

Can zero-knowledge and blockchains help humanity survive?

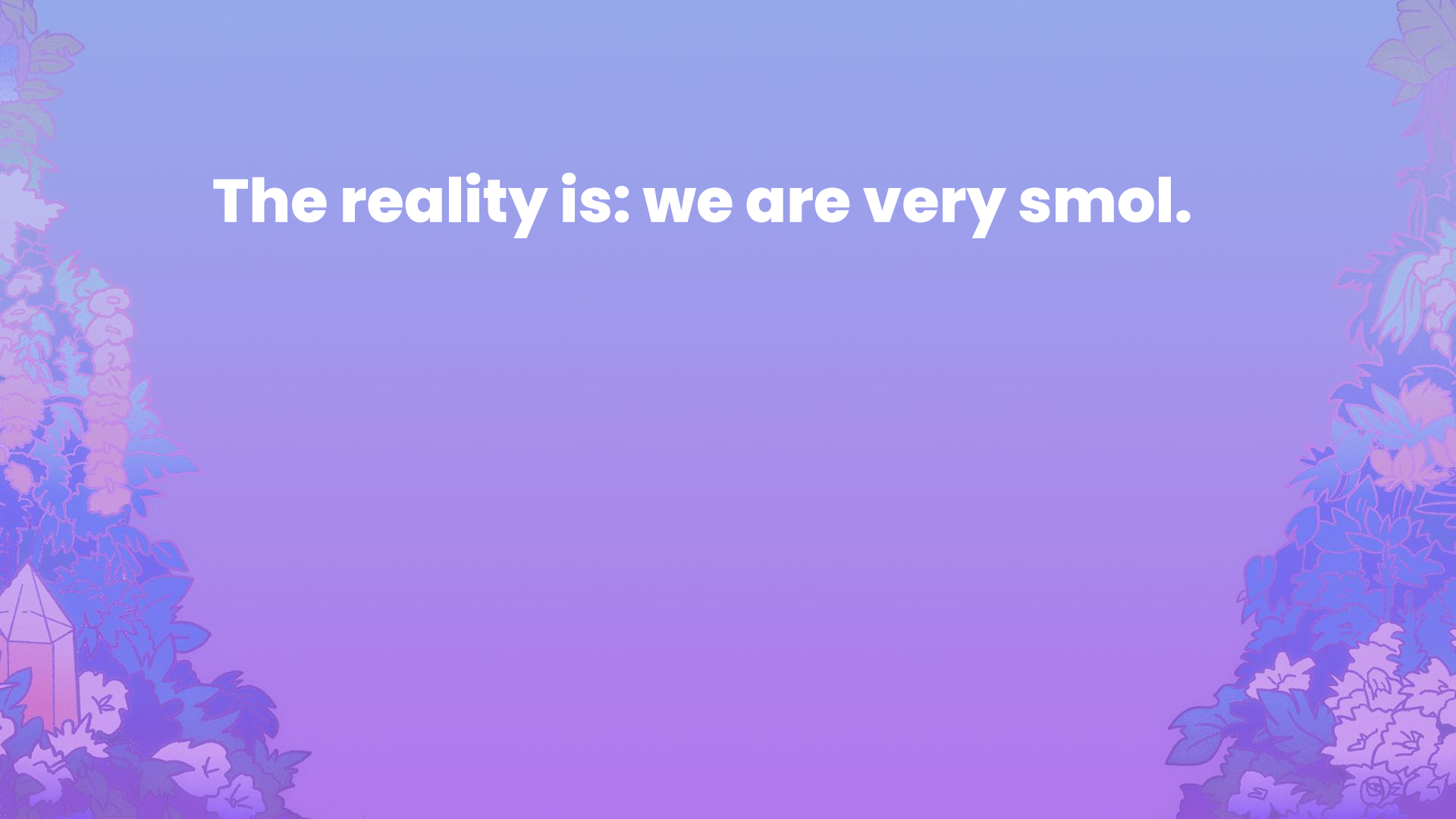
What can we learn from mushrooms?

