BYONT

# ZERO-KNOWLEDGE PROOF

## PRESENTATION 1

BY VITALI BESTOLKAU AND IGNAS APSEGA

BYONT

# TABLE OF CONTENTS ...


1. Introduction: What is ZKP?
2. Verifier and Prover
3. ZKP Properties
4. ZKP TYPES
5. ZKP APPLICABILITY
6. ZKP EXAMPLES
    a. Ali Baba cave
    b. Color-blind friend
    c. 3-Colorable grap
7. Main Points
8. Summary
9. Q and A

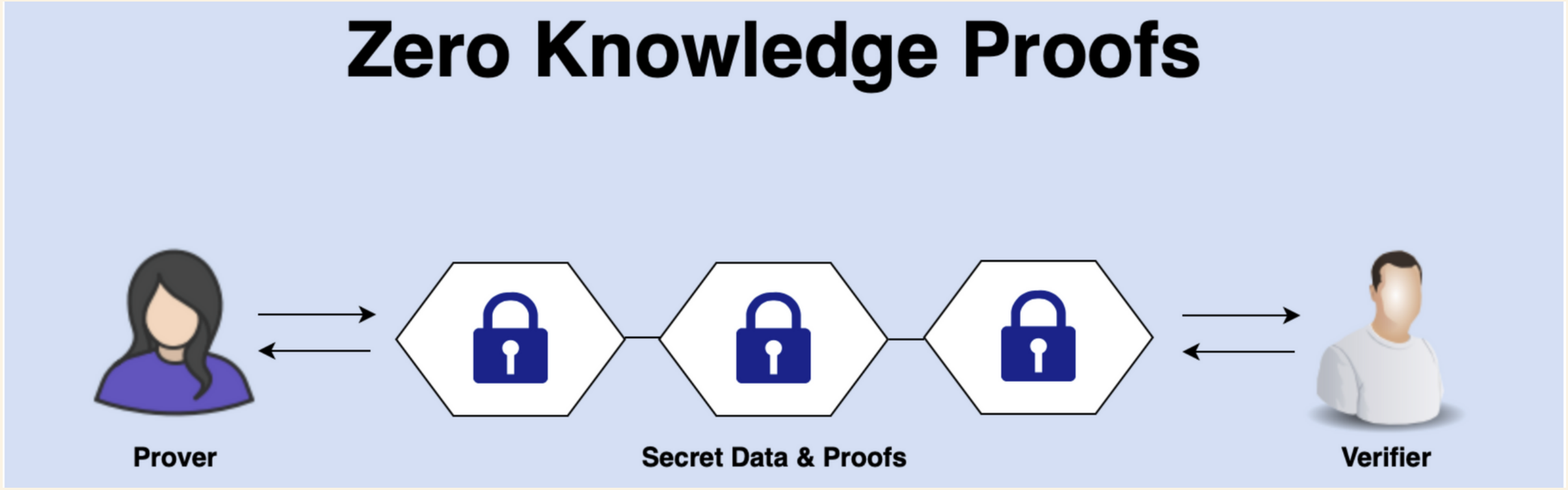
BYONT



# WHAT IS ZKP?

Zero-Knowledge Proof is a technique to define whether the provided information is true without revealing it.

# PROVER AND VERIFIER



BYONT



# ZKP PROPERTIES


COMPLETNESS


SOUNDNESS


ZERO KNOWLEDGE

BYONT



# ZKP TYPES

| | INTERACTIVE ZKP | NON-INTERACTIVE ZKP |
|---|---|---|
| Advantages | • Easy to execute | • Scalable<br>• Transferable |
| Disadvantages | • Limited Transferability<br>• Not scalable | • Requires a lot of computational power |

