ZERO-KNOWLEDGE PROOFS (ZKP)

Yijia Chen

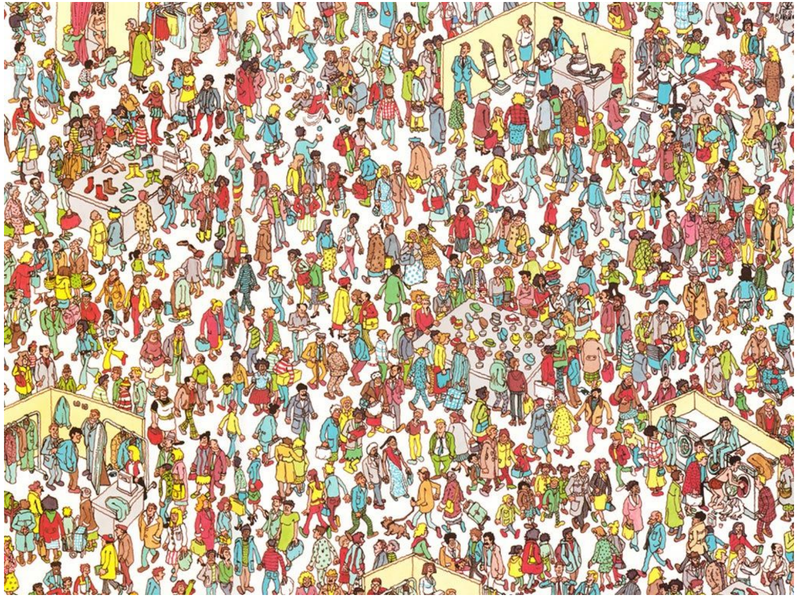
Dec 4, 2021

DISCUSSION

Food for Thought

DISCUSSION

Food for Thought



AGENDA

01 ZKPs: Cryptographic Intro

02 Applications

03 ZK-Rollups and Layer 2

04 Developer Ecosystems

05 Discussion

AGENDA

01 ZKPs: Cryptographic Intro

02 Applications

03 ZK-Rollups and Layer 2

04 Developer Ecosystems

05 Discussion

TOPIC

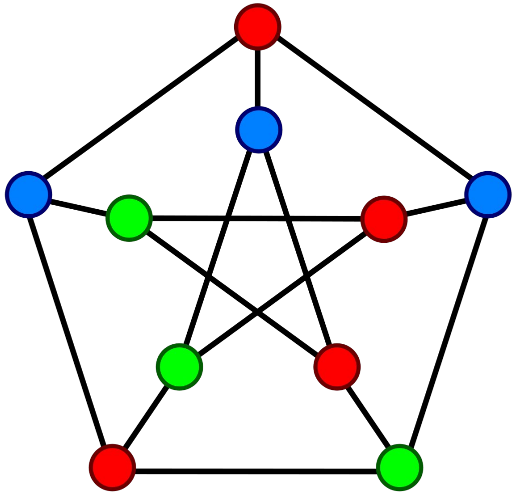
ZKPs: Definition and Origin

- ZKPs: Zero-Knowledge Proofs
- Allows one party (the prover) to prove to another (the verifier) that a statement is true, without revealing any information beyond the validity of the statement itself.
- Coined by MIT researchers Shafi Goldwasser, Silvio Micali, Charles Rackoff

EXAMPLE

3-Coloring Problem

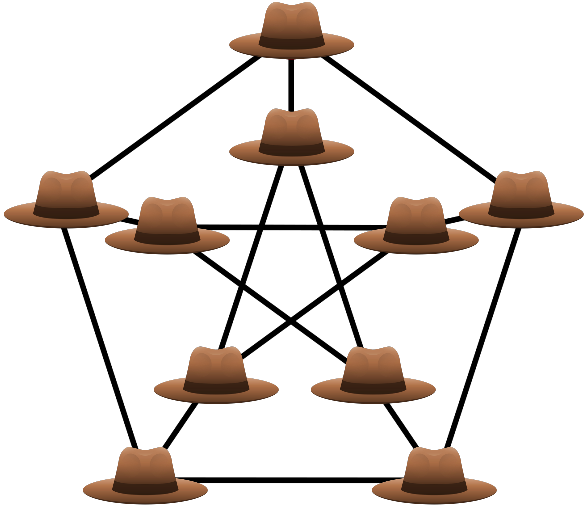
- Given a graph *G*, can all vertices be colored with 3 colors so that no edge has vertices of the same color?
- This is an NP-complete problem
  - i.e. very hard in the general case
- Andy wishes to prove existence of solution to Conan
  - Conan starts a new uncolored version of *G*.
  - Privately, Andy colors all vertices with a **permutation** of the 3 colors, and then hides all vertices under "hat"s.
  - Conan picks an edge, of which Andy reveals both vertices.
  - If the vertices are of the same color, Andy loses.
  - If the vertices are of different colors, then it remains possible that Andy has a solution. To start another round of *challenge-response*, they repeat from the first step.



