Trust Legos:
Luring Web2 into Web3 with Crypto Primitives



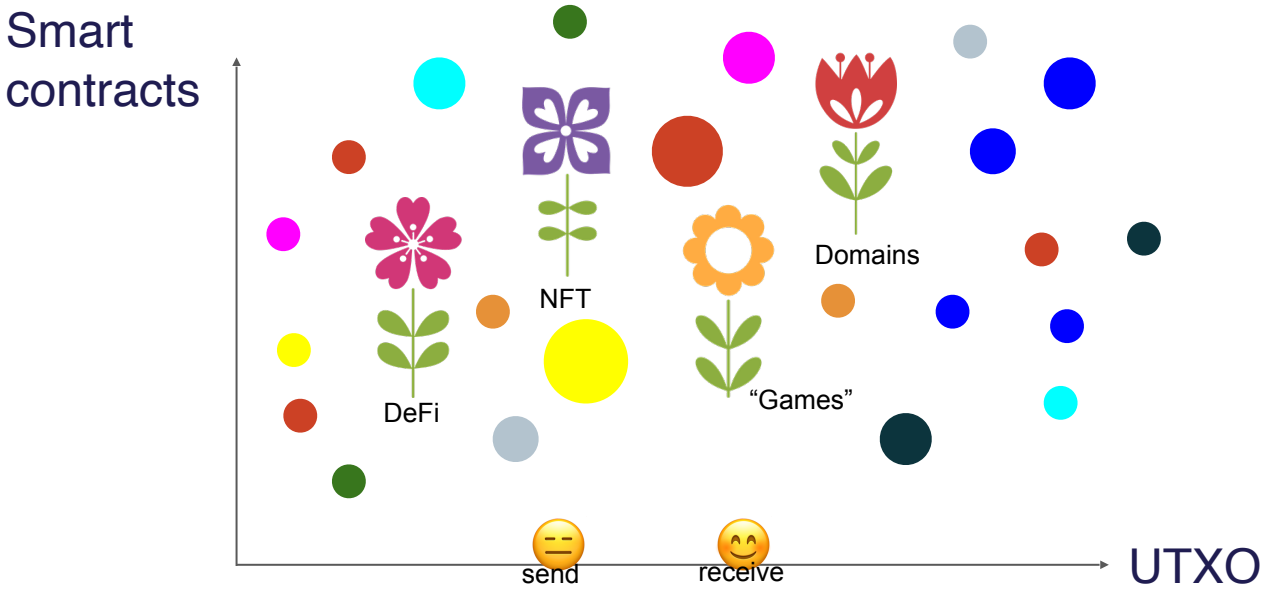
0xAlizk

We have been at this blockchain thing for a while now..

We have been at this blockchain thing for a while now..

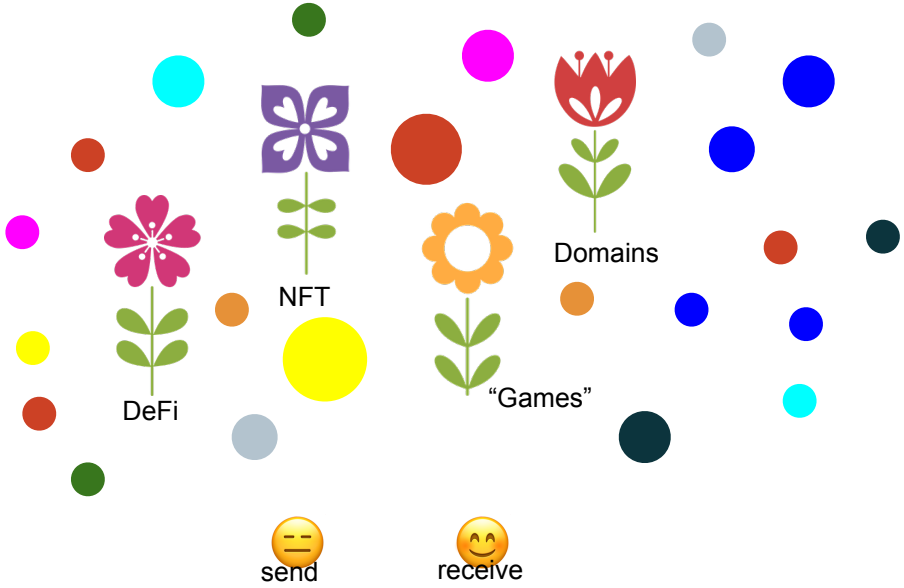


We have been at this blockchain thing for a while now..

