Unlocking the Web with Programmable Cryptography

@GoblinOats @TonkLabs

Introduction

Goblin

- Co-founder of Tonk
- Did some ML @ Yahoo
- Did some HCI/Dev tools @ Deco Software ➡️ Airbnb
- Did some Art @ Willow Common Studio

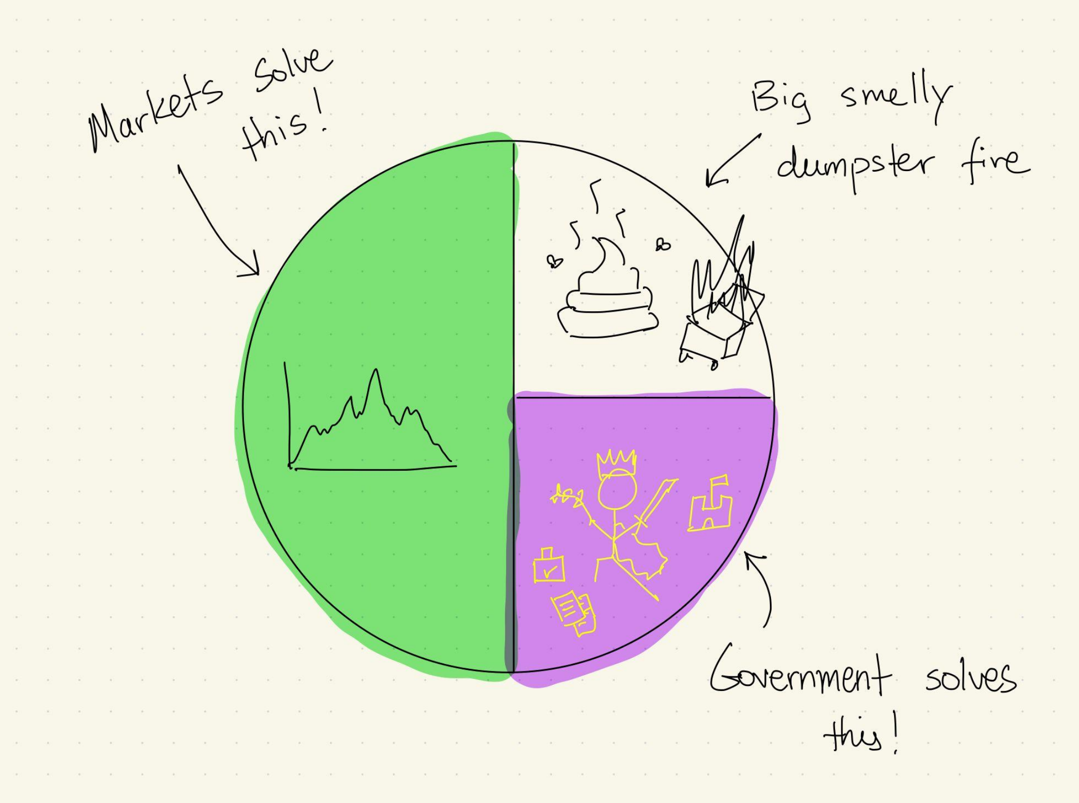
Tonk

- Liberate the Web
- Work: Dappicom, Tonk Attack, Gribi SDK, Speakeasy

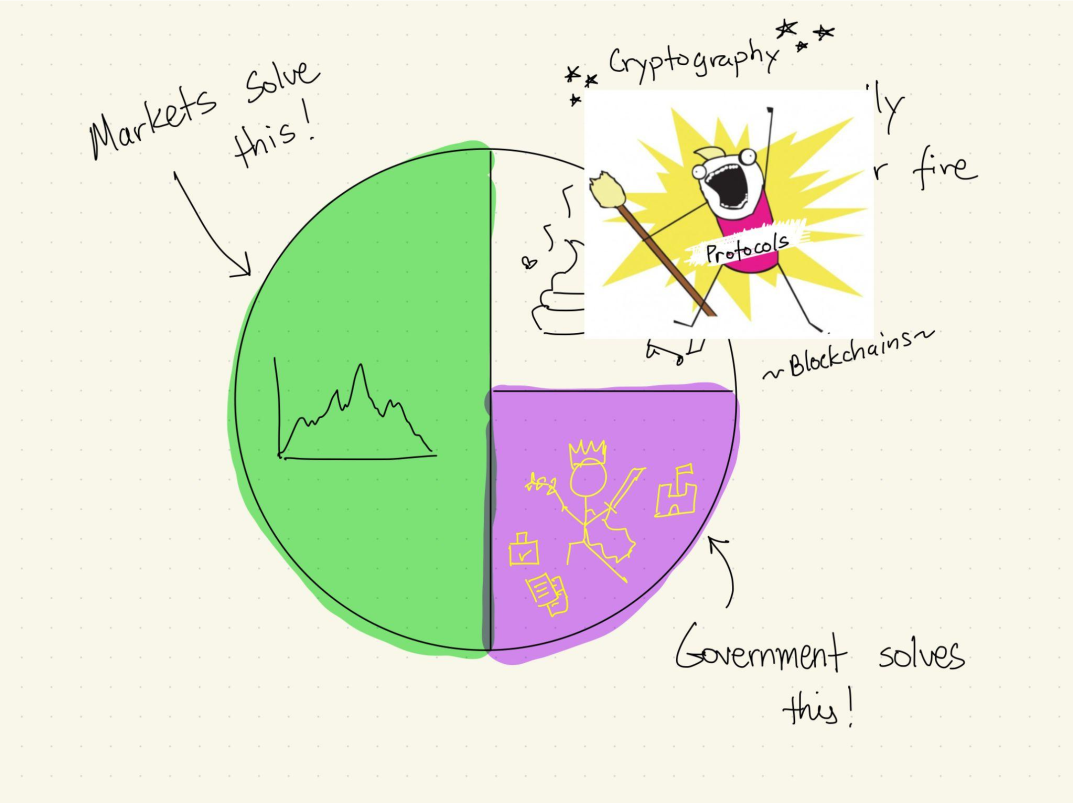
News flash

EUROPE
BLACK SEA
TURKEY
IRAN
ALGERIA
LIBYA
EGYPT
SAUDI ARABIA
MAURITANIA
MALI
NIGER
AFRICA
CHAD
SUDAN
KENYA
ZAMBIA
BOTSWANA
NTIC
INDIAN

The world has problems



Network protocols solve these problems!

