

And now  
for something  
completely different...





# ***UCAN Control Your Stuff***

**Local-First Authority Without Boundaries**



**LOCAL  
-FIRST  
CONF**



**Brooklyn Zelenka**

@expede





# Brooklyn Zelenka

@expede

- Open source, standards, PLT, DSys
- Knows a few things about UCAN
- Began UCAN for "the Rails of LoFi"
  - Now many use cases: CRDTs, storage, compute
- Runs an online distributed systems reading group
  - <https://lu.ma/distributed-systems>







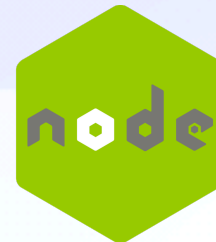


# Client/Server

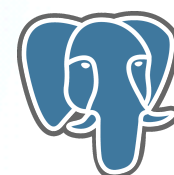
Auth 



Compute 



Data 



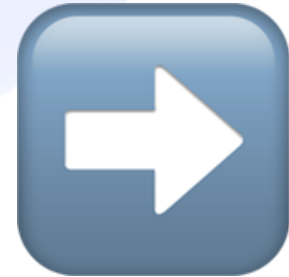
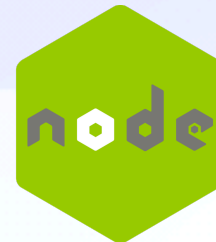


# Client/Server

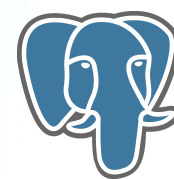
Auth 



Compute 




Data 






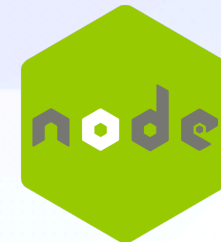
# Client/Server


# LoFi

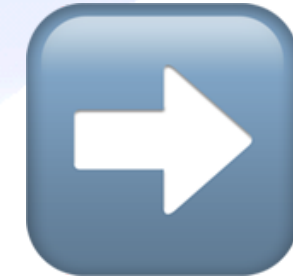
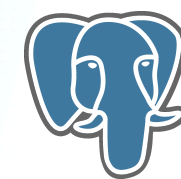
Auth 




