2024

Dear [context],

[message]

Signed by,
An anonymous human that has not signed a message in [context] before.

Dear Emerging Project,

Please airdrop to 0xaf5753765.

--- Anon human

A way of signing messages as a *unique anonymous human*.

at World, always combined with Zero-Knowledge Proofs

Dear DAO,

Please allocate 23 tokens to a quadratic vote for Approve .

--- Anon human

Dear Farcaster,

Please register @eatscode as my alt.

--- Same anon human as before.

Dear Farcaster,

Please register @recmo as belonging to a real human.

--- Anon human

World Foundation

2024

Proof of Human

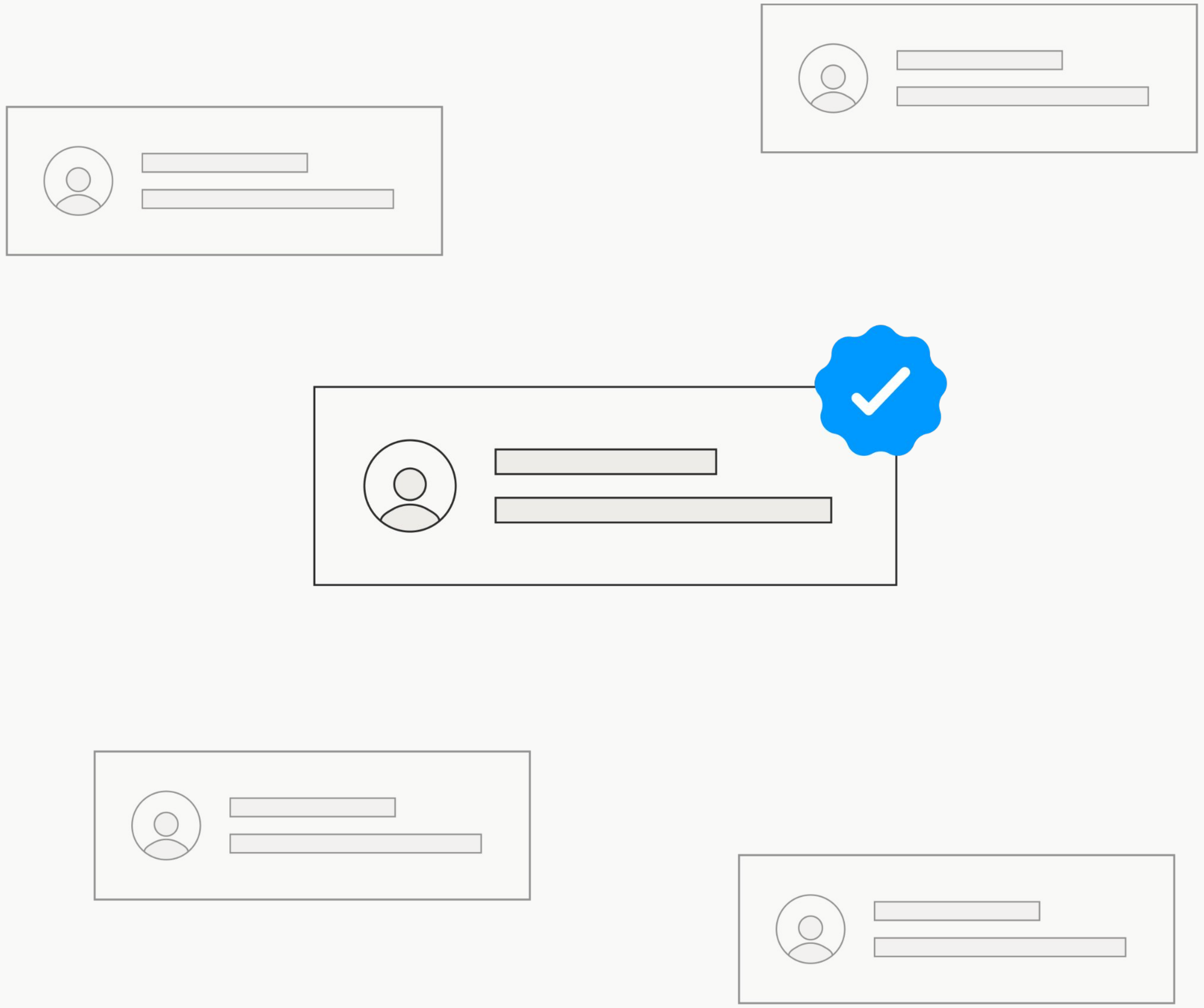
Privacy, Biometrics and Why it Needs Ethereum

Remco Bloemen

1

What is Proof of Personhood?