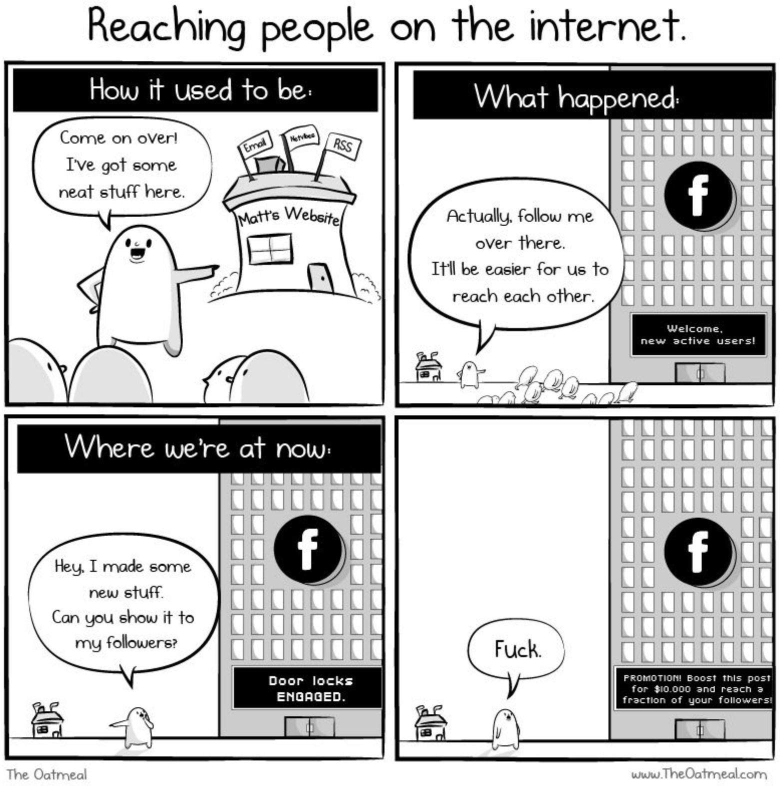


This happened

And this happened

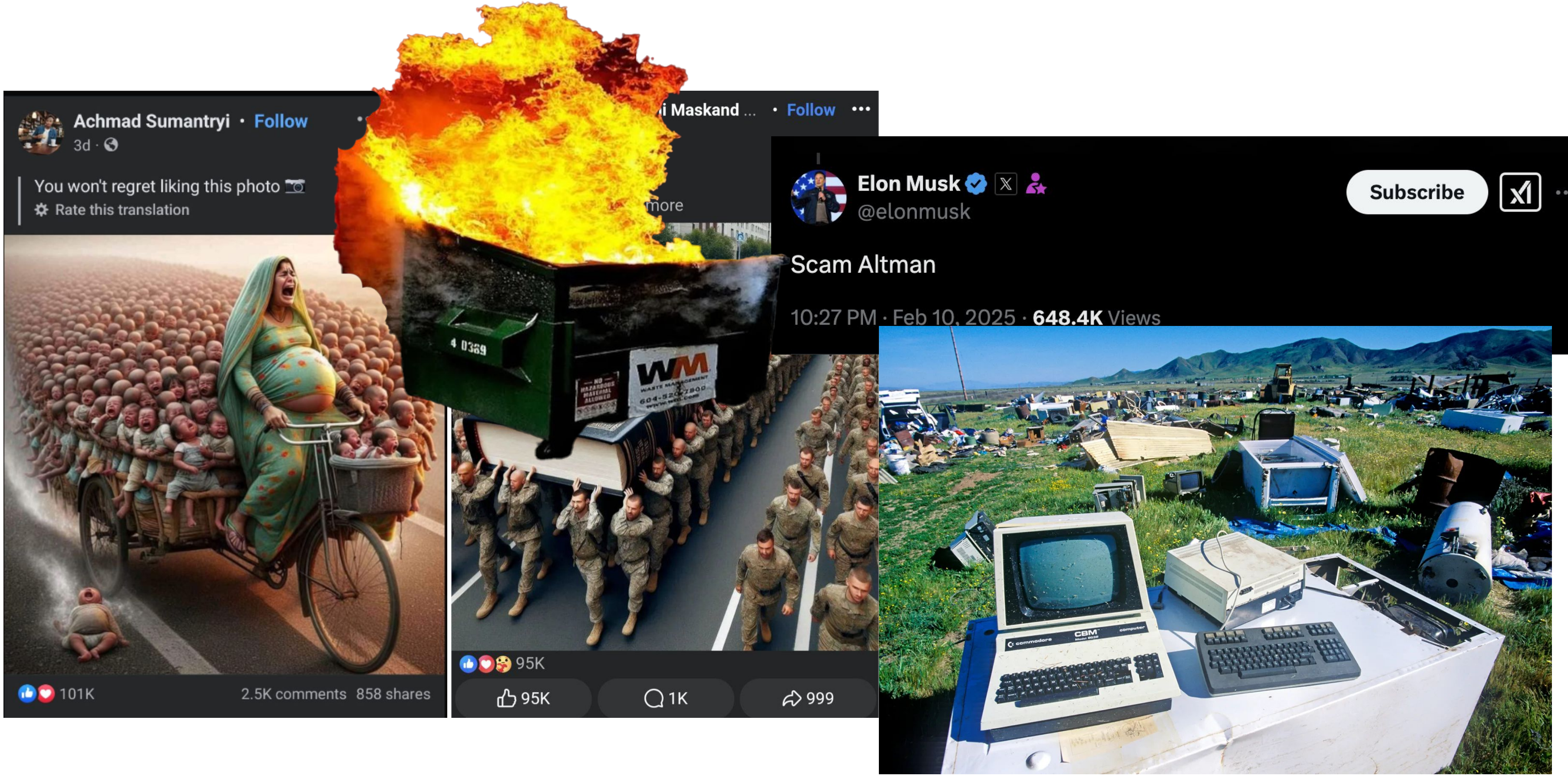
The Rise of Defi, from TRASTRAblog

Meanwhile on the Internet


Reaching people on the internet.
How it used to be:
Come on over! I've got some neat stuff here.
Email
Netvibes
RSS
Matt's Website
What happened:
Actually, follow me over there. It'll be easier for us to reach each other.
Welcome, new active users!
Where we're at now:
Hey, I made some new stuff. Can you show it to my followers?
Door locks ENGAGED.
Fuck.
PROMOTION! Boost this post for $10,000 and reach a fraction of your followers!
The Oatmeal
www.TheOatmeal.com

Cartoon from The Oatmeal by Matthew Inman

Now the Internet is dying



Achmad Sumantryi · Follow

3d ·

You won't regret liking this photo 📷

Rate this translation

101K

2.5K comments 858 shares

i Maskand ... · Follow ···

more

95K

95K

1K

999

Elon Musk

@elonmusk

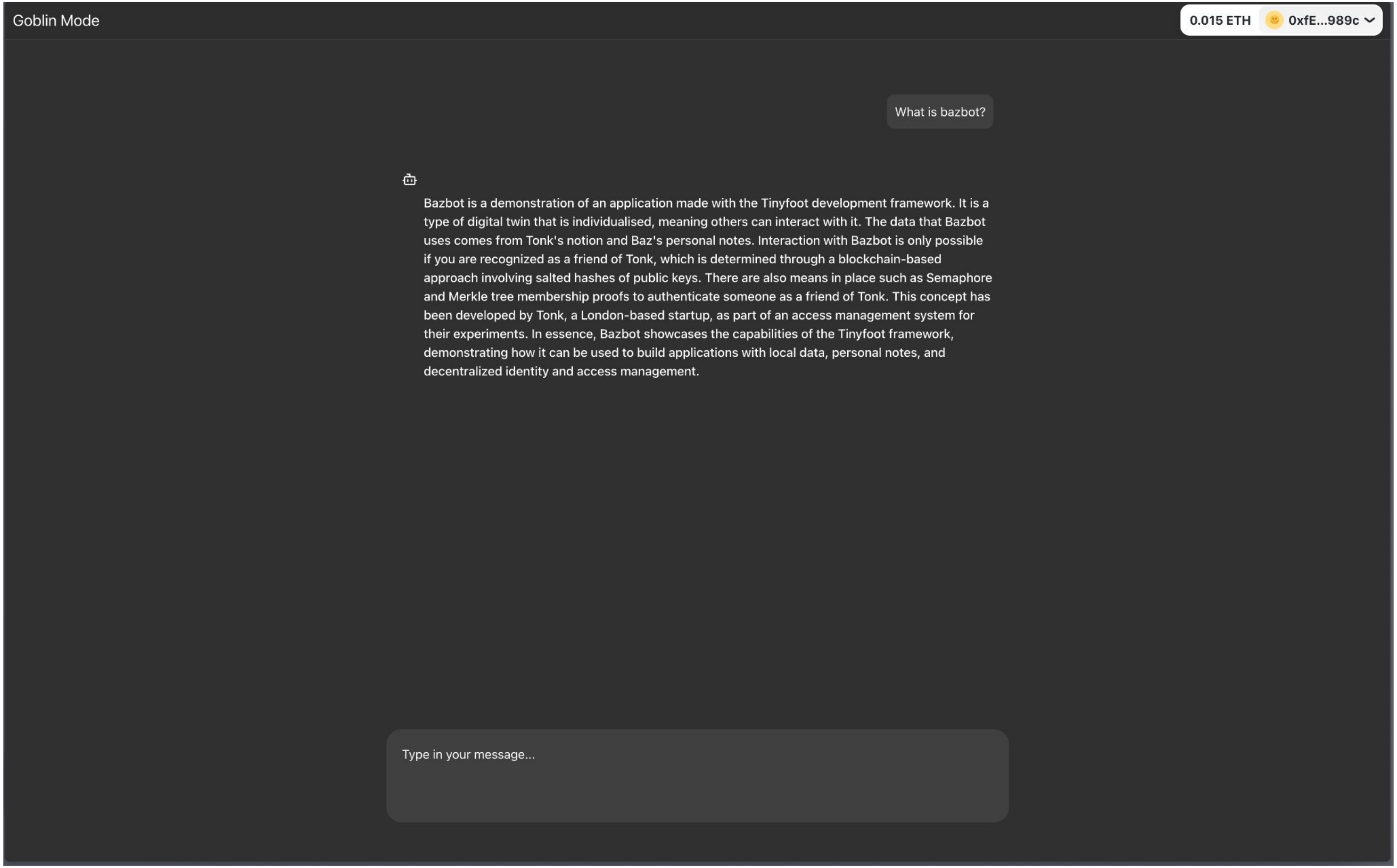
Subscribe

Scam Altman

10:27 PM · Feb 10, 2025 · 648.4K Views

And a new one struggles to be born

Demo



What is bazbot?

Bazbot is a demonstration of an application made with the Tinyfoot development framework. It is a type of digital twin that is individualised, meaning others can interact with it. The data that Bazbot uses comes from Tonk's notion and Baz's personal notes. Interaction with Bazbot is only possible if you are recognized as a friend of Tonk, which is determined through a blockchain-based approach involving salted hashes of public keys. There are also means in place such as Semaphore and Merkle tree membership proofs to authenticate someone as a friend of Tonk. This concept has been developed by Tonk, a London-based startup, as part of an access management system for their experiments. In essence, Bazbot showcases the capabilities of the Tinyfoot framework, demonstrating how it can be used to build applications with local data, personal notes, and decentralized identity and access management.

BazBot

Example of **personal software** using **personal data** for my **personal network**

Other Examples

- Social media just for my friends and family without shock content
- Private app to track health and share with family, doctor
- Collaborative note-taking, but the notes are all local to your device
- Sync all of our calendars to find the next RWC event

How can software and the networks that power it be that personal?

Basic Affordances of Programmable Cryptography

SQUISHY

SNARKY

PRIVY

Squishyness: it’s programmable stupid!

MAKE THE STUFF TALK TO THE OTHER STUFF

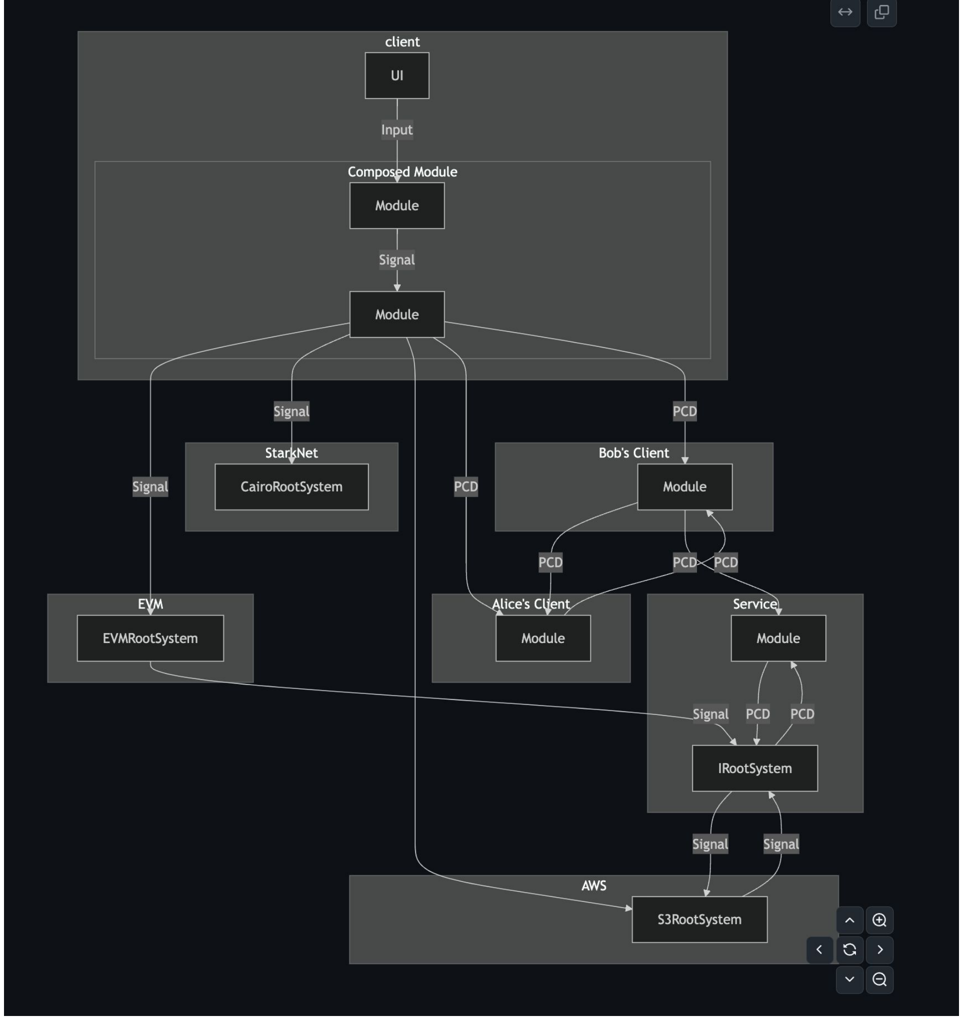
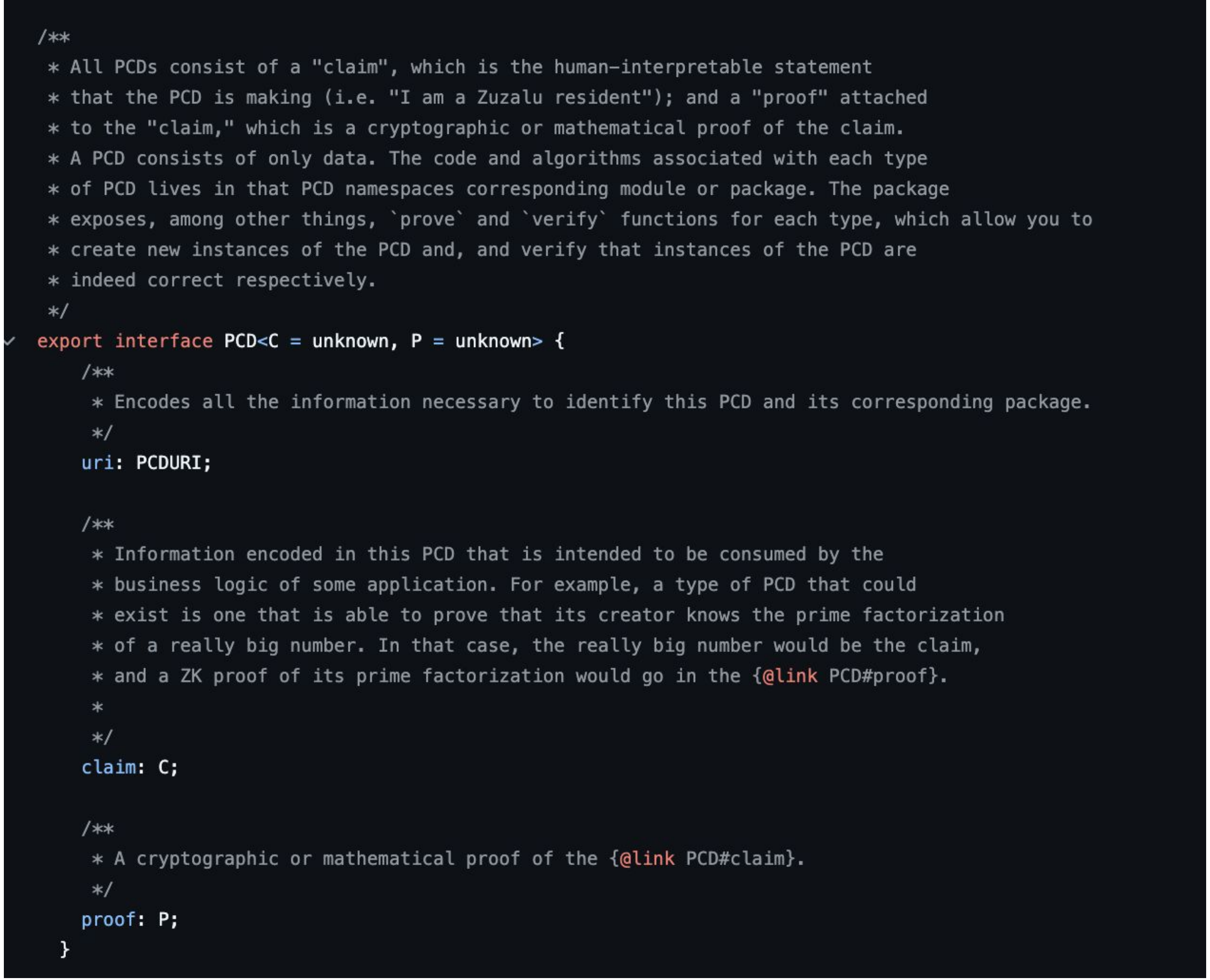