EXAMPLE

3-Coloring Problem

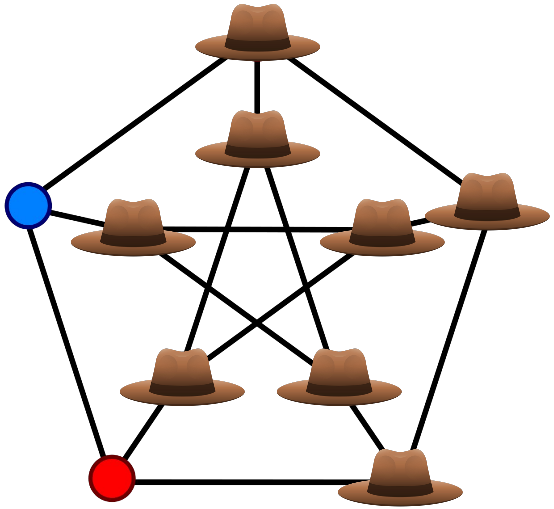
- Given a graph *G*, can all vertices be colored with 3 colors so that no edge has vertices of the same color?
- This is an NP-complete problem
  - i.e. very hard in the general case
- Andy wishes to prove existence of solution to Conan
  - Conan starts a new uncolored version of *G*.
  - Privately, Andy colors all vertices with a **permutation** of the 3 colors, and then hides all vertices under “hat”s.
  - Conan picks an edge, of which Andy reveals both vertices.
  - If the vertices are of the same color, Andy loses.
  - If the vertices are of different colors, then it remains possible that Andy has a solution. To start another round of *challenge-response*, they repeat from the first step.



EXAMPLE

3-Coloring Problem

- Given a graph *G*, can all vertices be colored with 3 colors so that no edge has vertices of the same color?
- This is an NP-complete problem
  - i.e. very hard in the general case
- Andy wishes to prove existence of solution to Conan
  - Conan starts a new uncolored version of *G*.
  - Privately, Andy colors all vertices with a **permutation** of the 3 colors, and then hides all vertices under “hat”s.
  - Conan picks an edge, of which Andy reveals both vertices.
  - If the vertices are of the same color, Andy loses.
  - If the vertices are of different colors, then it remains possible that Andy has a solution. To start another round of *challenge-response*, they repeat from the first step.



TOPIC

Three Important Properties

Valid ZKPs must satisfy the following conditions:

Completeness

If B is telling the truth, then B will eventually convince A.

Soundness

B can only convince A if they're telling the truth.