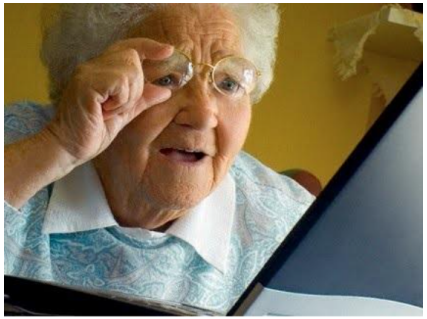


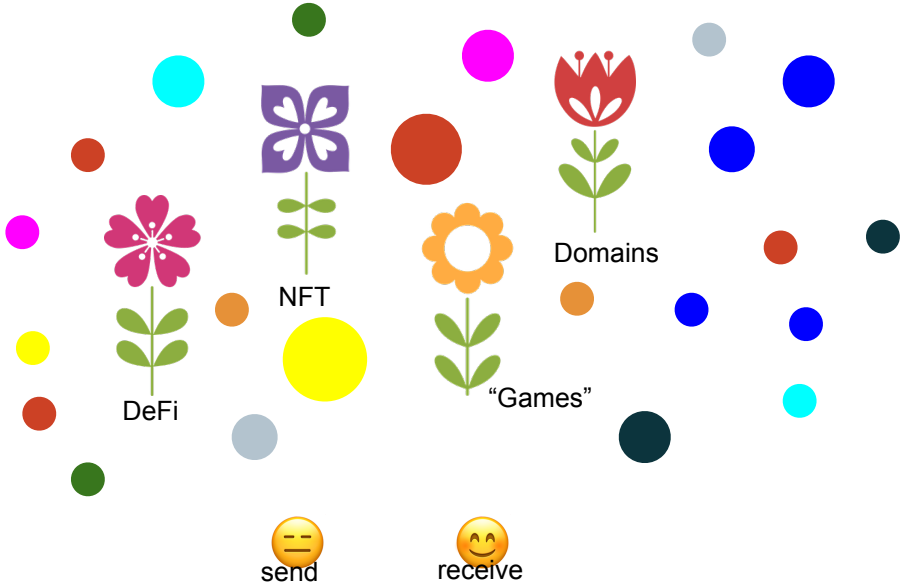
“Grandma is coming on-chain any minute now …”





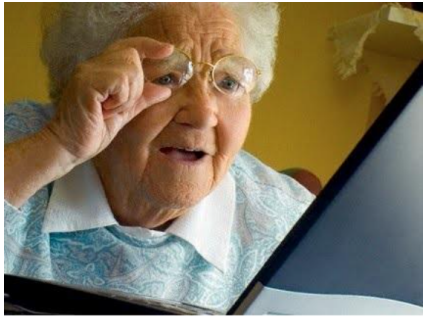
“Grandma is coming on-chain any minute now …”





Narrator: she didn’t.

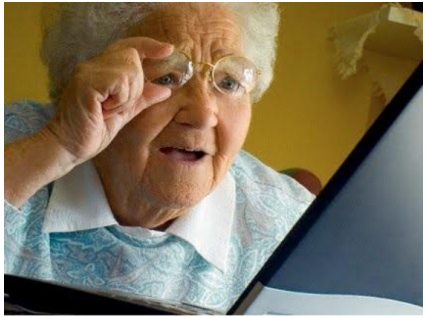
“Grandma is coming on-chain any minute now …”



Narrator: she didn’t.

We can no longer blame it on scalability because that has been solved

“Grandma is coming on-chain any minute now …”



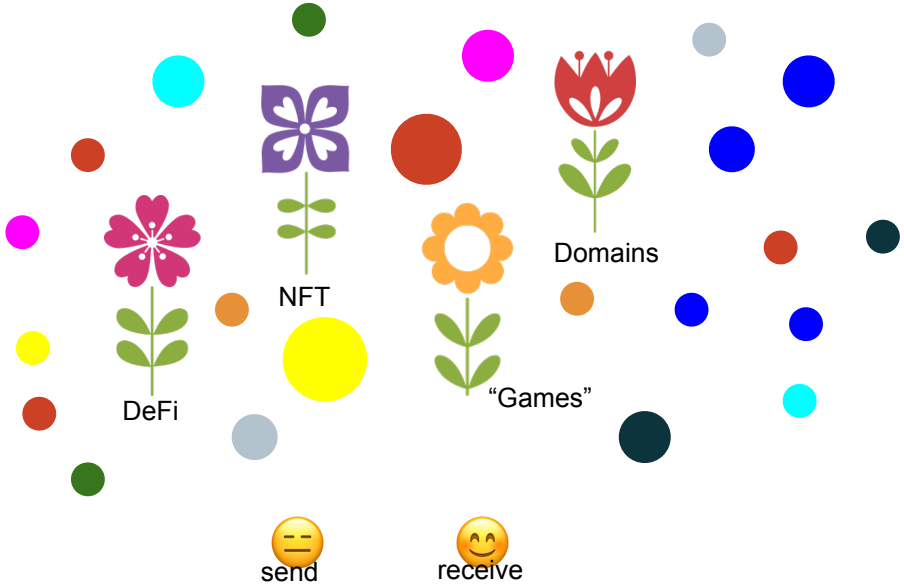
Narrator: she didn’t.

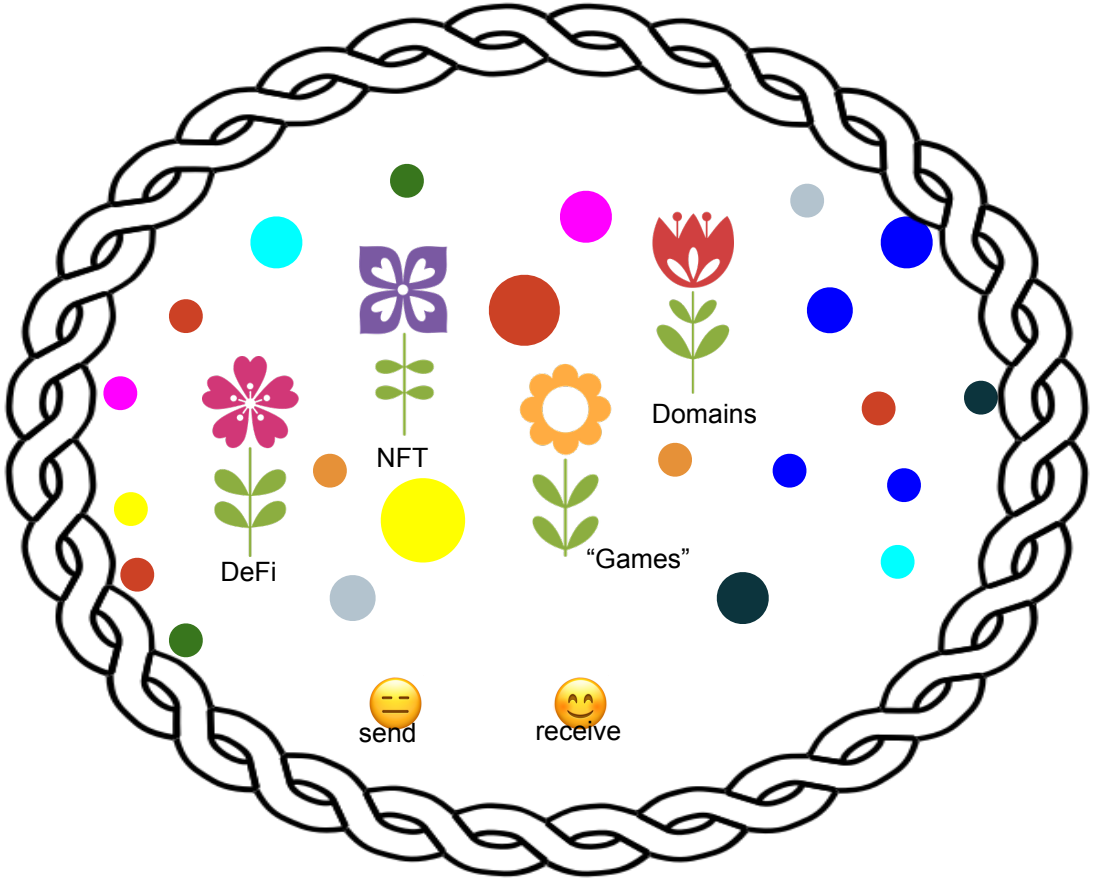
We can no longer blame it on **scalability** because that has been **solved**