Compute 



Data 



Compute 

Data 

Auth 



# ***Schools of Thought***





Schools of Thought

***ACL Model***



Schools of Thought

***ACL Model***





Schools of Thought

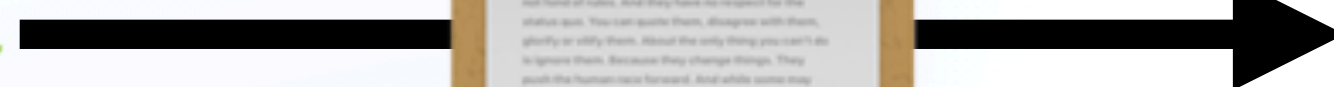
***ACL Model***





# Schools of Thought

# *ACL Model*





# Schools of Thought

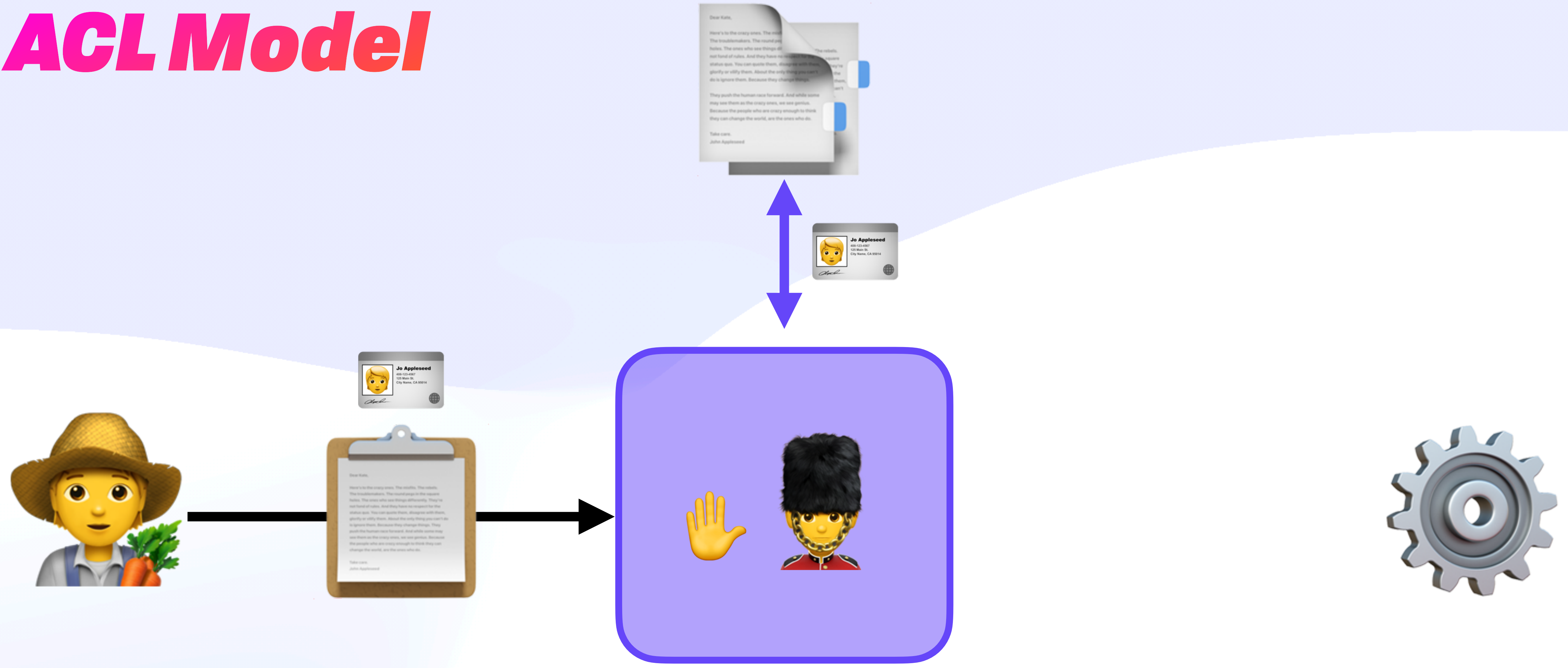
# *ACL Model*





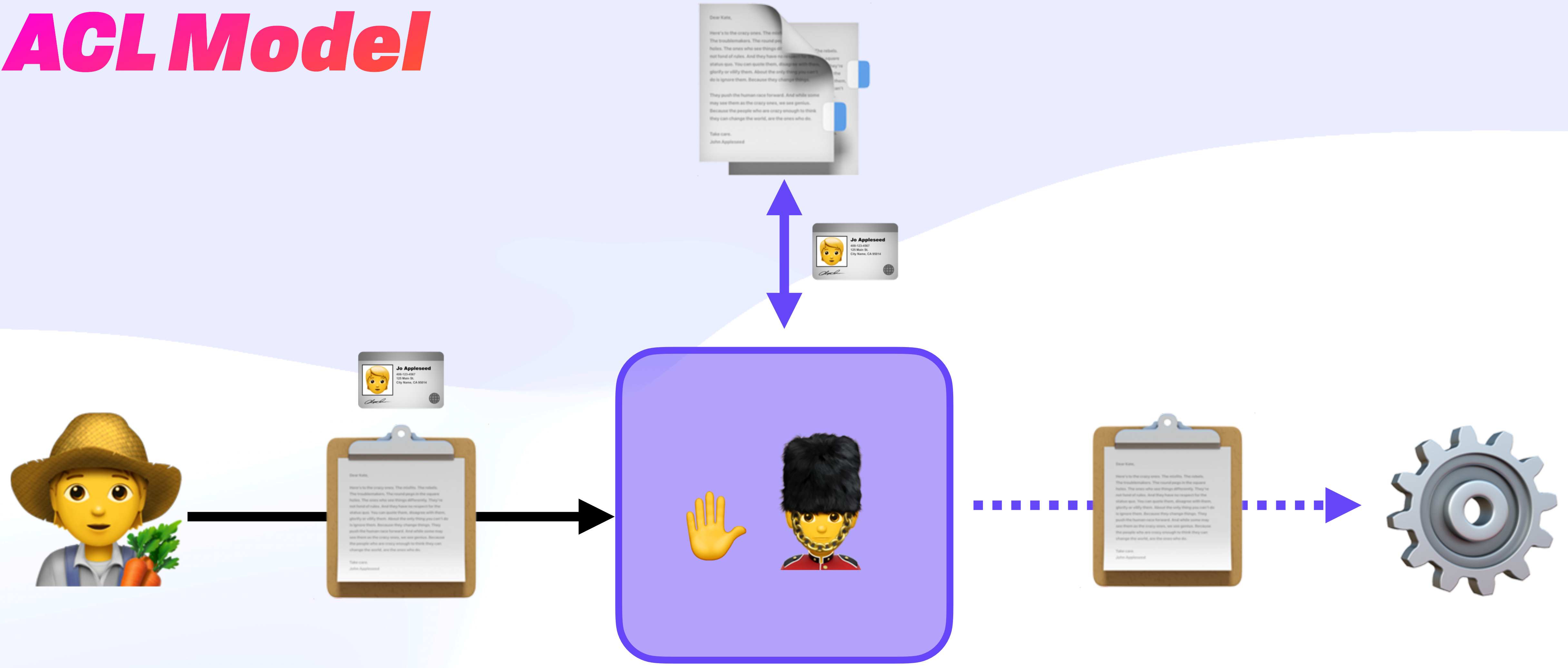
# Schools of Thought

# ACL Model



# Schools of Thought

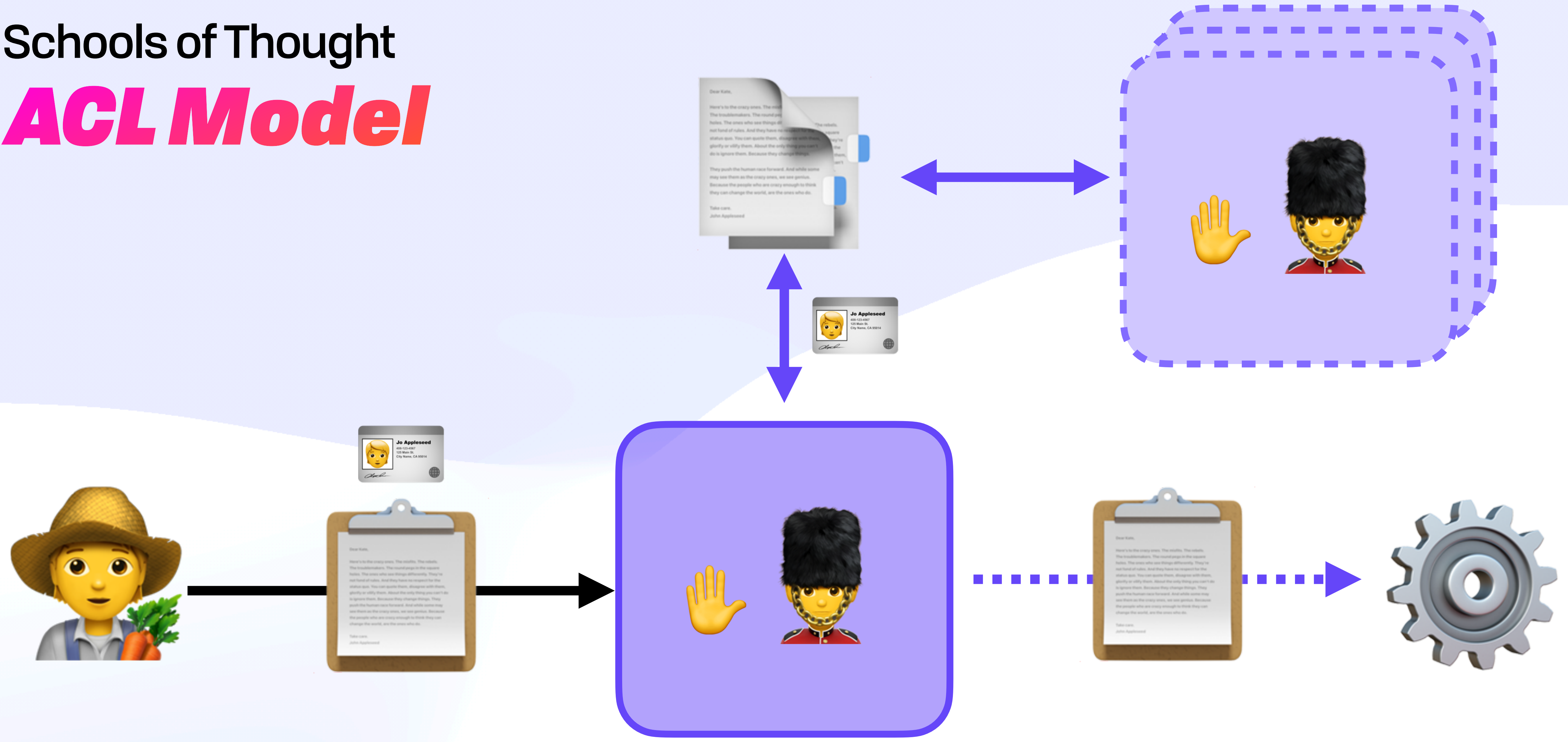
# ACL Model





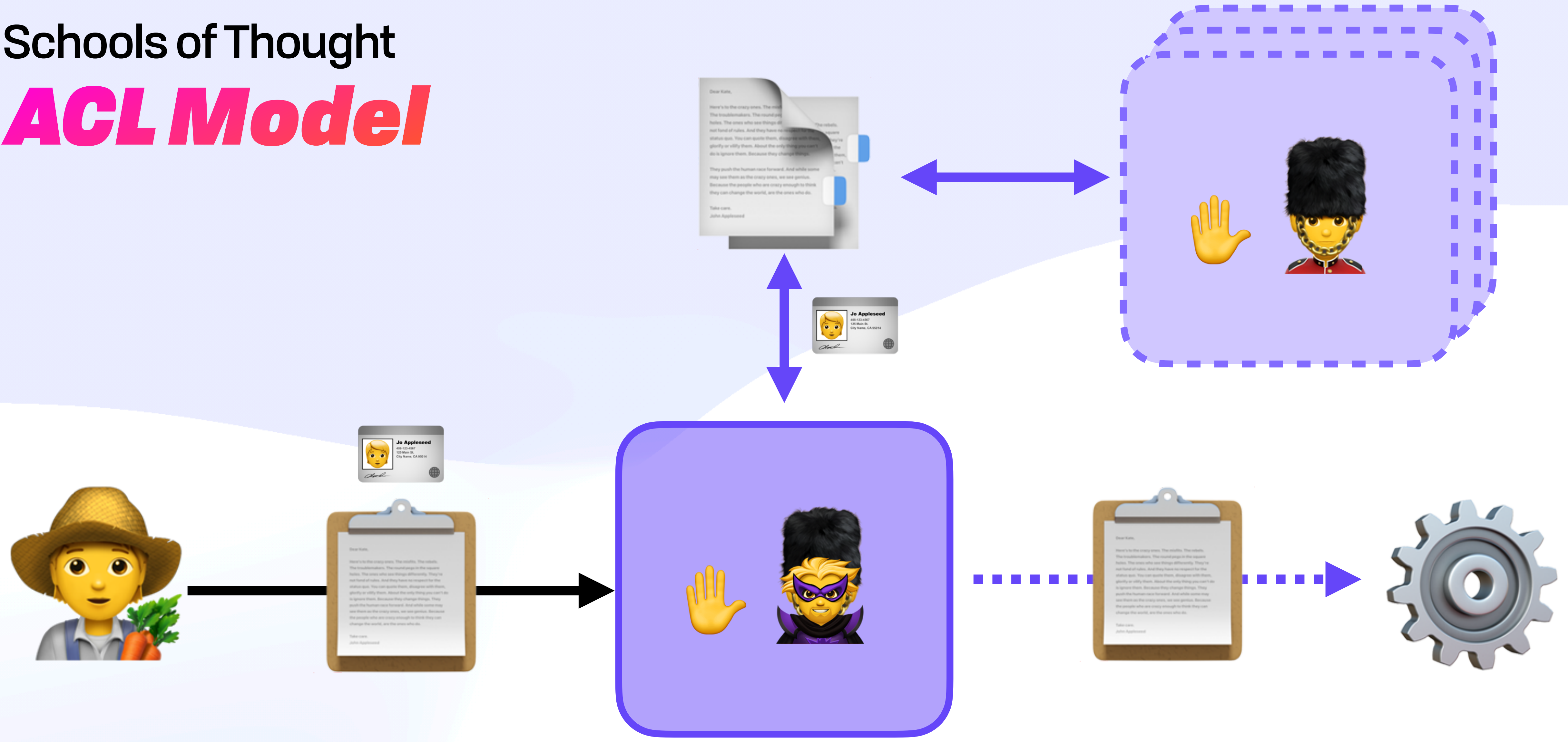
# Schools of Thought

## *ACL Model*



# Schools of Thought

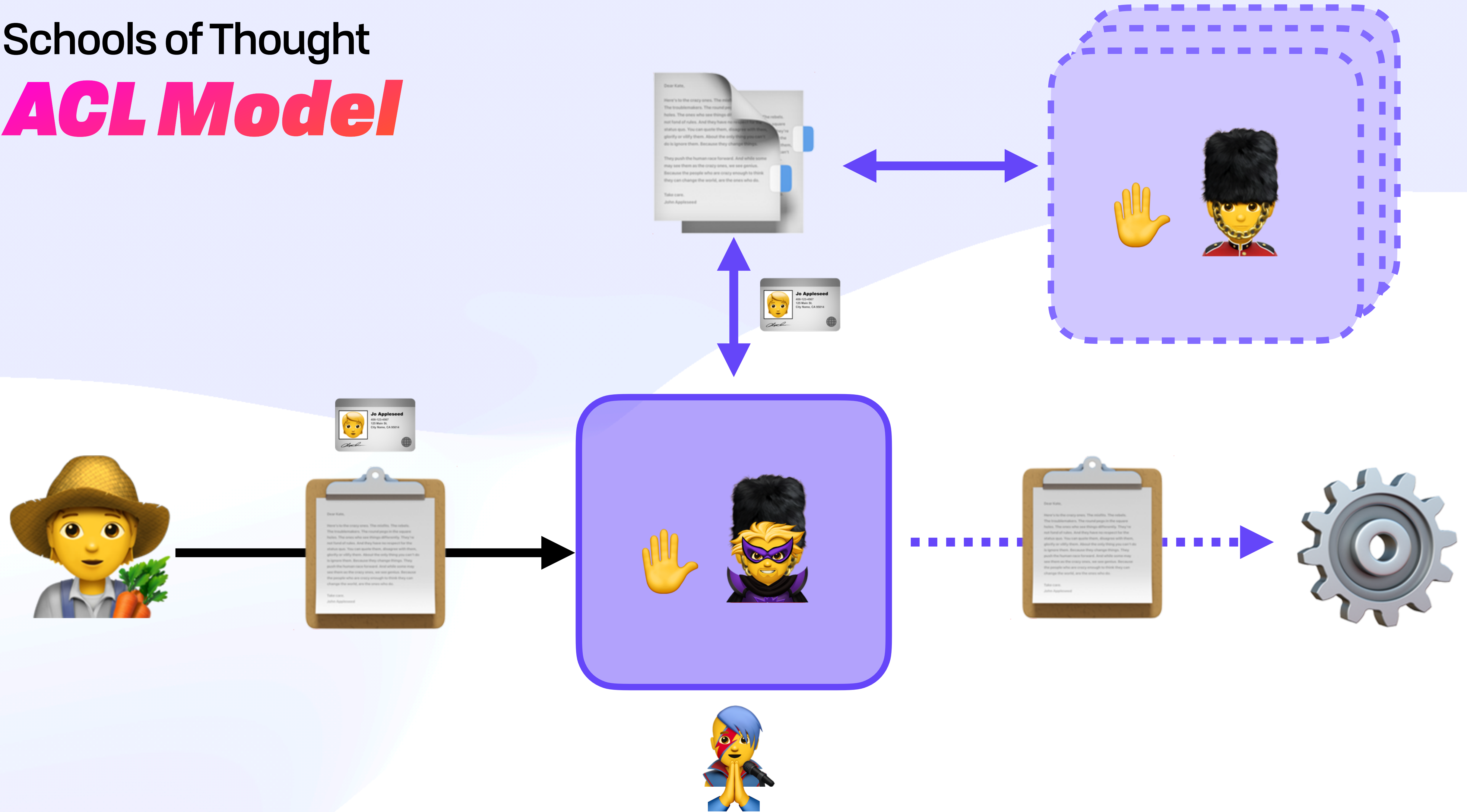
## *ACL Model*





# Schools of Thought

## *ACL Model*



Schools of Thought

# ***Certificate Capability Model***



Schools of Thought

# *Certificate Capability Model*



Schools of Thought

# *Certificate Capability Model*





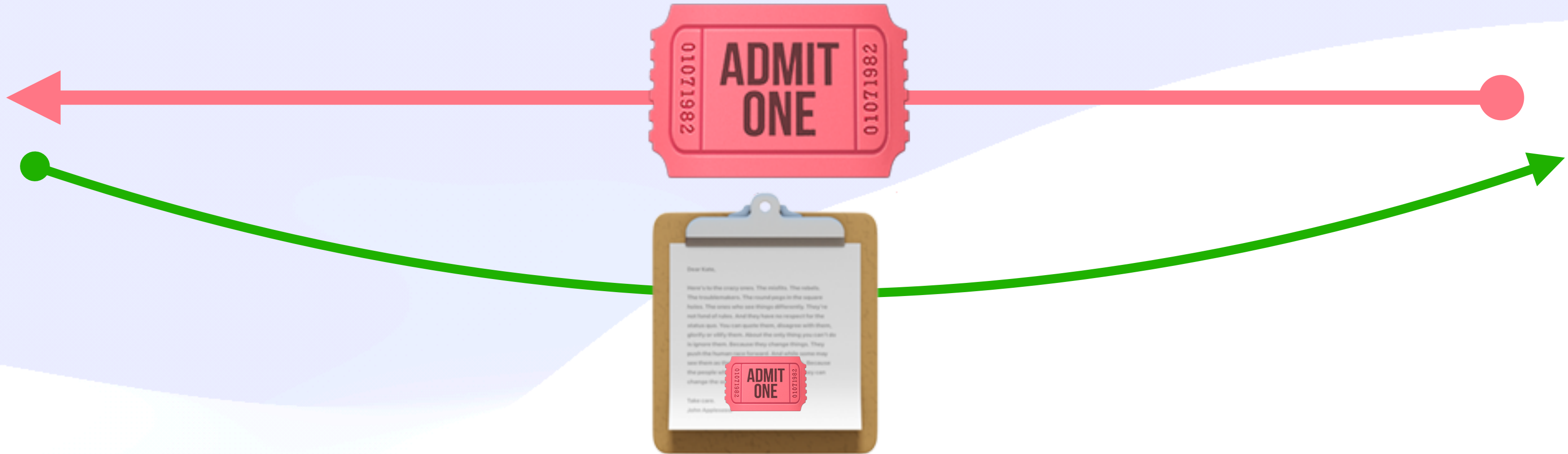