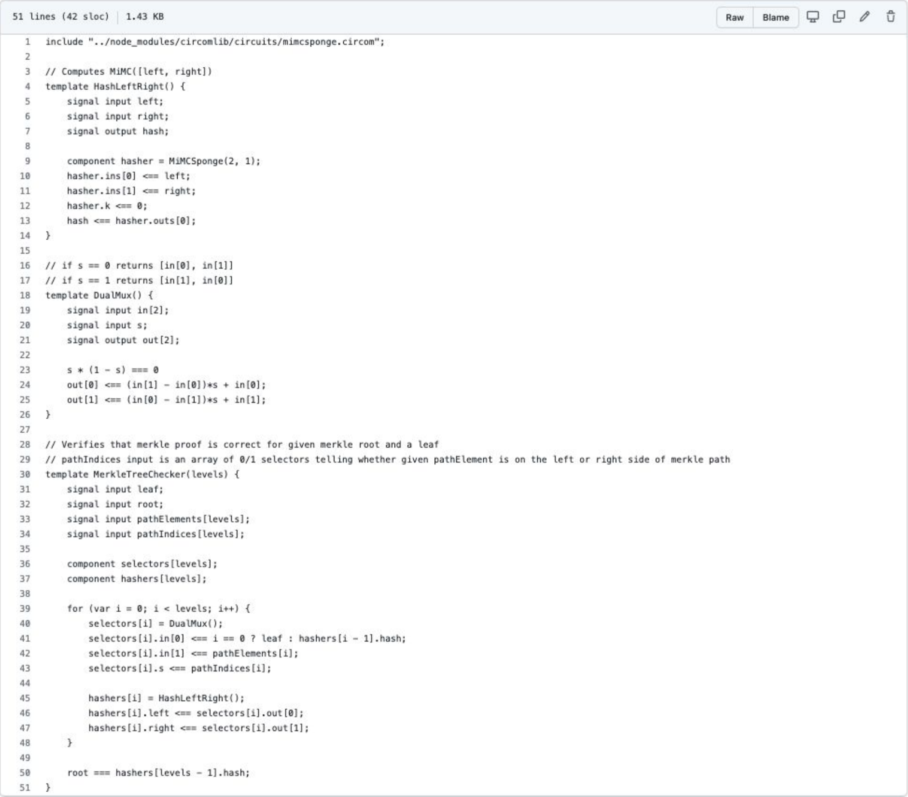
Zero-Knowledgeness

A does not learn anything else about B's proof.

TOPIC

ZK-SNARKs

- ZK-SNARK: Zero-Knowledge Succinct Non-Interactive ARgument of Knowledge
    - Succinct: short and well-defined
    - Non-interactive: once for all; no challenge-response dynamic
    - Sublinear verification time with respect to input
- Example written in Circom on the right



```
include "../node_modules/circomlib/circuits/mimcsponge.circom";

// Computes MiMC([left, right])
template HashLeftRight() {
    signal input left;
    signal input right;
    signal output hash;

    component hasher = MiMCSponge(2, 1);
    hasher.ins[0] <== left;
    hasher.ins[1] <== right;
    hasher.k <== 0;
    hash <== hasher.outs[0];
}

// if s == 0 returns [in[0], in[1]]
// if s == 1 returns [in[1], in[0]]
template DualMux() {
    signal input in[2];
    signal input s;
    signal output out[2];

    s * (1 - s) === 0
    out[0] <== (in[1] - in[0])*s + in[0];
    out[1] <== (in[0] - in[1])*s + in[1];
}

// Verifies that merkle proof is correct for given merkle root and a leaf
// pathIndices input is an array of 0/1 selectors telling whether given pathElement is on the left or right side of merkle path
template MerkleTreeChecker(levels) {
    signal input leaf;
    signal input root;
    signal input pathElements[levels];
    signal input pathIndices[levels];

    component selectors[levels];
    component hashers[levels];

    for (var i = 0; i < levels; i++) {
        selectors[i] = DualMux();
        selectors[i].in[0] <== i == 0 ? leaf : hashers[i - 1].hash;
        selectors[i].in[1] <== pathElements[i];
        selectors[i].s <== pathIndices[i];

        hashers[i] = HashLeftRight();
        hashers[i].left <== selectors[i].out[0];
        hashers[i].right <== selectors[i].out[1];
    }

    root === hashers[levels - 1].hash;
}
```

AGENDA

01 ZKPs: Cryptographic Intro

02 Applications

03 ZK-Rollups and Layer 2

04 Developer Ecosystems

05 Discussion

TOPIC

Blockchains and ZK-SNARKs

- Due to the technical design of blockchains, everything on-chain is **fully transparent** to everyone.
  - This includes one’s entire transaction history (including income stream), NFT possessions, gameplay stats, etc.
  - As blockchain use cases expand, the list could soon include much more sensitive information such as one’s health data.
  - A land of zero privacy…
- Founding value of blockchains: zero-trust/permissionlessness
- Dilemma: permissionlessness or privacy?
- Another problem: incomplete-information for fully-on-chain game
  - Imagine a game of poker
  - Fact: Current crypto games like Axie are not fully on-chain

CASE STUDY

Applications in DeFi

Zcash

- A Bitcoin fork with privacy features, created in 2016
- Transactions can be "transparent" and similar to bitcoin transactions in which case they are controlled by a t-addr, or they can be "shielded" and are controlled by a z-addr.
- Allows "selective disclosure", allowing a user to prove payment for auditing purposes. One such reason is to allow private transactors the choice to comply with anti-money laundering or tax regulations.