Lisa Akselrod

Tech. writer, Aztec



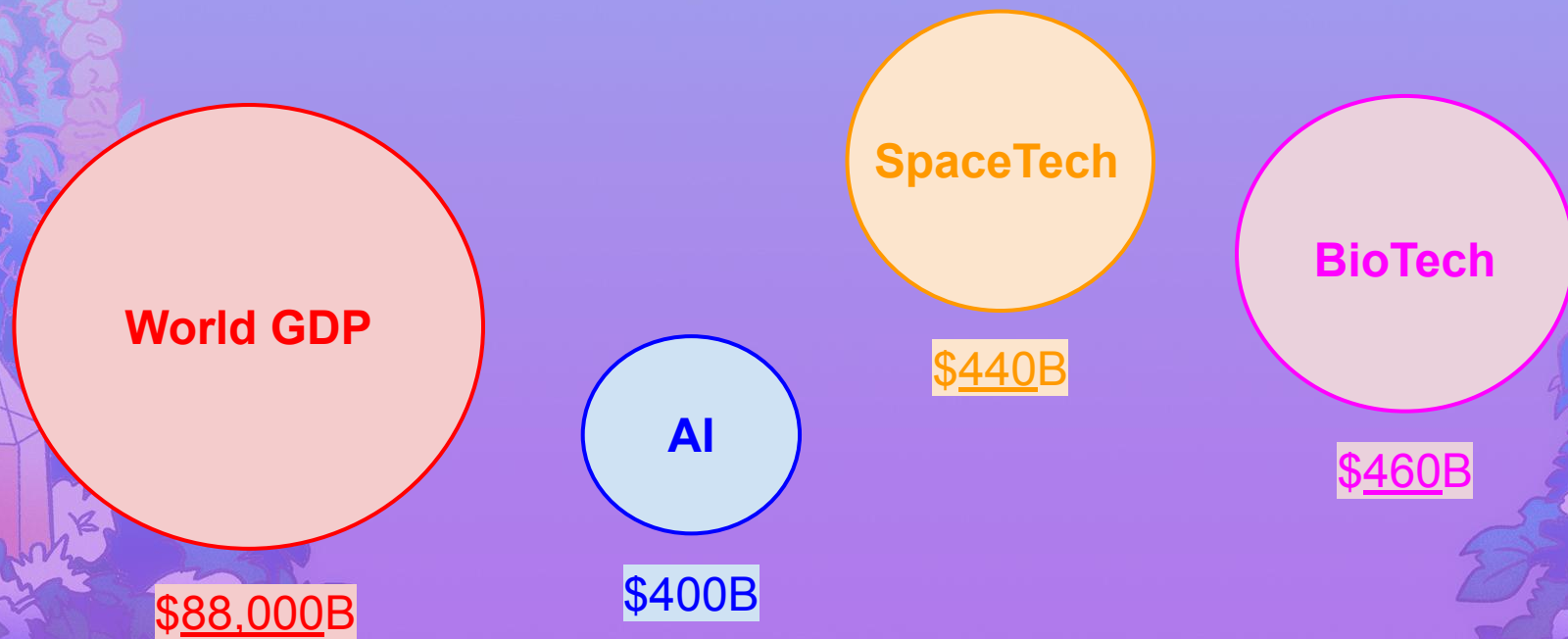
The reality is: we are very smol.



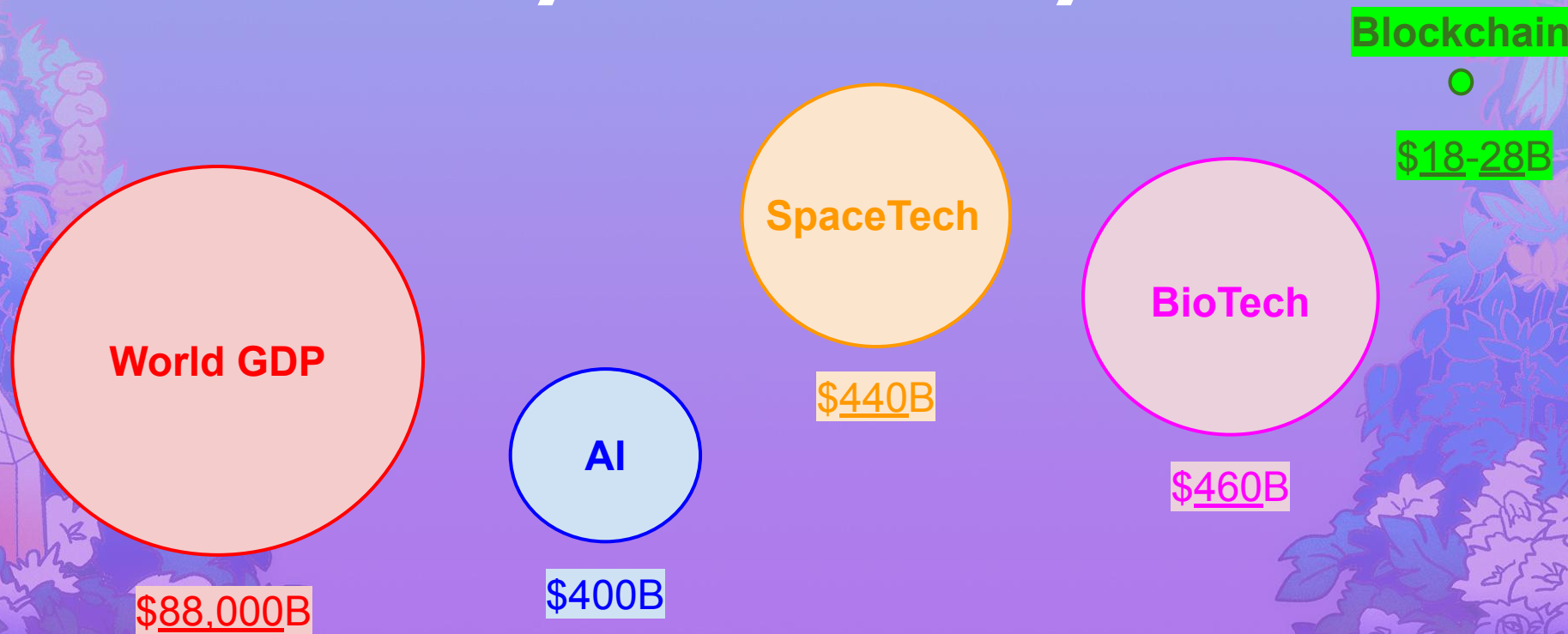
The reality is: we are very smol.