Grandma ain’t coming for no one.

***We* go to her.**





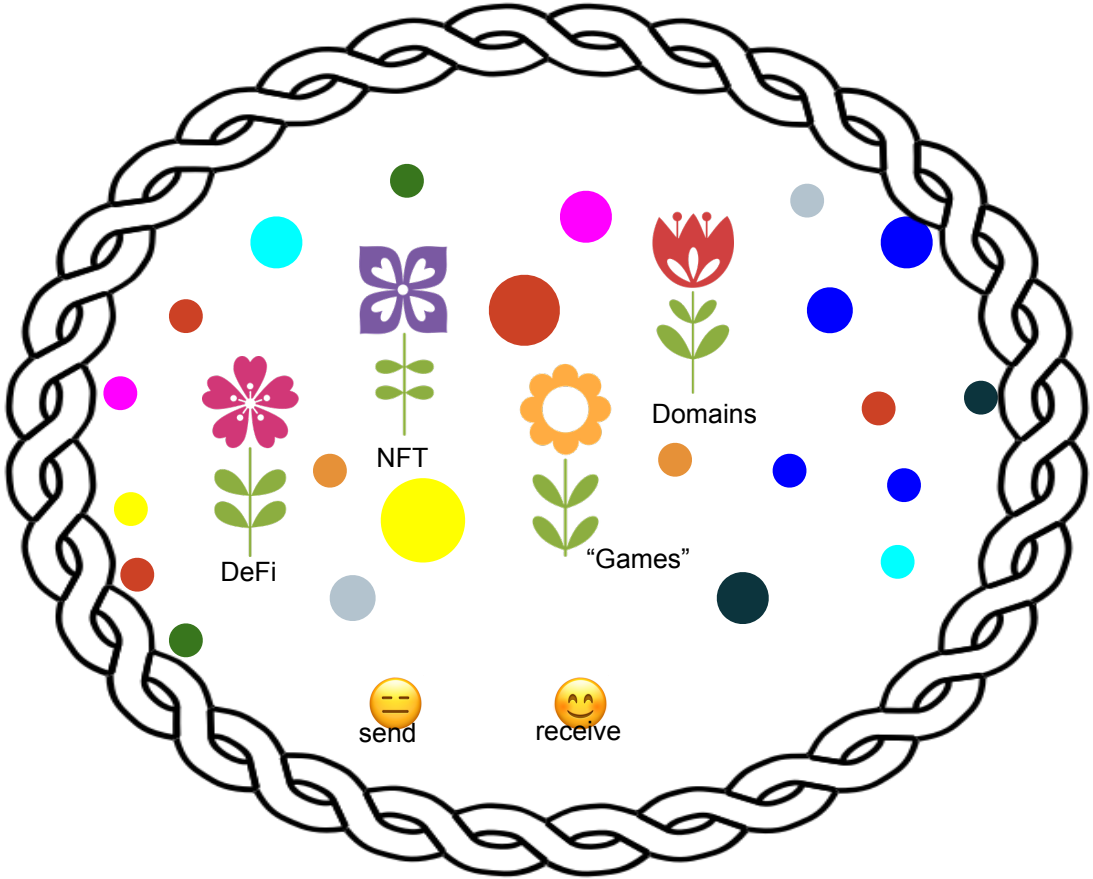
Mostly isolated from the “real” world

Inb4 Oracles:

🔭 May not support your feed of interest

🔒 Can’t oraclize private data

☠️ Garden variety of trust assumptions



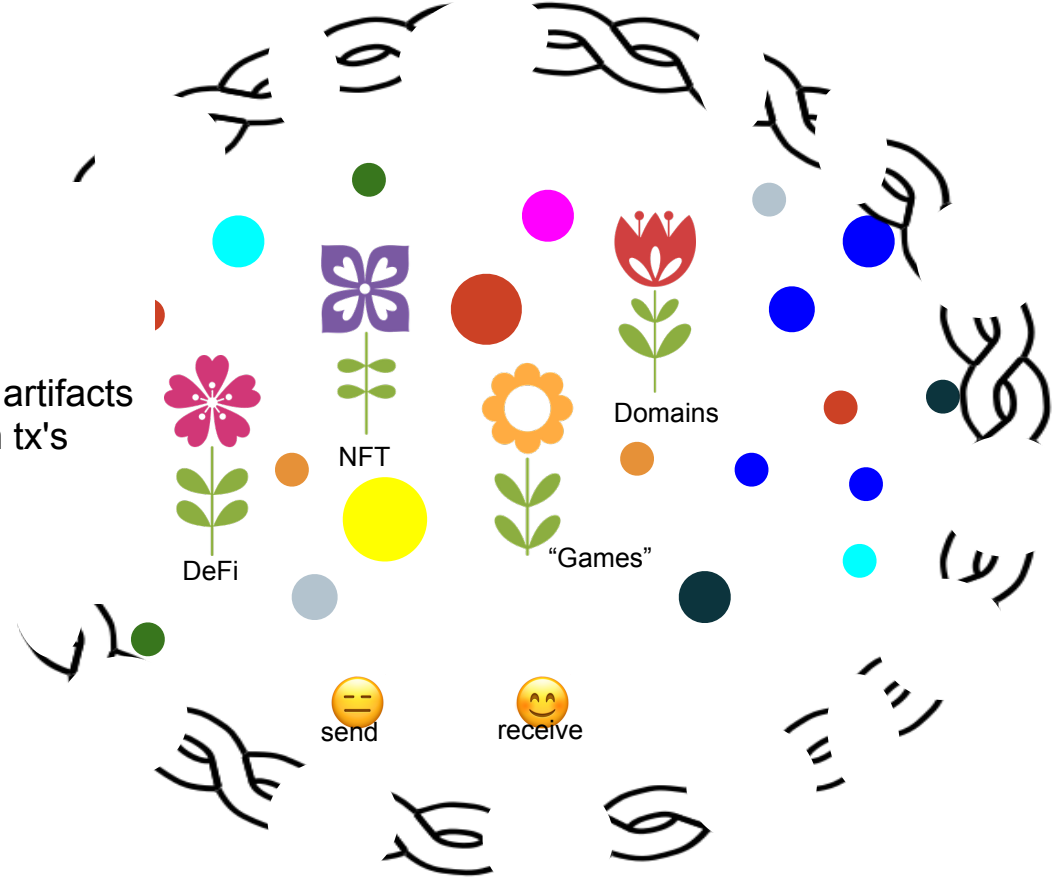
Mostly isolated from the “real” world

Programmable Cryptography To the Rescue

Connectivity:

- "if it's signed, we can prove it"
- no intermediary oracles needed
    - recycling & re-purposing of:
        - web2 cryptographic artifacts
        - historical blockchain tx's

and states

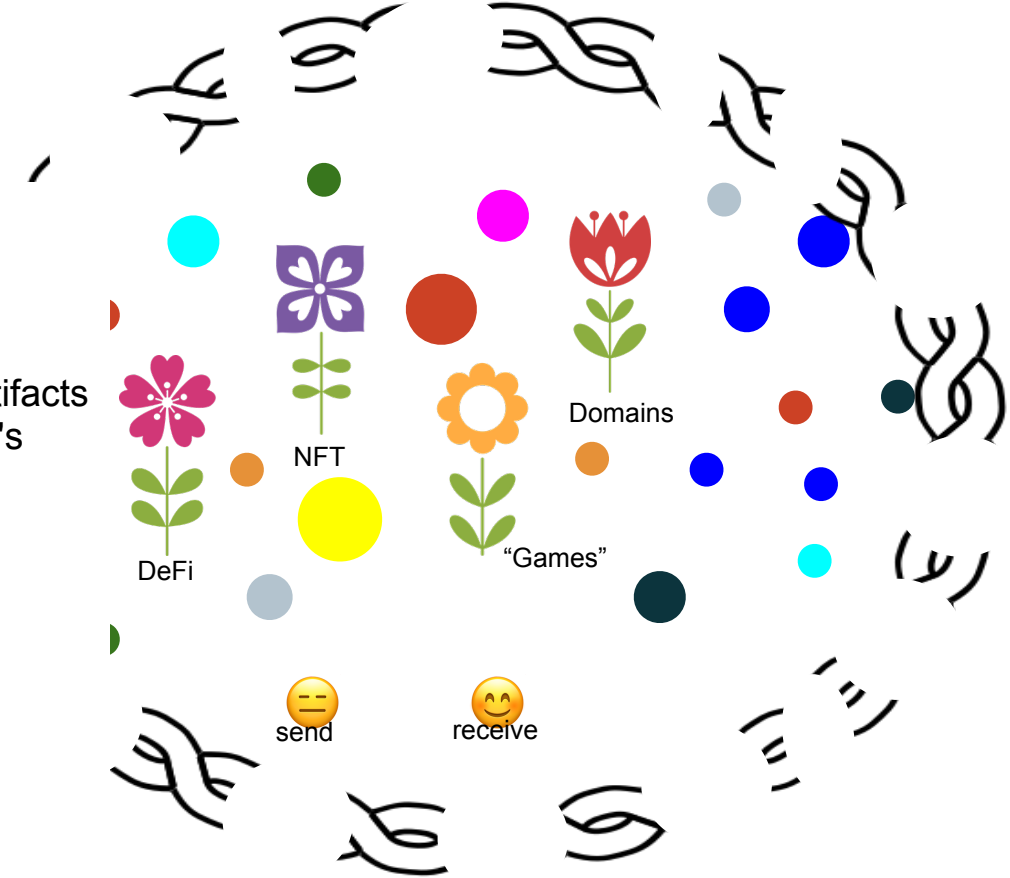


Programmable Cryptography To the Rescue

Connectivity:
- "if it's signed, we can prove it"
- no intermediary oracles needed
- recycling & re-purposing of:
- web2 cryptographic artifacts
- historical blockchain tx's