Diagram of Gribi SDK verified data flows, by Tonk Labs (2024)



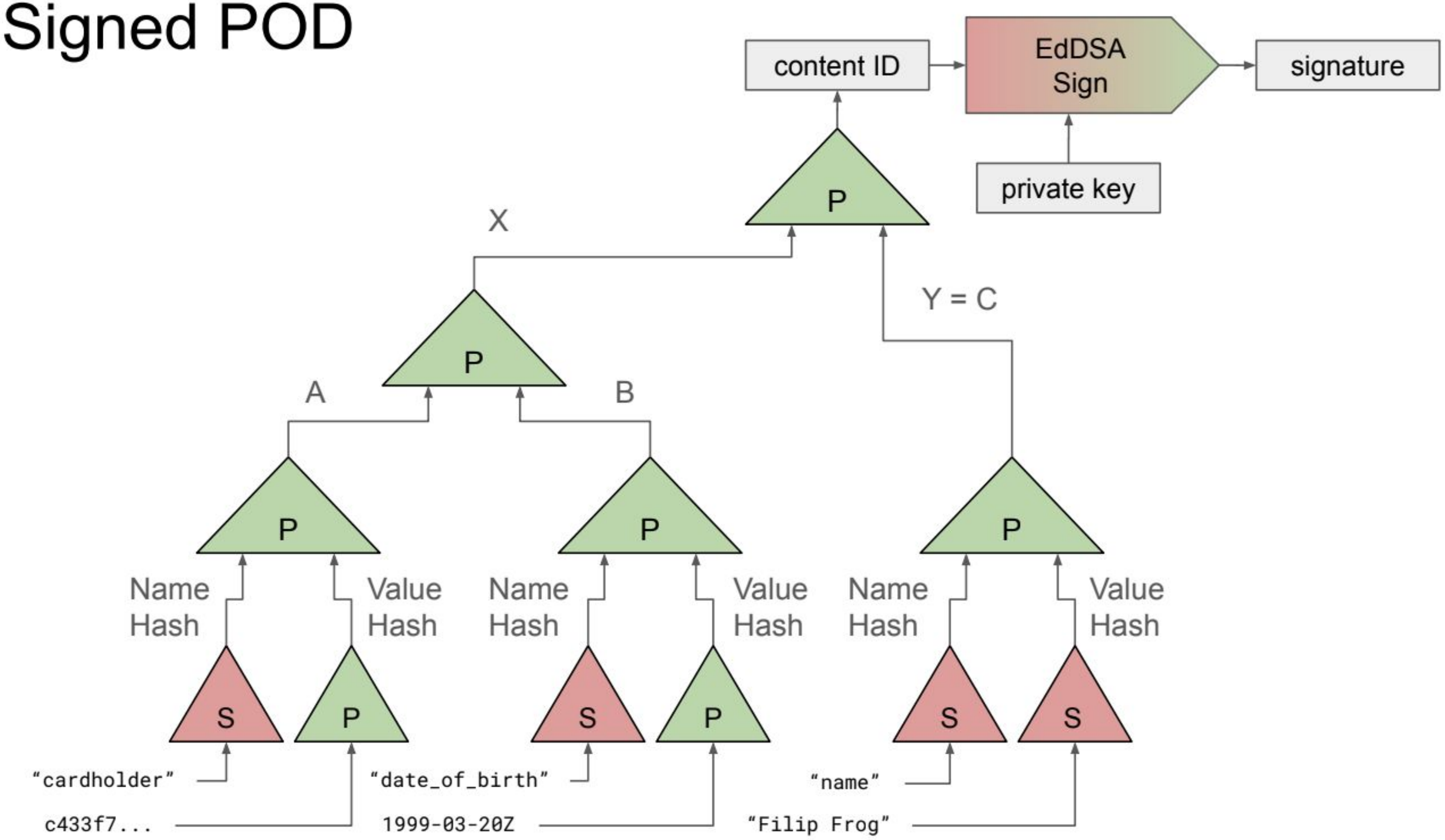
```typescript
/**
 * All PCDs consist of a "claim", which is the human-interpretable statement
 * that the PCD is making (i.e. "I am a Zuzalu resident"); and a "proof" attached
 * to the "claim," which is a cryptographic or mathematical proof of the claim.
 * A PCD consists of only data. The code and algorithms associated with each type
 * of PCD lives in that PCD namespaces corresponding module or package. The package
 * exposes, among other things, `prove` and `verify` functions for each type, which allow you to
 * create new instances of the PCD and, and verify that instances of the PCD are
 * indeed correct respectively.
 */
export interface PCD<C = unknown, P = unknown> {
    /**
     * Encodes all the information necessary to identify this PCD and its corresponding package.
     */
    uri: PCDURI;

    /**
     * Information encoded in this PCD that is intended to be consumed by the
     * business logic of some application. For example, a type of PCD that could
     * exist is one that is able to prove that its creator knows the prime factorization
     * of a really big number. In that case, the really big number would be the claim,
     * and a ZK proof of its prime factorization would go in the {@link PCD#proof}.
     *
     */
    claim: C;

    /**
     * A cryptographic or mathematical proof of the {@link PCD#claim}.
     */
    proof: P;
  }
```

Forked PCD interface in Gribi SDK, by Tonk Labs (2024)

Signed POD



Signed POD merkelization, from Devcon talk A Deep Dive into ZK Proofs of PODs

Basic Affordances of Programmable Cryptography

SQUISHY - It's programmable!

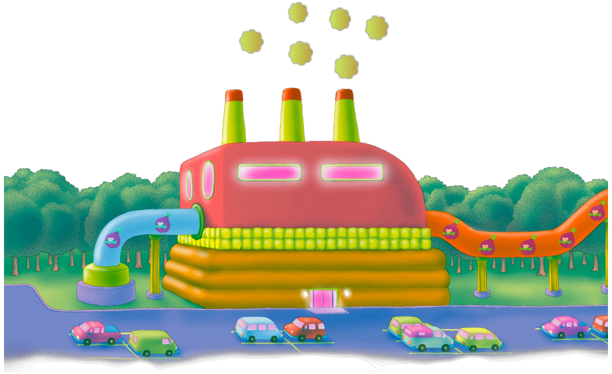
SNARKY

PRIVY

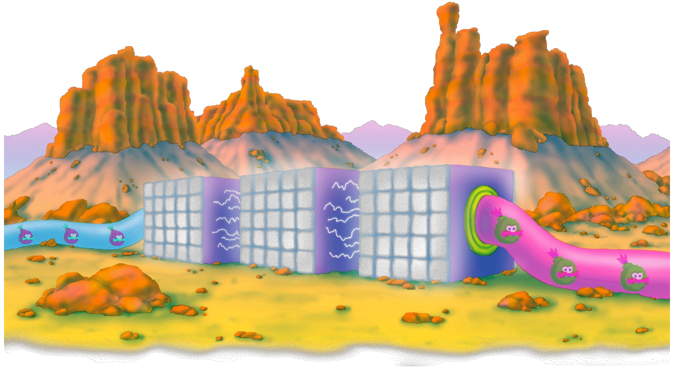
Snarkyness is magical scaling

The obvious thing

BEEFY
ZKVM

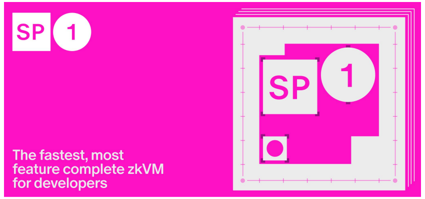


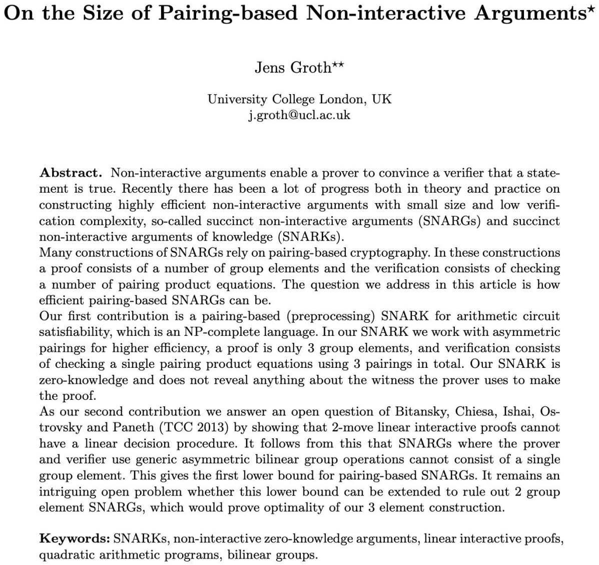
PROOF
ON CHAIN



Illustrations from Dappicom release, by Tonk Labs. Illustrator Hi-Bred. (2023)