Proof of Personhood

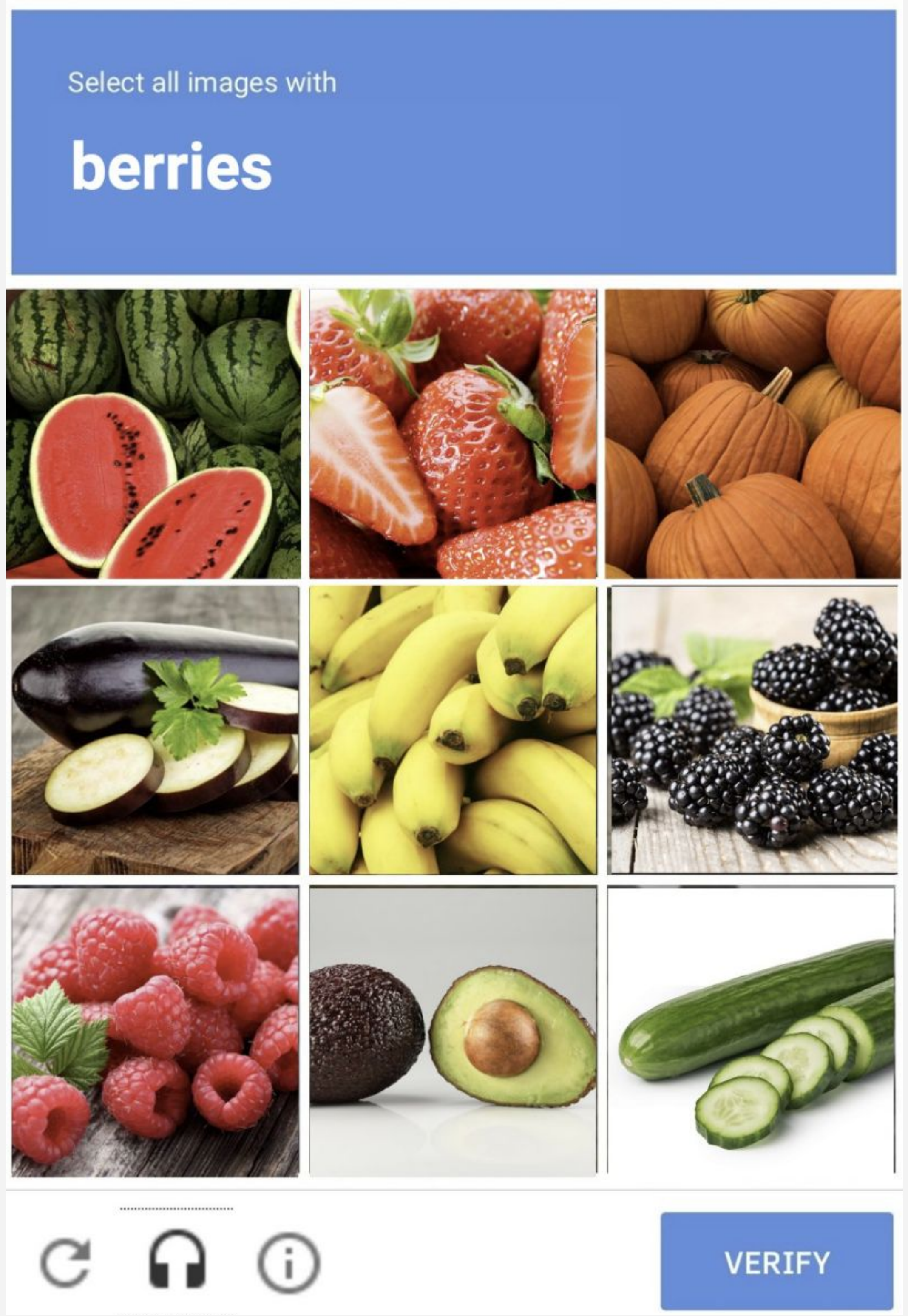


A way to limit account registration to few (ideally one) per human.

