

**ProgCryptoSG**

# **Intro to ZK**

Flying Nobita

2024-10-16

# Content



**01**

*What is ZK*

*Use for?*



**02**

*What is ZK?*

# How ZK is used in blockchain?

2024 Electric Capital ZK Market Map		6		273		53								
August 8, 2024 V1.0		X @ElectricCapital		tech layers		unique projects		categories						
User Facing	<b>Apps</b> <b>23</b> projects <b>6</b> categories	<b>Wallets</b> <b>General</b> Argent, Auro Wallet, Aival, Braavos, Leo Wallet, Payy Wallet, Puzzle Silk, Wesabi Zashi, zkBob	<b>Identity &amp; Data Management</b> <b>General</b> Outdid, Persona, Privasea, zCloak Network, zkMe	<b>Public Goods</b> <b>General</b> clrfund, Rarimo Freedom Tool, Vocdoni	<b>Gaming</b> <b>Community Platforms</b> Showdown	<b>Games</b> zkHoldem	<b>Fiat Onramp &amp; Payments</b> P2P.X, zkP2P	<b>11</b> <b>5</b> <b>3</b> <b>2</b> <b>2</b>						
	<b>Protocols</b> <b>38</b> projects <b>9</b> categories	<b>DeFi</b> <b>Shielded Pools</b> Hinkal, Namada, Penumbra	<b>DEXes</b> dYdX, Lighter, Lumina	<b>Mixers</b> Satari, Privacy Pools, Tornado Cash	<b>General</b> NOVA	<b>Identity &amp; Data Management</b> <b>General</b> Holonym, id-Mask, iden3, Privado ID	<b>Privacy &amp; Shielding</b> <b>General</b> Fin Protocol, Nym, Panther Protocol, Railgun, Zerochain, zkEmail	<b>Gaming</b> <b>General</b> Dark Forest, Dark Frontier, Pioneer	<b>Content Provenance</b> Irys, Maya Labs	<b>14</b> <b>10</b> <b>9</b> <b>3</b> <b>2</b>				
	<b>Developer Tools &amp; Services</b> <b>64</b> projects <b>10</b> categories	<b>Tools</b> <b>Languages</b> Cairo, Circom, Leo, Lurk, Noir, Ola, Vampir, ZoKrates	<b>SDKs</b> arkworks, gnark, ojs, PlonKathon, Rinkathon, snarkjs	<b>Gaming</b> Argus Labs, Cartridge, Dojo, Lattice, Palma, Spin	<b>Verifiable Data</b> Opacity Network, Pluto, Reclaim, ZKON	<b>Privacy</b> Sunscreen, Tonk	<b>Deployment</b> <b>RaaS</b> AltLayer, Caldera, Conduit, Gateway.fm, Gelato	<b>Frameworks &amp; SDKs</b> Airchains, Madara, Sovereign Labs, Zeko, ZKCross, Zypher Network	<b>Integrity &amp; Security</b> <b>Audits</b> Sherlock, SnarkLabs, Spearbit, Veridise, Zelic, ZK Labs, zkSecurity	<b>Compliance</b> Oxbow, Credora, Hakata, Keyring Network, Proven, Sealance	<b>Researchers</b> <b>General</b> OxPARC, Aerius Labs, Cursive, Delirium, Equilibrium, Geometry, Privacy and Scaling Explorations, Vad, Verificatum	<b>26</b> <b>16</b> <b>13</b> <b>9</b>		
	<b>Interoperability &amp; Middleware</b> <b>72</b> projects <b>13</b> categories	<b>Proof Supply Chain</b> <b>Demand Aggregation</b> Eigen Network, Gevulot, Irreducible, Lita Foundation, Lumoz, Marlin, Kalyso, Maya ZK, Nil Foundation, NovaNet	<b>RISC Zero</b> Bonsai, Sindr, Snarkify, Sorella Labs, Strobe, Succinct, Taralli Labs, Zero Computing, ZKPool	<b>Verifying</b> Aligned Layer, Electron, Hyle, Nebra, Pi Squared, zkVerify	<b>Sequencing</b> Astria, Espresso, NodeKit, Radius, Rome Protocol	<b>Supply Aggregation</b> Gevulot, Zero Computing	<b>Coprocessors</b> <b>Data</b> Axiom, Brevis, Herodotus, Lagrange, Relic, Space and Time, vlayer	<b>Compute</b> Automata, Bloccless, Clique, Delphinus Labs, Marlin, Phala, WeMeta	<b>MPC</b> Arcium, Fairblock, Jiritsu Network, Silence Labs, Tangle Network	<b>Oracles</b> Ora, PADG, Pragma, ZKML, Percept	<b>Bridges &amp; Cross-Chain Messaging</b> <b>General</b> Axelar, Hyperbridge, Mystiko, Polyhedra, Router Protocol, Sygma, Union, Wormhole, zkCross, ZKM	<b>Asset Bridges</b> Gasp, Orbiter	<b>ML/AI</b> <b>Verified Inference</b> Aizel Network, EZKL, Giza, Inference Labs, Modulus	<b>31</b> <b>24</b> <b>12</b> <b>5</b>
	<b>Core Infrastructure</b> <b>76</b> projects <b>15</b> categories	<b>L2s</b> <b>Ethereum Virtual Machine</b> Cronos zkEVM, ImmutableX, INTMAX, Kakarot, Kroma, Linea, Loopring, Manta Pacific, Morph, Myria, OKX X Layer, Payy Network	<b>Polygon zkEVM</b> Scroll, Sophon, Taiko, Zircuit, ZKBase, ZKFair, zkSync	<b>Bitcoin</b> Alpen, Bison Labs, BNZK, Chakra, Citrea, Twilight, ZeroSync	<b>Other</b> Aztec, Blockssense, Eclipse, Ola, Starknet	<b>L1s</b> <b>Contract Platforms</b> Anoma, Findora, Fluent, Manta Atlantic, Mina, Nockchain, Ziesha	<b>Privacy Enabled Contract Platforms</b> Aleo, Aleph Zero, DarkFi, Dusk, Inco	<b>zkVMs</b> <b>STARK</b> CairoVM, Eigen ZKM, Lita Valida, OlavM, Polygon Miden, RISC Zero, RISCO, Succinct SP1, TritonVM	<b>SNARK</b> aTBS, Jolt, Also snarkVM, Delphinus Lab, ZKWASM, Nexus zkVM, Nock zkVM	<b>Other</b> powdr	<b>Hardware</b> <b>General</b> Accessal, Cysic, Fabric, Ingonyama, Irreducible, Supranational	<b>Execution Layers</b> QED Protocol, Silent Protocol	<b>L3s</b> Spire, zkLink	<b>Data Compression</b> Light Protocol