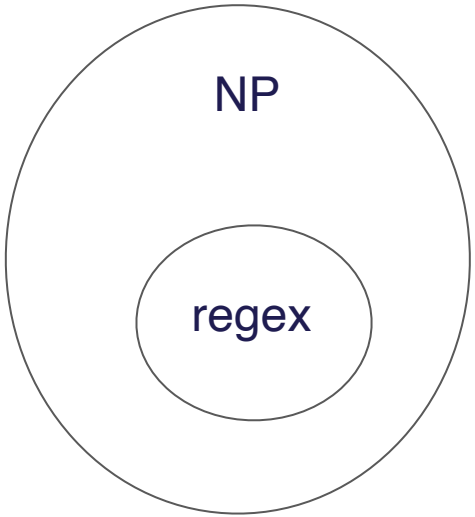
and states

New primitives:
- Privacy-preserving:
  - Grouping
  - Signaling
  - Privacy-preserving gatekeeping
- Collusion-resistant signaling



Some Emerging ProgCrypto Primitives and Paradigms

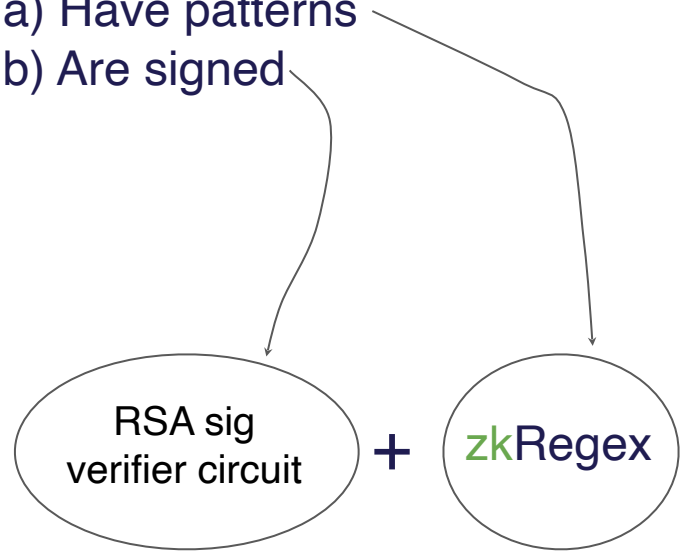
- Arithmetic circuits are NP-complete, regex is in NP, therefore we can decide arbitrary regex in Circom or Halo2 or zkVMs



- Arithmetic circuits are NP-complete, regex is in NP, therefore we can decide arbitrary regex in Circom or Halo2 or zkVMs



- Arithmetic circuits are np-complete, therefore we can decide arbitrary regex in Circom or Halo2 or zkVMs
- Emails:
  - a) Have patterns
  - b) Are signed



- Arithmetic circuits are np-complete, therefore we can decide arbitrary regex in Circom or Halo2 or zkVMs
- Emails:
  - a) Have patterns
  - b) Are signed



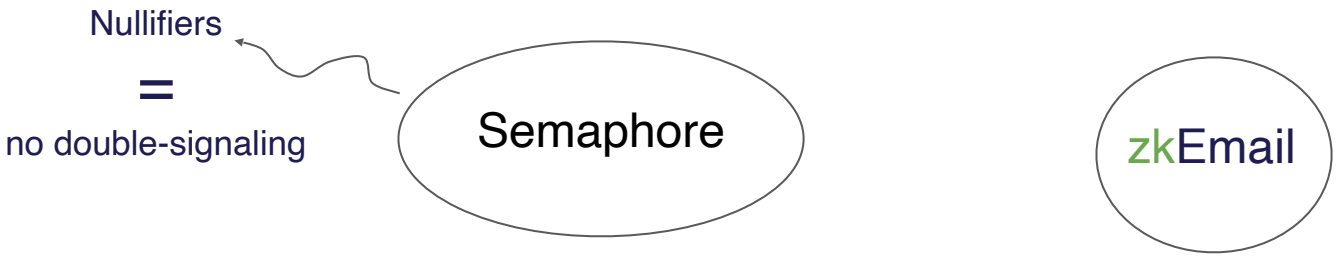
- **Group** members are leaves in an Incremental Merkle trees
- In-circuit proof of:

  “*I'm a member of this group and I vote for …*”



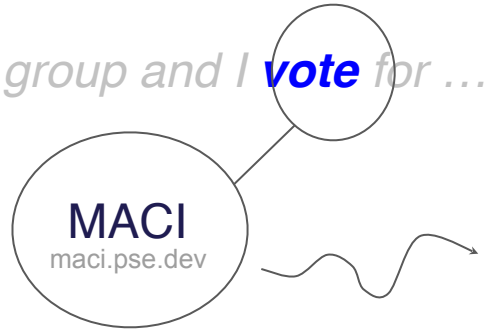
- Group members are leaves in an Incremental Merkle trees
- In-circuit proof of:

  “*I'm a member of this group and I vote for …*”



- Group members are leaves in an Incremental Merkle trees
- In-circuit proof of:

