Behind Zupass

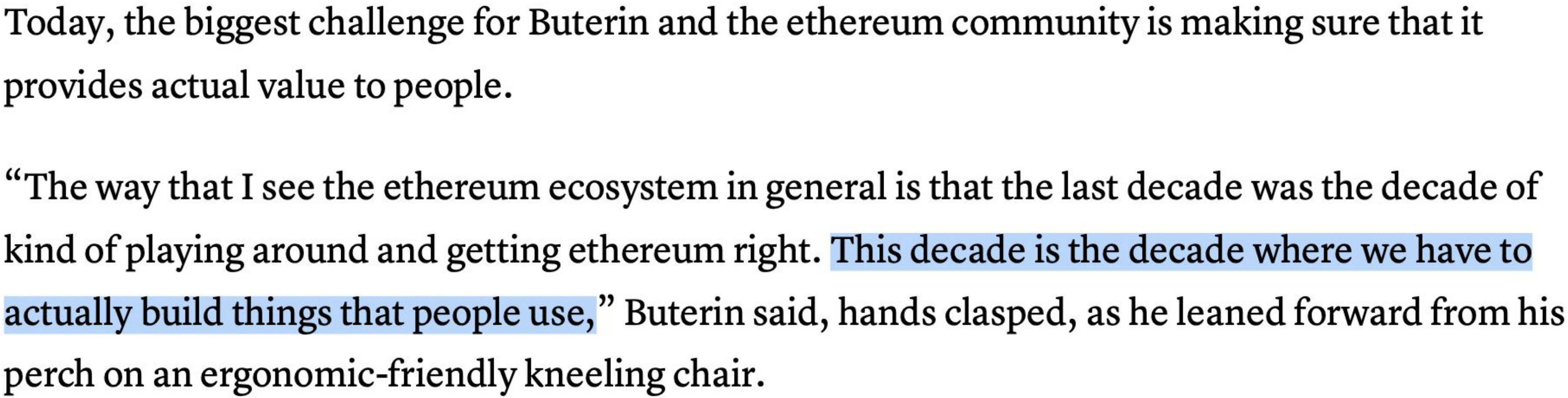
Applied Cryptography For Consumers

Richard Liu

0xPARC

Ethereum That People Use

Ethereum That People Use



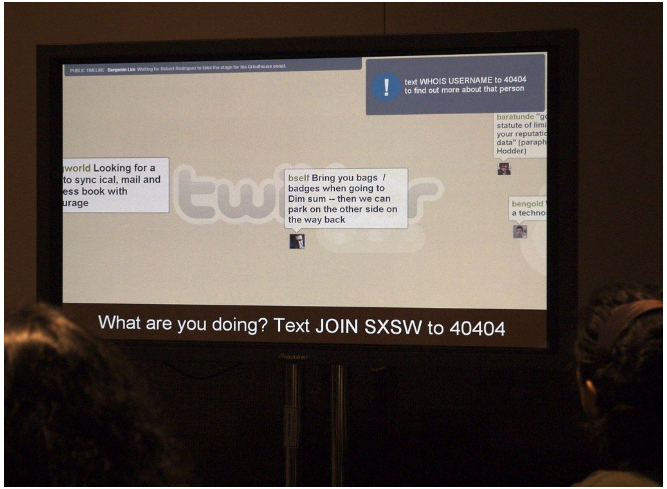
Today, the biggest challenge for Buterin and the ethereum community is making sure that it provides actual value to people.

“The way that I see the ethereum ecosystem in general is that the last decade was the decade of kind of playing around and getting ethereum right. This decade is the decade where we have to actually build things that people use,” Buterin said, hands clasped, as he leaned forward from his perch on an ergonomic-friendly kneeling chair.

Conferences as Ground Zero

Conferences as Ground Zero

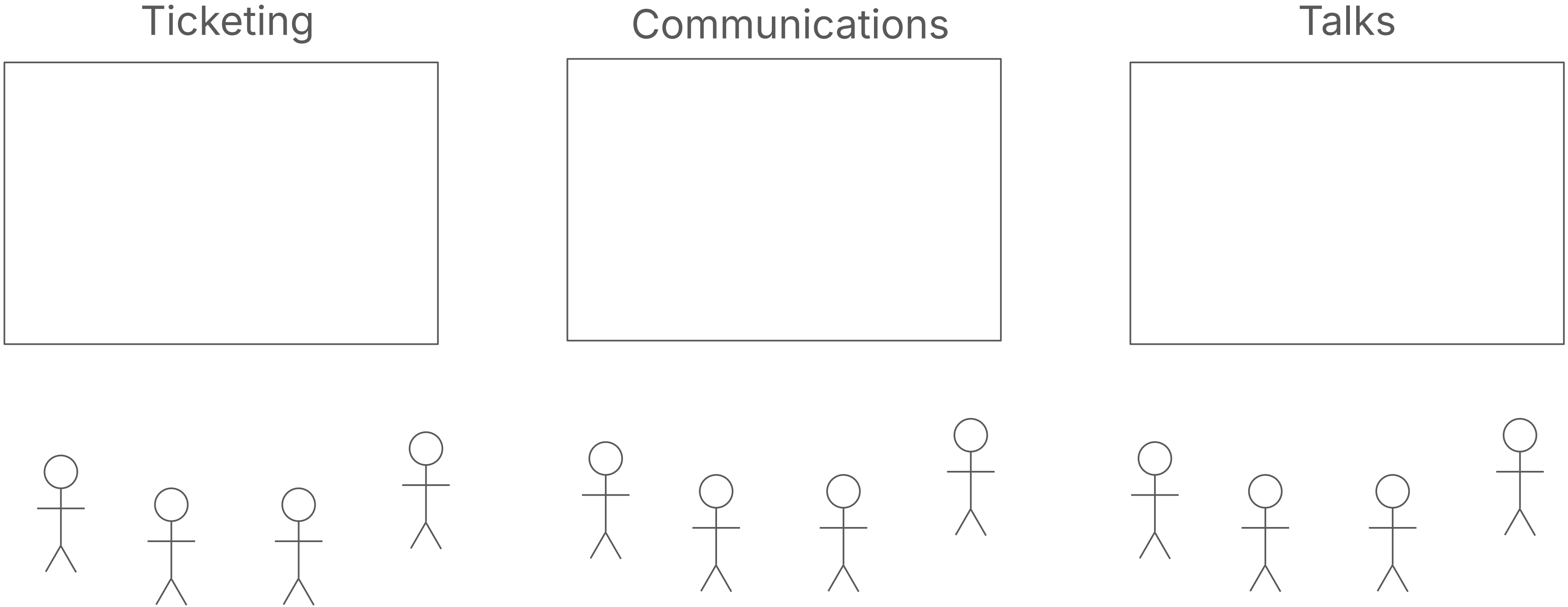
- Conferences are early glimpses of what's possible
- Events can be an accelerated "contact with reality" for early-stage products with a particular audience


PUBLIC TIMELINE Benjamin Lim Waiting for Robert Rodriguez to take the stage for his Grindhouse panel.
text WHOIS USERNAME to 40404 to find out more about that person
baratunde "g statute of limi your reputatio data" (paraph Hodder)
world Looking for a to sync ical, mail and ess book with urage
bself Bring you bags / badges when going to Dim sum -- then we can park on the other side on the way back
bengold a techno
twitter
What are you doing? Text JOIN SXSW to 40404
Pioneer

What did “going to an Ethereum conference” feel like 5-10 years ago?

