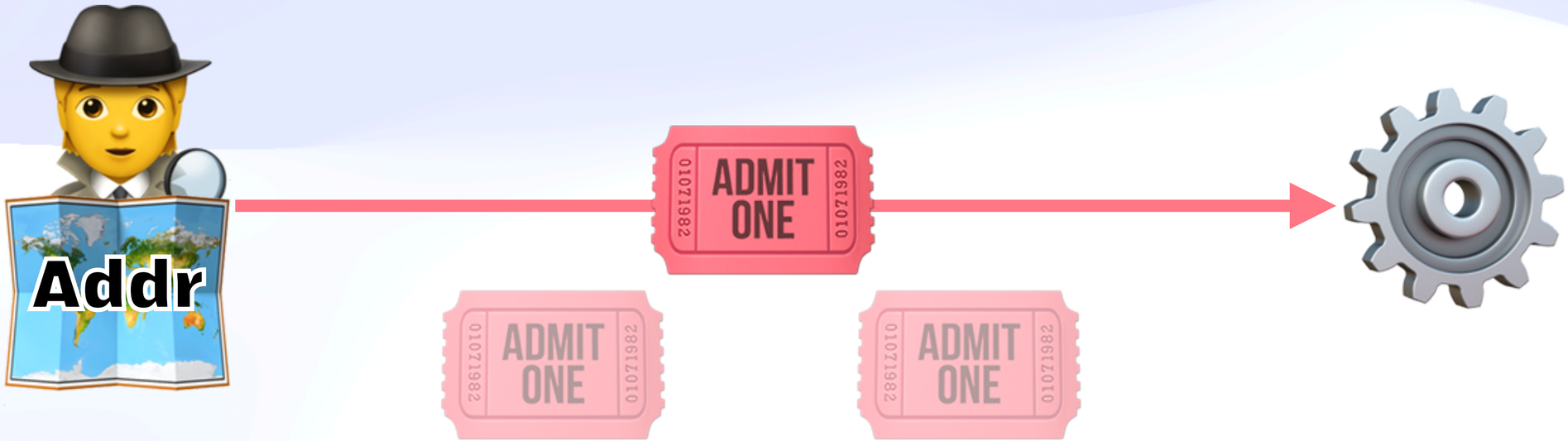
Capabilities 101

Caps: Stateless Auth



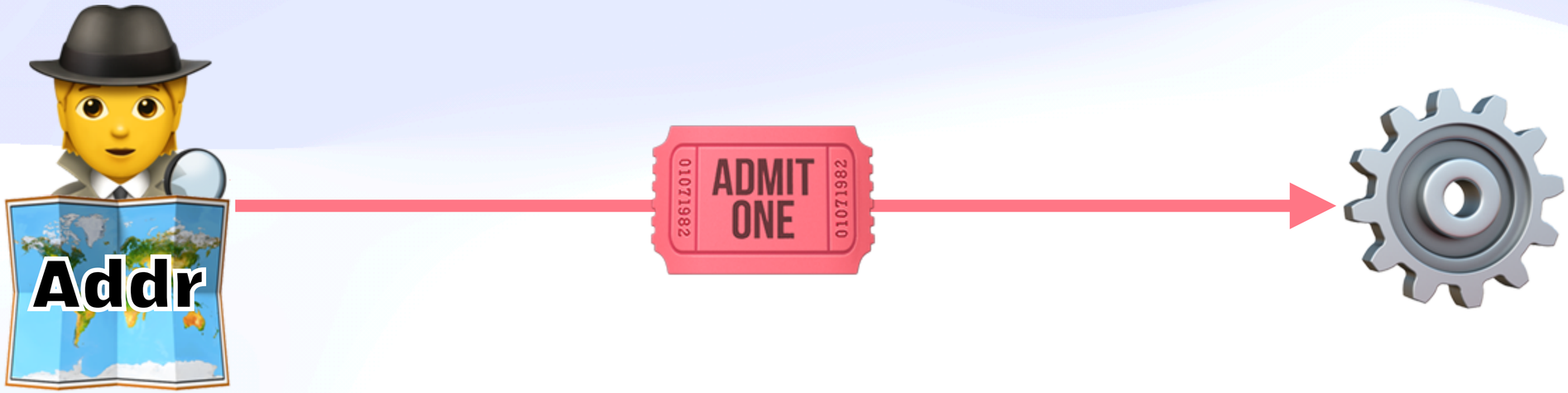
Capabilities 101

Caps: Stateless Auth



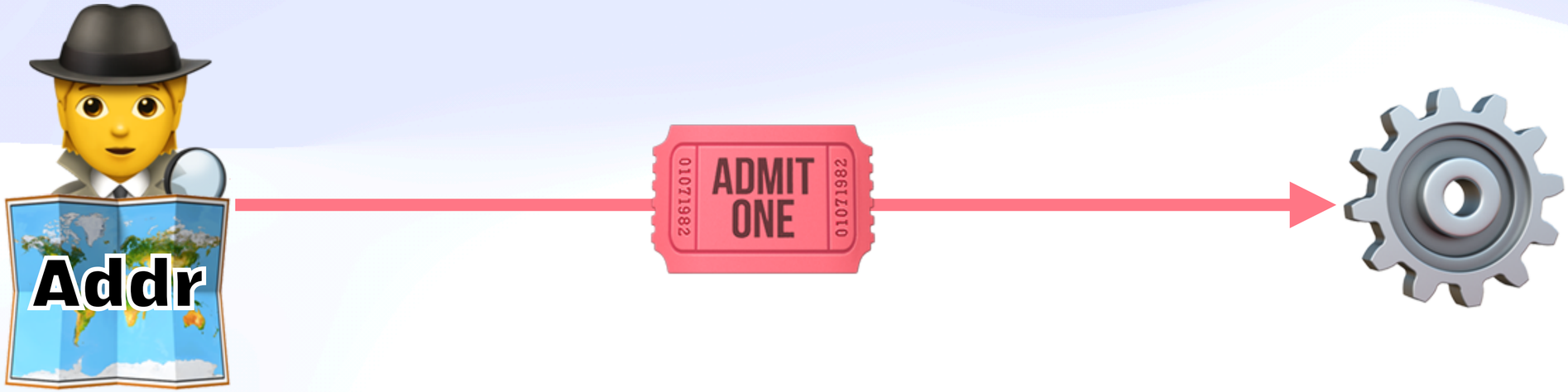
Capabilities 101

Caps: Stateless Auth



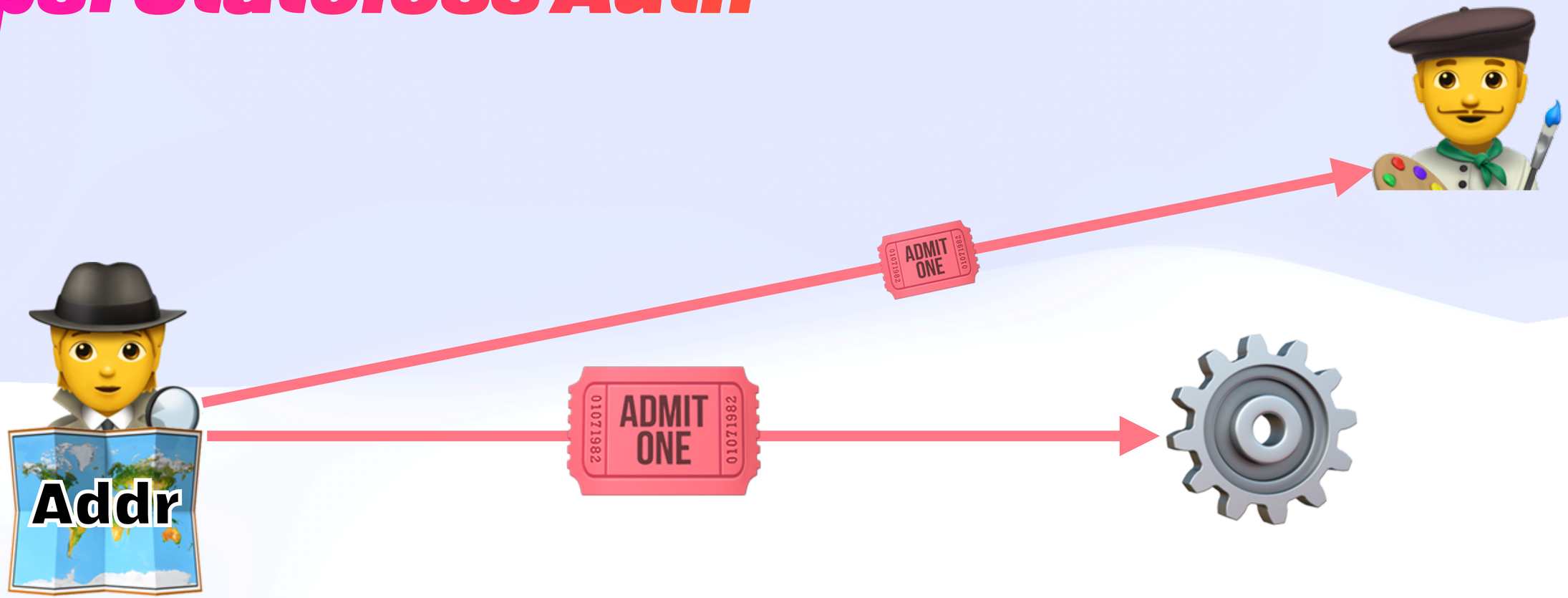
Capabilities 101

Caps: Stateless Auth



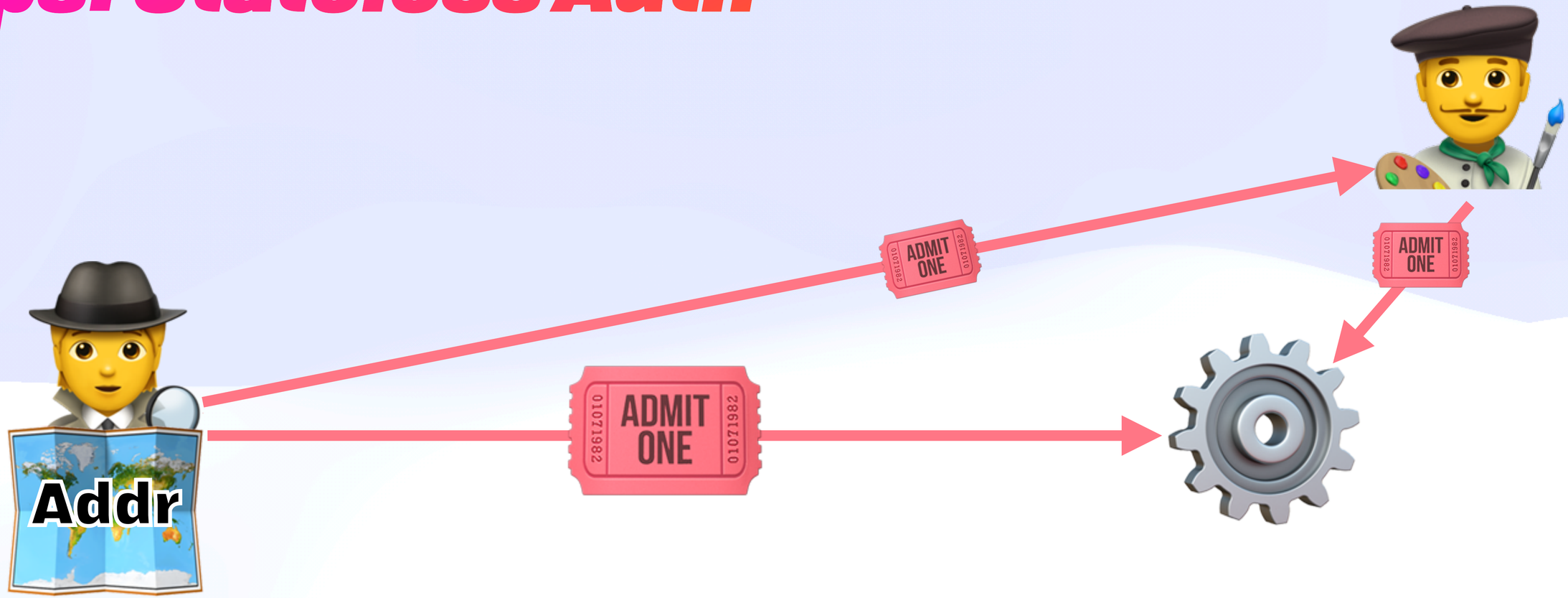
Capabilities 101

Caps: Stateless Auth



Capabilities 101

Caps: Stateless Auth



Capabilities 101

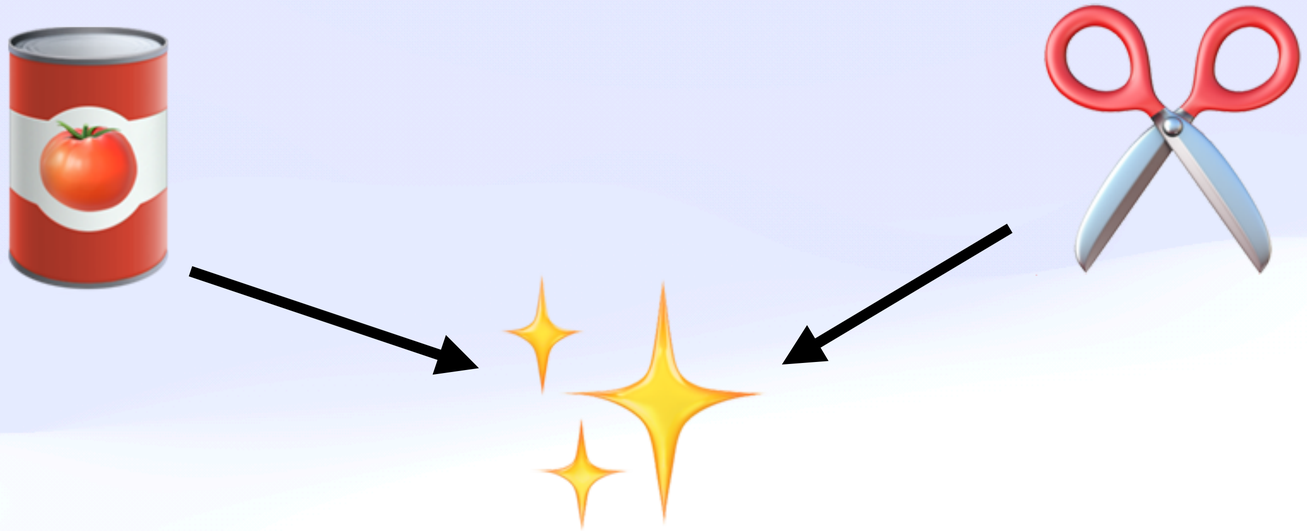
Composition — "Amplification"

Capabilities 101 🎟️

Composition — "Amplification"

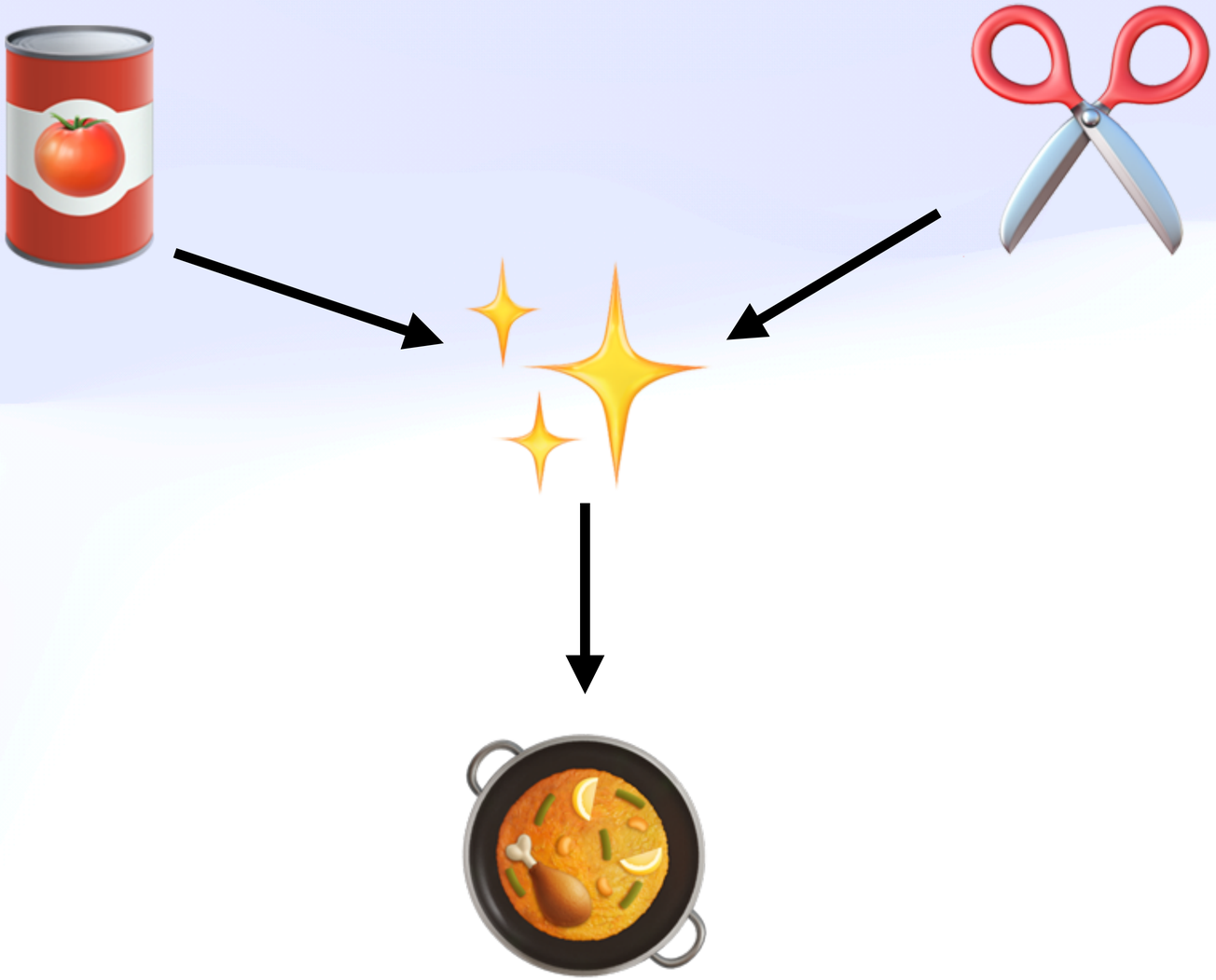
Capabilities 101 🎟️

Composition — "Amplification"