Schools of Thought

# *Certificate Capability Model*



# Schools of Thought

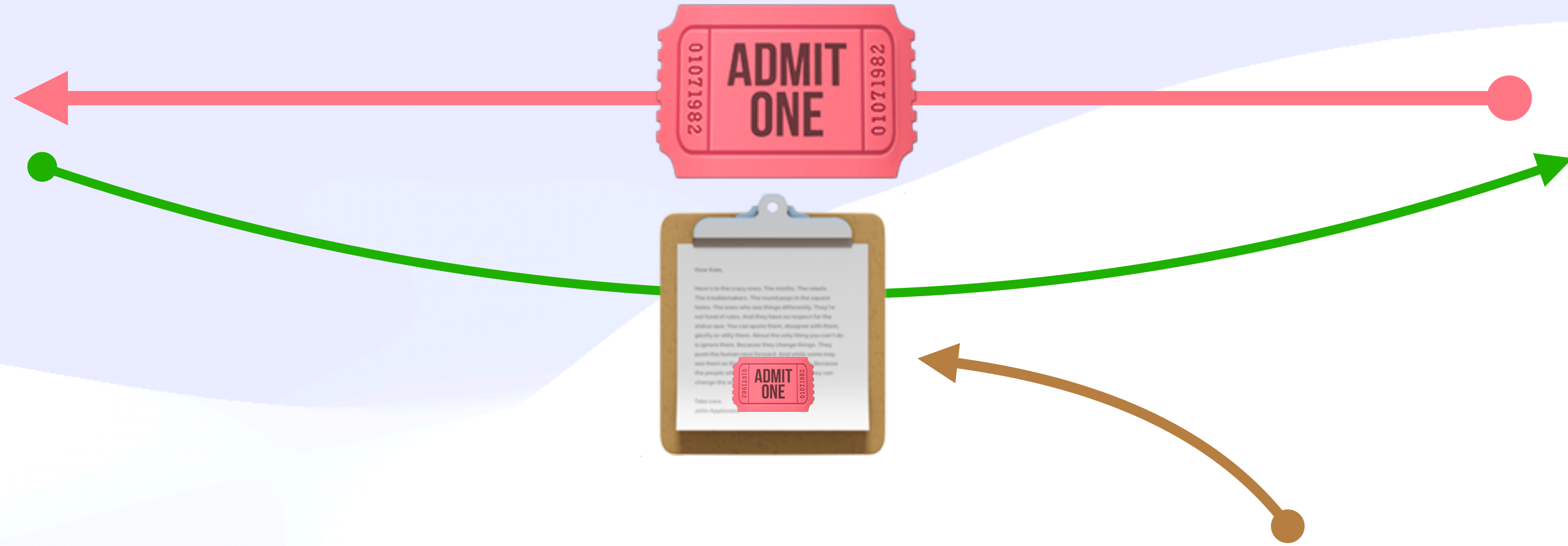
# *Certificate Capability Model*





Schools of Thought

# Certificate Capability Model



**Self-contained:  
has all required info**

Schools of Thought

# *Certificate Capability Model*





Schools of Thought

# *Certificate Capability Model*



Schools of Thought

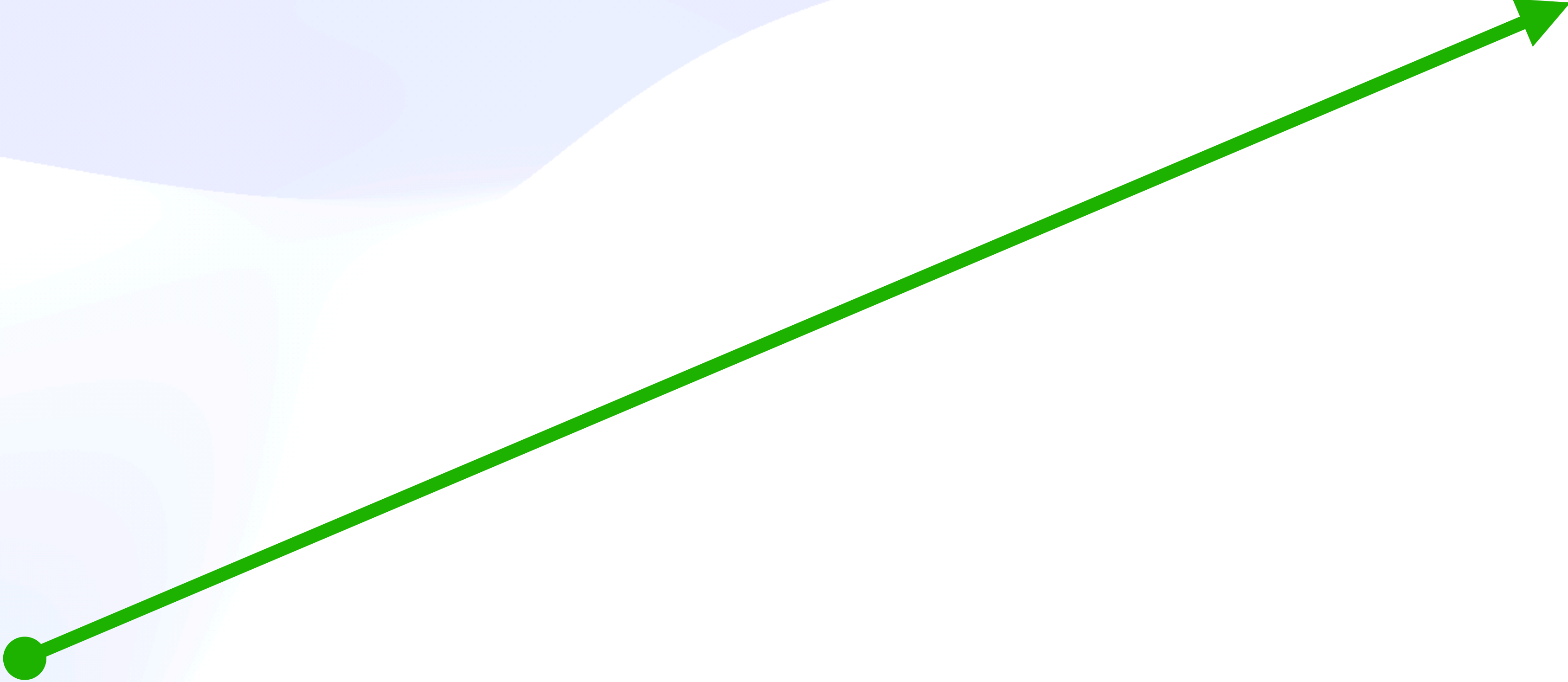
# *Certificate Capability Model*





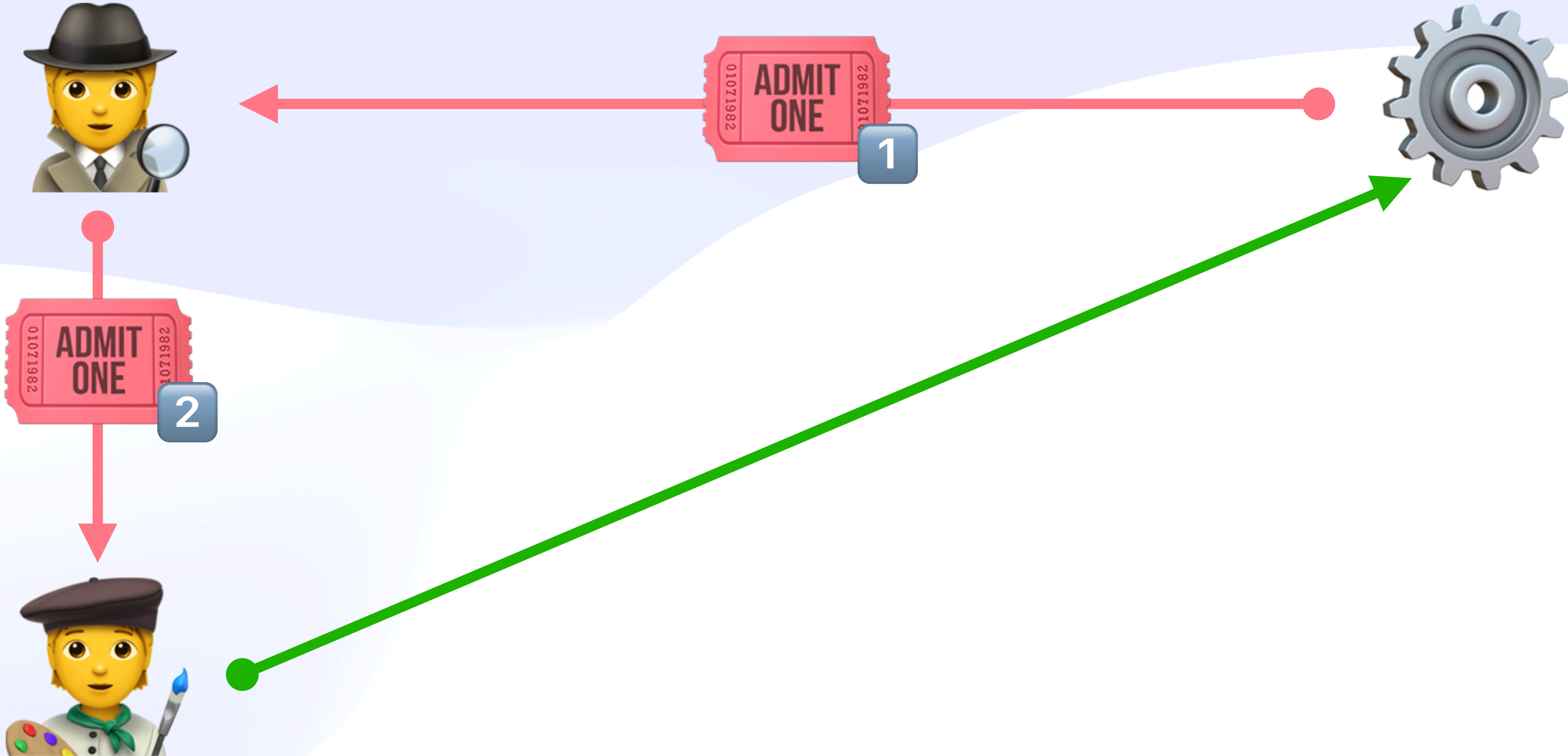
Schools of Thought

# *Certificate Capability Model*



Schools of Thought

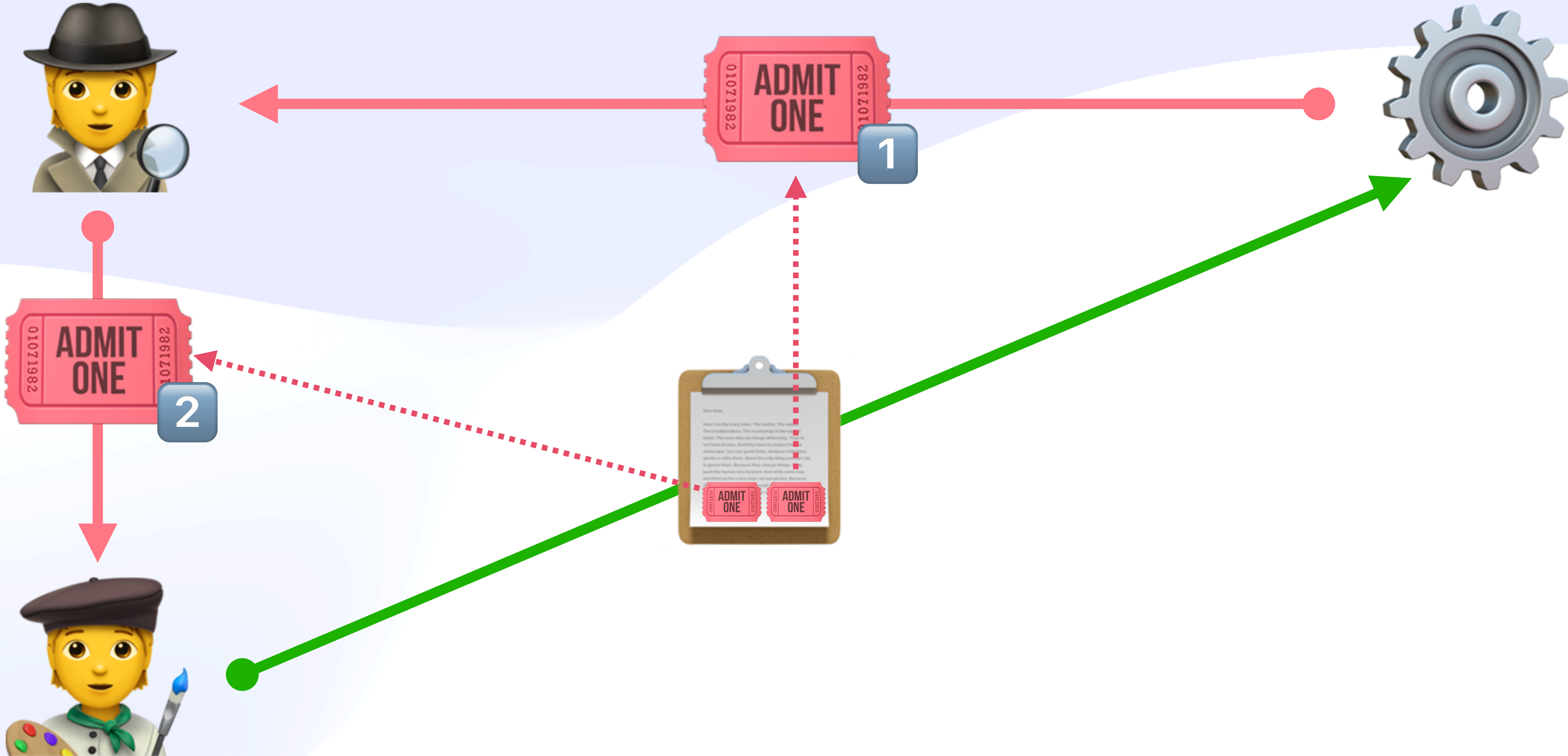
# *Certificate Capability Model*





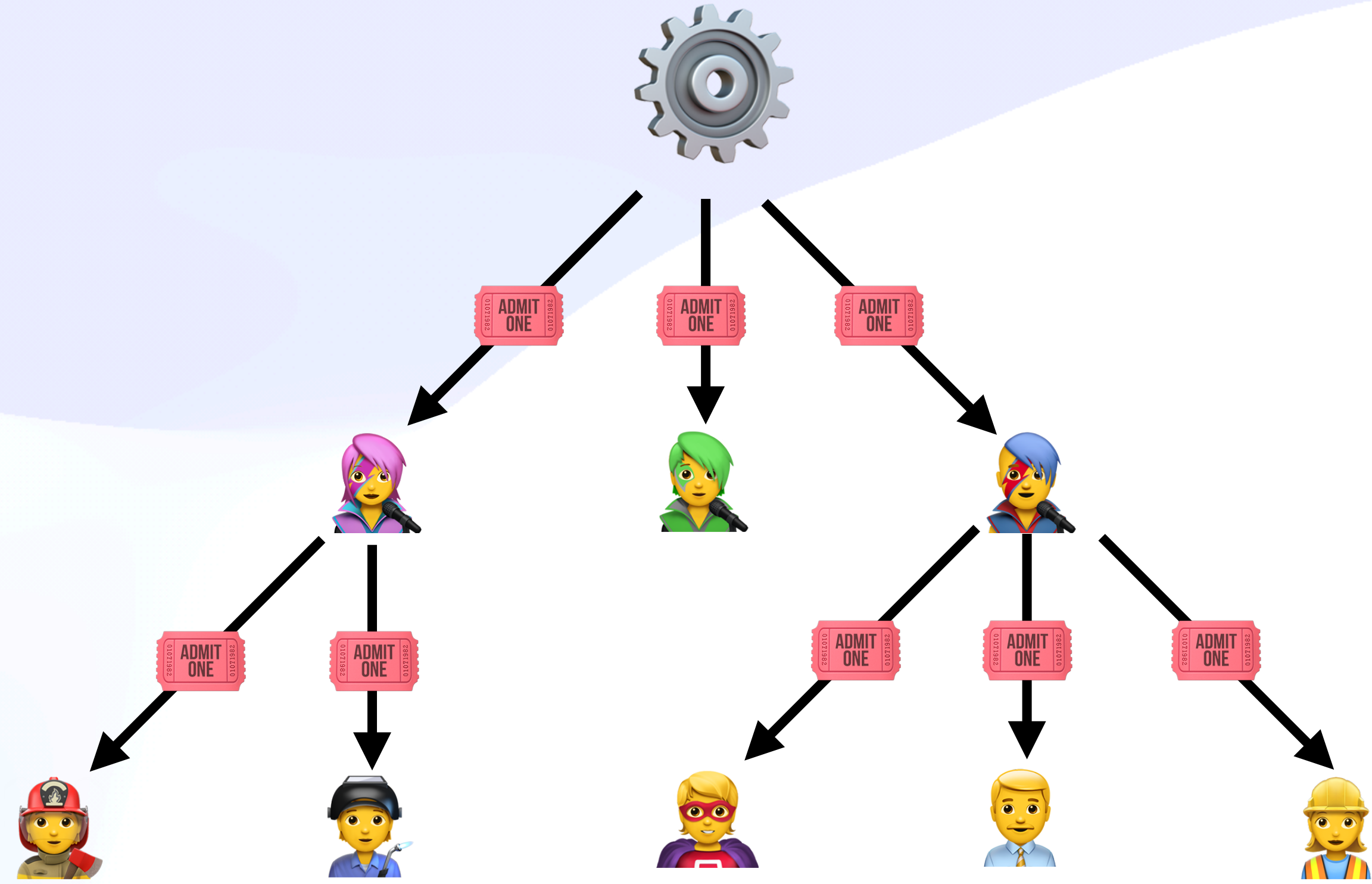
# Schools of Thought

# *Certificate Capability Model*



# Schools of Thought

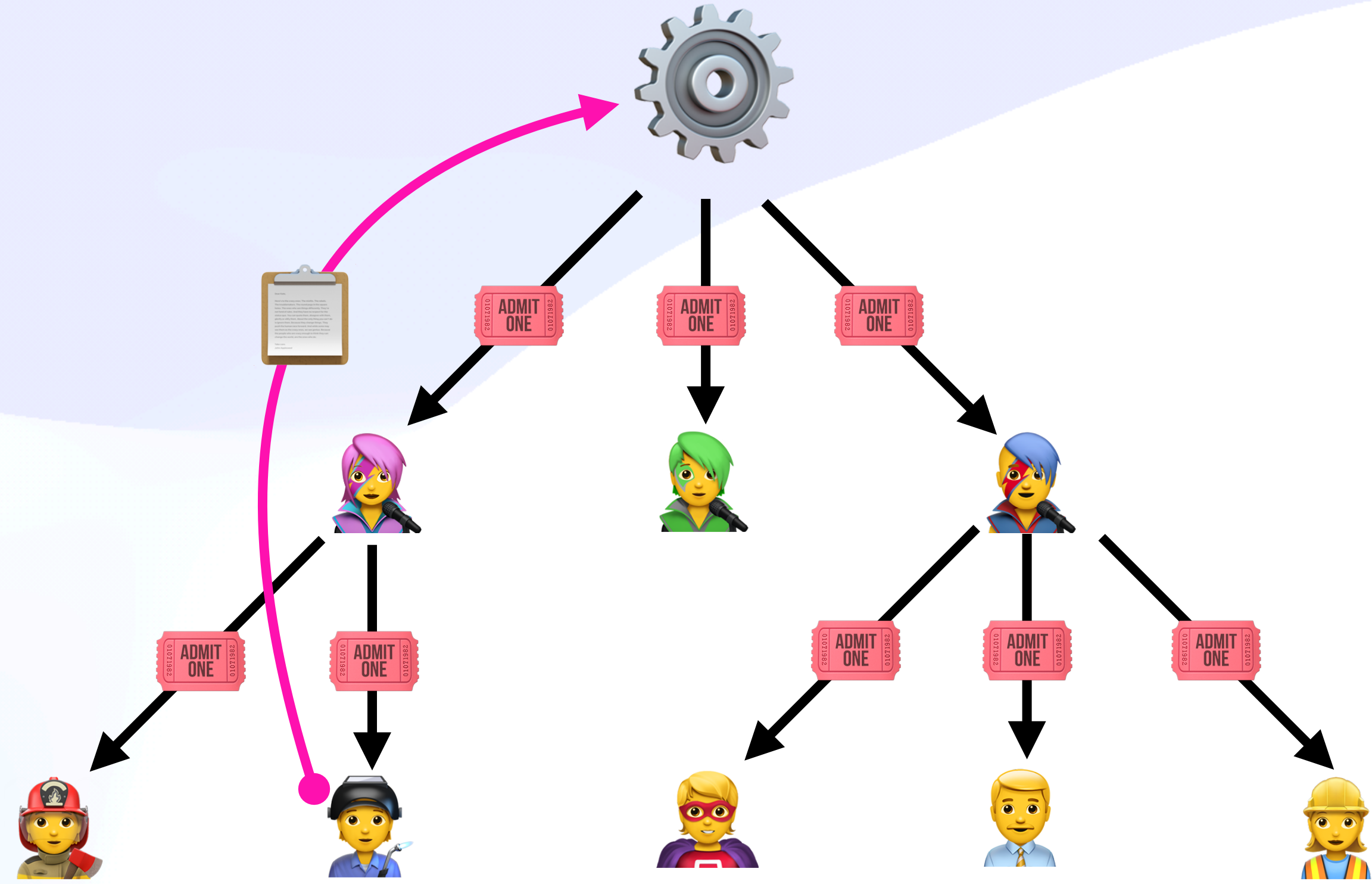
# *On a Need to Know Basis*





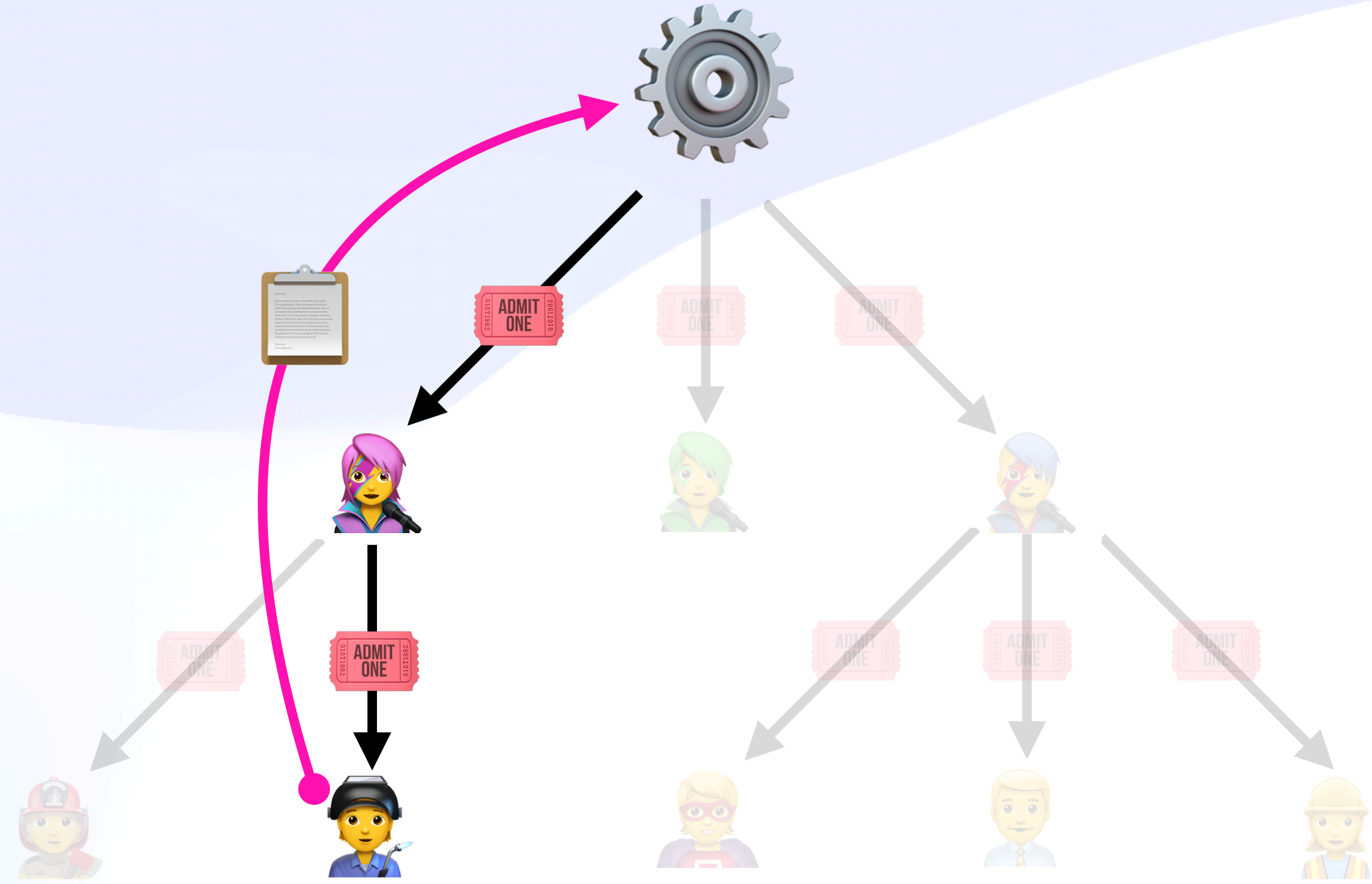