# Outsourcing Computation

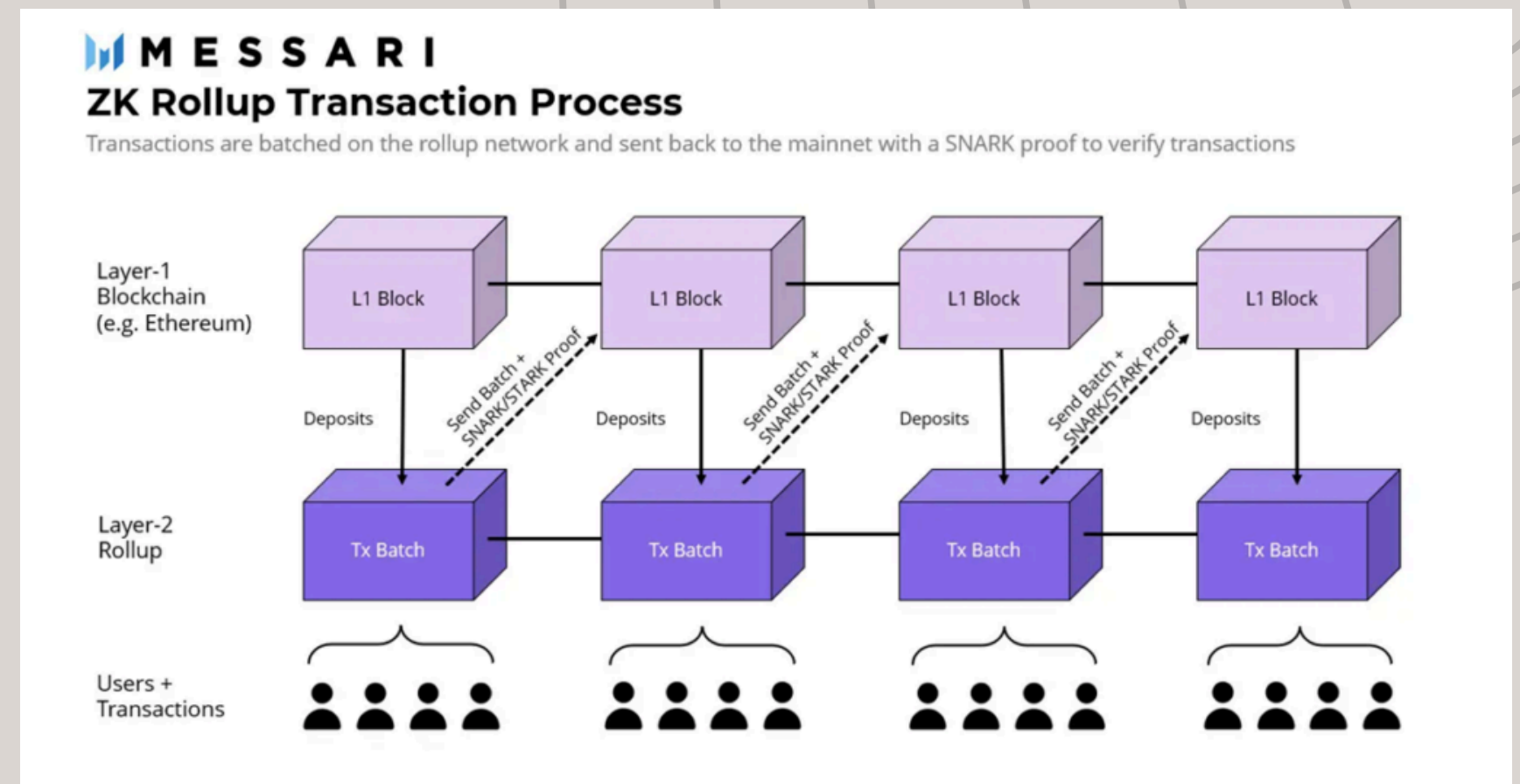
**Weaker** machines (blockchain):