What is it not?

It is not a CAPTCHA.

No human-in-the-loop required,
humans can still automate their accounts.


Select all images with

berries

Fig. Separating humans from BOTanists.

Why do we want Proof of Personhood?

AI will make it impossible to distinguish on behavior.

AI fueled economic disruption requires human oriented financial solutions.

Individual as a programmable primitive.

Strong decentralization.

Financial primitives with a concept of individual (insurance, loans, pensions, UBI, etc.)

World Chain human prioritized blockspace.

Sybil resistance.

Limit spam bots.

Why would we not want Proof of Personhood?

“Unique human” often just a proxy for a more precise requirement.

i.e. don't ban bots, but think about what would be the requirements to make the fully qualified participants.

Internet should be neutral on man vs dog vs machine.

No limit on number of Alts.

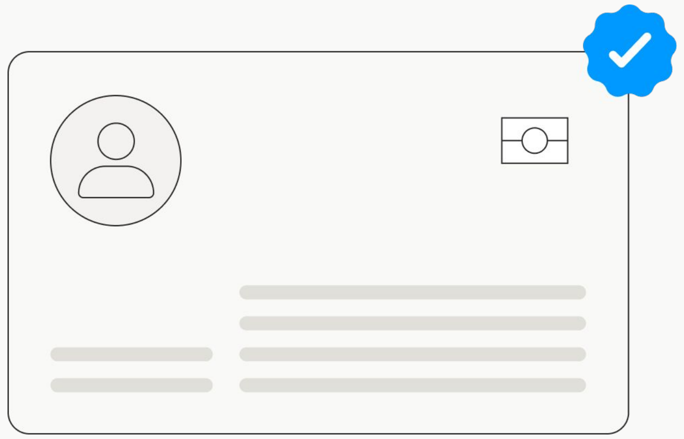
Maximal anonymity means no distinct individuals.

2

How is it implemented?