# Schools of Thought

# *On a Need to Know Basis*



# Schools of Thought

# *On a Need to Know Basis*





Schools of Thought  
***Auth Flow***

Schools of Thought

# ***Auth Flow***





Schools of Thought

# *Auth Flow*



# Schools of Thought

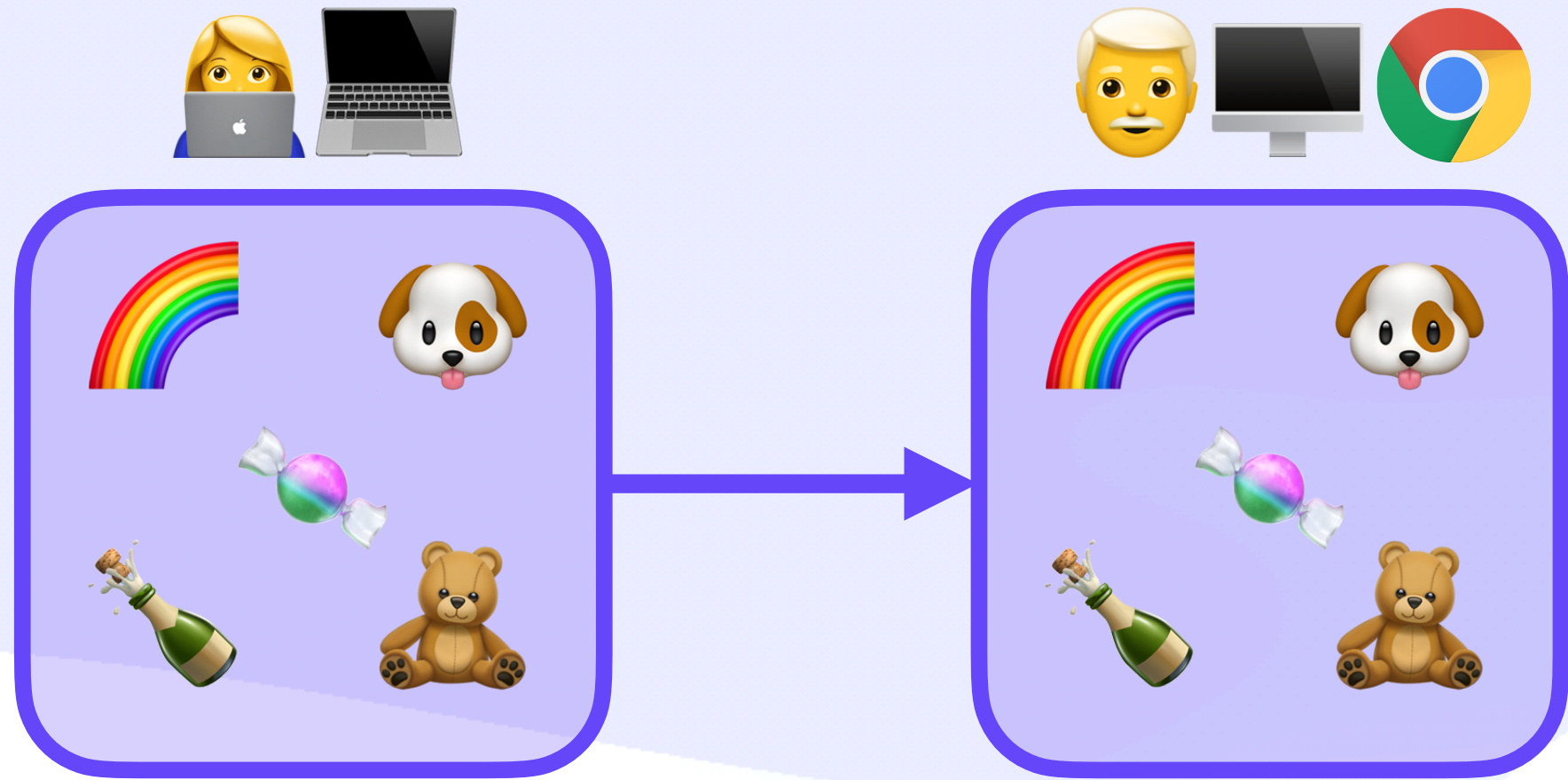
# *Auth Flow*





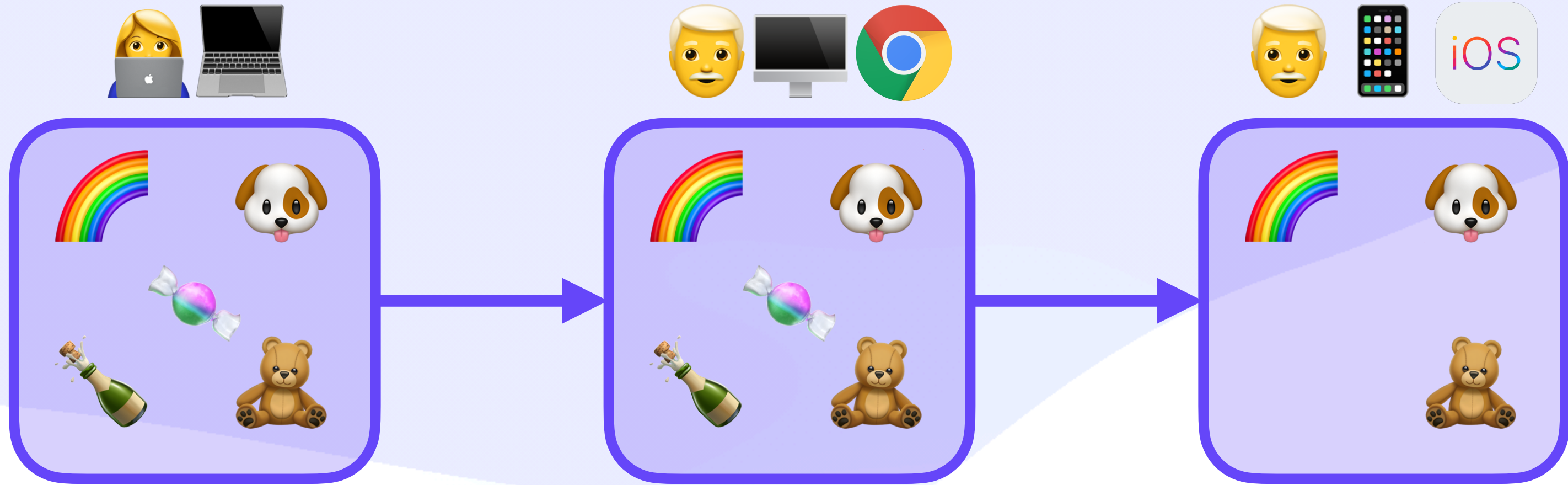
# Schools of Thought

# *Auth Flow*



# Schools of Thought

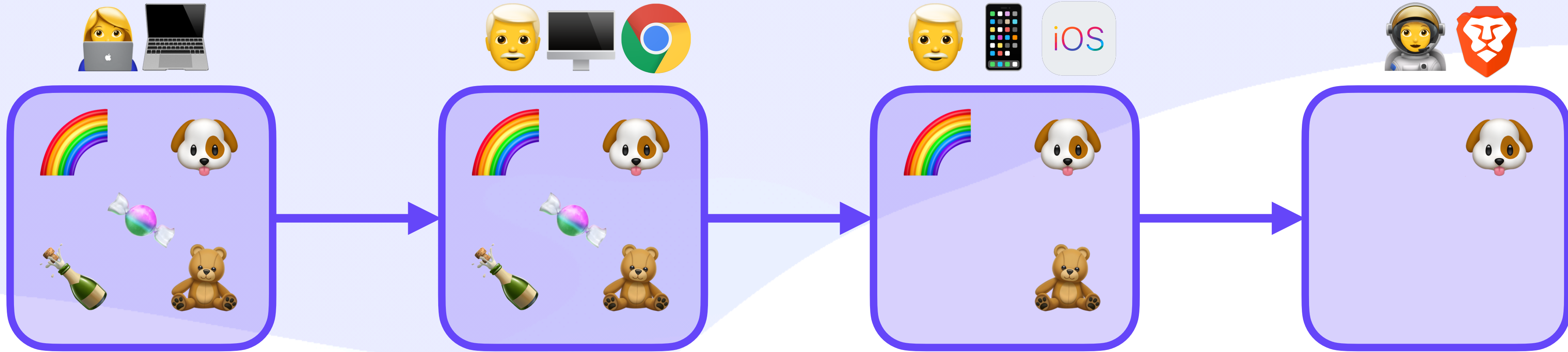
# *Auth Flow*





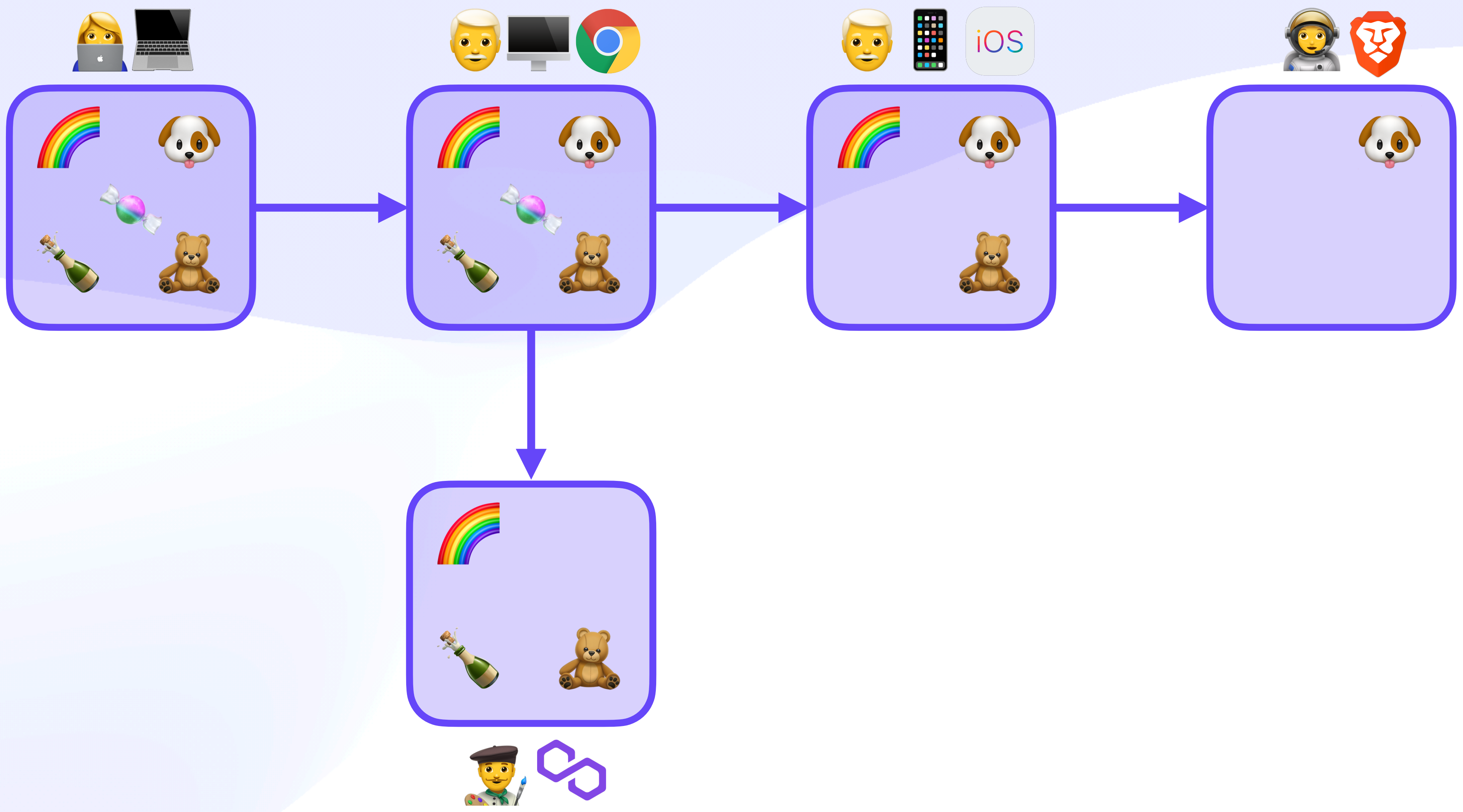
# Schools of Thought

# *Auth Flow*



# Schools of Thought

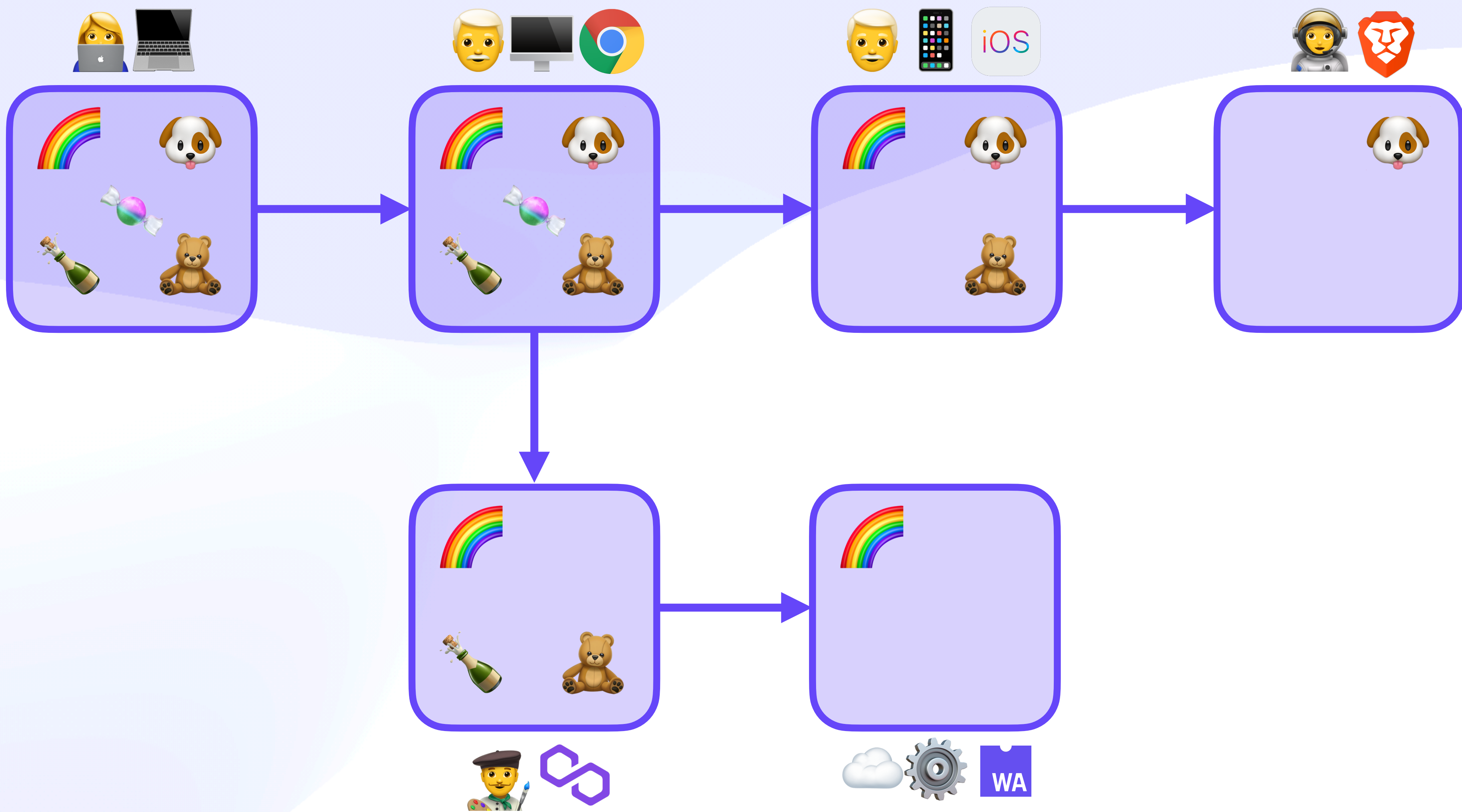
# *Auth Flow*





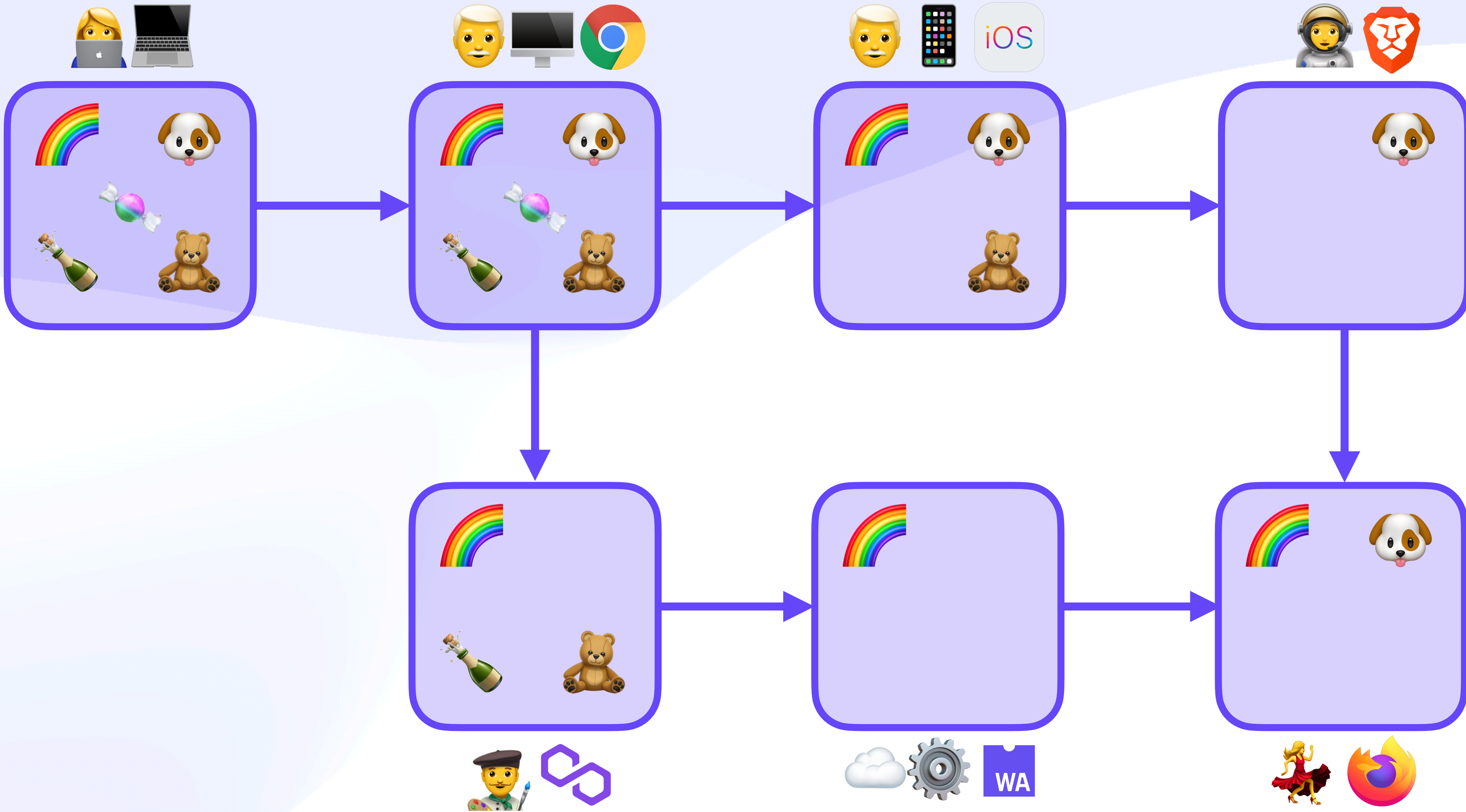
# Schools of Thought

# *Auth Flow*



# Schools of Thought

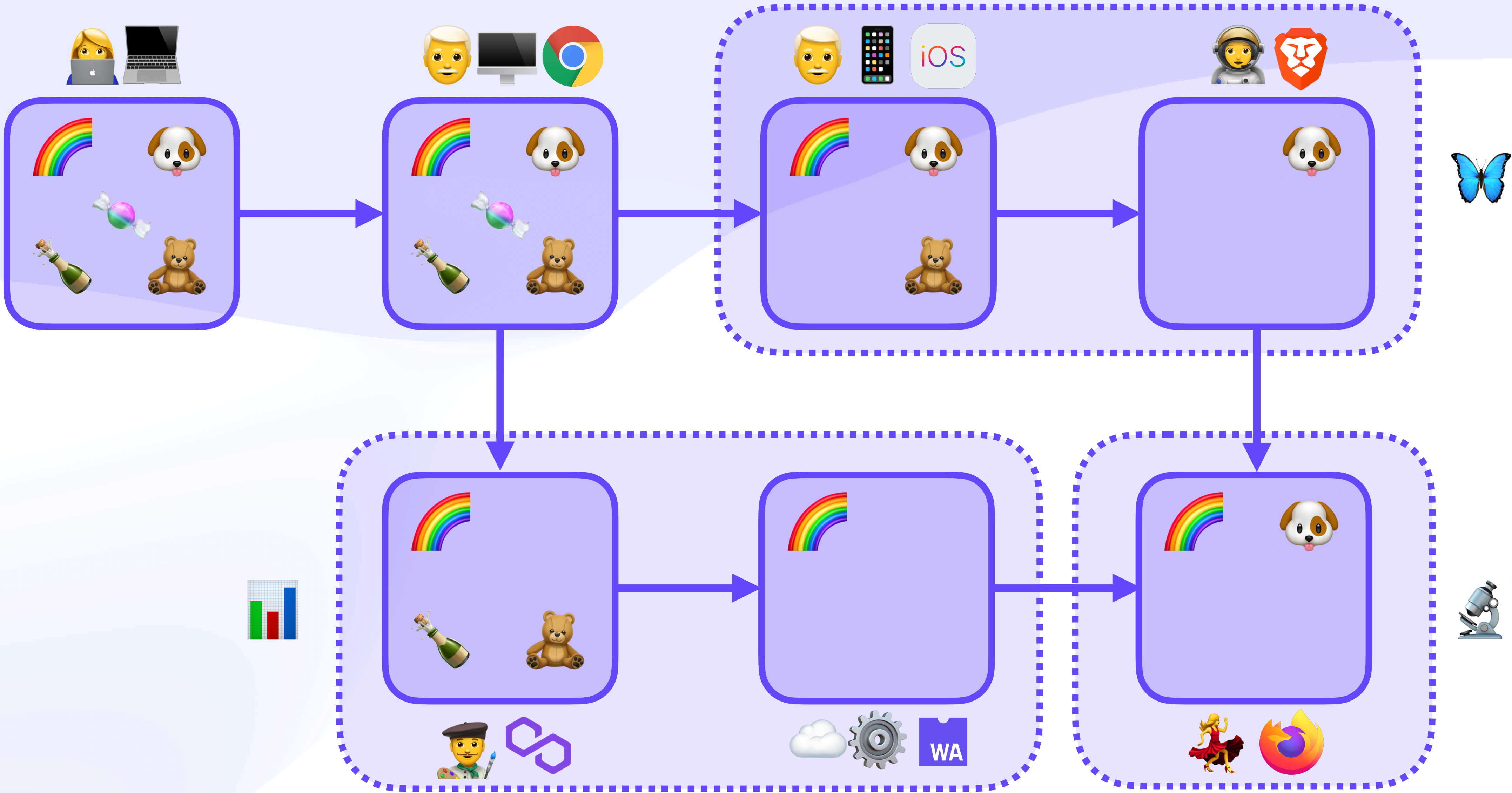
# *Auth Flow*





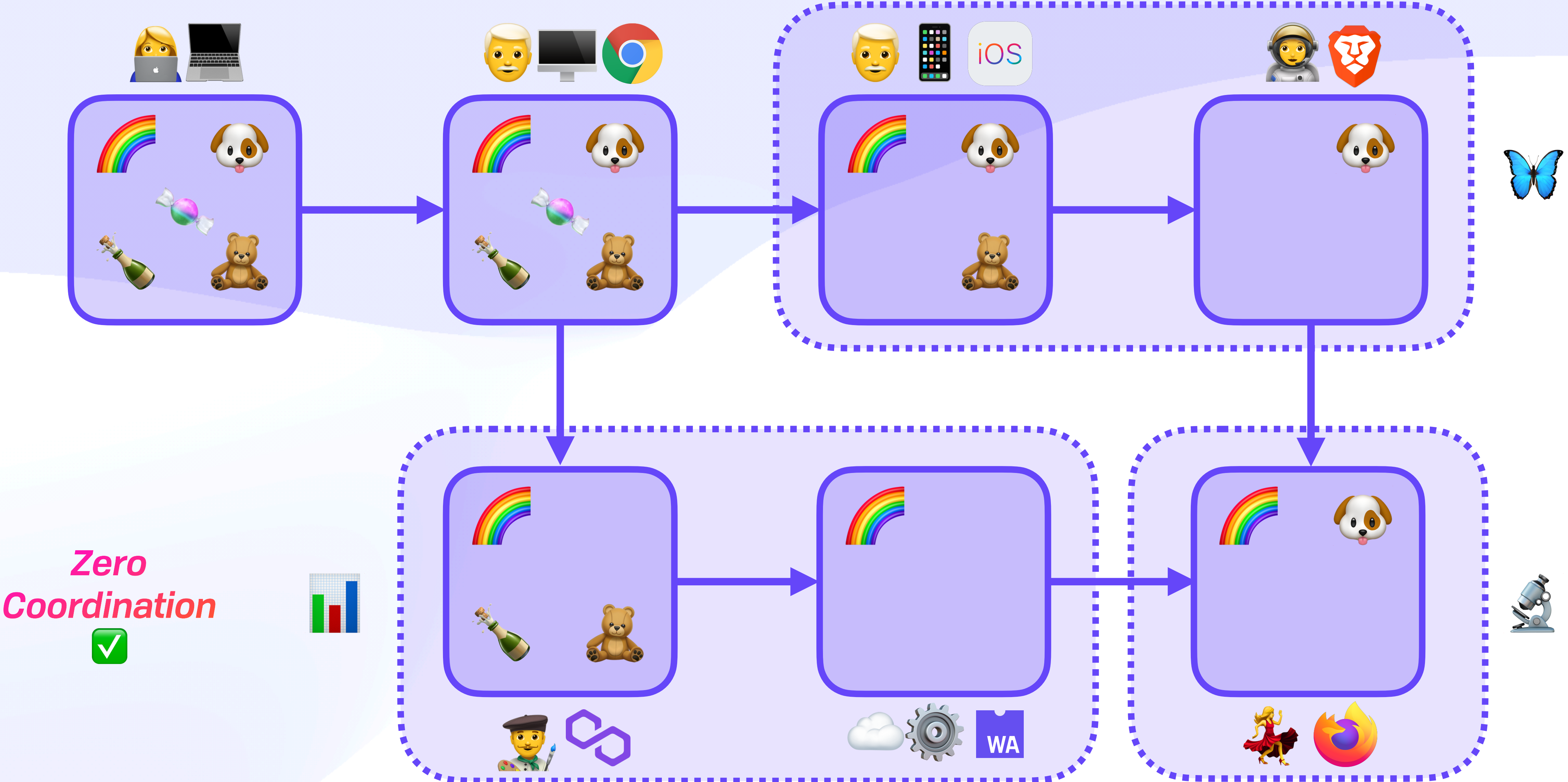