What did “going to an Ethereum conference” feel like 5-10 years ago?

(from a technology perspective)



Ticketing

Communications

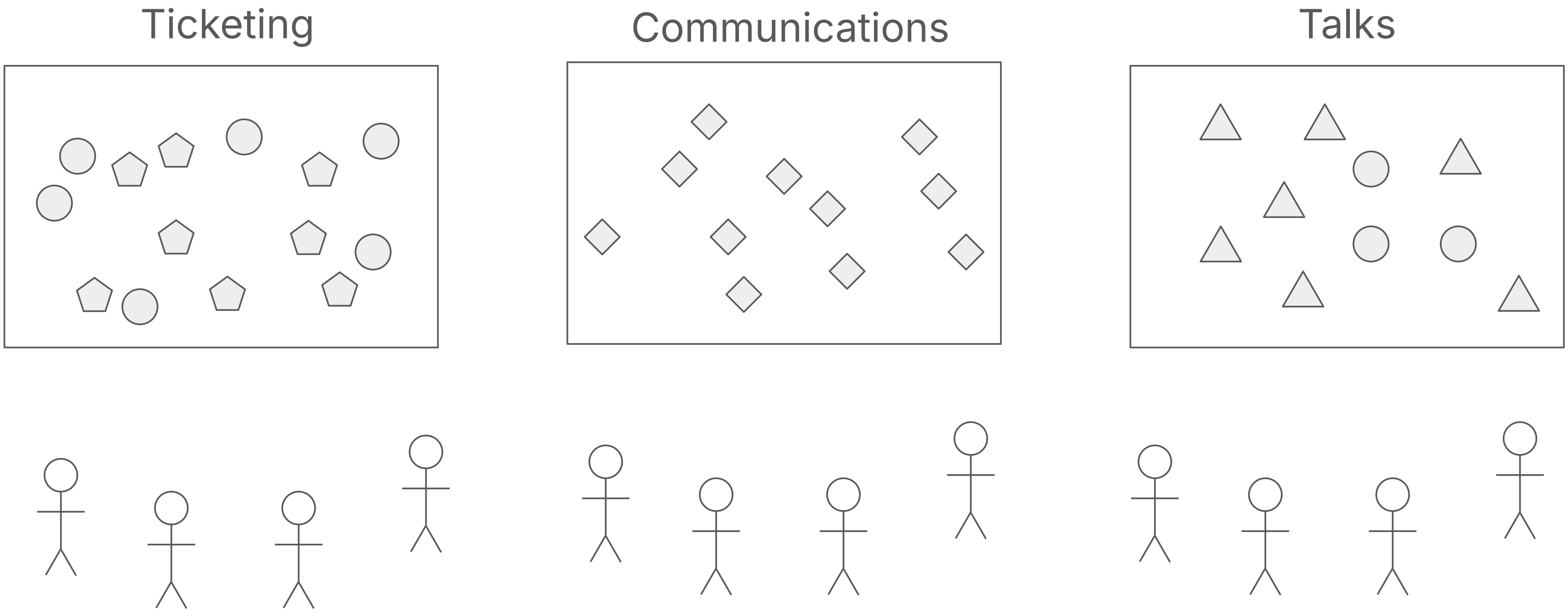
Talks

⬠ Transaction

○ Attendance

◇ Permission (QR)