All the good work





On the Size of Pairing-based Non-interactive Arguments*

Jens Groth**

University College London, UK
j.groth@ucl.ac.uk

Abstract. Non-interactive arguments enable a prover to convince a verifier that a statement is true. Recently there has been a lot of progress both in theory and practice on constructing highly efficient non-interactive arguments with small size and low verification complexity, so-called succinct non-interactive arguments (SNARGs) and succinct non-interactive arguments of knowledge (SNARKs).
Many constructions of SNARGs rely on pairing-based cryptography. In these constructions a proof consists of a number of group elements and the verification consists of checking a number of pairing product equations. The question we address in this article is how efficient pairing-based SNARGs can be.
Our first contribution is a pairing-based (preprocessing) SNARK for arithmetic circuit satisfiability, which is an NP-complete language. In our SNARK we work with asymmetric pairings for higher efficiency, a proof is only 3 group elements, and verification consists of checking a single pairing product equations using 3 pairings in total. Our SNARK is zero-knowledge and does not reveal anything about the witness the prover uses to make the proof.
As our second contribution we answer an open question of Bitansky, Chiesa, Ishai, Ostrovsky and Paneth (TCC 2013) by showing that 2-move linear interactive proofs cannot have a linear decision procedure. It follows from this that SNARGs where the prover and verifier use generic asymmetric bilinear group operations cannot consist of a single group element. This gives the first lower bound for pairing-based SNARGs. It remains an intriguing open problem whether this lower bound can be extended to rule out 2 group element SNARGs, which would prove optimality of our 3 element construction.

Keywords: SNARKs, non-interactive zero-knowledge arguments, linear interactive proofs, quadratic arithmetic programs, bilinear groups.

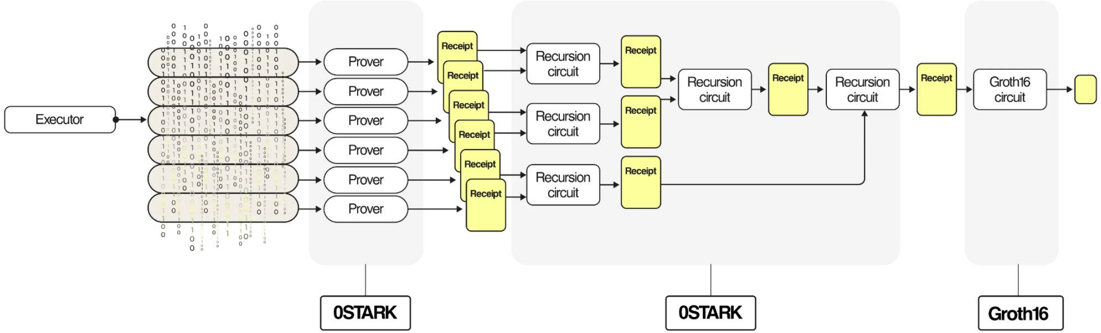
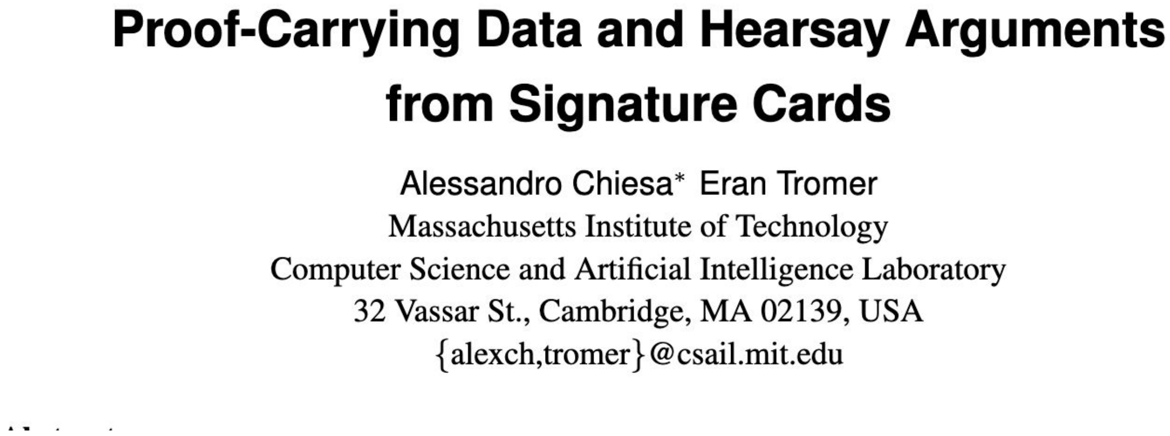


Diagram from RiscZero's blog post in 2024, Designing High-Performance zkVMs

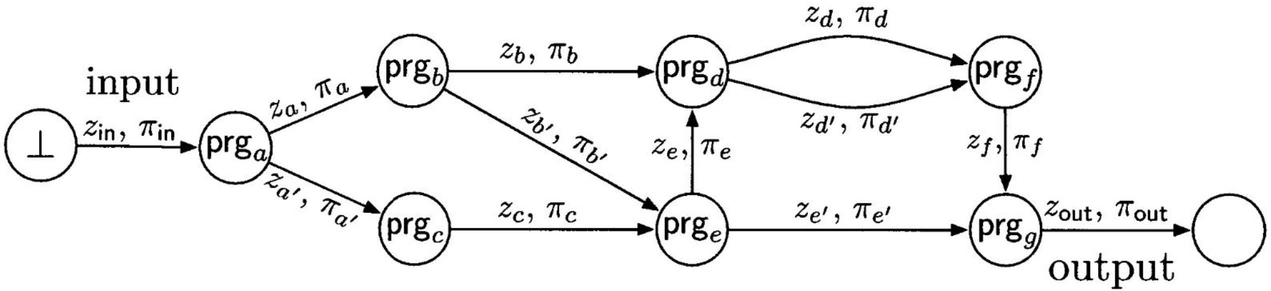
Snarky + Squishy!



Proof-Carrying Data and Hearsay Arguments from Signature Cards

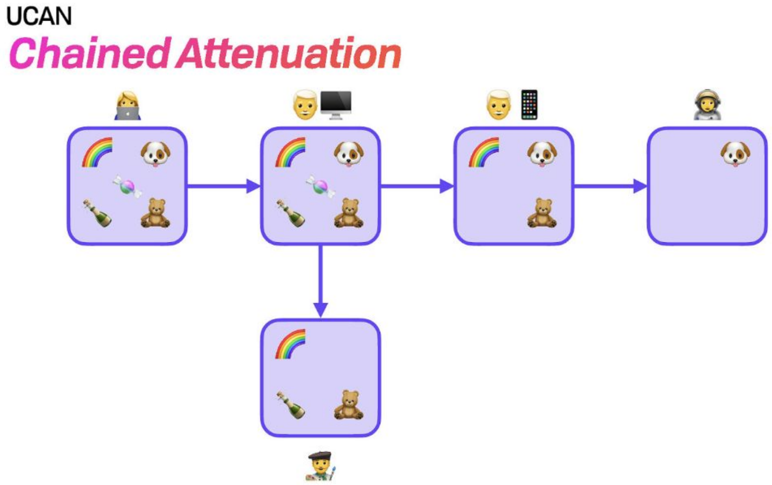
Alessandro Chiesa[*] Eran Tromer
Massachusetts Institute of Technology
Computer Science and Artificial Intelligence Laboratory
32 Vassar St., Cambridge, MA 02139, USA
{alexch,tromer}@csail.mit.edu

Snarky + Squishy!