The reality is: we are very smol.



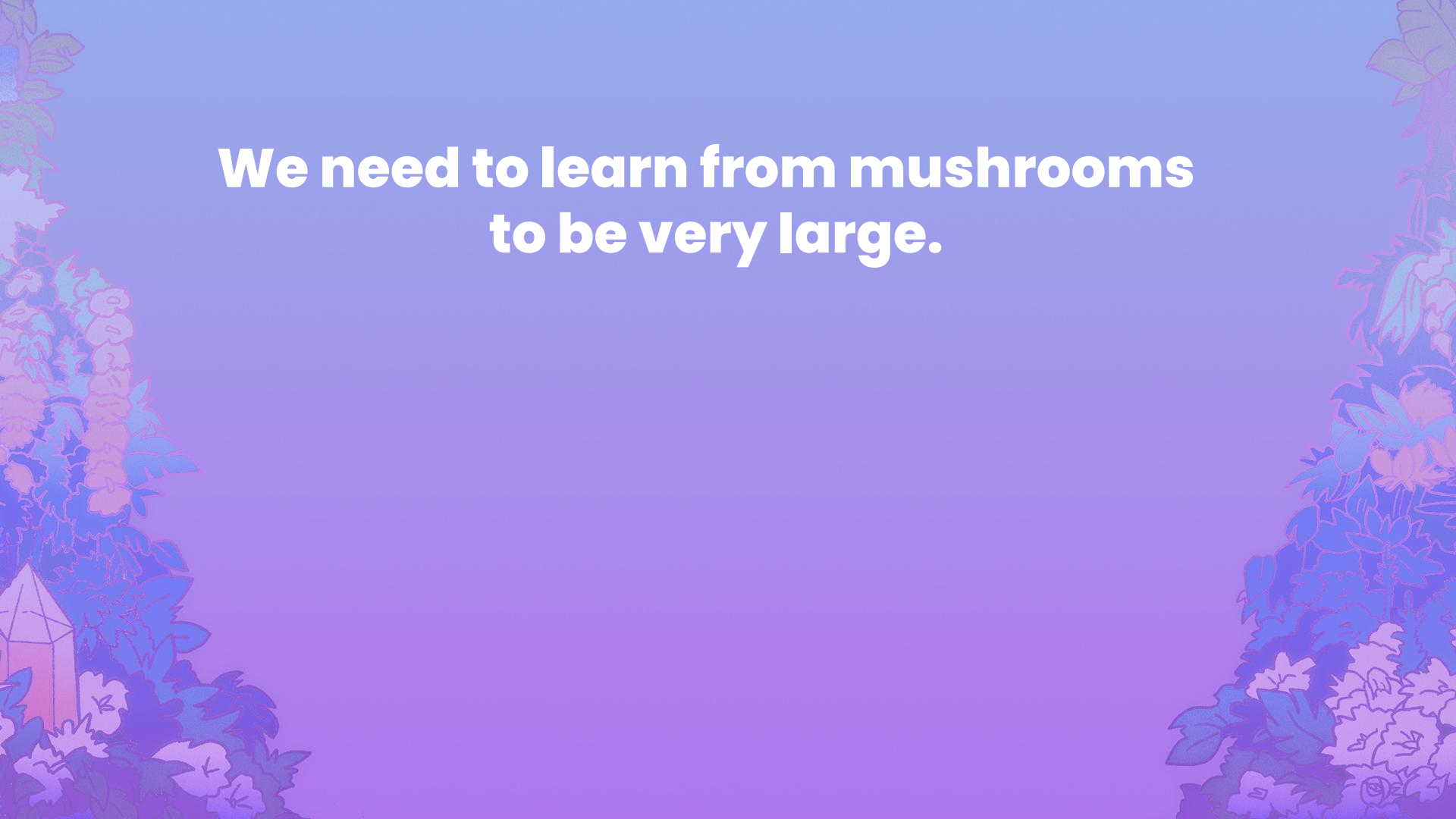
The reality is: we are very smol.