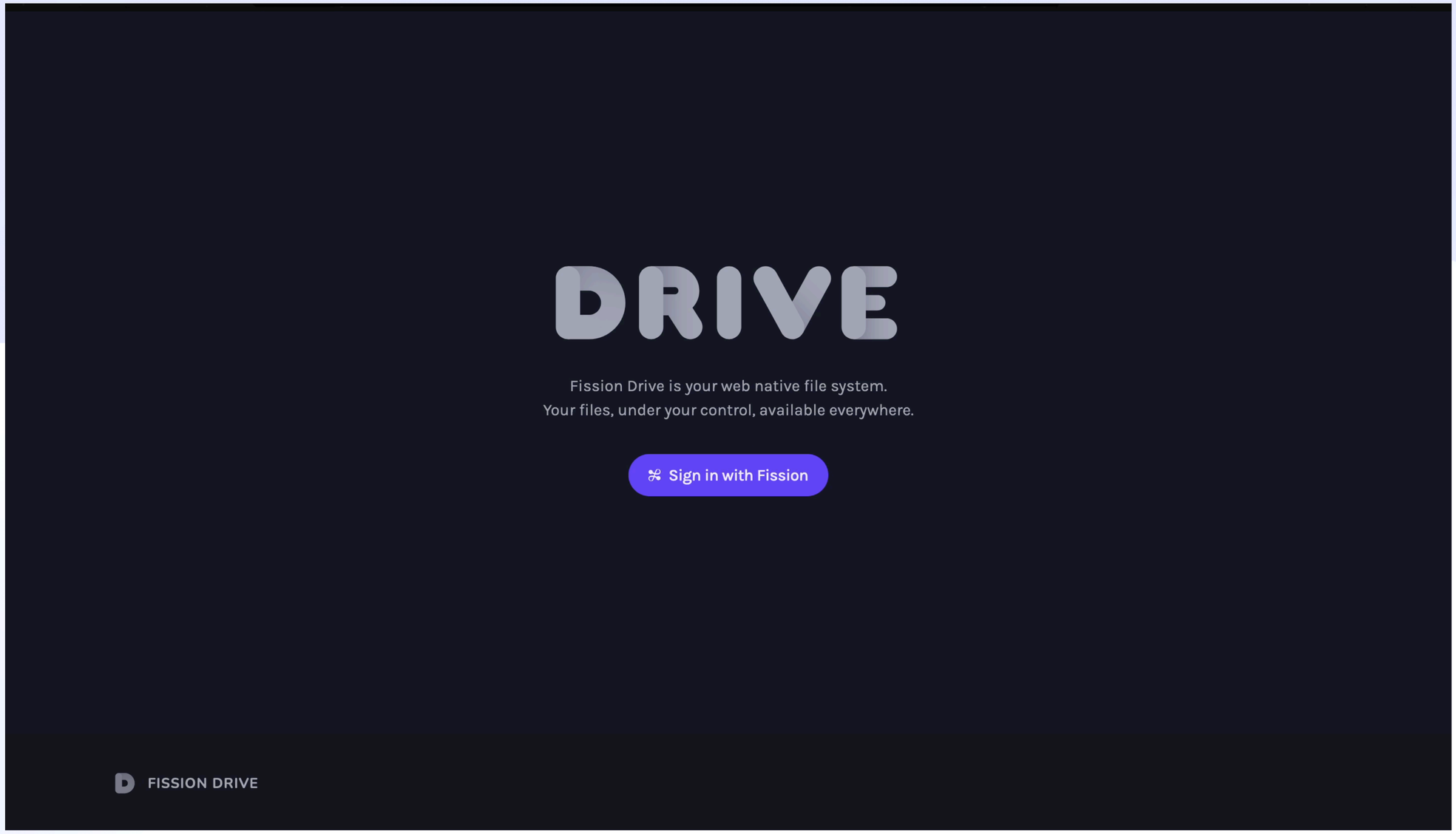
Capabilities 101

Composition — "Amplification"



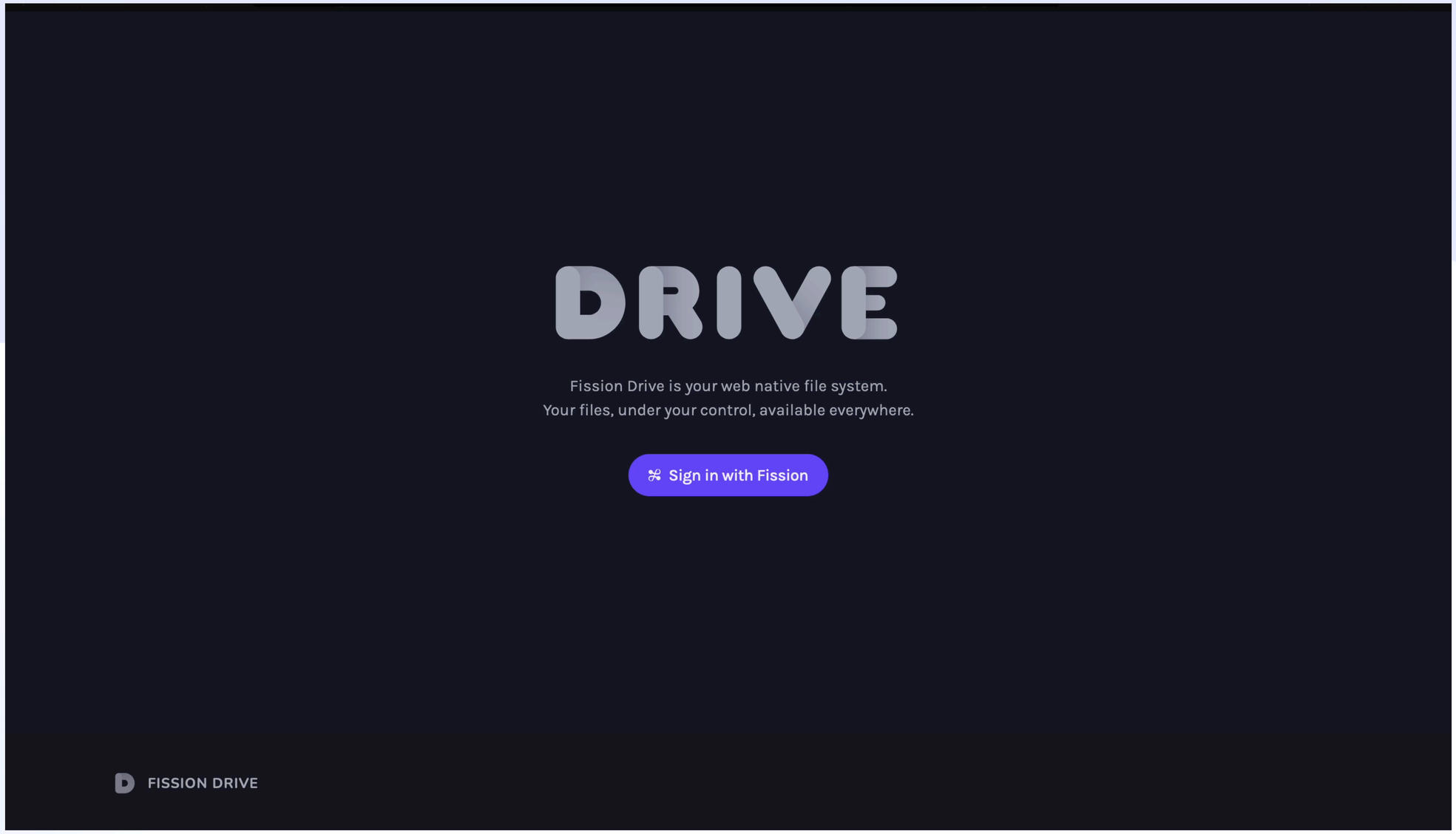
Capabilities 101

Auth Should be Boring!



Capabilities 101

Auth Should be Boring!



Under the Microscope

Under the Microscope 🔬

"Who" vs "What"

Under the Microscope 🔬

"Who" vs "What"

DIDs say who ***you are***

Under the Microscope 🔬

"Who" vs "What"

DIDs say who **you are**

UCANs show what **you can do**

Under the Microscope 🔬

"Who" vs "What"

AuthN

DIDs say who **you are**

UCANs show what **you can do**

AuthZ

Under the Microscope 🔬

Teaser Token


```
{
    "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99",
    "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
    "exp": 9256939505,
    "nbf": 1639608293,
    "cap": {
        "nns://demouser.fission.name/public/notes/": {
            "wnfs/append": [{"mime": "image/png"}]
        }
    }
}
```

Under the Microscope 🔬

Teaser Token


```
{
    "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99",
    "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
    "exp": 9256939505,
    "nbf": 1639608293,
    "cap": {
        "nns://demouser.fission.name/public/notes/": {
            "wnfs/append": [{"mime": "image/png"}]
        }
    }
}
```

Under the Microscope 🔬

Teaser Token


```
{
    "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99",
    "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
    "exp": 9256939505,
    "nbf": 1639608293,
    "cap": {
        "nns://demouser.fission.name/public/notes/": {
            "wnfs/append": [{"mime": "image/png"}]
        }
    }
}
```

Under the Microscope 🔬

Teaser Token


```
{
    "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99",
    "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
    "exp": 9256939505,
    "nbf": 1639608293,
    "cap": {
        "nns://demouser.fission.name/public/notes/": {
            "wnfs/append": [{"mime": "image/png"}]
        }
    }
}
```

Under the Microscope 🔬

Teaser Token


```
{
    "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99",
    "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
    "exp": 9256939505,
    "nbf": 1639608293,
    "cap": {
        "nns://demouser.fission.name/public/notes/": {
            "wnfs/append": [{"mime": "image/png"}]
        }
    }
}
```

Under the Microscope 🔬

JWT → UCAN


```
{
    "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
    "aud": "did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",
    "nbf": 1639608293,
    "exp": 9256939505,
    "cap": {
        "nns://demouser.fission.name/public/photos/": {
            "store/overwrite": [{}]
        }
        "nns://demouser.fission.name/public/notes/": {
            "store/append": [{}]
        }
    },
    "prf": [
        "bafkreifhbe7hcm47j4wkvghwmbtgqtdt7laiwq2t6duoi4rhigrdtgyq7e",
        "bafkreigpbimktgowom47jv7frt3xvhb7ati4upgguykyn2cuunt32l63ya"
    ]
}
```

Under the Microscope 🔬

JWT → UCAN

Header

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

Payload

```
{
    "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
    "aud": "did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",
    "nbf": 1639608293,
    "exp": 9256939505,
    "cap": {
        "nns://demouser.fission.name/public/photos/": {
            "store/overwrite": [{}]
        }
        "nns://demouser.fission.name/public/notes/": {
            "store/append": [{}]
        }
    },
    "prf": [
        "bafkreifhbe7hcm47j4wkvghwmbtgqtdt7laiwq2t6duoi4rhigrdtgyq7e",
        "bafkreigpbimktgowom47jv7frt3xvhb7ati4upgguykyn2cuunt32l63ya"
    ]
}
```

Signature

```
"kwRdqPN74pkcpXGgdk
7Z7FW3M1mRRYaDE5ZgX
G6srAuu6V6mvMVRdBLn
D5CWid-X4tDIKpliVjl
CSLTntB4pCw"
```

Under the Microscope 🔬

JWT → UCAN

Header

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

Payload

```
{
    "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
    "aud": "did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",
    "nbf": 1639608293,
    "exp": 9256939505,
    "cap": {
        "nns://demouser.fission.name/public/photos/": {
            "store/overwrite": [{}]
        }
        "nns://demouser.fission.name/public/notes/": {
            "store/append": [{}]
        }
    },
    "prf": [
        "bafkreifhbe7hcm47j4wkvghwmbtgqtdt7laiwq2t6duoi4rhigrdtgyq7e",
        "bafkreigpbimktgowom47jv7frt3xvhb7ati4upgguykyn2cuunt32l63ya"
    ]
}
```

✅

Signature

```
"kwRdqPN74pkcpXGgdk
7Z7FW3M1mRRYaDE5ZgX
G6srAuu6V6mvMVRdBLn
D5CWid-X4tDIKpliVjl
CSLTntB4pCw"
```

Under the Microscope 🔬

JWT → UCAN

Header

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

Payload

```
{
    "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
    "aud": "did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",
    "nbf": 1639608293,
    "exp": 9256939505,
    "cap": {
        "nns://demouser.fission.name/public/photos/": {
            "store/overwrite": [{}]
        }
        "nns://demouser.fission.name/public/notes/": {
            "store/append": [{}]
        }
    },
    "prf": [
        "bafkreifhbe7hcm47j4wkvghwmbtgqtdt7laiwq2t6duoi4rhigrdtgyq7e"
        "bafkreigpbimktgowom47jv7frt3xvhb7ati4upgguykyn2cuunt32l63ya"
    ]
}
```

✅

Signature

```
"kwRdqPN74pkcpXGgdk
7Z7FW3M1mRRYaDE5ZgX
G6srAuu6V6mvMVRdBLn
D5CWid-X4tDIKpliVjl
CSLTntB4pCw"
```