# Schools of Thought

# Auth Flow



# Schools of Thought

# Auth Flow





# ***Raw Mechanics***





# Raw Mechanics

## Checking Chains

About: 

From: 

To: 

Can: [, ]

About: 

From: 

To: 

Can: [, ]

About: 

From: 

To: 

Can: []




 [\*]



 [, ]



 [, ]



 []





# Raw Mechanics

## Checking Chains

About:  

From: 

To: 

Can: [, ]

About: 

From: 

To: 

Can: [, ]

About: 

From: 

To: 

Can: []



 [\*]



 [, ]



 [, ]



 []



# Raw Mechanics

## Checking Chains

About:  

From: 

To: 

Can: [, ]

About: 

From: 

To: 

Can: [, ]

About: 

From: 

To: 

Can: []




 [\*]



 [, ]



 [, ]

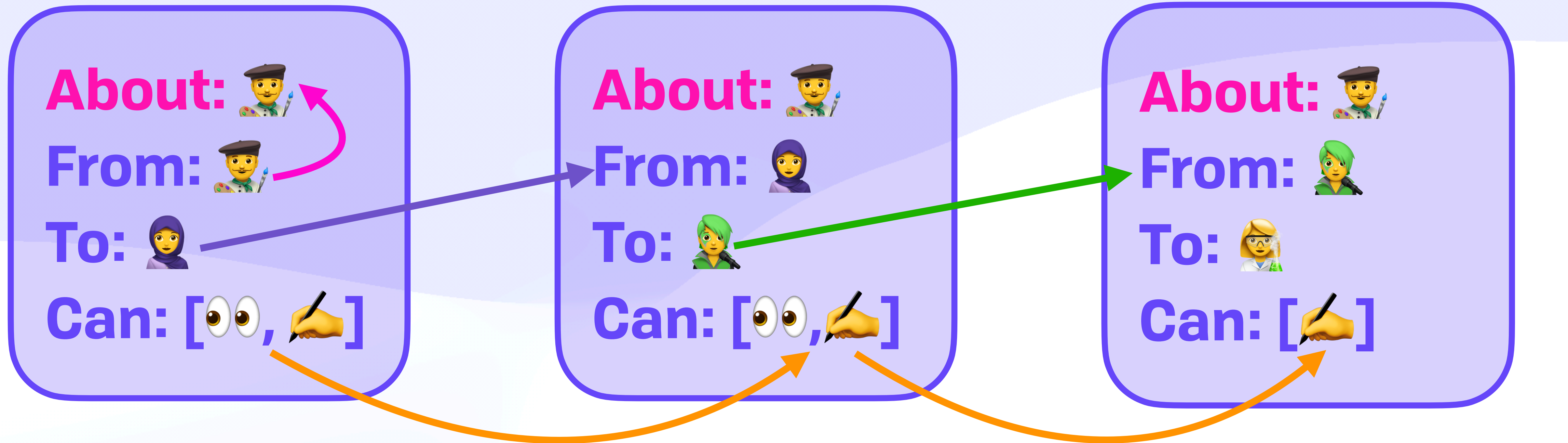


 []



# Raw Mechanics

## Checking Chains



[Artist emoji] [\*]

[Woman emoji] [Eyes emoji, Hand writing emoji]

[Woman with microphone emoji] [Eyes emoji, Hand writing emoji]

[Woman with glasses emoji] [Hand writing emoji]

# Raw Mechanics

## *Syntactically Driven*

```