BYONT



# ZKP APPLICABILITY

ONLINE VOTING

COVIDPASS

LICENSE AND INSURANCE

PRIVACY/SECURITY/
CONFIDENTIALITY

PERFORMANCE
OPTIMISATION

ZK-STARKS, ZK-SNARKS

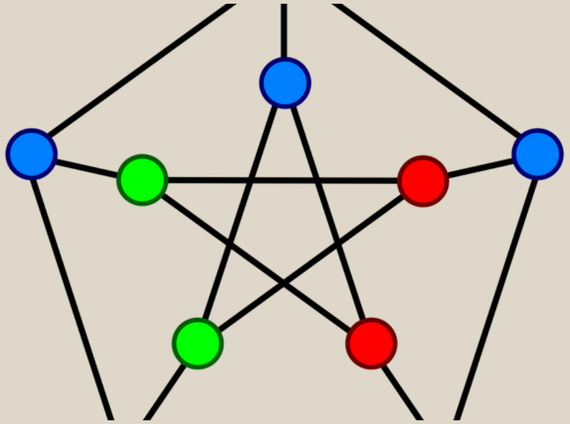
BYONT



# ZKP EXAMPLES

ALI BABA CAVE

COLOR-BLIND FRIEND



3-COLORABLE GRAPH

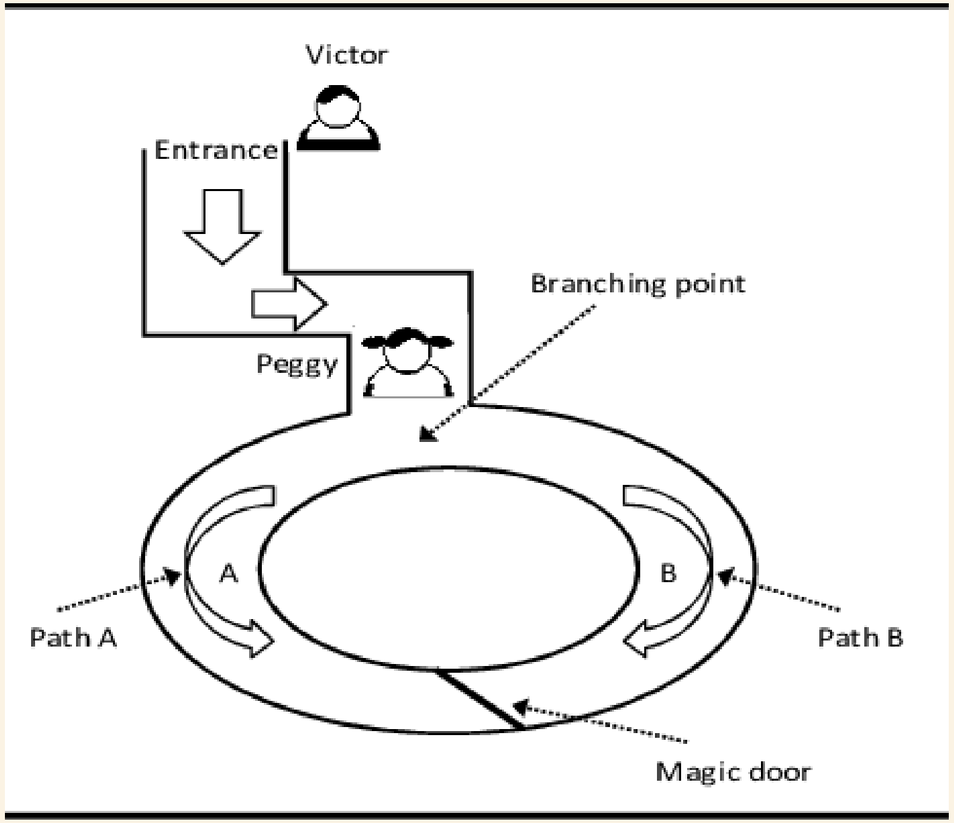
BYONT



# ALI BABA CAVE

Peggy is a prover, that wants to prove she knows a secret phrase for a magic door, Victor is a verify, who wants to verify that Peggy knows the phrase. That's what they do:

*Peggy enters the cave → Peggy takes a random path → Victor enters the cave → Victor shouts a name of a random path → Peggy returns using the path Victor shouted (in case she got unlucky and she didn't know the secret word, she would return by the other path).*
*Then they repeat this action until Victor is convinced that Peggy knows the phrase.*