Under the Microscope 🔬

Anatomy of a Capability

Under the Microscope 🔬

Anatomy of a Capability

Under the Microscope 🔬

Anatomy of a Capability

Under the Microscope 🔬

Anatomy of a Capability

Under the Microscope 🔬

Stop 👏 Moving 👏 Keys 👏

Under the Microscope 🔬

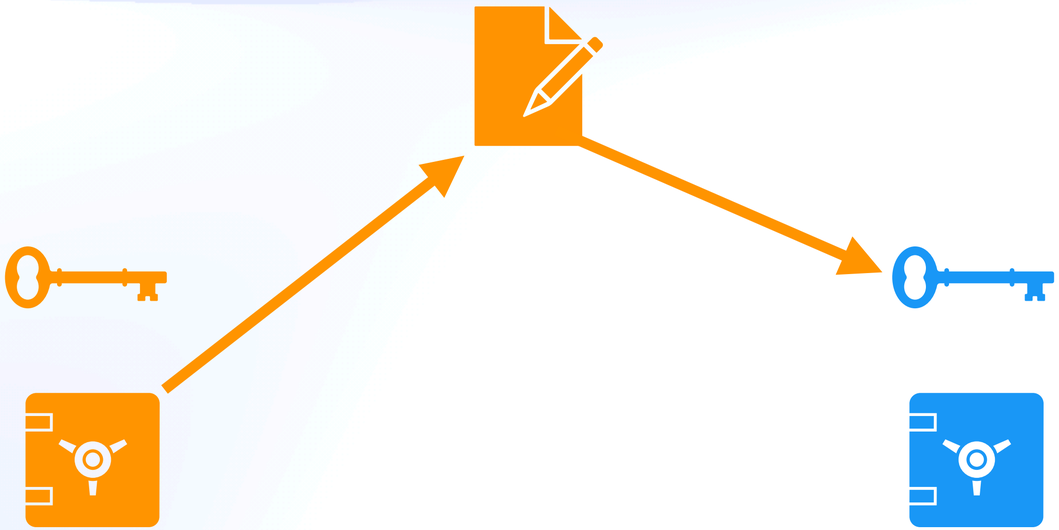
Stop 👏 Moving 👏 Keys 👏

Under the Microscope 🔬

Stop 👏 Moving 👏 Keys 👏

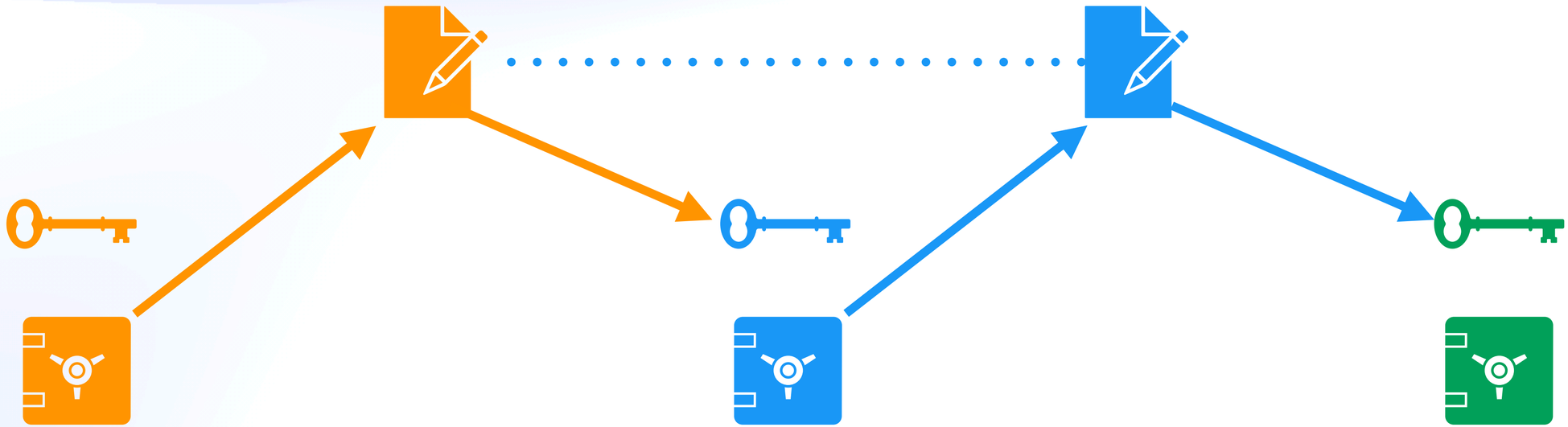
Under the Microscope 🔬

Stop 👏 Moving 👏 Keys 👏



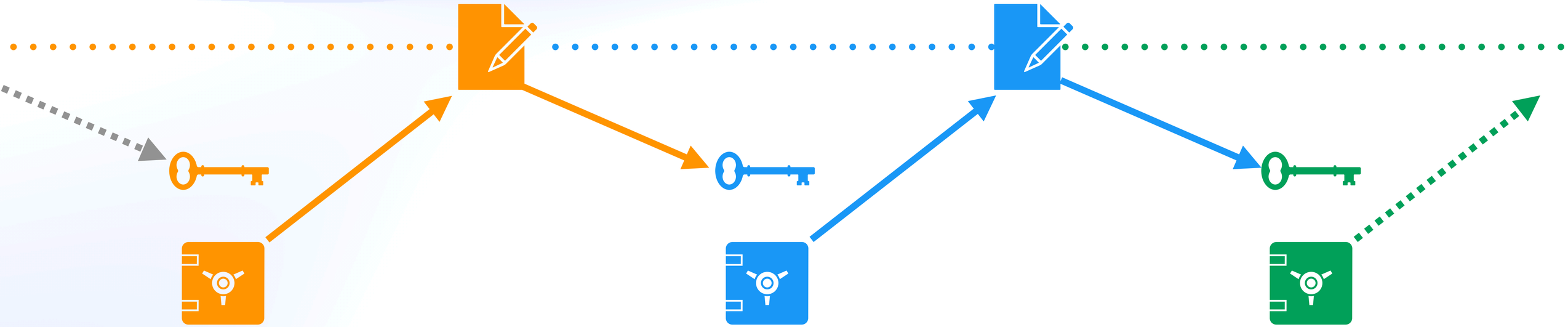
Under the Microscope 🔬

Stop 👏 Moving 👏 Keys 👏



Under the Microscope 🔬

Stop 👏 Moving 👏 Keys 👏



Under the Microscope 🔬

Attenuation

Under the Microscope 🔬

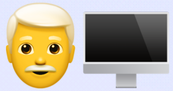
Attenuation

Under the Microscope 🔬

Attenuation

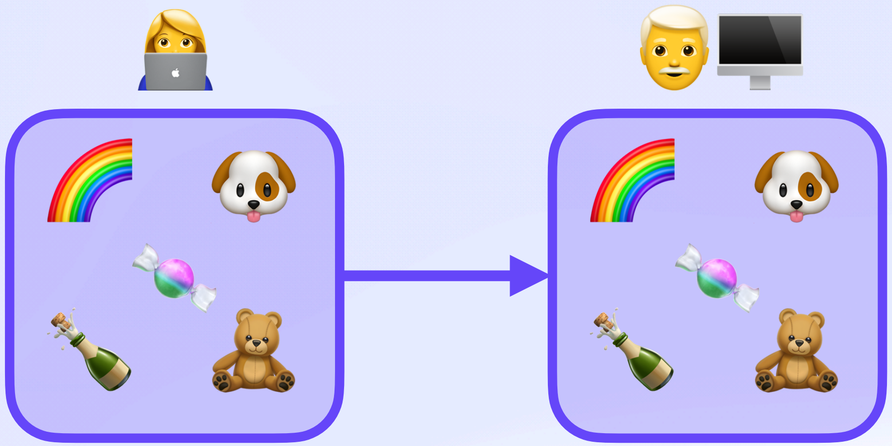
Under the Microscope 🔬

Attenuation



Under the Microscope 🔬

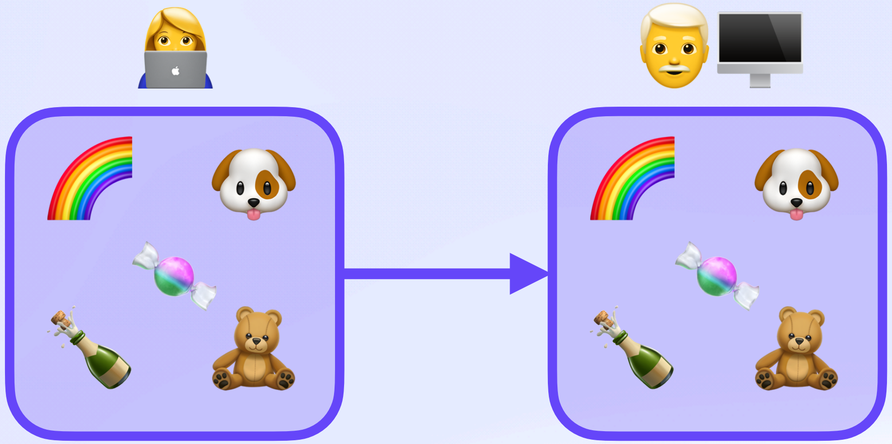
Attenuation



Under the Microscope 🔬

Attenuation

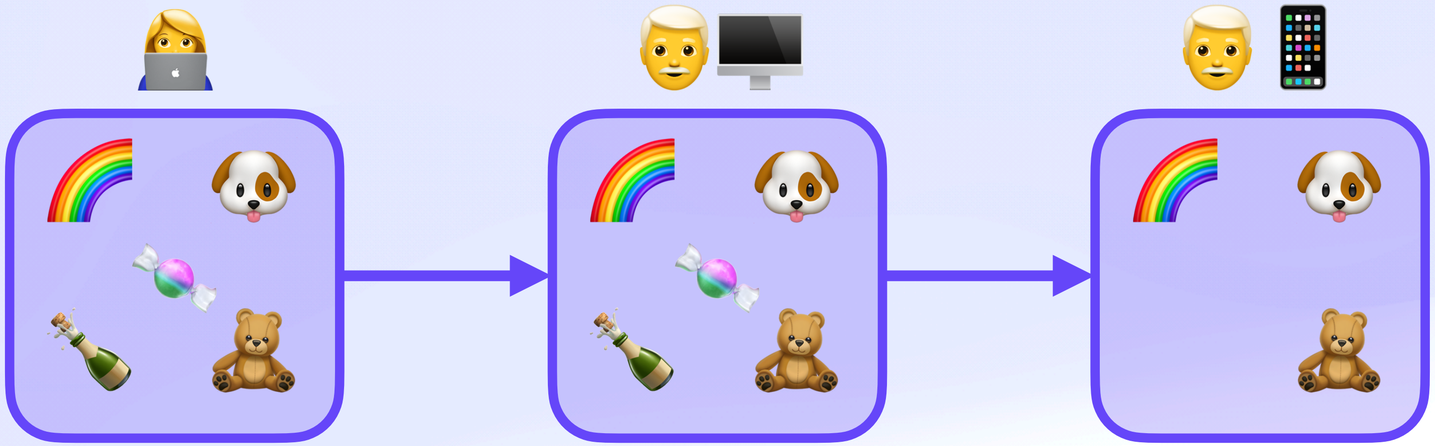
```
"prf": [
    "bafkreifhbe7hcm47j4wkvghwmbtgqtdt7laiwq2t6duoi4rhigrdtgyq7e",
    "bafkreigpbimktgowom47jv7frt3xvhb7ati4upgguykyn2cuunt32l63ya"
]
```



Under the Microscope 🔬

Attenuation

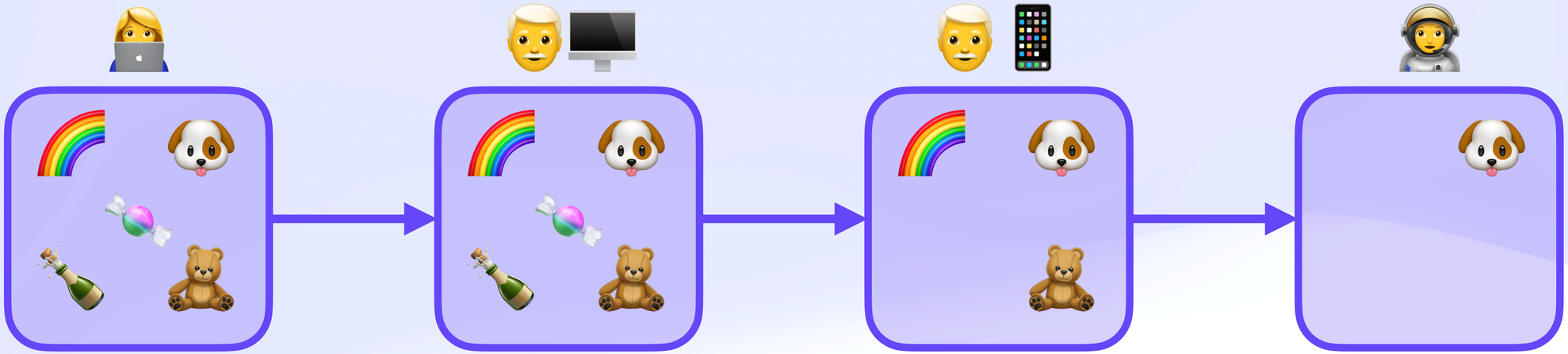
```
"prf": [
    "bafkreifhbe7hcm47j4wkvghwmbtgqtdt7laiwq2t6duoi4rhigrdtgyq7e",
    "bafkreigpbimktgowom47jv7frt3xvhb7ati4upgguykyn2cuunt32l63ya"
]
```



Under the Microscope 🔬

Attenuation

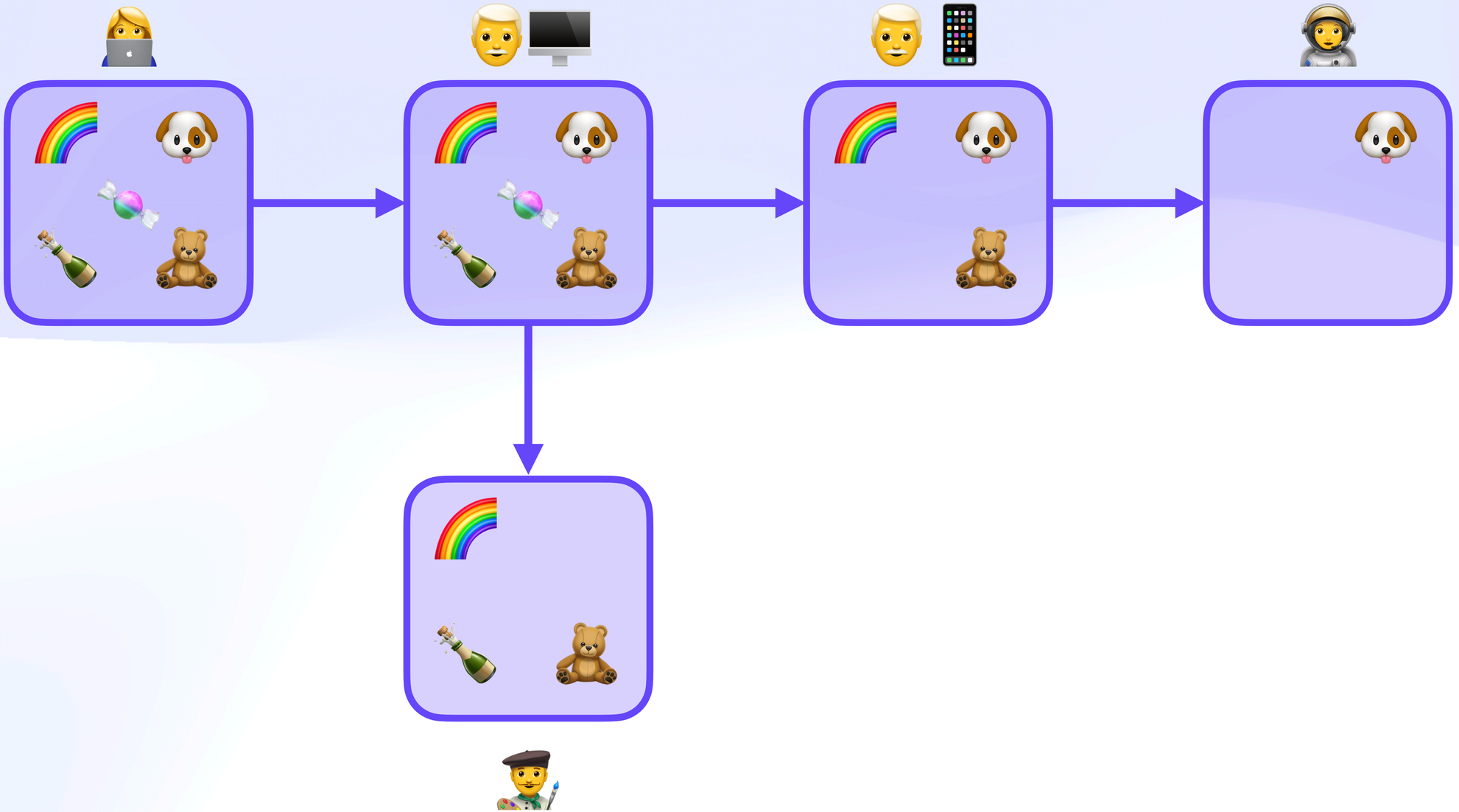
```
"prf": [
    "bafkreifhbe7hcm47j4wkvghwmbtgqtdt7laiwq2t6duoi4rhigrdtgyq7e",
    "bafkreigpbimktgowom47jv7frt3xvhb7ati4upgguykyn2cuunt32l63ya"
]
```



Under the Microscope 🔬

Attenuation

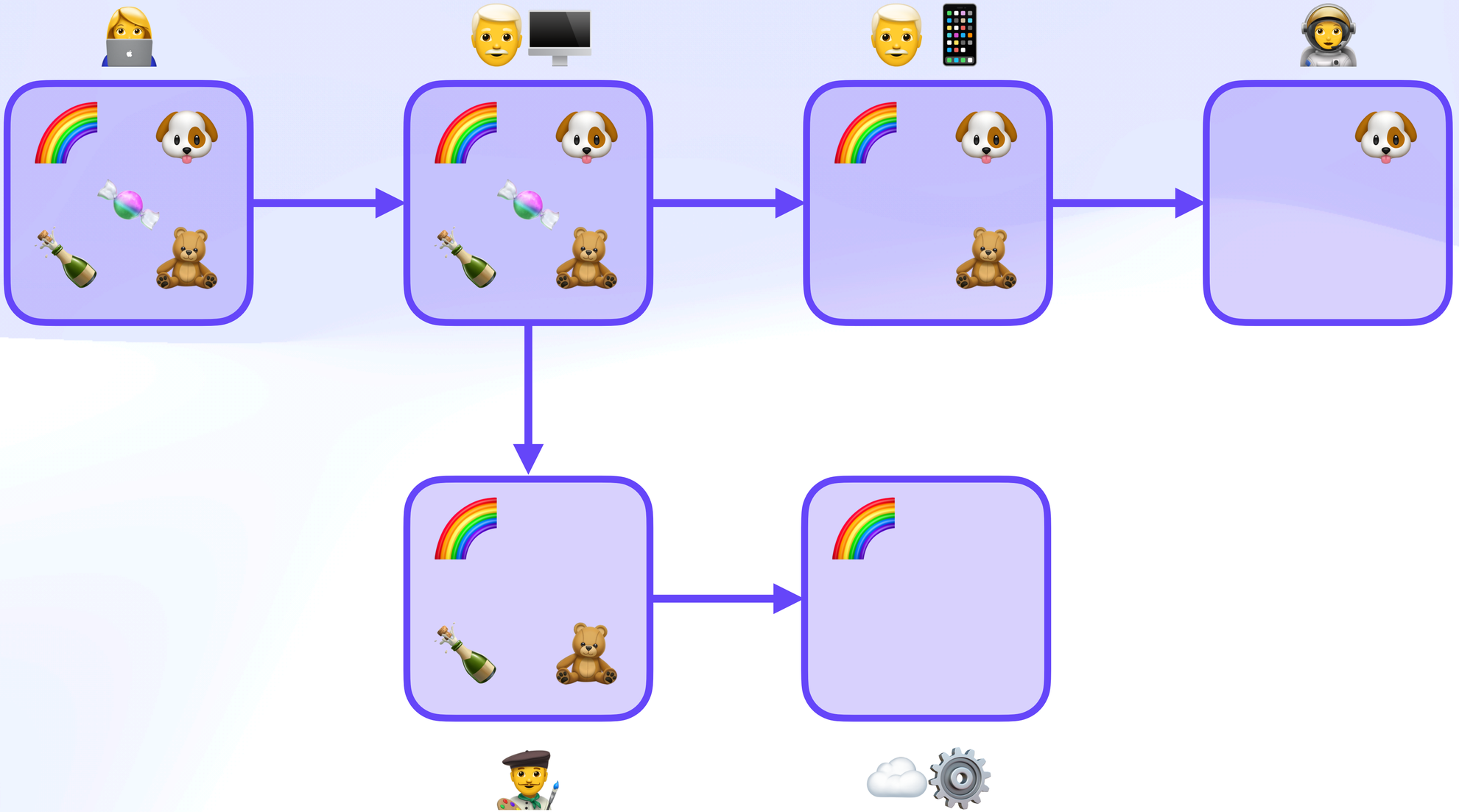
```
"prf": [
    "bafkreifhbe7hcm47j4wkvghwmbtgqtdt7laiwq2t6duoi4rhigrdtgyq7e",
    "bafkreigpbimktgowom47jv7frt3xvhb7ati4upgguykyn2cuunt32l63ya"
]
```