Oracle problem

Humans are a physical phenomena



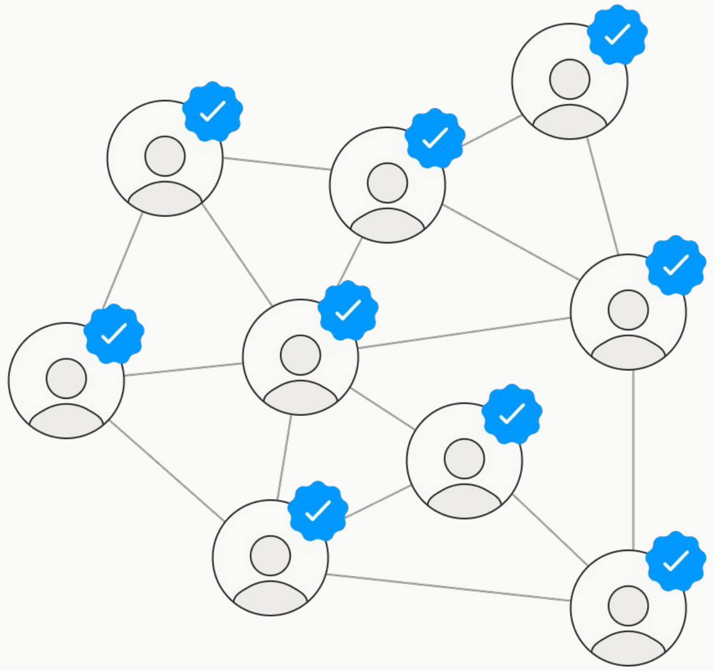
Authority based

Passports

Credit cards

Phone number

Online accounts

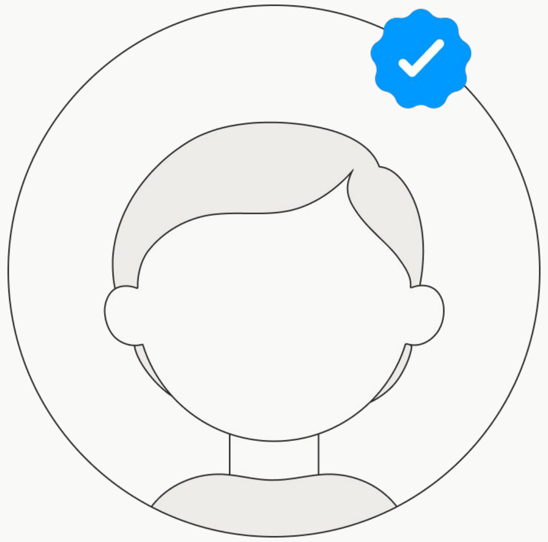


Graph based

Social vouching

Video based vouching

Simultaneous captcha solving



Biometric based

Face

Fingerprint

Iris

Authority based

Passports, credit cards, phone number, etc

Strengths

Conventional solution

Easily scalable

Easy to implement

ZK-eMRTD strongprivacy and good uniqueness

Can proof more than humanness

Weaknesses

Good to weak uniqueness

Weak inclusivity

Central authority(SIM Swapping)

Active verification required.

Reveals personal information (without ZK)

Transferable

Graph based

Social graphs, video vouching, simultaneous captcha solving

Strengths

Decentralized

Weaknesses

Clique attack

Some hard to scale

Some reveal face or social graph

May not be AI resistant.

Reveals social connections, face.

Face/Voice based essentially biometric.

Involved

Biometric based

Face, finger print, iris

Strengths

- Perfect uniqueness
- Non-transferable

Weaknesses

- Immutable
- Trusted sensors
- Physical interaction
- Varying false-match / non-match rates

Biometric

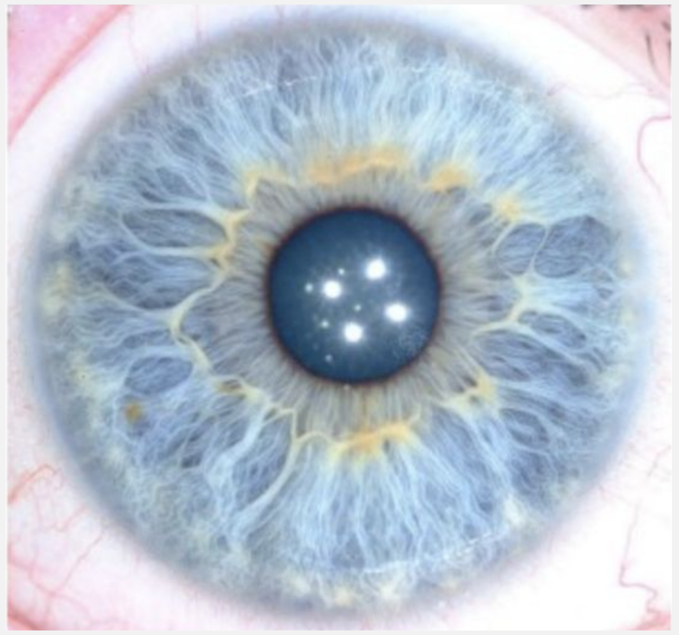
Common misconceptions

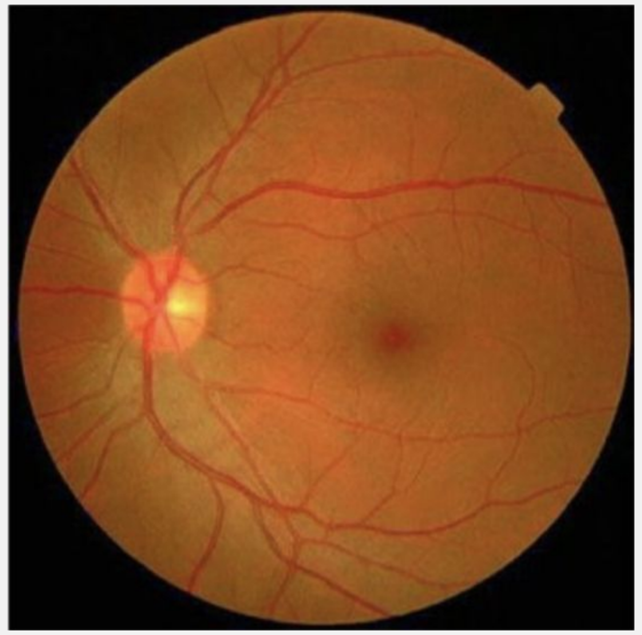
Biometric ≠ Private Key

More like public key: your friends know your face, but only you have it on a body.