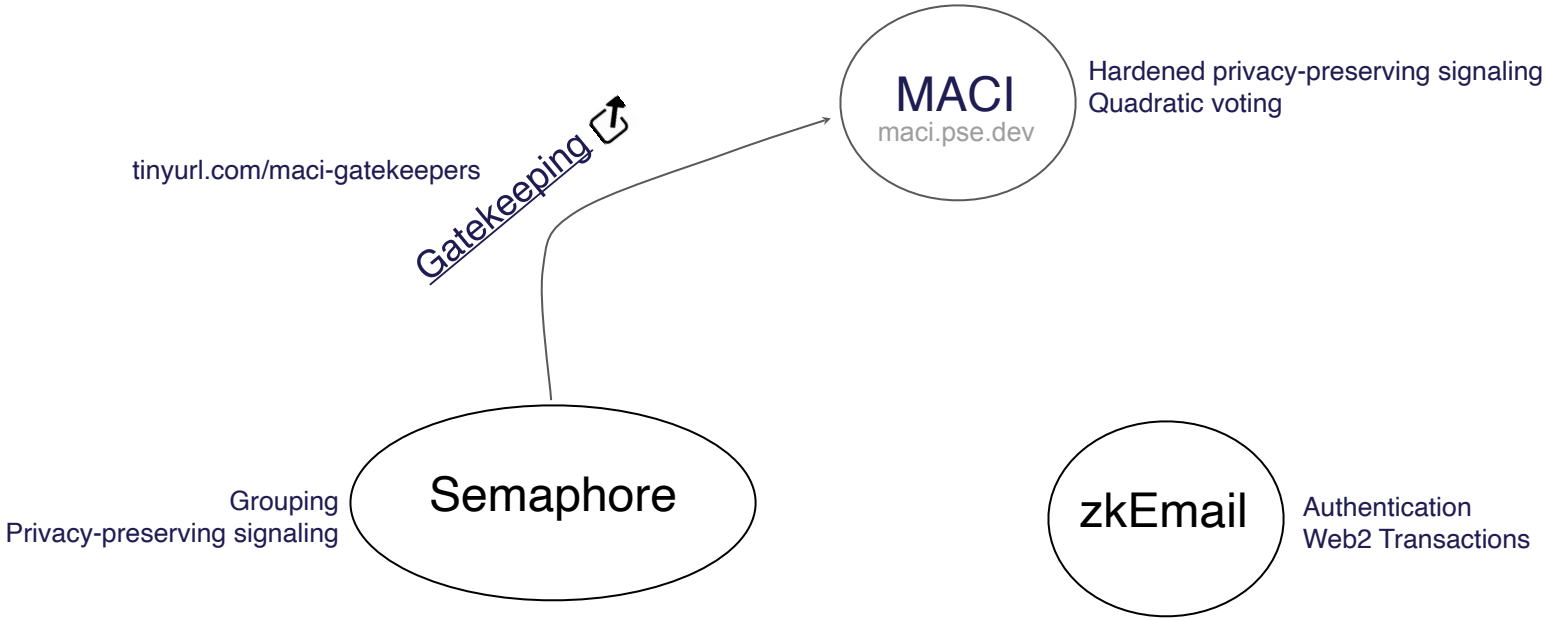
  *"I'm a member of this group and I **vote** for …"*



- Collusion resistance
- Quadratic voting

Semaphore

zkEmail


MACI
maci.pse.dev
Hardened privacy-preserving signaling
Quadratic voting
tinyurl.com/maci-gatekeepers
Gatekeeping
Grouping
Privacy-preserving signaling
Semaphore
zkEmail
Authentication
Web2 Transactions



tlsnotary.org
pluto.xyz
reclaimprotocol.org

Proving Web2 traffic

MP-TLS
(Multi-party TLS)

tlsnotary.org
pluto.xyz
reclaimprotocol.org

MPC between a **prover** and a **notary** to:

- Split session keys sent to a web2 Server
- Authenticate server identity
- Authenticate TLS response

Notary attests to **commitments** of server identity/ response text, hence <u>does not see either</u>

Prover can convince the world of the Web server response by **selectively "opening"** part of to response text

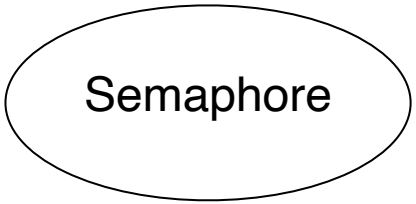


Portability of Web2 authenticated data
Recycling and repurposing Web2 crypto artifacts



Hardened privacy-preserving signaling
Quadratic voting

Grouping
Privacy-preserving signaling





Authentication
Web2 Transactions

MP-TLS
(Multi-party TLS)

MACI
maci.pse.dev

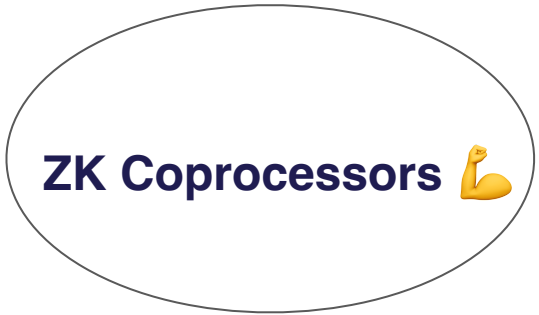
ZK Coprocessors 💪

Trustlessly access and compute over historical Ethereum blocks:

- headers
- states,
- transactions
- receipts

Semaphore

zkEmail

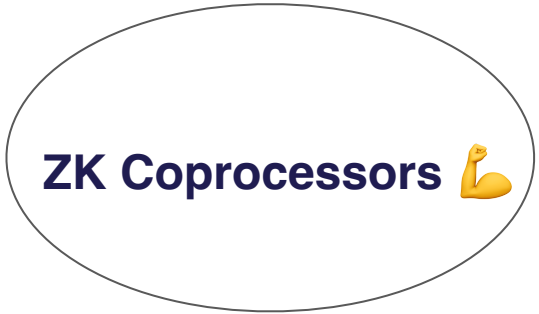


Consume history in custom business logic (Go) in-circuit off-chain

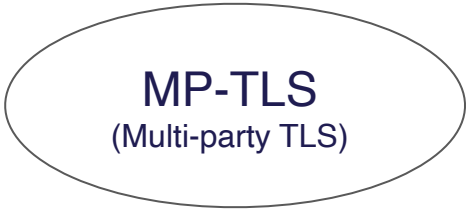
axiom.xyz
brevis.network
lagrange.dev

Query Ethereum's history from within smart contracts

First verifiably transform blockchain history to ZK-friendly db (change encoding function, a different hash fun, tree), *then* query against that



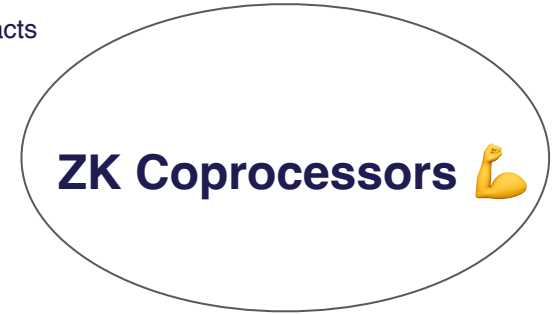
- Disintermediated x-chain oraclizing
- Beefy smart-contract hooks
- Smart and privacy-preserving airdrops
- **Integrating zkEmails and MP-TLS, …**
- ….
- ….