- **outsources** hard computations to powerful machines
- **verifies** the **succinct** proofs that ensure the transactions are valid

**ZK Rollups scale** blockchain by reducing **costs**:

1. transactions executed and batched on L2 by rollup nodes
2. proof is generated that prove the transactions are valid
3. batched transaction and proof are submitted to L1

Cost is **amortized** across many transactions and users



# Outsourcing Computation

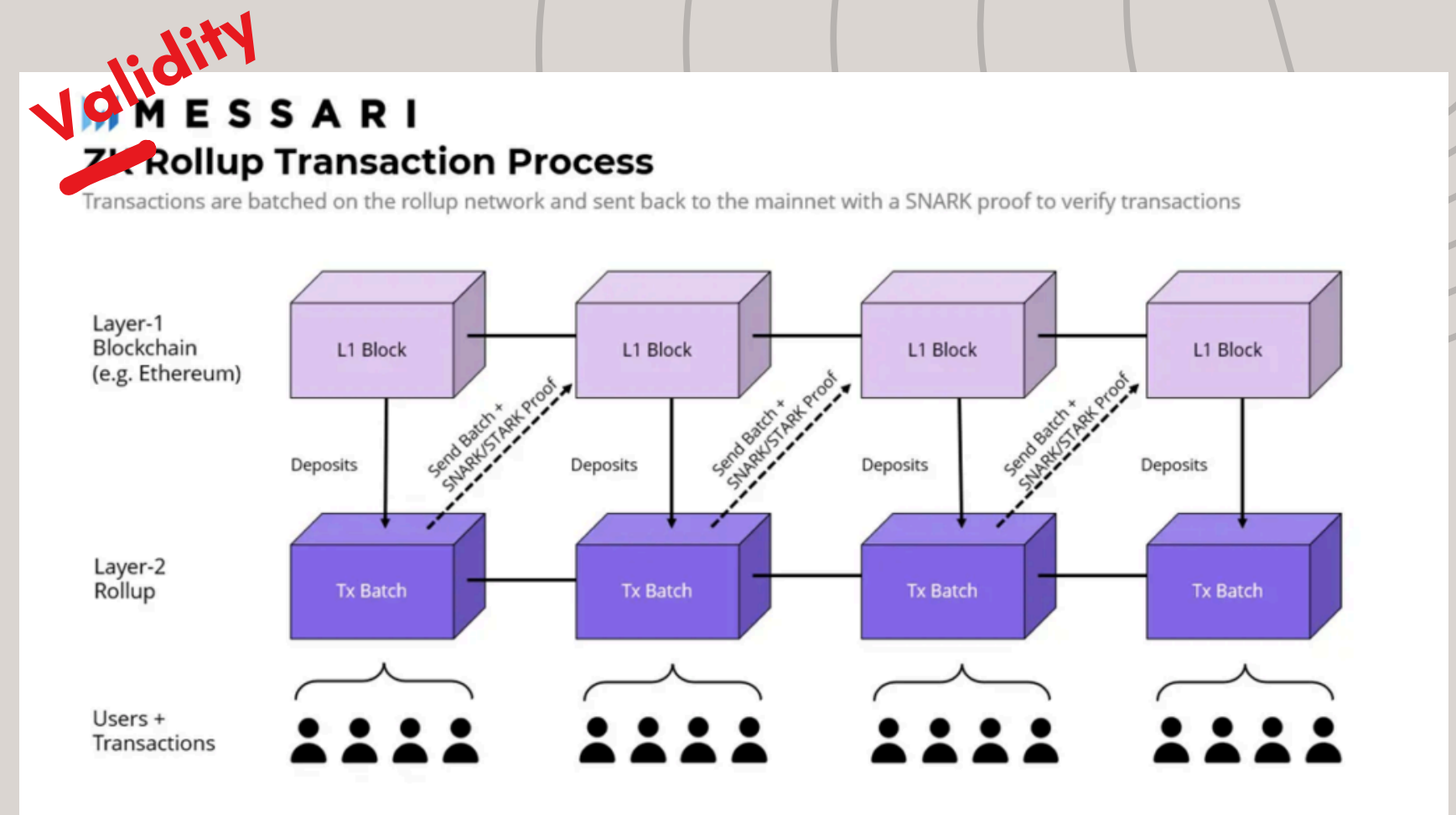
**Weaker** machines (blockchain):