Tornado

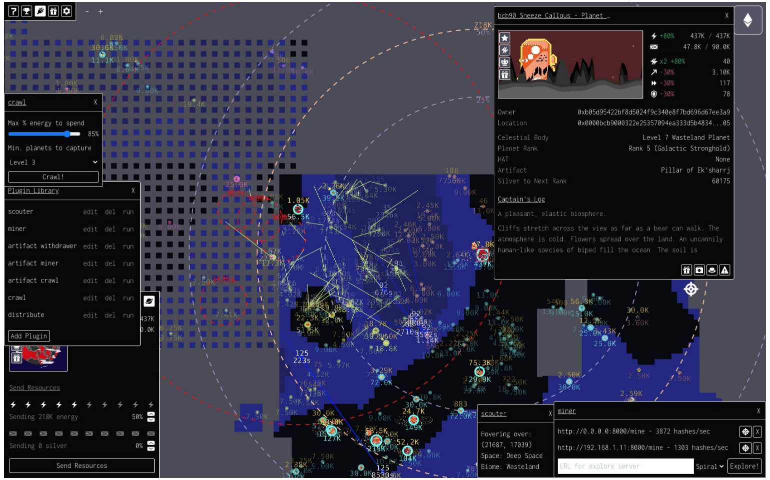
- A protocol for private transactions for ERC-20 tokens

$$\mathcal{S}[R, h, A, f, t] = \{\text{I KNOW } k, r \in \mathbb{B}^{248}, l \in \mathbb{B}^{16}, O \in Z_p^{16} \text{ SUCH THAT } h = H_1(k) \\ \text{AND } O \text{ is the opening of } H_2(k||r) \text{ at position } l \text{ to } R\}$$

CASE STUDY

Applications in Gaming

- In traditional games, nothing is on-chain.
- In current crypto games (Axie, Cryptomines, etc.), the ownables are on-chain in the form of NFTs, and thus tradable.
- In Dark Forest, the ownables as well as game logic is on-chain.
- Metaverse, composability, and interoperability



crawl

Max % energy to spend 85%

Min. planets to capture

Level 3

Plugin Library

scouter	edit	del	run
miner	edit	del	run
artifact withdrawer	edit	del	run
artifact miner	edit	del	run
artifact crawl	edit	del	run
crawl	edit	del	run
distribute	edit	del	run

Send Resources

Sending 218K energy 50%

Sending 0 silver 0%

bcb90 Sneeze Callous - Planet …

+80%	437K / 437K
	47.8K / 90.0K
x2 +80%	40
-30%	3.10K
-30%	117
-30%	78

Owner	0xb05d95422bf8d5024f9c340e8f7bd696d67ee3a9
Location	0x0000bcb9000322e25357094ea333d5b4834...05
Celestial Body	Level 7 Wasteland Planet
Planet Rank	Rank 5 (Galactic Stronghold)
HAT	None
Artifact	Pillar of Ek'sharrj
Silver to Next Rank	60175

Captain's Log

A pleasant, elastic biosphere.

Cliffs stretch across the view as far as a bear can walk. The atmosphere is cold. Flowers spread over the land. An uncannily human-like species of biped fill the ocean. The soil is