△ Role, e.g. speaker



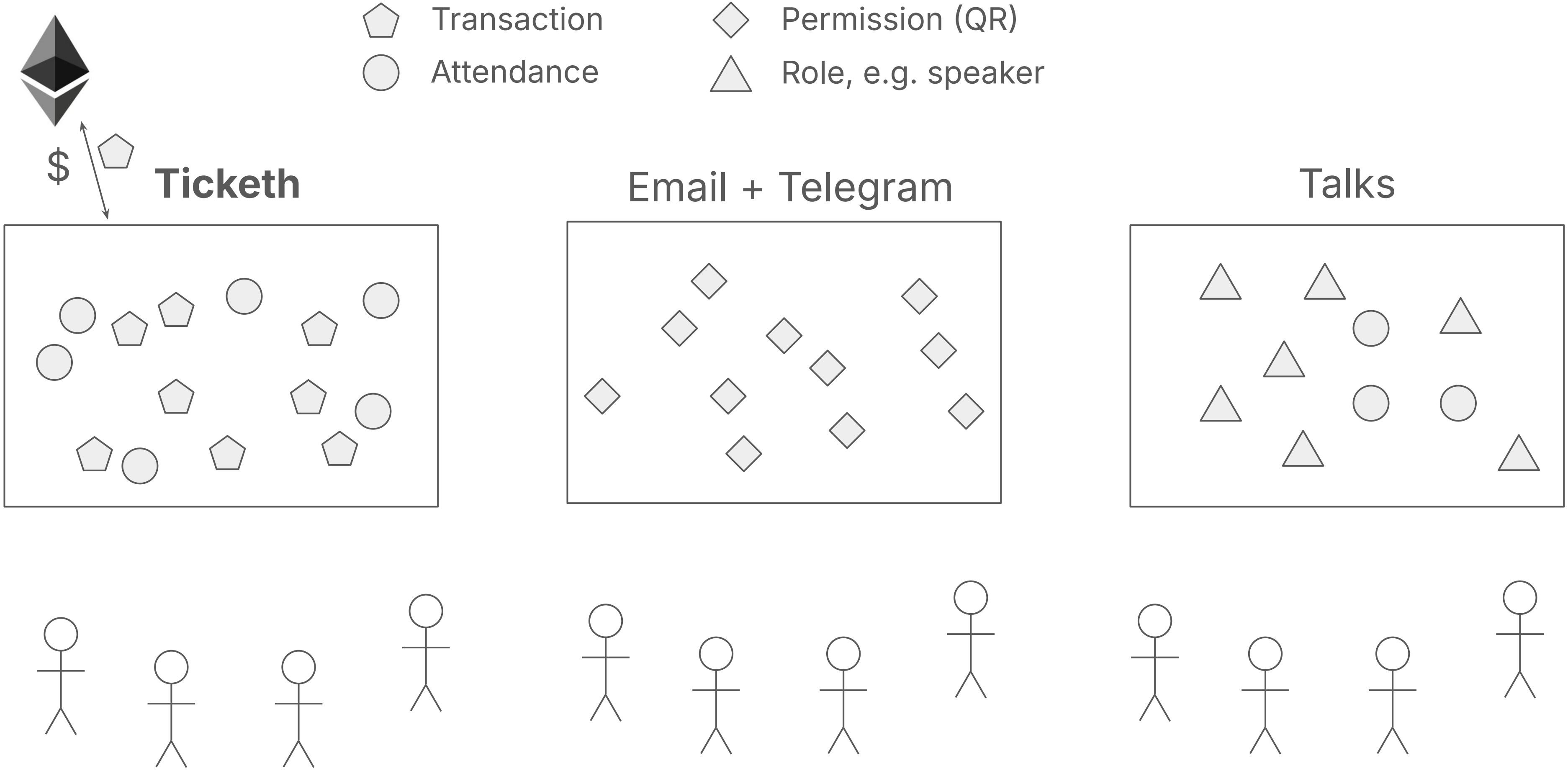
Ticketing

Communications

Talks

What does “going to a Ethereum conference” feel like in 2023?

(from a technology perspective)



⬠ Transaction

○ Attendance

◇ Permission (QR)

△ Role, e.g. speaker

$

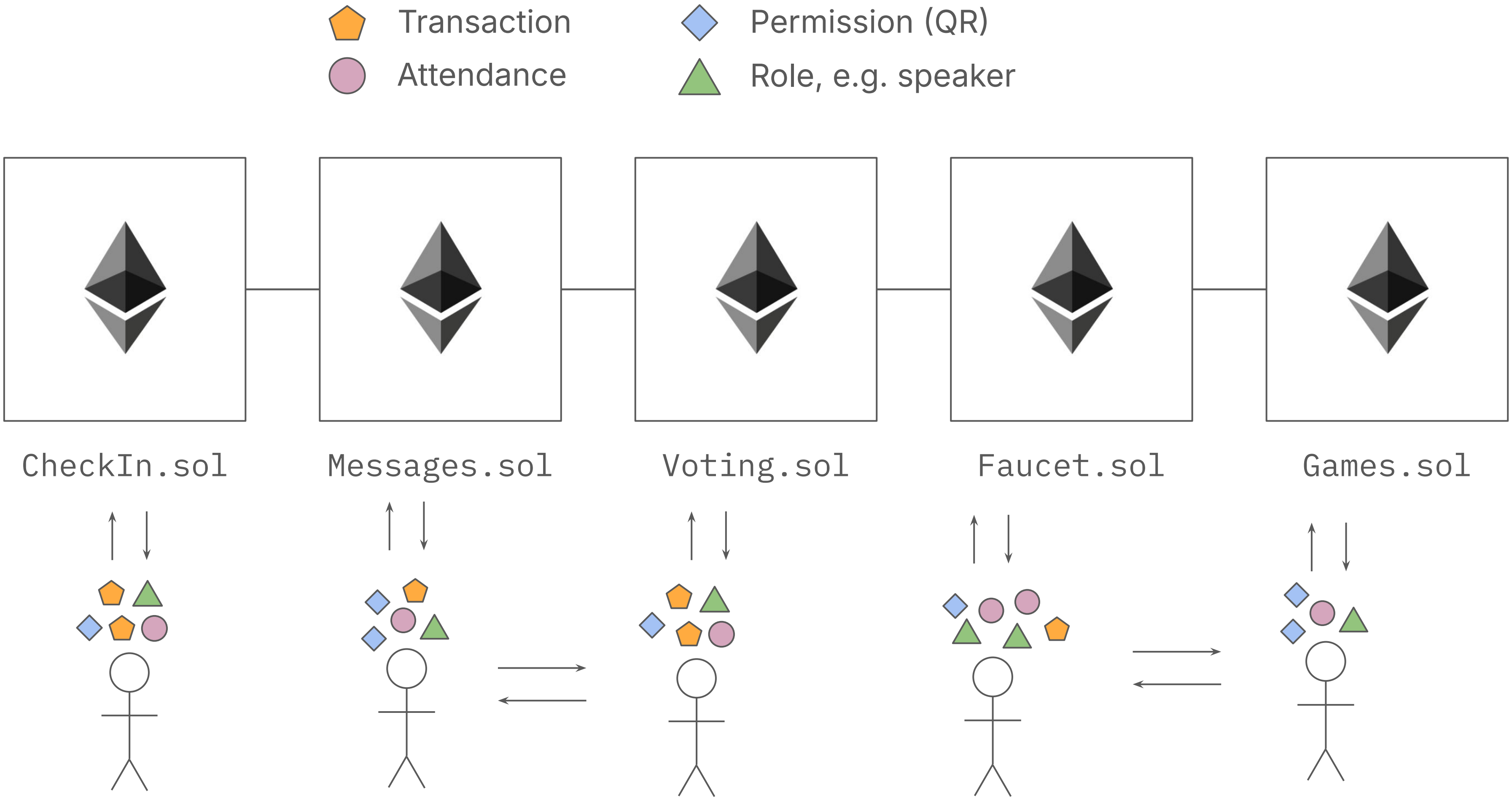
Ticketh

Email + Telegram

Talks

What could “going to an Ethereum conference” feel like in the future?

(from a technology perspective)

⬟ Transaction
● Attendance
◆ Permission (QR)
▲ Role, e.g. speaker
CheckIn.sol
Messages.sol
Voting.sol
Faucet.sol
Games.sol

Hot take: If the Ethereum conference of a few years from now can't substantially "run on Ethereum," *something is wrong*.

Thought exercise: What would it mean to run conferences *entirely* on Ethereum mainnet and rollups?

All-in on Ethereum

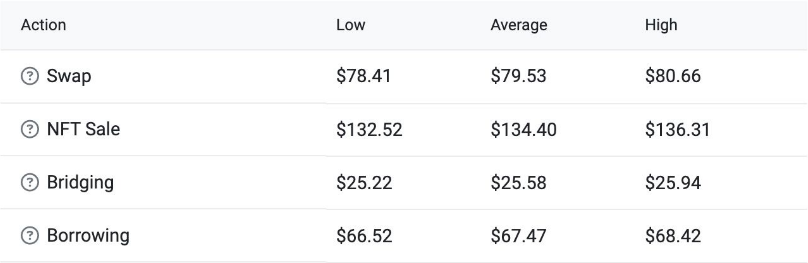
What are the benefits?

- Data is **owned by the user**, not a centralized intermediary
- Data is **composable** across different applications
- Apps can **permissionlessly** request data and compute
- All data and computation on top of that data are **cryptographically verifiable**

All-in on Ethereum

What’s holding us back?