Under the Microscope 🔬

Attenuation

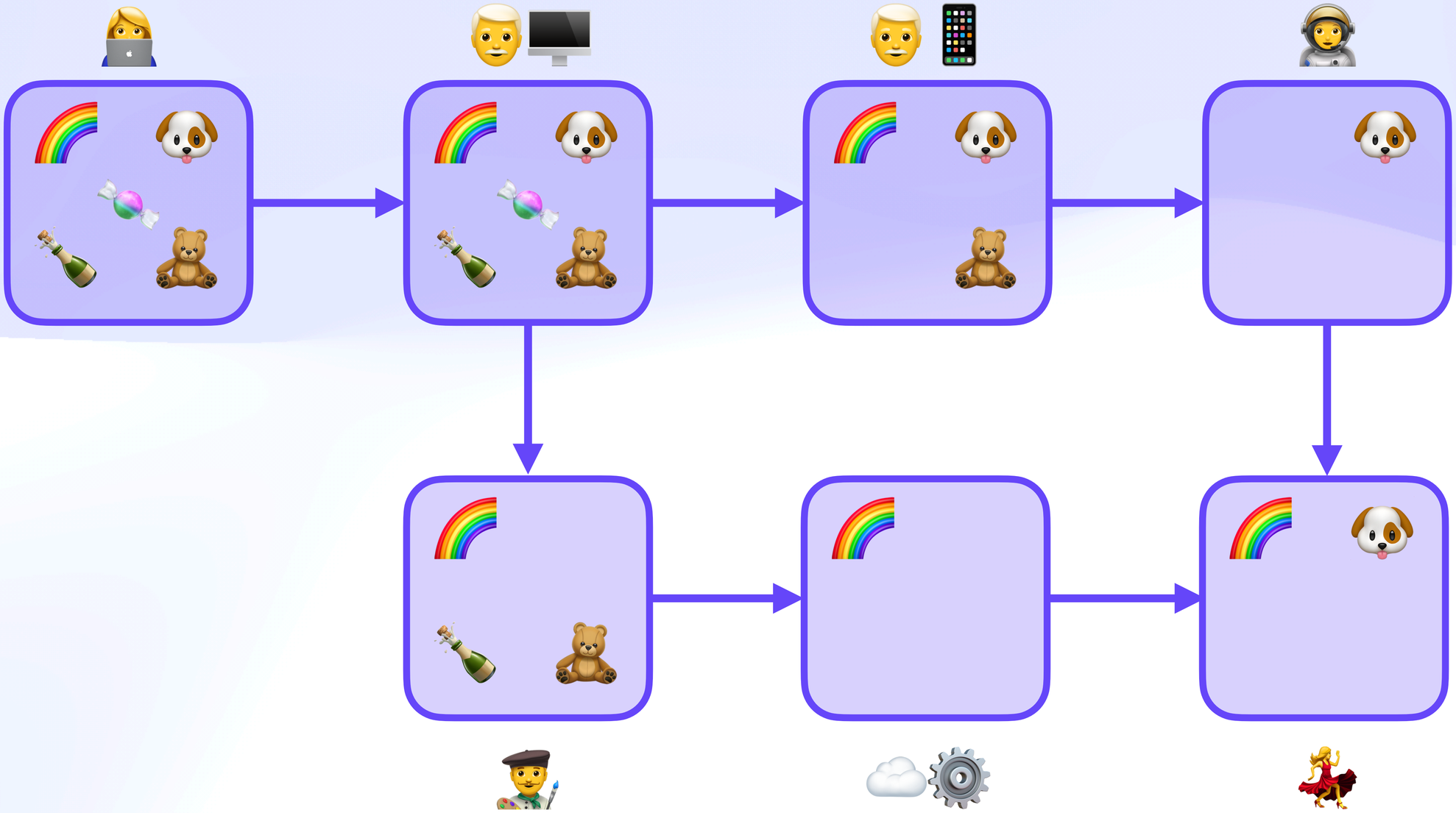
```
"prf": [
    "bafkreifhbe7hcm47j4wkvghwmbtgqtdt7laiwq2t6duoi4rhigrdtgyq7e",
    "bafkreigpbimktgowom47jv7frt3xvhb7ati4upgguykyn2cuunt32l63ya"
]
```



Under the Microscope 🔬

Attenuation

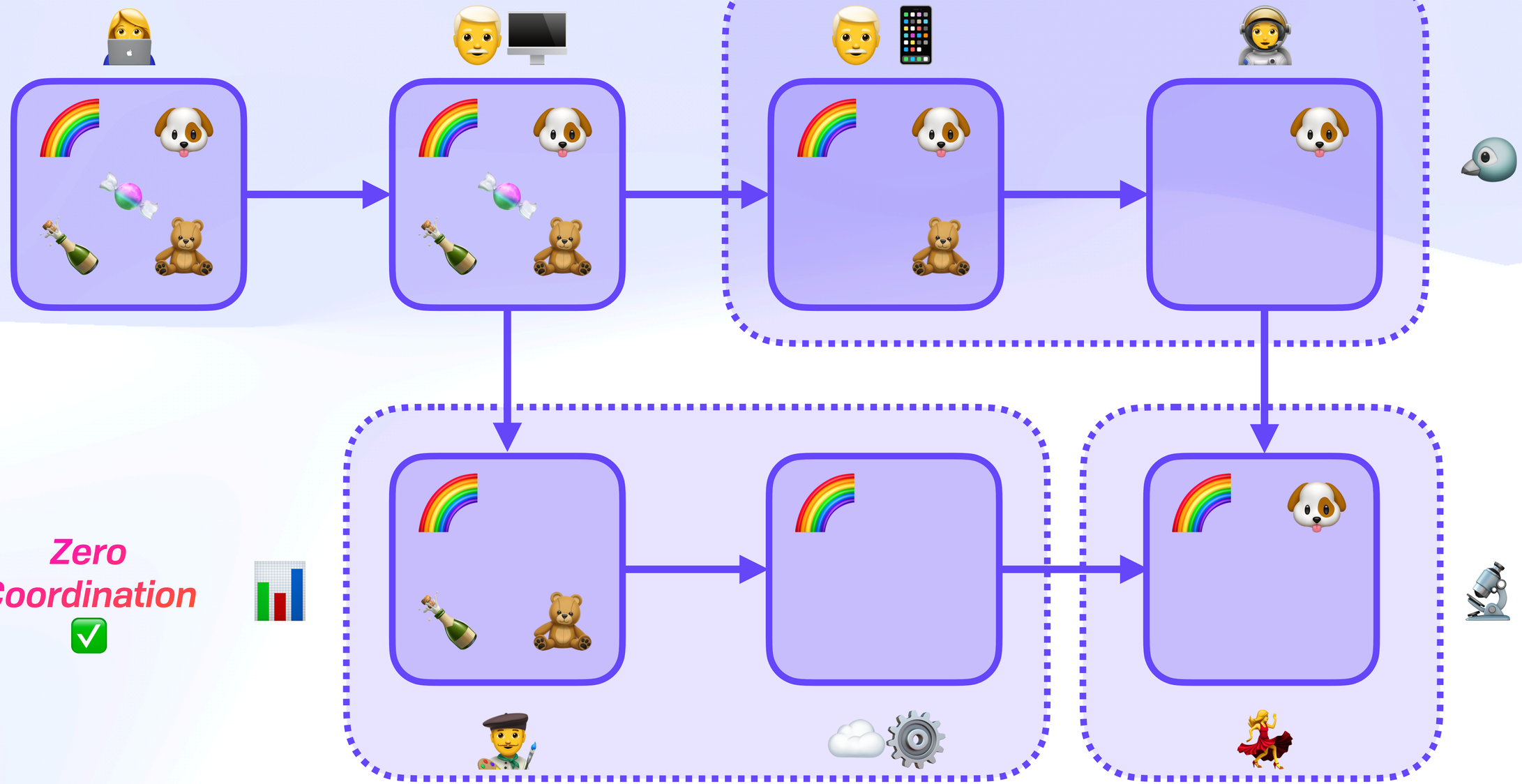
```
"prf": [
    "bafkreifhbe7hcm47j4wkvghwmbtgqtdt7laiwq2t6duoi4rhigrdtgyq7e",
    "bafkreigpbimktgowom47jv7frt3xvhb7ati4upgguykyn2cuunt32l63ya"
]
```



Under the Microscope

Attenuation

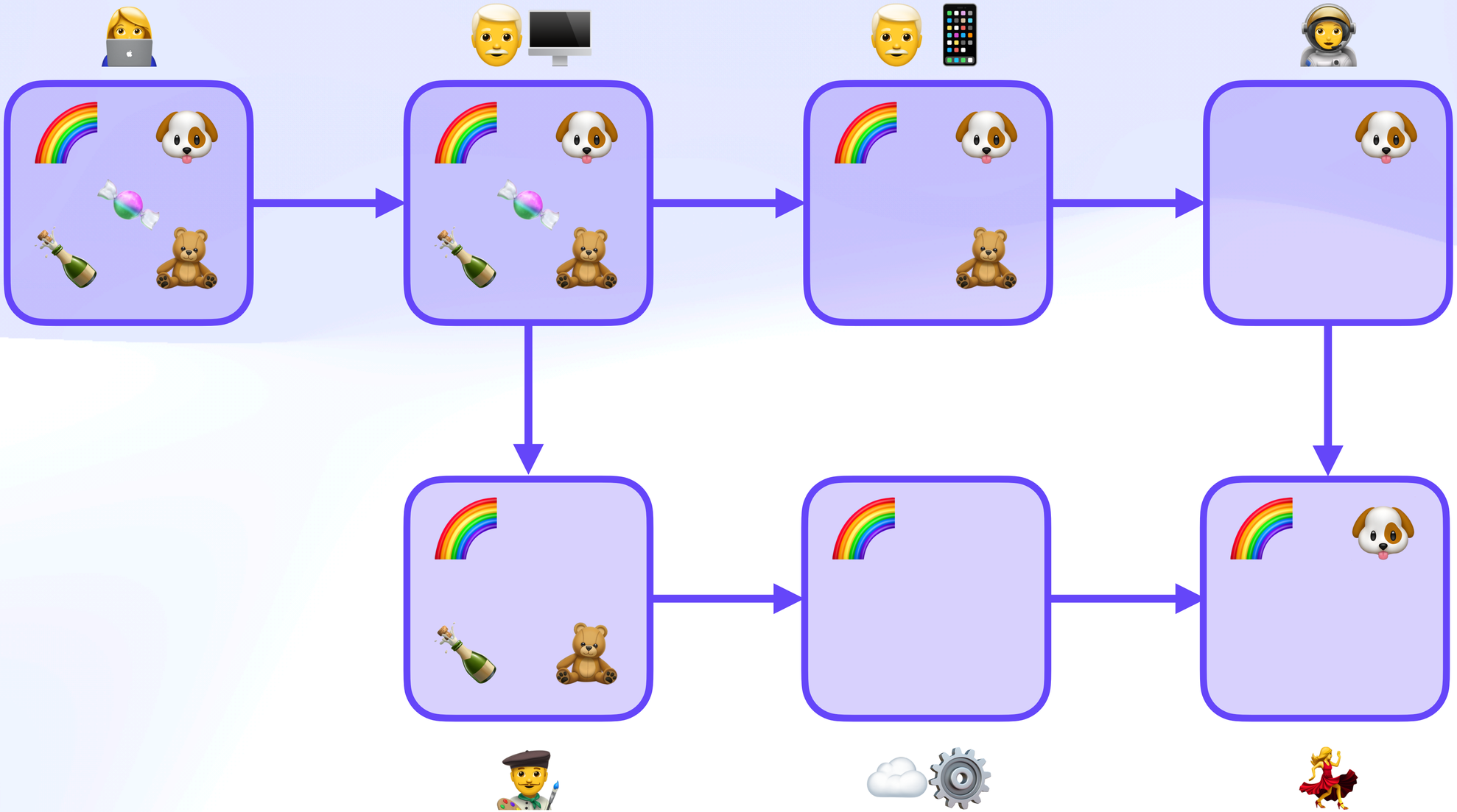
```
"prf": [
    "bafkreifhbe7hcm47j4wkvghwmbtgqtdt7laiwq2t6duoi4rhigrdtgyq7e",
    "bafkreigpbimktgowom47jv7frt3xvhb7ati4upgguykyn2cuunt32l63ya"
]
```



Zero Coordination ✅

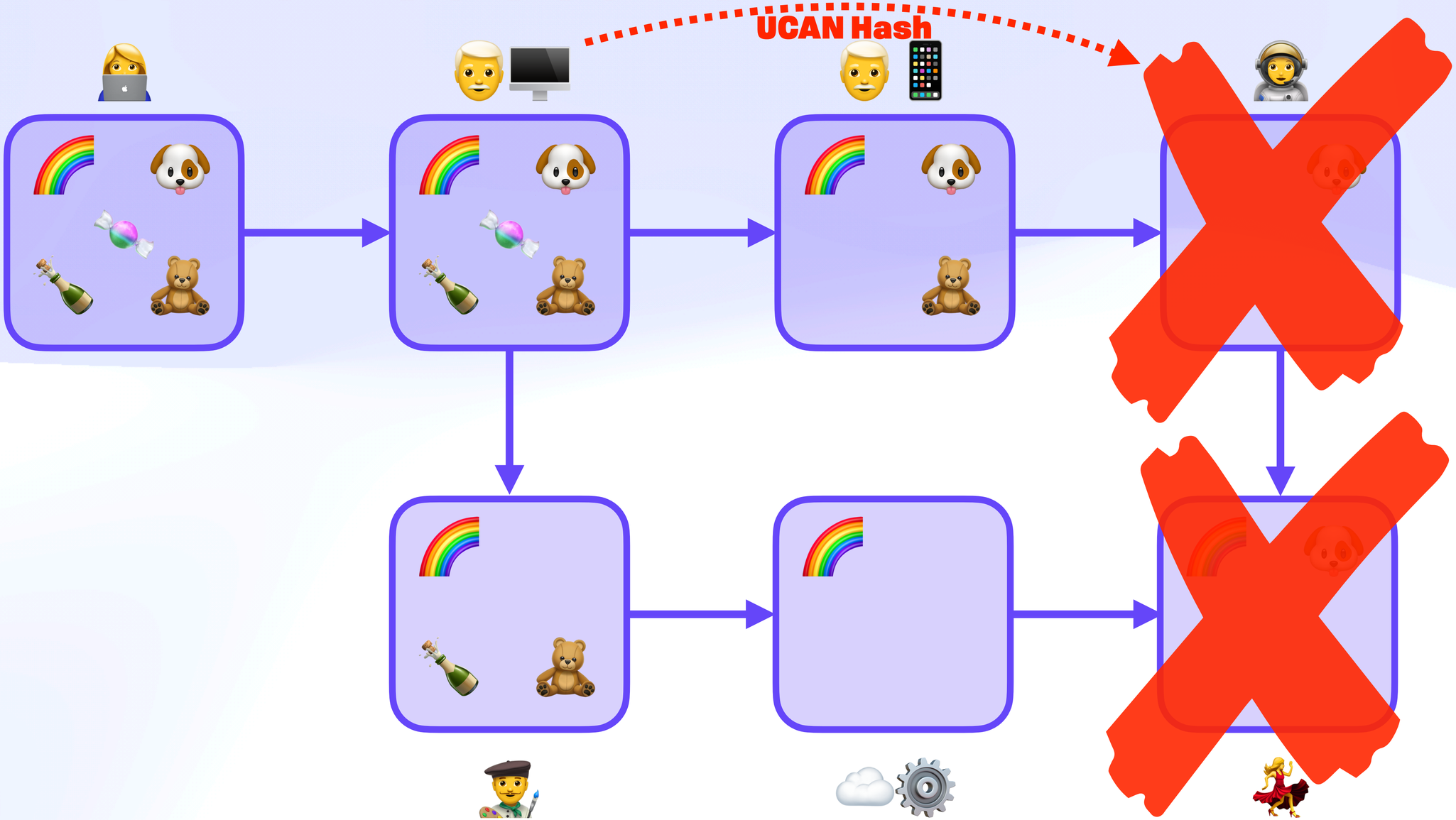
Under the Microscope 🔬

Revocation Cascade



Under the Microscope 🔬

Revocation Cascade



Under the Microscope 🔬

Composable Standard Library

Under the Microscope 🔬

Composable Standard Library

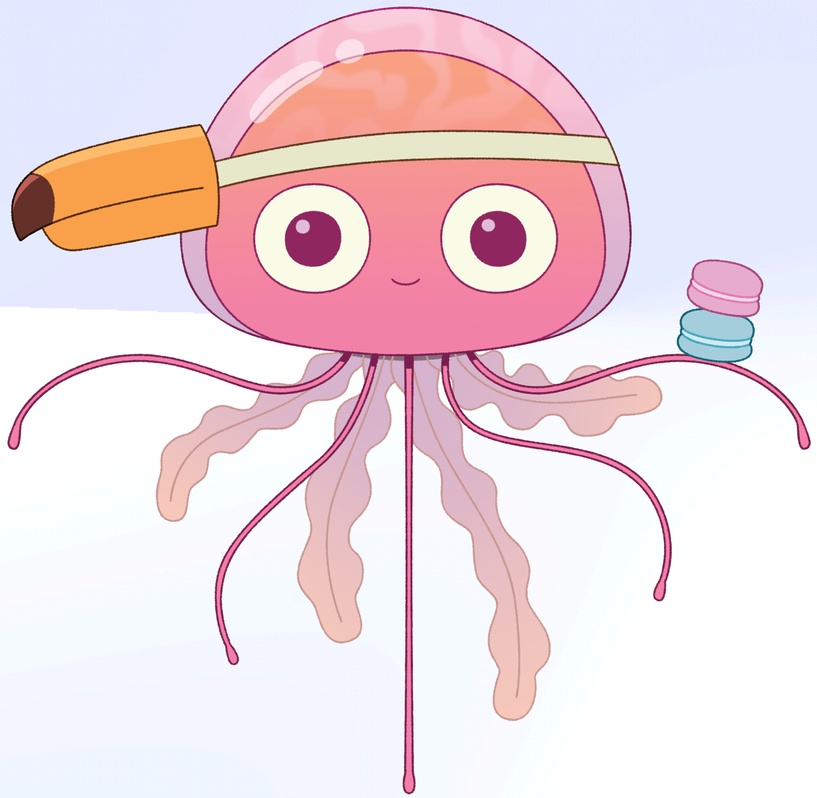
Resource (URI)	Ability (Cap)
https:	crud/create
mailto:	crud/read
file:	crud/update
wnfs:	crud/destroy
dns:	
news:	msg/send
	msg/receive
	group/ban
	group/join