- **outsources** hard computations to powerful machines
- **verifies** the **succinct** proofs that ensure the transactions are valid

**ZK Validity Rollups scale** blockchain by reducing **costs**:

1. transactions executed and batched on L2 by rollup nodes
2. proof is generated that prove the transactions are valid
3. batched transaction and proof are submitted to L1

Cost is **amortized** across many transactions and users

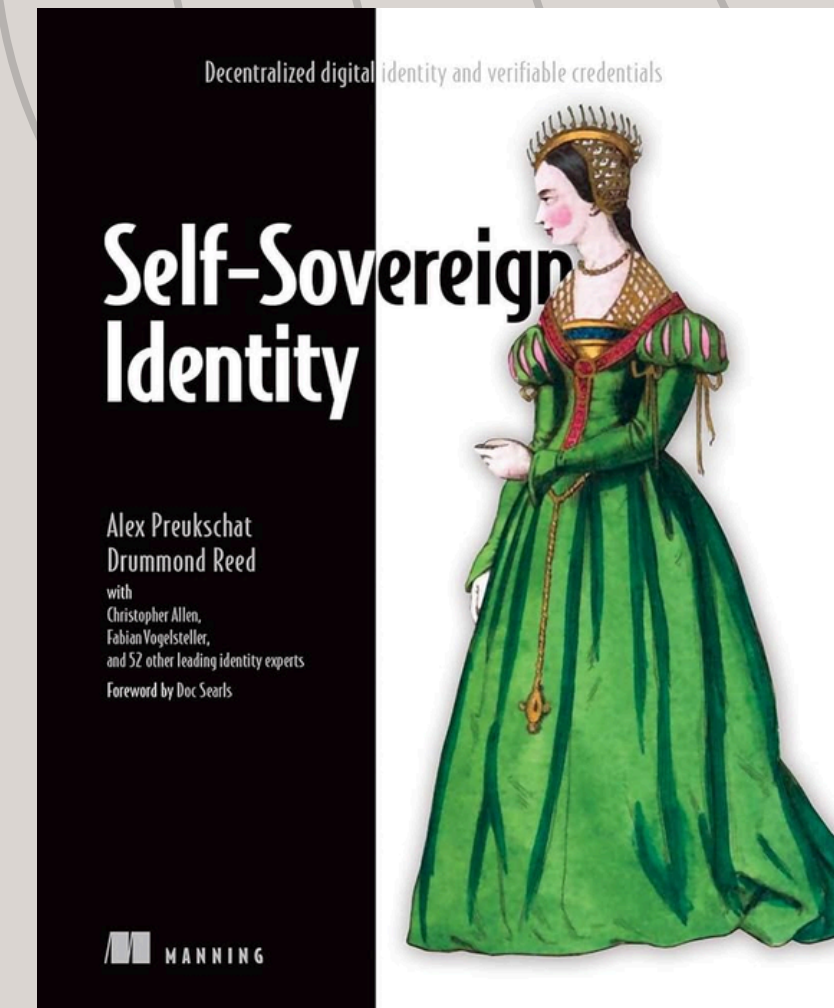


# Self-Sovereign Identity

Self-sovereign identity requires:

- **selective disclosure** of attributes to **prove predicates** without disclosing the attributes themselves
- **unlinkability** between proofs
- cheap on-chain verification with **succinct** proofs for on-chain KYC

Require **Zero Knowledge Proofs** + other cryptographic primitives



# Some more..

## Privacy-oriented blockchain & Dapps

- **private** transactions and states
- e.g. Zcash, Aleo, Aztec, Mina

## ZK Coprocessors

- a form of **outsourcing computation**
- used at the smart contracts layer

## ZK Bridges

- states on chain 1 can be **succinctly** verified on chain 2
- allow transactions to flow across chains
- replaces multisigs or centralized bridges