{
  iss: "did:key:alice",
  aud: "did:key:bob",
  sub: "did:key:doc"
  cmd: "/automerge/update",
  pol: [
    ["gt", ".foo[1].bar", "42"],
    ["eq", ".prev", 0x98ea6e4f216f2fb4b69fff9b3a44842c38686ca685f3f55dc48c5d3fb1107be4]
  ]
}
```

```
{
  iss: "did:key:bob",
  aud: "did:key:doc",
  sub: "did:key:doc"
  prf: [hash(delegation), hash(more_chain)]
  cmd: "/automerge/update",
  args: {
    foo: [
      {bar: 100}, // > 42
      {quux: "unconstrained"}
    ],
    prev: 0x98ea6e4f216f2fb4b69fff9b3a44842c38686ca685f3f55dc48c5d3fb1107be4
  }
}
```



## Raw Mechanics

# *Syntactically Driven*

```
{
  iss: "did:key:alice",
  aud: "did:key:bob",
  sub: "did:key:doc",
  cmd: "/automerge/update",
  pol: [
    ["gt", ".foo[1].bar", "42"],
    ["eq", ".prev", 0x98ea6e4f216f2fb4b69fff9b3a44842c38686ca685f3f55dc48c5d3fb1107be4]
  ]
}
```

```
{
  iss: "did:key:bob",
  aud: "did:key:doc",
  sub: "did:key:doc",