Under the Microscope 🔬

`ucan-ipld` & CACAO

Under the Microscope 🔬

ucan-ipld & CACAO



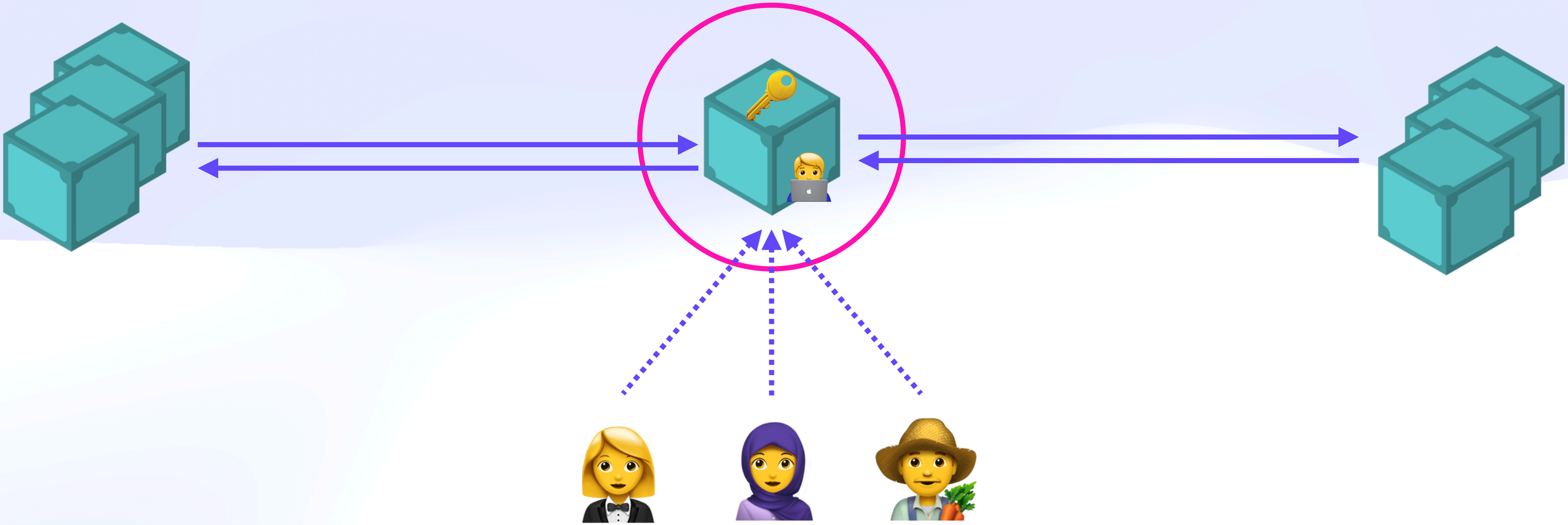
```
type UCAN struct {
  v String

  iss Principal
  aud Principal
  s Signature

  att [Capability]
  prf [&UCAN]
  exp Int

  fct [Fact]
  nnc optional String
  nbf optional Int
} representation map {
  field fct default []
  field prf default []
}
```