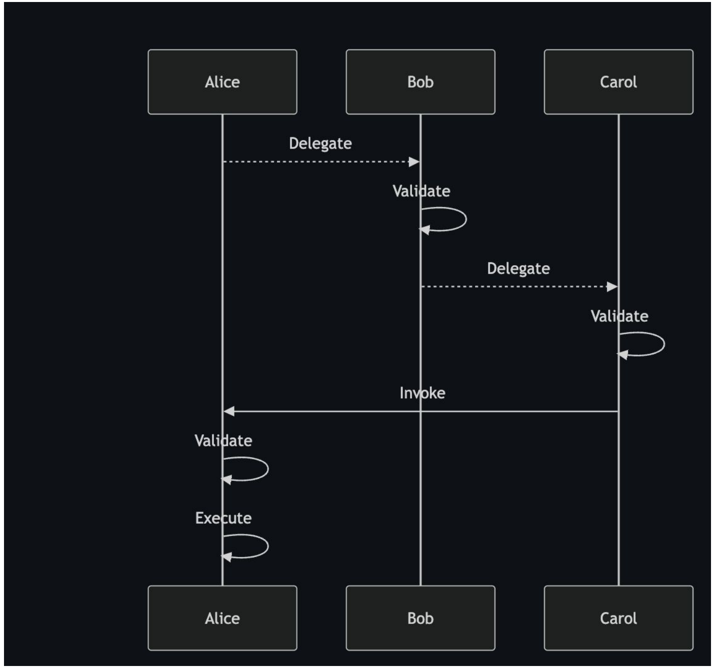


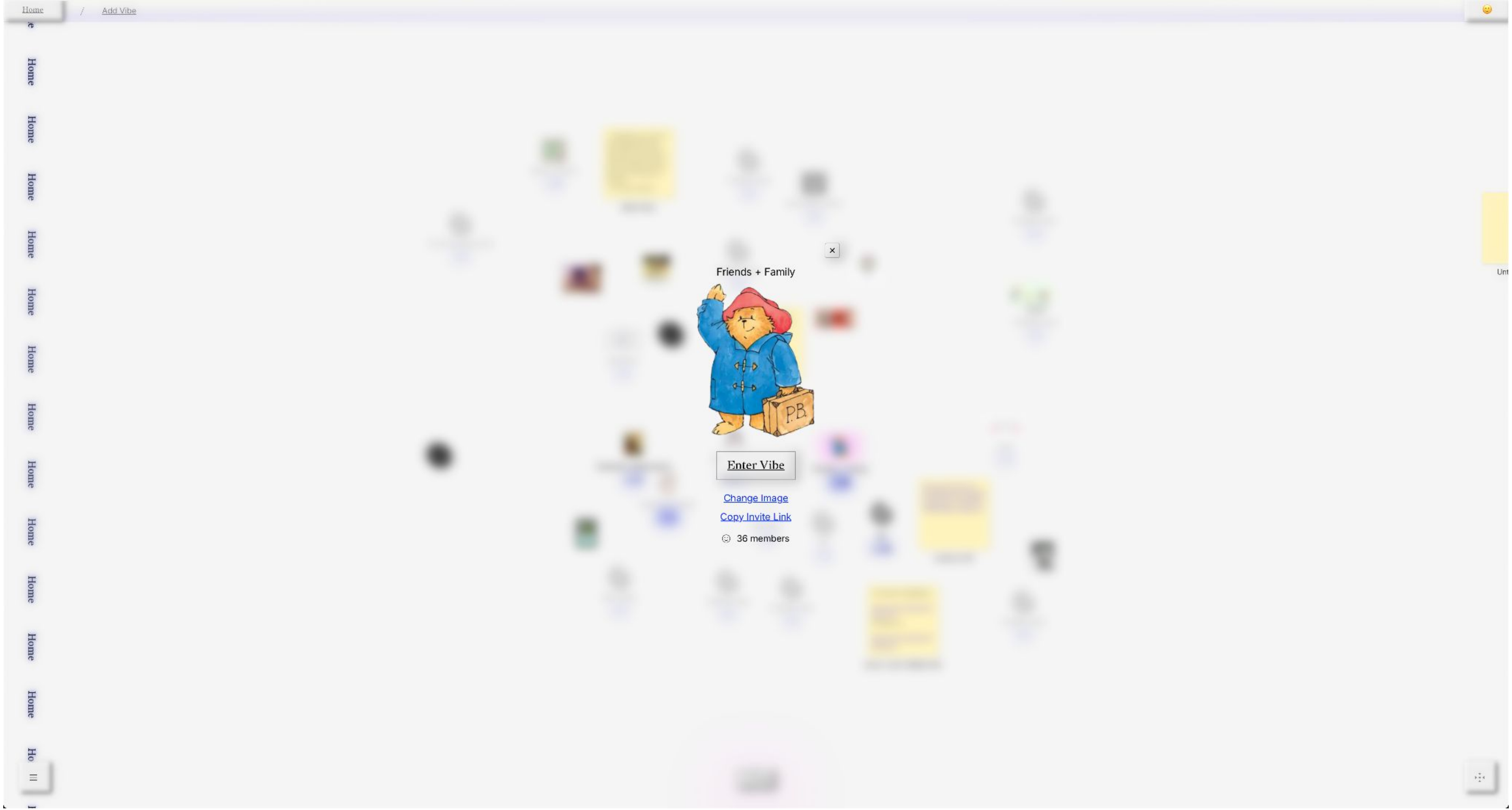
Chiesa, A. (2009). *Example of an augmented distributed computation transcript: Proof-Carrying Data*.

Compressing chains of signatures in OCAP



Chained Attenuation and UCAN diagram. [UCAN working group](#) and A presentation at [UCAN for FileCoin](#) in August 2021 in by [Brooklyn Zelenka](#)





Speakeasy Internal Prototype by Tonk Labs (2024)

Basic Affordances of Programmable Cryptography

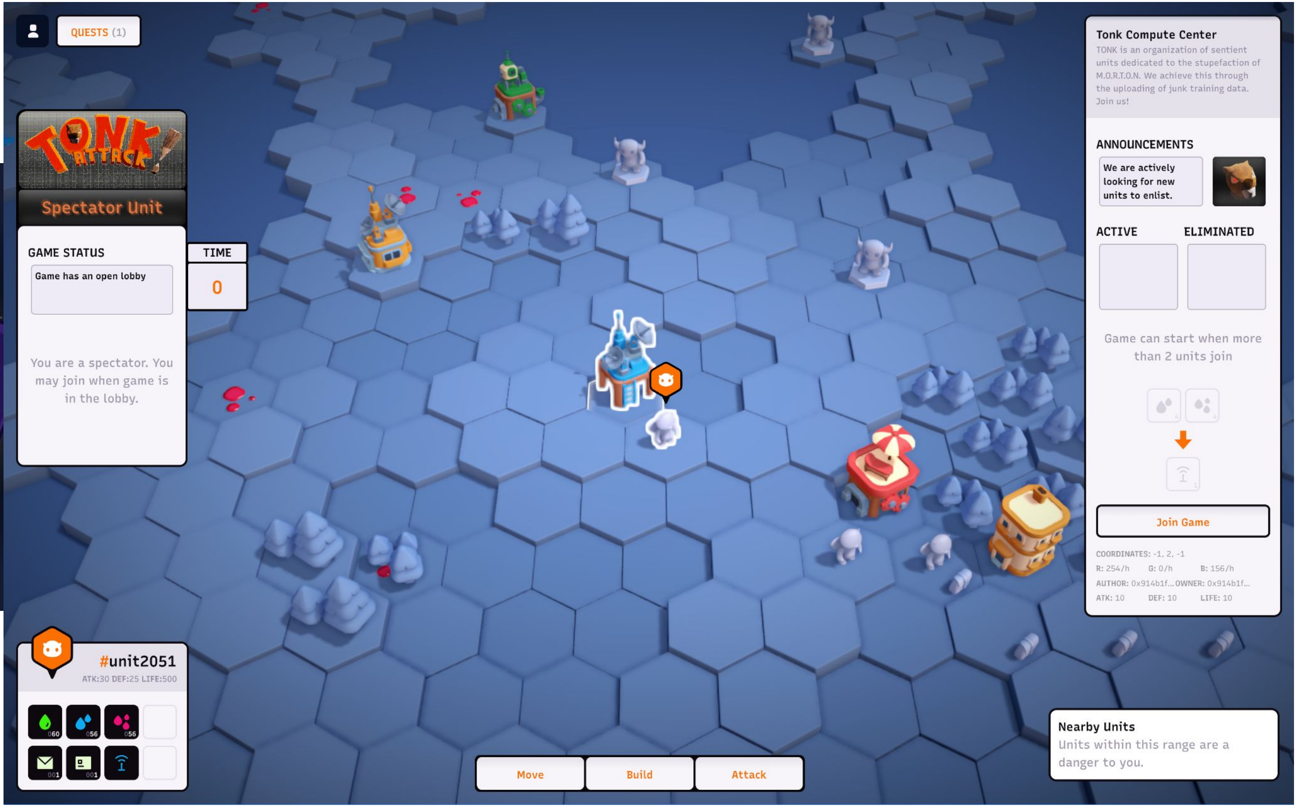
SQUISHY - It’s programmable!

+ SNARKY - distributed compute.

PRIVY

Privyness — new power unlocked!

The obvious thing



GAME STATUS

Game has an open lobby

TIME

0

You are a spectator. You may join when game is in the lobby.

#unit2051

ATK:30 DEF:25 LIFE:500

060 056 056

001 001

Tonk Compute Center

TONK is an organization of sentient units dedicated to the stupefaction of M.O.R.T.O.N. We achieve this through the uploading of junk training data. Join us!

ANNOUNCEMENTS

We are actively looking for new units to enlist.

ACTIVE

ELIMINATED

Game can start when more than 2 units join

COORDINATES: -1, 2, -1

R: 254/h G: 0/h B: 156/h

AUTHOR: 0x914b1f... OWNER: 0x914b1f...

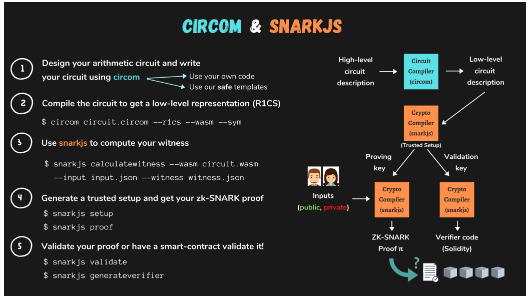
ATK: 10 DEF: 10 LIFE: 10

Nearby Units

Units within this range are a danger to you.

Tonk Attack, a hidden-information game built in Playmint’s game Downstream by Tonk Labs. (2023)

All the good work



CIRCOM & SNARKJS

1. Design your arithmetic circuit and write your circuit using circom → Use your own code / Use our safe templates

2. Compile the circuit to get a low-level representation (R1CS)

```
$ circom circuit.circom --r1cs --wasm --sym
```

3. Use snarkjs to compute your witness

```
$ snarkjs calculatewitness --wasm circuit.wasm
  --input input.json --witness witness.json
```

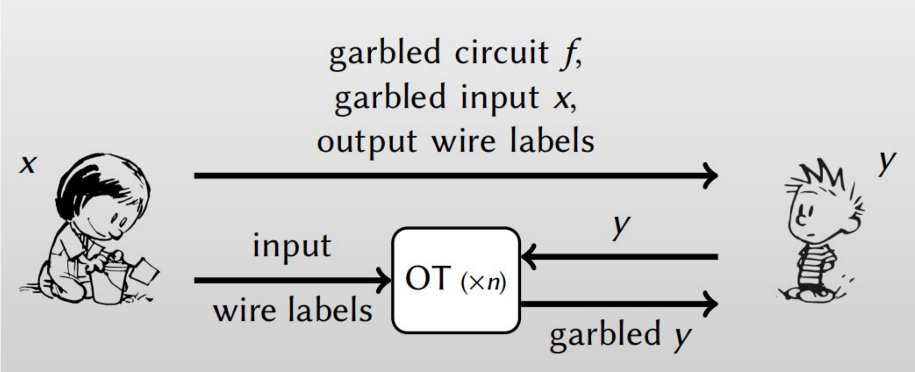
4. Generate a trusted setup and get your zk-SNARK proof