# Content



**01**

*What is ZK  
used for?*

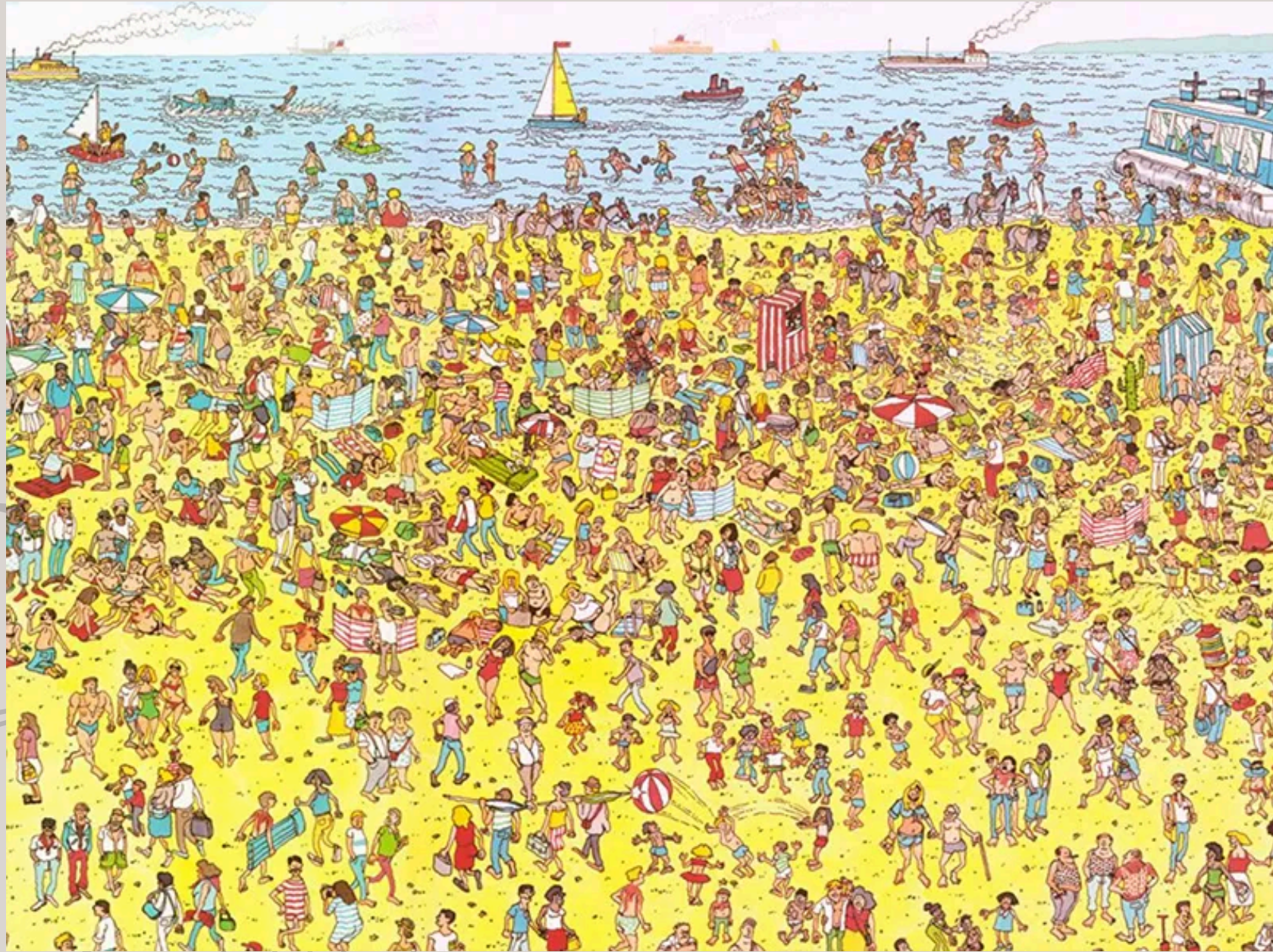


**02**

*What is ZK?*



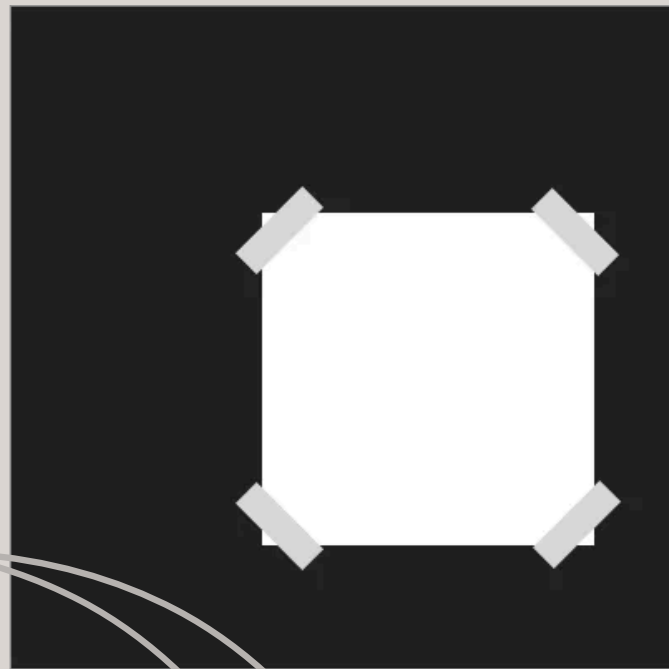