github.com/ucan-wg/ucan-ipld

Solving the Case Study

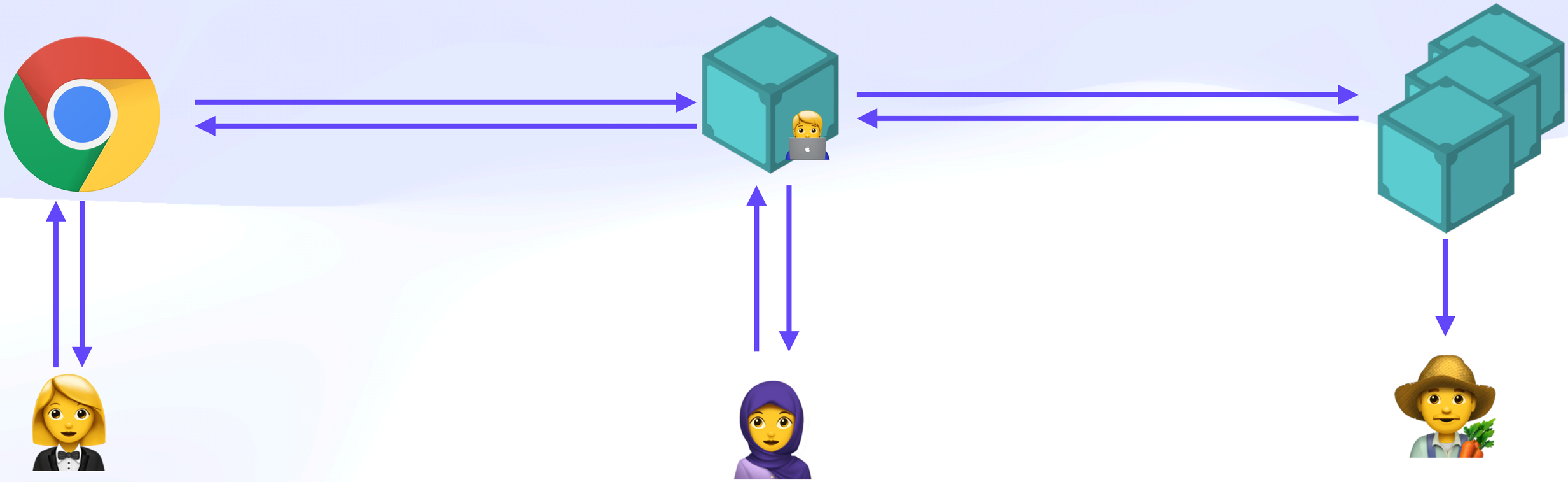
Solving the Case Study 🕵️

Case Study: IPNS



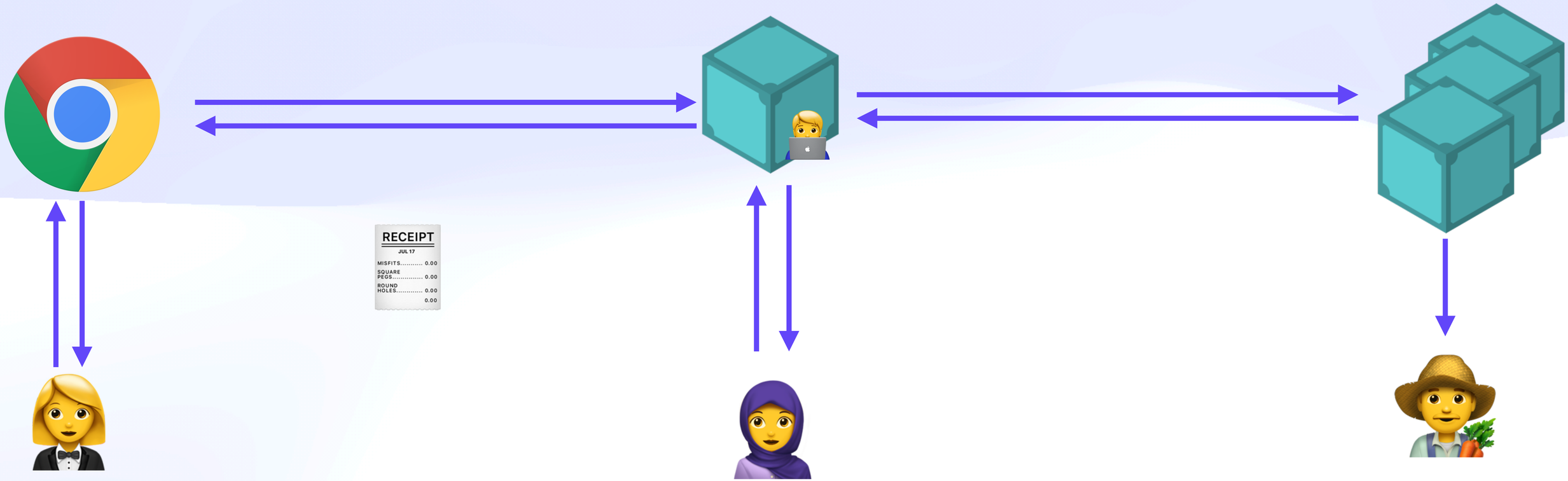
Solving the Case Study 🕵️

Case Study: NNS



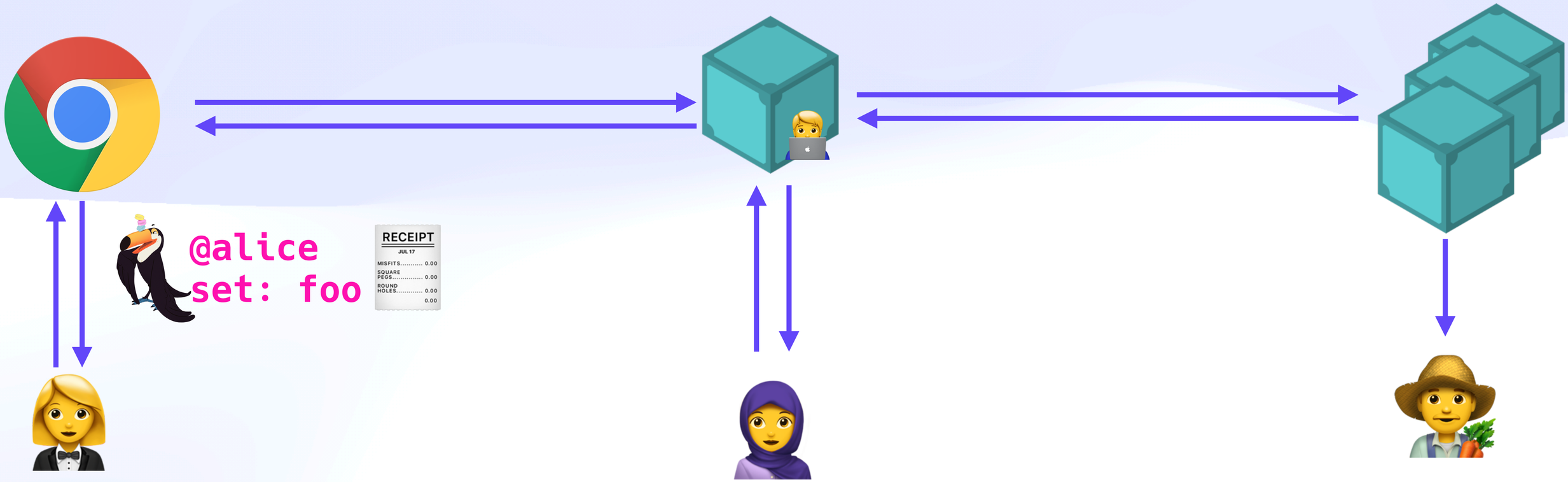
Solving the Case Study 🕵️

Case Study: NNS



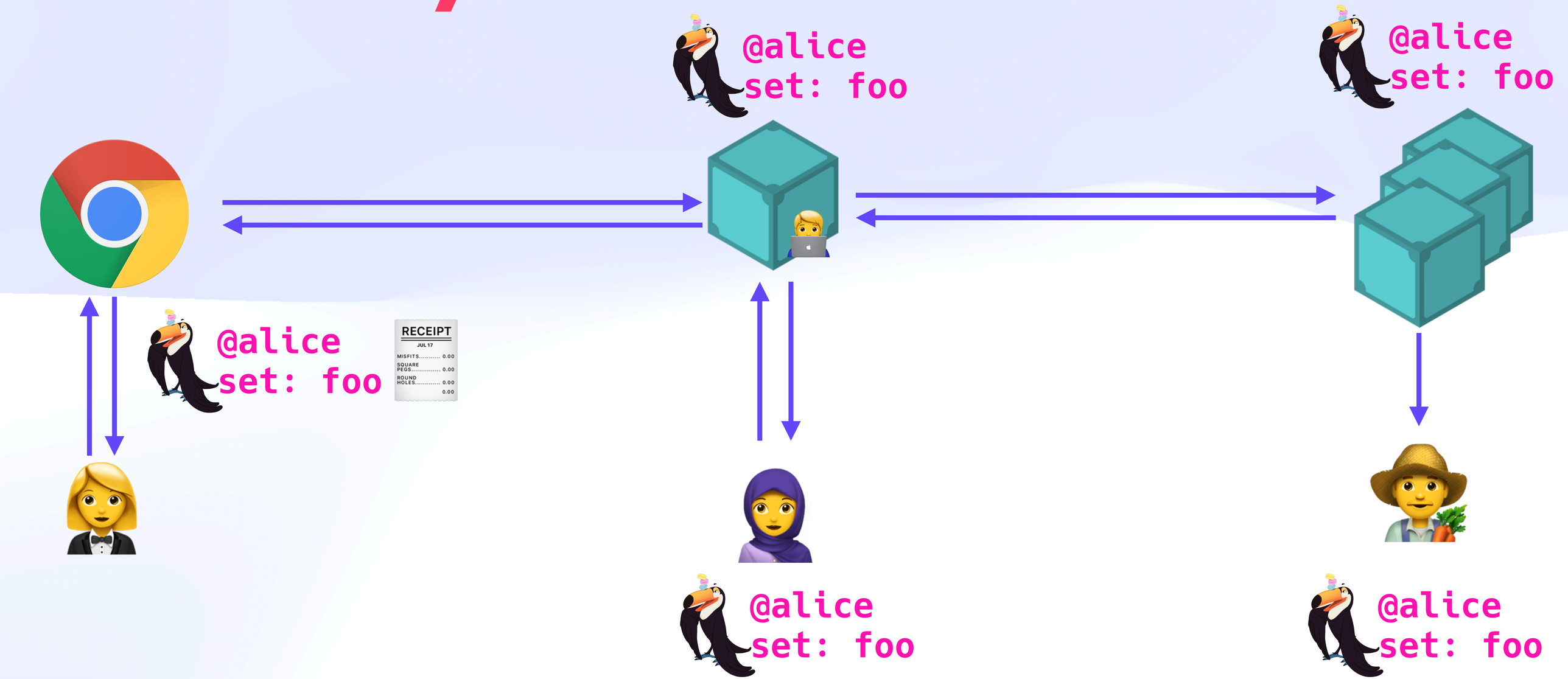
Solving the Case Study 🕵️

Case Study: NNS



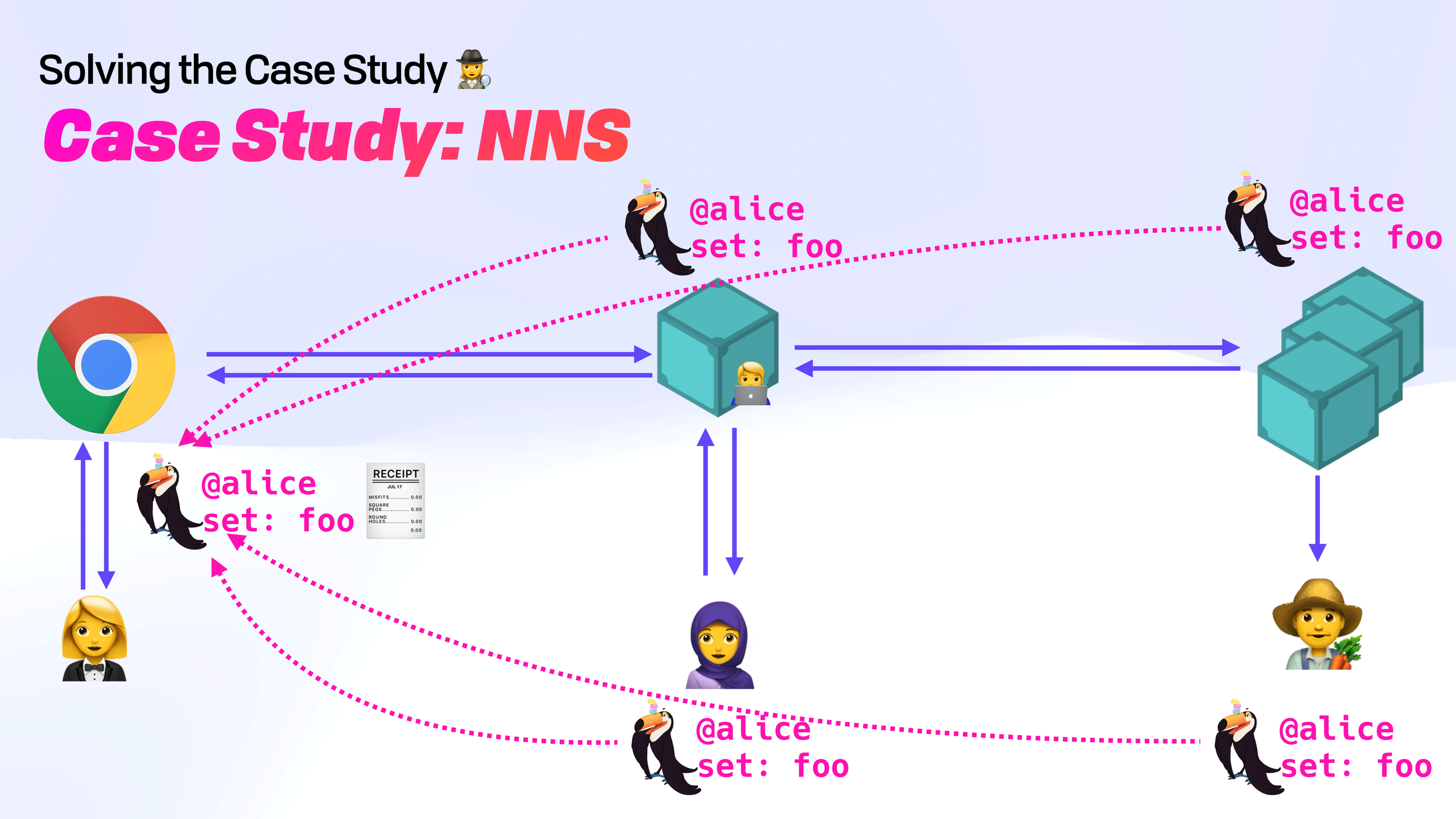
Solving the Case Study 🕵️

Case Study: NNS



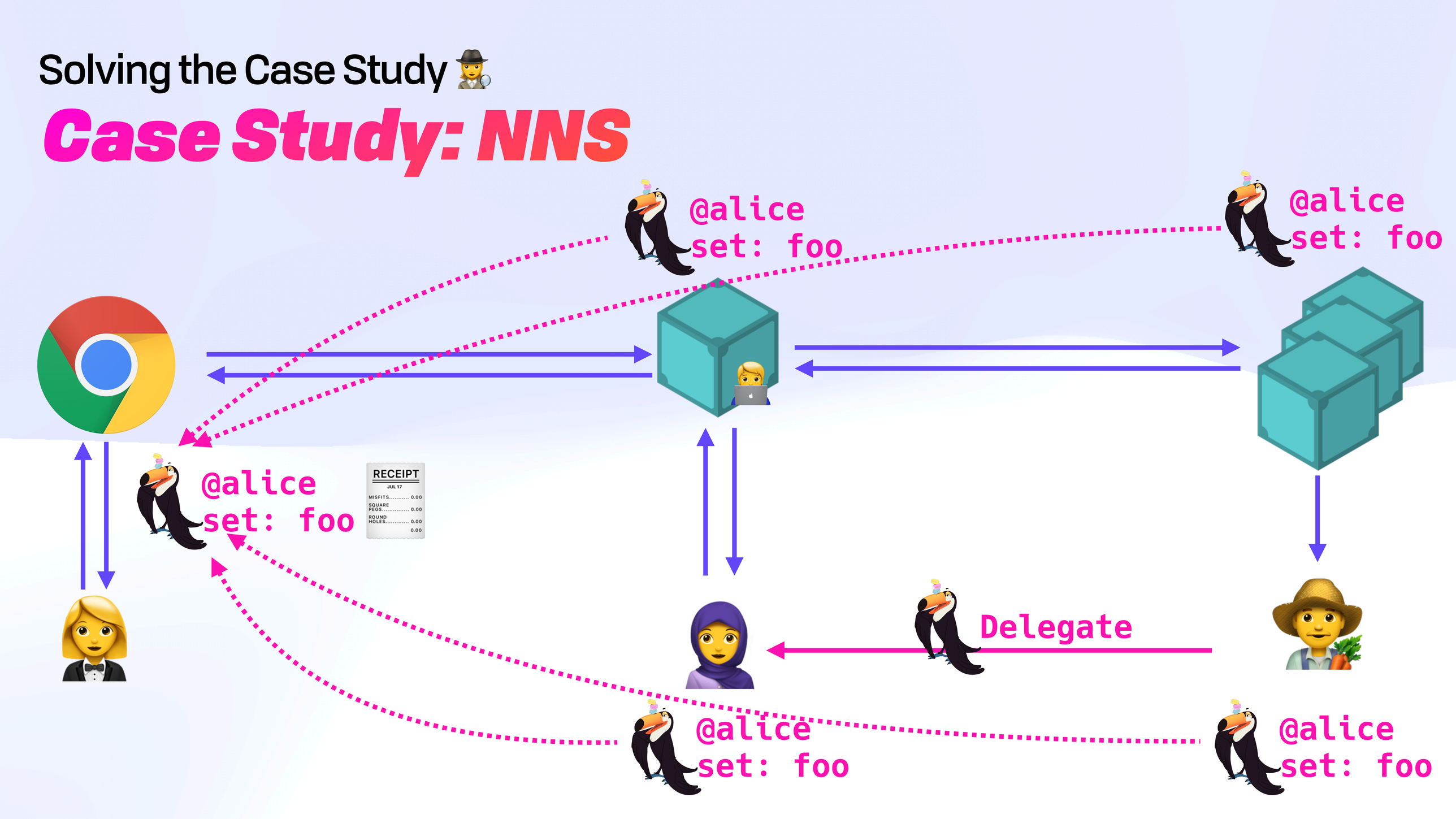
Solving the Case Study 🕵️

Case Study: NNS



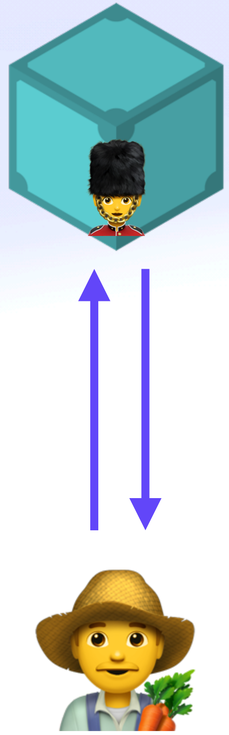
Solving the Case Study 🕵️

Case Study: NNS



Solving the Case Study 🕵️

Authorised Data Retrieval



Solving the Case Study 🕵️

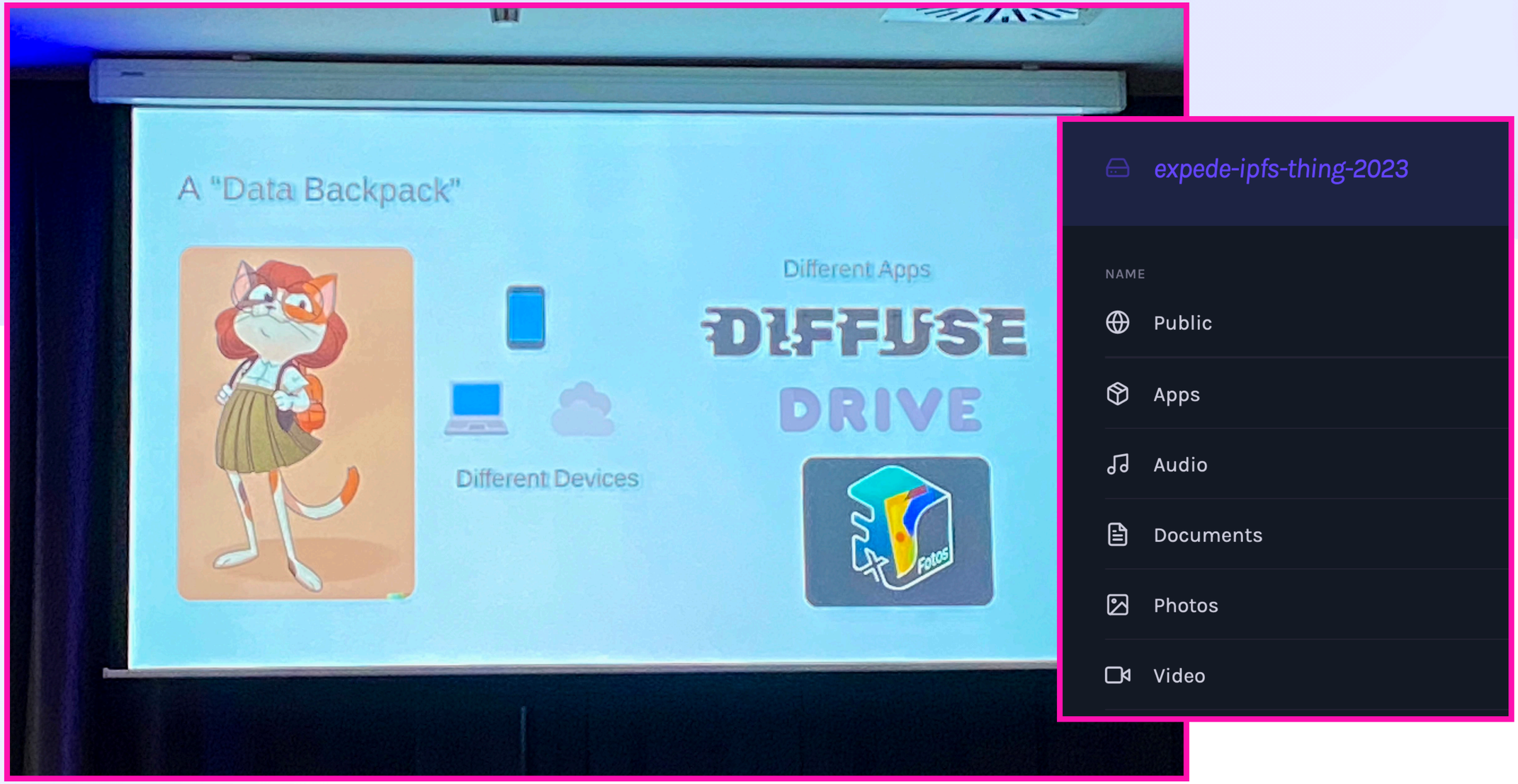
Authorised Data Retrieval

Solving the Case Study 🕵️

User Controlled Apps: IPFS ❤️ UCAN

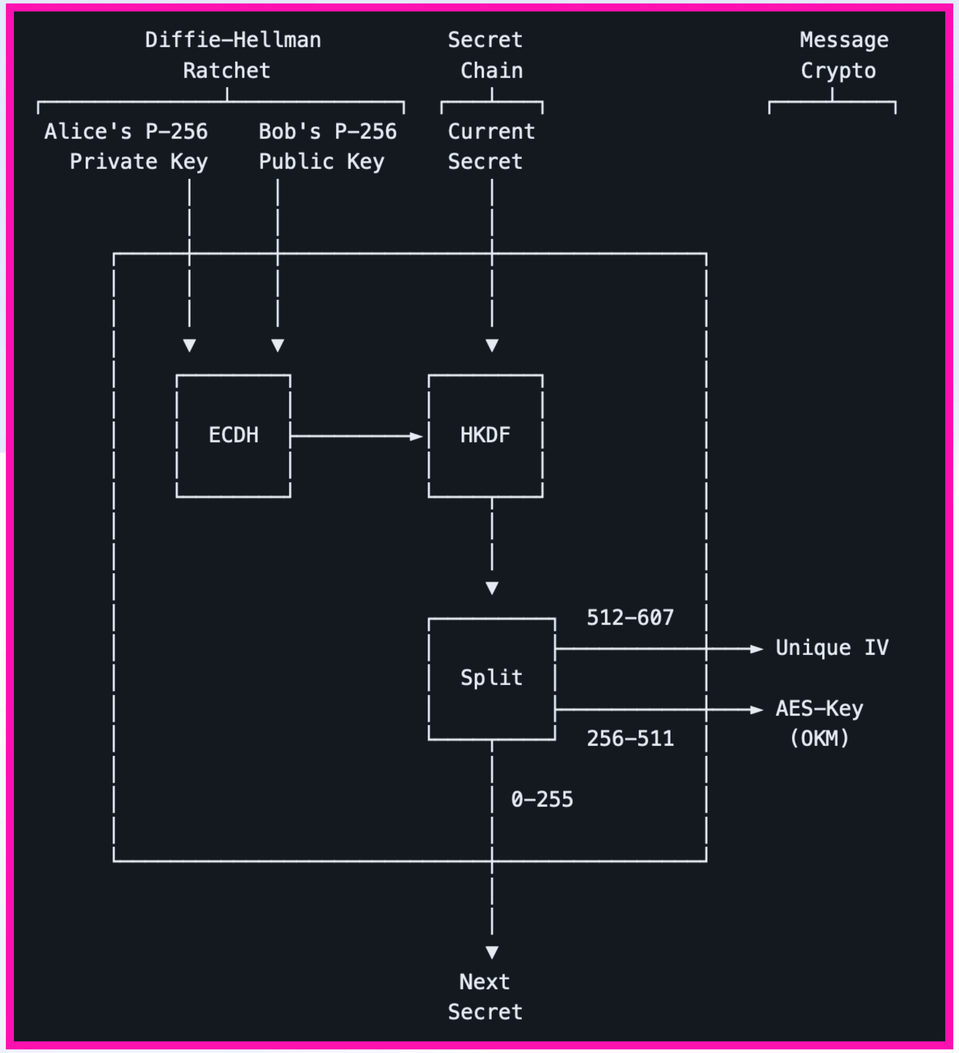
Solving the Case Study 🕵️

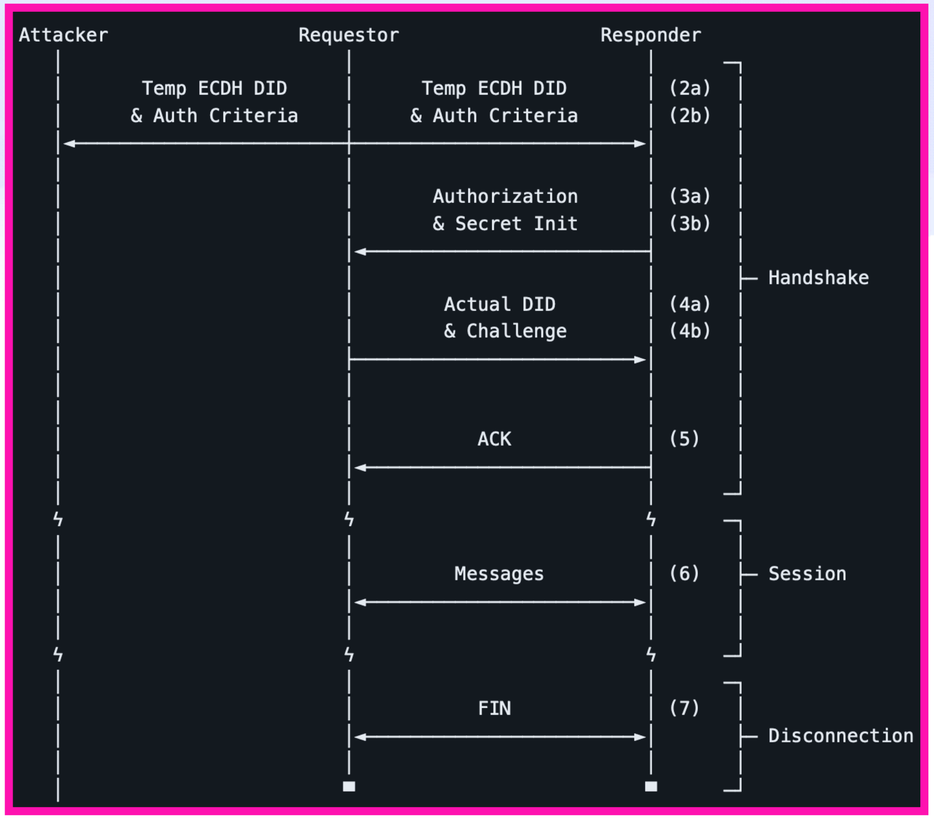
User Controlled Apps: IPFS ❤️ UCAN



Solving the Case Study 🕵️

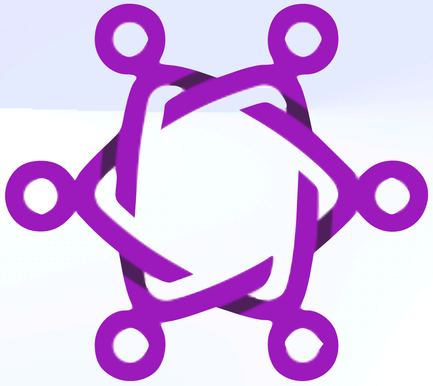
AWAKE: Authorised Channels

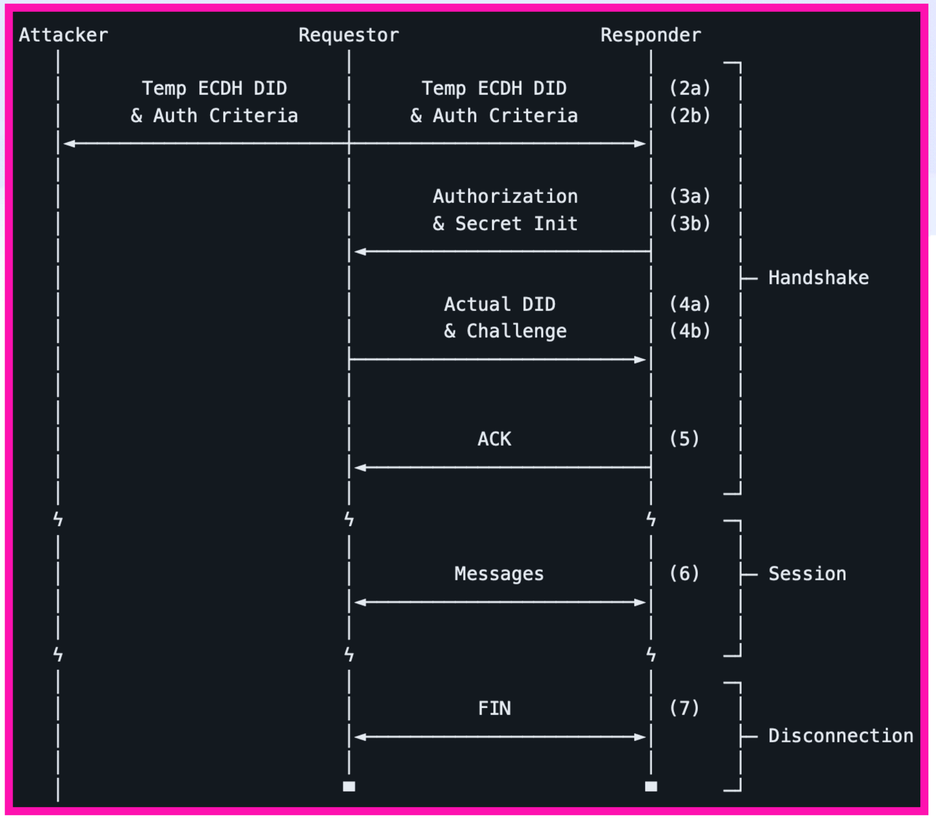




Solving the Case Study 🕵️

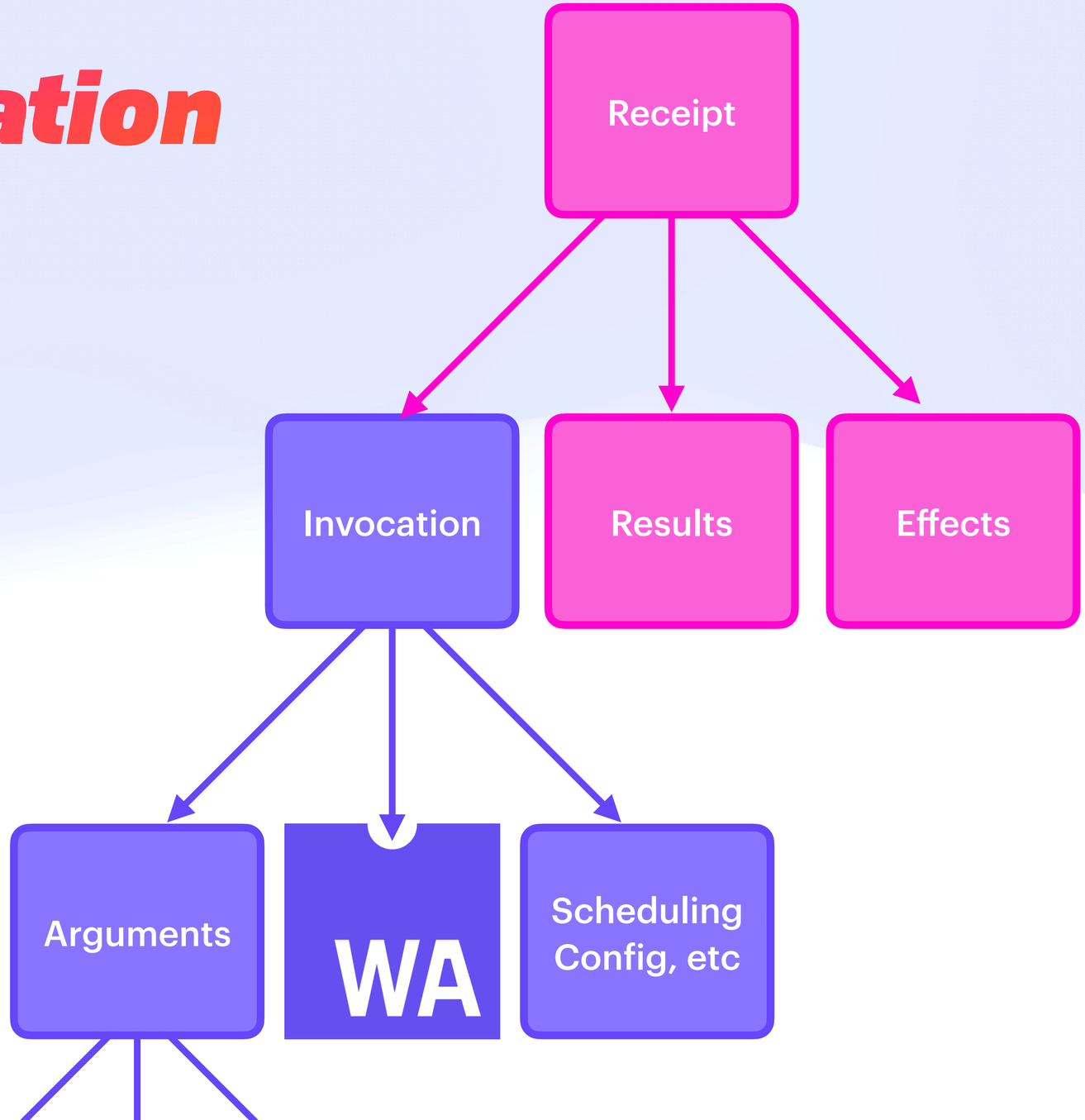