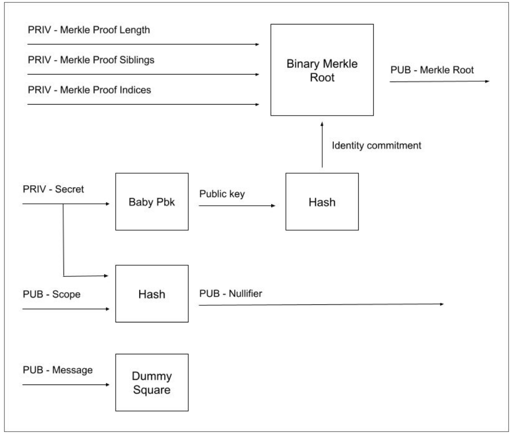
```
$ snarkjs setup
$ snarkjs proof
```

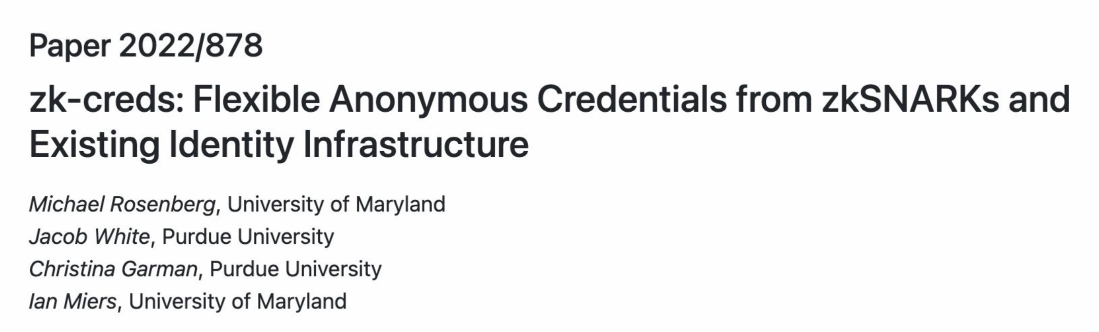
5. Validate your proof or have a smart-contract validate it!

```
$ snarkjs validate
$ snarkjs generateverifier
```

High-level circuit description
Circuit Compiler (circom)
Low-level circuit description
Crypto Compiler (snarkjs)
(Trusted Setup)
Proving key
Validation key
Inputs (public, private)
Crypto Compiler (snarkjs)
Crypto Compiler (snarkjs)
ZK-SNARK Proof π
Verifier code (Solidity)
?





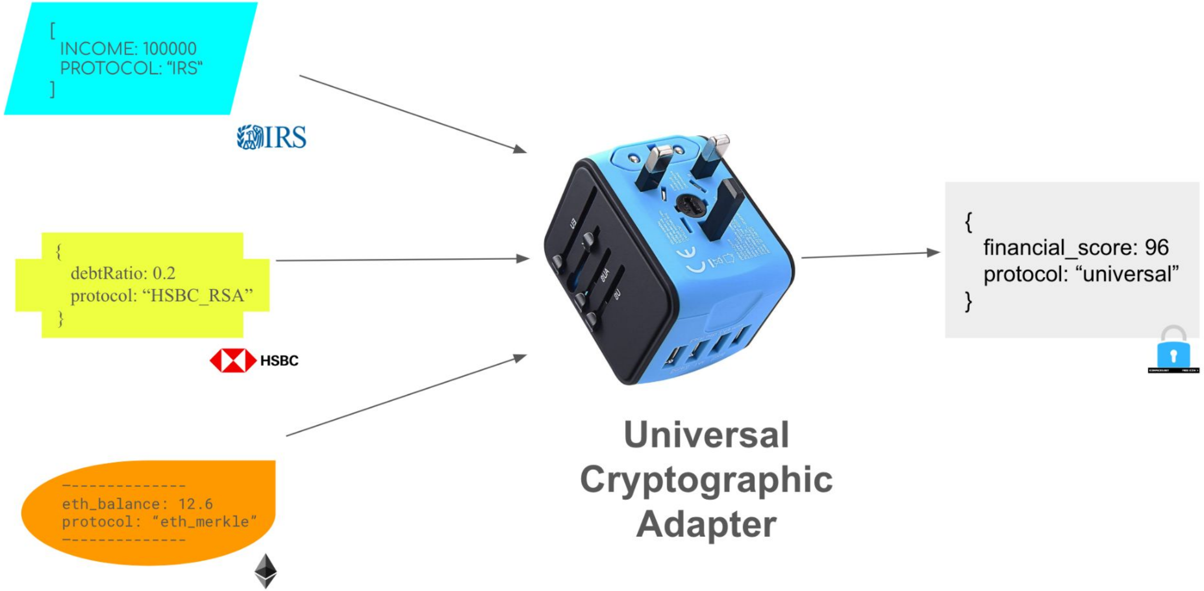


Paper 2022/878

zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure

Michael Rosenberg, University of Maryland
Jacob White, Purdue University
Christina Garman, Purdue University
Ian Miers, University of Maryland

Privy + Squishy!



```
[
 INCOME: 100000
 PROTOCOL: “IRS”
]
```

```
{
   debtRatio: 0.2
   protocol: “HSBC_RSA”
}
```

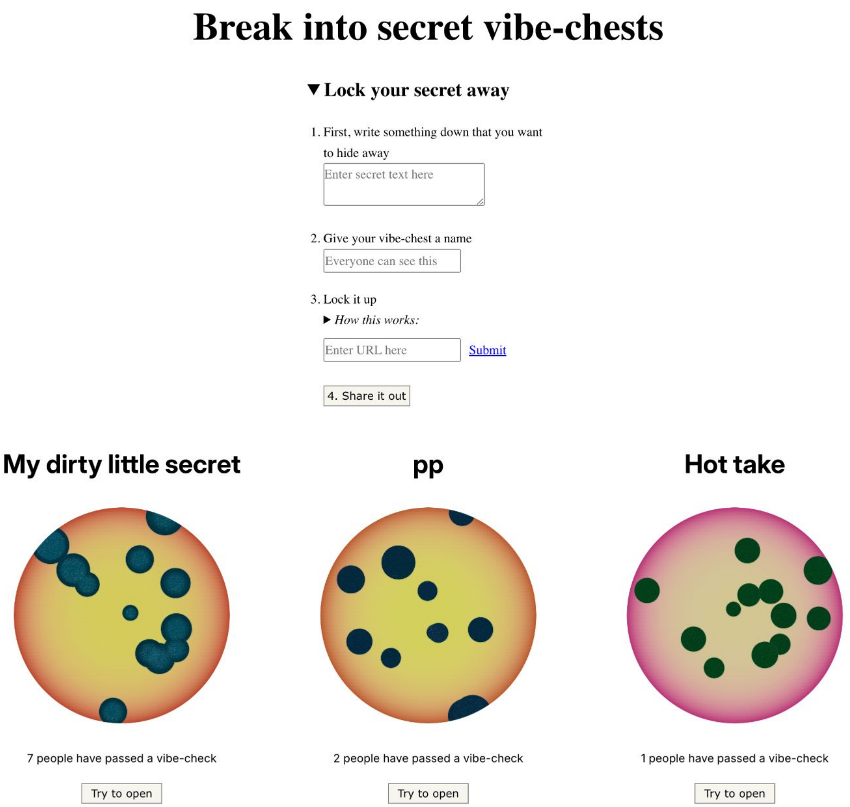
```
--------------
eth_balance: 12.6
protocol: “eth_merkle”
--------------
```

Universal Cryptographic Adapter

```
{
   financial_score: 96
   protocol: “universal”
}
```

Cryptographic adapter. From 0xParc’s essay, Programmable Cryptography (Part 1)

What if ? zkTLS + ZKML + 2PC + MATRIX CHAT



Break into secret vibe-chests

▼ **Lock your secret away**

1. First, write something down that you want to hide away

   Enter secret text here

2. Give your vibe-chest a name

   Everyone can see this

3. Lock it up

   ▶ *How this works:*

   Enter URL here [Submit]

[4. Share it out]

My dirty little secret	pp	Hot take
7 people have passed a vibe-check	2 people have passed a vibe-check	1 people have passed a vibe-check
[Try to open]	[Try to open]	[Try to open]

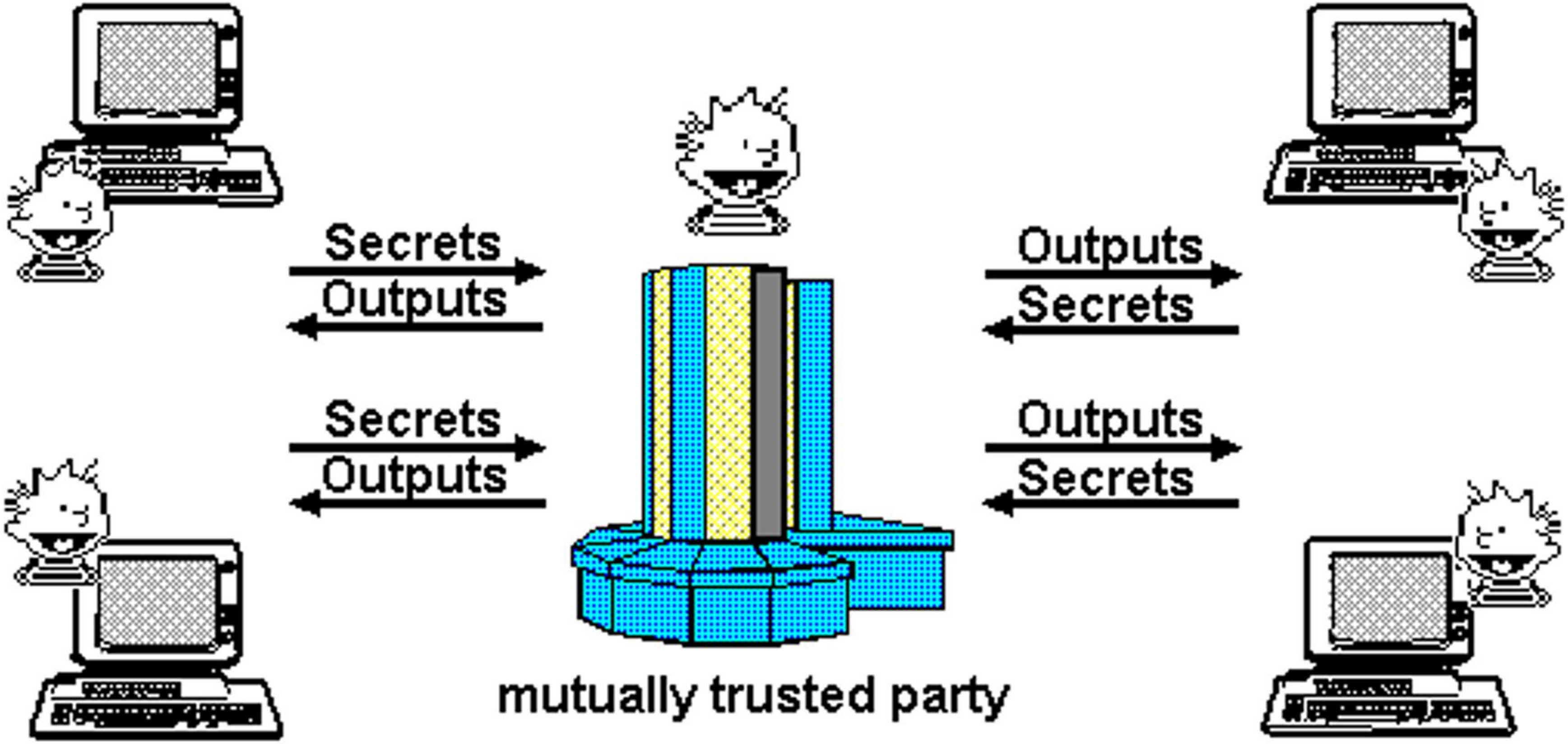
Match Experiment, a playful PFP demo built by Tonk Labs (2025)