We need to be very large.



**We need to learn from mushrooms
to be very large.**



We need to learn from mushrooms to be very large.

Blockchain:
3 mushroom network

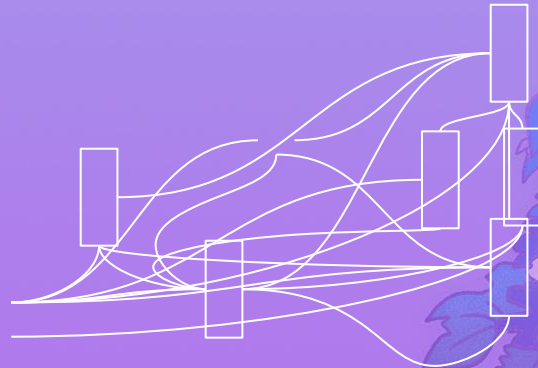


We need to learn from mushrooms to be very large.

Blockchain:
3 mushroom network



Mushrooms:
3 trillion mushroom network

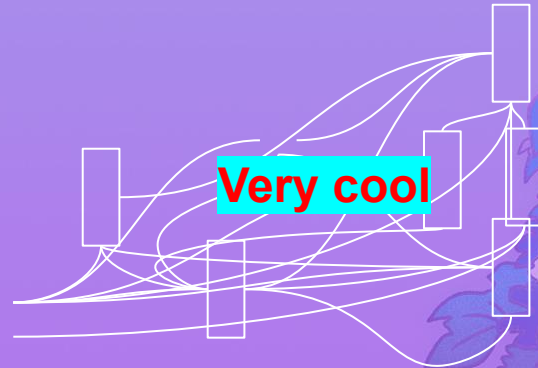


We need to learn from mushrooms to be very large.

Blockchain:
3 mushroom network



Mushrooms:
3 trillion mushroom network



We need to learn from mushrooms to be very large.