# Where's Wally?



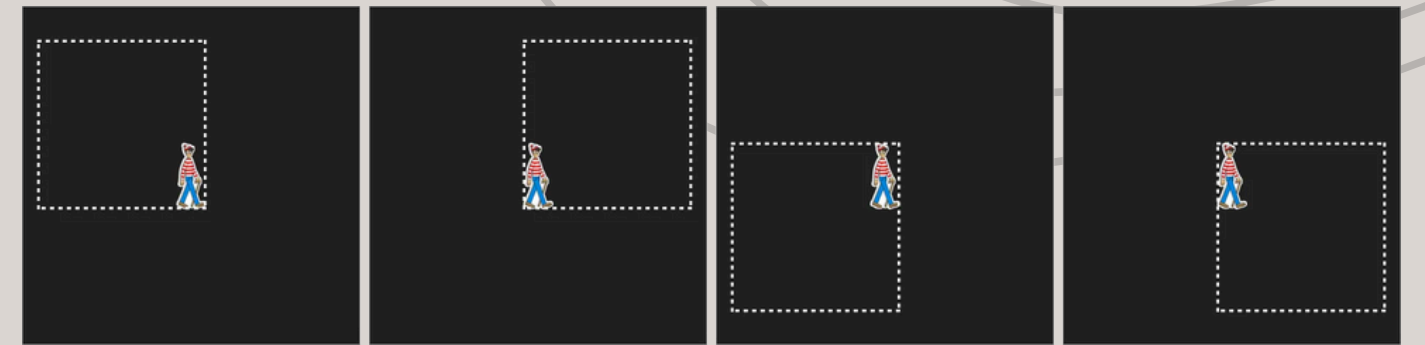
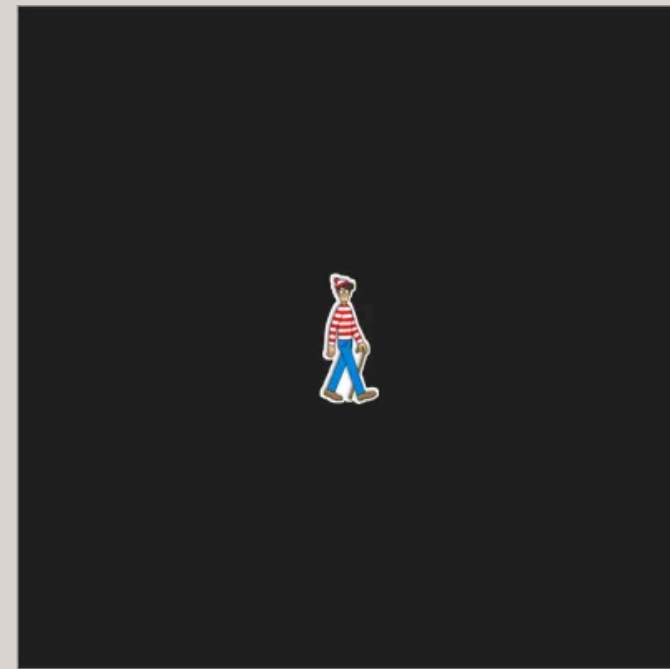
*How can I prove to you I know  
where Wally is without giving the  
answer away?*