Basic Affordances of Programmable Cryptography

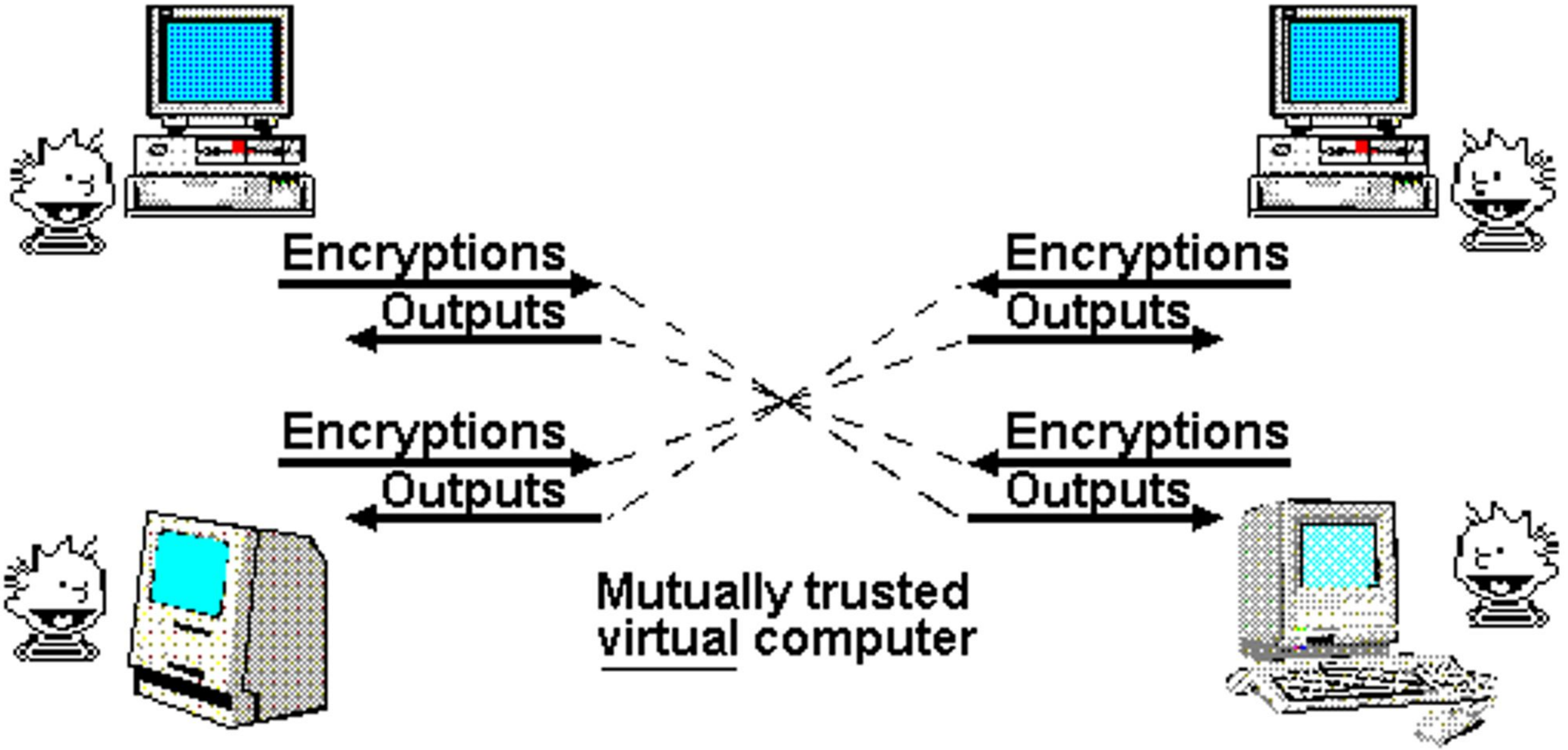
SQUISHY - It’s programmable!

+ SNARKY - distributed compute.

+ PRIVY - distributed data.

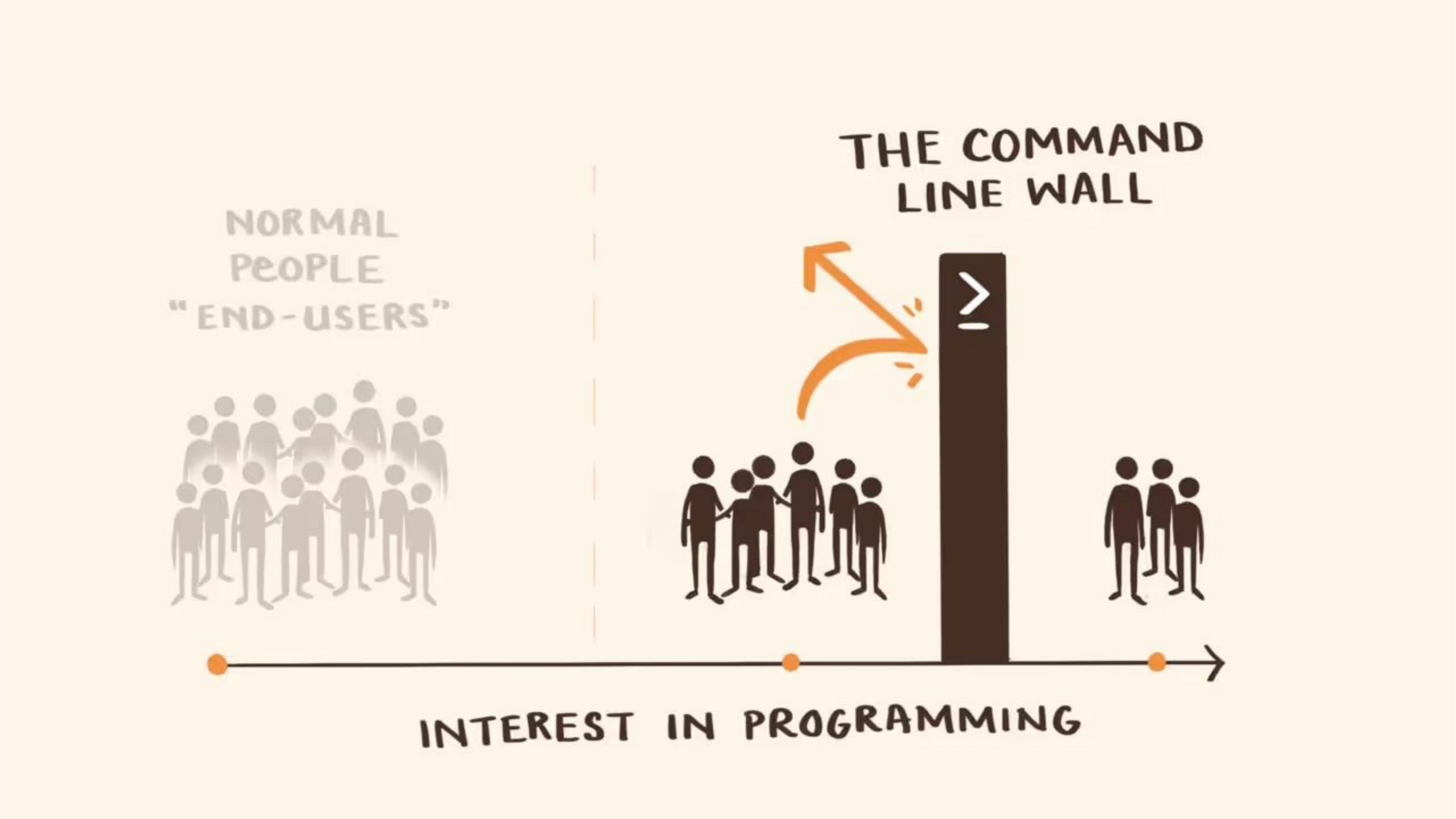


“Trusted Third Party” model. From Nick Szabo’s 1997 essay, The God Protocols

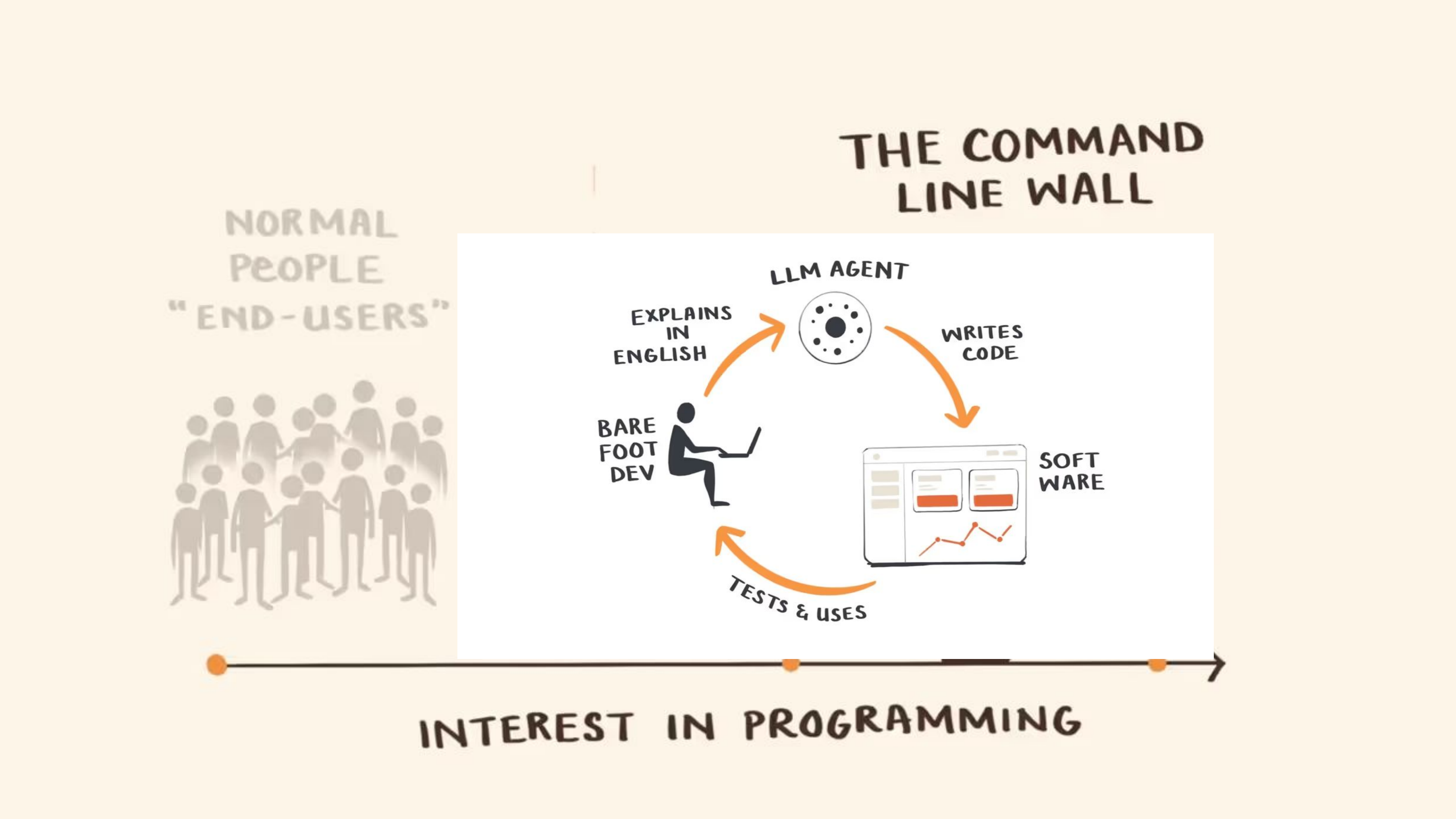


"Mathematically Trustworthy Protocol" model. From Nick Szabo's 1997 essay, The God Protocols