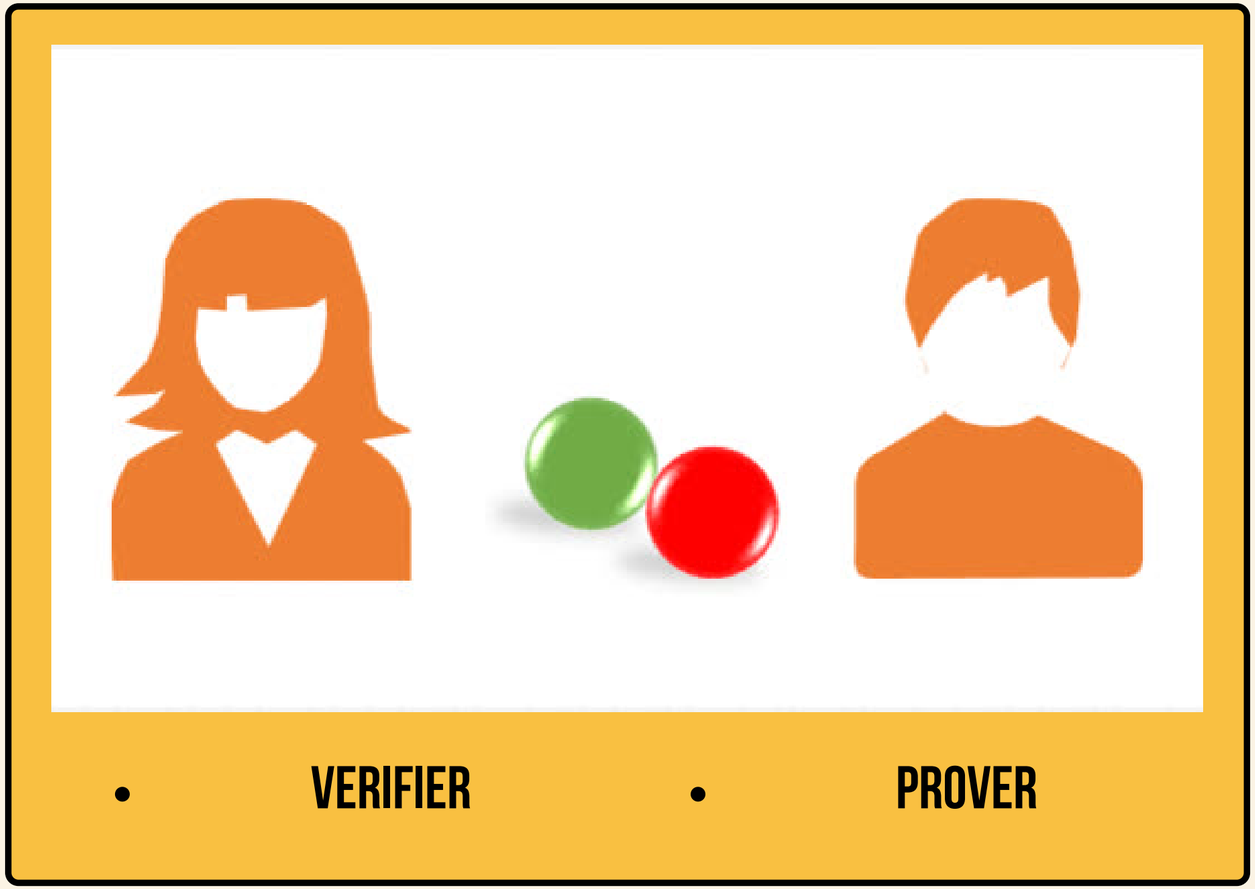


BYONT



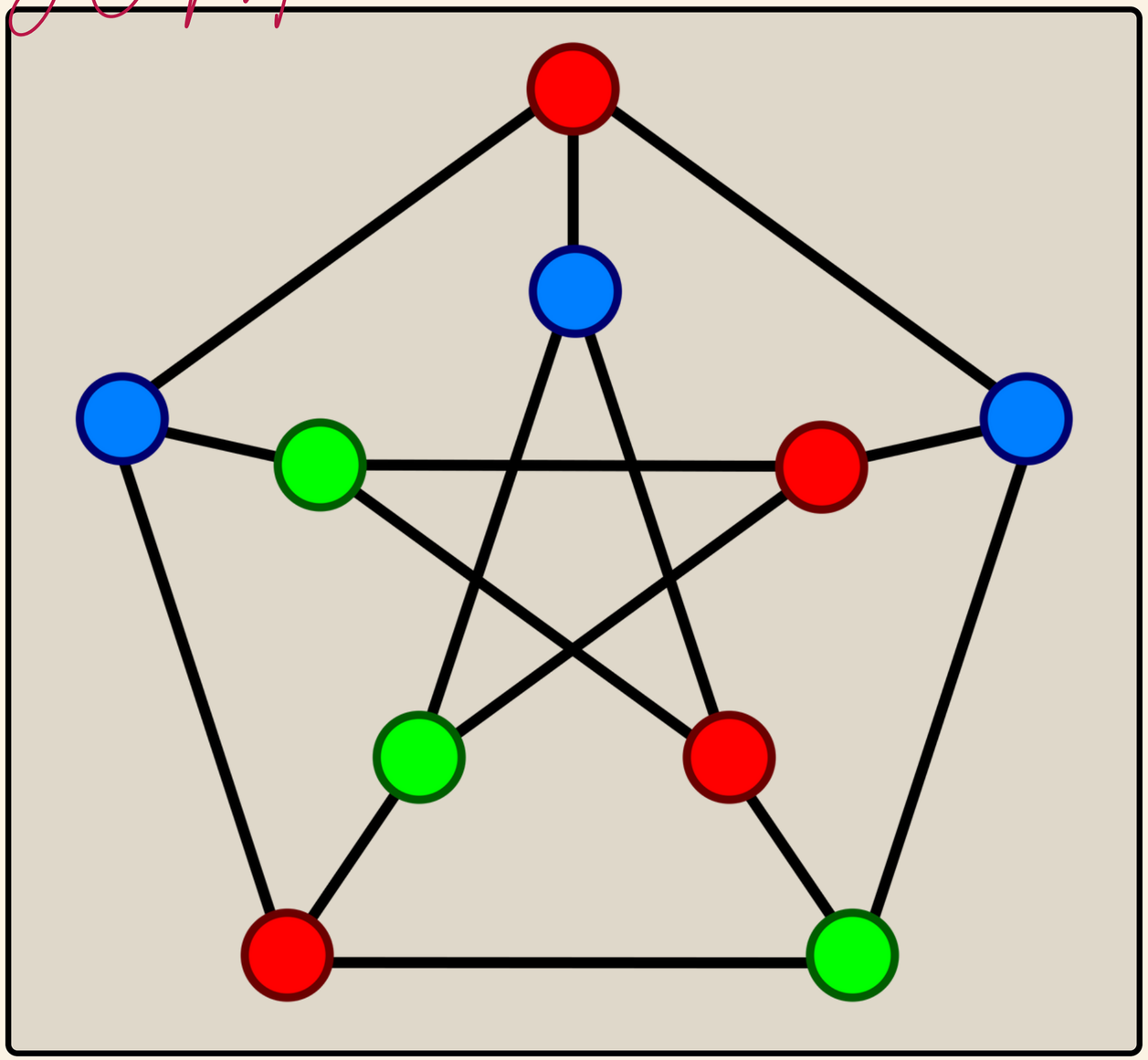
# COLOR-BLIND FRIEND

- A colorblind friend(verifier) has the balls
- Switches or the balls behind the back
- Asks the other friend(prover) if they switched the balls
- Repeat



BYONT





# 3-COLORABLE GRAPH

A verifier is provided with a graph with hidden vertices, and they need to verify that the graph is 3-colorable. They do the next thing:

- A verifier checks a single edge with connected vertices at a time.
- After every check, the colors change.
- Everything repeats until the verifier is convinced that the graph is 3-colorable.

Example: https://web.mit.edu/~ezyang/Public/graph/svg.html

BYONT



# MAIN POINTS

While using Zero-Knowledge Proof technique, a verifier never learns the information that should be verified.

In order to maximize the likelihood of the provided data to be true, a set of actions is repeated multiple times.

When using ZKP a verifier can never be 100% confident that the received information is true.

# SUMMARY

- Zero-Knowledge Proof is a technique to define whether the provided information is true without revealing it
- There are usually two main parties participating in ZKP: a prover and a verifier.
- The three main ZKP properties are Completeness, Soundness, and Zero-Knowledge.
- There are two types of ZKP: interactive and non-interactive.
- ZKP is able to bring privacy, confidentiality, scalability to the blockchain

# Q & A