Critical to any biometric is the liveness-check

Iris ≠ Retina



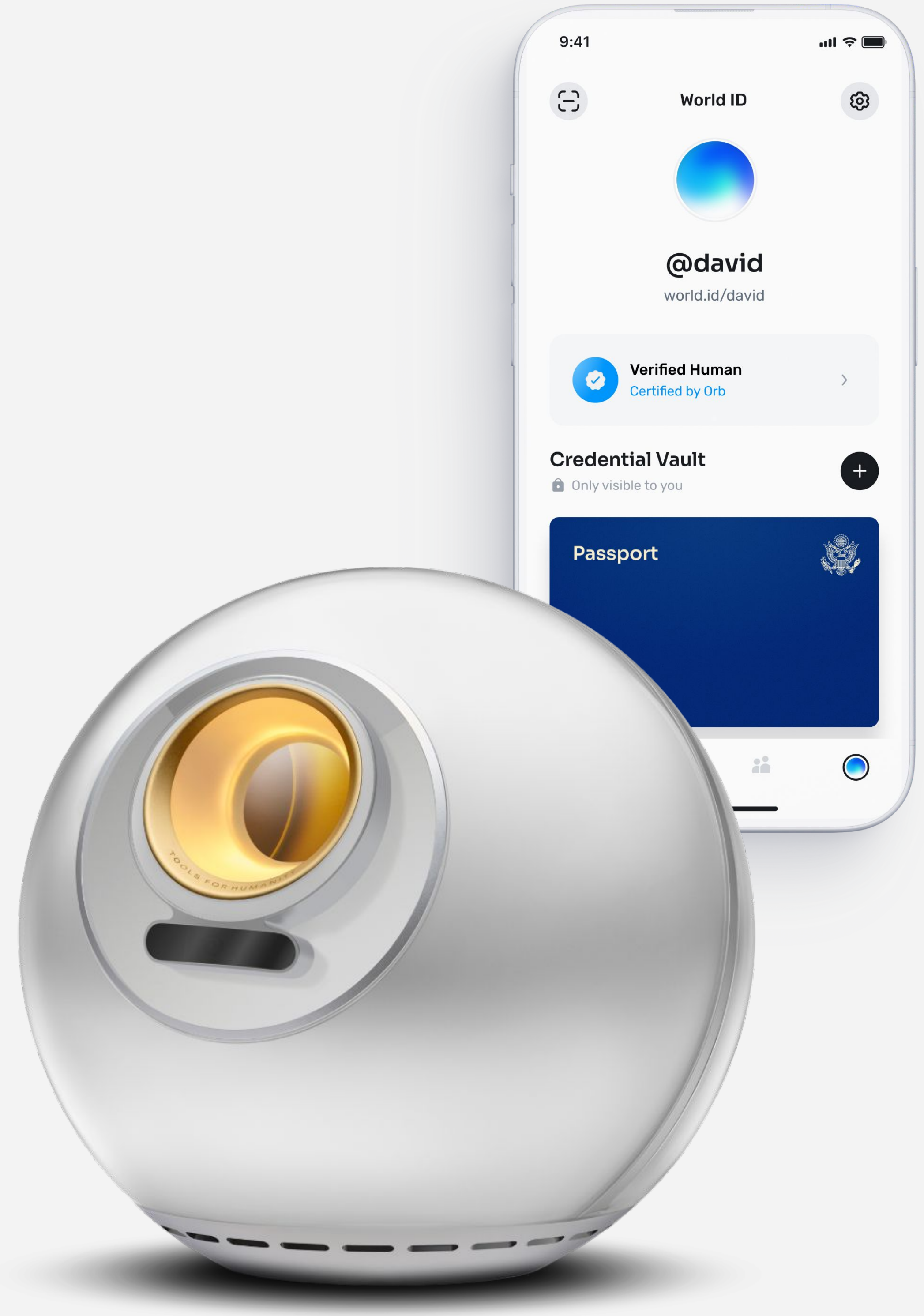


3

World's Approach

World’s tiered system

1. Orb (Iris)
2. NFC Passport
3. Device ID