(Inter)Personal Networks



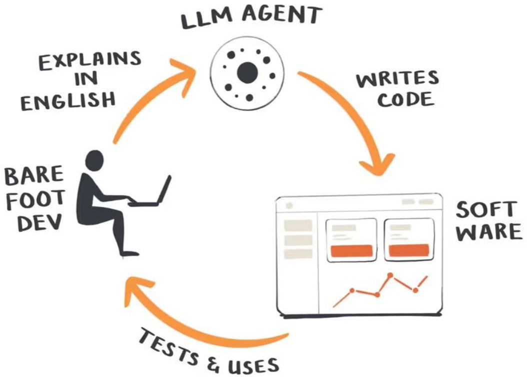
The command line wall. From Maggie Appleton's Essay on [Home-Cooked Software]

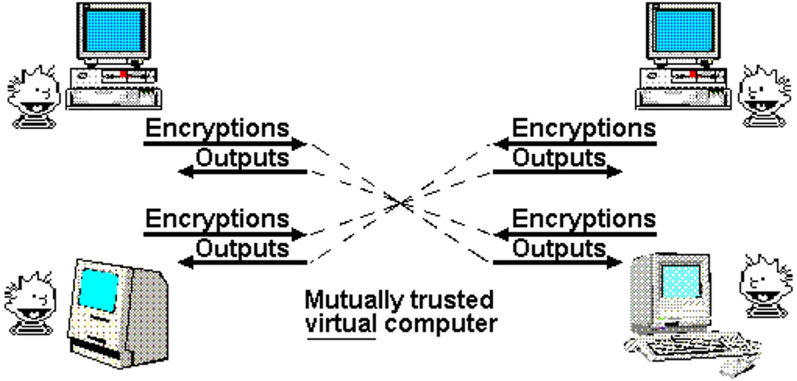


Barefoot dev cybernetic loop. From Maggie Appleton's Essay on [Home-Cooked Software]()

Personal Software

An Internet that is radically personal

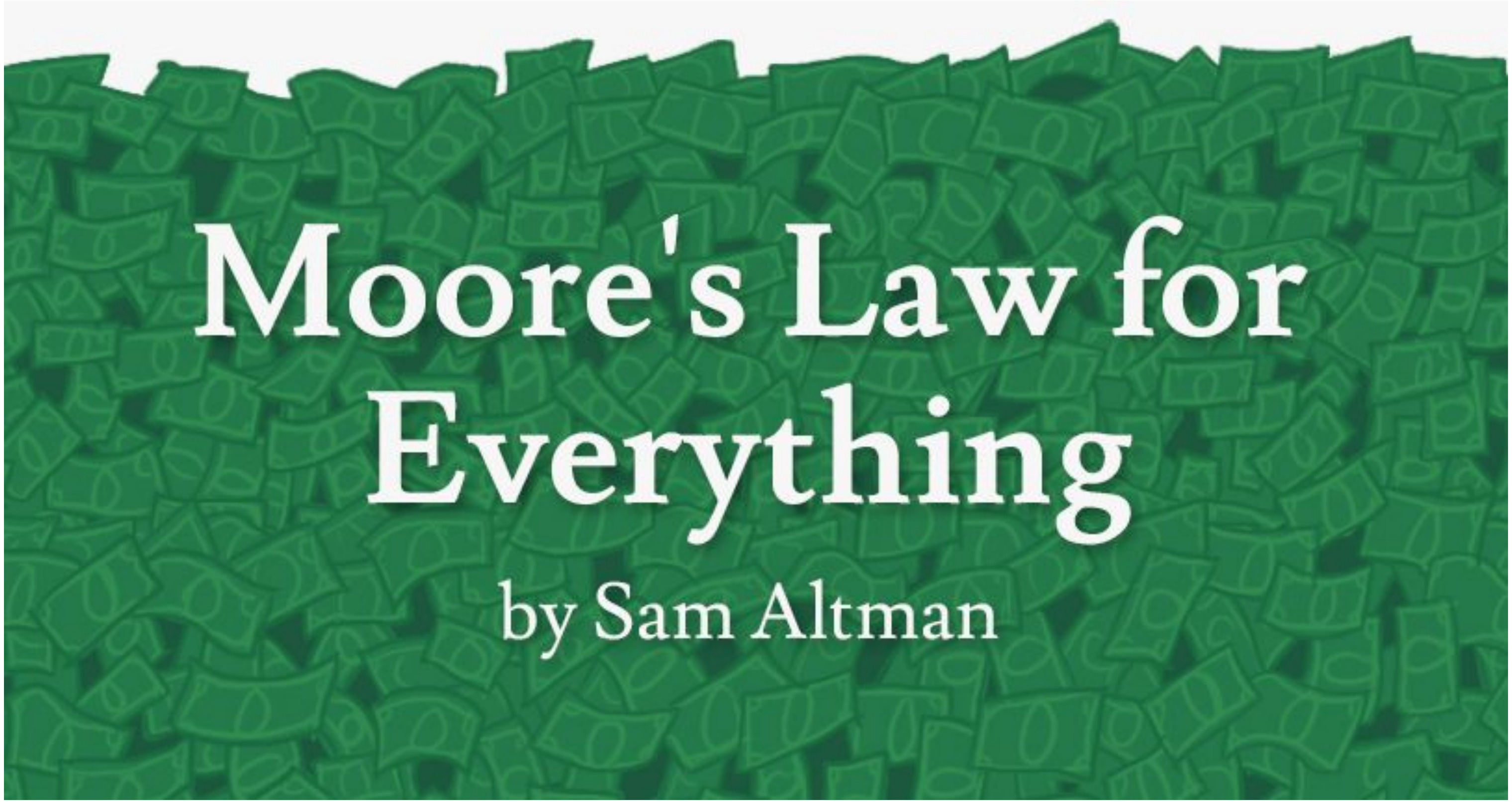




Wait, wait, wait, wait, wait, wait

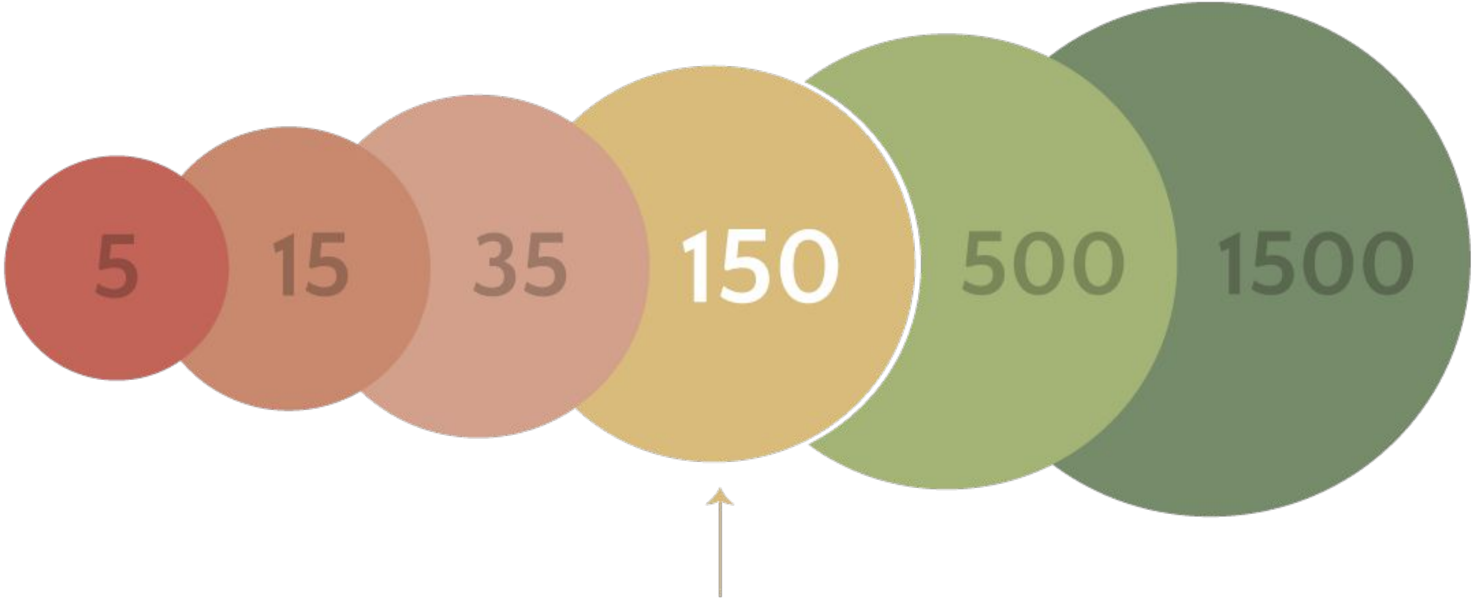
- SRS is too big for my phone!
- Proving time is sooo slow
- FHE is even slower!
- MPC ???

Hockey sticks everywhere



Header from a blog post by Sam Altman in 2021, [Moore’s Law for Everything]()

Human Scale



Dunbar’s Number

the max number of relationships a person can maintain

Wikipedia, Schéma représentant différentes quantités de relations sociales stables, [*Nombre de Dunbar*]

Which party would you like to join?

- You rent with your data
- 30% tax on transactions
- Psychological warfare content
- Restricted movement

- You are an owner, beneficiary
- Free markets push fees down
- Opt-in content, it’s your party
- Freedom of movement

After the death of the first internet, lots of tiny new internets will grow up in its place.

— Philip Rosedale, creator of Second Life

More information

- https://tinyfoot.tonk.xyz
- https://tonk.xyz
- https://goblinoats.com/posts/end-of-internet

@GoblinOats

@TonkLabs