AWAKE: Authorised Channels





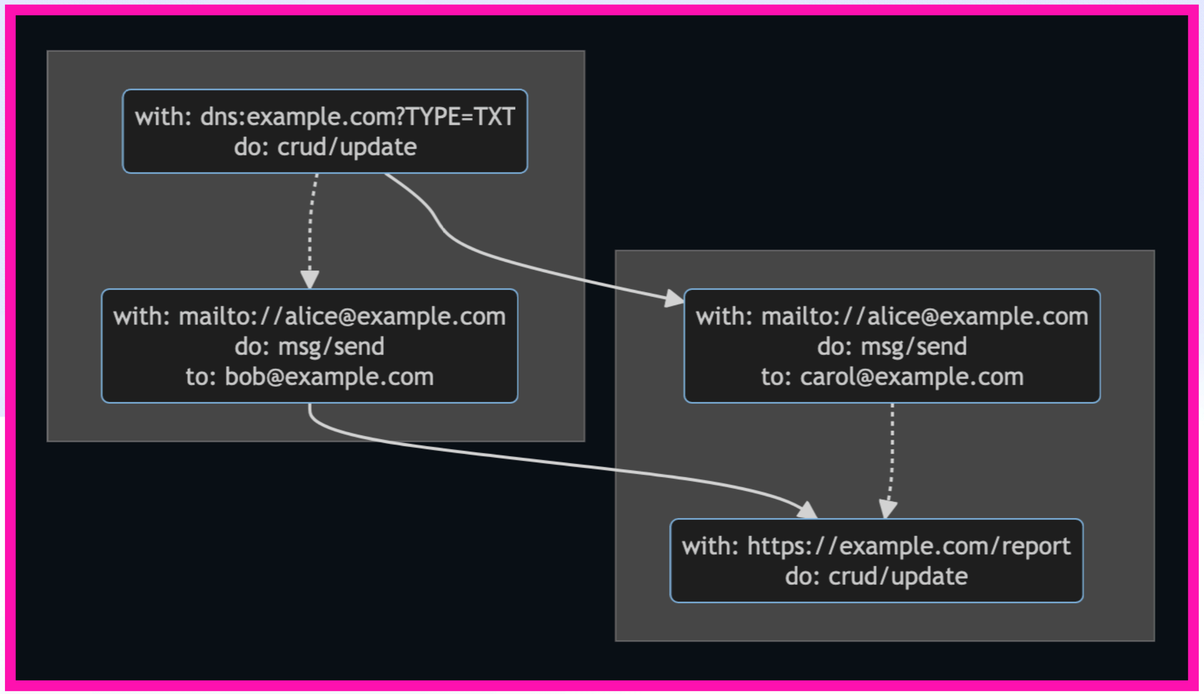
Solving the Case Study 🕵️

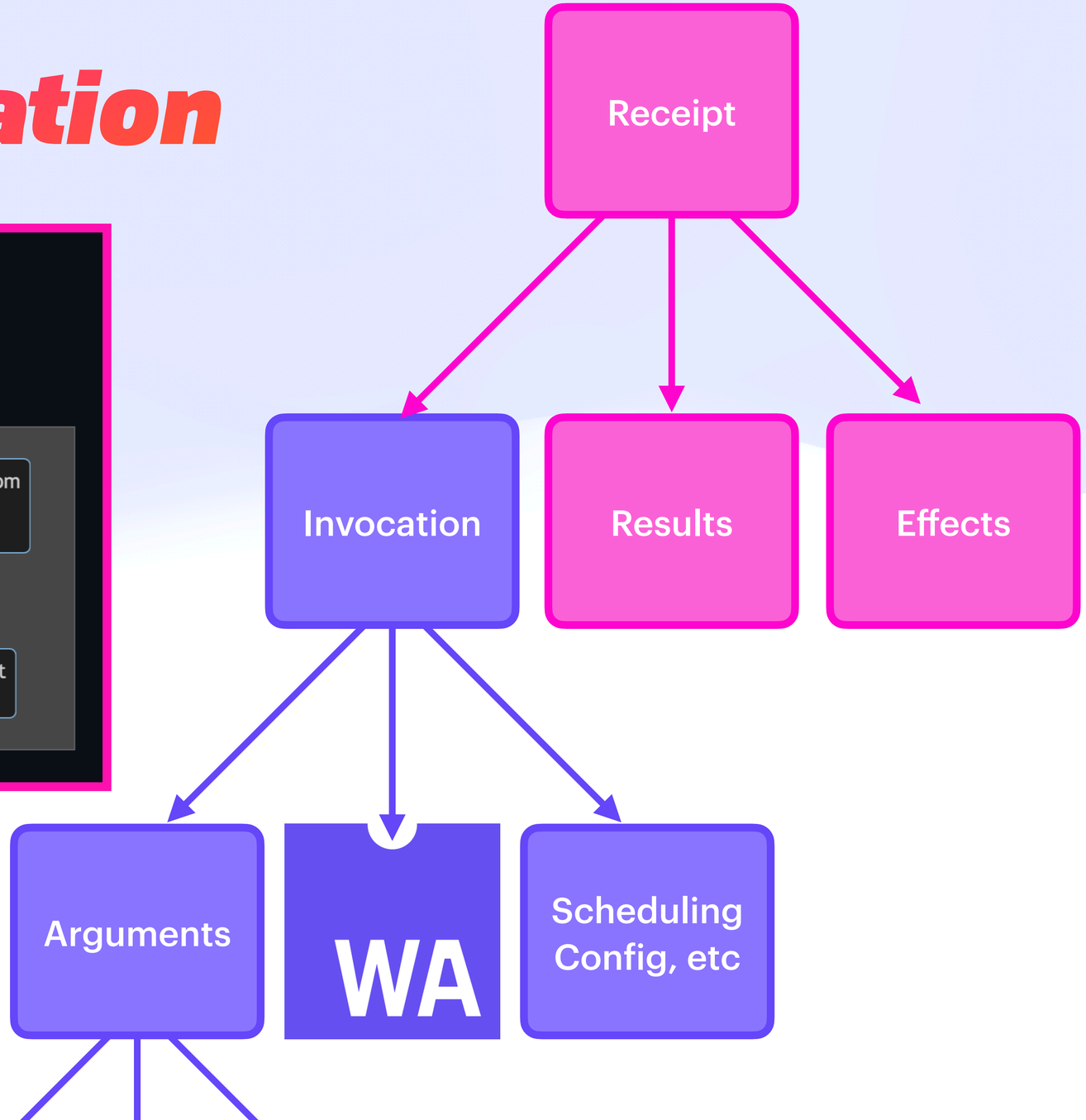
Distributed Invocation



Solving the Case Study 🕵️

Distributed Invocation





Resources

Resources 📚

Further Reading

Resources 📚

Further Reading

- **Community**: https://github.com/ucan-wg

Resources 📚

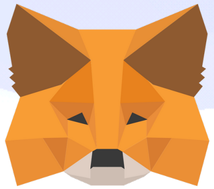
Further Reading

- **Community**: https://github.com/ucan-wg

Resources 📚

Further Reading

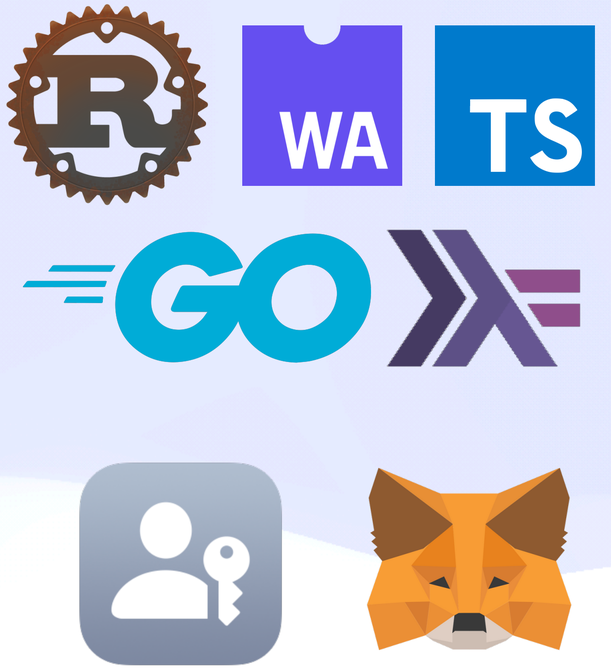
- **Community**: https://github.com/ucan-wg

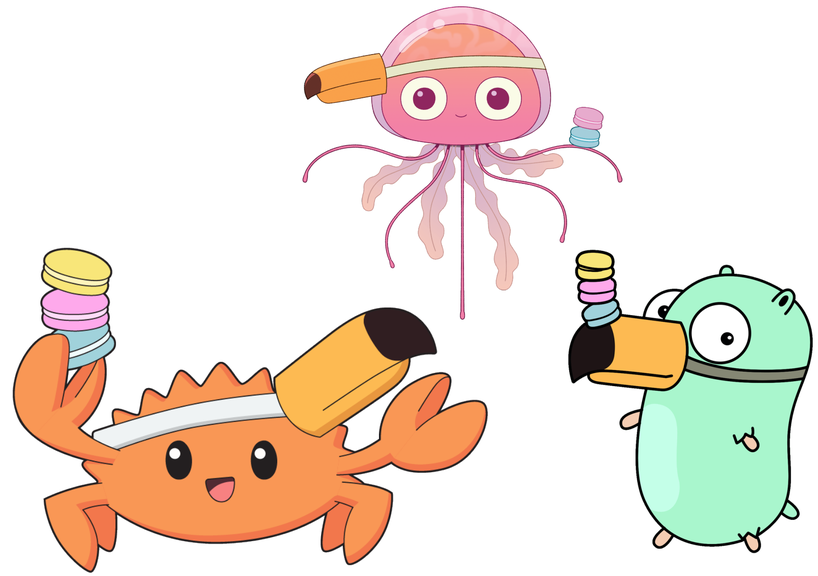


Resources 📚

Further Reading

- **Community**: https://github.com/ucan-wg

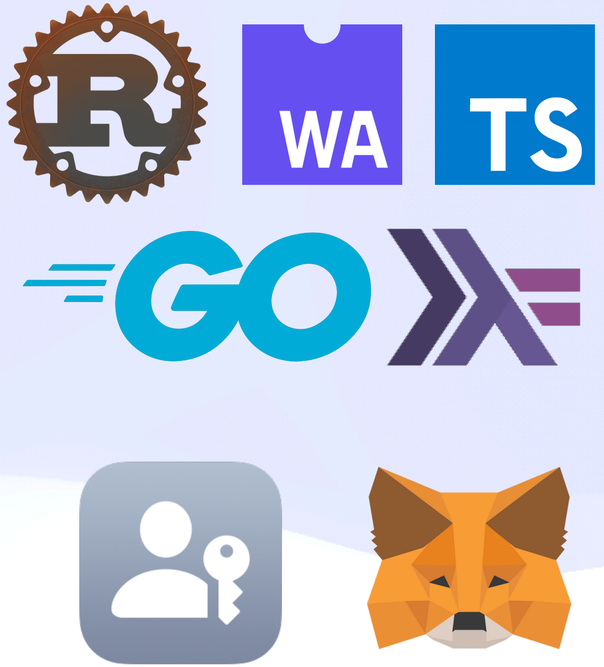




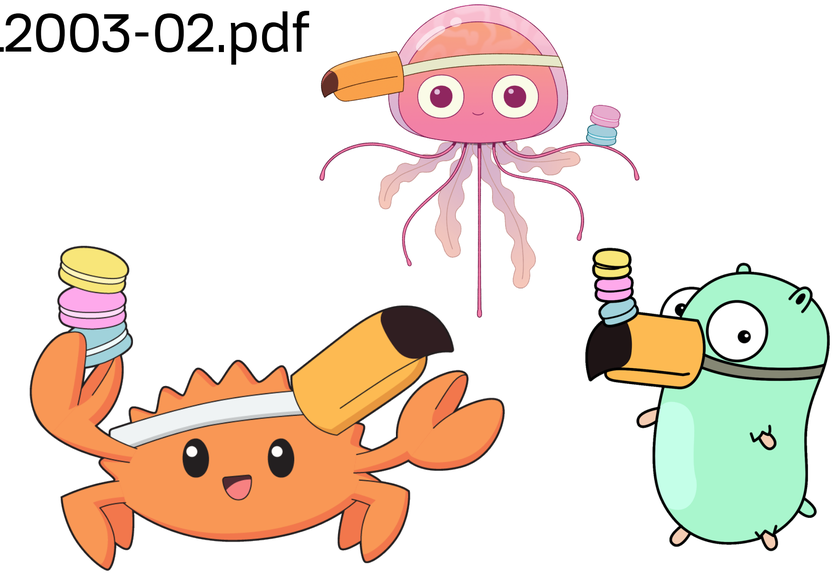
Resources 📚

Further Reading

- **Community**: https://github.com/ucan-wg



- **Capability Myths Demolished**: https://srl.cs.jhu.edu/pubs/SRL2003-02.pdf

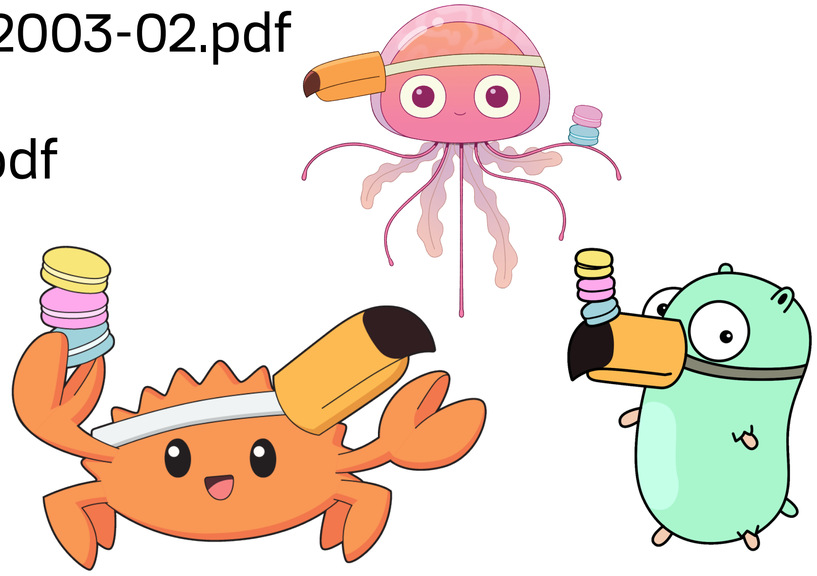


Resources 📚

Further Reading

- **Community**: https://github.com/ucan-wg

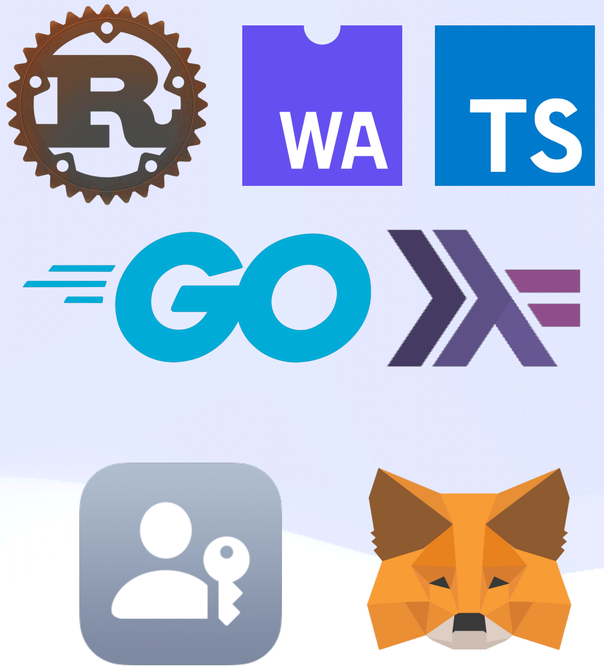
- **Capability Myths Demolished**: https://srl.cs.jhu.edu/pubs/SRL2003-02.pdf
- **ACLs Don't**: http://waterken.sourceforge.net/aclsdont/current.pdf