Blockchain:
3 mushroom network

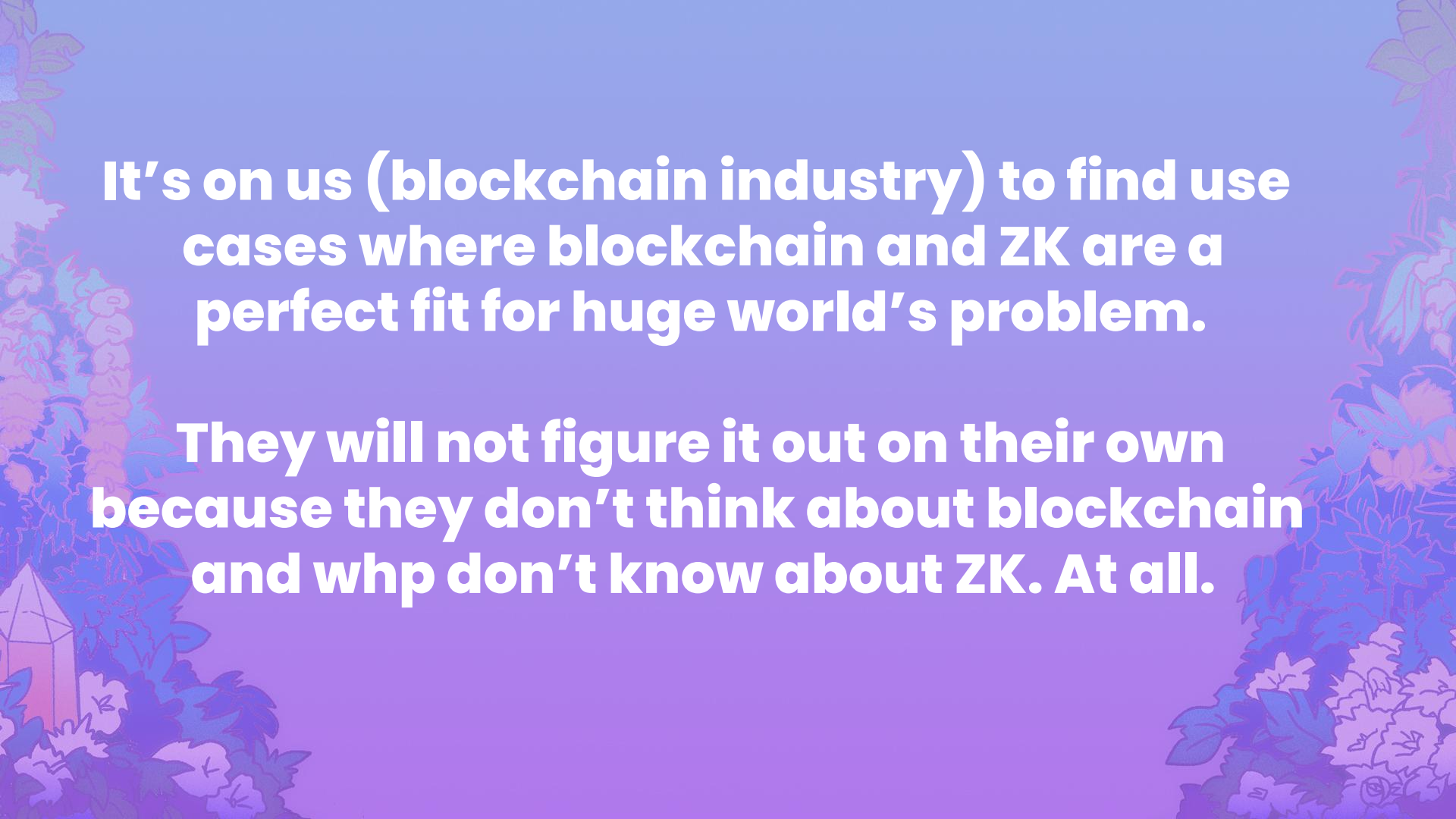
Not very cool



Mushrooms:
3 trillion mushroom network

Very cool





It's on us (blockchain industry) to find use cases where blockchain and ZK are a perfect fit for huge world's problem.

They will not figure it out on their own because they don't think about blockchain and whp don't know about ZK. At all.



ZK for verifiable computations + blockchain for coordination

**Three real-world use cases that are crucial
for humanity survival:**



In the space:

Satellite coordination:

- Many countries operating in the space
- Many of them are not friends
- But they have to coordinate their activity in the space
- How can China prove the US that their satellite won't clash into some US space facility?
 - You promise? I promise.
 - ZKPs for proof of route or proof of hitting the coordinate.
- How should they coordinate these ZKPs by hundreds of parties, for thousands of satellites, 24/7, without disclosing any sensitive information?
 - Privacy-preserving programmable blockchain.

In the agriculture:

Self-piloting agricultural machines coordination:

- In many countries, agriculture is run by self-piloting machines i.e. computers with software running on it.
- If tractors, cultivators, and balers are out of operation for the whole country – its economy stops and the country is in deep economic crises.
- How can a smol human force thousands of machines with different programs running on top to report them what's on their mind?
 - ZKPs
- But what about a network with thousands machines and thousands humans transmitting ZKPs in arbitrary directions 24/7?
 - Privacy-preserving programmable blockchain.

In the nuclear war*:

Nuclear missiles launch coordination:

- If country A has a concern that a country B launched a nuclear missile towards it – its president has several minutes (<5) to call their president and ask 'did you do it?'
- Can we zk-prove that something hasn't happen? Can one prove that they haven't launched the nuclear missile? And if they did, can they prove that this particular country is not a destination?
- I think it's doable.



Can zero-knowledge help
humanity survive?

Can zero-knowledge help
humanity survive?
Yes



Can blockchain help humanity survive?



Can blockchain help humanity survive?
Yes but



Can blockchain help humanity survive?
**Yes but it MUST be privacy-preserving
programmable blockchain.**

No privacy – no blockchain adoption. That simple.

Lisa Akselrod

Tech. writer, Aztec

tg: @l_girl

twitter: @cryptobuilder_