scouter

Hovering over:
(21687, 17039)
Space: Deep Space
Biome: Wasteland

miner

http://0.0.0.0:8000/mine - 3872 hashes/sec

http://192.168.1.11:8000/mine - 1303 hashes/sec

URL for explore server

Spiral

Dark Forest

AGENDA

01 ZKPs: Cryptographic Intro

02 Applications

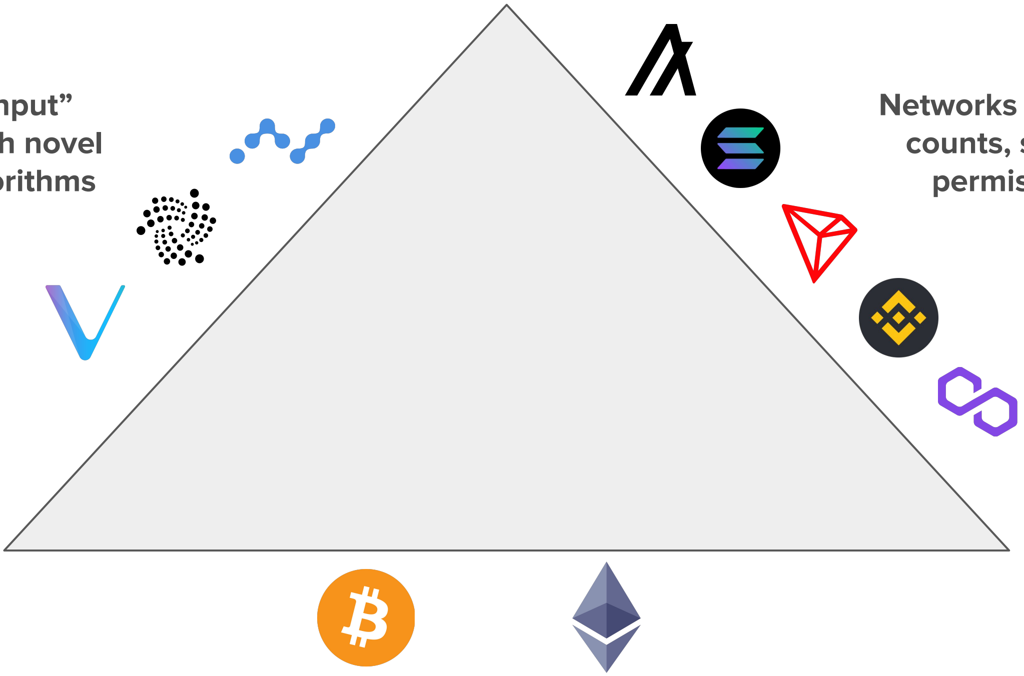
03 ZK-Rollups and Layer 2

04 Developer Ecosystems

05 Discussion

TOPIC

The Trilemma



Scalability

“High throughput” blockchains with novel consensus algorithms

Networks with low validator counts, such as DPoS or permissioned chains

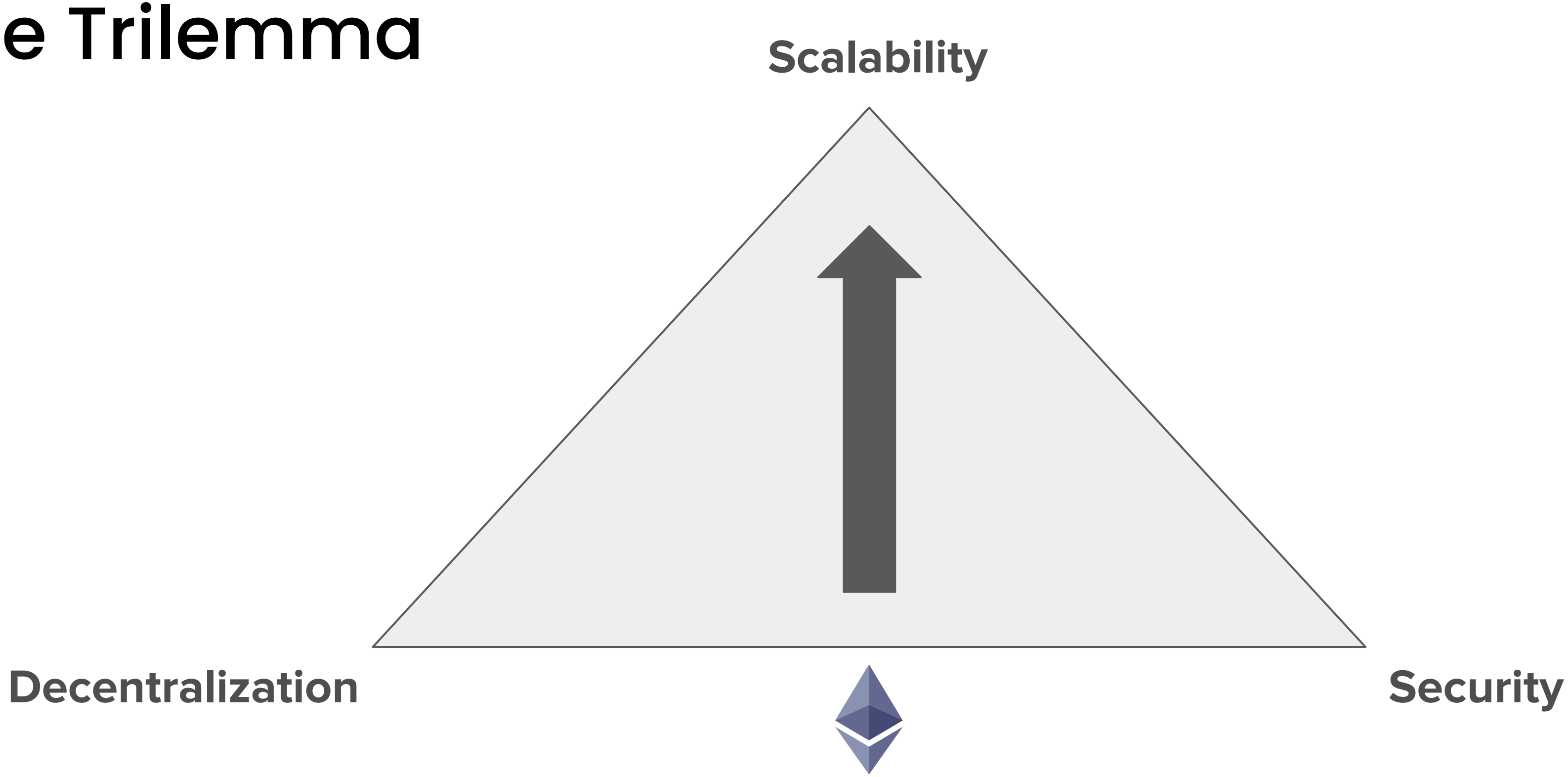
Decentralization

Security

Often PoW chains with strong monetary premium

TOPIC

The Trilemma



Often PoW chains with strong monetary premium

TOPIC

Why L2 Rollup + Sharding

- Layer 1 scaling: increase throughput -> harder to verify -> higher threshold for verifier -> more centralized -> less sustainable
- Technical sustainability
    - Whatever the most centralized of L1s can do, zkR can do much better, with significantly higher TPS. Further, multiple zk-rollups can effectively attain global scale in aggregate.
- Economic sustainability
    - Zk-rollups have a miniscule fraction of the cost overhead of a centralized L1, allowing it to offer orders of magnitude greater throughput with similar fees; or similar throughput with a fraction of the fees.