- All state is **public by default** (sans cryptography)
- Most of the world’s data still lives on web2 services
- Onboarding onto smart contract development is **hard**
- Computation on Ethereum is **expensive and high-latency**!



Action	Low	Average	High
Swap	$78.41	$79.53	$80.66
NFT Sale	$132.52	$134.40	$136.31
Bridging	$25.22	$25.58	$25.94
Borrowing	$66.52	$67.47	$68.42

In 2024, going all-in is too high friction

What’s a meaningful first step?

Today: Can we get **80%** of the way there with only **20%** more friction today?

What’s a meaningful first step?

Today: Can we get **80%** of the way there with only **20%** more friction today?

Observation: Zupass has started to make this possible, through its data (PODs) and its ecosystem of apps (“Zapps”).

What’s a meaningful first step?

Today: Can we get **80%** of the way there with only **20%** more friction today?

Observation: Zupass has started to make this possible, through its data (PODs) and its ecosystem of apps (“Zapps”).

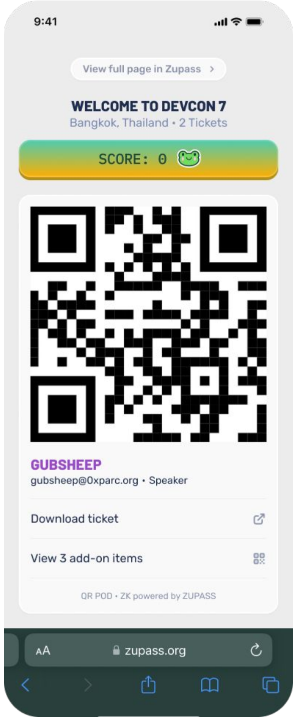
Data is not directly stored on Ethereum, but any computation over that data is easily cryptographically verifiable on Ethereum.

Quick Primer

- **PODs:** Generic key-value data that makes statements about the world, and contains a proof of its own correctness
- **Zapps:** Applications that can request permissions to read, write, update, and request proofs from PODs
- **Zupass:** software for storing and manipulating PODs
- **GPC:** A highly efficient way to make proofs of PODs on lightweight devices by specifying a JSON

Examples

Examples: PODs



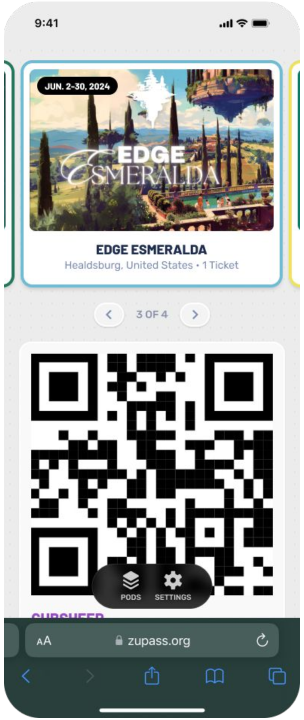
WELCOME TO DEVCON 7

Bangkok, Thailand • 2 Tickets

GUBSHEEP

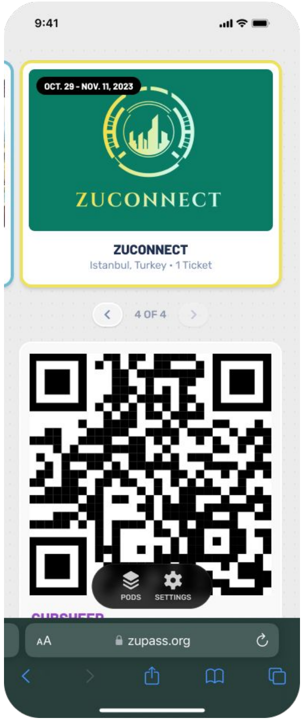
gubsheep@0xparc.org • Speaker

QR POD • ZK powered by ZUPASS



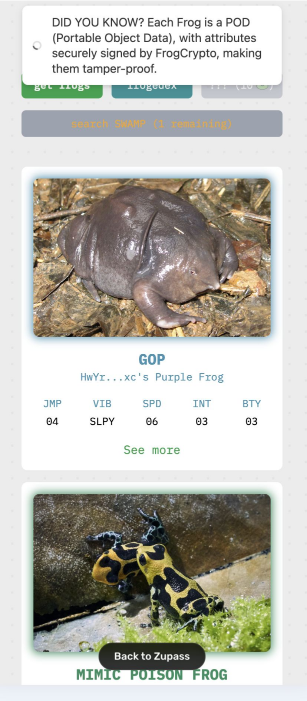
EDGE ESMERALDA

Healdsburg, United States • 1 Ticket



ZUCONNECT

Istanbul, Turkey • 1 Ticket

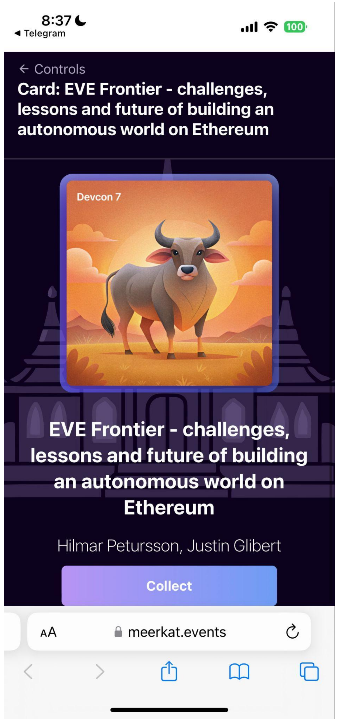

DID YOU KNOW? Each Frog is a POD (Portable Object Data), with attributes securely signed by FrogCrypto, making them tamper-proof.

GOP

HWYr...xc's Purple Frog

JMP	VIB	SPD	INT	BTY
04	SLPY	06	03	03

MIMIC POISON FROG

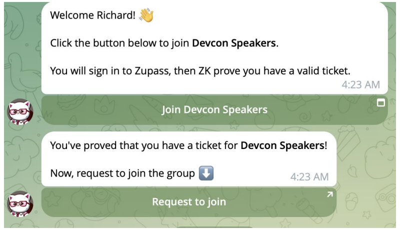


Card: EVE Frontier - challenges, lessons and future of building an autonomous world on Ethereum

EVE Frontier - challenges, lessons and future of building an autonomous world on Ethereum

Hilmar Petursson, Justin Glibert

Examples: Zapps



Welcome Richard! 👋

Click the button below to join **Devcon Speakers**.

You will sign in to Zupass, then ZK prove you have a valid ticket.

