Blog 1 Explanation Document

How it works and the Alibaba Cave Experiment

Zero-Knowledge Proof
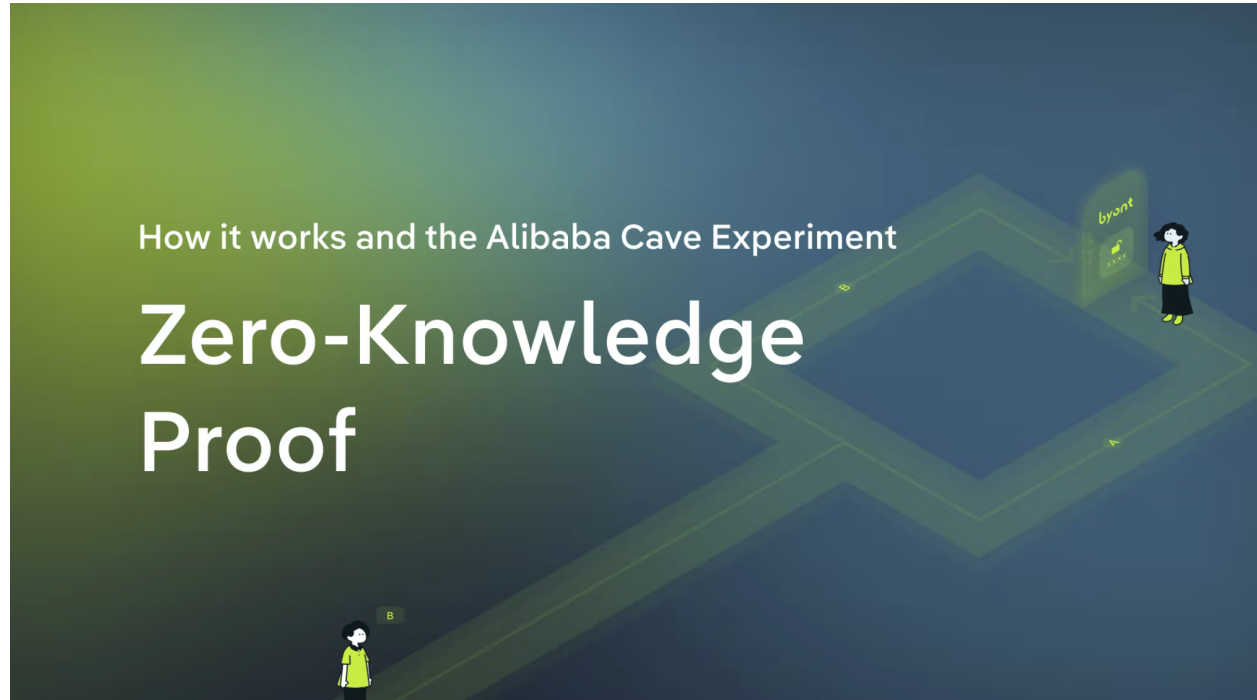
Introduction

The purpose of this document is to explain the research findings toward Zero-Knowledge Proof (ZKP). ZKP is seen as one of the best solutions regarding blockchain privacy issues. To understand its full potential and probable applicability, we decided to dive deeper into this subject, as this technology can also be the main tool for solving DAO privacy and management issues.

Reasoning

Before going in-depth with ZKP research, we needed to get a clear picture of how it works and where it can be (or where it is already) applied. That is why we decided on examples that could help get a better understanding of what Zero-Knowledge Proof is and why and how it is used.

Learning outcomes

After conducting needed research and writing this article, we learned:
- What ZKP is
- How it works
- ZKP application in real life and blockchain
- How it manages to protect data

Contribution

Vitali's part:

- What is Zero-Knowledge Proof?
- How do Zero Knowledge Proofs work?
- The Ali Baba cave example
- [Interactive Ali Baba cave example](#)

Ignas' part:

- Use-cases of Zero-Knowledge Proofs
- Real-life examples
- Blockchain examples

Joint part:

- Introduction to the series
- Recollection

Conclusion

As we've learned general knowledge about Zero-Knowledge Proof and how it works, we will proceed to go deeper and will learn about the main ZKP protocols and their implementation in the blockchain.