    - e.g. Solana yearly $36.5M revenue, $4B inflationary reward
- Conclusion
    - The blockchain industry does not yet possess the technology to achieve global scale.
    - Zk-rollups are the only solution that can scale to millions of TPS, attaining global scale, while remaining technically and economically sustainable. They can do this while remaining highly secure, decentralized, permissionless, trustless, and credibly neutral.

AGENDA

01 ZKPs: Cryptographic Intro

02 Applications

03 ZK-Rollups and Layer 2

04 Developer Ecosystems

05 Discussion

TOPIC

Developer Ecosystems

- Layer 2
  - Cairo by StarkWare
  - Zinc by Matter Labs (zkSync)
- ZK-SNARK
  - Circom by iden3, written in Rust
- ZK-EVMs
  - C, Rust, etc.
- ZK hardware acceleration

AGENDA

01 ZKPs: Cryptographic Intro

02 Applications

03 ZK-Rollups and Layer 2

04 Developer Ecosystems

05 Discussion

DISCUSSION

Some Interesting Directions for ZKP

- ZK-NFT
    - Yi Protocol
- ZK games
    - Interoperability
    - Test ground for under-collateralized lending?
    - Challenges
- ZK in pure social settings, such as a DAO
    - Whistleblower, manifested by Semaphore (used by Worldcoin)
        - Allows any Ethereum user to signal their endorsement of an arbitrary string, revealing only that they have been previously approved to do so, and not their specific identity
- etc.