# Where's Wally?

Back



Front



front black card > 2X size of puzzle

you only know that I know the answer,  
but you still need to find Wally yourself

# So What Does ZK Really Mean?

By **ZK**, we mean

**Zero Knowledge Proof System**

# Classical Proofs

Traditionally, proofs are:

- static statements that follow axioms and logical deductions
- checked step-by-step for correctness

Proof:

$$\text{When } n=1, \frac{n(n+1)(2n+1)}{6} = \frac{1(2)(3)}{6} = 1^2.$$

$$\text{Suppose that } 1^2 + 2^2 + 3^2 + \dots + k^2 = \frac{k(k+1)(2k+1)}{6}$$

$$\text{Then, } 1^2 + \dots + k^2 + (k+1)^2$$

$$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

$$= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6}$$

$$= \frac{(k+1)(k(2k+1) + 6(k+1))}{6}$$

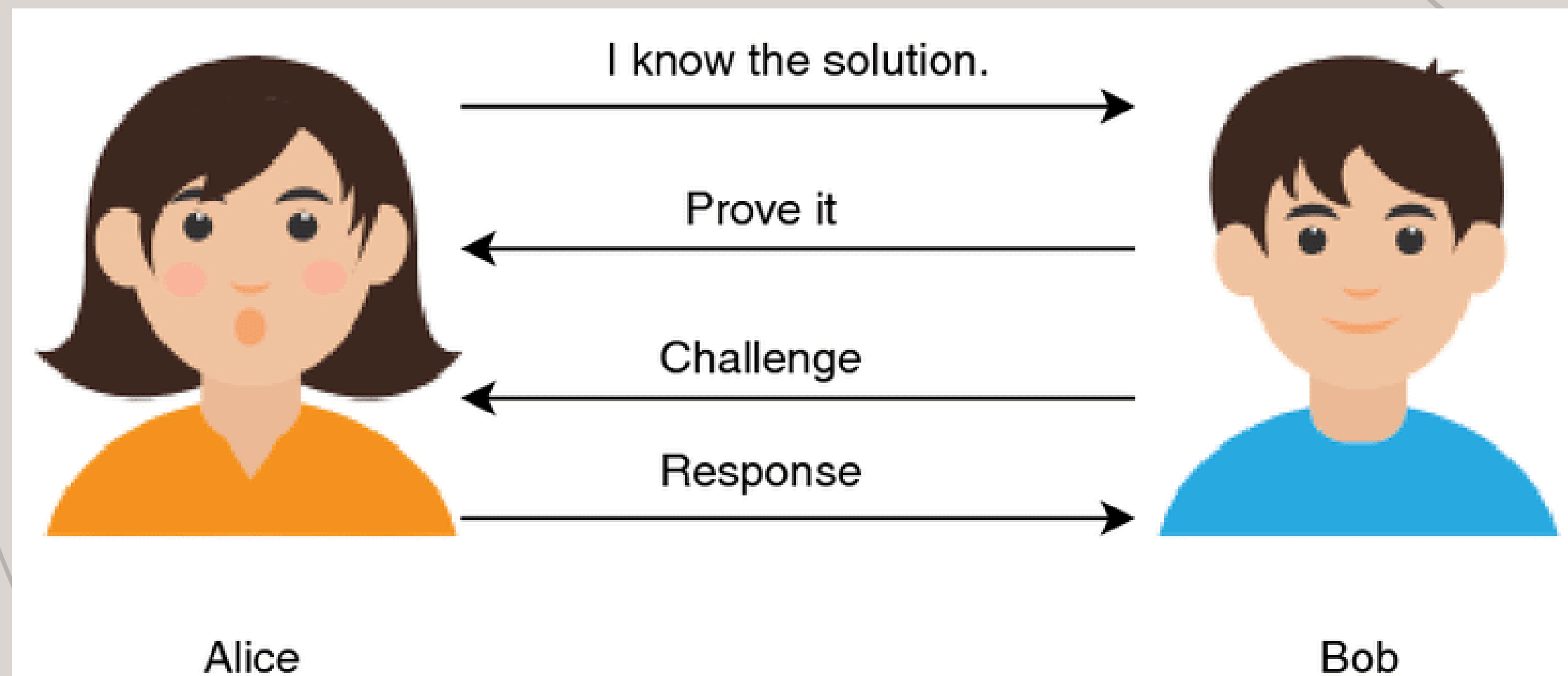
$$= \frac{(k+1)(2k^2 + 7k + 6)}{6}$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}$$