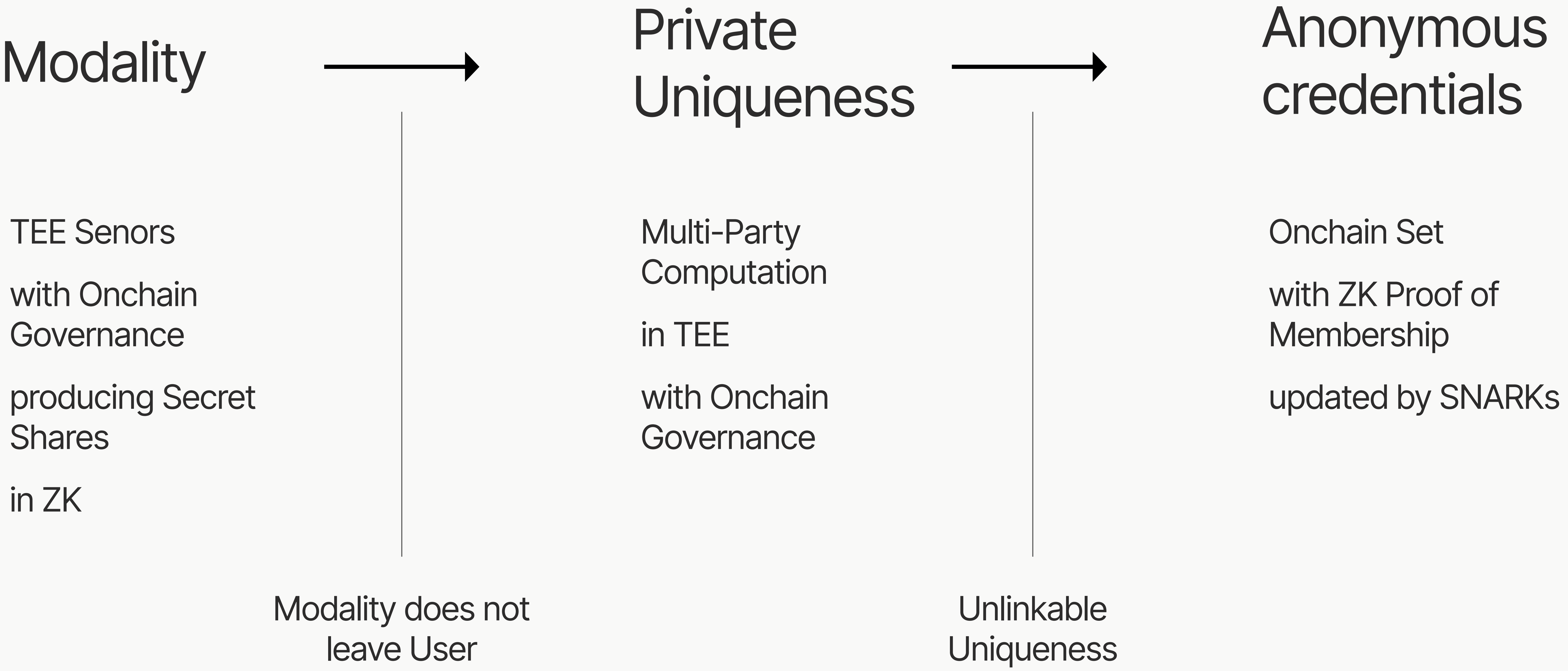
4

World’s implementation

World’s implementation

	Public	Private
Local	Compute,SNARK	ZK-SNARK
Global	Programmable Consensus Algorithms	MPC,FHE,TEE