4:23 AM

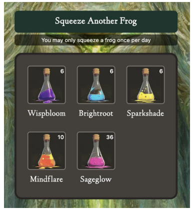
Join Devcon Speakers

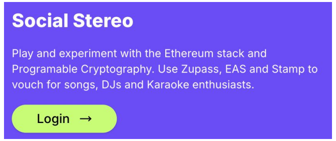
You've proved that you have a ticket for **Devcon Speakers**!

Now, request to join the group ⬇️

4:23 AM

Request to join

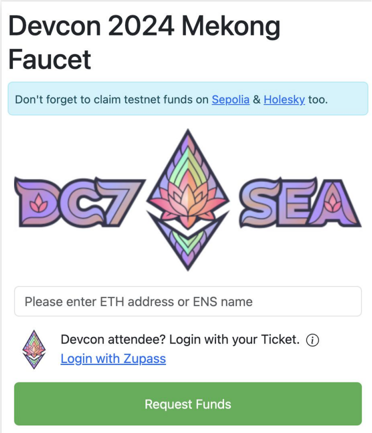




Social Stereo

Play and experiment with the Ethereum stack and Programable Cryptography. Use Zupass, EAS and Stamp to vouch for songs, DJs and Karaoke enthusiasts.

Login →



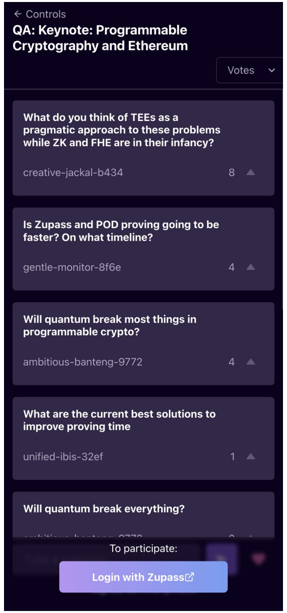
Devcon 2024 Mekong Faucet

Don't forget to claim testnet funds on Sepolia & Holesky too.

Please enter ETH address or ENS name

Devcon attendee? Login with your Ticket. ⓘ
Login with Zupass

Request Funds



← Controls

QA: Keynote: Programmable Cryptography and Ethereum

Votes ⌄

What do you think of TEEs as a pragmatic approach to these problems while ZK and FHE are in their infancy?
creative-jackal-b434 8 ▲

Is Zupass and POD proving going to be faster? On what timeline?
gentle-monitor-8f6e 4 ▲

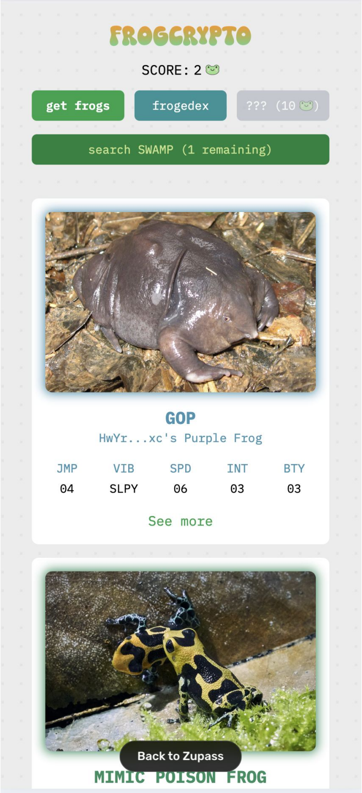
Will quantum break most things in programmable crypto?
ambitious-banteng-9772 4 ▲

What are the current best solutions to improve proving time
unified-ibis-32ef 1 ▲

Will quantum break everything?

To participate:

Login with Zupass



FROGCRYPTO

SCORE: 2 🐸

get frogs | frogedex | ??? (10 🐸)

search SWAMP (1 remaining)

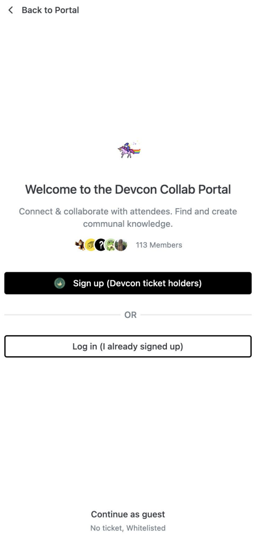
GOP
HwYr...xc's Purple Frog

JMP	VIB	SPD	INT	BTY
04	SLPY	06	03	03

See more

Back to Zupass

MIMIC POISON FROG



‹ Back to Portal

Welcome to the Devcon Collab Portal

Connect & collaborate with attendees. Find and create communal knowledge.

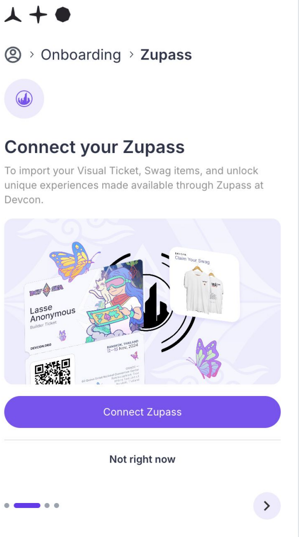
113 Members

Sign up (Devcon ticket holders)

OR

Log in (I already signed up)

Continue as guest
No ticket, Whitelisted



Onboarding › Zupass

Connect your Zupass

To import your Visual Ticket, Swag items, and unlock unique experiences made available through Zupass at Devcon.

Connect Zupass

Not right now

derive novel substances from frogs

enter the lab

With these capabilities, what can “going to Devcon” feel like?

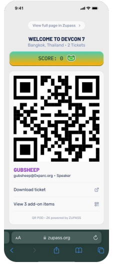
(from a technology perspective)

⬟ Transaction

◆ Permission (QR)

● Attendance

▲ Role, e.g. speaker



9:41

View full page in Zupass >

WELCOME TO DEVCON 7

Bangkok, Thailand • 2 Tickets

SCORE: 0

GUBSHEEP

gubsheep@0xparc.org • Speaker

Download ticket

View 3 add-on items

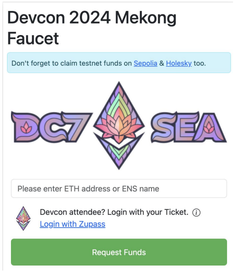
QR POD • ZK powered by ZUPASS

zupass.org

CheckIn.js

Messages.js

Voting.js



Devcon 2024 Mekong Faucet

Don't forget to claim testnet funds on Sepolia & Holesky too.