# Interactive Proofs

Proofs involve **interaction** between **Prover** and **Verifier**



# How to get started?

Let's translate Where's Wally into  
a ZK Proof problem!

# Let's Rephrase It *(informal)*

**Objective:**

Alice wants to prove to Bob that she knows where Wally is, without revealing the answer

**Statement  $s$**  – can only be True or False:

Alice knows where Wally is in Where's Wally Beach puzzle

**Witness  $w$**  – Alice's solution:

Wally's location (only one in this case)

**Instance  $x$**  – a specific problem:

Where's Wally Beach puzzle (Wally can be hiding in other places in another puzzle)

**Relation  $R$  for NP** – set of ordered pairs  $(x, w)$ :

$R_{\text{Wally}}$ . We say "The pair (Beach, Wally's Location) is in  $R_{\text{Wally}}$ "

**Language  $L$**  – the set of all satisfiable instances for  $R$  i.e.  $L(R)$

Set of all Where's Wally puzzles and their locations. i.e.  $S$  is in  $L(R_{\text{Wally}})$

# Now we're ready to define our ZKP Statement

To give proof that an **instance** is in the **language** defined by some **relation**, without revealing the **witness**.

*I can prove that I know the solution to this puzzle, without giving away the actual solution. You can take the proof and verify it easily.*



# Privacy (Zero Knowledge)

Allow the Prover to prove to the Verifier that:

1. Prover knows the solution
2. The proof doesn't reveal anything else  
except 1



# Compression (Succinctness)

How to get **efficient verification**?

We need **short proofs**:

- short proof lengths ( $O(\log)$ )
- quick verification time ( $O(\log)$  or  $O(1)$ )

**Probabilistically Checkable Proof (PCP) Theorem:**

Any problem that can be verified by Classical Proof can also be verified by a special IP proofs where Verifier reads **a few random bits** from the proof

**Proofs** -> **succinct** by using *Polynomial Commitment Schemes*



# But..

## What's the catch?

A **tiny** chance that an **incorrect proof** passes verification.

**But** it's so small that we can basically **ignore** it!

## What if I don't want interactivity?

There's a trick we can make IP **non-interactive** again (*Fiat-Shamir transformation*)

# Some More Important Properties

## **Completeness:**

If the proposed solution is correct, the Verifier will accept it.

*i.e. if it's true, it stays true*

## **Soundness:**

If the proposed solution is incorrect, the Verifier will not accept it.

*i.e. if it's false, it stays false*

# **We now have ZKP System!**

***ZKP = Language + IP + Compression +  
Completeness + Soundness +  
Privacy (optional) +  
Convert back to NI (optional but common)***

# Thank you

**List of ZK Resources**



# References

1. Proofs, Arguments & Zero-Knowledge, Jul 18, 2023, Justin Thaler
2. Do You Need a Zero Knowledge Proof?, 2024, Ernstberger et al
3. ZK Market Map (Aug 8, 2024), Electric Capital, <https://www.cryptomarketmap.org/zk>



# Appendix



# Argument vs Proof vs Knowledge