High level strategy



Modality →

TEE Senors

with Onchain Governance

producing Secret Shares

in ZK

Modality does not leave User

Private Uniqueness →

Multi-Party Computation

in TEE

with Onchain Governance

Unlinkable Uniqueness

Anonymous credentials

Onchain Set

with ZK Proof of Membership

updated by SNARKs

Orb

Multi-Party Compute at World Scale

16M
Users

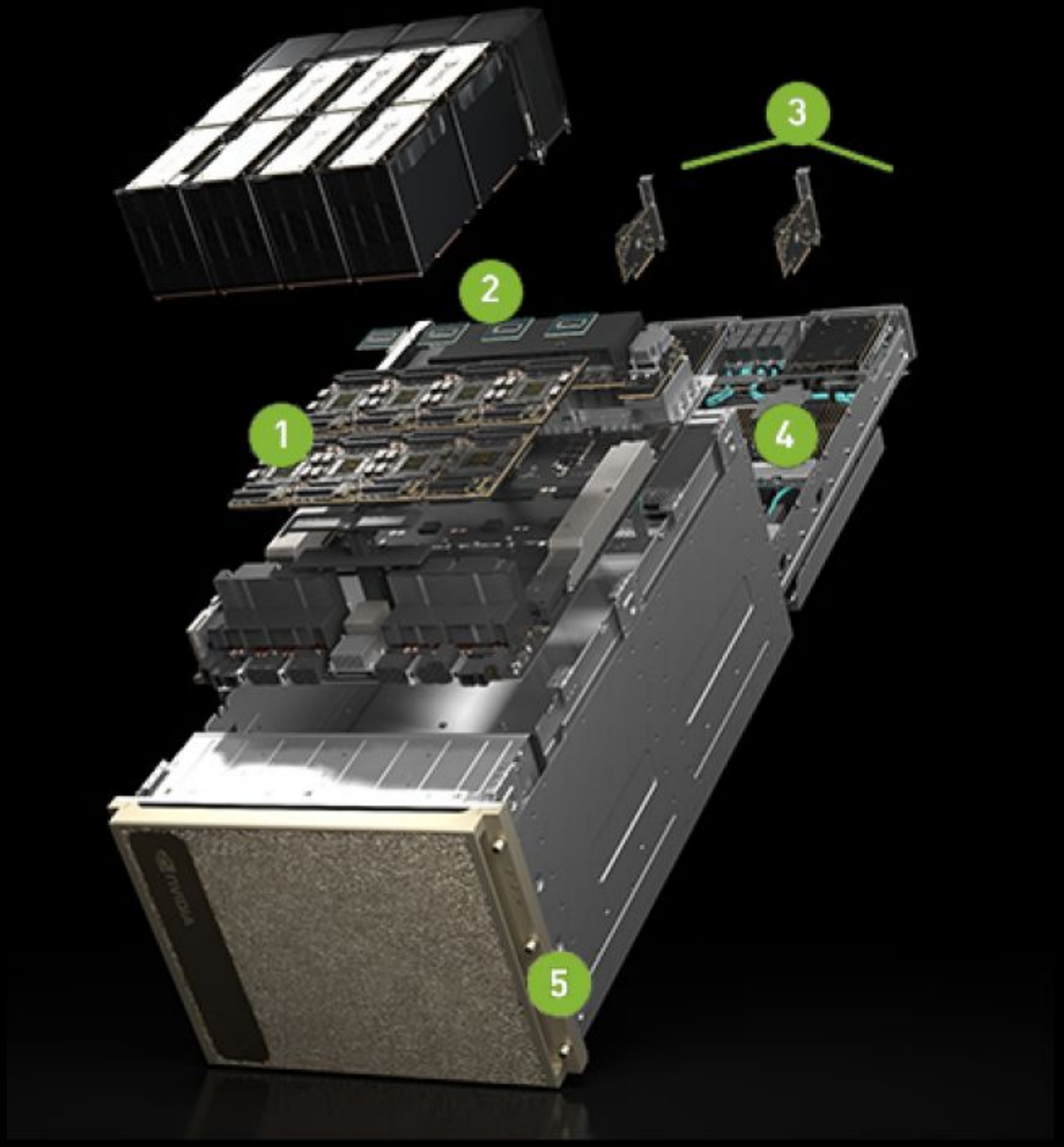
4×8 NVidia
H100 GPUs

8M
Orb tier

762 GiB (GPU)
Memory

10 /s
Verifications

2.5 Tb/s
Network



2024

Multi-Party Compute at World Scale

Participants

Berkeley
Center for Responsible,
Decentralized Intelligence

Universität
Zürich UZH
Blockchain Center

FAU
Friedrich-Alexander-Universität
Erlangen-Nürnberg

NETHERMIND

Governance

MPC in TEE

Protocol Governance DAO

5

Summary

World ID offers Biometric,
Passport and Device based PoP Tiers

Modality is kept private to the User

Uniqueness is anonymous by default

6

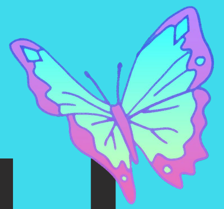
Next Steps

- Mini-apps
- World Chain
- Client side proving
- Programmable ZK-Identity

https://world.org

2024

Thank you



Remco Bloemen
remco@worldcoin.org