Please enter ETH address or ENS name

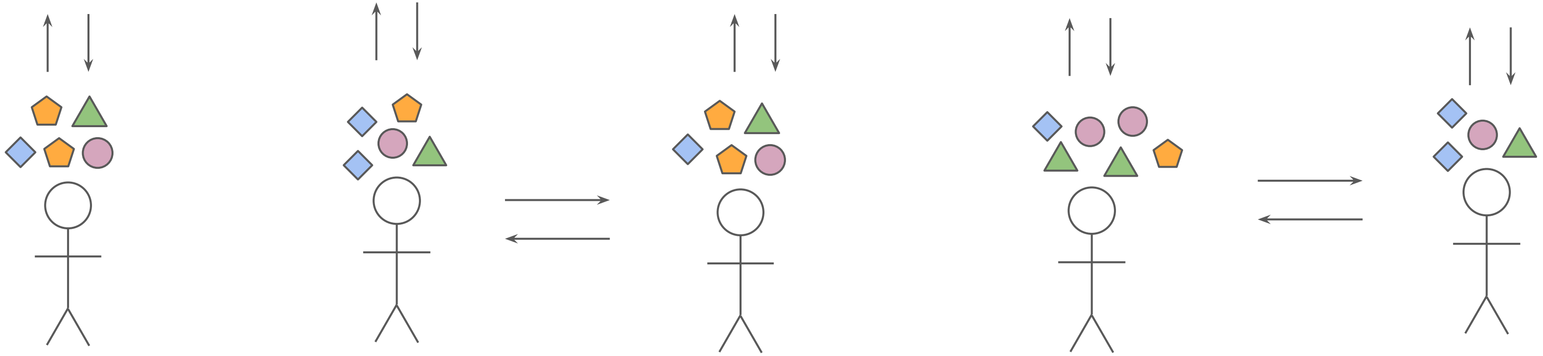
Devcon attendee? Login with your Ticket.

Login with Zupass

Request Funds

Faucet.js

FROGNET.js

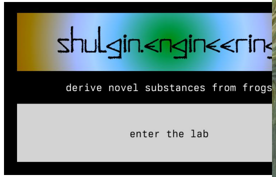


⬟ Transaction

● Attendance

◆ Permission (QR)

▲ Role, e.g. speaker



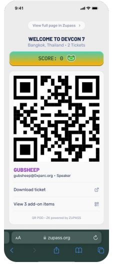
shulgin.engineering

derive novel substances from frogs

enter the lab

Squeeze Another Frog

You may only squeeze a frog once per day



9:41

View full page in Zupass ›

WELCOME TO DEVCON 7

Bangkok, Thailand • 2 Tickets

SCORE: 0

GUBSHEEP

gubsheep@0xparc.org • Speaker

Download ticket

View 3 add-on items

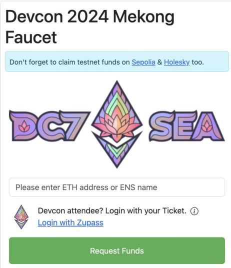
QR POD • ZK powered by ZUPASS

zupass.org

CheckIn.js

Messages.js

Voting.js



Devcon 2024 Mekong Faucet

Don't forget to claim testnet funds on Sepolia & Holesky too.

Please enter ETH address or ENS name

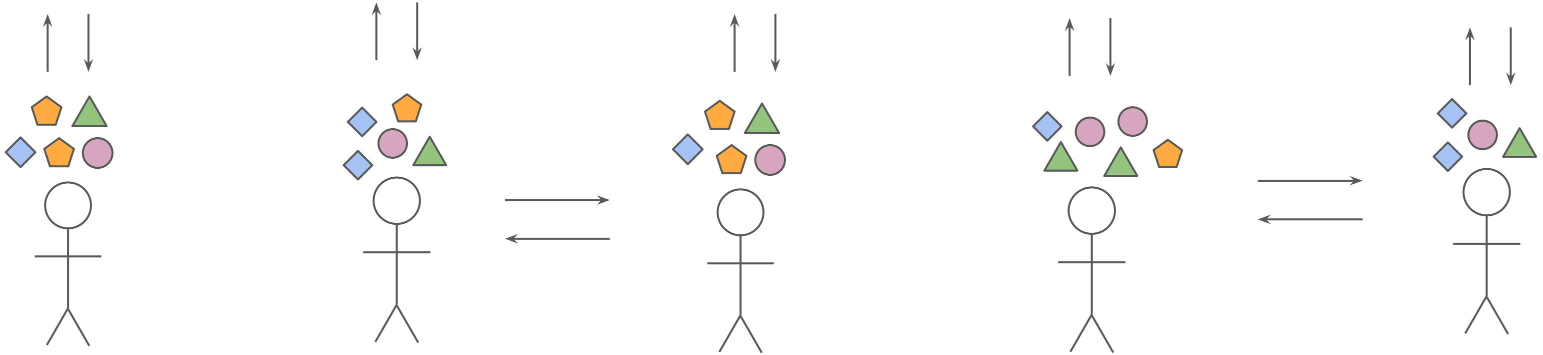
Devcon attendee? Login with your Ticket.

Login with Zupass

Request Funds

Faucet.js

FROGNET.js



Projecting with high error bars, what can “engaging on the internet” feel like?

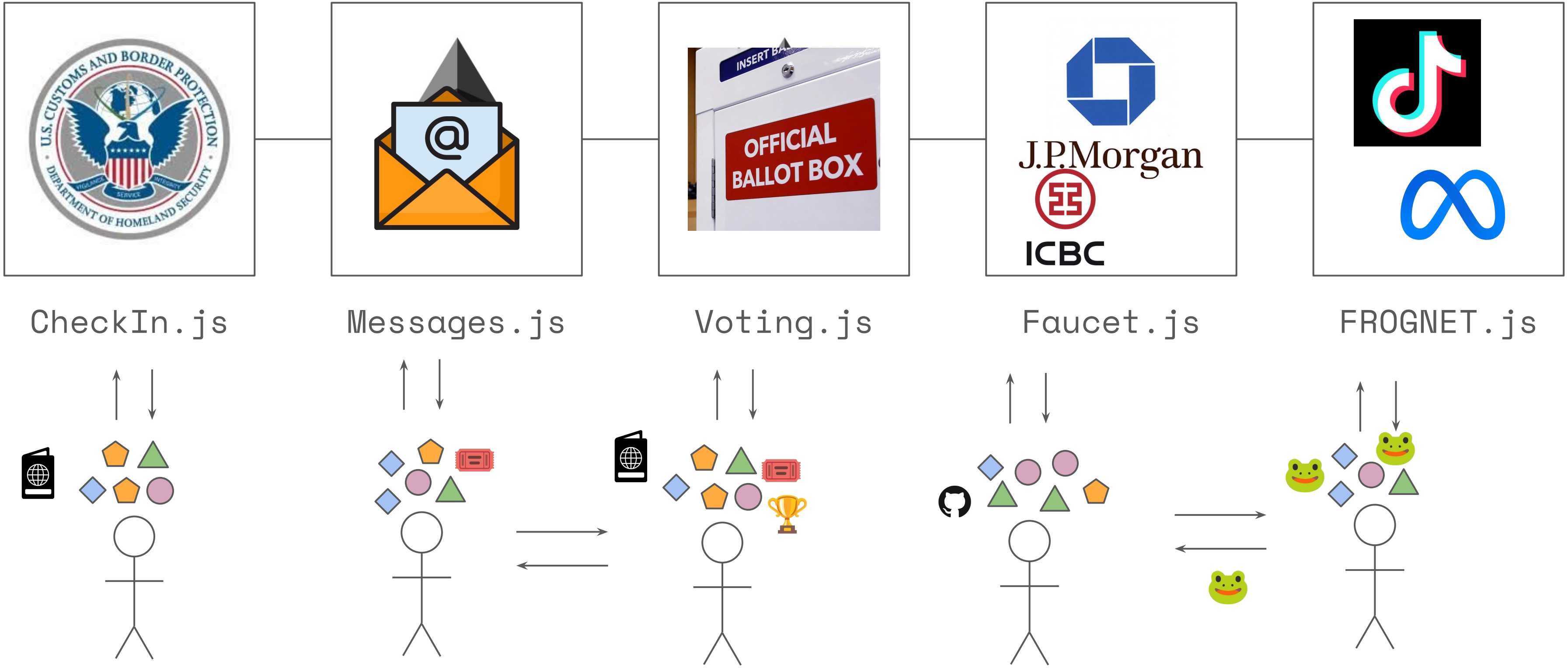
(from a technology perspective)