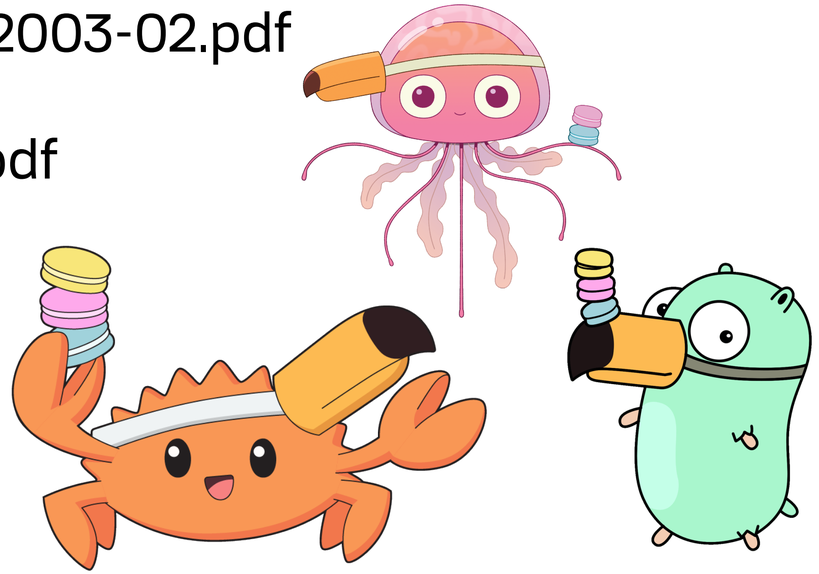
Resources 📚

Further Reading

- **Community**: https://github.com/ucan-wg



- **Capability Myths Demolished**: https://srl.cs.jhu.edu/pubs/SRL2003-02.pdf
- **ACLs Don't**: http://waterken.sourceforge.net/aclsdont/current.pdf
- **ERights**: https://erights.org

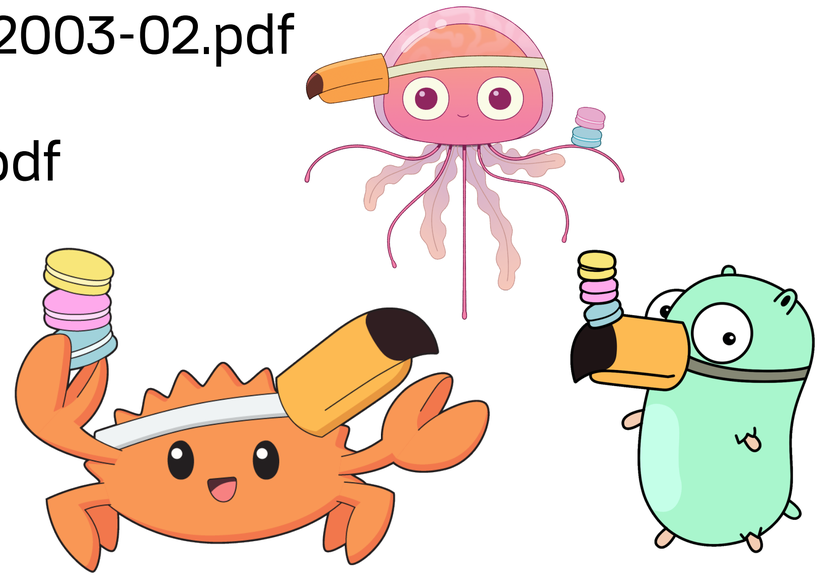


Resources 📚

Further Reading

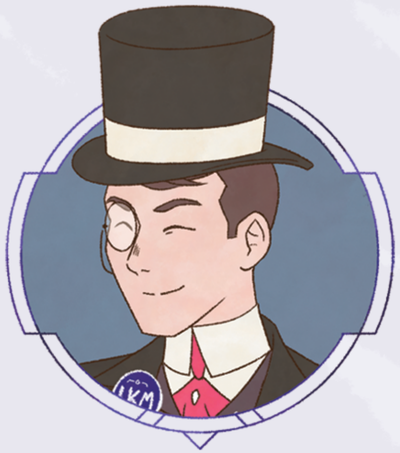
- **Community**: https://github.com/ucan-wg

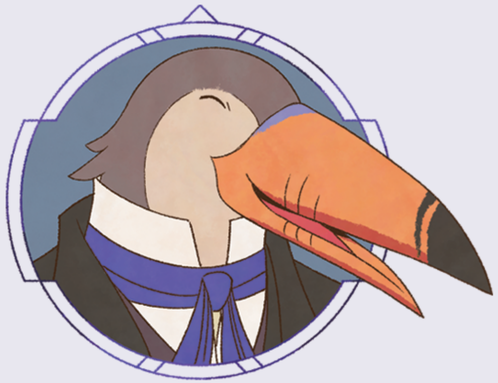
- **Capability Myths Demolished**: https://srl.cs.jhu.edu/pubs/SRL2003-02.pdf
- **ACLs Don't**: http://waterken.sourceforge.net/aclsdont/current.pdf
- **ERights**: https://erights.org
- **SPKI**: https://theworld.com/~cme/html/spki.html



Resources 📚

UCAN Adventure





UCAN ADVENTURE

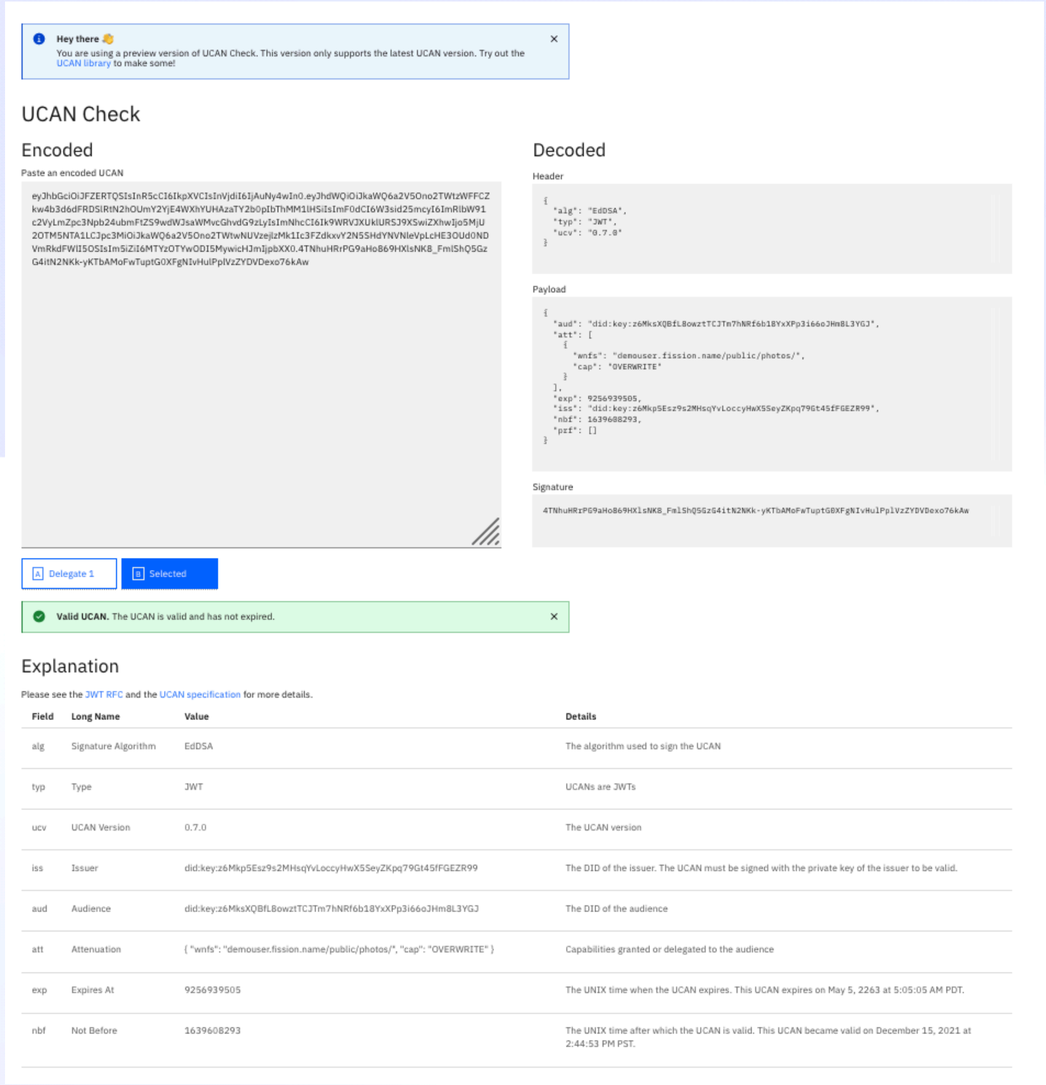
https://UCAN.lol

Resources 📚

ucan.xyz — Online Explorer / Validator

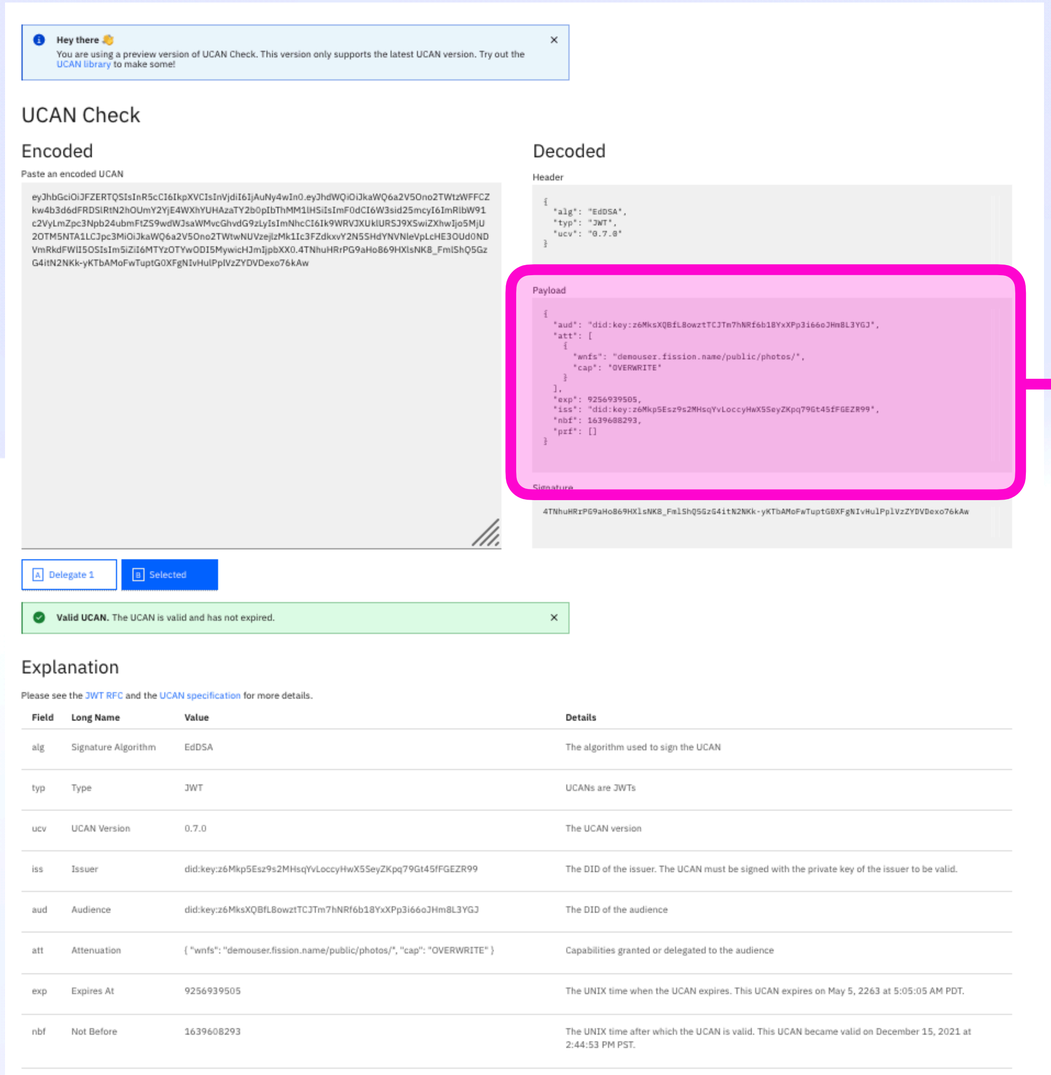
Resources 📚

ucan.xyz — Online Explorer / Validator



Resources 📚

ucan.xyz — Online Explorer / Validator

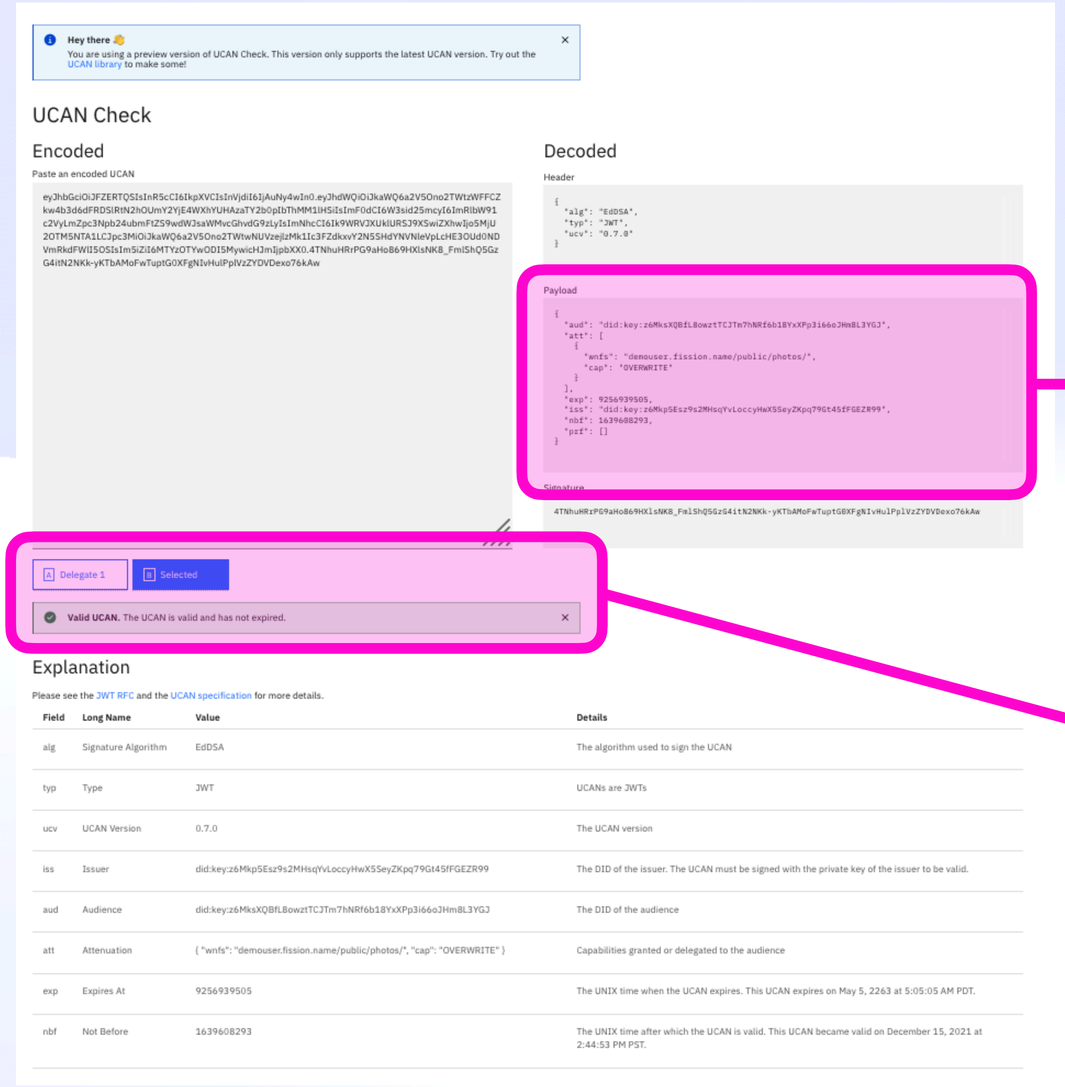


Payload

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

Resources 📚

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": []
}
```


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

A Delegate 1 B Selected

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

ucan.xyz
github.com/ucan-wg
lu.ma/wecan

🎉 þank you, IPFS þing 🇧🇪

brooklyn@fission.codes
discord.gg/fissioncodes
github.com/expede

ucan.xyz
github.com/ucan-wg
lu.ma/wecan

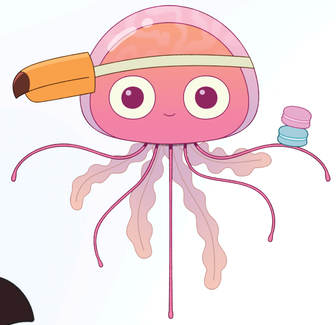
þank you, IPFS þing 🇧🇪

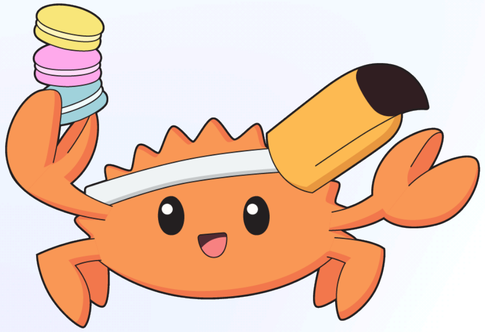
brooklyn@fission.codes
discord.gg/fissioncodes
github.com/expede

ucan.xyz
github.com/ucan-wg
lu.ma/wecan

I have stickers!

þank you, IPFS þing 🇧🇪





brooklyn@fission.codes
discord.gg/fissioncodes
github.com/expede