Portability of Web2 authenticated data
Recycling and repurposing Web2 crypto artifacts

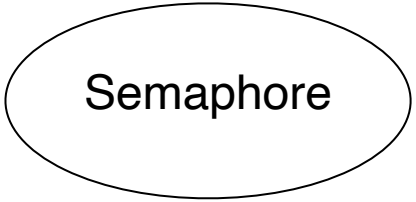


Hardened privacy-preserving signaling
Quadratic voting



Disintermediated x-chain oraclizing
Beefy smart-contract hooks
Smart and privacy-preserving airdrops
Integrating zkEmails and MP-TLS, …

Grouping
Privacy-preserving signaling





Authentication
Web2 Transactions

Example use cases

MP-TLS discord roles as authentication and gatekeeping for peers to give appreciation tokens

Anon but web2-gov-authenticated collusion-resistant voting

Email Wallet & Social Recovery

MP-TLS discord roles as authentication and gatekeeping for peers to give appreciation tokens

Collusion-resistance in strategy games

zkEmail to prove booking non-refundable booking → submit review on an independent review platform

Selective disclosure of PIIs

Collusion-resistant wiki edit votes

Group blogging: collective rep but anon authors

Projects...

zkp2p.org:
- Web2 domains marketplace
- zkEmail-powered fiat (venmo) on-ramp
- Web2 ticketing secondary market

hacks...

more hacks...

Anonymous Grouping and Hardened Signaling

Privacy-preserving sybil-resistance

Recycling and repurposing cryptographic artifacts:

- Signed emails
- Notarized TLS sessions: banking, web2 social, …
- Historical blockchain tx's, states, receipts, ..