🏆 Awards

🎟 Past tickets

Third-party accounts

🛂 Signed IDs/passports



CheckIn.js

Messages.js

Voting.js

Faucet.js

FROGNET.js

A Concrete Path Forward

A Concrete Path Forward

Three “project areas”:

- Upgrading core cryptographic technology
- Importing more useful and valuable data
- Expanding the Zapp developer ecosystem

A Concrete Path Forward

Three “project areas”:

- **Upgrading core cryptographic technology**
- Importing more useful and valuable data
- Expanding the Zapp developer ecosystem

Upgrading core cryptographic technology

- We chose a stack in 2023 given the most feasible tech stack at the time
  - **POD/GPC** was our update in early 2024, but the technology continues to evolve!
- Improvements in **recursion** and development of the **PEX** framework allow us to import more data with complex proofs like ZKEmail or arbitrary zkVMs
- Continuing to improve performance and capabilities for client-side cryptography
  - We have upstreamed memory management fixes to the SnarkJS and Semaphore repos
  - More investigations into delegated proving, WebGPU, native proving (e.g. MoPro)

A Concrete Path Forward

Three “project areas”:

- Upgrading core cryptographic technology
- **Importing more useful and valuable data**
- Expanding the Zapp developer ecosystem

⬟ Transaction

◆ Permission (QR)

● Attendance

▲ Role, e.g. speaker

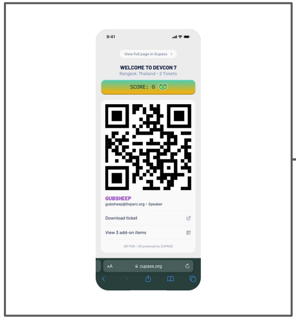
shulgin.engineerin

derive novel substances from frogs

enter the lab

Squeeze Another Frog

You may only squeeze a frog once per day


9:41

View full page in Zupass

WELCOME TO DEVCON 7

Bangkok, Thailand • 2 Tickets

SCORE: 0

GUBSHEEP

gubsheep@0xparc.org • Speaker

Download ticket

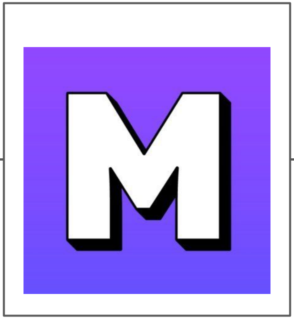
View 3 add-on items

QR POD • ZK powered by ZUPASS

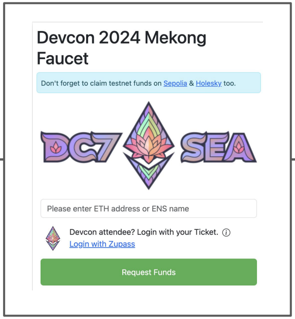
zupass.org

CheckIn.js

Messages.js



Voting.js


Devcon 2024 Mekong Faucet

Don't forget to claim testnet funds on Sepolia & Holesky too.

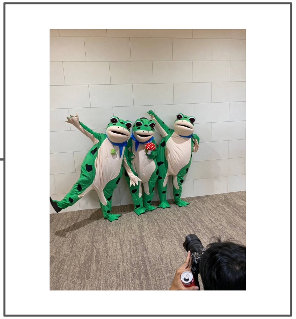
Please enter ETH address or ENS name

Devcon attendee? Login with your Ticket.