  prf: [hash(delegation), hash(more_chain)]
  cmd: "/automerge/update",
  args: {
    foo: [
      {bar: 100}, // > 42
      {quux: "unconstrained"}
    ],
    prev: 0x98ea6e4f216f2fb4b69fff9b3a44842c38686ca685f3f55dc48c5d3fb1107be4
  }
}
```

## Raw Mechanics

# *Syntactically Driven*

```
{  
  iss: "did:key:alice",  
  aud: "did:key:bob",  
  sub: "did:key:doc",  
  cmd: "/automerge/update",  
  pol: [  
    ["gt", ".foo[1].bar", "42"],  
    ["eq", ".prev", 0x98ea6e4f216f2fb4b69fff9b3a44842c38686ca685f3f55dc48c5d3fb1107be4]  
  ]  
}
```

```
{  
  iss: "did:key:bob",  
  aud: "did:key:doc",  
  sub: "did:key:doc",  
  prf: [hash(delegation), hash(more_chain)]  
  cmd: "/automerge/update",  
  args: {  
    foo: [  
      {bar: 100}, // > 42  
      {quux: "unconstrained"}  
    ],  
    prev: 0x98ea6e4f216f2fb4b69fff9b3a44842c38686ca685f3f55dc48c5d3fb1107be4  
  }  
}
```