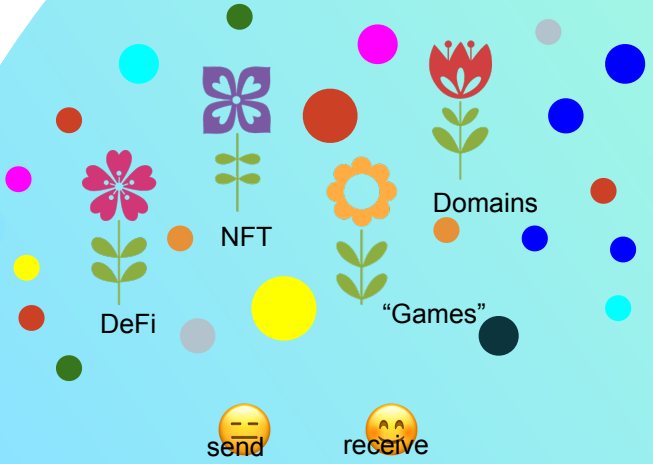
Web2

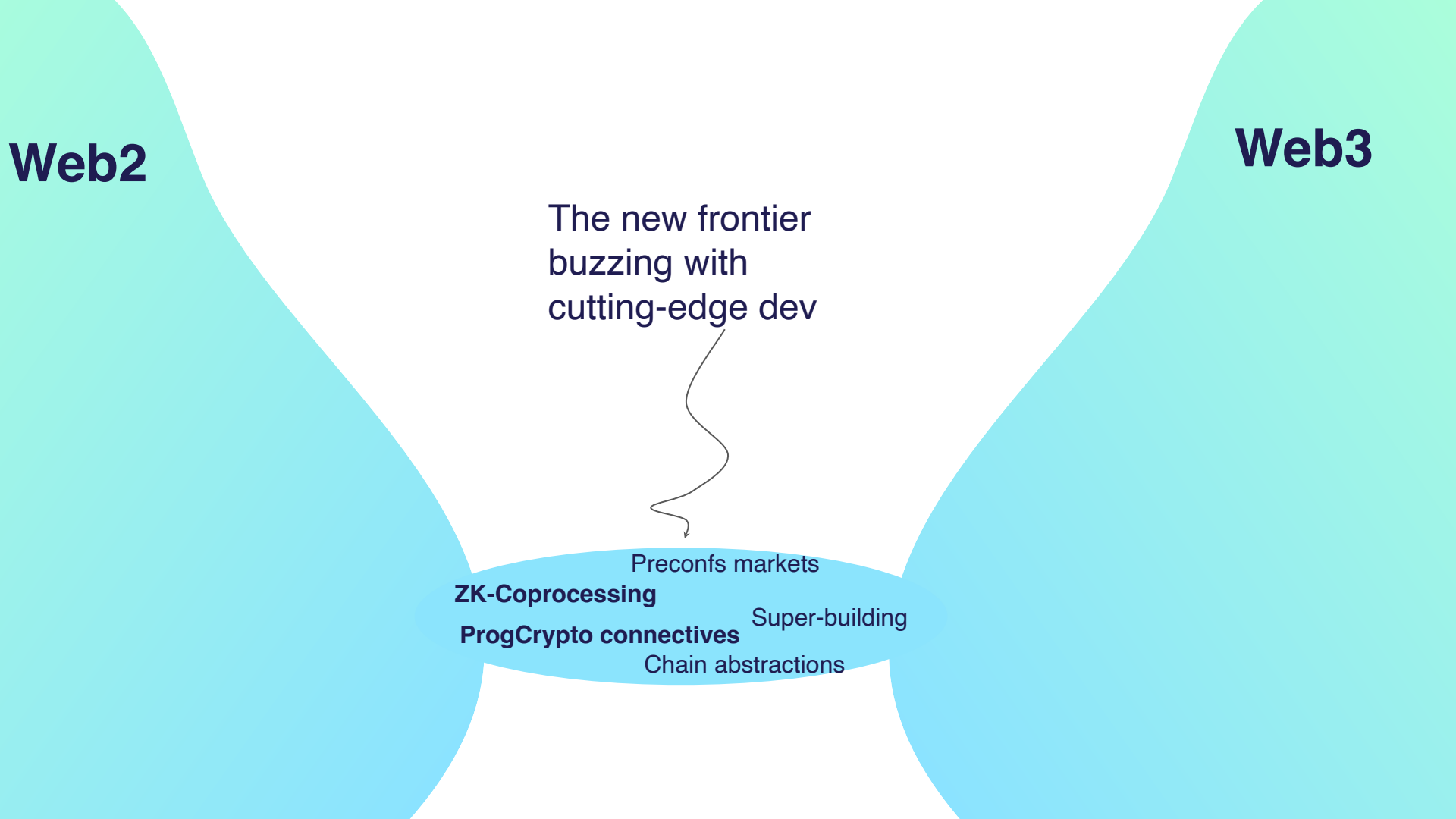
Identities

Reputations

Assets

Web3




Web2
Web3
The new frontier buzzing with cutting-edge dev
Preconfs markets
ZK-Coprocessing
Super-building
ProgCrypto connectives
Chain abstractions

~~Web2~~

~~Web3~~

The Web

Blockchain as a DBMS abstracted from app-devs

Preconfs markets

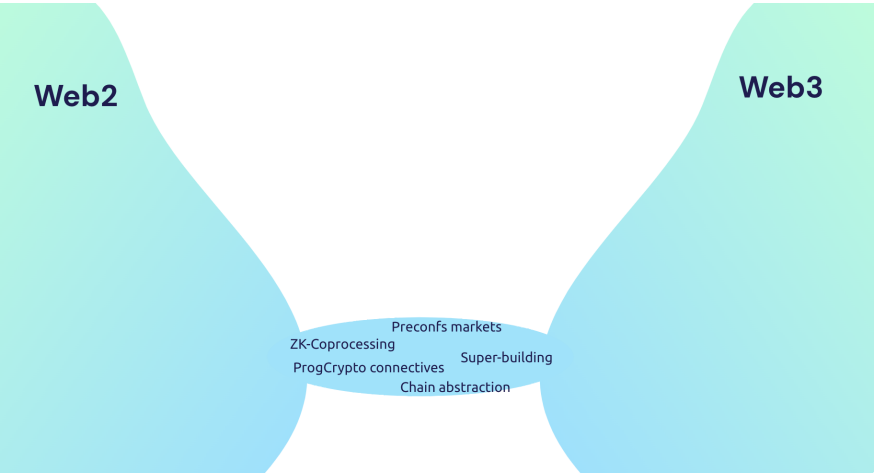
ZK-Coprocessing

Super-building

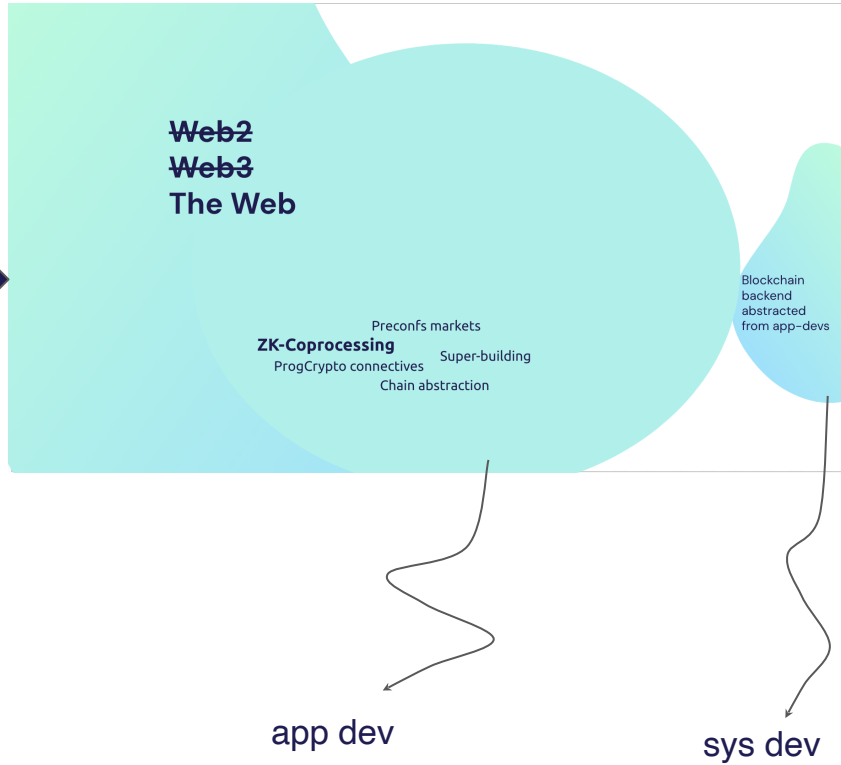
ProgCrypto connectives

Chain abstractions

Now


Web2
Web3
Preconfs markets
ZK-Coprocessing
Super-building
ProgCrypto connectives
Chain abstraction

Future


~~Web2~~
~~Web3~~
The Web
Preconfs markets
ZK-Coprocessing
Super-building
ProgCrypto connectives
Chain abstraction
Blockchain backend abstracted from app-devs
app dev
sys dev

Thanks



slides