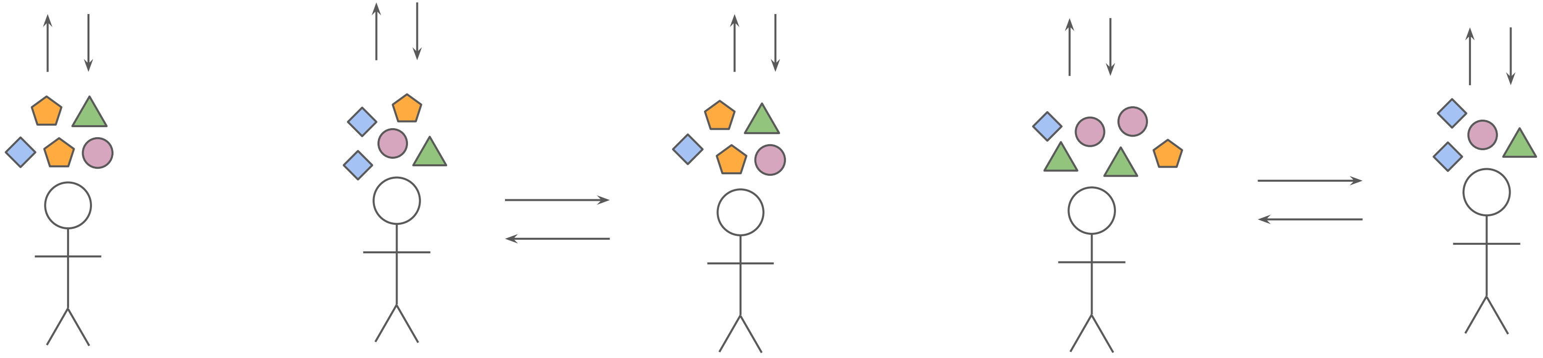
Login with Zupass

Request Funds

Faucet.js



FROGNET.js

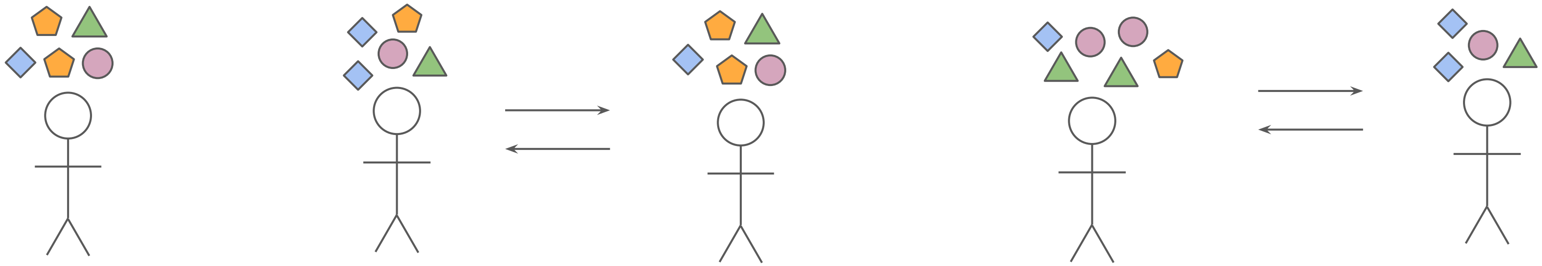


⬟ Transaction

◆ Permission (QR)

● Attendance

▲ Role, e.g. speaker

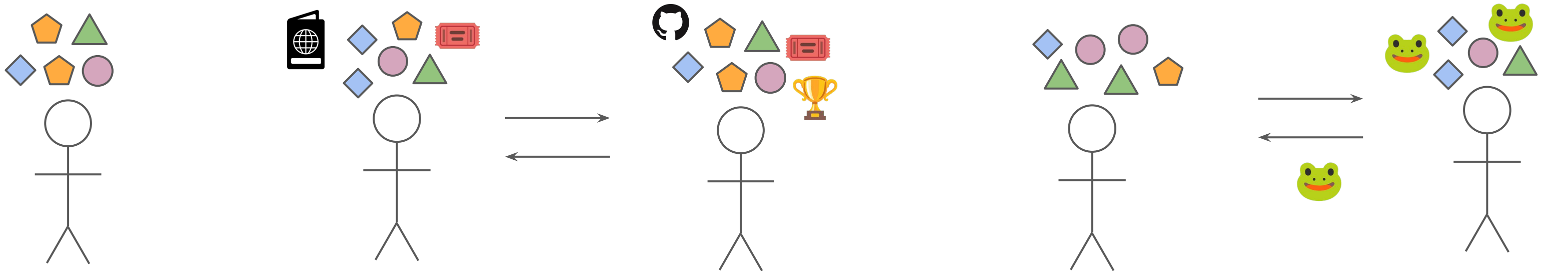


🏆 Awards

🎟️ Past tickets

Third-party accounts

🛂 Signed IDs/passports



Importing more useful and valuable data

- Kicking off conversations with various builders
  - Cryptographic government IDs (Anon Aadhar, OpenPassport, mDL)
  - Hardware attestations (miniPOD)
  - Online data (ZKEmail, TLSNotary)
- Identity and real-world data
  - Universities, governments, financial service providers
- Portability with platforms like Farcaster, Bluesky, X

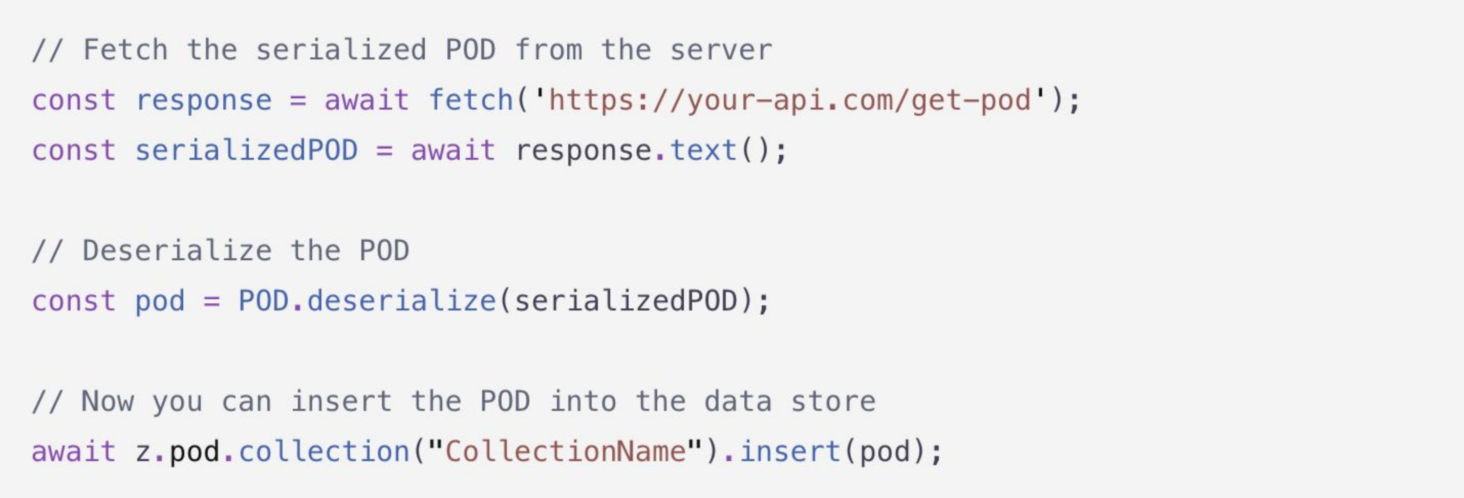
A Concrete Path Forward

Three “project areas”:

- ZK Proofs for Real Use Cases
- Issuing useful and interesting EZ Data
- **Resources for Zapp developers**

Resources for Zapp Developers

- PC for generalist developers – cryptography expertise not required
- Starter kits and libraries for curious developers in <10 lines of code
  - Takes hackers hours, not weeks, to ship an exciting application
  - To learn more, **Building Consumer Apps with PC** workshop on **Friday @ 2:15pm**



```
// Fetch the serialized POD from the server
const response = await fetch('https://your-api.com/get-pod');
const serializedPOD = await response.text();

// Deserialize the POD
const pod = POD.deserialize(serializedPOD);

// Now you can insert the POD into the data store
await z.pod.collection("CollectionName").insert(pod);
```

Resources for Zapp Developers

Resources:

- Documentation at pod.org
- Telegram group at t.me/zupass

Upcoming sessions:

- **Today, 2:30pm:** Introducing Provable Object Data (POD)
- **Today, 3pm:** A Deep Dive into ZK Proofs of PODs
- **Tomorrow, 10am:** Programmable / Frogrammable Cryptography CLS
    - Build a Zapp with PODs @ **2:15pm**

fin