# Raw Mechanics

## *Syntactically Driven*

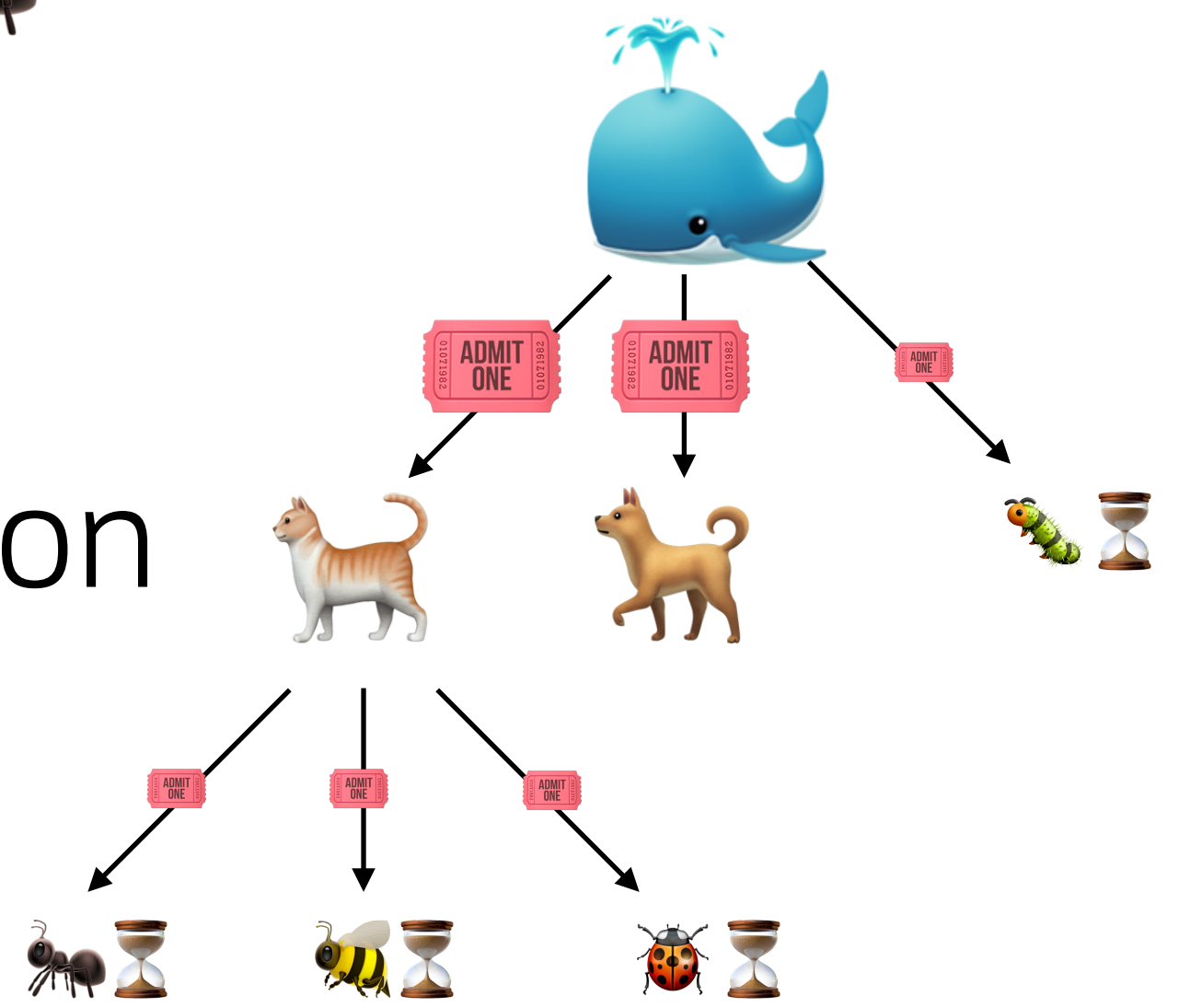
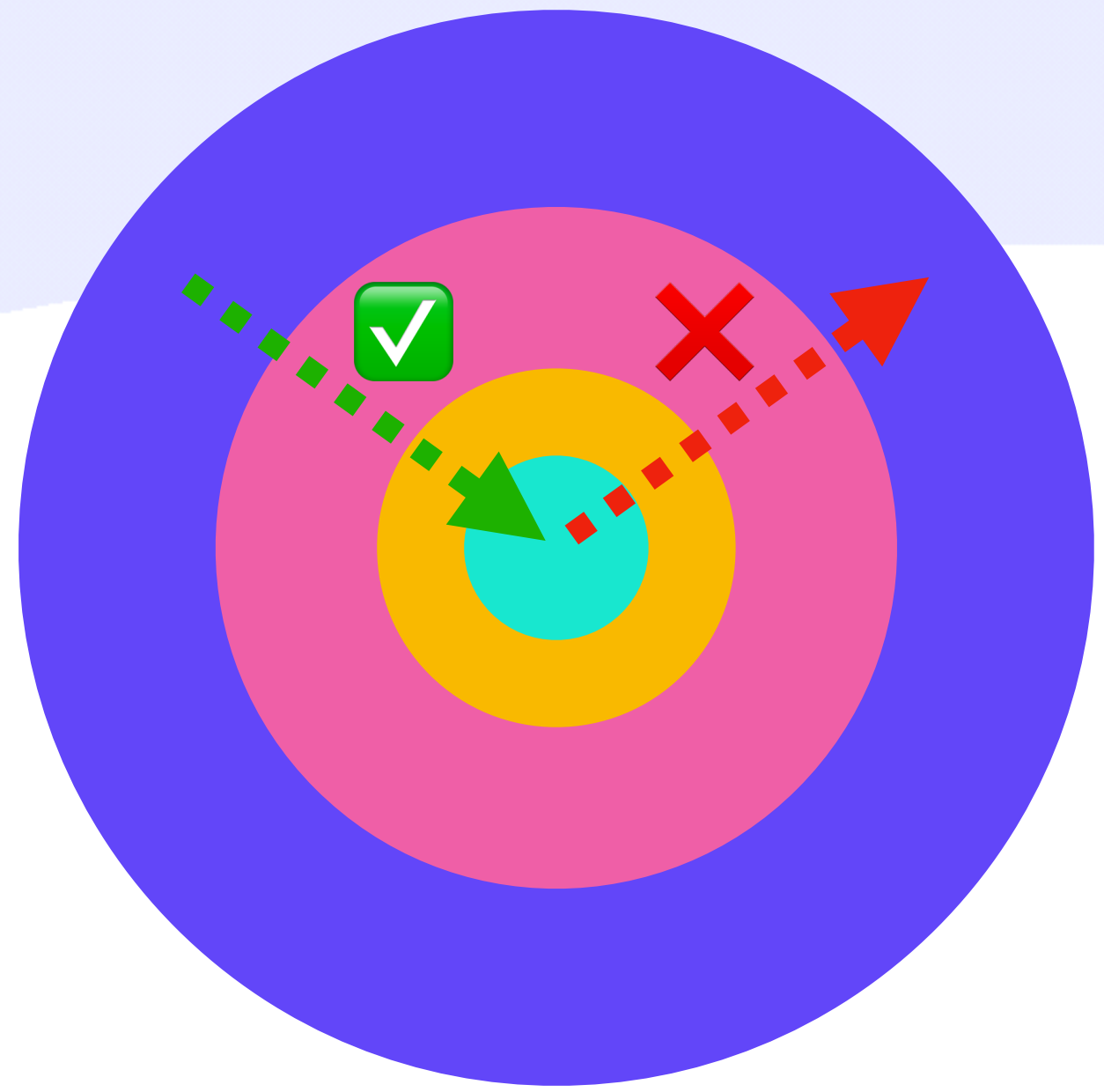
```
{  
  iss: "did:key:alice",  
  aud: "did:key:bob",  
  sub: "did:key:doc",  
  cmd: "/automerge/update",  
  pol: [  
    ["gt", ".foo[1].bar", "42"],  
    ["eq", ".prev", 0x98ea6e4f216f2fb4b69fff9b3a44842c38686ca685f3f55dc48c5d3fb1107be4]  
  ]  
}
```

```
{  
  iss: "did:key:bob",  
  aud: "did:key:doc",  
  sub: "did:key:doc",  
  prf: [hash(delegation), hash(more_chain)]  
  cmd: "/automerge/update",  
  args: {  
    foo: [  
      {bar: 100}, // > 42  
      {quux: "unconstrained"}  
    ],  
    prev: 0x98ea6e4f216f2fb4b69fff9b3a44842c38686ca685f3f55dc48c5d3fb1107be4  
  }  
}
```

# The Freedom of Least Authority

## *Ad Hoc Caveats*

- Agents are **abundant**
  - Few human system administrators 🐳
  - Billions of throwaway single-purpose workers 🐜
- Arbitrarily restrict authority
  - i.e. don't even allow an LLM to hallucinate intention





## The Freedom of Least Authority

# *Minimal Surface Area*

- Avoid the **confused deputy problem**
  - (Happens when an agent uses their authority to fulfil a request)
- UCAN
  - Executor never runs under their own "ambient authority"
  - All info in request: run with exactly that level of auth
    - "Just run with the handle you were handed"

**Yes... UCAN!**

***Wrap Up***





## Capabilities Worldview

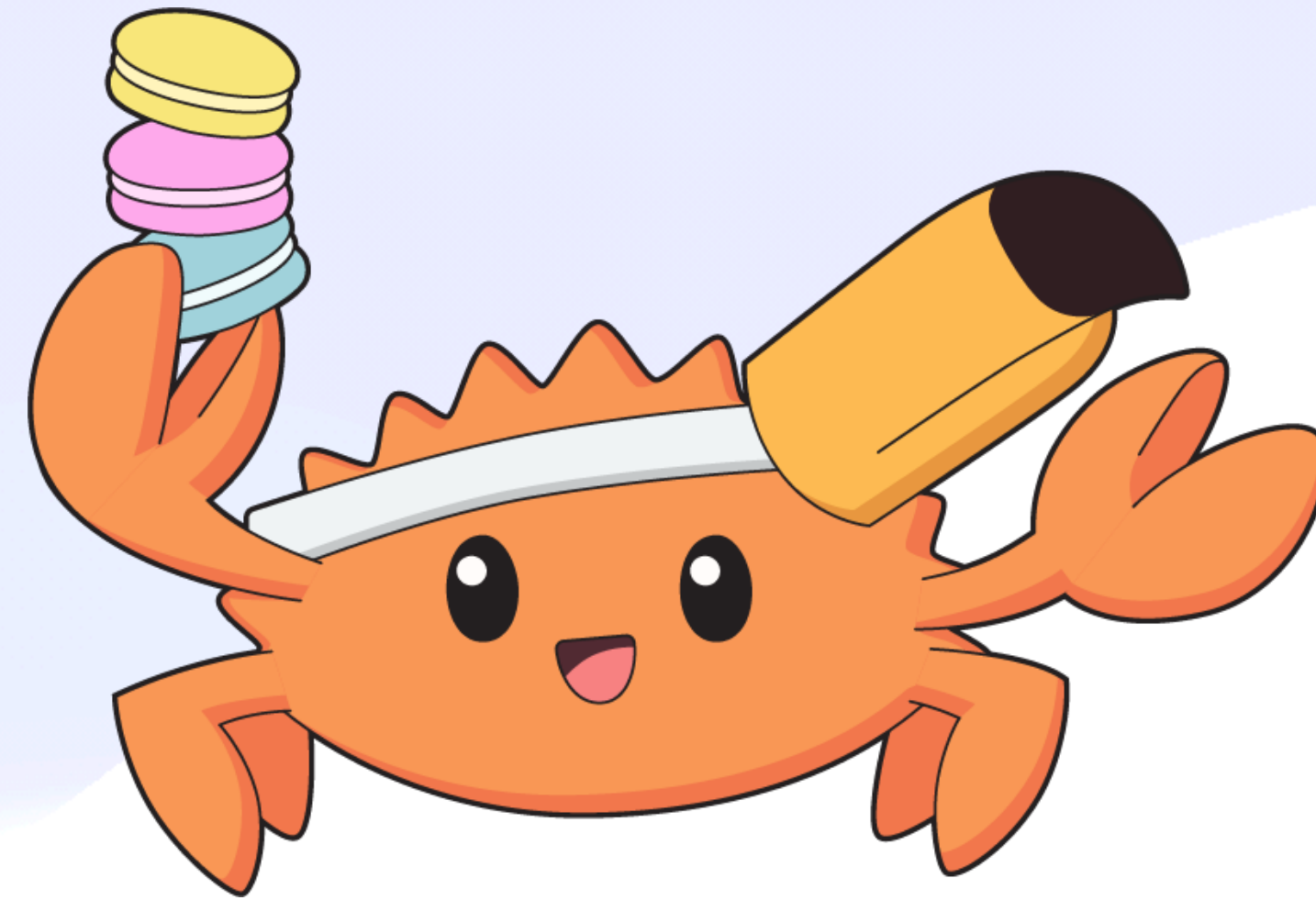
# *Honest Model, Simple to Use*

- "If you have it, you can use it & share it"
- Closely models auth **ground truth**
- Natural **programming** model "like passing handles"

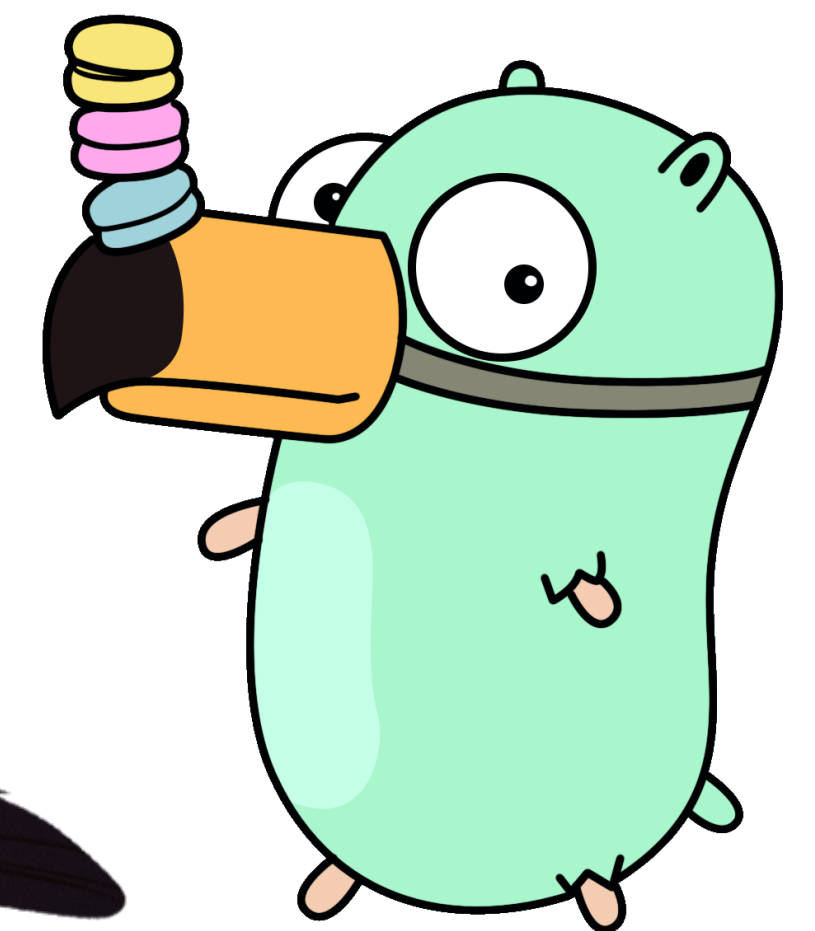
# Resources

## *(Some) Existing Subprojects*

- ◆ <https://github.com/ucan-wg/>
  - ◆ Specs & Improvement Proposals
  - ◆ v1.0 "any moment now"
- ◆ ts-ucan
- ◆ rs-ucan
- ◆ go-ucan
- ◆ hs-ucan
- ◆ AWAKE secure channels & login



AWAKE





<https://ucan.xyz>

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

 ***Thank You, Berlin*** 

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

@expede

# The Freedom of Least Authority

## *Capability Space*

- Fewest resources
- Lowest amount of power
- Least amount of time
- (Revocation considered a last resort)

